ÁLGEBRA

Una Introducción a la Aritmética y la Combinatoria

Ricardo Podestá y Paulo Tirao

Primera Edición
Marzo de 2017

"El álgebra es generosa; a menudo da más de lo que se le pide."
Jean Le Rond dÁlembert

Índice general

Prólogo

"Si no te gusta tu analista, visita a tu algebrista local."
Gert Almkvist

A partir de las notas de clase que oportunamente preparáramos para dictar la materia *Algebra I* de la Facultad de Matemática, Astronomía y Física (FaMAF) de la Universidad Nacional de Córdoba (UNC), durante las primeras mitades de 2012 y 2013, fuimos preparando un manuscrito que los alumnos conocieron como 'Notas de Algebra'. Este libro surgió como consecuencia natural de ese primer esfuerzo; corrigiendo, completando, reordenando y embelleciendo los contenidos y la presentación de dichas notas primigenias. En ese proceso las notas crecieron y maduraron hasta convertirse en un libro de texto que excede el contenido de un curso de un que ocupe la mitad del año.

La aritmética y las nociones básicas de la matemática discreta son muy adecuadas como un primer contacto con la matemática formal. Permiten introducir de manera bastante natural las formas y modos del quehacer matemático, la forma de escribir y enunciar en matemática, la forma de validar los "resultados" a través de demostraciones, la forma de definir objetos abstractos y construir teorías con ellos.

El libro puede usarse como libro de texto para un primer curso de álgebra o de matemática discreta dirigido a alumnos de grado sin experiencia previa en matemática. Dado todo el material disponible el curso podría ocupar la mitad del año o el año completo y puede orientarse a a grupos de alumnos con intereses distintos. Los tópicos presentados se desarrollan de manera completa y más o menos extensa; hay muchos ejemplos, ejercicios y problemas. Las elecciones posibles, para el profesor a cargo, son muy variadas.

El libro se ocupa de dos grandes temas: la *aritmética* y la *combinatoria*. La aritmética trata sobre distintos conjuntos numéricos, sobre sus operaciones y sus propiedades. También incluye un estudio más profundo sobre sus estructuras subyacentes. La combinatoria se presenta como el arte de 'contar sin contar', el arte de contar inteligentemente. Se presentan métodos y formas de pensar novedosas, distintas de las utilizadas en aritmética, pero complementarias.

El trabajar estas dos áreas en un mismo curso da una perspectiva sobre el dinamismo de la matemática y cómo áreas diferentes, con caracterísitcas propias bien definidas interactuan enriqueciéndose mutuamente.

El lector notará, sin embargo, que hemos dedicado una buena parte del libro, la primera, a los fundamentos de la matemática. En nuestra experiencia docente hemos notado que un

grave déficit en la comprensión de los curso inciales (y de la matemática en general), por parte de los alumnos, es la falta de manejo en lo que se refiere a la lógica de los enunciados, las demostraciones y a objetos básicos como los conjuntos y las funciones. Esto da una base firme para el estudio y la comprensión del resto del libro (¡y de la matemática!).

Los *objetivos* principales de este curso se pueden resumir en los 3 aspectos siguientes:

- Aprender a aprender matemática.
- Aprender a hacer matemática.
- Aprender aritmética y combinatoria.

El primero implica el desarrollo de la capacidad de leer definiciones y enunciados matemáticos, de comprender cómo son sus objetos y descubrir cómo sus verdades se articulan entre sí.

El segundo objetivo es de central importancia, ya que el hacer algo de matemática por uno mismo es uno de los mejores caminos para aprender matemática. Estudiar matemática es un proceso activo, que requiere mucho esfuerzo, mucha práctica y mucha constancia por parte de quien lo acomete. Una parte importante del "hacer" matemática es una actividad individual, pero que se enriquece enormemente con el intercambio de ideas con otros colegas que hacen matemática. Es muy conveniente hacerse y contestarse preguntas a uno mismo además de hacer y contestar preguntas a los otros.

Vamos a decirlo una vez mas, es fundamental plantearse siempre nuevos interrogantes, aunque no tengamos idea de la respuesta. Esto nos llevará a entender lo que estamos estudiando, a reforzar lo que ya sabemos y, primordialmente, a generar nuevas ideas.

Por último, y muy importante desde lo práctico, está el aprender contenidos específicos. En el camino que lleva a aprender estos contenidos se aprende, lentamente, a aprender y a hacer matemática.

En este libro conviven, intencionalemnte, lo *riguroso*, que a veces resulta algo tedioso y se sospecha no demasiado útil, con lo *práctico*, listo para usar, que a veces puede dejar la sensación de falta de fundamento o de ser algo impreciso. Ambos modos se complementan para facilitar el aprendizaje de cada tema expuesto, con todos los fundamentos y rigor necesarios pero también desarrollando habilidades prácticas para poder usar con confianza lo aprendido.

Es nuestro deseo que éste libro les resulte útil y práctico, y que su lectura sea amena. Es un libro pensado para estudiar, pero tambien para consultar y deleitarse luego de haber rendido la materia. Esperamos que los aliente a trabajar duro y con mucho entusiasmo, para que puedan disfrutar de aprender y aprender a disfrutar del álgebra.

Ricardo y Paulo, Córdoba, 13 de marzo de 2017.

Introducción

"En teoría, no hay diferencia entre la teoría y la práctica, pero en la práctica si la hay"
Jan L. A. van de Snepscheut

Este libro está orientado a estudiantes universitarios de grado de carreras afines con la matemática o que precisan de ella. Es asequible para aquellos con poca o ninguna experiencia previa en el estudio sistemático de la matemática. Puede ser usado como libro de texto de diversos de cursos introductorios de Álgebra y Matemática Discreta. Eligiendo adecuadamente algunos capítulos y secciones es posible dar cursos distintos y con orientaciones diferentes. El libro completo contiene mucho material, suficiente para dos cursos de medio año completos.

Es un libro introductorio a la matemática misma. Muestra desde las primeras páginas formas claras sobre la presentación de objetos matemáticos nuevos y la manera de construir conceptos matemáticos. Estimula actitudes orientadas para que cada uno haga matemática por sí mismo. Incluye numerosos ejemplos, algunos desarrollados extensamente y en profundidad, y todos los capítulos incluyen ejercicios que facilitan la interacción con los temas presentados y también algunos problemas que desafían al lector y cuyas soluciones pueden ser no tan fáciles de encontrar.

Esta introducción al estudio de la aritmética y la combinatoria consta de cuatro partes:

Parte I. **Fundamentos**

Parte II. **Números y aritmética**

Parte III. **Aritmética modular**

Parte IV. **Combinatoria**

Las segunda y cuarta partes pueden ser el núcleo de un curso típico de aritmética y combinatoria. La primera parte, de fundamentos, puede ser complementaria en la mayoría de los casos. Puede servir de repaso en algunos casos o de referencia para aquellos que no tengan los fundamentos básicos sólidamente incorporados. La tercera parte es algo más avanzada y puede servir como introducción a las estrcuturas algebraicas.

Contenidos específicos

En "Fundamentos", además de un presentación breve de conjuntos, relaciones y funciones, hay un capítulo referido a los enunciados y a la demostración en matemática. Para

alumnos sin ninguna experiencia previa creemos que vale la pena leerlo y reflexionar sobre su contenido, ya que sin dudas les será de gran ayuda para el primer curso de matemática que tomen y toda otra actividad matemática que hagan.

En la segunda parte, "Números y aritmética", comenzamos discutiendo los números reales y su aritmética combinando un punto de vista axiomático y uno pragmático aprovechando lo que todos conocemos sobre ellos. Hacemos varias referencias a los racionales y su aritmética en relación con la de los reales. Esta sección es muy instructiva, y por ser la primera requiere un esfuerzo especial. Continuamos con los naturales, que luego de una breve introducción, dan paso al principio de inducción. Una herramienta básica fundamental en la matemática toda. La aprehención de esta herramienta lleva tiempo y requiere de mucha práctica. Esta sección tiene muchos ejemplos y ejercicios que recomendamos enfáticamente.

Luego discutimos la muy rica aritmética entera, empezando con el concepto fundamental de divisibilidad. Estudiamos el máximo común divisor, el mínimo común múltiplo, los números primos y la notación decimal para enteros. También hay una sección dedicada al sistema binario de representación.

Finalmente, hay un capítulo dedicado a un primer encuentro con los números complejos, algo que puede ser novedoso para algunos.

En la tercera parte nos ocupamos de la "Aritmética modular". Primero introducimos la noción de números congruentes módulo un entero m. Esto da lugar a la relación de congruencia. Estudiamos las congruencias módulo m y sus propiedades. Esta es una idea de Gauss que ha resultado ser sumamente fecunda, ya que simplifica sobremanera muchos tipos de cálculos que de otra manera serían muy tediosos. La aplicación más sencilla de éstas son las reglas de divisibilidad, pero algoritmos famosos de encriptación para seguridad de datos se basan en ellos. Las clases de equivalencia de las congruencias dan lugar a los enteros modulares y con ellos toda una nueva aritmética, la aritmética modular. haciendo una analogía, podriamos decir que se trata de al aritmética de los relojes de m horas. Este es un tópico nuevo que requiere cierto grado de abstracción y constituye un primer ejemplo de objetos y teoría matemática un poco más abstracta que la que el lector probablemente conoce. finalmente nos planteamos el problema de resolver ecuaciones lineales de congruencia, ya sea una sola o un sistema de ellas.

La cuarta parte, "Combinatoria", es distinta de las anteriores. Esta area usa técnicas y métodos distintos a los que estamos acostumbrados, y aceptar o entender esto suele ser la principal dificultad. El tema principal es el de *conteo sin contar*. Es decir, determinar de cuántas formas puede ocurrir un suceso sin tener que enumerar cada uno de los casos posibles (que casi siempre son muchos). Más que aprender una gran cantidad de resultados, presentamos distintas estrategias generales de conteo para estimular el desarrollado de habilidades para contar adecuademente. Las situaciones arquetípicas, presentadas a través de ejemplos, ayudan mucho a este fin. Es necesario en este punto tener muy claro el concepto de biyección entre dos conjuntos y tener cierta madurez para escribir de manera clara argumentos a veces sofisticados.

Organización

Cada una de las cuatro partes está organizada en capítulos y secciones, y dentro de ellas se distinguen claramente las definiciones, los párrafos explicativos y los resultados, además de ejemplos y notas que facilitan la compresión de lo expuesto.

A lo largo de las notas usaremos distintos rótulos para facilitar su lectura.

- Definición. Es una descripción completa y precisa de un objeto o concepto matemático nuevo.
- Lema. Generalmente, precede a una proposición o teorema. Es un resultado generalmente técnico, necesario como parte de un argumento de un resultado más importante.
- Proposición. Es un resultado importante en sí mismo, aunque puede referirse a algo particular y cuyo enunciado puede requerir elementos definidos recientemente en el contexto en el que se enmarca.
- Teorema. Es un resultado importante en sí mismo de carácter general que muchas veces engloba resultados previos necesarios para su demostración o resultados menores o particulares ya establecidos. Su enunciado es en general comprensible en términos ampliamente conocidos en la teoría en la que se enmarca.
- Corolario. Es un resultado que se deriva directa y, en general, fácilmente de una proposición o teorema.
- Demostración. Es la prueba de un resultado, y siempre aparecen a continuación de un enunciado matemático, es decir después lemas, proposiciones, teoremas y corolarios. Como es estándar en matemátoica, indicamos el fin de una prueba con el símbolo □ a la derecha del último renglón.
- Observación. Las observaciones son de carácter preciso y riguroso, sirven para complementar o completar un concepto o resultado matemático presentado.
- Nota. Bajo este título aparecen comentarios de diversa índole sobre algún aspecto de lo tratado.
- Nota histórica. Es una nota de carácter histórico referida a los conceptos matemáticos tratados o a matemáticos famosos relacionados con los mismos.
- Notación. Bajo este título se introducen nuevas formas de denotar o nombrar objetos matemáticos ya definidos.
- Convención. Es un acuerdo sobre el uso o abuso de alguna notación específica, sobre la extensión de una definición o concepto ya existente o sobre algún aspecto praćtico que simplifique el quehacer matemático.
- Ejemplos. Un ejemplo es una instancia particular concreta de algún resultado o fenómeno estudiado. Puede ser útil para entender más claramente alguna de las razones de la validez del mismo o para entender en qué marco o bajo que hipótesis vale. En

muchos casos indicaremos el final de un ejemplo con el símbolo ◊ a la derecha del último renglón.

- Digresión. Es una nota de color que puede no ser parte de la exposición, aunque ilustra algún aspecto interesante relacionado con la misma.

En todo el libro hay secciones complementarias marcadas con una daga † y otras con una doble daga ‡. Ninguna forma parte del núcleo de los contenidos desarrollados, en general no son necesarias para lo que sigue y por lo tanto pueden ser omitidas sin causar dificultades posteriores. Para aquellos curiosos con deseos de pronfundizar lo que están aprendiendo puede resultarles instructivo leerlas y dedicarles algún tiempo a entenderlas. Aquellas marcadas con ‡ pueden resultar más difíciles ya que pueden requerir mayor abstracción y madurez. En ellas en general se discuten temas más avanzados, con herramientas y demostraciones más sofisticadas.

Al final de cada capítulo hay una lista de ejercicios y una lista de problemas. Los ejercicios sirven para que el lector trabajando por sí mismo incorpore lo aprendido. En general deberían ser accesibles con lo expuesto en el capítulo. En cambio los problemas pueden requerir un esfuerzo intelectual mayor y entrenamiento en la resolución de problemas.

Parte I

Fundamentos

En matemática la noción de verdad es absoluta. Éste es un aspecto fundamental y distintivo de la matemática respecto de toda otra ciencia.

Históricamente la lógica matemática y los fundamentos de la matemática son las áreas encargadas de construir el marco para desarrollar la matemática sin contradicciones y con una noción de verdad inequívoca.

En esta primera parte presentamos algunos aspectos de los fundamentos de la matemática que están presentes en todas las ramas de la matemática.

Por un lado presentamos algunas nociones de lógica proposicional y discutimos la implicación lógica como medio para validar los resultados en matemática. En este marco también discutimos aspectos de las demostraciones en matemática, elemento fundamental del quehacer matemático.

Por otro lado presentamos las nociones básicas de la teoría de conjuntos, y aspectos elementales sobre relaciones y sobre funciones, todos éstos objetos que se encuentran en los cimientos de la matemática.

Capítulo 1

Enunciados y demostraciones

"La lógica es la anatomía del pensamiento."
John Locke, filósofo inglés (1632 – 1704)

Una parte del quehacer de los matemáticos consiste en construir los "objetos" de la matemática (e.g. números, conjuntos, funciones, relaciones, figuras geométricas, anillos, espacios topológicos) y reglas de juego claras para ellos, para luego estudiar sus propiedades y describir y explicar los patrones que rigen su funcionamiento.

El hacer preguntas es una actitud muy natural en matemática, que promueve el descubrimiento. Las afirmaciones matemáticas, y en particular las respuestas a las preguntas que se plantean, deben ser enunciadas sin ambiguedad alguna. Es decir, estos enunciados deben tener un valor de verdad bien definido, que sólo puede ser verdadero o falso. El conocimiento matemático se expresa a través de enunciados, llamados teoremas, que describen las verdades de la matemática. La manera de validar estos teoremas es a través de la demostración.

En este capítulo describimos someramente algunos aspectos sobre los enunciados de la matemática y presentamos algunas formas usuales de demostraciones que serán usadas a lo largo de todo el libro. El contenido de este capítulo forma parte de la *lógica matemática*.

1.1. El lenguaje coloquial y el lenguaje matemático

Frases como "tengo 35 años", "nunca estuve en Francia", "alguna vez comí jabalí", "todos mis hermanos terminaron el secundario" no generan duda sobre su significado. Todos entendemos lo mismo. Está claro que pude haber comido jabalí una sola vez, o quizás fueron dos o cinco. Y si mis hermanos son Rafael, Diego y Marcos, está completamente claro que Rafael terminó, Diego terminó y Marcos también terminó.

Ahora, frases como "en la fiesta estaban todos los amigos de Juli y Renata" o "me iban a dar oficina nueva y un aumento o más vacaciones y cumplieron!" pueden dar lugar a distintas interpretaciones. ¿La primera frase dice que en la fiesta estaban todos los amigos que tienen en común las dos chicas o que estaban todos los amigos de Juli y además también estaban todos los amigos de Renata? O incluso, ¿estaban todos los amigos de Juli y además Renata? Agus, que es amigo de Renata pero no de Juli, ¿estaba o no?

De la segunda frase, ¿entendemos que le dieron todo, o que le dieron quizá sólo más vacaciones, o quizá oficina y un aumento, u oficina y más vacaciones? ¿Entendemos que en cualquier caso le dieron oficina nueva?

La manera en que está usado el lenguaje en estas frases da lugar a estas distintas interpretaciones. Es posible escribirlas de otra forma para que tengan un sentido preciso, aquel que querramos trasmitir. Por ejemplo, si queremos decir que en la fiesta estaban todos los amigos que tienen Renata y Juli en común, no como Agus, podemos decir: "en la fiesta estaban todos los amigos de Juli que también son amigos de Renata", "estaban los que son amigos de ambas" o simplemente "en la fiesta estaban todos los amigos que tienen Renata y Juli en común". En cambio, si queremos decir que estaban todos los amigos de Juli y también todos los amigos de Renata podemos decir: "estaban todos los que son amigos de Renata o de Juli", "estaban todos los amigos de Juli y todos los amigos de Renata" o simplemente "estaban todos los amigos de Juli y también todos los amigos de Renata". En todos los casos hicieron falta frases más largas para ser más claros. En el lenguaje coloquial, muchas veces, para simplificar las frases se resigna su precisión a tal punto de resultar confusas.

Los enunciados en matemática no deben tener distintas interpretaciones. Para esto existen reglas claras y precisas para escribir los enunciados en matemática. Estas reglas ayudan a decidir si un enunciado es falso o verdadero. Por ejemplo, consideremos los enunciados:

- "Ningún par es divisible por 3".
- "No todos los pares no son divisibles por 3".

Nadie duda de que el primer enunciado es FALSO. El 6 es par y es divisible por 3. El segundo enunciado es más complicado de entender. ¿Es falso o verdadero? Para decidir es conveniente redactarlo de otra forma. Reescribimos los dos enunciados así:

- "No hay ningún número par divisible por 3".
- "Hay números pares divisibles por 3".

Debe quedar claro que estos enunciados y los de más arriba dicen lo mismo. En el caso de "No todos los pares no son divisibles por 3" y "Hay números pares divisibles por 3", el primer enunciado afirma que no todos los pares tienen cierta propiedad, la de no ser divisible por 3, que es lo mismo que decir que algún par si la tiene. Ahora si es claro que que el segundo enunciado es VERDADERO. El 6 es par y es divisible por 3.

En las segundas redacciones de los enunciados considerados están explícitas las reglas básicas para escribir enunciados en matemática. Éstas se refieren al uso de las conjunciones "y" y "o", al uso de la negación "no" y al uso de los cuantificadores "para todo" y "hay".

1.2. Proposiciones, conectivos y tablas de verdad

En lógica, una *proposición* es un enunciado declarativo con un valor de verdad bien definido, que sólo puede ser *verdadero* (V) o *falso* (F), pero no ambos o ninguno de ellos. En

general usaremos las letras p, q y r para referirnos a proposiciones de este tipo, y encerraremos entre comillas el enunciado de dicha proposición.

Ejemplos. Los siguientes enunciados son proposiciones:

(1) p : "2+2=4" (V)

(2) q : "7 es un número par." (F)

(3) r : "Borges escribió el libro *Ficciones*." (V)

Entre paréntesis hemos indicado con V o F si la proposición es verdadera o falsa. ◊

Sin embargo, no son proposiciones las órdenes, preguntas y exclamaciones como "che", "¡hola!", "¡fuera de aquí!", "compra 5 kilos", "¡qué bien!", "¿vas a volver?". Tampoco resultan proposiciones aquellos enunciados en que el valor de verdad puede cambiar según quien lo interprete o cuándo se lo interprete.

Ejemplos. Los siguientes enunciados no son proposiciones.

(1) *"Los lunes llueve"*. Este enunciado será verdadero algunos días lunes en algún lugar, mientras que será falso otros días lunes y en otros lugares; su valor de verdad cambia con el tiempo y con el lugar, luego no es una proposición.

(2) *"Es un día hermoso"*. Este enunciado depende de la apreciación personal de quien lo dice. Por ejemplo, un día lluvioso puede ser hermoso para algunos y no serlo para otros. Aquí, el valor de verdad del enunciado cambia según la persona.

(3) "$x - y > 0$". Aun asumiendo que x e y son números reales, el enunciado depende de los valores de x e y. Para algunos valores de x e y es verdadero y para otros es falso. Por ejemplo, si $x = 3, y = 1$ entonces $x - y > 0$ es V, y si $x = 1, y = 5$ entonces $x - y > 0$ es F. ◊

Observación. Si "cuantificamos" la frase $x - y > 0$ y determinamos un "universo" (es decir un conjunto en el que x, y "vivan"), ésta puede convertirse en una proposición bien definida:

- Para todo par de números reales x e y, $x - y > 0$.
- Existen números enteros negativos x e y tales que $x - y > 0$.
- No hay ningún par de primos x e y tales que $x - y > 0$.

Estas proposiciones son respectivamente F, V y F.

1.2.1. Negación, conjunción y disyunción

Al igual que en el lenguaje ordinario es posible combinar diferentes proposiciones usando *conectivos lógicos* para formar nuevas proposiciones y así, a partir de proposiciones simples, construir otras más complejas. Hay tres conectivos lógicos básicos:

- la NEGACIÓN: "no", en símbolos "$\neg$";
- la CONJUNCIÓN: "y", en símbolos "$\wedge$";
- la DISYUNCIÓN: "o", en símbolos "$\vee$".

Si p es cualquier proposición, su negación, que se lee "no p" y se denota por

$$\neg p$$

se define como la proposición cuyos valores de verdad son opuestos a los de p. Es decir, $\neg p$ es verdadera exactamente cuando p es falsa y viceversa.

Dadas dos proposiciones p y q, la conjunción de p con q, denotada por

$$p \wedge q$$

que se lee "p y q", es una nueva proposición que es verdadera cuando p y q son ambas verdaderas y es falsa en todo otro caso.

Y la disyunción de p con q, denotada por

$$p \vee q$$

que se lee "p ó q", es una nueva proposición que es falsa cuando p y q son ambas falsas y es verdadera en todo otro caso.

La negación en un conectivo *unario*, que a partir de una proposición p construye otra $\neg p$, mientras que la conjunción y la disyunción son conectivos *binarios*, ya que a partir de dos proposiciones p, q construyen una tercera $p \vee q$ y $p \wedge q$, respectivamente.

La conjunción y la disyunción satisfacen dos leyes muy importantes:

- Asociatividad:

$$\begin{aligned} p \wedge (q \wedge r) &= (p \wedge q) \wedge r \\ p \vee (q \vee r) &= (p \vee q) \vee r \end{aligned} \tag{1.1}$$

- Distributividad:

$$\begin{aligned} p \wedge (q \vee r) &= (p \wedge q) \vee (p \wedge r) \\ p \vee (q \wedge r) &= (p \vee q) \wedge (p \vee r) \end{aligned} \tag{1.2}$$

Gracias a la asociatividad podemos escribir sin ambigüedad $p \wedge q \wedge r$ y $p \vee q \vee r$ sin usar paréntesis.

1.2.2. Proposiciones compuestas y tablas de verdad

Una *proposición compuesta* es una proposición construida a partir de otras usando conectivos lógicos, como por ejemplo las expresiones en (1.1), (1.2), o $(\neg p \wedge q) \vee r$.

El valor de verdad de un proposición compuesta depende únicamente de los valores de verdad de sus componentes. Cada conectivo tiene una tabla de verdad que expresa esta dependencia.

Una *tabla de verdad* de una proposición compuesta es una tabla en la que se listan todas las posibles combinaciones de valores de verdad de cada una de las componentes de la proposición y los correspondientes valores de verdad de la proposición compuesta.

Por ejemplo, la tabla de verdad de la negación es simplemente

p	$\neg p$
V	F
F	V

(1.3)

mientras que las tablas de verdad de la conjunción y la disyunción están dadas por

p	q	$p \wedge q$	$p \vee q$
V	V	V	V
V	F	F	V
F	V	F	V
F	F	F	F

(1.4)

Estas tablas de verdad expresan lo que representan la conjunción y la disyunción como operaciones lógicas. Ambas existen también en el lenguaje cotiadiano con un significado muy similar.

Nota. En el lenguaje coloquial, el uso del "o" como disyunción puede tener un significado algo distinto, ya que a veces se usa de manera excluyente. Por ejemplo, cuando un padre dice "te compro el helado o el licuado", tiene claro que sólo comprará una de las dos cosas y no ambas; en ese caso el "o" es excluyente. Pero cuando dice "pediré panqueques o café", entiende no se excluye la posibilidad de pedir ambas cosas. Sin embargo, en matemática, la disyunción es siempre inclusiva ¡por definición!. Si es un matemático el que le dice a su hijo "te compro el helado o el licuado" probablemente termine comprando ambos[*].

Cuando haga falta considerar una disyunción excluyente bastará con decir "p ó q, pero no ambas".

Es importante saber negar una proposición compuesta, en particular las conjunciones y disyunciones. Usando las tablas (1.3) y (1.4) podemos escribir las tablas de verdad de las negaciones $\neg(p \wedge q)$ y $\neg(p \vee q)$. Resulta

p	q	$\neg(p \wedge q)$	$\neg(p \vee q)$
V	V	F	F
V	F	V	F
F	V	V	F
F	F	V	V

(1.5)

[*]Un conocido matemático fue padre, y al preguntarle "¿es nene o nena?" éste respondió "si, claro".

Ejemplo. En el siguiente ejemplo, tanto la conjunción "y" como la disyunción "o", tienen el mismo sentido que para la lógica proposicional.

Ayer que no trabajé, quería hacer algo distinto; pensé en ir al cine y en ir a cenar con amigos.

Ante la pregunta "¿hiciste lo que querías?", la respuesta depende del sentido de la frase anterior. Más precisamente, la frase anterior podría tener alguno de lo siguientes dos sentidos:

- Pensé hacer ambas cosas juntas, ir al cine y a cenar con amigos.
- Pensé hacer al menos una de las dos.

Para formalizar esto consideremos las proposiciones

$$\begin{aligned} p &: \text{"}\textit{fui al cine}\text{"}, \\ q &: \text{"}\textit{fui a cenar}\text{"}, \end{aligned}$$

y consideremos las situaciones

$$\begin{aligned} p \wedge q &: \text{"}\textit{fui al cine y a cenar}\text{"}, \\ p \vee q &: \text{"}\textit{fui al cine o a cenar}\text{"}. \end{aligned}$$

En la primera situación, las posibles respuestas son:

- SI, fui al cine y luego a cenar con amigos.

- NO, fui al cine, pero me volví a casa luego.

- NO, no fui al cine pues llegué tarde, pero fui a cenar con amigos.

- NO, al final me quedé en casa, no fui al cine ni a cenar con amigos.

En la segunda situación, respuestas posibles son:

- SI, fui al cine y luego a cenar con amigos.

- SI, fui al cine, aunque me volví a casa luego.

- SI, no fui al cine pues llegué tarde, pero fui a cenar con amigos.

- NO, al final me quedé en casa, no fui al cine ni a cenar con amigos.

En fin, cosas de la vida. ◊

Observación. Dadas dos proposiciones cualesquiera p y q, entonces, a priori, se podrían definir tantas proposiciones nuevas y distintas como tablas de verdad distintas hay. Como p y q tienen 2 valores posibles de verdad, y estos se combinan en VV, VF, FV y FF, habrá 16 proposiciones compuestas $P(p, q)$ a partir de 2 proposiciones cualesquiera p y q. Éstas corresponden a los valores

$$\begin{aligned} &\text{VVVV}, \quad \text{VVVF}, \quad \text{VVFV}, \quad \text{VFVV}, \quad \text{FVVV}, \quad \text{VVFF}, \quad \text{VFVF}, \quad \text{VFFV}, \\ &\text{FVVF}, \quad \text{FVFV}, \quad \text{FFVV}, \quad \text{VFFF}, \quad \text{FVFF}, \quad \text{FFVF}, \quad \text{FFFV}, \quad \text{FFFF}. \end{aligned}$$

Hemos visto 4 de ellas: $p \wedge q$, $p \vee q$, $\neg(p \wedge q)$ y $\neg(p \vee q)$. También es claro que $p \vee \neg p$ y $p \wedge \neg p$ dan VVVV y FFFF, respectivamente. ¿Se anima a encontrar las que faltan?

1.3. Condicionales y equivalencia

Presentamos ahora otro tipo de proposiciones compuestas, los condicionales y bicondicionales, sus recíprocas y contrarrecíprocas.

1.3.1. La proposición condicional

Dadas dos proposiciones p y q, se define una nueva proposición compuesta llamada *condicional* o *proposición condicional* denotada por

$$p \to q$$

que se lee "si p entonces q". Decimos que p es el *antecedente*, *premisa* o *condición suficiente* y que q es el *consecuente*, *conclusión* o *condición necesaria* del condicional. La tabla de verdad del condicional es, por definición, la siguiente:

p	q	$p \to q$
V	V	V
V	F	F
F	V	V
F	F	V

(1.6)

Es decir, el condicional es falso sólo cuando la premisa es verdadera y la conclusión es falsa.

En el lenguaje coloquial, la proposición condicional $p \to q$ se expresa de varios modos distintos, entre ellos:

- "si p, q" o "q si p."
- "q cuando p", "q siempre que p".
- "p solo si q."
- "p implica q."
- "q se sigue de p."
- "q pues p", "q puesto que p."
- "q a condición de p."
- "p es (condición) suficiente para q."
- "q es (condición) necesaria para p."

No es tan común usar la expresión "q sólo si p" en el lenguaje coloquial como sinónimo de "si p entonces q" ya que puede causar confusión.

Nota. En el condicional no existe necesariamente la relación de causa-efecto entre el antecedente y el consecuente. Conviene tener presente esto para no confundirse con la implicación que discutiremos más adelante. Son dos cosas distintas aunque tienen mucho que ver, tanto que ya hemos dicho que el uso permite referirse al condicional $p \to q$ como "p implica q".

Ejemplos. Las siguientes son algunas instancias en el lenguaje coloquial de las 4 situaciones posibles. Dado que en el lenguaje coloquial tendemos a forzar la relación causa-efecto, algunas de estas situaciones nos resultan sin sentido o confusas.

(1) Antecedente y consecuente verdaderos. En el condicional *"si como mucho, entonces engordo"* hay una relación de causa y efecto; pero en el condicional *"si 2 es par, entonces Gauss fue matemático"* evidentemente no; ambas cosas son ciertas, pero la paridad de 2 no implica la profesión de Gauss. Ambos condicionales son verdaderos.

(2) Antecedente verdadero y consecuente falso. En este caso el condicional es falso. Podemos pensar informalmente en este caso como el de "una promesa rota". Por ejemplo, si un padre le dice a un hijo: *"si te portas bien, te compraré una golosina"* y luego, habiéndose portado bien el niño, éste no cumple con el regalo (promesa rota). El condicional es falso.

(3) Antecedente falso y consecuente verdadero. Aunque puede resultar contrario a la intuición, los condicionales "si 1=2, entonces 2=2" y "si las manzanas son azules, los tomates son rojos" son verdaderos.

(4) Antecedente y consecuente falsos. En el lenguaje coloquial se usa para enfatizar algo improbable: "si Arjona es músico, yo soy Gardel"; "si tu hermano juega bien al fútbol, entonces yo soy D1eg0". En ambos casos el condicional es verdadero. ◊

1.3.2. Recíproca, contraria y contrarrecíproca

Dada una proposición condicional

$$p \to q$$

se definen tres proposiciones asociadas: la recíproca, la contraria y la contrarrecíproca. La *recíproca* de $p \to q$ es

$$q \to p$$

que puede escribirse $p \leftarrow q$; la *contraria* es

$$\neg p \to \neg q$$

y la *contrarrecíproca* es

$$\neg q \to \neg p$$

Notar que, por definición, la contrarrecíproca es la recíproca de la contraria o, también, la contraria de la recíproca, y de ahí su nombre.

Sus tablas de verdad se determinan a partir de las tablas de verdad del condicional y de la negación; éstas son:

p	q	$p \leftarrow q$	$\neg p \to \neg q$	$\neg q \to \neg p$
V	V	V	V	V
V	F	V	V	F
F	V	F	F	V
F	F	V	V	V

(1.7)

Observamos que el condicional (ver tabla (1.6)) y la contrarrecíproca tienen la misma tabla de verdad, y lo mismo sucede con la contraria y la recíproca. Estos son ejemplos de proposiciones equivalentes, como veremos más adelante.

Ejemplo. En este ejemplo mostramos como, a partir de las proposiciones p : "llueve" y q : "hace frío", se construyen el condicional $p \to q$, su recíproca, contraria y contrarrecíproca.

Al construirlas no asumimos ninguna relación de causa-efecto. Ni tampoco no nos interesa el valor de verdad de ninguna de estas proposciones.

- $p \to q$: "Si llueve, entonces hace frío".
- $q \to p$: "Si hace frío, entonces llueve".
- $\neg p \to \neg q$: "Si no llueve, entonces no hace frío".
- $\neg q \to \neg p$: "Si no hace frío, entonces no llueve".

1.3.3. La proposición bicondicional

Dadas dos proposiciones p y q, la proposición *bicondicional*

$$p \leftrightarrow q$$

se define como la proposición compuesta

$$(p \to q) \wedge (p \leftarrow q)$$

Es decir, es la conjunción de una condicional con su recíproca. La tabla de verdad de la proposición bicondicional se sigue de las tablas del condicional (1.6), de la contraria (1.7) y de la conjunción (1.4). Se tiene que

p	q	$p \to q$	$p \leftarrow q$	$p \leftrightarrow q$
V	V	V	V	V
V	F	F	V	F
F	V	V	F	F
F	F	V	V	V

(1.8)

De esta manera, $p \leftrightarrow q$ es verdadera si p y q son ambas verdaderas o ambas falsas, o sea si ambas tienen el mismo valor de verdad. En el lenguaje coloquial, la proposición bicondicional $p \leftrightarrow q$ se expresa de varios modos distintos, entre ellos:

- "p si y sólo si q."
- "p es (condición) necesaria y suficiente para q."

1.3.4. Tautologías y contradicciones †

Sea P una proposición compuesta, obtenida a partir de las proposiciones $p_1, p_2, \ldots, p_n$ usando conectivos lógicos. Diremos que P es una *tautología* si P es siempre verdadera, cualesquiera sean los valores de verdad de $p_1, p_2, \ldots, p_n$. Por el contrario, si P es siempre falsa para todos los posibles valores de verdad de $p_1, p_2, \ldots, p_n$ diremos que P es una *contradicción*. Si P no es ni una tautología ni una contradicción (el caso más general), se dice que P es una *contingencia*. Por ejemplo, dada una proposición p, $p \vee \neg p$ es una tautología, mientras que $p \wedge \neg p$ es una contradicción, como puede verse en sus tablas de verdad:

p	$\neg p$	$p \vee \neg p$
V	F	V
F	V	V

p	$\neg p$	$p \wedge \neg p$
V	F	F
F	V	F

1.3.5. Proposiciones equivalentes

Vimos que a partir de proposiciones dadas se pueden construir, usando los conectivos lógicos, nuevas proposiciones llamadas *compuestas*. Por ejemplo si p, q y r son proposiciones dadas, entonces $p \wedge \neg(q \vee r)$, $q \vee (\neg p \wedge r)$ y $p \to (q \wedge r)$ son todas proposiciones compuestas.

Dos proposiciones compuestas son *lógicamente equivalentes*, o simplemente *equivalentes*, si tienen el mismo valor de verdad para todo los posibles valores de verdad de sus componentes. Si P y Q son equivalentes, escribimos $P \equiv Q$.

Las siguientes son tres situaciones de equivalencias que se usan muy frecuentemente y sin mencionarlo:

- Las negaciones de la conjunción y de la disyunción.

$$\begin{aligned} \neg(p \wedge q) &\equiv \neg p \vee \neg q \\ \neg(p \vee q) &\equiv \neg p \wedge \neg q. \end{aligned} \tag{1.9}$$

  En efecto sus tablas de verdad son

p	q	$\neg(p \wedge q)$	$\neg p \vee \neg q$
V	V	F	F
V	F	V	V
F	V	V	V
F	F	V	V

p	q	$\neg(p \vee q)$	$\neg p \wedge \neg q$
V	V	F	F
V	F	F	F
F	V	F	F
F	F	V	V

  A las equivalencias lógicas en (1.9) se las conoce como *identidades de De Morgan*. Más adelante veremos que algo similar también vale en el contexto de conjuntos.

- Las leyes asociativas y distributivas para $\wedge$ y $\vee$ mencionadas en (1.1) y (1.2).
  - Asociatividad:
$$p \wedge (q \wedge r) \equiv (p \wedge q) \wedge r$$
$$p \vee (q \vee r) \equiv (p \vee q) \vee r$$
  - Distributividad:
$$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$$
$$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$$

  Estas equivalencias se pueden deducir sin dificultad usando tablas de verdad de la conjunción y de la disyunción. Dejamos esto como ejercicio para el lector (ver Ejer. 1.??).

- La equivalencia de una proposición condicional cualquiera y su contrarrecíproca. Podemos comprobar fácilmente que
$$p \to q \equiv \neg q \to \neg p$$
  mirando sus tablas de verdad (las recordamos de (1.6) y (1.7)):

p	q	$p \to q$
V	V	V
V	F	F
F	V	V
F	F	V

p	q	$\neg q \to \neg p$
V	V	V
V	F	F
F	V	V
F	F	V

Algunas proposiciones compuestas tienen un valor de verdad definido, independiente de los valores de verdad de las proposiciones que la forman. Este es el caso de las *tautologías*, siempre verdaderas, y de las *contradicciones*, siempre falsas.

1.3.6. Negación de proposiciones compuestas

Es importante poder negar correctamente proposiciones construidas a partir de otras. En particular, resultará muy útil saber expresar la negación de una proposición compuesta en términos de las negaciones de las proposiciones que la forman.

Las identidades de De Morgan (1.9) nos dicen cómo negar las proposiciones construidas usando la conjunción o la disyunción. Precisamente, éstas dicen, que la negación de la conjunción de dos proposiciones es la disyunción de las negaciones de cada una y que la negación de la disyunción de dos proposiciones es la conjunción de las negaciones de cada una.

Ejemplo. Si p es "fui al cine" y q es "fui a cenar afuera", entonces $p \wedge q$ es "fui al cine y a cenar afuera". Para que esta última afirmación resulte falsa, debe pasar que no sea cierto que "fui al cine y a cenar afuera". O sea, debe haber sucedido que no fui a uno de los dos lugares, o que no fui a ninguno. Es decir, "no fui al cine o no fui a cener afuera". Esta proposición es la disyunción de "no fui al cine" y "no fui a cenar afuera", tal cual indica De Morgan. En otras palabras,

$$\neg(p \wedge q) : \textit{no es cierto que "fui al cine y a cenar afuera"}$$

es exactamente igual a

$$\neg p \vee \neg q : \text{"}\textit{no fui al cine}\text{"} \text{ o } \text{"}\textit{no fui a cenar afuera}\text{"}$$

lo cual es claro para todos. ◊

Ejemplo. Consideremos las proposiciones p y q siguientes:

$$\begin{aligned} p &: \textit{"16 es impar"}, \\ q &: \textit{"16 es positivo"}. \end{aligned}$$

A partir de éstas, tenemos

$$\begin{aligned} p \wedge q &: \textit{"16 es impar y positivo"}, \\ p \vee q &: \textit{"16 es impar o positivo"}, \end{aligned}$$

y sus negaciones

$$\begin{aligned} \neg(p \wedge q) &: \textit{"16 no es impar y positivo a la vez"}, \\ \neg(p \vee q) &: \textit{"16 no es impar o positivo "}. \end{aligned}$$

Estas últimas pueden ser reescritas

$$\begin{aligned} \neg p \vee \neg q &: \textit{"16 no es impar o no es positivo"}, \\ \neg p \wedge \neg q &: \textit{"16 no es impar ni es positivo"}. \end{aligned}$$

Está claro que p es falsa y q es verdadera. De esto se sigue que $p \wedge q$ es falsa, que $p \vee q$ es verdadera, que $\neg(p \wedge q)$ es verdadera y que $\neg(p \vee q)$ es falsa. Esto debe también quedar claro de los enunciados de estas proposiciones compuestas tal como están escritas más arriba. ◊

1.4. Cuantificadores

Los cuantificadores permiten utilizar en el lenguaje formal, de manera precisa, las nociones de cantidad o frecuencia referidas a proposiciones, expresadas en el lenguaje coloquial como "todos", "ninguno", "alguno", "hay", "hay al menos uno", "siempre", "nunca" o "cada vez", entre otras.

1.4.1. Funciones proposicionales

Normalmente el uso de proposiciones como las que hemos visto es insuficiente para todos los propósitos de la matemática. Es necesario considerar proposiciones en las cuales sus términos puedan ser variables. Éstas son las *funciones proposicionales*. Esto es, familias de proposiciones de la forma $P(x)$ ó $P(x, y)$, donde x e y son variables que toman sus valores en un determinado *dominio*. Por ejemplo, la función $P(x)$ con dominio X determina una proposición $P(x_0)$ por cada x_0 en X.

Ejemplo. Cosideremos las siguientes funciones proposicionales con dominio los números enteros. Dados x e y enteros:

$$\begin{aligned} P(x) &: x+1 \text{ es impar} \\ Q(x) &: 2x+1 \text{ es impar} \\ R(x,y) &: x+y \text{ es impar} \end{aligned} \tag{1.10}$$

Si $x = 1$ entonces $x + 1 = 2$ es par y por lo tanto $P(1)$: "2 es impar" es F. En cambio, si $x = 2$ entonces $x + 1 = 3$ es impar y $P(2)$: "3 es impar" es V. En general tenemos que $P(2k)$ es V y $P(2k + 1)$ es F cualquiera sea el natural k.

Para cada elección de un entero x y un entero y, las funciones proposicionales P, Q y R devuelven una proposición particular. Por ejemplo, para $x = -3$ e $y = 7$:

$$\begin{aligned} P(x) &: -3+1 = -2 \text{ es impar} \\ Q(x) &: 2(-3)+1 = -5 \text{ es impar} \\ R(x,y) &: -3+7 = 4 \text{ es impar} \end{aligned} \tag{1.11}$$

El dominio de las variables x e y en las funciones proposicionales $P(x)$, $Q(x)$ y $R(x, y)$ es el conjunto de números enteros como dijimos al principio. A veces, el dominio de las variables se indica en la misma proposición; por ejemplo podemos reescribir:

$$\begin{aligned} P(x) &: \ x+1 \text{ es impar y } x \text{ es entero} \\ P(x) &: \ x+1 \text{ es impar, } x \in \mathbb{Z} \end{aligned}$$

donde $\mathbb{Z}$ denota el conjunto de números enteros. ◊

Nota. En general, para cualquier número natural n, se pueden considerar funciones proposicionales $P(x_1, x_2, \ldots, x_n)$ en n-variables $x_1, \ldots, x_n$, con dominios $X_1, \ldots, X_n$ respectivamente.

1.4.2. Proposiciones cuantificadas

Las funciones proposicionales no son, en general, proposiciones ya que pueden no tener un valor de verdad definido, sino que éste depende de la variable. Las funciones proposicionales pueden ser cuantificadas; una vez cuantificadas se convierten en proposiciones con un valor de verdad definido.

Informalmente en el lenguaje coloquial usamos expresiones de la forma "siempre", "a veces", "nunca", "toda vez que", "cada vez que", "siempre que", "uno", "varios", "muchos", "todos", "ninguno", "alguno", "existe", "hay", etc, para cuantificar expresiones. Decimos, por ejemplo, "nunca gano la quiniela"; "cada vez que la veo me largo a llorar"; "siempre que voy a la cancha perdemos"; "hay alguien que no limpia la mesa"; "sólo él pudo haberlo hecho".

En matemática, sólo es necesario usar dos de éstas, "*existe*" y "*para todo*", simbolizados por $\exists$ y $\forall$, respectivamente. Estos son los llamados *cuantificador existencial* y *cuantificador universal*, respectivamente. También se usa el *cuantificador existencial único*, denotado por $\exists!$.

En lo que sigue nos referiremos principalmente a funciones proposicionales de la forma $P(x)$ o $P(x, y)$, aunque todo lo que digamos es también válido para funciones proposicionales con más variables.

Dada una función proposicional $P(x)$, una *particularización* de ésta es la proposición $P(c)$, que resulta de $P(x)$ sustituyendo x por el valor c, donde c es uno de los posibles valores que puede tomar x. Definimos ahora las cuantificaciones de una función proposicional.

- La *cuantificación existencial* de $P(x)$, es la proposición

$$\exists\, x\; P(x)$$

que se lee "existe un elemento x que cumple $P(x)$", "existe un elemento x que satisface $P(x)$", "existe un elemento x con $P(x)$" o "existe x tal que $P(x)$". Ésta es verdadera si hay por lo menos una particularización de $P(x)$ verdadera. O sea, si existe al menos un c en el dominio de x tal que $P(c)$ es verdadera.

- La *cuantificación universal* de $P(x)$, es la proposición

$$\forall x\; P(x)$$

que se lee "para todo x se cumple $P(x)$", "para todo x se satisface $P(x)$" o "para todo x, $P(x)$". Ésta es verdadera si toda particularización de $P(x)$ es verdadera, es decir si $P(c)$ es verdadera para todo c en el dominio de x.

También se usa la *cuantificación existencial única* de $P(x)$, que es la proposición

$$\exists!\, x\; P(x)$$

que se lee "existe un único x tal que $P(x)$", que es verdadera si hay *exactamente una* particularización verdadera de $P(x)$. En otras palabras, si existe un c en el dominio de x tal que $P(c)$ es verdadera y c es el único con esa propiedad; es decir, si existe c' tal que $P(c')$ es verdadera, entonces $c = c'$. En símbolos, $\exists!\, x\; P(x)$ si y solo si

$$\exists\, c\; P(c) \quad \wedge \quad (\exists\, c'\; P(c') \;\Rightarrow\; c = c')$$

Ejemplos. Consideremos algunas proposiciones construidas a partir de las funciones proposicionales $P(x)$, $Q(x)$ y $R(x, y)$ en (1.10), usando los cuantificadores. Recordemos que x, y son números enteros.

(1) Para $P(x)$ tenemos:

$$\begin{aligned} \forall x\; P(x) &: \text{ para todo } x,\ x+1 \text{ es impar} \\ \exists\, x\; P(x) &: \text{ existe al menos un } x \text{ tal que } x+1 \text{ es impar} \end{aligned}$$

(2) Para $Q(x)$ tenemos:

$$\begin{aligned} \forall x\; Q(x) &: \text{ para todo } x,\ 2x+1 \text{ es impar} \\ \exists\, x\; Q(x) &: \text{ existe al menos un } x \text{ tal que } 2x+1 \text{ es impar} \end{aligned}$$

(3) Para $R(x, y)$ tenemos:

$$\begin{array}{rcl} \exists\, x\, \exists\, y\ R(x,y) & : & \text{existen al menos un } x \text{ y un } y \text{ tales que } x+y \text{ es impar} \\ \forall x\, \exists\, y\ R(x,y) & : & \text{para todo } x\text{, existe al menos un } y \text{ tal que } x+y \text{ es impar} \\ \exists\, x\, \forall y\ R(x,y) & : & \text{existe un } x \text{ tal que para todo } y\text{, } x+y \text{ es impar} \\ \forall x\, \forall y\ R(x,y) & : & x+y \text{ es impar para todo } x \text{ e } y \end{array}$$

En el caso de haber más de una variable, cada una puede ser cuantificada con $\exists$ o $\forall$ independientemente. Observamos que en caso de cuantificar una variable con $\exists$ y otra con $\forall$ el orden de los cuantificadores es relevante. Esto es así aun en el caso en el que las variables tengan el mismo rol o se puedan intercambiar como en el caso de la función proposicional $R(x, y)$. En efecto, la proposición

$$\forall x\, \exists\, y\ R(x,y) : \text{para todo } x\text{, existe (al menos) un } y \text{ tal que } x+y \text{ es impar}$$

es VERDADERA, pues cualquiera sea el x dado, eligiendo $y = -x+1$ resulta que $x+y = 1$ que es impar. Ahora, la proposición

$$\exists\, x\, \forall y\ R(x,y) : \text{existe un } x \text{ tal que para todo } y\text{, } x+y \text{ es impar}$$

es FALSA, pues no existe un x tal que sumado a todo otro entero de una suma impar, ya que por ejemplo la suma $x + (-x) = 0$ que es par. ◊

1.4.3. Negación de proposiciones cuantificadas

Es importante saber negar correctamente proposiciones con cuantificadores. Las negaciones de los cuantificadores existencial y universal son las siguientes:

$$\begin{array}{rcl} \neg(\exists\, x\ P(x)) & \equiv & \forall x\ \neg P(x) \\ \neg(\forall x\ P(x)) & \equiv & \exists x\ \neg P(x) \end{array}$$

Es común omitir los paréntesis de arriba. Repitamos estas negaciones, pero ahora usando el lenguaje común.

- $\neg\exists\, x\ P(x)$: "no es cierto que exista al menos un x tal que $P(x)$" que es lo mismo que decir que "para ningún x, se cumple $P(x)$" o "para todo x, no se cumple $P(x)$".
- $\neg\forall x\ P(x)$: "no es cierto que para todo x, $P(x)$ es verdadera" que es lo mismo que decir que "para algún x, no vale $P(x)$" o "existe al menos un x para el cual $P(x)$ no vale".

Por último veamos cómo es la negación del cuantificador existencial único. Para que no se cumpla que existe un único x tal que vale $P(x)$ pueden pasar dos cosas: o bien no existe ningún x que satisfaga $P(x)$, o bien existen más de un x que satisfacen $P(x)$. En símbolos, tenemos

$$\neg\exists!\, x\ P(x) \ \equiv\ \big(\neg\exists\, x\ P(x)\big)\ \vee\ \big(\exists\, x, y,\ x \neq y,\ P(x) \wedge P(y)\big)$$

Ejemplos. Estudiemos ahora las proposiciones de los ejemplos anteriores construidas cuantificando las funciones proposicionales P y Q. Para ello, determinamos sus valores de verdad y enunciamos correctamente sus negaciones.

(1) Sea $P(x)$: "$x+1$ es impar", donde x toma valores en los números enteros.

- $\forall x\ P(x)$: "*para todo* x, $x+1$ *es impar*". Esta proposición es FALSA, pues 1+1 es par. Es decir, si $c=1$, la particularización $P(c)$: "$c+1$ es impar" es falsa. Cabe aclarar que, en este caso, hay otras particularizaciones de $P(x)$ también falsas, por ejemplo con $c=3$, $c=5$ o $c=157$ y también hay paricularizaciones que son verdaderas, como con $c=2$, $c=4$ o $c=156$. Sólo basta encontrar un c que falle para mostrar la falsedad de la proposición.
- $\neg\forall x\ P(x)$: "*existe al menos un* x *tal que* $x+1$ *es par*". Esta proposición es VERDADERA, pues 1+1 es par. Esto no sorprende pues ésta es la negación de la anterior, que es verdadera.
- $\exists\, x\ P(x)$: "*existe al menos un* x *tal que* $x+1$ *es impar*". Esta proposición es VERDADERA, pues 2+1 es impar; es decir si $c=2$ la particularización $P(c)$ es verdadera. Como en el caso anterior, en éste, hay muchos enteros que la hacen verdadera, como por ejemplo 4, 6 y 128 entre otros.
- $\neg\exists\, x\ P(x)$: "*no existe ningún* x *tal que* $x+1$ *es par*". Esta proposición es FALSA, pues 1+1 es par.

(2) Sea $Q(x)$: "$2x+1$ es impar", donde x es un número entero.

- $\forall x\ Q(x)$: "*para todo* x, $2x+1$ *es impar*". Esta proposición es VERDADERA, ya que $2x+1$ dividido 2 nunca es entero.
- $\neg\forall x\ Q(x)$: "*existe* x *tal que* $2x+1$ *es par*". Esta proposción es FALSA, ya que como dijimos antes $2x+1$ nunca es par.
- $\exists\, x\ Q(x)$: "*existe al menos un* x *tal que* $2x+1$ *es impar*". Esta proposición es VERDADERA, ya que si $c=0$, $2c+1=1$ es impar.
- $\neg\exists\, x\ Q(x)$: "*no existe ningún* x *tal que* $2x+1$ *es impar*"; o dicho de otra manera, "*para todo* x, $2x+1$ *es par*". Esta proposición es FALSA, ya que como observamos antes $2x+1$ nunca es par. ◊

Dada una función proposicional de dos variables $P(x,y)$, la expresión $\forall x\forall y\, P(x,y)$ es una abreviatura de $\forall x(\forall y\, P(x,y))$. Lo mismo sucede con el cuantificador existencial. Cuando los cuantificadores son los mismos, no hay diferencia en el orden en que aparecen x e y y se puede abreviar usando $\forall x, y$ en lugar de $\forall x\forall y$. De este modo tenemos

$$\begin{aligned}
\forall x\forall y\, P(x,y) \quad &\equiv \quad \forall x, y\, P(x,y) \quad \equiv \quad \forall y, x\, P(x,y) \quad \equiv \quad \forall y\forall x\, P(x,y),\\
\exists x\exists y\, P(x,y) \quad &\equiv \quad \exists x, y\, P(x,y) \quad \equiv \quad \exists y, x\, P(x,y) \quad \equiv \quad \exists y\exists x\, P(x,y).
\end{aligned}$$

Es útil pensar que $\forall x(\forall y P(x,y))$ es igual a la proposición $\forall x\, Q(x,y)$, donde $Q(x,y)$ es la proposición cuantificada $\forall y\, P(x,y)$, i.e.

$$\forall x(\underbrace{\forall y\, P(x,y)}_{Q(x,y)}) = \forall x\, Q(x,y).$$

De esta manera resulta más fácil negar la proposición $\forall x \forall y P(x,y)$. Simplemente aplicamos lo que ya sabemos paso a paso. Resulta que

$$\begin{aligned} \neg(\forall x \forall y\, P(x,y)) &\equiv \neg\forall x(\forall y P(x,y)) \equiv \neg\forall x\, Q(x,y) \\ &\equiv \exists x\, \neg Q(x,y) \equiv \exists x(\neg\forall y\, P(x,y)) \\ &\equiv \exists x \exists y\, (\neg P(x,y)). \end{aligned}$$

Cuando los cuantificadores son distintos, el orden de éstos no puede intercambiarse, i.e. en general

$$\begin{aligned} \forall x \exists y\, P(x,y) &\not\equiv \exists y \forall x\, P(x,y), \\ \exists x \forall y\, P(x,y) &\not\equiv \forall y \exists x\, P(x,y). \end{aligned}$$

A partir de la función proposicional $P(x,y)$, se pueden obtener hasta 6 [*] proposiones cuantificadas distintas:

$$\begin{array}{lll} \forall x \forall y\, P(x,y) & \forall x \exists y\, P(x,y) & \forall y \exists x\, P(x,y) \\ \exists x \forall y\, P(x,y) & \exists y \forall x\, P(x,y) & \exists x \exists y\, P(x,y) \end{array}$$

Sin embargo, si el enunciado es "simétrico" en x e y, es decir los roles de x e y pueden ser intercambiados sin cambiar el enunciado, entonces:

$$\begin{aligned} \forall x \exists y\, P(x,y) &\equiv \forall y \exists x\, P(x,y) \\ \exists x \forall y\, P(x,y) &\equiv \exists y \forall x\, P(x,y) \end{aligned}$$

Esto sucede en el siguiente ejemplo.

Ejemplo. Sea $R(x,y)$: "$x+y$ es impar" con x e y números enteros.

- $\exists\, x \exists\, y\ R(x,y)$: *"existen al menos un x y un y tales que $x+y$ es impar"*. Esta proposición es VERDADERA, ya que $1+2=3$ es impar. Es decir, la particularización $R(1,2)$ es verdadera. Está claro que hay muchos pares x, y tales que su suma $x+y$ es impar, aunque también hay muchos otros pares cuya suma es par. Por ejemplo, $R(2m, 2n+1)$ y $R(2m+1, 2n)$ son verdaderas cualesquiera sean los enteros m y n.
- $\neg(\exists\, x\, \exists\, y\ R(x,y))$: *"no existe ningún par de enteros x, y tales que $x+y$ es impar"*. Esto equivale a $\forall\, x \forall\, y\ \neg R(x,y)$ o sea, *"la suma $x+y$ de cualquier par de enteros x, y es par"*. Esta proposición es FALSA, ya que por ejemplo $0+1=1$ es impar, es decir $R(0,1)$ es una particularización falsa. Nuevamente hay muchos otros pares x, y cuya suma es par.
- $\forall x\, \exists\, y\ R(x,y)$: *"para todo x, existe al menos un y tal que $x+y$ es impar"*. Esta proposición es VERDADERA, pues dado x cualquiera si $y = x+1$, entonces $x+y = x+x+1 = 2x+1$ que es impar. Notamos que el y que proponemos depende de x, es decir si cambiamos x, cambia y. Además notamos que el y que elegimos no es la única elección posible; por ejemplo si $y = x+3$, o $y = 3x+1$ la suma $x+y$ también es impar.

[*] Son 6 pues ya dijimos que $\forall x \forall y = \forall y \forall x$ y $\exists x \exists y = \exists y \exists x$.

- $\neg(\forall x\, \exists y\ R(x,y))$: equivale a $\exists x \forall y\, \neg R(x,y)$, o sea *"existe al menos un x, tal que para todo y, la suma $x+y$ es par"*. Esta proposición es FALSA. Cualquiera sea x, si $y = x+1$, $x+y = 2x+1$ es impar, luego es imposible encontrar un x tal que al sumarle cualquier número el resultado sea siempre par.

- $\exists x\, \forall y\ R(x,y)$: *"existe un x, tal que para todo y, $x+y$ es impar"*. Esta proposición es FALSA, pues para que $x+y$ sea impar, x e y deben tener distinta paridad, es decir x es par e y impar o viceversa. Luego, no puede existir un x de la forma buscada.

- $\neg(\exists x\, \forall y\ R(x,y))$: equivale a $\forall x \exists y \neg R(x,y)$, o sea *"para todo x, existe un y tal que $x+y$ es par"* . Esta proposición es VERDADERA. Dado x, sea $y = x$. Luego $x + y = 2x$ que siempre es par.

- $\forall x\, \forall y\ R(x,y)$: *"para todo x e y, $x+y$ es impar"*. Esta proposición es FALSA, ya que $1+1$ es par.

- $\neg(\forall x\, \forall y\ R(x,y))$: *"existen x e y, tales que $x+y$ es par"*. Esta proposición es claramente VERDADERA; es muy fácil exhibir pares de enteros cuya suma es par.

Resumiendo, tenemos

$\exists x\, \exists y\ R(x,y)$	VERDADERO
$\forall x\, \exists y\ R(x,y)$	VERDADERO
$\exists x\, \forall y\ R(x,y)$	FALSO
$\forall x\, \forall y\ R(x,y)$	FALSO

Vemos que los valores de verdad las proposiciones con $\exists$ y $\forall$ son distintos al cambiar el orden de los cuantificadores. ◊

Nota. Terminamos esta sección con un comentario sobre como justificar un enunciado cuantificado. Por simplicidad consideramos el caso de una función proposicional de una sola variable $P(x)$.

Consideremos primero la proposición $\forall x\, P(x)$. Si ésta es veradera, debemos "demostrar" dicha proposición, es decir, dar un argumento que muestre que para un x arbitrario, $P(x)$ es V. Mientras que si es falsa, bastará dar un *contraejemplo*, esto es, exhibir un c en el dominio de P tal que $P(c)$ es F.

Ahora consideremos la proposición $\exists x\, P(x)$. Si esta proposición es verdadera, bastará con exhibir un *ejemplo*, esto es, un c tal que $P(c)$ es V. Mientras que si resulta falsa, entonces habrá que demostrar que cualquiera sea x, $P(x)$ es falsa.

Podemos resumir lo dicho en este cuadro:

Enunciado	V	F
$\forall x\, P(x)$	DEMOSTRACIÓN	CONTRAEJEMPLO
$\exists x\, P(x)$	EJEMPLO	DEMOSTRACIÓN

1.5. Demostraciones

Los resultados o verdades de la matemática, los teoremas, se validan con demostraciones o pruebas.

Una *prueba* o *demostración* es una sucesión finita de proposiciones verdaderas, que comienza con una que se asume verdadera, la *hipótesis*, y tal que la verdad de cada una de las otras se deduce lógicamente de la verdad de la anterior por medio de argumentos válidos. Éstos deben ser correctos, simples, claros y convincentes. El último enunciado en la cadena recibe el nombre de *tesis*. El paso de una proposición p a la siguiente q en una demostración es lo que se denomina *implicación* de p a q:

$$p \Rightarrow q$$

que se lee:

- p implica (lógicamente) q,
- q se sigue (lógicamente) de p,
- q es consecuencia (lógica) de p,
- q es implicada (lógicamente) por p.

Vimos que asociadas al condicional $p \to q$ hay otras proposiciones: recíproca, contraria y contrarrecíproca. Éstas mismas existen para la implicación $p \Rightarrow q$, a saber:

- Implicación *recíproca*: $q \Rightarrow p$.
- Implicación *contraria*: $\neg p \Rightarrow \neg q$.
- Implicación *contrarrecíproca*: $\neg q \Rightarrow \neg p$.

La implicación $p \Rightarrow q$ y su contrarrecíproca resultan equivalentes, y esta equivalencia da un método de demostración útil, usado con frecuencia en matemática.

Por último, asociado al bicondicional $p \leftrightarrow q$ existe la doble implicación o equivalencia

$$p \Leftrightarrow q$$

que se lee

- p si y sólo si q;
- p implica y es implicada por q;
- p es (condición) necesaria y suficiente para q;
- p y q son equivalentes.

1.5.1. La implicación

La implicación es un concepto fundamental de la lógica. Es la base del método deductivo, método esencial para la validación de los resultados en todas las ciencias. La implicación de una proposición q de otra p, es la justificación de la veracidad de q a partir de la veracidad de p en un marco dado y de acuerdo a reglas preestablecidas.

Observamos que la implicación $p \Rightarrow q$ y el condicional $p \to q$ no son lo mismo, aunque guardan alguna relación. Es por esto que muchas veces se confunde una con otra. Una primera diferencia que podemos remarcar es que la implicación $p \Rightarrow q$ no es una proposición compuesta de p y q en el sentido de la sección anterior, cómo si lo es el condicional $p \to q$.

La relación entre $\Rightarrow$ y $\to$ no es nuestro objeto de estudio. Sin embargo queremos discutir brevemente sobre la implicación y el condicional, pues lo aprendido en el marco formal sobre el condicional $p \to q$ resulta útil como marco para comprender mejor la implicación $p \Rightarrow q$.

El hecho básico y fundamental de la implicación es que a partir de una proposición verdadera p, por medio de argumentos válidos, sólo se obtienen nuevas proposiciones verdaderas q. Esto hace que podemos pensar que la veracidad de la implicación $p \Rightarrow q$ indica que la verdad de q se deduce de la veracidad de p. Así, si p es verdadera y q se deduce de p, concluimos que q es también verdadera. Esto se conoce como *"modus ponens"* y es uno de los más elementales métodos de deducción de la lógica. Este es el método de validación que usamos en matemática:

> *Modus ponens*: Para validar una proposición, debemos mostrar que se sigue, por medio de un número finito de argumentos válidos, de otra(s) cuya veracidad ya fue(ron) establecida(s) previamente.

modus ponens

p	$p \Rightarrow q$	q
V	V	V

Notamos que ésto coicide con el primer renglón de la tabla de verdad del condicional $p \to q$.

p	q	$p \to q$
V	V	V

En otras palabras: *si partimos de algo verdadero y argumentamos correctamente, obtenemos nuevas verdades*. De esto se sigue que si partimos de algo verdadero y argumentando obtenemos algo falso, los argumentos no son correctos. (Ya que de ser correctos la conclusión es verdadera.) Notamos que esto es el segundo renglón de la tabla de verdad del condicional.

p	q	$p \to q$
V	F	F

Los dos últimos renglones de la tabla de verdad del condicional $p \to q$

p	q	$p \to q$
F	V	V
F	F	V

expresan que a partir de una proposición falsa es posible, por medio de razonamientos lógicos correctos, deducir tanto cosas falsas como verdaderas. Por ejemplo, si partimos de la proposición (falsa) $1 = 2$, multiplicando ambos miembros de la igualdad por un mismo número obtenemos una nueva igualdad entre números. Así multiplicando por 2, obtenemos que $2 = 4$ (falso) y multiplicando por 0, obtenemos que $0 = 0$ (verdadero).

Ya dijimos que asociadas a la implicación $p \Rightarrow q$, existen otras implicaciones:

- Implicación *recíproca*: $q \Rightarrow p$.
- Implicación *contraria*: $\neg p \Rightarrow \neg q$.
- Implicación *contrarrecíproca*: $\neg q \Rightarrow \neg p$.

Destacamos que la equivalencia de la implicación $p \Rightarrow q$ con su contrarrecíproca $\neg q \Rightarrow \neg p$ es un método de demostración útil, usado con frecuencia en matemática.

La doble implicación

$$p \Leftrightarrow q,$$

es una manera abreviada de escribir la implicación $p \Rightarrow q$ junto con su recíproca $p \Leftarrow q$. En este caso la proposición q se sigue de p y la proposición p se sigue de q. Es decir son equivalentes. Son formas o expresiones posiblemente distintas de una misma verdad.

1.5.2. Tipos de demostraciones

En esta sección presentamos, de manera un tanto informal, distintos tipos de demostraciones que se utilizan frecuentemente. Aclaramos que esta no pretende ser una clasificación completa de dichos tipos. Se trata mas bien de una discusión que muestra algunos aspectos a tener en cuenta sobre las demostraciones; y que sirve para orientar al lector cuando se encuentre con una demostración que pretenda entender, o bien cuando deba escribir la demostración de un hecho por sí mismo.

Según la lógica: directa, indirecta y por el absurdo

Recordemos que un teorema es un enunciado verdadero para el cual existe una demostración. Hay tres tipos generales de demostración que materializan diferentes estrategias lógicas: DIRECTA, INDIRECTA y POR EL ABSURDO. Veamos en qué consisten y cómo funcionan en el caso de un enunciado de la forma

$$p \Rightarrow q$$

que es la forma más común en que suelen presentarse los resultados en matemática. Aquí p es la hipótesis o premisa y q es la tesis o conclusión.

- Demostración directa: se asume que p es verdadera; y en un número finito de pasos, y por medio de argumentos válidos y usando otros resultados previamente establecidos, se deduce que q es verdadera.

  La regla de inferencia *modus ponens* asegura que si P es verdadera y la implicación $P \Rightarrow Q$ es verdadera, entonces Q es verdadera. Si tenemos una cadena de implicaciones que comienza con p

  $$p \Rightarrow p_1, \quad p_1 \Rightarrow p_2, \quad \dots \quad p_{n-1} \Rightarrow p_n, \quad p_n \Rightarrow q$$

  por modus ponens, como p es verdadera por hipótesis y p_1 es consecuencia por medio de argumentos válidos de p, p_1 es verdadera; de la misma forma se sigue que p_2 es verdadera y así sucesivamente hasta concluir que q es verdadera.

- Demostración indirecta o contrarrecíproca: aquí, en lugar de probar la implicación $p \Rightarrow q$, se prueba su contrarrecíproca $\neg q \Rightarrow \neg p$. O sea, suponiendo que q es falsa hay que (de)mostrar que p también es falsa.

  Como ya vimos, la implicación $p \Rightarrow q$ y su contrarrecíproca $\neg q \Rightarrow \neg p$ son equivalentes.

- Demostración por el absurdo: en general, si queremos probar que una proposición r es verdadera, suponemos que r es falsa y, a partir de esto, deducimos la falsedad de algo que sabesmos que es verdadero. Esto es lo que se llama un absurdo o contradicción, lo cual es inaceptable en matemática. Esta contradicción proviene de suponer que r es falso, por lo cual concluimos que r debe ser (es) verdadero.

Las demostraciones por el absurdo y las indirectas comparten la misma esencia. Las indirectas o contrarrecíprocas, son casos particulares de demostraciones por el absurdo. Como dijimos, una prueba indirecta de $p \Rightarrow q$, asume que q (lo que queremos mostrar que es verdadero) es falso, y a partir de esto conlcuimos que p es falso, siendo que lo habíamos asumido verdadero. Esto es un absurdo o contradicción.

Saber cuándo utilizar una u otra técnica es parte del arte de hacer matemática. Por ejemplo, en una prueba larga es usual encontrar varios de estos tipos de demostración en distintas etapas de la misma.

A continuación ilustramos estos métodos mostrando algunos teoremas, del tipo que encontraremos más adelante, con sus correspondientes demostraciones.

Ejemplos.

(1) Demostración directa.

Teorema. *La suma de dos enteros pares es par.*

Demostración. Sean x e y enteros pares. Luego $x = 2m$, $y = 2n$ para ciertos enteros m, n. Entonces $x + y = 2m + 2n = 2(m + n)$, y como $m + n$ es un entero, $x + y$ es un entero par. □

Notar que el enunciado del teorema se puede poner de la forma $p \Rightarrow q$ así: "x, y pares implican $x + y$ par" o "si x y y son pares, entonces $x + y$ es par".

(2) Demostración indirecta.

Teorema. *Si n es entero y n^2 es par, entonces n es par.*

Demostración. Supongamos que n es impar, o sea $n = 2k+1$ para algún entero k. Luego $n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 4(k(k+1)) + 1$ es impar. Hemos probado que "n impar $\Rightarrow n^2$ impar". Por equivalencia con la contrarrecíproca, probamos que "n^2 par $\Rightarrow n$ par". □

Nota. El enunciado "n entero par $\Rightarrow n^2$ par" se prueba directamente. Si $n = 2k$ con k entero, entonces $n^2 = 4k^2 = 2(2k^2)$ es par. Si quisiéramos probar la recíproca "n^2 par $\Rightarrow n$ par", de manera directa, nos encontramos con dificultades. En efecto, si $n^2 = 2k$, $k \in \mathbb{Z}$, entonces $n = \pm\sqrt{2k}$ es entero, pero no hay forma de saber si es par o impar.

(3) Demostración por el absurdo.

Teorema. *El número real $\sqrt{2}$ es irracional.*

Demostración. Supongamos que $\sqrt{2}$ fuera racional. Entonces $\sqrt{2} = \frac{m}{n}$ con m, n enteros. Elevando al cuadrado, tenemos que $2m^2 = n^2$. Por el teorema fundamental de la aritmética (TFA) que veremos más adelante, todo entero se factoriza como producto de números primos de forma única (salvo el orden de los factores). Ahora, el primo 2 aparece en la factorización de $2m^2$ y luego debe aparecer en la de n^2. Como la factorización de n^2 es la de n duplicada y lo mismo ocurre con la factirización de m^2, vemos que en el miembro de la derecha, n^2, el 2 aparece un número par de veces, mientras que en el miembro de la izquierda, $2m^2$, aparece un número impar de veces. Esto contradice la unicidad del TFA. Por lo tanto, $\sqrt{2}$ es irracional. □

Según el método: constructiva, existencial, exhaustiva e inductiva

Además de los tipos de demostración descriptos, según la estrategia lógica adoptada, también podemos distinguir tipos de demostraciones según cómo se llevan adelante; esto tiene que ver con la naturaleza de lo que se quiere demostrar. No son tipos excluyentes entre sí; por ejemplo hay demostraciones constructivas por inducción y demostraciones existenciales exhaustivas.

- Constructiva: Se demuestra la existencia de un objeto matemático construyénlo, para exhibirlo explícitamente.
- Existencial (no constructiva): Se demuestra la existencia de un objeto matemático, sin construirlo ni ser capaz de exhibirlo.
- Exhaustiva: Se consideran todos los casos posibles que pueden ocurrir en una determinada situación de interés y se los prueba uno por uno.
- Inductiva: Sirve para probar proposiciones con una variable natural de la forma $\forall n\ P(n)$ y la herramienta es el principio de inducción (que veremos más adelante).

Nota. Éstos son solo cuatro tipos de demostraciones en los que se distingue algún método de características particulares. Se podrían agregar a esta lista muchos más, algunos propios de áreas particulares. Por ejemplo, podríamos agregar las demostraciones combinatorias (o "combinatóricas"), presentes frecuentemente en Matemática Discreta.

Ejemplos.

(1) Demostración constructiva.

Teorema. *Dados 2 números reales $a < b$, existe un c tal que $a < c < b$.*

Demostración. Sea

$$c = \tfrac{a+b}{2}$$

(el punto medio del segmento $\overline{ab}$). Como $a < b$ tenemos $a = \frac{a+a}{2} < \frac{a+b}{2} = c$ y del mismo modo $c = \frac{a+b}{2} < \frac{b+b}{2} = b$. □

En esta demostración se muestra cómo construir un número c concreto con las propiedades esperadas (entre a y b).

(2) Demostración existencial (no constructiva).

Teorema. *En todo conjunto de 13 o más personas, hay por lo menos dos de ellas que cumplen años el mismo mes.*

Demostración. Elijamos 12 personas al azar del conjunto total. Si hay 2 que cumplen el mismo mes ya está. Consideremos entonces que las 12 cumplen años en meses distintos, es decir una en cada uno de los 12 meses del año. Ahora, cualquiera sea la decimotercera persona que elijamos necesariamente cumplirá años el mismo mes que alguna de las 12 primeras. □

En un conjunto concreto de personas, por ejemplo los alumnos del curso, uno podría preguntar las fechas de nacimiento. Sin embargo, la afirmación es sobre un grupo arbitrario de personas, del cual no sabemos nada. De todas formas, fuimos capaces de probar la afirmación sin necesidad de exhibir el par de personas que cumplen años el mismo mes ni tampoco qué mes es éste.

(3) Demostración por exhaución.

Teorema. *El producto de 3 naturales consecutivos es múltiplo de 3.*

Demostración. Sea n un número natural cualquiera y sea

$$m = n(n+1)(n+2).$$

Queremos ver que m es múltiplo de 3. Notamos que basta mostrar que uno de los tres factores es múltiplo de 3. Consideremos el resto, r, de dividir a n por 3. Hay 3 casos posibles, pues $0 \leq r \leq 2$.

(i) Si $r = 0$, entonces $n = 3k$ para algún k, y así m es múltiplo de 3.

(ii) Si $r = 1$, entonces $n = 3k+1$ para algún k, y por lo tanto $n+2 = 3k+3 = 3(k+1)$. Luego m es múltiplo de 3.

(iii) Si $r = 2$, entonces $n = 3k+2$ para algún k, y $n+1 = 3k+3 = 3(k+1)$, de donde se sigue que m es múltiplo de 3.

En todos los casos obtenemos que m es múltiplo de 3. □

En esta prueba por exhausión, analizamos cada una de las tres situaciones en las que dividimos el problema dado. Observamos que siempre alguna de ellas nos permite

deducir lo que queremos, aunque no es simpre la misma. Por ejemplo, el producto $4 \cdot 5 \cdot 6$ es múltiplo de 3, pues el tercer factor lo es; en cambio el producto $11 \cdot 12 \cdot 13$ es múltiplo de 3 porque el segundo factor lo es.

(4) Demostración inductiva.

Teorema. *El número $3^{2n+1} + 2^{n+2}$ es múltiplo de 7 para todo $n \in \mathbb{N}$.*

Demostración. La dejamos para más adelante. □

El enunciado se refiere a algo que vale para todo número natural. Si $n = 1$, entonces $3^{2n+1} + 2^{n+2} = 27 + 8 = 35 = 7 \cdot 5$. Si $n = 2$, entonces $3^{2n+1} + 2^{n+2} = 243 + 16 = 259 = 7 \cdot 37$. Si $n = 3$, entonces $3^{2n+1} + 2^{n+2} = 2187 + 32 = 259 = 7 \cdot 317$. Con ayuda de una computadora podríamos seguir chequeando que esto se cumple para n's muy grandes. Sin embargo, jamás terminaríamos. Esto requiere la técnica de la inducción que veremos más adelante (ver Capítulo 7, §7.2). ◊

De más está decir que un mismo resultado puede en ciertas ocasiones ser demostrado de muchas formas distintas y por distintos métodos.

Notación. En general el fin de una demostracón se indica explícitamente. Para esto se usan los símbolos //, □, ■, o la sigla QED [*], por "Quad Erat Demonstradum", que significa 'lo que debía ser demostrado'. El símbolo □ se debe a Paul Halmos (1916-2006), quien fue pionero en su uso.

Digresión. Fijemos nuestra atención en dos citas de dos de los más grandes matemáticos de la historia. Carl Friedrich Gauss dijo *"He tenido mis resultados por un largo tiempo, pero aún no se como llegar a ellos"*. Por otra parte, Georg Bernhard Riemann sentenció *"¡Si tan solo tuviera los teoremas! Entonces podría hallar las pruebas fácilmente"*.

Esto ilustra dos situaciones opuestas que se plantean con frecuencia en el quehacer diario de un matemático. A veces, uno tiene un enunciado del cual está seguro que es verdad (ya sea por intuición, porque ha analizado numerosos casos particulares, porque ha reunido demasiada evidencia a favor, etc), pero del que puede ser muy difícil hallar una prueba. Otras, cuesta encontrar el enunciado correcto que refleja lo que uno quiere y que uno puede probar con las herramientas disponibles.

Pruebas gráficas y geométricas. Finalmente mencionamos otro tipo de demostración, las pruebas gráficas (que hacen uso de gráficos, esquemas, dibujos, etc). Aunque hoy en general, las pruebas gráficas pueden ser consideradas insuficientes como demostraciones acabadas, fueron muy usadas en la antigüedad. De todos modos los dibujos, diagramas y gráficos ayudan mucho a la intuición del matemático y pueden inspirar una prueba o un resultado. Por ejemplo, usaremos los llamados diagramas de Venn cuando veamos conjuntos en el siguiente capítulo y ciertas representaciones de puntos para obtener fórmulas en el Capítulo 5.

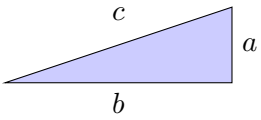
Algunos argumentos geométricos tienen verdadero status de prueba, como lo muestra el siguiente ejemplo, y podemos hablar en este caso de pruebas geométricas.

[*] A veces, cuando la demostración es difícil e ingeniosa, algunos profesores escriben en la pizarra QEPD por 'queda entonces perfectamente demostrado', aunque algunos alumnos pudieran darle un significado mas lapidario...

Ejemplo. Consideremos el famoso Teorema de Pitágoras [**].

TEOREMA. *En todo triángulo rectángulo, la suma de los cuadrados de las medidas de los catetos, es igual al cuadrado de la medida de la hipotenusa.*

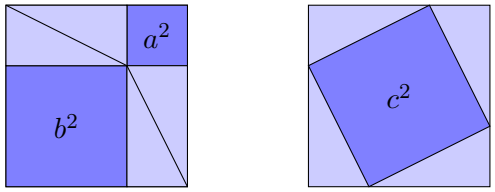
Es decir, si a y b denotan las medidas de los catetos y c denota la medida de la hipotenusa,



entonces

$$a^2 + b^2 = c^2.$$

Una demostración gráfica muy conocida es la siguiente:



Como los 4 triangulitos son equivalentes, las áreas de los cuadrados son iguales!

En la red encontrará muchísimas pruebas más de este teorema. ◊

1.5.3. Conjeturas, ejemplos y contraejemplos †

Las conjeturas, los ejemplos y los contraejemplos son muy útiles en la construcción y el descubrimiento del saber matemático.

Las conjeturas

Una *conjetura* es una afirmación matemática de la cual no se conoce su valor de verdad, pero que se cree verdadera (y por eso se enuncia).

Goldbach. El ejemplo más famoso es sin dudas la *Conjetura de Goldbach*, dada en una carta de Goldbach a Euler fechada en 1742.

CONJETURA. *Todo entero par, mayor que 2, es suma de dos números primos.*

Por ejemplo, para los primeros 10 casos, tenemos

$$\begin{array}{lll} 4 = 2 + 2, & 6 = 3 + 3, & 8 = 3 + 5, \\ 10 = 3 + 7 = 5 + 5, & 12 = 5 + 7, & 14 = 3 + 11 = 7 + 7, \\ 16 = 3 + 13 = 5 + 11, & 18 = 5 + 13, & 20 = 3 + 17 = 7 + 13; \end{array}$$

[**] Probablemente el único teorema mundialmente conocido por gente que no estudia ni estudiará matemática, y el único teorema que recuerde de toda su formación escolar.

incluso el 22 se puede escribir de 3 formas distintas

$$22 = 3 + 19 = 5 + 17 = 11 + 11.$$

De hecho, podríamos seguir diviertiéndonos un rato ya que se ha chequeado con computadoras que la conjetura es cierta para números muy grandes. Sin embargo, esto no constituye una prueba (de hecho, ¡faltan chequear infinitos casos!). Aunque el enunciado es tan sencillo como para que cualquier chico de primaria puede entenderlo, la veracidad o no de ésta sigue aun increíblemente sin respuesta después de más de 270 años [***].

Primos gemelos. Otra conjetura famosa y de larga data es la de los *primos gemelos*, es decir pares de primos de la forma p, $p + 2$, como el par formado por 3 y 5.

Conjetura. *Existen infinitos primos gemelos*.

Es muy fácil encontrar algunos pares de primos gemelos pequeños. Por ejemplo, los pares con p menor que 100 son: $(3, 5)$, $(5, 7)$, $(11, 13)$, $(17, 19)$, $(29, 31)$, $(41, 43)$, $(59, 61)$, $(71, 73)$. Después se complica, aunque se conocen $808.675.888.577.436$ pares de primos gemelos menores que 10^{18}. Algunos de los mayores pares conocidos fueron encontrados con computadoras entre 2007 y 2011. Estos son $2.003.663.613 \cdot 2.195.000 \pm 1$ con 58.711 cifras, $65.516.468.355 \cdot 2.333.333 \pm 1$ con 100.355 cifras y

$$3.756.801.695.685 \cdot 2.666.669 \pm 1$$

con 200.700 cifras! La conjetura, sin embargo, aún está lejos de ser resuelta[****].

Fermat. Todos conocen el teorema de Pitágoras "*dado un triángulo rectángulo, la suma de los cuadrados de los catetos, es igual al cuadrado de la hipotenusa*". Sabemos que hay triángulos rectángulos de lados enteros, es decir existen soluciones enteras a la ecuación

$$x^2 + y^2 = z^2$$

Una de ellas está dada por la terna $(3, 4, 5)$ y otra por $(5, 12, 13)$. En realidad, existen infinitas ternas (x, y, z) que la satisfacen, llamadas *ternas pitagóricas*, dadas por

$$x = m^2 - n^2, \qquad y = 2mn, \qquad z = m^2 + n^2$$

donde m y n son enteros arbitrarios. Las ternas primitivas, o sea con x, y, z mutuamente coprimos, se obtienen si y sólo m, n son coprimos (luego $m > n \geq 1$) y uno de ellos es par (¡chequear estas afirmaciones!) El teorema de Fermat dice que el teorema de Pitágoras no puede ser generalizado a potencias mayores que 2.

Una generalización de este teorema sería encontrar ternas de enteros x, y, z que satisfagan $x^3 + y^3 = z^3$ ó $x^4 + y^4 = z^4$. De hecho, podríamos pensar en cualquier potencia

$$x^n + y^n = z^n, \qquad n \geq 3.$$

En 1637, Pierre de Fermat conjeturó que la ecuación de arriba no tiene soluciones enteras más que las triviales ($x = 0$ o $y = 0$). De hecho, el creyó haberlo demostrado, ya que en el margen de su copia del libro *Arithmetica* de Diofanto escribió

[***] Hay incluso una linda novela sobre el tema, *El tío Petros y la conjetura de Goldbach* escrita en 1992 por el griego Apostolos Doxiadis, muy recomendable para las vacaciones (el libro, no así demostrar la conjetura).

[****] Por favor, no intente esto en casa! Al menos rinda la materia primero.

> "*he descubierto una prueba realmente maravillosa de este hecho, pero este margen es demasiado angosto para contenerla*."

Clásicamente se lo llamó el "último Teorema de Fermat", aunque en algunos libros viejos se lo encuentra como Conjetura de Fermat.

Desde entonces, algunos de los más insignes matemáticos intentaron resolverla sin suerte. De hecho, fue una de las conjeturas más famosas de la historia de la matemática que pérmaneció abierta por 358 años, hasta que en 1995 Andrew Wiles logró por fin demostrala, luego de 10 años de trabajo continuo en total aislamiento usando matemática muy difícil y avanzada. Desde entonces, se trata de un teorema.

Teorema (Fermat-Wiles). *Para todo $n > 2$, no existen enteros positivos x, y, z distintos de cero tales que $x^n + y^n = z^n$.*

Existen muchísimas otras conjeturas en la actualidad, en todas las áreas de la matemática, esperando ser resueltas. Una de las más famosas, problema por el cual hay un premio de u$s 1.000.000 (además de la fama, claro) para quien lo resuelva, es la llamada *Hipótesis de Riemann*. Sin embargo, esta es demasiado complicada para enunciarla aquí. Solo diremos que se trata de encontrar los ceros de la función llamada "zeta de Riemann" y que éstos tienen que ver con la distribución de los números primos [*****].

Los ejemplos

Un *ejemplo* es una instancia verdadera de una proposición más general. Sirven para empezar a entender un enunciado que puede ser muy complicado, por ejemplo si está planteado con demasiada generalidad. Hasta aquí, ya hemos dado numerosos ejemplos de ejemplos.

En el caso de las ternas pitagóricas, $(3, 4, 5)$ y $(5, 12, 13)$ son ejemplos (que corresponden a $m = 2$, $n = 1$ y $m = 3$, $n = 2$). Tomando $m = 4$ y $n = 1$ o $n = 3$ tenemos las ternas pitagóricas $(8, 14, 15)$ y $(7, 24, 25)$, respectivamente.

Los contraejemplos

Un *contraejemplo* es una instancia falsa de una proposición más general. O sea, un ejemplo en donde se muestra que tal enunciado resulta falso. Por ejemplo, si quisieramos demostrar que la conjetura de Goldbach es falsa, sólo bastaría exhibir un contraejemplo, es decir un número par > 2 que no pueda ser escrito como suma de ningún par de números primos.

Ejemplos. Veamos 2 ejemplos instructivos para ver como razonar y proceder.

(1) Consideremos la función cuadrática

$$p(n) = n^2 + n + 41$$

[*****] Dos citas al respecto: *"Si despertara después de haber dormido por 150 años, mi primera pregunta sería: ¿ya se probó la Hipótesis de Riemann?"* –David Hilbert; y *"Si pudieras ser el Diablo y ofrecer a matemáticos vender su alma por la prueba de un teorema, ¿cual sería el teorema más solicitado? Creo que sería la Hipótesis de Riemann."* –Hugh L. Montgomery.

y evaluémosla en los enteros no negativos. Vemos que $p(0) = 41$ es primo, $p(1) = 43$ es primo y $p(2) = 47$ también lo es. Si seguimos, también vemos que $p(3) = 53$, $p(4) = 61$ y $p(5) = 71$ son primos. ¿Será cierto que $p(n)$ es primo para más valores de n? Pueden (deben) chequear por su cuenta que efectivamente $p(6)$, $p(7)$, $p(8)$, $p(9)$ y $p(10)$ son también primos. Bueno, ¡esto se pone interesante! Conjeturamos que $p(n)$ es primo para todo n. Curiosamente, $p(n)$ es primo para $1 \leq n \leq 39$, sin embargo es falso para $n = 40$, ya que $p(40) = 1681 = 41^2$. Es decir, $n = 40$ es un contraejemplo para nuestra conjetura, que resulta definitivamente falsa. El polinomio $p(n)$ fue encontrado por Leonhard Euler en 1772 (En 1798, Legendre observó que $q(n) = n^2 - n + 41$ da los mismos 40 primos para $1 \leq n \leq 40$).

(2) Consideremos los números de la forma

$$F_n = 2^{2^n} + 1 \qquad \text{para } n \geq 0 \tag{1.12}$$

Observemos que $F_0 = 2^1 + 1 = 3$, $F_1 = 2^2 + 1 = 5$, $F_2 = 2^4 + 1 = 17$ y $F_3 = 2^8 + 1 = 257$ son todos primos. Con un poco más de esfuerzo calculamos $F_4 = 2^{16} + 1 = 65.536$ y chequeamos que es primo. ¿Será cierto que F_n es siempre primo? Esto fue conjeturado por Fermat y por eso estos números reciben el nombre de *números de Fermat*. El siguiente es

$$F_5 = 2^{32} + 1 = 4.294.967.297.$$

¿Es primo? De manera muy ingeniosa, Euler (¡otra vez, cuando no!) demostró que $F_5 = 641 \cdot 6.700.417$. Es decir F_5 es compuesto, y por lo tanto constituye un contraejemplo que tira por tierra la conjetura. De todas formas, aun no se sabe si existen infinitos primos de Fermat, es decir infinitos n para los cuales F_n es primo. ◊

1.6. Ejercicios y problemas

Fragmento de una digresión del libro de Gentile [**5**, Cápitulo 0] a propósito de la lógica proposicional:

> *"En este curso de álgebra (y en general en matemática) se hacen afirmaciones, se enuncian propiedades, se definen cosas, se hacen demostraciones, se dan ejemplos y contraejemplos. Es claro que para que nuestra labor tenga un desarrollo feliz debemos lograr que todas las formulaciones se hagan con la máxima precisión.*
>
> *Es pues altamente deseable poseer un lenguaje que nos permita efectuar nuestras afirmaciones sin ambigüedades, con claridad y también economía.*
>
> *Puede ser útil un ejemplo para fijar ideas.*
>
> *Tomemos el juego de ajedrez. El lector que estudie un poco de matemática, notará que el esquema de juego del ajedrez es bastante análogo al esquema de trabajo en Matemática. Tablero y fichas corresponde a tener entes matemáticos (por ejemplo, puntos, rectas, conjuntos numéricos, funciones, matrices, etc.) y las reglas de movimiento corresponden a reglas válidas de razonamiento. Mover las piezas corresponde a "hacer matemáticas" (esencialmente: probar teoremas).*
>
> *Pero además, los ajedrecistas poseen una forma de escribir sus partidas: 1. $P4R$, $P4R$; 2. $C3AD$, $C3AR$; 3. $P4A$, $P3D$; . . . Esta situación es ideal. En matemática es muchísimo más complicado lograr un lenguaje realmente útil y práctico* [. . .]"

Ejercicios

Ejercicio 1.1. Indique cuáles de los siguientes enunciados son una proposición; para aquellos que lo son, determinar su valor de verdad.

(a) 7416 es un número par.

(b) Todos los profesores son buenos.

(c) $x > 5$.

(d) Hay al menos 3 números impares.

(e) Este enunciado es falso.

(f) Córdoba es mas populosa que Rosario.

Ejercicio 1.2. Determinar el valor de verdad de las proposiciones p y q dadas a continuación. Además, enunciar y determinar el valor de verdad de $p \wedge q$, $p \vee q$, $\neg(p \wedge q)$, $(\neg p) \wedge q$ y $\neg(p \vee q)$.

(a) p: Todos los cuadriláteros son cuadrados.
q: Existen triángulos no equiláteros.

(b) p: Todos los números enteros pares son positivos.
q: Los números impares son primos.

Ejercicio 1.3. Para cada una de las siguientes funciones proposicionales escribir el cuantificador existencial, el cuantificador universal y el cuantificador existencial único. Determinar el valor de verdad de cada uno de ellos sobre el conjunto $\mathbb{Z}$. Justificar.

(a) $P(x) : x(x+1)$ es par.

(b) $P(x) : x(x+1)$ es múltiplo de 3.

(c) $P(x) : x^2 = 1$.

(d) $P(x) : x + 5 = 5$.

Ejercicio 1.4. Para las proposiciones p y q dadas a continuación determinar su valor de verdad. Además, enunciar y determinar el valor de verdad de $p \wedge q$, $p \vee q$, $-(p \wedge q)$, $(-p) \wedge q$ y $-(p \vee q)$.

(a) p: 18 es divisible por 3.
q: No hay múltiplos de 7 entre 22 y 27.

(b) p: Todo número entero menor que 8 no es divisible por 11.
q: El profesor del teórico es más joven que todos los profesores del práctico.

Ejercicio 1.5. Consideremos las siguientes proposiciones condicionales:

(a) Si n es par y mayor que 2, entonces n no es primo.

(b) Si $x > 2$ ó $x < -2$, entonces $x^2 > 4$.

Para cada una de ellas, escribir las proposiciones recíproca, contraria y contrarrecíproca, como así también la proposición bicondicional. Determinar el valor de verdad de todas ellas.

Ejercicio 1.6. El parcial y el examen final tienen parte práctica y parte teórica. Para aprobar el parcial hay obtener un total de por lo menos 60 puntos u obteer en alguna de las dos partes al menos 45 puntos. Para aprobar el final hay que obtener en cada parte al menos 30 puntos. Decidir qué alumnos aprobaron el parcial y qué alumnos aprobaron el final.

Alumno	Parcial	Resultado	Final	Resultado
Analía	$35/25$		$40/25$	
Pedro	$45/10$		$40/30$	
Ramiro	$25/30$		$35/25$	
Paula	$50/35$		$40/45$	
Julia	$40/50$		$50/25$	

Problemas

Problema 1.7. Probar, usando tablas de verdad, las leyes asociativas y distributivas para la conjunción y la disyunción enunciadas más arriba.

Problema 1.8. Para cada una de las siguientes funciones proposicionales en dos variables escribir las distintas combinaciones de cuantificadores existencial y universal. Determinar el valor de verdad de cada uno de ellos sobre el conjunto $\mathbb{N}$ para la primera, y sobre $\mathbb{Z}$ para la segunda. Justificar.

(a) $P(x, n) : x^n = 1$.

(b) $P(x, y) : x + y = 0$.

Problema 1.9. Probar, dando un contraejemplo, que las siguientes proposiciones son falsas.

(a) Los números primos son impares.

(b) $\forall x \in \mathbb{N}, \quad x^2 - 10x + 24 \geq 0$.

(c) Todo subconjunto de $\mathbb{N}$ es finito.

(d) Toda recta del plano pasa por el origen.

Nota: En el ejercicio anterior el contraejemplo es un buen recurso para probar la no validez de los enunciados pues dichas proposiciones involucran el cuantificador universal.

Problema 1.10. Indique cuáles de los siguientes enunciados son proposiciones. Para aquellas que sean proposiciones determinar su valor de verdad. En caso contrario completarlas, de alguna manera, para que resulten proposiciones.

(a) Todos los números que son divisibles por 4 son divisibles por 2.

(b) $x > 0$.

(c) Existe un número par divisible por 3.

(d) Existe una solución de $x^2 = 2$.

Problema 1.11. Para cada una de las funciones proposicionales dadas en el **Ejercicio 1.3** escribir la negación de sus cuantificadores existencial, universal y existencial único. Determinar el valor de verdad de cada uno de ellos sobre el conjunto $\mathbb{Z}$. Justificar.

Problema 1.12. Probar las siguientes afirmaciones usando el método de prueba indicado.

(a) Para cada $n \in \mathbb{Z}$, n es impar $\Leftrightarrow -n$ es impar (*prueba directa*).

(b) Para todo $n \in \mathbb{Z}$, $n^3 + n^2 + n$ es impar $\Rightarrow n$ es impar (*contrarrecíproco*).

(c) Si m, n son enteros tales que $m^2 + m = 3n$, entonces n es par (*por contradicción*).

Problema 1.13. En cierto deporte por equipos se obtienen y pierden puntos durante el desarrollo de un partido. Gana el primero en obtener 10 puntos o una diferencia de por lo menos 5 puntos a su rival. En finales, para ganar hay que lograr 12 puntos o una diferencia de 5 puntos a su rival teniendo por lo menos 7 puntos. En cada decir en que momento se acaba el partido indicando el ganador.

Partido 1	Ganador	Partido 2	Ganador	Final 1	Ganador	Final 2	Ganador
0-0		0-0		0-0		0-0	
1-0		2-0		2-0		0-2	
2-0		2-1		3-0		0-5	
3-0		2-3		3-0		2-5	
4-0		4-3		5-0		5-5	
4-1		6-3		6-0		5-8	
4-2		6-6		6-0		7-8	
5-2		8-6		8-0		7-11	
6-2		10-6		8-0		7-12	
7-2		10-10		10-0		10-12	
7-3		10-11		12-0		11-12	

Capítulo 2

Conjuntos

"Nadie podrá expulsarnos del paraíso que Cantor creó para nosotros"
David Hilbert, matemático alemán (1862 – 1943)

Los conjuntos son objetos matemáticos que están en los cimientos de la matemática toda. Resulta imprescindible para todo estudiante de matemática conocer los aspectos básicos de la teoría de conjuntos.

En esta sección presentamos algunos conceptos elementales sobre conjuntos. Cabe destacar que la teoría de conjuntos es muy sofisticada y bien podría llevar uno o dos cursos completos aprender algo de ella. Basta hojear algunos de los libros específicos [**?**] para convercerse de ello.

En esta presentación recurrimos a la idea intuitiva de conjunto que la mayoría tenemos para evitar dar una definición totalmente rigurosa en un marco axiomático puro. Nos concentraremos en mostrar qué podemos hacer con ellos. La buena noticia es que lo que veamos aquí es suficiente para todos los temas posteriores del libro.

2.1. Definiciones básicas

Pertenencia, igualdad, contención

Un *conjunto* es una colección bien definida de objetos. La noción principal de la teoría de conjuntos es la de pertenencia. Si x es un *elemento* del conjunto A, decimos que x *pertenece* a A y escribimos

$$x \in A$$

y, en cambio, si x no es un elemento del conjunto A decimos que x *no pertenece* a A y escribimos

$$x \notin A$$

Dos conjuntos A y B son *iguales*,

$$A = B$$

si tienen los mismos elementos; es decir, si todo elemento de A pertenece a B y todo

elemento de B pertence a A. Los conjuntos A y B son distintos,

$$A \neq B$$

si algún elemento de A no pertence a B o si algún elemento de B no pertenece a A.

Si A y B son conjuntos y todo elemento de A pertence a B decimos que A es un *subconjunto* de B o que A está *incluido* o *contenido* en B. En este caso escrbimos

$$A \subseteq B \qquad \text{ó} \qquad B \supseteq A$$

Notemos que siempre vale $A \subseteq A$ y además que si A es un subconjunto de B y B es un subconjunto de C entonces A es un subconjunto de C, o sea

$$A \subseteq B \quad \text{y} \quad B \subseteq C \quad \Rightarrow \quad A \subseteq C$$

Si A está contenido en B y $A \neq B$, decimos que A está *contenido propiamente* en B. (A veces se escribe $A \subsetneq B$ para enfatizar esto.)

Se sigue que dos conjuntos son iguales si uno es subconjunto del otro y viceversa. Así, en la práctica para mostrar que dos conjuntos A y B son iguales muchas veces se prueba que $A \subseteq B$ y que $B \subseteq A$.

En símbolos,

$$\begin{array}{lcll} A \subseteq B & \Leftrightarrow & \forall x \in A,\, x \in B & \Leftrightarrow \quad \text{“}x \in A \Rightarrow x \in B\text{”} \\ A \not\subseteq B & \Leftrightarrow & \exists x \in A,\, x \notin B & \Leftrightarrow \quad \exists x \notin B,\, x \in A \\ A = B & \Leftrightarrow & A \subseteq B \text{ y } B \subseteq A & \Leftrightarrow \quad \text{“}x \in A \Leftrightarrow x \in B\text{”} \end{array} \tag{2.1}$$

Si dos conjuntos no tienen ningún elemento en común, se dice que son *disjuntos*. En símbolos, A y B son disjuntos si

$$x \in A \Rightarrow x \notin B$$

lo cual es equivalente a $x \in B \Rightarrow x \notin A$.

Los siguientes ejemplos sirven para aclarar los conceptos y definiciones dadas.

Ejemplos.

(1) Si $R = \{*, X, 23, \alpha, f_2\}$ y $S = \{\varnothing, \beta^\circ, X\}$ podemos decir que $23 \in R$ y que $* \in R$ pero $23 \notin S$ y $* \notin S$; que $X \in R$ y $X \in S$; que γ no pertenece a R ni a S; que R tiene cinco elementos y S tres.

(2) Sean L el conjunto de letras del alfabeto, V el conjunto de vocales y C el conjunto de consonantes. Luego $V \subsetneq L$ y $C \subsetneq L$, es decir V y C son subconjuntos propios de L. Además, V y C son disjuntos.

(3) Sea A el conjunto formado por los números $0, 3, 8, 15, 24, 35, 48$ y B el conjunto de los números de la forma $n^2 - 1$ con $1 \leq n \leq 7$. Es claro, por inspección, que ambos conjuntos son iguales. ◊

Conjunto universal y conjunto vacío

En la teoría de conjuntos existen dos conjuntos distinguidos, el conjunto vacío y el conjunto universal. El *conjunto vacío* es el conjunto que no tiene elementos y es denotado por $\varnothing$. Éste está contenido en todo otro conjunto.

En general, es de utilidad fijar de antemano el "universo" de objetos con que se quiere trabajar. Por ejemplo, en aritmética interesan principalmente los números naturales y enteros, mientras que en análisis interesan más los números reales y complejos. El conjunto *universal*, usualmente denotado $\mathcal{U}$, es el conjunto más grande en una discusión, y todos los demás conjuntos considerados serán subconjuntos de éste. Muchas veces este universo está tácitamente dado, o se sobreentiende del contexto en el que se está trabajando. Otras veces es necesario indicarlo. Por ejemplo, el conjunto de los números pares es $\{2, 4, 6, 8, \ldots\}$ en los naturales, mientras que resulta $\{\ldots, -6, -4, -2, 0, 2, 4, 6, \ldots\}$ si estamos trabajando con los números enteros.

Todo conjunto A está contenido en el conjunto universal y contiene al vacío, o sea

$$\varnothing \subseteq A \subseteq \mathcal{U}$$

Nota. Una manera de justificar que el vacío es subconjunto de todo otro conjunto A es la siguiente (por el absurdo). Para que esto no sea cierto, debería haber un conjunto A que no contiene al vacío, es decir $\varnothing \not\subseteq A$. Ahora, para que esto sea posible, debería haber un elemento de $\varnothing$ que no pertenece a A. Como es imposible hallar un tal elemento, no hay un tal conjunto A y $\varnothing \subseteq A$ para todo A.

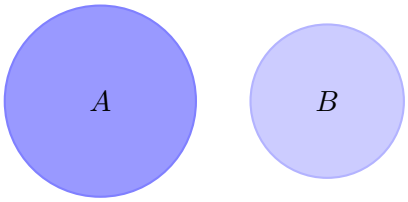
Diagramas de Venn

Los diagramas de Venn permiten representar gráficamente conjuntos genéricos sin importar la naturaleza de sus elementos. Esta representación resulta útil para entender algunos aspectos básicos de la teoría de conjuntos, como son las operaciones con conjuntos y algunas identidades de conjuntos.

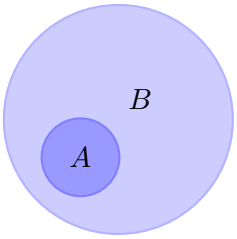
No daremos ninguna definición formal de diagrama de Venn, simplemente los presentamos de manera informal apelando al sentido común de los lectores. Para nuestros fines, basta pensar que a cada conjunto lo representamos como un círculo u óvalo.

Los siguientes diagrams de Venn representan a dos conjuntos abstractos A y B (no vacíos) en un mismo universo, mostrando distintas situaciones posibles según los elementos que compartan y los que no.

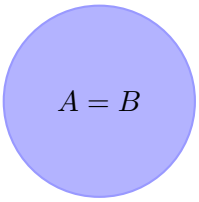
- Los conjuntos A y B no comparten ningún elemento (son disjuntos).



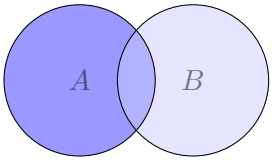
- Todos los elementos de A son elementos de B, es decir $A \subseteq B$, aunque son distintos.



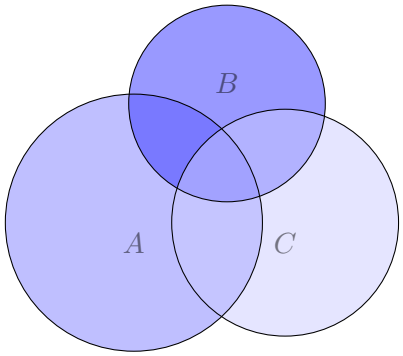
- $A = B$, es decir tienen los mismos elementos.



- A y B tienen algunos elementos en común, pero ninguno está contenido en el otro.



La situación general para 3 conjuntos es la siguiente



Nota histórica. Los *diagramas de Venn* fueron introducidos en 1880 por John Venn en el trabajo titulado "On the Diagrammatic and Mechanical Representation of Propositions and Reasonings" en la revista "Philosophical Magazine and Journal of Science", sobre diferentes formas de representar proposiciones por diagramas. El uso de estos tipos de diagramas, si bien se originaron antes, están asociados a Venn ya que fue él quien hizo un uso apropiado de ellos y formalizó y popularizó su uso. Venn no usaba el nombre "diagramas de Venn" y se refería a ellos como "círculos Eulerianos". El primero en usar el término "diagramas de Venn" fue Clarence Irving Lewis en 1918, en su libro "A Survey of Symbolic Logic".

2.2. Cómo definir conjuntos

Para definir conjuntos debemos de una manera u otra especificar qué objetos lo forman (¡y quienes no!). Existen básicamente dos formas distintas de hacerlo.

- Por EXTENSIÓN o definidos explícitamente: el conjunto se define listando o describiendo explícitamente cada uno de sus elementos.
- Por COMPRENSIÓN o definidos implícitamente: el conjunto de define por una o varias propiedades, quedando el conjunto determinado por aquellos objetos que tienen o satisfacen las propiedades listadas.

A un conjunto definido por extensión se lo denota en general listando sus elementos entre llaves. Por ejemplo, el conjnuto A formado por los elementos $a_1, a_2, \ldots, a_n$ se escribe

$$A = \{a_1, a_2, \ldots, a_n\}$$

A veces resulta conveniente usar puntos suspensivos para denotar elementos que se sobreentiende están en el conjunto. Así, por ejemplo, el conjunto $D = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ de dígitos puede escribirse sin lugar a dudas $D = \{0, 1, 2, \ldots, 8, 9\}$. Es aún mas común usar esto para conjuntos infinitos, por ejemplo los naturales $\mathbb{N} = \{1, 2, 3, 4, 5, \ldots\}$, ya que de otro modo sería imposible listar todos sus elementos.

Un conjunto definido por comprensión se denota en general usando llaves $\{\ \}$ y la propiedad definidora P. Por ejemplo, si B es el conjunto de todos los elementos x que cumplen la propiedad $P(x)$ se escribe

$$B = \{x \in \mathcal{U} : P(x)\}$$

y se lee B es "el conjunto de los x tal que $P(x)$". En general, puede haber varias propiedades $P_1, \ldots, P_n$ definidoras de un conjunto. En este caso

$$B = \{x \in \mathcal{U} :\ P_1(x), P_2(x), \ldots, P_n(x)\}$$

Cuando el universo $\mathcal{U}$ está sobreentendido, simplemente se escribe

$$B = \{x\ :\ P(x)\} \quad \text{o} \quad B = \{x\ :\ P_1(x), P_2(x), \ldots, P_n(x)\}.$$

Dado un elemento a de un conjunto A, es muy importante distinguir claramente entre este elemento y el conjunto formado por ese único elemento, denotado $\{a\}$. El primero es un elemento de A, mientras que el segundo es un subconjunto de A. En símbolos

$$a \in A, \qquad \{a\} \subset A, \qquad a \neq \{a\}$$

Ejemplos. Consideremos el universo de todas las letras de los alfabetos romano y griego. Sean $A = \{a, b, c, \ldots, z\}$ el conjunto de todas las letras del alfabeto romano y $\Lambda = \{\alpha, \beta, \gamma, \ldots, \zeta\}$ las del alfabeto griego.

(1) $a \in A$, $a \notin \Lambda$ y $\alpha \notin A$, $\alpha \in \Lambda$.

(2) A y Λ son disjuntos.

(3) Si $V = \{a, e, i, o, u\}$ es el conjunto de vocales y C el de consonantes, tenemos que V y C son disjuntos. El conjunto $D = \{a, e, o\}$ de vocales fuertes es un subconjunto propio de V.

(4) El conjunto de letras de la palabra "matematica" $B = \{m, a, t, e, i, c\}$ tiene 6 elementos. B tiene elementos en común con V y también con C, por lo tanto no es disjunto con ellos. Sin embargo, tampoco es un subconjunto de ninguno de ellos.

(5) Los conjuntos $\{p, q, \beta, s\}$ y $\{t, \theta, v\}$ son distintos y disjuntos.

(6) $\{p, \pi, r, s, \rho\} \neq \{s, \rho, u, v\}$, pero no son disjuntos.

(7) Los conjuntos $\{\delta, q, r, \epsilon, t, u, v\}$ y $\{\delta, t, u, v\}$ son distintos y el segundo es subconjunto del primero. ◊

Ejemplo. En este texto nos interesarán los conjuntos de números. Por ejemplo los conjuntos de números naturales, enteros y racionales, denotados respectivamente por

$$\mathbb{N} = \{1, 2, 3, 4, 5, \ldots\}$$
$$\mathbb{Z} = \{\ldots, -3, -2-, 1, 0, 1, 2, 3, \ldots\}$$
$$\mathbb{Q} = \{\tfrac{a}{b} : a, b \in \mathbb{Z}, b \neq 0\}$$

Pero también nos interesarán los números pares $\{2k : k \in \mathbb{Z}\}$ e impares $\{2k+1 : k \in \mathbb{Z}\}$; los múltiplos de siete $7\mathbb{Z} = \{7k : k \in \mathbb{Z}\}$; los múltiplos de cualquier $n \in \mathbb{Z}$, $n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$; los que tienen resto r, $0 \leq r < q$, al dividirlos por q, $\{qk + r : k \in \mathbb{Z}\}$. De vital importancia resultarán los números primos $\mathbb{P} = \{2, 3, 5, 7, 11, 13, 17, \ldots\}$. ◊

Ejemplos. Mostramos aquí algunos conjuntos definidos explícitamente y otros definidos implícitamente.

(1) Los conjuntos $A = \{p, \alpha, 10\}$ y $B = \{1, *, f, \square\}$ están dados explícitamente.

(2) El conjunto $B = \{\text{los alumnos de algebra de país}\}$ está dado implícitamente.

(3) Los conjuntos $C = \{\text{argentinos con pasaporte terminado en } 3\}$ y $D = \{\text{números enteros mayores que } -5 \text{ que no son múltiplos de } 3\}$ están dados implícitamente a partir de universos indicados explícitamente. En el primer caso *todos los argentinos* y en el segundo *los números enteros mayores que* -5.

(4) Dado $\mathcal{U} = \{\text{cordobeses}\}$, los conjuntos $B = \{\text{los que miden más de } 1,71 \text{ metros}\}$ y $C = \{\text{los que cumplen años en marzo}\}$ están dados implícitamente.

(5) Sea $\mathcal{U} = \mathbb{Z}$, el conjunto de todos los números enteros. El conjunto $A = \{-1, 0, 1\}$ está dado explícitamente, mientras que $B = \{z : z > 0\}$ y $D = \{z : \text{tales que su resto en la división por 3 es } 1\}$ están dados implícitamente. ◊

Las propiedades que se usen para definir conjuntos deben tener un valor de verdad definido, no ambiguo, para los objetos del universo elegido. Éste debe depender solamente del objeto. Por ejemplo, si el universo es el de todos los números naturales, la propiedad de *ser par* tiene un valor de verdad definido para cada número. El 4 es par y el 7 no es par. Veamos ejemplos de lo que no consideraremos como conjuntos.

Ejemplos. Ahora mostramos algunas descripciones que no definen conjuntos tal como queremos.

(1) Tanto las colecciones de "mujeres bonitas", de "buenos gobernantes" o de "políticos honestos", como las de "'cracks'de fútbol" o de "artistas exitosos" no son conjuntos en el sentido matemático que nos interesa.

(2) Si consideremos todos los números naturales que escritos en castellano ocupan menos de un renglón, éstos no forman un conjunto. La propiedad de *ocupar menos de un renglón al ser escrito en castellano* no tiene un valor de verdad definido, pues la longitud de dicha escritura depende del tamaño del renglón y de la persona que escriba, además del número en sí. Luego, esta propiedad no puede ser usada para definir implícitamente un conjunto de números naturales. ◊

Hemos presentado algunos aspectos básicos sobre cómo definir conjuntos. En el trabajo cotidiano con conjuntos aparecerán diversas formas más o menos flexibles de definir conjuntos que resultan muy prácticas y por ello son muy difundidas. Es bueno aceptar éstas y otras formas que pudieran surgir siempre y cuando no tengan ninguna ambigüedad y no dejen dudas respecto a los elementos que forman el conjunto que se quiere definir. Por ejemplo, es común el uso de puntos suspensivos "..." en algunas definiciones.

Hay que destacar que un mismo conjunto admite múltiples formas de ser presentado o descripto, como ya vimos en algunos ejemplos. En particular, cuando se listan explícitamente los elementos de un conjunto, el orden en que aparacen es irrelevante.

Ejemplos.

(1) $V = \{\text{vocales del español}\} = \{a, e, i, o, u\} = \{e, o, u, i, a\}$.

(2) $L = \{\text{letras del alfabeto}\} = \{a, b, c, \ldots, x, y, z\} = \{a, e, i, o, u, z, y, x, \ldots, d, c, b\}$.

(3) El conjunto de números naturales pares se puede definir por extensión:

$$P = \{2, 4, 6, 8, 10, 12, 14, 16, \ldots\}$$

y también por comprensión:

$$P = \{2m \,:\, m \in \mathbb{N}\} = \{n \in \mathbb{N} : n = 2k \text{ para algún } k \in \mathbb{N}\}.$$

(4) El conjunto vacío se puede describir por extensión así $\varnothing = \{\ \}$, y por comprensión así $\varnothing = \{x : x \neq x\}$. ◊

Observación. Una forma alternativa de definir conjuntos, aceptada y muy usada, es aquella en la que los elementos del mismo se construyen por medio de una FÓRMULA. Los elementos n del conjunto

$$C = \{n : n = m^2 + 2m - 3, m \in \mathbb{N}\}$$

se construyen por medio de la fórmula $n = m^2 + 2m - 3$, con m recorriendo los naturales. Es posible entonces (comenzar a) listarlos. Tomando $m = 1, 2, 3$ y 4 se obtienen respectivamente $0, 5, 12, 21 \in C$. Se dice que el conjunto C está dado PARAMÉTRICAMENTE, donde m es

el *parámetro*. Puede haber repeticiones. Por ejemplo, si pensamos en el conjunto definido por la misma fórmula pero sobre los enteros

$$D = \{n : n = m^2 + 2m - 3, m \in \mathbb{Z}\}$$

vemos que, como $m^2+2m-3 = (m-3)(m+1)$, para $m = 0$ se obtiene el mismo elemento que para $m = 2$, para $m = -1$ el mismo que para $m = 3$, y en general para $-k$ el mismo que para $k + 1$, para todo $k > 0$.

Digresión (Explícito versus implícito)**.**

• Explícito. Si un conjunto A está dado explícitamente, resulta fácil exhibir alguno de sus elementos, para esto basta tomar uno de los listados. Aún en el caso en que A esté dado paramétricamente, para exhibir un elemento basta tomar un valor cualquiera permititdo para el parámetro y exhibir el correspondiente elemento de A. Por ejemplo, si

$$A = \{n = 2m^2 + m - 1, \text{ con } m \in \mathbb{N}\}$$

tomamos $m = 1$ y exhibimos el elemento $n = 2 + 1 - 1 = 2$ de A.

Por otro lado, si un conjunto A está dado explícitamente, puede no ser fácil decidir si un cierto elemento del universo pertenece o no a A. Por ejemplo, decidir si un número dado está en el conjunto $A = \{$números de libreta de todos los alumnos de la Universidad$\}$ puede requerir comparar el número dado con cada uno de los elementos de A.

Otros ejemplos: ¿Es 4928931 un número telefónico válido en la guía de Córdoba? ¿Pertenece 15.672.899.267.736.398.490.958.843.758.375.875.983 al conjunto de números primos? ¿Está $10^{100} + 2^{17} + 3$ en el conjunto de los números divisibles por 167?

• Implícito. Si un conjunto B está dado implícitamente, resulta en principio fácil decidir si un elemento del universo pertenece o no a B, ya que para esto sólo hay que verificar que el elemento elegido tiene las propiedades que definen a B. Está claro que la dificultad de esta verificación depende de las propiedades en sí. Por ejemplo, si tomamos el conjunto de números que tienen resto 1 al dividir por 3,

$$B = \{n : n = 3k + 1, k \in \mathbb{N}\}$$

para decidir si el 50 o el 100 pertenecen a B debemos dividirlos por 3 y mirar su resto. Como $50 = 3 \cdot 16 + 2$ y $100 = 3 \cdot 33 + 1$ se sigue que $50 \notin B$ y $100 \in B$.

En cambio, puede no ser fácil exihibir algún elemento de B, pues para esto hay que encontrar algún elemento del universo que tenga todas las propiedades que definen a B. Por ejemplo, si

$$P = \{p \in \mathbb{N} : p \text{ primo y } p > 2^{2015}\}$$

no es fácil ni siquiera con una máquina exhibir un primo tan grande.

Paradojas †

Finalmente, como ya hemos mencionado, insistimos en que no cualquier propiedad o proposición es aceptable para definir un conjunto. Esto sucede por ejemplo si quisieramos

considerar "el conjunto" formado por todos los conjuntos que no se tienen a sí mismos como uno de sus elementos. Supongamos que definimos el "conjunto"

$$M = \{X : X \notin X\}$$

es decir, usando la propiedad $P(X) : X \notin X$. Veamos si la noción de pertenencia es clara en este caso. Suponiendo que M fuera un conjunto, tomemos $X = M$ y veamos si M pertenece o no a M.

- Si $M \in M$ entonces ¡¡ $M \notin M$!!
- Si $M \notin M$ entonces ¡¡ $M \in M$!!

En ambos casos se llega a una contradicción. Luego, M no es un conjunto. El problema aquí está en la propiedad usada. Este fenómeno fue observado por Bertrand Russell y es llamado una *paradoja* [*].

Una versión de la paradoja de Russell es la conocida como la *paradoja del barbero*: Un rey de una lejana comarca, al darse cuenta de la falta de barberos en su región, ordenó que los barberos sólo afeitaran a aquellas personas que no pudieran hacerlo por sí mismas. Cierto día el rey llamó a un barbero para que lo afeitara y éste aprovecho la ocasión y le contó su problema:

> *"En mi pueblo soy el único barbero. No puedo afeitar al barbero de mi pueblo, ¡que soy yo!, ya que si lo hiciera, entonces podría afeitarme por mí mismo, por lo tanto ¡no debería afeitarme! Pero, si por el contrario no me afeito, entonces algún barbero debería afeitarme, ¡pero yo soy el único barbero de allí!"*

Al rey le gustó la argumentación del barbero y lo recompensó.

Nota. Existen muchas otras paradojas, por ejemplo las paradojas lógicas. Invitamos al lector curioso a investigar sobre ellas por su cuenta, ya que es divertido y muy instructivo. Las más conocidas de este tipo son la *paradoja del mentiroso* (atribuída al griego Eubulides de Mileto, quien vivió en el siglo IV a.C.) dada por *"esta oración es falsa"* y la *paradoja de la suerte* dada por *"ser supersticioso es de mala suerte"*. A veces se suele confundir a la conjetura del mentiroso con la *paradoja de Epiménides* (poeta y filósofo del siglo VI a.C.), quien siendo cretense dijo: *"todos los cretenses son mentirosos"*. Cuando veamos conjuntos infinitos veremos algunas paradojas más.

2.3. Operaciones con conjuntos

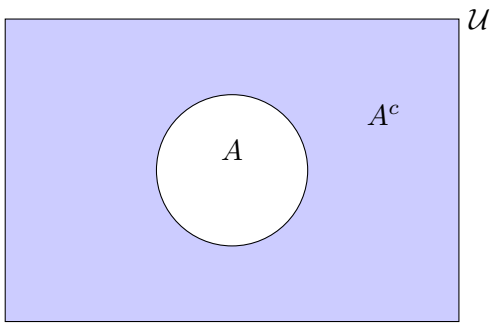
Hasta aquí hemos discutido cómo definir conjuntos. Ahora describiremos algunas cosas que podemos hacer con ellos. En particular, mostraremos cómo construir nuevos conjuntos a partir de otros dados por medio de operaciones simples. Son estas operaciones las que hacen de los conjuntos una herramienta útil en matemática. No sólo permiten construir estructuras sino también permiten describir estructuras complicadas en términos de otras más simples.

[*]Del latín *paradoxus* y ésta del griego *paradoxon*; es una proposición en apariencia verdadera que conlleva a una contradicción lógica o a una situación que infringe el sentido común.

Mostramos a continuación varias maneras de construir nuevos conjuntos a partir de uno o de dos conjuntos dados. Estas operaciones permiten hacer una suerte de aritmética con conjuntos. Sus reglas, identidades y resultados, son válidos para cualqueir tipo de conjuntos independientemente de la naturaleza de sus elementos.

- COMPLEMENTO DE UN CONJUNTO. Dado un conjunto A en un universo $\mathcal{U}$, el *complemento* de A, denotado A^c, es el conjunto de todos los elementos de $\mathcal{U}$ que no pertenecen a A.

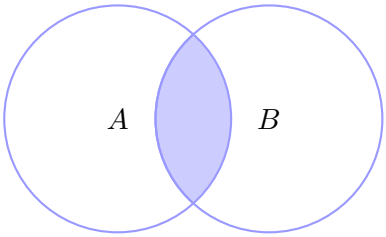
$$A^c = \{x \in \mathcal{U} : x \notin A\} = \{x : x \notin A\}$$



  Nota: en algunos textos se usan otras notaciones como $\mathbf{C}A$ o $\bar{A}$.

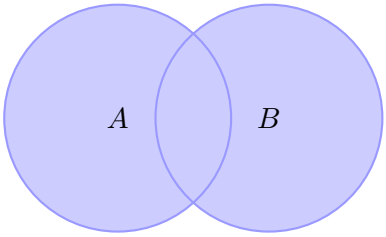
- INTERSECCIÓN DE DOS CONJUNTOS. Dados dos conjuntos A y B, la *intersección* de A y B, denotada $A \cap B$, es el conjunto formado por los elementos que tienen en común A y B.

$$A \cap B = \{x : x \in A \wedge x \in B\}$$



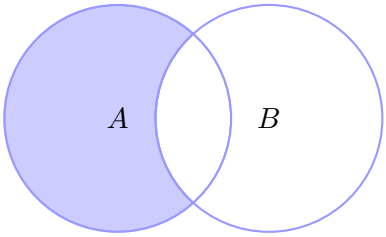
- UNIÓN DE DOS CONJUNTOS. Dados dos conjuntos A y B, la *unión* de A y B, denotada $A \cup B$, es el conjunto formado por todos los elementos que tienen A y B.

$$A \cup B = \{x : x \in A \vee x \in B\}$$



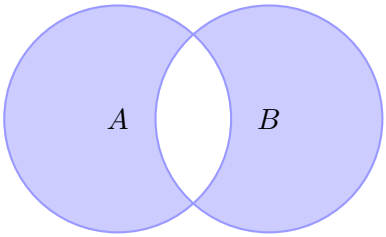
- DIFERENCIA DE DOS CONJUNTOS. Dados dos conjuntos A y B, la *diferencia* de A y B, denotada $A - B$, es el conjunto formado por los elementos de A que no pertenecen a B. En símbolos,

$$A - B = \{x : x \in A \wedge x \notin B\}$$



- DIFERENCIA SIMÉTRICA DE DOS CONJUNTOS. La *diferencia simétrica* de dos conjuntos A y B, denotada $A \triangle B$, es la unión de las diferencias $A - B$ y $B - A$. Es decir, es el conjunto formado por los elementos de A que no pertenecen a B y los elementos de B que no pertenecen a A. En símbolos,

$$A \triangle B = \{x : (x \in A \wedge x \notin B) \vee (x \in B \wedge x \notin A)\} = (A - B) \cup (B - A)$$



Ejemplos.

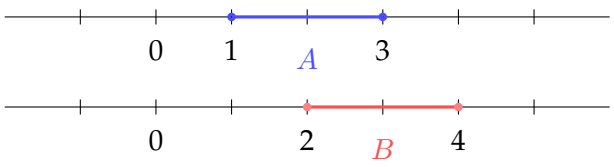
(1) Sean A el conjunto de naturales pares entre 1 y 13 y B el conjunto de múltiplos de 3 entre 1 y 13. Es decir

$$A = \{2, 4, 6, 8, 10, 12\} \quad \text{y} \quad B = \{3, 6, 9, 12\}.$$

Se tiene entonces que

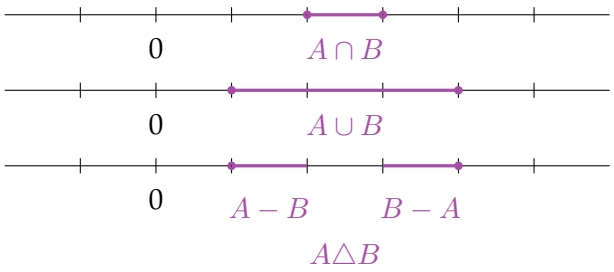
$$A \cap B = \{6, 12\}, \qquad A \cup B = \{2, 3, 4, 6, 8, 9, 10, 12\},$$
$$A - B = \{2, 4, 8, 10\}, \qquad B - A = \{3, 9\}, \qquad A \triangle B = \{2, 3, 4, 8, 9, 10\}.$$

(2) Consideremos los intervalos de números reales $A = [1, 3]$ y $B = [2, 4]$, que representamos gráficamente así:



Se tiene entonces que

$$A \cap B = [2, 3], \qquad A \cup B = [1, 4],$$
$$A - B = [1, 2), \qquad B - A = (3, 4], \qquad A \triangle B = [1, 2) \cup (3, 4].$$



La validez de las siguientes identidades es inmediata a partir de las definiciones. Aquí A es cualquier conjunto del universo $\mathcal{U}$.

$$\begin{aligned} A \cup \varnothing = A \quad &\text{y} \quad A \cap \varnothing = \varnothing \\ A \cup A = A \quad &\text{y} \quad A \cap A = A \\ A \cup \mathcal{U} = \mathcal{U} \quad &\text{y} \quad A \cap \mathcal{U} = A \\ \mathcal{U}^c = \varnothing \quad &\text{y} \quad \varnothing^c = \mathcal{U} \\ A \cup A^c = \mathcal{U} \quad &\text{y} \quad A \cap A^c = \varnothing \end{aligned} \tag{2.2}$$

También se sigue directamente de las definiciones que la intersección y la unión de conjuntos son conmutativas y asociativas. Para conjuntos A, B, C cualesquiera vale que

$$\begin{aligned} A \cup B &= B \cup A \\ A \cap B &= B \cap A \end{aligned} \tag{2.3}$$

y que

$$\begin{aligned} A \cup (B \cup C) &= (A \cup B) \cup C \\ A \cap (B \cap C) &= (A \cap B) \cap C \end{aligned} \tag{2.4}$$

La unión y la intersección de una familia de conjuntos †

Las operaciones de unión e intersección de conjuntos pueden realizarse para cualquier número finito n de conjuntos $A_1, A_2, \ldots, A_n$:

$$\bigcap_{i=1}^{n} A_i = A_1 \cap A_2 \cap \cdots \cap A_n = \{x : x \in A_1 \wedge x \in A_2 \wedge \cdots \wedge x \in A_n\}$$
$$\bigcup_{i=1}^{n} A_i = A_1 \cup A_2 \cup \cdots \cup A_n = \{x : x \in A_1 \vee x \in A_2 \vee \cdots \vee x \in A_n\}$$

Todavía con más generalidad podemos considerar una familia arbitraria $\mathcal{F}$ de conjuntos y su unión e intersección

$$\bigcap_{A \in \mathcal{F}} A = \{x : \ x \in A \text{ para todo } A \in \mathcal{F}\} = \{x : \forall A \in \mathcal{F}, x \in A\}$$
$$\bigcup_{A \in \mathcal{F}} A = \{x : x \in A \text{ para algún } A \in \mathcal{F}\} = \{x : \exists A \in \mathcal{F}, x \in A\}$$

Si la familia está *indexada* por un conjunto I, es decir $\mathcal{F} = \{A_i\}_{i \in I}$ donde I es un conjunto de índices y hay un conjunto A_i para cada índice $i \in I$, entonces tenemos

$$\bigcap_{i \in I} A_i = \{x : x \in A_i \text{ para todo } i \in I\}$$
$$\bigcup_{i \in I} A_i = \{x : x \in A_i \text{ para algún } i \in I\}$$

Si $I = \mathbb{N}$ se dice que $\mathcal{F}$ es una familia numerable de conjuntos y en este caso se escribe

$$\bigcap_{i=1}^{\infty} A_i \qquad \text{y} \qquad \bigcup_{i=1}^{\infty} A_i$$

2.4. Identidades de conjuntos

A partir de ciertos conjuntos dados podemos construir nuevos conjuntos usando las operaciones descriptas anteriormente. A veces, distintas combinaciones de estas operaciones determinan en última instancia un mismo conjunto. Es una verdad de las construcciones elegidas. Esto es una *identidad* de conjuntos. Recordamos que para probar que dos conjuntos dados son iguales, podemos por un lado probar que uno está contenido en el otro y que éste contiene al primero.

Por ejemplo, ya hemos observado que tanto la unión como la intersección son *asociativas*, es decir que $A \cup (B \cup C) = (A \cup B) \cup C$ y $A \cup (B \cap C) = (A \cap B) \cap C$. Ahora nos

preguntamos qué ocurre si se combinan la unión con la intersección. Por ejemplo, ¿es verdad que $A \cap (B \cup C) = (A \cap B) \cup C$? Usando diagramas de Venn, es fácil inferir que esta identidad no debería ser cierta. A partir de esto, es fácil dar ejemplos de conjuntos A, B, C que no satisfacen la "identidad" de arriba (por favor no sea haragán y de algunos usted mismo!) Luego, en general tenemos que

$$A \cap (B \cup C) \neq (A \cap B) \cup C$$

Veamos ahora algunas identidades importantes.

Proposición 2.1. *Sean A, B y C conjuntos arbitrarios. Valen las siguientes identidades.*

(a) Doble complemento o idempotencia:

$$(A^c)^c = A$$

(b) Leyes distributivas de $\cap$ y $\cup$:

$$\begin{aligned} A \cap (B \cup C) &= (A \cap B) \cup (A \cap C) \\ A \cup (B \cap C) &= (A \cup B) \cap (A \cup C) \end{aligned}$$

(c) Leyes de De Morgan:

$$\begin{aligned} (A \cap B)^c &= A^c \cup B^c \\ (A \cup B)^c &= A^c \cap B^c \end{aligned}$$

Demostración. En todos los casos usaremos (2.1).

(a) Simplemente notar que, como $A^c = \{x : x \notin A\}$, se tiene que

$$x \in (A^c)^c \quad \Leftrightarrow \quad x \notin A^c \quad \Leftrightarrow \quad x \in A$$

y esto implica que $(A^c)^c = A$.

(b) Usaremos las leyes distributivas entre $\wedge$ y $\vee$ en (1.2). Para la primera igualdad hacemos

$$\begin{aligned} x \in A \cap (B \cup C) &\Leftrightarrow (x \in A) \wedge (x \in B \cup C) \\ &\Leftrightarrow (x \in A) \wedge (x \in B \vee x \in C) \\ &\Leftrightarrow (x \in A \wedge x \in B) \vee (x \in A \wedge x \in C) \\ &\Leftrightarrow x \in (A \cap B) \cup (A \cap C). \end{aligned}$$

Leyendo las flechas $\Rightarrow$ probamos que $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$. Recíprocamente, leyendo las flechas en el sentido contrario $\Leftarrow$, probamos que $A \cap (B \cup C) \supseteq (A \cap B) \cup (A \cap C)$.

Análogamente, para la segunda igualdad, tenemos que

$$\begin{aligned} x \in A \cup (B \cap C) &\Leftrightarrow (x \in A) \vee (x \in B \cap C) \\ &\Leftrightarrow (x \in A) \vee (x \in B \wedge x \in C) \\ &\Leftrightarrow (x \in A \vee x \in B) \wedge (x \in A \vee x \in C) \\ &\Leftrightarrow x \in (A \cup B) \cap (A \cup C). \end{aligned}$$

Luego, hemos probado que $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$ y $A \cup (B \cap C) \supseteq (A \cup B) \cap (A \cup C)$.

(c) Aquí usaremos las negación de una conjunción y de una disyunción vista en (1.5). En el primer caso se tiene

$$\begin{aligned} x \in (A \cap B)^c &\Leftrightarrow x \notin A \cap B \\ &\Leftrightarrow \neg(x \in A \wedge x \in B) \\ &\Leftrightarrow \neg(x \in A) \vee \neg(x \in B) \\ &\Leftrightarrow (x \in A^c) \vee (x \in B^c) \\ &\Leftrightarrow x \in A^c \cup B^c. \end{aligned}$$

La segunda identidad puede ser probada similarmente y lo dejamos como ejercicio. Resulta más interesante probarla usando las propiedades ya vistas. Aplicando la ley de De Morgan ya probada a los conjuntos A^c y B^c (en lugar de a A y a B) tenemos

$$A \cup B = (A^c)^c \cup (B^c)^c = (A^c \cap B^c)^c.$$

Tomando complementos, por (a), obtenemos

$$(A \cup B)^c = ((A^c \cap B^c)^c)^c = A^c \cap B^c,$$

que es lo que queríamos probar. □

Observación. Observar que las identidades en (b) y (c) de la Proposición 2.1 son duales, en el sentido que intercambiando "unión" por "intersección" en la primera se obtiene la segunda y viceversa. En las pruebas, esto equivale a intercambiar los roles de "y" con "o".

Nota. Es un buen ejercicio interpretar y comprobar las identidades previas usando diagramas de Venn. De hecho, notemos que usando dichos diagramas, tomando el miembro izquierdo (resp. derecho) en cualquiera de las identidades de la Proposición 2.1 podríamos "adivinar" o intuir la expresión de la derecha (resp. izquierda).

Volvamos sobre las operaciones básicas de unión e intersección. Es claro, y se sigue inmediatamente de la definición, que para cualquier par de conjuntos A y B se tiene

$$A \subseteq A \cup B \quad \text{y} \quad A \cap B \subseteq A$$

Es decir, si a un conjunto A le unimos un conjunto B, el resultado es un conjunto más grande (que A), mientras que si a A lo intersecamos con B, obtenemos un conjunto más chico (que A).

Ahora, no es cierto que siempre $A \cup B$ es estrictamente más grande que A ni que $A \cap B$ es estrictamente más chico que A. La proposición que sigue dice exactamente cuándo la unión y la intersección son estrictamente más grande y estrictamente más chica, respectivamente. Además muestra cómo se comporta el complemento respecto a la inclusión.

Proposición 2.2. *Para todo par de conjuntos A y B vale que:*

(a) $A \subseteq B \quad \Leftrightarrow \quad B^c \subseteq A^c$.

(b) $A \cup B = B \quad \Leftrightarrow \quad A \subseteq B$.

(c) $A \cap B = A \quad \Leftrightarrow \quad A \subseteq B$.

Demostración. (a) Sabemos que $A \subseteq B$ es lo mismo que decir $x \in A \Rightarrow x \in B$. Esta implicación es equivalente a su contrarrecíproca $x \notin B \Rightarrow x \notin A$, o sea $B^c \subseteq A^c$.

(b, $\Rightarrow$) Sea $x \in A \subseteq A \cup B$. Luego $x \in A$ o $x \in B$, pero como $A \cup B = B$ se tiene que $x \in B$; como x es arbitrario se sigue que $A \subseteq B$.

(b, $\Leftarrow$) Si $x \in A \cup B$, entonces $x \in A$ o $x \in B$. Como $A \subseteq B$, por hipótesis, en cualquiera de los dos casos se sigue que $x \in B$. Luego resulta que $A \cup B \subseteq B$.

(c) Tomando complementos, la identidad en (c) es equivalente a $A^c = (A \cap B)^c = A^c \cup B^c$, por la ley de De Morgan. Por (b), esto pasa si y sólo si $B^c \subseteq A^c$. Ahora, por (a), esto pasa si y sólo si $(A^c)^c \subseteq (B^c)^c$; como $(A^c)^c = A$ y $(B^c)^c = B$ resulta lo que queríamos demostrar. □

Observación. El item (c) se puede probar de manera análoga al item (b). ¿Se anima a intentarlo? Nosotros preferimos hacerlo usando las leyes de De Morgan y los items (a) y (b) que acabábamos de probar.

Mirando los diagramas de Venn que describen la diferencia y la diferencia simétrica es posible imaginar que ambas se pueden definir a partir de los conjuntos dados usando la intersección, el complemento y la unión. En efecto,

Proposición 2.3. *Para todo par de conjuntos A y B se tiene que:*

(a) $A - B = A \cap B^c = (A^c \cup B)^c$.

(b) $A \triangle B = (A \cap B^c) \cup (B \cap A^c)$.

Demostración.
(a) Para la primera igualdad tenemos $x \in A - B \;\Leftrightarrow\; x \in A \wedge x \notin B \;\Leftrightarrow\; x \in A \cap B^c$. La segunda igualdad sale tomando complemento, aplicando la ley de De Morgan y por último la idempotencia.
(b) Usando (a), tenemos que $A \triangle B = (A - B) \cup (B - A) = (A \cap B^c) \cup (B \cap A^c)$. □

Como consecuencia tenemos una nueva expresión alternativa para la diferencia simétrica.

Corolario 2.4. *Para cualquier par de conjuntos A y B vale*

$$A \triangle B = (A \cup B) - (A \cap B)$$

Demostración. Usando las leyes distributivas y de De Morgan repetidas veces tenemos que

$$\begin{aligned} A\triangle B &= (A\cap B^c)\cup(B\cap A^c)\\ &= \big((A\cap B^c)\cup B\big)\cap\big((A\cap B^c)\cup A^c\big)\\ &= \big((A\cup B)\cap(B^c\cup B)\big)\cap\big((A\cup A^c)\cap(B^c\cup A^c)\big)\\ &= (A\cup B)\cap(B^c\cup A^c)\\ &= (A\cup B)\cap(B\cap A)^c\\ &= (A\cup B)-(A\cap B) \end{aligned}$$

Notar que hemos usado además que $C\cup C^c=\mathcal{U}$ y $C\cap\mathcal{U}=C$. □

2.5. Producto cartesiano

El producto cartesiano de dos o más conjuntos es un nuevo conjunto que se contruye a partir de éstos. Una diferencia sustancial con las construcciones estudiadas más arriba, es que los elementos del producto cartesiano son de una naturaleza distinta a la de los elementos de los conjuntos dados. Todas las contrucciones anteriores producen conjuntos en el mismo universo del que son parte los conjuntos dados. En este caso no sucede lo mismo.

Recordemos que $\{a,b\}=\{b,a\}$, ya que no importa el orden en que listamos los elementos de un conjunto. Sin embargo, muchas veces será de gran utilidad considerar listas de elementos donde sí importa el orden. Un *par ordenado* es un conjunto de 2 elementos, denotado por

$$(a,b)$$

donde importa el orden; en general $(a,b)\neq(b,a)$. Decimos que a es el primer elemento del par ordenado (a,b) y que b es el segundo elemento del par. Una manera formal de definir el par ordenado es

$$(a,b)=\{\{a\},\{a,b\}\}$$

Con esta definición es claro que $(a,b)\neq(b,a)$, si $a\neq b$. Notar que $(a,a)=\{\{a\}\}$.

Definición. Dados dos conjuntos A y B, el *producto cartesiano* [*] de A por B, denotado por $A\times B$, es el conjunto de pares ordenados cuyo primer elemento pertenece a A y el segundo pertenece a B. En símbolos,

$$A\times B=\{(a,b):\ a\in A,\ b\in B\}$$

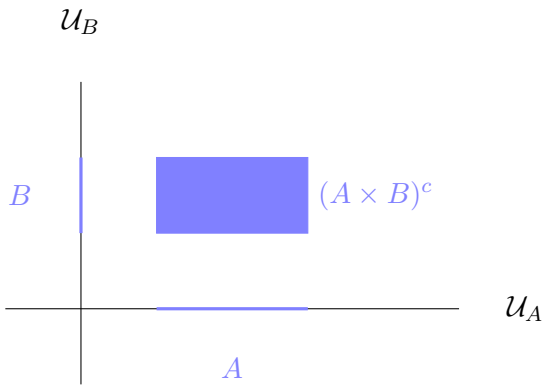
Por ejemplo, si $A=\{a_1,a_2\}$ y $B=\{b_1,b_2,b_3\}$ entonces $A\times B$ consta de los pares (a_1,b_1), (a_1,b_2), (a_1,b_3), (a_2,b_1), (a_2,b_2) y (a_2,b_3).

Observación. Si los respectivos conjuntos universales para A y B son $\mathcal{U}_A$ y $\mathcal{U}_B$, el conjunto universal para $A\times B$ es el producto de los conjuntos universales de A y B, es decir

$$\mathcal{U}_{A\times B}=\mathcal{U}_A\times\mathcal{U}_B$$

[*] El nombre producto cartesiano es atribuido a Frechèt, en honor a Renè Descartes y el uso que éste hacía de pares de números para representar puntos del plano en geometría analítica.

Resulta muy conveniente representar gráficamente al producto cartesiano $A \times B$ en un sistema cartesiano, es decir en el plano con dos rectas, una horizontal y otra vertical, que reprentan a $\mathcal{U}_A$ y $\mathcal{U}_B$ respectivamente. Genéricamente, un producto cartesiano se ve como un rectángulo en el plano.

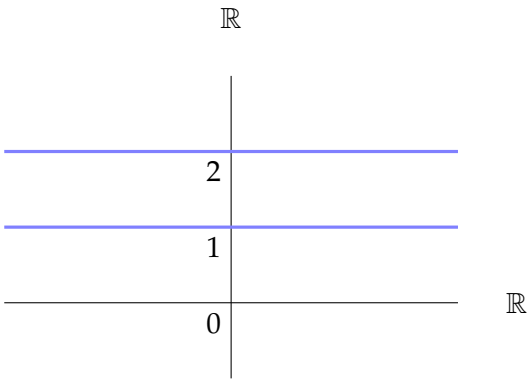


Cabe mencionar que esta representación nada tiene que ver con la representación por diagramas de Venn. Además, ésta es exclusiva para el producto cartesiano de 2 o 3 conjuntos (en este caso usamos 3 ejes). Para el producto cartesiano de 4 o más conjuntos, ya no es posbile hacer una representación gráfica decente.

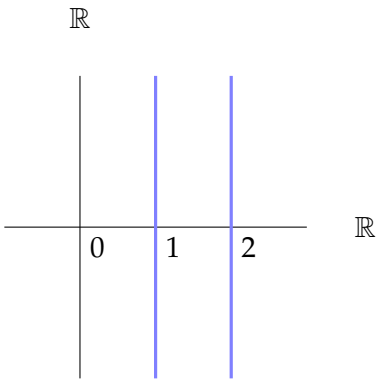
Ejemplos.

(1) Uno de los productos cartesianos más conocidos es quizás $\mathbb{R} \times \mathbb{R}$. La identificación usual de $\mathbb{R} \times \mathbb{R}$ con el plano permite entender al producto cartesiano y éste resulta muy útil para, por ejemplo, entender la geometría Euclidea del plano. En este universo consideramos distintos productos cartesianos:

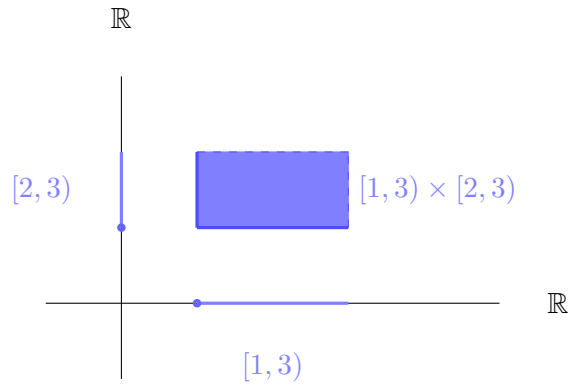
(i) $\mathbb{R} \times \{1, 2\}$.



(II) $\{1,2\} \times \mathbb{R}$.

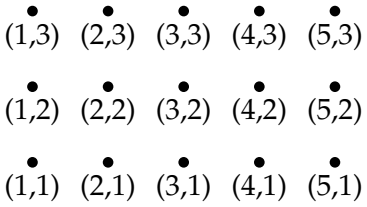


(III) $[1,3) \times [2,3)$.

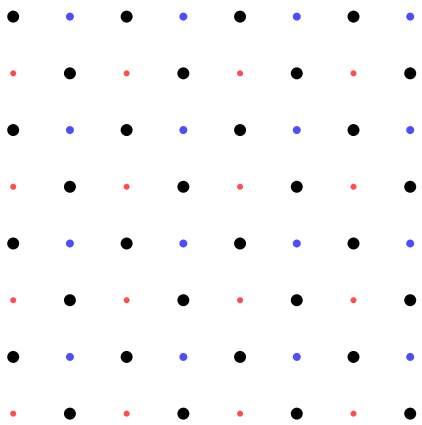


(2) Consideremos en $\mathbb{N} \times \mathbb{N}$ los siguientes productos cartesianos.

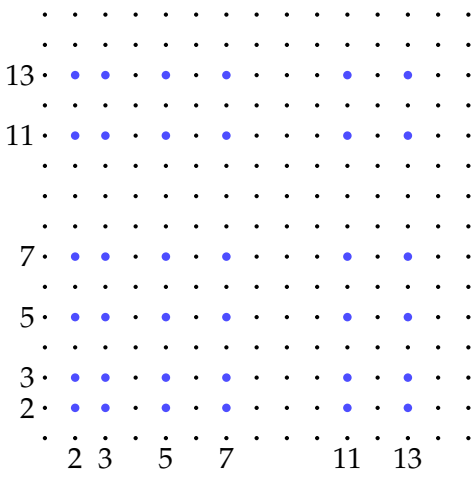
(I) $\{1,2,3,4,5\} \times \{1,2,3\}$.



(II) $I = \{\text{impares}\} \times \{\text{impares}\}$,
$P = \{\text{pares}\} \times \{\text{pares}\}$ y
$C = \{\text{pares}\} \times \{\text{impares}\} \cup \{\text{impares}\} \times \{\text{pares}\}$.



(3) $\mathcal{P} \times \mathcal{P}$, donde $\mathcal{P}$ es el conjunto de números primos menores que 15.



(4) Sean $A = \{d, \square, \alpha, \text{zapallo}\}$ y $B = \{1, 2\} \times \{x, y, z\}$. El producto cartesiano $A \times B$ tiene 4×6 elementos. Seis de sus pares ordenados tienen como primer elemento a d, entre ellos $(d, (2, x))$ y $(d, (1, z))$. El par $(\alpha, 2)$ no es un elemento de $A \times B$ ni tampoco lo es $(\alpha, 2, x)$. Tres elementos de $A \times B$ con primer elemento "zapallo" son: $(\text{zapallo}, (1, x))$, $(\text{zapallo}, (1, y))$ y $(\text{zapallo}, (1, z))$. ◊

Nos preguntamos ahora sobre las operaciones de conjuntos que vimos y el producto cartesiano. Para pensar en estas preguntas e intentar responderlas puede ser útil pensar en la representación de los productos cartesianos como rectángulos del plano.

Preguntas.

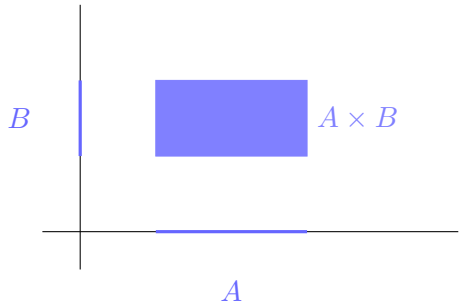
(1) ¿Es $(A \times B)^c = A^c \times B^c$?

(2) ¿Hay alguna buena descripción para el conjunto $(A \times B) \cup (A' \times B')$?

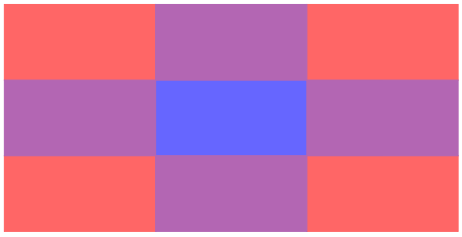
(3) ¿Y para $(A \times B) \cap (A' \times B')$?

Mirando algunos ejemplos, para lo cual ayuda la representación gráfica, podemos intuir las respuestas para las preguntas previas. Este es un buen ejercicio para la casa.

Ejemplo. Los siguientes dibujos sirven para contestar la primera pregunta. Vemos en el centro al rectángulo que representa a $A \times B$, y todo lo que está fuera de él, es su complemento.



En este dibujo vemos $(A \times B)^c$ dividido en ocho regiones, 4 rojas y 4 violetas.



Las regiones rojas forman el producto cartesiano $A^c \times B^c$. Por lo tanto, la respuesta a la primera pregunta es NO. Las regiones violetas forman $(A \times B^c) \cup (B \times A^c)$.

También vemos que las restantes cuatro regiones, en violeta, están formadas por pares de puntos uno en A y otro en el complemento de B o uno en complemento de A y otro en B. De aquí podemos deducir una expresión para el complemento de $A \times B$:

$$(A \times B)^c = (A^c \times B^c) \cup (A \times B^c) \cup (A^c \times B)$$

Análogamente, del dibujo se deduce que

$$(A \times A') \cap (B \times B') = (A \cap A') \times (B \cap B')$$

y que $(A \times A')$ y $(B \times B')$ son disjuntos si y sólo si A y A' o B y B' lo son.

Dejamos la demostración formal de estas fórmulas como ejercicio (ver Problemas 2.14 y 2.15). ◊

Veamos que el producto cartesiano distribuye uniones e intersecciones, y por lo tanto la diferencia de conjuntos.

Proposición 2.5. *Para A, B y X conjuntos arbitrarios valen las siguientes identidades.*

(a) $(A \cup B) \times X = (A \times X) \cup (B \times X)$.

(b) $(A \cap B) \times X = (A \times X) \cap (B \times X)$.

(c) $(A - B) \times X = (A \times X) - (B \times X)$.

Demostración. Basta usar las definiciones de producto cartesiano y las leyes distributivas de $\wedge$ y $\vee$ en cada caso.

(a) Tenemos que

$$\begin{aligned}
(c,x) \in (A \cup B) \times X \quad &\Leftrightarrow \quad (c \in A \cup B) \ \wedge \ (x \in X) \\
&\Leftrightarrow \quad (c \in A \ \vee \ c \in B) \ \wedge \ (x \in X) \\
&\Leftrightarrow \quad (c \in A \ \wedge \ x \in X) \ \vee \ (c \in B \ \wedge \ x \in X) \\
&\Leftrightarrow \quad (c,x) \in A \times X \ \vee \ (c,x) \in B \times X \\
&\Leftrightarrow \quad (c,x) \in (A \times X) \cup (B \times X)\,.
\end{aligned}$$

(b) Ahora,

$$\begin{aligned}
(c,x) \in (A \cap B) \times X \quad &\Leftrightarrow \quad (c \in A \cap B) \ \wedge \ (x \in X) \\
&\Leftrightarrow \quad (c \in A \ \wedge \ c \in B) \ \wedge \ (x \in X) \\
&\Leftrightarrow \quad (c \in A \ \wedge \ x \in X) \ \wedge \ (c \in A \ \wedge \ x \in X) \\
&\Leftrightarrow \quad (c,x) \in A \times X \ \wedge \ (c,x) \in B \times Y \\
&\Leftrightarrow \quad (c,x) \in (A \times X) \cap (B \times X)\,.
\end{aligned}$$

(c) Finalmente,

$$\begin{aligned}
(c,x) \in (A - B) \times X \quad &\Leftrightarrow \quad (c \in A - B) \ \wedge \ (x \in X) \\
&\Leftrightarrow \quad (c \in A \wedge c \notin B) \ \wedge \ (x \in X) \\
&\Leftrightarrow \quad (c,x) \in (A \times X) \ \wedge \ (c,x) \in (B^c \times X) \\
&\Leftrightarrow \quad (c,x) \in (A \times X) - (B \times X)\,.
\end{aligned}$$

La prueba está completa. □

Observación. De la definición, es claro que el producto cartesiano no es ni conmutativo ni asociativo. Es decir, en general $A \times B \neq B \times A$ (obvio, pues $(a,b) \neq (b,a)$ si $a \neq b$) y

$$A \times (B \times C) \neq (A \times B) \times C$$

Por ejemplo $A \times (B \times C)$ es el conjunto de pares $(a,(b,c))$ mientras que $(A \times B) \times C$ es el conjunto de pares $((a,b),c)$, con $a \in A$, $b \in B$ y $c \in C$. La naturaleza de los elementos de uno y otro producto cartesiano son distintas. En el primer caso los primeros elementos son pares ordenados (de elementos de A y B) mientras que en el segundo caso los primeros elementos son elementos de A. Sin embargo, veremos mas adelante que es posible identificar estas ternas y pensar que estos conjuntos son equivalentes (o iguales) en algún sentido.

Nota. De manera análoga al caso de dos conjuntos se puede definir el producto cartesiano de más de dos conjuntos. En este caso sus elementos en lugar de ser pares ordenados son

n-uplas ordenadas. Si $A_1, A_2, \ldots, A_n$ son n conjuntos dados, el producto cartesiano de ellos es

$$A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \ldots, a_n) : \ a_i \in A_i\}$$

donde la n-upla ordenada $(a_1, a_2, \ldots, a_n)$ se define recursivamente de manera similar a como definimos el par ordenado (a, b).

Nota histórica. La definición formal de par ordenado $(a, b) = \{\{a\}, \{a, b\}\}$ fue introducida por Kazimierz Kuratowski en 1921 y es la aceptada y usada desde entonces. Sin embargo hubo otras propuestas previas. En 1914, Norbert Wiener propuso la definición $(a, b) = \big\{\{\{a\}, \varnothing\}, \{\{b\}\}\big\}$ mientras que Felix Hausdorff propuso esta otra $(a, b) = \{\{a, 1\}, \{b, 2\}\}$, donde 1 y 2 son 'objetos' diferentes de a y b.

2.6. Partes de un conjunto

Dado un conjunto A, consideramos el conjunto formado por todos los subconjuntos de A. Este nuevo conjunto se llama *conjunto de partes de* A, o simplemente *partes de* A, y se lo denota por $\mathcal{P}(A)$. En símbolos,

$$\mathcal{P}(A) = \{B : \ B \subseteq A\}$$

Los elementos de partes de A son de naturaleza distinta a los elementos de A, ya que son subconjuntos de elementos de A. Aún el subconjunto formado por un sólo elemento de A es distinto de ese elemento; $a \neq \{a\}$. Si $a \in A$,

$$\{a\} \subset A \qquad \text{y} \qquad \{a\} \in \mathcal{P}(A)$$

Ejemplos.

(1) Si $A = \varnothing$, entonces $\mathcal{P}(A) = \{\varnothing\}$.

(2) Si $A = \{1\}$, entonces $\mathcal{P}(A) = \{\varnothing, \{1\}\}$.

(3) Si $A = \{1, 2\}$, entonces $\mathcal{P}(A) = \{\varnothing, \{1\}, \{2\}, \{1, 2\}\}$.

(4) Sea $A = \{1, 2, 3\}$, entonces

$$\mathcal{P}(A) = \{\varnothing, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}.$$

Hacemos notar que siempre $A \in \mathcal{P}(A)$ y también que $\varnothing \in \mathcal{P}(A)$ para cualquier conjunto A; en particular se sigue que

$$\bigcup_{X \in \mathcal{P}(A)} X = A \qquad \text{y} \qquad \bigcap_{X \in \mathcal{P}(A)} X = \varnothing$$

La proposición que sigue expresa las propiedades del conjunto de partes respecto a la contención, unión e intersección de dos conjuntos.

Proposición 2.6. *Dados conjuntos arbitrarios A y B, valen las siguientes propiedades:*

(a) $A \subseteq B \quad \Rightarrow \quad \mathcal{P}(A) \subseteq \mathcal{P}(B)$.

(b) $\mathcal{P}(A \cap B) = \mathcal{P}(A) \cap \mathcal{P}(B)$.

(c) $\mathcal{P}(A \cup B) \supseteq \mathcal{P}(A) \cup \mathcal{P}(B)$.

(d) Si $A \cup B \neq A$ *y* $A \cup B \neq B$, *entonces* $\mathcal{P}(A) \cup \mathcal{P}(B) \subsetneq \mathcal{P}(A \cup B)$.

Demostración.
(a) Dado x un subconjunto de A, como A es subconjunto de B, por transitividad x es subconjunto de B. En símbolos:

$$x \in \mathcal{P}(A) \quad \Rightarrow \quad x \subseteq A \subseteq B \quad \Rightarrow \quad x \in \mathcal{P}(B).$$

(b) Tenemos que

$$\begin{aligned} x \in \mathcal{P}(A \cap B) &\Leftrightarrow x \subseteq A \cap B \\ &\Leftrightarrow x \subseteq A \text{ y } x \subseteq B \\ &\Leftrightarrow x \in \mathcal{P}(A) \text{ y } x \in \mathcal{P}(B) \\ &\Leftrightarrow x \in \mathcal{P}(A) \cap \mathcal{P}(B). \end{aligned}$$

(c) Si $x \in \mathcal{P}(A) \cup \mathcal{P}(B)$, entonces $x \in \mathcal{P}(A)$ o $x \in \mathcal{P}(B)$. Luego, $x \subseteq A$ o $x \subseteq B$, lo cual implica que $x \subseteq A \cup B$, de donde se sigue que $x \in \mathcal{P}(A \cup B)$.

(d) Si $A \cup B \neq A$ y $A \cup B \neq B$, entonces por la Proposición 2.2 hay un elemento b de B que no está en A y otro elemento a de A que no está en B. Luego el conjunto $y = \{a, b\}$ es un subconjunto de la unión $A \cup B$, pero no es subconjunto de A ni de B. Es decir $y \in \mathcal{P}(A \cup B)$ pero $y \notin \mathcal{P}(A) \cup \mathcal{P}(B)$, mostrando que la contención es estricta en este caso. □

Observación. La inclusión opuesta en el item (c) no vale en general. Esto está dicho en el item (d), ya que bajo cierta condiciones la inclusión es propia. Ahora, si $A \cup B = A$ o $A \cup B = B$, entonces claramente $\mathcal{P}(A \cup B) = \mathcal{P}(A)$ o $\mathcal{P}(A \cup B) = \mathcal{P}(B)$ respectivamente.

Ejemplo. Si $A = \{-2, -1, 0\}$ y $B = \{0, 1, 2\}$ y tomamos $x = \{-1, 0, 1\}$, entonces $x \in \mathcal{P}(A \cup B)$ pero $x \not\subseteq A$ y $x \not\subseteq B$.

Nota. Dado un conjunto A tenemos un nuevo conjunto $B = \mathcal{P}(A)$. Nada impide que consideremos el conjunto de partes de B, es decir $\mathcal{P}(B) = \mathcal{P}(\mathcal{P}(A))$. De esta forma podemos seguir construyendo conjuntos cada vez más grandes. Por ejemplo,

$$\begin{gathered} \mathcal{P}(\varnothing) = \{\varnothing\}, \\ \mathcal{P}(\mathcal{P}(\varnothing)) = \{\varnothing, \{\varnothing\}\}, \\ \mathcal{P}(\mathcal{P}(\mathcal{P}(\varnothing))) = \{\varnothing, \{\varnothing\}, \{\{\varnothing\}\}, \{\varnothing, \{\varnothing\}\}\}. \end{gathered}$$

Si $A = \{a, b\}$, entonces $\mathcal{P}(A) = \{\varnothing, \{a\}, \{b\}, \{a, b\}\}$ y $\mathcal{P}(\mathcal{P}(A))$ consta de los siguientes conjuntos

$$\begin{gathered}
\varnothing, \\
\{\varnothing\}, \quad \{a\}, \quad \{b\}, \quad \{a, b\} \\
\{\varnothing, \{a\}\}, \quad \{\varnothing, \{b\}\}, \quad \{\varnothing, \{a, b\}\}, \quad \{\{a\}, \{b\}\}, \quad \{\{a\}, \{a, b\}\}, \quad \{\{b\}, \{a, b\}\} \\
\{\varnothing, \{a\}, \{b\}\}, \quad \{\varnothing, \{a\}, \{a, b\}\}, \quad \{\varnothing, \{b\}, \{a, b\}\}, \quad \{\{a\}, \{b\}, \{a, b\}\} \\
\{\varnothing, \{a\}, \{b\}, \{a, b\}\}.
\end{gathered}$$

Particiones de un conjunto

El estudio de las relaciones de equivalencia está íntimamente relacionado al concepto de particiones de un conjunto. Una *partición* de un conjunto A es una familia $\mathcal{P}$ de subconjuntos de A que *cubren* a A y tal que dos cualesquiera son disjuntos. Es decir, $\mathcal{P} \subseteq \mathcal{P}(A)$ con $B \cap B' = \varnothing$ para todo $B, B' \in \mathcal{P}$ y

$$A = \bigcup_{B \in \mathcal{P}} B$$

Así, todo elemento de A pertence a uno y sólo uno de los subconjuntos de la partición $\mathcal{P}$.

Ejemplos. Mostramos aquí algunas particiones, algunas de las cuáles encontraremos nuevamente más adelante.

(1) Para todo conjunto X se tiene la partición trivial en singuletes

$$X = \bigcup_{x \in X} \{x\}$$

(2) Los enteros pares e impares define una partición de los mismos.

$$\mathbb{Z} = (2\mathbb{Z}) \cup (2\mathbb{Z} + 1)$$

(3) Podemos partir a los enteros de acuerdo a su resto en la división por 3. Los posibles restos son 0, 1 y 2 y la partición es

$$\mathbb{Z} = (3\mathbb{Z}) \cup (3\mathbb{Z} + 1) \cup (3\mathbb{Z} + 2)$$

Las partes están formadas respectivamente por los múltiplos de 3, los múltiplos de 3 más 1 y los múltiplos de 3 más 2.

(4) En general, dado r, podemos partir a los enteros según su resto en la división por r. Los posibles restos son $0, 1, 2, \ldots, r-1$ y la partición es

$$\mathbb{Z} = (r\mathbb{Z}) \cup (r\mathbb{Z} + 1) \cup \cdots \cup (r\mathbb{Z} + r - 1)$$

(5) La partición de los naturales en números primos ($\mathbb{P}$), compuestos y el 1. Es decir,

$$\mathbb{N} = \{1\} \cup \mathbb{P} \cup C$$

donde $C = \{n \neq 1 : n = p_1 \cdots p_r \text{ con } p_1, \ldots, p_r \in \mathbb{P}, r \geq 2\}$.

(6) La partición de los reales en intervalos unitarios

$$\mathbb{R} = \bigcup_{n\in\mathbb{Z}} (n, n+1]$$

o más generalmente, para cualquier $\alpha \in \mathbb{R}$,

$$\mathbb{R} = \bigcup_{n\in\mathbb{Z}} (\alpha+n, \alpha+n+1]$$

(7) La partición de los reales en racionales e irracionales $\mathbb{R} = \mathbb{Q} \cup \mathbb{Q}^c$.

(8) La partición de los racionales

$$\mathbb{Q} = \bigcup_{n\in\mathbb{N}} \mathbb{Q}_n$$

donde

$$\mathbb{Q}_n = \{\tfrac{a}{n} : a \in \mathbb{Z} \text{ y } \tfrac{a}{n} \text{ es una fracción reducida}\}.$$

Por ejemplo,

$$\begin{aligned}
\mathbb{Q}_1 &= \{0, \pm1, \pm2, \pm3, \ldots\} = \mathbb{Z} \\
\mathbb{Q}_2 &= \{\pm\tfrac{1}{2}, \pm\tfrac{3}{2}, \pm\tfrac{5}{2}, \pm\tfrac{7}{2}, \ldots\} \\
\mathbb{Q}_3 &= \{\pm\tfrac{1}{3}, \pm\tfrac{2}{3}, \pm\tfrac{4}{3}, \pm\tfrac{5}{3}, \pm\tfrac{7}{3}, \ldots\} \\
\mathbb{Q}_4 &= \{\pm\tfrac{1}{4}, \pm\tfrac{3}{4}, \pm\tfrac{5}{4}, \pm\tfrac{7}{4}, \ldots\} \\
\mathbb{Q}_5 &= \{\pm\tfrac{1}{5}, \pm\tfrac{2}{5}, \pm\tfrac{3}{5}, \pm\tfrac{4}{5}, \pm\tfrac{6}{5}, \ldots\} \\
\mathbb{Q}_6 &= \{\pm\tfrac{1}{6}, \pm\tfrac{5}{6}, \pm\tfrac{7}{6}, \pm\tfrac{11}{6}, \ldots\}
\end{aligned}$$

Vaya ejemplo mas bonito! ◊

2.7. Ejercicios y problemas

Teoría de conjuntos

Cada cuerpo tiene
su armonía y
su desarmonía.
En algunos casos
la suma de armonías
puede ser casi
empalagosa.
En otros
el conjunto
de desarmonías
produce algo mejor
que la belleza.

Mario Benedetti (1920-2009)

Ejercicios

Ejercicio 2.1. Dados $A = \{1, 3, 5, 7, 8, 11, 15\}$ y $B = \{-1, 3, -5, 7, -8, 11, 100, 115\}$, hallar los conjuntos $A \cap B$, $A \cup B$, $B - A$ y $B \triangle A$.

Ejercicio 2.2. Dado $A = \{1, 2, \{3\}\}$, determinar cuáles de las siguientes afirmaciones son verdaderas:

(a) $\{3\} \subseteq A$.

(b) $\{3\} \in A$.

(c) $\big\{\{3\}\big\} \subseteq A$.

(d) $\varnothing \in A$.

(e) $\varnothing \subseteq A$.

(f) $\{x \in \mathbb{N} : x < 3\} \subseteq A$.

Ejercicio 2.3. Sean A, B y C conjuntos. Representar con diagramas de Venn (donde todos los conjutos se intersecan entre sí):

(a) $A \cap (B \cup C)$.

(b) $A \cup (B \cap C)$.

(c) $(A \cup B^c) \cap C$.

(d) $A \triangle (B \cup C)$.

(e) $A \cup (B \triangle C)$.

(f) $(A \cup B) \cap (A \cup C)$.

Ejercicio 2.4. Escribir por extensión los siguientes conjuntos:

(a) $A = \{x \in \mathbb{N} : 5 < x \leq 12\}$.

(b) $B = \{x \in \mathbb{N} : x$ es impar y tiene una cifra$\}$.

(c) $C = \{x \in \mathbb{N} : 3 < x \leq 5, x$ divisible por $3\}$.

(d) $D = \{x = 2n + 1 : n \in \mathbb{N}\}$.

Ejercicio 2.5. Describir implícitamente los siguientes conjuntos:

(a) $A = \{2, 4, 6, 8, 10\}$.

(b) $B = \{11, 21, 31, 41, 51, 61, 71, 81, 91\}$.

(c) $C = \{1\}$.

(d) $D = \varnothing$.

Ejercicio 2.6. Sean $A = \{1, 2, 3\}$ y $B = \{1, 3, 5, 7\}$ hallar $A \times A$, $A \times B$, $B \times B$, $B \times A$ y $(A \cap B) \times (A \cup B)$.

Ejercicio 2.7. Hallar el conjunto $\mathcal{P}(A)$ de partes de A en los casos:

(a) $A = \{1\}$.

(b) $A = \varnothing$.

(c) $A = \{1, \{1, 2\}\}$.

(d) $A = \{1, 3, 5, \varnothing\}$.

Ejercicio 2.8. Realizar las siguientes operaciones entre conjuntos

(a) $\{x \in \mathbb{N} : 10 < x < 25\} \cup \{1, 7, 13, 24, 38\}$.

(b) $\{x \in \mathbb{N} : x \text{ múltiplo de } 3\} - \{x \in \mathbb{N} : x \geq 14\}$.

(c) $\{x \in \mathbb{N} : x \text{ par}\} \cap \{x \in \mathbb{N} : x \leq 11\}$.

(d) $\{x \in \mathbb{N} : 10 < x < 25\} \triangle \{1, 7, 13, 24, 38\}$.

Ejercicio 2.9. Dado $A = \{1, 2, 3\}$, determinar cuáles de las siguientes afirmaciones son verdaderas:

(a) $1 \in A$.

(b) $\{1\} \subseteq A$.

(c) $\{2\} \in A$.

(d) $\{2, 1\} \subseteq A$.

(e) $\{1, 3\} \in A$.

Ejercicio 2.10. Sea $A = \{10, 11, 12, 13, 14, 15\}$ escribir por extensión los siguientes conjuntos:

(a) $\{x : x = \frac{5a+1}{2} \in \mathbb{Z} \text{ donde } a \in A\}$.

(b) $\{x : x = a - b \text{ donde } a, b \in A\}$.

Ejercicio 2.11. Describir por extensión y traducir en símbolos los siguientes conjuntos:

(a) El conjunto de todos los números naturales menores que 300 y divisibles por 3.

(b) El conjunto de todos los números naturales mayores que 5 y menores que 76 que son cuadrados perfectos.

Ejercicio 2.12. Dados los conjuntos $A = \{x \in \mathbb{N} : 5 \leq x < 9\}$ y $B = \{x \in \mathbb{N} : x \text{ es cubo perfecto y } 25 < x \leq 64\}$ hallar $B \times B$, $A \times B$ y $(A \cap B) \times (A \cup B)$.

Ejercicio 2.13. Hallar el conjunto $\mathcal{P}(A)$ de partes de A en los casos:

(a) $A = \{a, b\}$.

(b) $A = \{x \in \mathbb{N} : x \text{ es par y } 30 < x \leq 37\}$.

(c) $A = \{1, a, \{-1\}\}$.

Problemas

Problema 2.14. Mostrar que las siguientes identidades no valen en general exhibiendo contraejemplos:

(a) $(A \times B)^c = A^c \times B^c$,

(b) $(A \times B) \cup (C \times D) = (A \cup C) \times (B \cup D)$.

Problema 2.15. Probar que $(A \times B) \cap (C \times D) = (A \cap C) \times (B \cap D)$.

Problema 2.16. Sean A y B conjuntos. Probar que $\mathcal{P}(A) \subseteq \mathcal{P}(B)$ si y sólo si $A \subseteq B$.

Problema 2.17. En un grupo de 112 alumnos hay 60 alumnos que estudian inglés y 45 que estudian alemán. Se sabe que 8 estudian los tres idiomas, 30 sólo estudian inglés, 20 sólo estudian alemán y 25 sólo estudian francés. ¿Cuántos alumnos estudian exactamente dos idiomas? ¿Cuántos inglés y alemán pero no fránces? ¿Cuántos estudian francés?

Problema 2.18. Determinar la validez de las siguientes afirmaciones. Justificar.

(a) $A \triangle B = (A \triangle C) \cup (B \triangle C)$.

(b) $C \subseteq A \quad \Rightarrow \quad B \cap C \subseteq (A \triangle B)^c$.

(c) $A \triangle B = \varnothing \quad \Leftrightarrow \quad A = B$.

(d) $(A \triangle B) - C = (A - C) \triangle (B - C)$.

Problema 2.19. Sean A, B y C conjuntos. Probar que:

(a) $(A \cup B) \times C = (A \times C) \cup (B \times C)$.

(b) $(A \cap B) \times C = (A \times C) \cap (B \times C)$.

(c) $(A - B) \times C = (A \times C) - (B \times C)$.

(d) $(A \triangle B) \times C = (A \times C) \triangle (B \times C)$.

Capítulo 3

Relaciones y funciones

3.1. Relaciones

Una *relación* en un conjunto A es un subconjunto $\mathcal{R}$ de pares ordenados de elementos de A, es decir

$$\mathcal{R} \subseteq A \times A$$

o, equivalentemente, $\mathcal{R} \in \mathcal{P}(A \times A)$. Los pares ordenados de $\mathcal{R}$ son los pares de elementos de A relacionados, así por ejemplo, además de escribir $(a, b) \in \mathcal{R}$ también se puede escribir

$$a\mathcal{R}b \quad \text{ó} \quad a \sim b$$

y que se lee *a está relacionado con b*. Muchas veces la relación tiene nombre propio, como en el caso de la relación dada por la inclusión de conjuntos; en ese caso en vez de $A\mathcal{R}B$ o $A \sim B$ se escribe $A \subseteq B$. Aquí, en lugar de decir que A y B están relacionados, decimos que A está incluido en B.

Dado un conjunto arbitrario X siempre se tienen las siguientes relaciones en X.

- El conjunto vacío $\varnothing$.
- El conjunto total $X \times X$, llamado la *relación trivial* en X. Aquí, $x \sim x'$ para todo $x, x' \in X$.
- La *diagonal* de X, $\Delta(X) = \{(x, x) : x \in X\}$, también llamada la relación identidad en X. Aquí, $x \sim y$ si y sólo si $x = y$.

Ejemplos.

(1) Sea $A = \{\text{ciudadanos de Córdoba}\}$ y sea $\mathcal{R} = \{(x, y) : x \text{ es padre de } y\}$.

Está claro que no todo par de ciudadanos estará necesariamente relacionado. Por un lado hay muchas personas que no están relacionadas con nadie (sin hijos o con hijos pero no viven en la ciudad). Por otro lado las personas con más de un hijo están relacionadas con todos ellos.

(2) Sea U un conjunto, sea $P = \mathcal{P}(U)$ y sea $\mathcal{R}$ la relación en P dada por la inclusión; es decir: dados $A, B \in P$ entonces $(A, B) \in \mathcal{R}$ si $A \subseteq B$.

En este ejemplo también sucede que habrá pares de conjuntos no relacionados. Además se tiene que el vacío $\varnothing$ está relacionado con todos, que todos están relacionados con U, y que todo conjunto está relacionado con sí mismo.

(3) Sea $A = \mathbb{R}$, el conjunto de números reales y sea $\mathcal{R}$ la relación "es menor que". Es decir $(a, b) \in \mathcal{R}$ si $a < b$.

En este ejemplo todo par de números distintos, está relacionado en un sentido o en otro. Sin embargo, ningún número está relacionado con sí mismo.

(4) Sea $A = \mathbb{R}$, el conjunto de números reales y sea $\mathcal{R}$ la relación "es menor o igual que". Es decir $(a, b) \in \mathcal{R}$ si $a \leq b$.

Este es un primer ejemplo en el que todo par de números, distintos o no, está relacionado en uno u otro sentido.

(5) Sea A el conjunto de pares ordenados de enteros, $A = \mathbb{Z} \times \mathbb{Z}$, y sea $\sim$ la relación en A dada por: (a, b) está relacionado con (c, d) si los 'productos cruzados' coinciden, es decir

$$(a, b) \sim (c, d) \quad \Leftrightarrow \quad ad = bc$$

La misma relación de pares de enteros, pero en $\mathbb{Z} \times \mathbb{Z}^*$, donde $\mathbb{Z} = \mathbb{Z} \setminus \{0\}$, es la que define a los números racionales, pues $\frac{a}{b} = \frac{c}{d}$ si y sólo si $ad = bc$. ◊

3.1.1. Propiedades de una relación

Las relaciones en un conjunto son una estructura adicional que puede enriquecer a otras estructuras que haya en el conjunto, como por ejemplo operaciones. Las relaciones serán una herramienta útil de acuerdo a sus propiedades y a su compatibilidad con las otras estructuras presentes. Entre las propiedades usuales de relaciones que aparecen naturalmente están las siguientes.

Una relación $\sim$ en un conjunto A puede ser:

- Reflexiva. Si para todo $a \in A$, $a \sim a$.
- Simétrica. Si $a \sim b$, entonces $b \sim a$.
- Antisimétrica. Si $a \sim b$ y $b \sim a$, entonces $a = b$.
- Transitiva. Si $a \sim b$ y $b \sim c$, entonces $a \sim c$.
- Total. Si para todo a y b, se tiene que $a \sim b$ ó $b \sim a$.

Además puede satisfacer:

- Dicotomía. Si para todo a y b, se tiene que $a \sim b$ ó $b \sim a$ y una sola de ellas.
- Tricotomía. Si para todo a y b, se tiene que $a \sim b$, $b \sim a$ ó $a = b$ y una sola de ellas.

Veamos cuáles de estas propiedades tienen las relaciones de los ejemplos anteriores.

Relación	Refl.	Sim.	Antisim.	Trans.	Total	Dicot.	Tricot.
x es padre de y	no	no	si *	no	no	no	no
$A \subseteq B$	si	no	si	si	no	no	no
$a < b$	no	no	si *	si	no	no	si
$a \leq b$	si	no	si	si	si	si	no
$ad = bc$	si	si	no	si	no	no	no

* En estos casos la relación es antisimétrica pues si $a \sim b$, entonces nunca $b \sim a$, luego la hipótesis de antisimetría nunca se satisface y por lo tanto la implicación es verdadera.

Observación. Algunas de las propiedades listadas son excluyentes, como la dicotomía y la tricotomía. Notar que si una relación es a la vez simétrica y antisimétrica, entonces los únicos relacionados son los pares de la forma (a, a). Además ciertas propiedades se siguen de algunas otras. Por ejemplo, una relación total y simétrica, es transitiva.

Dos tipos de relaciones muy importantes y frecuentes en matemática son:

- Relación de orden. Una relación es de orden si es reflexiva, antisimétrica y transitiva.
- Relación de equivalencia. Una relación es de equivalencia si es reflexiva, simétrica y transitiva.

3.1.2. Relaciones de orden

Entre los ejemplos que vimos más arriba hay dos relaciones que son de orden (marcadas en azul).

Relación	Refl.	Sim.	Antisim.	Trans.	Total	Dicot.	Tricot.
x es padre de y	no	no	si	no	no	no	no
$A \subseteq B$	si	no	si	si	no	no	no
$a < b$	no	no	si	si	no	no	si
$a \leq b$	si	no	si	si	si	si	no
$ad = bc$	si	si	no	si	no	no	no

La dada por la inclusión de conjuntos $\subseteq$ no es total, mientras que la relación dada por el menor o igual $\leq$ para números reales es total.

Destacamos que la relación dada por el menor $<$ para números reales no es una relación de orden, pues no es reflexiva.

Un ejemplo interesante, que todo el mundo conoce, es el orden alfabético con el cuál se ordenan las palabras en el diccionario. A partir de cómo están ordenadas las letras del alfabeto

$$\mathrm{a} < \mathrm{b} < \mathrm{c} < \cdots < \mathrm{x} < \mathrm{y} < \mathrm{z}$$

se ordenan todas las palabras que se pudieran formar con estas letras. Así tenemos que

$$\text{aereo} < \text{bala} < \text{barral} < \text{mero} < \text{nariz}$$

La regla para ordenarlas es muy simple. Dadas dos palabras se comparan la primera letra de una con la primera letra de la otra, resultando mayor la palabra que tiene la mayor primera letra. Si tienen la misma primera letra se continua con la segunda letra de cada una, y se decide según ésta. Ahora si éstas son iguales se consideran las terceras letras y así sucesivamente hasta la primera letra en la que difieren. En el orden alfabético está implícito el uso del espacio o "letra vacía" considerada menor que la "a". Así dadas las palabras "fruta" y "frutales" resulta

$$\text{fruta} < \text{frutales}$$

pues ambas tienen las mismas primeras 5 letras y la sexta de "fruta" es la letra vacía que es menor que la sexta de "frutales", la "l".

La idea del orden alfabético se puede replicar para ordenar el producto cartesiano. El orden que resulta se llama *lexicográfico*.

El orden lexicográfico

Dado un conjunto totalmente ordenado $\mathcal{A}$, el "alfabeto", el orden lexicográfico para el producto cartesiano

$$\mathcal{A}^n = \underbrace{\mathcal{A} \times \cdots \times \mathcal{A}}_{n}$$

está definido de la siguiente manera. Dados $(a_1, \ldots, a_n) \neq (b_1, \ldots, b_n)$ sea i el primer índice tal que $a_i \neq b_i$ (siempre existe pues las n-uplas son distintas). Entonces

- Si $a_i < b_i$, entonces $(a_1, \ldots, a_n) < (b_1, \ldots, b_n)$.
- Si $a_i > b_i$, entonces $(a_1, \ldots, a_n) > (b_1, \ldots, b_n)$.

Al producto cartesiano $\mathcal{A}^n$ lo podemos ver como el conjunto de todas las palabras escritas con letras del alfabeto $\mathcal{A}$ de exactamente n letras (las n-palabras de $\mathcal{A}$).

Podemos considerar palabras de longitudes arbitrarias haciendo

$$\mathcal{A}^\infty = \bigcup_{n \in \mathbb{N}} \mathcal{A}^n$$

donde el orden lexicografico en $\mathcal{A}^\infty$ es, como hicimos antes para las palabras ordinarias, usando el espacio vacío para comparar palabras de distintas longitudes.

Ejemplo. Sea $\mathcal{A} = \{\beta, k, F\}$ ordenado totalmente por

$$\beta < k < F$$

El producto cartesiano $\mathcal{A} \times \mathcal{A}$ tiene 9 elementos, totalmente ordenados lexicográficamente como sigue:

$$\beta\beta < \beta k < \beta F < k\beta < kk < kF < F\beta < Fk < FF$$

De manera análoga quedan totalmente ordenados todos los elementos del producto cartesiano de $\mathcal{A}$ con $\mathcal{A}$ varias veces. Por ejemplo, en el producto cartesiano $\mathcal{A} \times \mathcal{A} \times \mathcal{A} \times \mathcal{A} \times \mathcal{A}$, que tiene $3^5 = 243$ palabras, las primeras tres son:

$$\beta\beta\beta\beta\beta < \beta\beta\beta\beta k < \beta\beta\beta\beta F$$

las tres que siguen son

$$\beta\beta\beta k\beta < \beta\beta\beta kk < \beta\beta\beta kF$$

y las últimas tres son

$$FFFF\beta < FFFFk < FFFFF$$

Además, es claro que

$$\beta < \beta\beta < \beta\beta\beta < \beta\beta\beta\beta < \beta\beta\beta\beta\beta < k$$

En general, en $\mathcal{A}^\infty$, vale

$$\underbrace{\beta\beta\cdots\beta}_{n} < k$$

para cualquier n. ◊

Ejemplo. Si el alfabeto que consideramos son los dígitos, $\mathcal{A} = \{0,1,2,3,4,5,6,7,8,9\}$, el conjunto de palabras de longitud arbitraria coincide con el conjunto de los números naturales

$$\mathcal{A}^\infty = \bigcup_{i=1}^{\infty} \mathcal{A}_i = \mathbb{N}$$

El orden lexicográfico en $\mathbb{N}$ no es el mismo que el orden natural en $\mathbb{N}$. En efecto

$$123 < 124 < 123456$$

mientras que

$$123 <_\ell 123456 <_\ell 124$$

donde $<_\ell$ representa el orden lexicográfico en $\mathbb{N}$. ◊

3.1.3. Relaciones de equivalencia

Entre los ejemplos que vimos más arriba hay una relación de equivalencia.

Relación	Refl.	Sim.	Antisim.	Trans.	Total	Dicot.	Tricot.
x es padre de y	no	no	si	no	no	no	no
$A \subseteq B$	si	no	si	si	no	no	no
$a < b$	no	no	si	si	no	no	si
$a \leq b$	si	no	si	si	si	si	no
$ad = bc$	si	si	no	si	no	no	no

Otras relaciones de equivalencia son, por ejemplo, la paridad de los números enteros y la semejanza de triángulos en la geometría del plano. La relación de paridad clasifica a los enteros en pares e impares. La relación de semejanza clasifica a los triángulos por su "forma". Un teorema de geometría de la escuela dice que dos triángulos que tienen los mismos ángulos son semejantes.

Esto es un hecho general de las relaciones de equivalencia, ya que toda relación de equivalencia en un conjunto A determina una partición del mismo (ver §2.5), donde las partes están formadas por los elementos relacionados (o equivalentes), y recíprocamente, una partición de A define una relación que es de equivalencia.

Veamos con más detalle que tener una relación de equivalencia en A es lo mismo que tener una partición de A.

• Comenzamos mostrando que una relación de equivalencia induce una partición. Supongamos que $\sim$ es una relación de equivalencia en un conjunto A y para cada elemento $a \in A$, consideremos el conjunto de elementos relacionados con a,

$$P(a) = \{b \in A : a \sim b\}$$

El conjunto $P(a)$ se llama *clase de equivalencia* del elemento a (a veces también es denotado por $[a]$, $\bar{a}$ ó $\tilde{a}$). Como la relación es reflexiva, es inmediato que $a \in P(a)$ y como la relación es simétrica se sigue que si $a \in P(b)$, entonces $b \in P(a)$. Una tercera propiedad, es que dos de estos conjuntos $P(a)$ y $P(b)$ son iguales o disjuntos, es decir

$$P(a) = P(b) \qquad \text{ó} \qquad P(a) \cap P(b) = \varnothing$$

En efecto, supongamos que $P(a) \cap P(b) \neq \varnothing$ y sea $c \in P(a) \cap P(b)$. Ahora si $x \in P(a)$, tenemos $x \sim a$, $a \sim c$ y $c \sim b$, de donde $x \sim b$. Luego $x \in P(b)$ y resulta $P(a) \subseteq P(b)$. Análogamente se ve que $P(b) \subseteq P(a)$.

De esto se sigue el siguiente hecho fundamental:

$$a \sim b \quad \Leftrightarrow \quad P(a) = P(b)$$

Es decir, dos elementos están relacionados si y sólo si sus clases de equivalecia son iguales.

Al conjunto de clases de equivalencia de $\sim$ en A se lo denota por $A/_\sim$, es decir

$$A/_\sim = \{P(a) : a \in A\}$$

Ahora, de cada clase de equivalencia elegimos un elemento y formamos un *conjunto de representantes* de la relación dada, $\{a_i : i \in I\}$. Resulta que

$$A = \bigcup_{i \in I} P(a_i)$$

donde los conjuntos $P(a_i)$, las partes, son todos disjuntos entre sí. Esto quiere decir que $P(a_i) \cap P(a_j) = \varnothing$ para todo $i \neq j$, y se suele decir que los conjuntos $P(a_i)$ son disjuntos dos a dos.

• Mostramos ahora cómo una partición de A define una relación de equivalencia. Dada una partición de A

$$A = \bigcup_{i \in I} A_i$$

definimos la relación $\sim$ en A por:

$$a \sim b \qquad \Leftrightarrow \qquad a, b \in A_i \quad \text{para algún } i$$

Es inmediato chequear que esta relación es reflexiva, simétrica y transitiva y que además $A_i = P(i)$.

Para resumir lo visto, hemos probado lo siguiente.

Proposición 3.1. *Toda relación de equivalencia $\sim$ en un conjunto X determina una partición de X en clases de equivalencia. Recíprocamente, toda partición de X da lugar a una relación de equivalencia $\sim$ en X. Las construcciones son mutuamente recíprocas.*

Observación. Si comenzamos con una $\sim$ de equivalencia, construimos la partición asociada y definimos la relación correspondiente, obtenemos la misma $\sim$ con la que comenzamos. Recíprocamente, si comenzamos con una partición, definimos la $\sim$ asociada y definimos la partición correspondiente, obtenemos la misma partición con la que comenzamos.

3.2. Funciones

3.2.1. Función, dominio e imagen

Dados dos conjuntos A y B, una *función* de A en B es una manera de asignarle, mediante alguna regla precisa, a cada elemento de A un, y sólo un, elemento de B. Si esta función se llama f, se escribe

$$f : A \to B$$

El conjunto A o conjunto de partida es el *dominio* de la función f y B o conjunto de llegada es el *codominio* de f. La flecha representa la regla que define a la función.

Dado $a \in A$, $b = f(a)$ es la *imagen* de a por f o el *valor* de f en a. Para destacar esto, es usual escribir

$$a \mapsto b \qquad \text{ó} \qquad a \mapsto f(a)$$

El subconjunto de B formado por todos los elementos que son imágenes de algún elemento de A, es la *imagen* de f y se lo denota por $Im(f)$ o por $f(A)$. Es decir

$$Im(f) = \{b \in B \,:\, \exists\, a \in A \text{ con } b = f(a)\} = \{f(a) : a \in A\}$$

La imagen de una función está definida así de manera implícita naturalmente.

En algunos casos se usa como sinónimo de función el término *transformación* y a la imagen de un elemento a por una tranformación f se lo llama *transformado* de a por f.[*] Este nombre induce a imaginar una función como un proceso que transforma los elementos de A (materia prima) en elementos de B (productos).

No hay una única manera de definir funciones. Cuando el dominio es finito, es posible definir una función exhaustivamente. En algunos casos se definen funciones de manera implícita y en muchos casos una función está definida por una fórmula que permite "calcular" la imagen de cada elemento de su dominio.

[*] r: decir algo de mapa??

Ejemplos.

(1) Si $A = \{\alpha, t, X\}$ y $B = \{1, 2, 3, 4, 5\}$ podemos definir funciones de A en B indicando que elemento le corresponde a cada uno de los 3 elementos de A. Por ejemplo, las siguientes son todas funciones ditintas.

- $f(\alpha) = 3$, $f(t) = 1$, $f(X) = 3$.
- $g(\alpha) = 5$, $g(t) = 4$, $g(X) = 3$.
- $h(\alpha) = 2$, $h(t) = 2$, $h(X) = 2$.

(2) Si $A = \{1, 2, 3, \ldots, 10\}$, entonces para definir una función de $f : A \to B$, para cualquier conjunto B (no necesariamente finito), basta con indicar explícitamente la imagen de cada uno de los 10 elementos de A. Es decir, definir una función de A en B es lo mismo que elegir de manera ordenada 10 elementos de B. O sea,

$$f(1) = b_1, \quad f(2) = b_2, \quad \ldots, \quad f(10) = b_{10}, \qquad b_1, \ldots, b_{10} \in B.$$

(3) Sea $p : \mathbb{N} \to \mathbb{N}$ la función que a cada $n \in \mathbb{N}$ le asigna el n-ésimo número primo. Sabemos que $p(1) = 2$, $p(2) = 3$, $p(3) = 5$. De hecho se conocen muchos valores de p, aunque como no se conocen todos los números primos no podemos decir cuánto vale $p(n)$ para todo n. Es decir, no hay una fórmula para p, aunque si una regla clara de formación. Es común denotar por p_n a $p(n)$.

(4) Sea $a : \mathbb{N} \to \mathbb{N}$, definida por $a(n) = 2(n + 1)$. Dado que a está definida por un fórmula y que ésta es fácil de evaluar, es posible decir cuál es la imagen de cualquier n dado; por ejmplo la imagen de 102 por a es 206.

(5) Si $g : \mathbb{R} \to \mathbb{R}$ está definida por $g(x) = \cos(x + 1)/(1 + x^2)$, entonces podemos calcular la imagen de x por g evaluando la fórmula dada. Esto no significa que cualquiera sea x tendremos una expresión de $g(x)$ como 1, 5/4 o $\sqrt{2}$. Por ejemplo, si $x = 1$, $g(x) = \frac{\cos(2)}{2}$ y si $x = \sqrt{3}$, entonces $g(x) = \frac{\cos(\sqrt{3})}{4}$; con estos números podemos calcular tal como con cualquier otro número real. ◊

Si $f : A \to B$ es una función dada, y $C \subset A$, entonces $f(C) = \{f(c) : c \in C\}$ es la imagen por f del subconjunto C. Cuando $C = A$, $f(C) = f(A)$ es la imagen de f.

Si $D \subset B$, la *preimagen* de D por f es el conjunto

$$f^{-1}(D) = \{a \in A : f(a) \in D\}$$

Ejemplos. Consideremos algunas de las funciones de los ejemplos anteriores y determinemos las imagenes de algunos subconjutos de sus dominios y las preimagenes de algunos subconjuntos de sus codominios.

(1) Consideremos la función f del item 1. En este caso la imagen de f es

$$Im(f) = \{1, 3\}$$

mientras que la imagen del subconjunto del dominio $C = \{t\}$ es $f(C) = \{1\}$. La preimagen del conjunto $D = \{2, 3, 4\}$ es $f^{-1}(D) = \{\alpha, X\}$, mientras que la preimagen de $\{4, 5\}$ es vacía.

(2) Si p es la función del item 3, entonces

$$p^{-1}(\{10, 11, 12, 13, 14, 15, 16, 17\}) = \{5, 6, 7\}$$

ya que 11, 13 y 17 son primos y son el quinto, el sexto y el séptimo primo respectivamente. Ahora la preimagen del conjunto de todos los pares mayores que 3, es vacía, ya que no hay ningún primo par mayor que 3.

(3) Por último estudiemos la función a del item 4, dada por la fórmula $a(n) = 2(n + 1)$. La imagen de los primeros 5 naturales es $\{4, 6, 8, 10, 12\}$. Para calcular la preimagen del conjunto $D = \{31, 32, 33, 34, 35, 36\}$, debemos determinar los n tales que $a(n) = 31, 32, 33, 34, 35, 36$. Primero observamos que $a(n)$ es siempre par, por lo tanto sólo debemos buscar n tal que $a(n) = 32, 34, 36$. Como $a(n) = 2(n + 1)$, si $a(n) = 32$ entonces no es difícil deducir que $n = 15$. De manera análoga resulta que si $a(n) = 34$ entonces $n = 16$ y si $a(n) = 36$ entonces $n = 17$. Así resulta que

$$a^{-1}(D) = \{15, 16, 17\}$$

Notemos que de nuestros cálculos se sigue que hay un único n tal que $a(n) = 32$ ($n = 15$) y lo mismo sucede en los otros casos. ◊

Las siguientes son algunas funciones que aparecen frecuentemente en matemática.

- FUNCIÓN CONSTANTE: dados A y B, para cada $b \in B$ existe una *función constante* f_b que asigna a todos los elementos de A el mismo elemento b. Ésta está definida por

$$f_b(a) = b$$

para todo $a \in A$.

- FUNCIÓN IDENTIDAD: para todo conjunto A, la función $f : A \to A$ definida por

$$f(a) = a$$

para todo $a \in A$ se llama la *identidad* de A. Algunas nombres usuales para esta función son I_A, 1_A o id_A.

- FUNCIÓN CARACTERÍSTICA: dado un conjunto A, para cada subconjunto B, la *función característica* de B, es la función $\chi_B : A \to \{0, 1\}$ definida por

$$\chi_B(a) = \begin{cases} 1, & \text{si } a \in B \\ 0, & \text{si } a \notin B \end{cases}$$

Dada una función $f : A \to B$, a un elemento genérico $a \in A$ se lo llama *variable*; en la evaluación de $f(a)$, a puede puede tomar cualquier valor en A, es decir puede variar dentro de A. Esto es particularmente consistente con la intuición cuando la función f está definida por una fórmula.

También es posible definir funciones de dos o más variables. En este caso el dominio es un producto cartesiano. Por ejemplo si $f : A \times B \to C$, f es una función con dos

variables; en la evaluación de $f(a,b)$, a puede variar dentro de A y b puede variar dentro de B. El dominio de f es el producto cartesiano $A \times B$, mientras que el dominio de la primra variable es A y el de la segunda es B. Ejemplos de funciones de dos variables son la función distancia y las operaciones en $\mathbb{R}$.

- La *función distancia* d en $\mathbb{R} \times \mathbb{R}$ se define como

$$d(x,y) = \sqrt{x^2 + y^2}.$$

  Esta función satisface $d(x,y) = d(y,x)$, $d(x,x) = 0$, $d(x,y) = 0$ si y sólo si $x = y = 0$, y la llamada desigualdad triangular $d(x,z) \leq d(x,y) + d(y,z)$.

- Las funciones suma $+ : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ y producto $\cdot : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$, que a un par de números a, b le asocian respectivamente los valores $+(a,b) = a + b$ y $\cdot(a,b) = a \cdot b$.

Nota. Más generalmente, se pueden definir funciones de varias variables. Una función de n-variables con valores en B es

$$f : A_1 \times A_2 \times \cdots \times A_n \to B$$

donde $f(a_1, a_2, \ldots, a_n) \in B$ para $a_i \in A_i$, $1 \leq i \leq n$.

Sucesiones

Una clase muy común de funciones que tiene especial interés en matemática son las sucesiones. Un *sucesión* es una función con dominio $\mathbb{N}$. Así una sucesión real es una función $\mathbb{N} \to \mathbb{R}$ y una sucesión compleja en una función $\mathbb{N} \to \mathbb{C}$. Si $f : \mathbb{N} \to A$ es una sucesión con valores en A, es usual denotar por f_n a la imagen por f de n, en lugar de $f(n)$. Es decir,

$$f : \mathbb{N} \to A, \qquad n \mapsto f_n$$

Otra forma frecuente de denotar a la sucesión f, es escribir $\{f_n\}_{n \in \mathbb{N}}$.

Ejemplos.

(1) Las sucesiones definidas por $a_n = 2n$ y $b_n = 2n-1$, para todo $n \in \mathbb{N}$, son las sucesiones de los números pares e impares, respectivamente.

(2) La sucesión dada por $c_n = (-1)^n$, $n \in \mathbb{N}$, toma solamente los valores 1 y -1 alternadamente, comenzando con $c_1 = -1$

(3) Sea E la sucesión definida por $E_n = \left[\frac{n+2}{2}\right]$, donde $[x]$ es la parte entera de x [**]. No es difícil calcular los primeros valores de E.

$$E_1 = 1, \quad E_2 = 2, \quad E_3 = 2, \quad E_4 = 3, \quad E_5 = 3, \quad E_6 = 4, \quad E_7 = 4, \ldots$$

Podemos conjeturar que la sucesión E toma cada valor natural 2 veces, salvo el 1.

[**] La parte entera $[x]$ de un número real x es el mayor de los enteros menores o iguales que x.

3.2.2. Restricción y extensión de funciones

Si $f : A \to B$ y $C \subseteq A$, a veces es conveniente considerar la *restrición* de f a C,

$$f|_C : C \to B$$

definida por

$$c \mapsto f(c), \quad \text{para todo } c \in C$$

Ésta es una nueva función diferente de f, con un nuevo dominio más chico. En C, f y su restricción a C, $f|_C$, coinciden; así podemos decir que en C ambas son "la misma" función.

Si $f : A \to B$ es una función dada, a veces es útil considerar una función con un dominio más grande que A y que coincida con f en A. Así si $g : \overline{A} \to B$, donde $A \subseteq \overline{A}$ y $g(a) = f(a)$ para todo $a \in A$, se dice que g es una *extensión* de f.

Notar que si g es una extensión de f, entonces f es la restricción de g a su dominio.

Ejemplo. Sea $f : \mathbb{N} \to \mathbb{N}$ definida por

$$f(n) = (-1)^n$$

Está claro que f toma sólo los valores 1 y -1 (según sea la paridad de n).

- La restricción de f al subconjunto de los naturales pares, es la función constante igual a 1.
- Una extensión de f a los números enteros es la función $g : \mathbb{Z} \to \mathbb{Z}$ definida por $g(m) = (-1)^m$. Otra extension de f a los números enteros es la función $h : \mathbb{Z} \to \mathbb{Z}$ definida por $h(m) = (-1)^m$ si m es natural y $h(m) = 0$ si m es negativo o igual a 0.

Observar que la restricción de una función $f : A \to B$ a un subconjunto $A' \subset A$ es única por definición. Sin embargo, puede haber muchas extensiones $g : \bar{A} \to B$, para un mismo $A \subset \bar{A}$, como lo muestra el ejemplo anterior

3.2.3. Funciones suryectivas, inyectivas y biyectivas

Dos propiedades de cualquier función que resultan relevantes tienen que ver con los valores del codominio que efectivamente alcanzan y cómo lo hacen.

Más precisamente, dada una función $f : A \to B$, ¿es todo elemento b de B alcanzado por la función? Para aquellos b que son alcanzados, ¿son alcanzados por un sólo elemento de A o por varios?

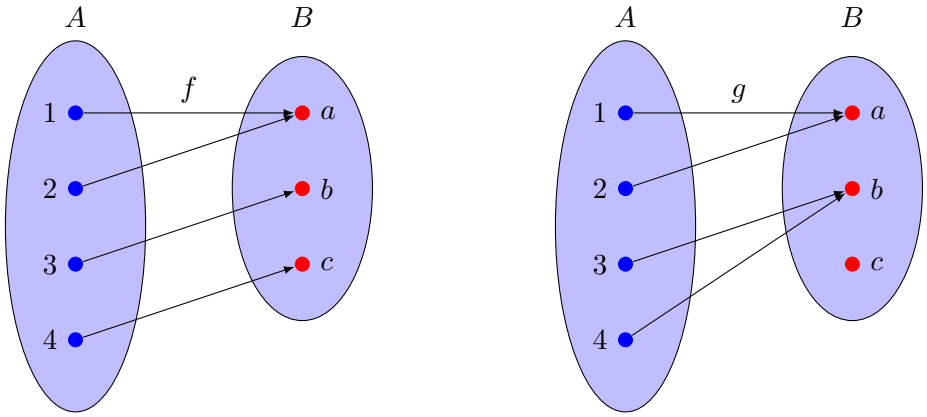
Las respuestas a estas preguntas determinan si f es suryectiva o si es inyectiva.

Funciones suryectivas

Una función $f : A \to B$ es *suryectiva* o *sobreyectiva* si su imagen es B, $Im(f) = B$. Es decir, si todo $b \in B$ es alcanzado por f. Esto es, si para todo $b \in B$ existe al menos un $a \in A$ que es por f asignado a b. En símbolos,

$$\forall b \in B,\ \exists a \in A \ :\ f(a) = b$$

Los siguientes gráficos ilustran dos funciones $f : A \to B$ y $g : A \to B$, con $A = \{1, 2, 3, 4\}$ y $B = \{a, b, c\}$.



Vemos que f es suryectiva, ya que toma todos los valores de B, mientras que g no lo es, ya que ningún elemento de A "va a parar por f" a $c \in B$.

Ejemplos.

(1) La función valor absoluto $|\cdot| : \mathbb{R} \to \mathbb{R}$, no es suryectiva, ya que el valor absoluto es siempre mayor o igual que cero. Así no existe ningún $x \in \mathbb{R}$ tal que $|x| = -1$. Luego $-1 \notin Im(|\cdot|)$ y $Im(|\cdot|) \subsetneq \mathbb{R}$.

(2) La función valor absoluto $|\cdot| : \mathbb{R} \to \mathbb{R}_{\geq 0}$, si es suryectiva, ya que todo número real mayor o igual que cero es alcanzado por esta función. Más precisamente si $y \geq 0$, entonces $|y| = y$. Es decir, la $Im(|\cdot|) = \mathbb{R}_{\geq 0}$.

Funciones inyectivas

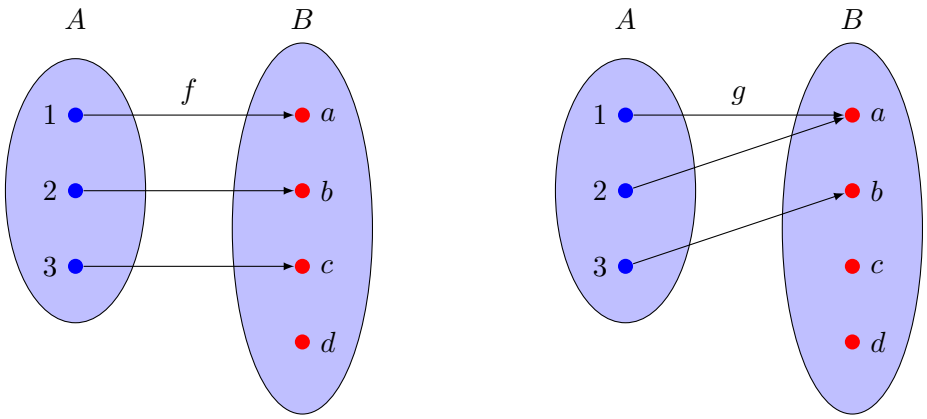
Una función $f : A \to B$ es *inyectiva* si elementos distintos de A son asignados a elementos distintos de B. Es decir,

$$a_1 \neq a_2 \qquad \Rightarrow \qquad f(a_1) \neq f(a_2)$$

Equivalentemente,

$$f(a_1) = f(a_2) \qquad \Rightarrow \qquad a_1 = a_2$$

Los siguientes gráficos ilustran una función inyectiva y otra no.



Si $f : A \to B$ es inyectiva, la preimagen de cualquier *singulete*, un subconjunto de B de un elemento, es vacía o tiene un único elemento. En efecto, $f^{-1}(\{b\}) = \varnothing$ si $b \notin Im(f)$ y $f^{-1}(\{b\}) = \{a\}$ si $b \in Im(f)$ donde a es el único elemento de a que es asignado a b.

Ejemplos.

(1) La función constante nunca es inyectiva, salvo que el dominio tenga un único elemento.

(2) La función identidad de A en A es inyectiva y sobreyectiva.

(3) La función valor absoluto $|\cdot| : \mathbb{R} \to \mathbb{R}_{\geq 0}$, no es inyectiva, ya que un número dado y su opuesto tienen el mismo valor absoluto. Es decir existen dos números distintos con el mismo valor absoluto.

(4) La función $f : \mathbb{R}_{\geq 0} \to \mathbb{R}$, $f(x) = x^2$, si es inyectiva. Ya que si dos números positivos elevados al cuadrado coinciden, entonces son iguales. Sólo hay dos números (no nulos) que elevados al cuadrado son iguales, uno es positivo y el otro negativo.

Antes de continuar nos detenemos un poquito a pensar las siguientes preguntas.

Preguntas.

(1) ¿Es la sucesión definida por $E_n = \left[\frac{n+2}{2}\right]$, donde $[\,\cdot\,]$ es la función parte entera, suryectiva o inyectiva?

(2) ¿Hay alguna función suryectiva de $A = \{1, 2\}$ en $B = \{a, b, c\}$?

(3) ¿Hay alguna función inyectiva de $A = \{1, 2\}$ en $B = \{a, b, c\}$?

(4) ¿Hay alguna función suryectiva de $\mathbb{N}$ en $\mathbb{Z}$?

Respuestas.

(1) Sobre la sucesión E_n, que fue introducida más arriba, hicimos una conjetura. Dijimos que E toma cada valor natural 2 veces, salvo el 1. Si efectivamente es así E no es inyectiva y es suryectiva sobre los números naturales.

Aún sin responer sobre la conjetura, podemos responder definitivamente a la pregunta que nos interesa ahora. Para mostrar que E no es inyectiva basta observar que $Ea_2 = 2 = E_3$, es decir que 2 y 3 son asignados a un mismo elemento el codominio. Para mostrar que E es suryectiva debemos encontrar, para cada natural m dado, un n tal que $a_n = m$. Según nuestra conjetura hay dos de tales n's si $m \neq 1$. Observamos que si n es par, entonces $\frac{n+2}{2}$ es natural, y su parte entera es $\frac{n+2}{2}$. Es decir, si n es par $E_n = \frac{n+2}{2}$. Ahora si queremos un n tal que $E_n = m$, y este n es par, tenemos que $\frac{n+2}{2} = m$ de donde deducimos que $n = 2m - 2$. Hemos encontrado un n, lo hemos encontrado par, tal que $E_n = m$ como queríamos.

(2) Dado que el dominio A es pequeño, podemos pensar en las funciones de A más o menos exhaustivamene. Una función de A en B queda totalmente determinada por sus valores en 1 y en 2. Ahora cualquiera sea el elemento de B que elijamos para 1 y cualqueira sea el elemento que elijamos para 2, siempre quedará un elemento de B sin elegir. Es decir, la imagen de f tendrá a lo sumo dos elementos y nunca será igual a B.

(3) Retomando el análisis de la pregunta anterior, es claro que para definir una función de A en B podemos elegir como imagenes de 1 y 2 dos elementos distintos de B. Una tal elección produce una función inyectiva. De hecho ha varias funcones inyectivas distintas. Por ejemplo

$$f: \ 1 \mapsto a \quad \text{y} \quad 2 \mapsto b$$
$$g: \ 1 \mapsto b \quad \text{y} \quad 2 \mapsto a$$
$$h: \ 1 \mapsto b \quad \text{y} \quad 2 \mapsto c$$

son todas inyectivas.

(4) En este caso tanto el dominio $\mathbb{N}$ como el codominio $\mathbb{Z}$ son conjuntos mucho más grandes que los considerados en las últimas dos preguntas. Sabemos que $\mathbb{N}$ es subconjunto propio de $\mathbb{Z}$, $\mathbb{N} \subseteq \mathbb{Z}$. Esto puede inducirnos a pensar que noes posible contruir una función suryctiva de $\mathbb{N}$ en $\mathbb{Z}$. Por otro lado, pensemos en el conjunto de naturales pares $2\mathbb{N} = \{2n : n \in \mathbb{N}\}$. Este es un subconjunto propio de $\mathbb{N}$. Ahora, en ese caso la función f que divide por 2, $f : 2\mathbb{N} \to \mathbb{N}$, $f(m) = \frac{m}{2}$, si es suryectiva. Esto muestra que el hecho de ser el dominio un subconjunto propio del codominio no es impedimento para la existencia de funciones suryectivas. Dado esto podemos intentar definir una función de los naturales en los enteros enviando los pres a los enteros positivos, por ejemplo, y a los impares a, los enteros negativos. no debemos olvidarnos del 0. Definamos $f : \mathbb{N} \to \mathbb{Z}$ por

$$f(n) = \begin{cases} \frac{n}{2} & \text{si } n \text{ es par,} \\ -\frac{(n-1)}{2} & \text{si } n \text{ es impar.} \end{cases} \tag{3.1}$$

Primero observamos que f está bien definida pues si n es par $\frac{n}{2}$ es natural y si n es impar $n - 1$ es par y luego $\frac{n-1}{2}$ es natural. Veamos que es suryectiva.

- Si m es un entero positivo, tomemos el par $n = 2m$. Ahora $f(n) = \frac{2m}{2} = m$.
- El 0 es también alcanzado, ya que $f(1) = \frac{1-1}{2} = 0$.

- Si m es un entero negativo ($-m$ es positivo), tomemos $n = -2m+1$ que es impar y positivo. Luego $f(n) = -\frac{n-1}{2} = -\frac{-2m+1-1}{2} = -(-m) = m$.

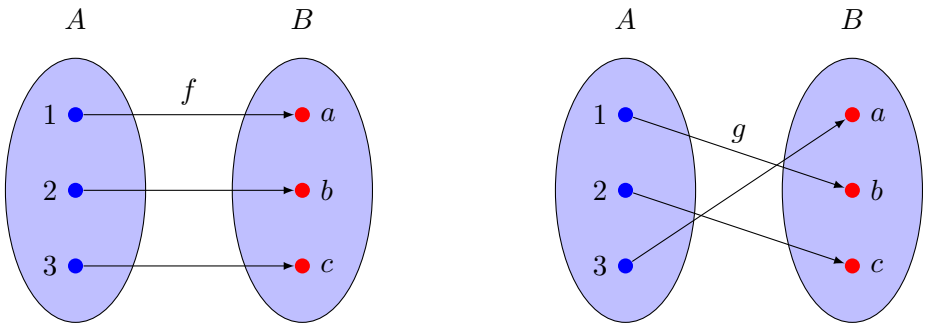
De este modo, para cualquier $m \in \mathbb{Z}$ existe un $n \in \mathbb{Z}$ tal que $f(n) = m$ y f resulta sobreyectiva.

Funciones biyectivas

Una función $f : A \to B$ es *biyectiva* si es inyectiva y suryectiva a la vez. Es decir, cada elemento de b es imagen de uno y sólo un elemento de A. En símbolos,

$$\forall b \in B,\ \exists! a \in A\ :\ f(a) = b$$

Ilustramos con el gráfico de dos funciones biyectivas f y g de $A = \{1, 2, 3\}$ en $B = \{a, b, c\}$



Una función biyectiva de A a B establece una correspondencia biunívoca entre A y B. Esto es como un diccionario entre A y B en el que cada elemento de A tiene un "significado" en B y viceversa. En muchos casos en matemática las biyecciones sirven para traducir estructuras de un conjunto a otro y luego también permiten traducir problemas y teoremas.

Entre los ejemplos de funciones que hemos visto hay algunas biyecciones y otras que no lo son.

Ejemplos.

(1) La función valor absoluto de números reales, de $\mathbb{R} \to \mathbb{R}$ no es biyectiva pues no es ni suryectiva ni inyectiva. El valor absoluto de $\mathbb{R} \to \mathbb{R}_{\geq 0}$ no es biyectivo, pues no es inyectivo. Ahora, si es biyectivo de $\mathbb{R}_{\geq 0} \to \mathbb{R}\geq 0$ ya que conincide con la función identidad de los reales mayores o iguales que 0, y también es biyectiva de $\mathbb{R}_{\leq 0} \to \mathbb{R}_{\geq 0}$.

(2) La función $f : \mathbb{N} \to \mathbb{Z}$ definida en (3.2) es una biyección. Ya vimos que es suryectiva. Además, por definición está claro que un entero positivo m es alcanzado por un natural par y más pecisamente por $2m$; es decir es alcanzado por uno y sólo un natural. Análogamente un entero negativo m es alcanzado por un impar, más precisamente por $n = -2m + 1$ y sólo por éste, que es impar y mayor que 1. Finalmente el 0, es alcanzado por el 1 y sólo por el 1.

(3) La función $x \mapsto x^2$, de $\mathbb{R}_{\geq 0} \to \mathbb{R}$, es inyectiva como ya vimos pero no es suryectiva, ya que el cuadrado de un número es siempre positivo y así ningun número negativo será alcanzado por esta función. Sin embargo si consideramos $x \mapsto x^2$ de $\mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ entonces si esta función es suryectiva y luego es biyectiva.

(4) La sucesión $E_n = [\frac{n+2}{2}]$ no es biyectiva como función de $\mathbb{N} \to \mathbb{N}$, pues no es inyectiva. Sin embargo es suryectiva como ya vimos. Ahora la restricción de esta sucesión al subconjunto $D = \{1, 2, 4, 6, 8, 10, \dots\} = 2\mathbb{N} \cup \{1\}$ es inyectiva y sigue siendo suryectiva. Por lo tanto $E|_D : D \to \mathbb{N}$ es una biyección.

3.2.4. Funciones inversas

La propiedad más importante de un función biyectiva, es la de poder "invertirse". Esto es, pensando a las funciones como procesos, la posibilidad de revertir un proceso. En la naturaleza hay procesos reversibles y hay procesos irreversibles. En matemática, también.

Sumar 1 a un entero, es reversible. El proceso inverso es restar 1. Elevar un número real o a un entero al cuadrado, no es reversible, pues a partir del resultado no podemos deducir de qué número se trataba. En efecto, si el resultado es 4, ¿se trata del número 2 o tal vez del -2? Imposible responder.

Sea $f : A \to B$ una función biyectiva. La *inversa* de f, es la función

$$f^{-1} : B \to A$$

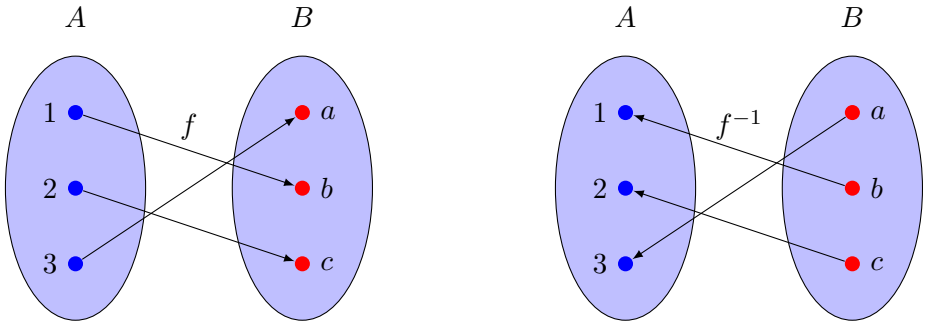
definida por

$$f^{-1}(b) = a \quad \text{si} \quad f(a) = b$$

donde a es el único elemento de A que es asignado por f a b.

La buena definición de la inversa se sigue de la biyectividad de la f. Por un lado, como f es suryectiva, cualquiera sea $b \in B$ existe al menos un $a \in A$ con $f(a) = b$; de esto se sigue que f^{-1} está definida en todo B (como debe ser). Por otro lado, por ser f inyectiva, el $a \in A$ tal que $f(a) = b$ es único, y luego no hay ambigüedad en la definición de f^{-1}.

Por ejemplo, tenemos



Observación. Si f es biyectiva, entonces su inversa f^{-1} es también biyectiva y su inversa es f. Es decir, $(f^{-1})^{-1} = f$. Volveremos sobre esto en la próxima sección.

Nota. Dada una función $f : A \to B$, no siempre es fácil determinar si es inyectiva o suryectiva. Y en caso de ser biyectiva no siempre es fácil describir su inversa.

Nota. Aunque los símbolos para la preimagen de f y la inversa de f son f^{-1}, no existe riesgo de confusión posible. Supongamos que $f : X \to Y$. Para empezar, la preimagen lleva asociado un conjunto en su notación. Es decir, hablamos de la preimagen $f^{-1}(B)$ de $B \subseteq Y$ por f. La preimagen de f es $f^{-1}(Y)$. Si el conjunto B consta de un único elemento, $B = \{b\}$, entonces $f^{-1}(\{b\}) = \{x \in X : f(x) = b\}$. En el caso particular en que f es inversible, con inversa f^{-1}, entonces es claro que para cada $y \in Y$ existe un único $x \in X$ tal que $f(x) = y$ y en ese caso tenemos $f^{-1}(y) = f^{-1}(\{y\})$ para todo $y \in Y$.

Ejemplos. Consideramos ahora algunas de las biyecciones vistas e intentamos describir sus inversas de alguna manera que resulte clara. Notamos que las inversas están bien defindas independientemene de nuestra capacidad para describirlas de manera satisfactoria. No siempre es imprescindible dar una fórmula; a veces una descripción "hablada" es mucho más clara.

(1) La función módulo $|\ |: \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ es una biyección; de hecho es la identidad. Luego su inversa es ella misma, la identidad. Ahora la función módulo $|\ | : \mathbb{R}_{\leq 0} \to \mathbb{R}_{\geq 0}$ también es una biyección. Su inversa tiene como dominio a los reales mayores o iguales que 0 y como imagen a los reales menores o iguales que 0. La inversa es la función "tomar el opuesto" o multiplicar por -1.

(2) Vimos que la función

$$f(n) = \begin{cases} \frac{n}{2} & \text{si } n \text{ es par,} \\ -\frac{(n-1)}{2} & \text{si } n \text{ es impar,} \end{cases} \tag{3.2}$$

que esencialmente es la función "dividir por 2" combinada con "tomar opuestos", es biyectiva de $\mathbb{N}$ en $\mathbb{Z}$. Su inversa de $\mathbb{Z}$ en $\mathbb{N}$ debe ser una combinación de "multiplicar por 2" y "tomar opuestos". No es díficil corroborar inspeccionando que la inversa está definida por

$$g(n) = \begin{cases} 2n & \text{si } n \geq 0, \\ -2n - 1 & \text{si } n < 0. \end{cases} \tag{3.3}$$

(3) Elevar al cuadrado, $x \mapsto x^2$, es biyactiva de $\mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$. Su inversa es la raíz cuadrada. Recordamos que dado un número positivo, como 2, hay dos números cuyo cuadrado es 2, uno positivo que es por definición su raíz cuadrada, y el otro su opuesto. En el caso de 2, éstos son $\sqrt{2}$ y $-\sqrt{2}$.

(4) Por último, vimos que la sucesión $E_n = \left[\frac{n+2}{2}\right]$ restringida al conjunto $D = \{1, 2, 4, 6, 8, \dots\}$ es una biyección de D en $\mathbb{N}$. Esta función lleva el 1 al 1 y si $n \geq 2$ y está en D, por ser par, resula que $E_n = \left[\frac{n+2}{2}\right] = \frac{n+2}{2} = \frac{n}{2} + 1$. Es fácil verificar que su inversa F, que es una biyección de $\mathbb{N}$ en D, está definida por

$$F_n = \begin{cases} 1 & \text{si } n = 1, \\ 2(n-1) & \text{si } n \geq 2. \end{cases} \tag{3.4}$$

3.2.5. La composición de funciones

Como siempre que tenemos un objeto matemático, en este caso las funciones, nos preguntamos ¿qué podemos hacer con ellas? ¿Cómo podemos hacerlas intereactuar entre sí? ¿Qué operaciones podemos definir entre ellas?

Para conjuntos vimos que podemos tomar uniones, intersecciones y complementos.

Sin dudas, para nuestros fines, la operación entre funciones más importante es la composición, que pasamos a describir. Dadas dos funciones g y f queremos construir una nueva función aplicando primero una función, digamos la f, y a continuación la otra función, en este caso la g. Para que esto sea posible, la imagen de f debe estar contenida en el dominio de g, es decir

$$Im(f) \subseteq Dom(g)$$

La nueva función obtenida se llama composición de f con g.

Más precisamente, dadas

$$f : A \to B \quad \text{y} \quad g : C \to D \quad \text{con} \quad B \subseteq C \tag{3.5}$$

entonces la *composición* de g con f, que se lee g *compuesta con* f (o simplemente $g\ o\ f$), es la función

$$g \circ f : A \to C, \qquad a \mapsto g(f(a))$$

Es decir, la imagen de un a por la composición de g con f es la imagen por g de la imagen por f de a; en símbolos

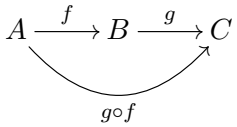
$$(g \circ f)(a) = g(f(a))$$

Observación. Observamnos que $Im(g \circ f) \subseteq Im(g)$ y que la contención puede ser estricta o no.

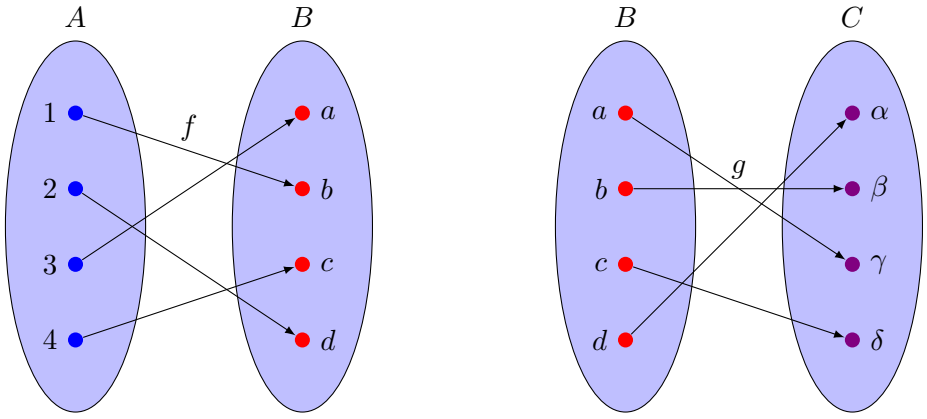
Dos situaciones en las que siempre pasa que $Im(f) \subseteq Dom(g)$ (es decir $B \subseteq C$ en (3.5)) y por lo tanto siempre podemos componer, son

- $f : A \to A$, $g : A \to A$.
- $f : A \to B$, $g : B \to C$.

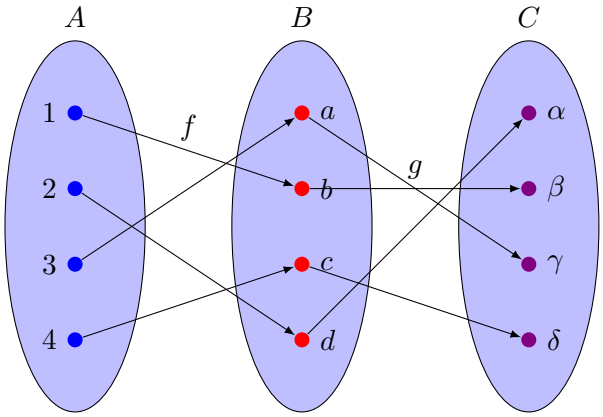
Gráficamente,



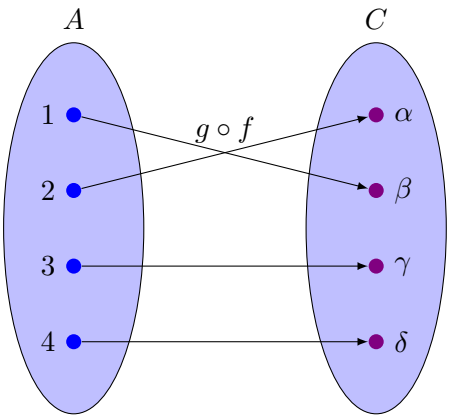
Por ejemplo, si tenemos $f : A \to B$ y $g : B \to C$ dadas por



entonces la composición de g con f es



es decir, $g \circ f : A \to C$ queda



De ahora en adelante, cuando escribamos $g \circ f$ asumiremos que tiene sentido hacer tal composición.

Nota. Si pensamos a las funciones como procesos o transformaciones, la composición de dos de éstos (cuándo el posible) es el proceso o la transformación que resulta de aplicar uno a continuación del otro.

Si uno de estos procesos es lijar y el otro pintar, la composición resulta en lijar y pintar. Notemos que el orden de la composición es relevante; no es lo mismo lijar y pintar que pintar y lijar.

En el caso particular en que $f : A \to A$, uno puede componer f con si misma, es decir $f \circ f$. Es usual denotar por f^2 a $f \circ f$, es decir $f^2(x) = f(f(x))$. Nada impide que compongamos una vez mas y se pone $f^3 = f \circ f^2 = f \circ (f \circ f)$. Es decir, $f^3(x) = f(f^2(x)) = f(f(f(x)))$. Esto puede hacerse el número de veces que uno quiera y en general se tiene

$$f^n = f \circ f^{n-1}$$

para cualquier número natural n.

Por ejemplo, si $f : \{1, 2, 3\} \to \{1, 2, 3\}$ está dada por $f(1) = 2$, $f(2) = 3$ y $f(3) = 1$ entonces f^3 es la identidad de $\{1, 2, 3\}$.

Nota. Aquí hay que tener cuidado con la notación y no confundir $f^n(x)$ con $f(x)^n$. Por ejemplo, $f^2(x) = f(f(x))$ con $f(x)^2 = f(x)f(x)$.

Nota. Para funciones, las operaciones más comunes son la suma y el producto, cuando estas puedan ser definidas. Dadas dos funciones $f, g : A \to B$ y supongamos que en B hay definida una suma (por ejemplo $B = \mathbb{R}$), se define la suma y el producto 'punto a punto', entre ellas. Es decir, la función *suma* $f + g$ es la función que en un punto a vale la suma de los valores de $f(a)$ y $g(a)$. Similarmente, la función *producto* fg, es la función que en un elemento a toma el valor del producto entre $f(a)$ y $g(a)$. En símbolos, tenemos

$$f + g : A \to B, \qquad (f + g)(a) = f(a) + g(a)$$

para la suma y

$$fg : A \to B, \qquad (fg)(a) = f(a)g(a)$$

para el producto.

Propiedades algebraicas y yectivas de la composición

Para entender mejor la composición nos hacemos algunas preguntas sobre propiedades básicas sobre las que es bueno pensar. En las primeras nos preguntamos por las propiedades algebraicas de la composición como operación. En las últimas, nos cuestionamos sobre la relación que hay entre la suryectividad e inyectividad de f o de g y la correspondiente suryectividad o inyectividad de $f \circ g$.

Preguntas.

(1) ¿Es la composición asociativa?

(2) ¿Es la composición conmutativa?

(3) Si f es suryectiva/inyectiva, ¿es $f \circ g$ suryectiva/inyectiva?

(4) Si g es suryectiva/inyectiva, ¿es $f \circ g$ suryectiva/inyectiva?

(5) Si $f \circ g$ es suryectiva/inyectiva, ¿es f suryectiva/inyectiva?

(6) Si $f \circ g$ es suryectiva/inyectiva, ¿es g suryectiva/inyectiva?

Respuestas.

(1) Las dos primeras preguntas se refieren a la validez de las identidades

$$f \circ (g \circ h) = (f \circ g) \circ h$$
$$f \circ g = g \circ f$$

donde f, g y h son funciones para las cuales están definidas todas las composiciones necesarias. Lo más elemental que podemos hacer para decidir si dos funciones son o no iguales es evaluarlas en algún elemento genérico de su dominio y ver que pasa. Supongamos que a está en el dominio de h. Entonces por un lado tenemos que

$$\big(f \circ (g \circ h)\big)(a) = f\big((g \circ h)(a)\big) = f(g(h(a)))$$

y por otro lado

$$\big((f \circ g) \circ h\big)(a) = (f \circ g)(h(a)) = f(g(h(a)))$$

Se sigue que ambas composiciones son iguales y la composición es entonces asociativa.

En el caso de la composición de dos funciones en uno y otro sentido, si procedemos de la misma manera obtenemos que

$$f \circ g(a) = f(g(a)) \quad \text{y} \quad g \circ f(a) = g(f(a))$$

de donde no se desprende que sean iguales, más aún debería hacernos suponer que es posible que haya funciones f y g para las cuales $f(g(a)) \neq g(f(a)$ al menos para algún a. En efecto este es el caso y no hace falta buscar mucho ya que es más difícil encontrar funciones f y g para las cuales si vale $f \circ g = g \circ f$. Por ejemplo, si f es la función constantemente igual a b y g es la función constantemente igual a c, entonces para todo a tenemos que

$$f \circ g(a) = f(c) = b \quad \text{y} \quad g \circ f(a) = g(b) = c$$

Así si $b \neq c$ tenemos un ejemplo como el que buscábamos.

(2) Las dos segundas preguntas indagan sobre qué propiedades yectivas de f y g pasan o son heredadas por la composición $f \circ g$. Es decir, si es suficiente que f o g tengan alguna propiedad yectiva para asegurar la misma propiedad para la composición.

Teniendo en cuenta que tanto f como g pueden ser, por ejemplo, constantes, se hace difícil creer que la composición pueda heredar alguna buena propiedad yectiva de f o g. Las funciones constantes están muy lejos de ser suryectivas y muy lejos de ser inyectivas. En efecto, si o bien f o bien g es constante, entonces la composición $f \circ g$ es constante. Luego, las respuestas a las tercera y cuarta preguntas son negativas.

(3) Las dos últimas van en el sentido opuesto de las que acabamos de contestar. Indgan sobre las propiedades yectivas de f ó g que son necesarias para que la composición tenga esas propiedades.

Dos cosas son claras. Si f no es sobreyectiva, $f \circ g$ tampoco lo es, pues $Im(f \circ g) \subseteq Im(f)$. Si g no es inyectiva, $f \circ g$ tampoco lo es, pues si $g(x) = g(y)$ con $x \neq y$, entonces $(f \circ g)(x) = (f \circ g)(y)$.

Así, para que $f \circ g$ sea suryectiva, es necesario que f lo sea. Para que $f \circ g$ sea inyectiva, es necesario que g lo sea.

Queda preguntarnos si hay más cosas necesarias. La respuesta es no. De hecho sucede que siendo f no inyectiva, $f \circ g$ si lo es. Por ejemplo, si $f(x) = x^2$ y $g(x) = e^x$ como funciones de $\mathbb{R}$ en $\mathbb{R}$, la composición $(f \circ g)(x) = e^{2x}$ es inyectiva a pesar de no ser f inyectiva. Esto es posible pues la imagen de g es un subconjunto del dominio de f donde f si es inyectiva. Es este ejemplo $Im(g) = \mathbb{R}_{>0}$. También sucede que $f \circ g$ es suryectiva a pesar de no serlo la función g. Este es el caso, por ejemplo, si tomamos $f(x) = \log(|x|)$, $f(0) = 0$ y $g(x) = x^2$. En efecto, $(f \circ g)(x) = 2\log(|x|)$ para $x \neq 0$ y $f(g(0)) = f(0) = 0$. Luego, $f \circ g$ es sobreyectiva, y de hecho su restricción a los reales positivos es sobreyectiva.

Composición de funciones e inversas

Sea ahora $f : A \to B$ una función biyectiva y sea $f^{-1} : B \to A$ su inversa. Evaluemmos las composiciones

$$f^{-1} \circ f : A \to A \qquad \text{y} \qquad f \circ f^{-1} : B \to B$$

Para la primera, tomamos un $a \in A$ y calculamos

$$(f^{-1} \circ f)(a) = f^{-1}(f(a)) = a$$

Para la segunda, tomamos un $b \in B$ y calculamos

$$(f \circ f^{-1})(b) = f(f^{-1}(b)) = b$$

Es decir,

$$f^{-1} \circ f = I_A \qquad \text{y} \qquad f \circ f^{-1} = I_B$$

donde I_A e I_B son las identidades de A y B respectivamente.

Observación. Hemos mostrado que las composiciones de una función biyectiva con su inversa son iguales a las funciones identidad de sus respectivos dominios. Resulta que esta propiedad caracteriza a las funciones biyectivas y a sus inversas. Supongamos que $f : A \to B$ es una función, en principio no necesariamente biyectiva, para la cual existe una función $g : B \to A$ tal que

$$g \circ f = I_A \qquad \text{y} \qquad f \circ g = I_B.$$

De estas identidades se sigue en primer término que f y g son biyectivas.

- INYECTIVIDAD: Si a_1 y a_2 son elementos de A tales que $f(a_1) = f(a_2)$, entonces $g(f(a_1)) = g(f(a_2))$; pero como $g \circ f = I_A$ se sigue que

$$a_1 = \big(g \circ f\big)(a_1) = \big(g \circ f\big)(a_2) = a_2.$$

- SURYECTIVIDAD: Dado $b \in B$ sea $a = g(b)$. Como $f \circ g = I_B$ se sigue que

$$b = \big(f \circ g\big)(b) = f(g(b))$$

  Es decir, $a = g(b)$ es asignado por f a b. Como b es arbitrario, resulta que f es suryectiva.

Ahora, se sigue además que g es la *inversa* de f. En efecto, si $a \in A$ y $f(a) = b$, como $a = g \circ f(a) = g(b)$, tenemos que $g(b) = a$. Como esto es cierto para todo $a \in A$,

$$g = f^{-1}$$

Notar que una consecuencia directa de esto es que la función inversa de f^{-1} es la misma f, es decir

$$(f^{-1})^{-1} = f$$

Coloquialmente podemos decir: la inversa de la inversa es la función con que empezamos.

Observación. Si U es un conjunto, entonces la relación definida en $\mathcal{P}(U)$ por

$$A \sim B \quad \Leftrightarrow \quad \text{existe una biyección de } A \text{ a } B$$

es de equivalencia. En efecto $A \sim A$ pues la identidad es una biyección de A en si mismo. Si $A \sim B$, entonces existe $f : A \to B$ biyectiva, luego su inversa $f^{-1} : B \to A$ es una biyección y así resulta $B \sim A$. Finalmente, si $A \sim B$ y $B \sim C$, entonces existen biyecciones $f : A \to B$ y $g : B \to C$. Como la composición $g \circ f$ es una biyección de A en C, resulta $A \sim C$.

3.2.6. Funciones y las operaciones de conjuntos

Sea f una función $f : A \to B$. Dados subconjuntos C y D del dominio, es decir $C \subseteq A$ y $D \subseteq A$, tenemos los conjuntos imágenes de éstos $f(C) \subseteq B$ y $f(D) \subseteq B$. Nos interesa investigar, por ejemplo, la relación entre $f(C \cap D)$ y $f(C) \cap f(D)$.

Ejemplo. Sean $A = \{1, 2, 3, 4, 5\}$, $B = \{\alpha, \beta, \gamma\}$ y $f : a \to B$ definida por:

$$f(1) = \alpha, \quad f(2) = \beta, \quad f(3) = \gamma, \quad f(4) = \beta, \quad f(5) = \alpha.$$

Si $C = \{1, 2, 3\}$ y $D = \{3, 4, 5\}$, entonces

$$C \cap D = \{3\} \quad \text{y} \quad f(C \cap D) = \{\gamma\}$$

$$f(C) = \{\alpha, \beta, \gamma\}, \quad f(D) = \{\alpha, \beta, \gamma\} \quad \text{y} \quad f(C) \cap f(D) = \{\alpha, \beta, \gamma\}.$$

En este caso resulta que $f(C \cap D) \subsetneq f(C) \cap f(D)$. ◊

Dado el ejemplo anterior no podemos esperar que en general $f(C \cap D) = f(C) \cap f(D)$. Queda preguntarnos si es o no cierto que siempre $f(C \cap D) \subseteq f(C) \cap f(D)$. Intentemos probar esto.

- Sea $a \in C \cap D$ cualquiera. Como $a \in C$, $f(a) \in f(C)$ y como $a \in D$, $f(a) \in f(D)$. Luego $f(a) \in f(C) \cap f(D)$. Hemos probado que $f(C \cap D) \subseteq f(C) \cap f(D)$.

Ya vimos un ejemplo en el que la contención es propia. También puede suceder que la contención sea una igualdad como sucede, por ejemplo, si f es la función identidad.

La proposición que sigue describe lo que sucede en varias situaciones de interés.

Proposición 3.2. *Sea $f : A \to B$ y sean $C, D \subseteq A$ y $E, F \subseteq B$. Entonces valen:*

(a) $f(C \cap D) \subseteq f(C) \cap f(D)$.

(b) $f(C \cap D) = f(C) \cap f(D)$ *si y sólo si* f *es inyectiva.*

(c) $f(C \cup D) = f(C) \cup f(D)$.

(d) $f^{-1}(E \cap F) = f^{-1}(E) \cap f^{-1}(F)$.

(e) $f^{-1}(E \cup F) = f^{-1}(E) \cup f^{-1}(F)$.

Aquí, $f^{-1}(E)$ es la preimagen por f de E.

Demostración.

(a) Sea $a \in C \cap D$ cualquiera. Como $a \in C$, $f(a) \in f(C)$ y como $a \in D$, $f(a) \in f(D)$. Luego $f(a) \in f(C) \cap f(D)$.

(b) Por el item anterior una contención vale siempre. Dado $b \in f(C) \cap f(D)$ y asumiendo que f es inyectiva, debemos mostrar que $b \in f(C \cap D)$. Notar que $f(C \cap D) \subseteq f(C)$ y $f(C \cap D) \subseteq f(D)$. Como $b \in f(C)$, existe un $c \in C$ tal que $f(c) = b$ y como $b \in f(D)$, existe un $d \in D$ tal que $f(d) = b$. Ahora como f es inyectiva y $f(c) = b = f(d)$ se sigue que $c = d$. Así hemos encontrado $c \in C \cap D$ tal que $f(c) = b$ como queríamos.

(c) Si $b \in f(C \cup D)$, existe $a \in C \cup D$ tal que $f(a) = b$. Luego $a \in C$ o $a \in D$ y así $b = f(a) \in f(C)$ ó $b = f(a) \in f(D)$. Es decir $b \in f(C) \cup f(D)$. Recíprocamente, si $b \in f(C) \cup f(D)$, entonces $b \in f(C)$ ó $b \in f(D)$. Luego existe $a \in C$ tal que $b = f(a)$ o existe $a \in D$ tal que $b = f(a)$. Es decir existe $a \in C \cup D$ tal que $b = f(a)$ y así $b \in f(C \cup D)$.

(d) Si $a \in f^{-1}(E \cap F)$, entonces $f(a) \in E \cap F$; luego $a \in f^{-1}(E)$ y $a \in f^{-1}(F)$, es decir $a \in f^{-1}(E) \cap f^{-1}(F)$.

Si $a \in f^{-1}(E) \cap f^{-1}(F)$, entonces $f(a) \in E$ y $f(a) \in F$, es decir $f(a) \in E \cap F$ y así $a \in f^{-1}(E \cap F)$.

(e) Si $a \in f^{-1}(E \cup F)$, entonces $f(a) \in E \cup F$, es decir $f(a) \in E$ o $f(a) \in F$. Luego $a \in f^{-1}(E)$ o $a \in f^{-1}(F)$ y así $a \in f^{-1}(E) \cup f^{-1}(F)$.

Si $a \in f^{-1}(E) \cup f^{-1}(F)$, entonces $a \in f^{-1}(E)$ o $a \in f^{-1}(F)$, es decir $f(a) \in E$ o $f(a) \in F$. Luego $f(a) \in E \cup F$ y así $a \in f^{-1}(E \cup F)$.

La demostración está completa. □

Es decir, la preimagen de f se 'porta bien' con las uniones e intersecciones mientras que tomar imagen por f respeta la unión, pero sólo respeta la intersección si f es inyectiva.

Claramente estas propiedades valen, con las mismas demostraciones, para uniones e intersecciones finitas. Es decir, para la imagen tenemos

$$f(A_1 \cap \cdots \cap A_n) \subseteq f(A_1) \cap \cdots \cap f(A_n)$$
$$f(A_1 \cup \cdots \cup A_n) = f(A_1) \cup \cdots \cup f(A_n)$$

con igualdad en la primera expresión válida si f es inyectiva, y para la preimagen vale

$$f^{-1}(A_1 \cap \cdots \cap A_n) = f^{-1}(A_1) \cap \cdots \cap f^{-1}(A_n)$$
$$f^{-1}(A_1 \cup \cdots \cup A_n) = f^{-1}(A_1) \cup \cdots \cup f^{-1}(A_n)$$

Similarmente, análogos resultados valen para uniones e interesecciones arbitrarias.

3.2.7. Producto cartesiano y funciones †

Dado un conjunto B, a veces es útil identificar el producto cartesiano $B \times B$ con el conjunto de todas las funciones del conjunto $\{1, 2\}$ en B. Esto es, entender a un par ordenado de elementos de B, (a, b), como la función $f : \{1, 2\} \to B$ definida por $f(1) = a$ y $f(2) = b$. Es decir,

$$B \times B \quad \longleftrightarrow \quad \{f : \{1, 2\} \to B\}$$

De manera análoga, para cualquier natural n, identificamos al producto cartesiano

$$B^n = \underbrace{B \times \cdots \times B}_{n-\text{veces}}$$

con el conjunto de todas las funciones de $\{1, 2, \ldots, n\}$ en B. Es decir,

$$B^n \quad \longleftrightarrow \quad \{f : \{1, 2, \ldots, n\} \to B\}$$

Estas identificaciones nos permiten ahora definir el producto cartesiano de B con B tantas veces como querramos. Por ejemplo, definimos entonces al producto cartesiano de B con B "$\mathbb{N}$-veces" como el conjunto de todas las funciones de $\mathbb{N}$ en B, es decir como el conjunto de todas las sucesiones con valores en B. A este producto cartesiano lo denotamos $B^{\mathbb{N}}$. Así

$$B^{\mathbb{N}} := \{f : \ f : \mathbb{N} \to B\} = \{\text{sucesiones con valores en } B\}$$

Notamos que esta notación es consistente con la usada para productos cartesianos finitos si entendemos a $B^n = B^{\{1,2,\ldots,n\}}$.

Por otro lado también tiene sentido considerar $B^{\mathbb{R}}$ como el conjunto de todas las funciones de $\mathbb{R}$ en B y en general B^A como el conjunto de todas las funciones de A en B.

Ejemplo. Sean $A = \{1, 2, 3, 4\}$ y $B = \{p, q, r, s\}$ y consideremos el producto cartesiano B^A que identificamos con B^4. Entendiendo a cada elemento de B^4 como una función tenemos:

- (q, q, q, q) es una función constante; es constantemente igual a q.
- (p, r, p, q) no es inyectiva pues p es alcanzado dos veces.
- (s, r, q, p) y (s, r, p, q) son dos biyecciones distintas.

3.3. Conjuntos finitos y cardinalidad

Todos sabemos contar. Al menos cantidades no muy grandes. Para cantidades pequeñas nos bastan los dedos de las manos y es con estos dedos que aprendemos a contar de chicos. Aun cuándo los chicos muy pequeñoss no saben los números, saben decir con los dedos si hay 2 o 3 caramelos. Aprenden a contar figuritas agregando un dedo a medida que pasan una por una. La mano es la regla para medir la cantidad de objetos que hay y el dedo es la unidad de medida. Queremos formalizar y generalizar esta forma de "contar con las manos".

Denotamos al subconjunto de los primeros n naturales por $[\![1, n]\!]$, es decir

$$[\![1, n]\!] = \{1, 2, 3, \ldots, n\} \tag{3.6}$$

En matemática usamos a los naturales y a estos subconjuntos distinguidos como "reglas" para medir el tamaño de conjuntos. Este conjunto tiene n elementos o tiene *cardinal* n.

Definición. Decimos que un conjunto A es *finito*, si existe una función biyectiva de $[\![1, n]\!]$ en A para algún $n \in \mathbb{N}$. Denotamos esto por $|A| < \infty$. Decimos que A es *finito de cardinal* n, si existe una función biyectiva de $[\![1, n]\!]$ en A y denotamos esto por

$$|A| = \#A = n$$

Finalmente, se dice que A es *infinito* si no es finito. Además, convenimos en que el cardinal del conjunto vacío es 0.

Ejemplos.

(1) El conjunto de vocales $V = \{$a,e,i,o,u$\}$ tiene cardinal 5. (Los dedos de una mano alcanzan.) Formalmente, la función $f : [\![1, 5]\!] \to V$, definida por

$$1 \mapsto \text{a}, \quad 2 \mapsto \text{b}, \quad 3 \mapsto \text{c}, \quad 4 \mapsto \text{d}, \quad 5 \mapsto \text{e},$$

es una biyección. Está claro que no es la única. La función definida por

$$1 \mapsto \text{e}, \quad 2 \mapsto \text{d}, \quad 3 \mapsto \text{c}, \quad 4 \mapsto \text{b}, \quad 5 \mapsto \text{a},$$

es otra.

(2) Los siguientes son ejemplos de conjuntos de cardinal n.

- $\{a_1, a_2, \ldots, a_{n-1}, a_n\}$, si los a_i son todos distintos.
- $\{1, 3, 5, \ldots, 2n - 3, 2n - 1\}$.

- $\{2, 2^2, 2^3, \ldots, 2^{n-1}, 2^n\}$.
- $\{\frac{1}{a+1}, \frac{1}{a+2}, \frac{1}{a+3}, \ldots, \frac{1}{a+n}\}$.
- $[\![2, n+1]\!] = \{2, 3, \ldots, n, n+1\}$.
- $[\![m, m+n-1]\!] = \{m, m+1, \ldots, m+n-2, m+n-1\}$.
- $[\![1, k]\!] \cup [\![\ell+1, \ell+n-k]\!]$, con $k \leq \ell$ (si $k = \ell$ tenemos $[\![1, n]\!]$).

Si intentamos leer estos conjuntos tal como están escritos, describiendo sus elementos uno por uno, estaremos describiendo una biyección de $[\![1, n]\!]$ en cada uno de ellos. Dejamos al lector el ejercicio de escribir formalmente éstas u otras biyecciones en cada caso.

(3) El conjunto $\mathbb{N}$ de los números naturales es infinito. Supongamos que fuera finito, entonces existiría una biyección entre $[\![1, n]\!]$ y $\mathbb{N}$ para algún $n \in \mathbb{N}$. Si $f : [\![1, n]\!] \to \mathbb{N}$ una biyección y $f(1) = a_1, f(2) = a_2, \ldots, f(n) = a_n$, sea $a = \max\{a_1, \ldots, a_n\}$. Como $a \in \mathbb{N}$ se sigue que $a + 1 \in \mathbb{N}$, pero $a + 1 \notin \mathrm{Im}(f)$, lo cual es absurdo pues f es en particular suryectiva. ◊

Observación. Si A y B son dos conjuntos del mismo cardinal, digamos n, entonces existe una biyección entre ambos. En efecto como A y B tienen cardinal n, existen una biyección $f : [\![1, n]\!] \to A$ y una biyección $g : [\![1, n]\!] \to B$. Ahora $g \circ f^{-1} : A \to B$ es una biyección.

Recíprocamene si A tiene cardinal n y B es tal que existe una biyección de A de B, entonces B tiene también cardinal n. En efecto, como A tiene cardinal n existe una biyección $f : [\![1, n]\!] \to A$ y si $g : A \to B$ es una biyección, entonces $g \circ f : [\![1, n]\!] \to B$ es una biyección y así B tiene cardinal n.

Si A es un conjunto finito, entonces la relación de equivalencia para subconjuntos de A vista en la Sección 3.2.5, dada por $B \sim C$ si y sólo si existe una biyección entre B y C, parte o clasifica a los subconjuntos de A según su cardinal. Los equivalentes a uno dado son todos los que tienen su mismo cardinal.

El tener una biyección entre dos conjuntos permite traducir los problemas y verdades de uno al otro. En particular, los problemas de conteo en conjuntos finitos se pueden expresar como problemas de conteo en los conjuntos $[\![1, n]\!]$. Es decir, ante un problema sobre un conjunto finito A, podemos suponer que $A = [\![1, n]\!]$. Un ejemplo de este principio es el siguiente problema.

Pregunta. ¿Cuántos subconjuntos tiene un conjunto finito?

El mismo enunciado del problema asume que la respuesta no depende de la naturaleza del conjunto y de sus elementos, sino solamente de su cardinal.

Respuesta. Si A es de cardinal n, entonces A tiene 2^n subconjuntos.

Es decir, si A es finito de cardinal n, entonces $\mathcal{P}(A)$ es también finito y de cardinal 2^n. Más adelante entenderemos porqué esto es así y daremos una demostración. Sin embargo mostramos ahora mismo cómo reducimos este problema al caso en que el conjunto A sea el conjunto patrón $[\![1, n]\!]$.

Veamos que una biyección de un conjunto finito F de cardinal n con $[\![1, n]\!]$, induce además una biyección natural entre los conjuntos de partes de estos conjuntos.

Proposición 3.3. *Si F es un conjunto finito de cardinal n y $f : [\![1, n]\!] \to F$ es una biyección, entonces f induce una biyección*

$$\tilde{f} : \mathcal{P}([\![1, n]\!]) \to \mathcal{P}(F)$$

tal que $\tilde{f}(\{i\}) = \{f(i)\}$, para todo $1 \leq i \leq n$. La biyección $\tilde{f}$ lleva subconjuntos de cardinal m en subconjuntos de cardinal m.

Demostración. Debemos definir la función $\tilde{f}$ para todo subconjunto de $[\![1, n]\!]$. Primero definimos $\tilde{f}(\varnothing) = \varnothing$. Luego, por hipótesis, debemos defirla en los singuletes como $\tilde{f}(\{i\}) = \{f(i)\}$. Ahora si $A \subseteq [\![1, n]\!]$, definimos $\tilde{f}(A) = \{f(i) : \ i \in A\}$.

Como f es biyección se sigue que $f|_A : A \to \tilde{f}(A)$ es una biyección y en particular A y $\tilde{f}(A)$ tienen el mismo cardinal.

Para mostrar que $\tilde{f}$ es una biyección construimos su inversa. Consideramos la inversa de f, $f^{-1} : F \to [\![1, n]\!]$ y definimos de manera análoga $\tilde{f^{-1}}$. Se sigue de la construcción de ambas que $\tilde{f}$ y $\tilde{f}^{-1}$ son inversas una de otra. □

La siguiente proposición afirma algo que es intuitivo para el caso de conjuntos finitos.

Proposición 3.4. *Si A es un conjunto finito de cardinal n y $B \subseteq A$ es un subconjunto también de cardinal n, entonces $B = A$.*

Demostración. Para dar una demostración de este hecho deberemos esperar un poco. □

3.3.1. Conjuntos infinitos y numerabilidad †

En general, mientras que nuestra intuición es correcta cuando trabajamos con conjuntos finitos, no lo es tanto cuando trabajamos con conjuntos infinitos. Por ejemplo, para conjuntos infinitos no es cierto que si $A \subseteq B$ y ambos tienen el mismo "cardinal", entonces son iguales.

No vamos a definir ni estudiar la noción de cardinal para conjuntos infinitos. Lo que si haremos es definir numerabilidad y consideraremos entonces conjuntos numerables y conjuntos no numerables.

Dado un conjunto infinito A decimos que es *numerable*, si existe una función biyectiva del conjunto de todos los naturales $\mathbb{N}$ en A. Un conjunto infinito que no es numerable se dice *no numerable*.

Observación. Al igual que en el caso de conjuntos finitos, si dados dos conjuntos infinitos hay una biyección entre ellos y uno es numerable, el otro también es numerable.

Como dijimos más arriba, el cardinal como noción de tamaño para conjuntos infinitos no siempre resulta intuitiva. Por ejemplo, el conjunto de números naturales tiene un subconjunto propio (en el sentido de la contención, estrictamente más chico) del mismo cardinal que $\mathbb{N}$, es decir también numerable. A saber, $2\mathbb{N} \subsetneq \mathbb{N}$ y ambos son numerables. La función que multiplica por 2 es una biyección de $\mathbb{N}$ en $2\mathbb{N}$ (su inversa es la función que divide por 2). Otro ejemplo usando los enteros es $\mathbb{N} \subsetneq \mathbb{Z}$; ambos son numerables. En la Sección 3.2.3 definimos una biyección de $\mathbb{N}$ en $\mathbb{Z}$. Los siguientes son varios ejemplos del mismo fenómeno.

Ejemplos. Los siguientes son subconjuntos propios numerables de $\mathbb{N}$.

(1) Los pares $2\mathbb{N}$ y los impares $2\mathbb{N}+1$.

(2) Los múltiplos de 3 y los conjuntos de números con resto 1 y 2 al dividir por 3, respectivamente. Es decir, $3\mathbb{N}$, $3\mathbb{N}+1$ y $3\mathbb{N}+2$.

(3) Para cualquier $a \in \mathbb{N}$, los conjuntos de resto r, $0 \leq r \leq n-1$, al dividir por a, es decir $a\mathbb{N}, a\mathbb{N}+1, \ldots, a\mathbb{N}+r, \ldots, a\mathbb{N}+(n-1)$.

(4) Los conjuntos de la forma $\{am+bn : m,n \in \mathbb{N}\}$, con $a,b \in \mathbb{N}$.

(5) Los números primos $\mathbb{P}$.

(6) Los conjuntos $[\![1,n]\!]^c = \{n+1, n+2, \ldots\} = \{m \in \mathbb{N} : m \geq n\}$ para cualquier $n \in \mathbb{N}$.

(7) Más generalmente, los complementos de los conjuntos finitos.

(8) Las potencias de 2, $\{2^n : n \in \mathbb{N}\}$.

(9) Las potencias pares de $a \in \mathbb{N}$, $\{a^{2n} : n \in \mathbb{N}\}$.

(10) Los números que contienen la cadena 2015 en su notación decimal.

(11) Los números que tienen exactamente 13 unos y 17 cuatros como dígitos.

(12) Cualquier sucesión $\{a_n\}$ con valores en $\mathbb{N}$, que tome infinitos valores distintos (si no sería un conjunto finito).

Dejamos a cargo del lector la tarea de encontrar una biyección explícita en cada caso. ◊

Nota. Todo conjunto infinito, es por lo menos numerable, en el sentido que contiene un subconjunto numerable. Ahora, existen conjuntos infinitos no numerables, es decir más grandes (mucho más grandes) que $\mathbb{N}$. Este es el caso, por ejemplo, del conjunto de números reales $\mathbb{R}$. Otro conjunto no numerable es el conjunto de partes de $\mathbb{N}$, $\mathcal{P}(\mathbb{N})$, que está en biyección con $\mathbb{R}$.

3.3.2. Operaciones de conjuntos y numerabilidad

Algunos conjuntos construidos a partir de conjuntos numerables resultan numerables. Conocer esto permite muchas veces probar que un conjunto es numerable de manera sencilla. Esto sucede por ejemplo con los números racionales.

Consideramos cinco situaciones que aparecen muy frecuentemente. En todos los casos presentamos ideas y damos argumentos que fundamentan la que sucede, aunque para dar demostraciones completas en necesario conocer mejor a los números naturales, los que estudiaremos en profundidad más adelante. De todas manera son verdades que podremos usar con confianza de ahora en mas.

- **Subconjuntos**
- **Conjuntos intermedios**

- **Intersecciones**
- **Uniones finitas**
- **Productos cartesianos finitos**

Subconjuntos

Si A es numerable y $B \subset A$, entonces B es a lo sumo numerable; esto es, puede ser finito, pero si no lo es, entonces es numerable.

En efecto, como A es numerable existe una biyección

$$f : A \to \mathbb{N}$$

Ahora la restricción de f a B tiene por imágen a un subconjunto de $\mathbb{N}$. Así todo se reduce a entender los subconjuntos de $\mathbb{N}$. Y éstos son finitos o numerables.

En efecto, si $B \subset \mathbb{N}$ procedemos de la siguiente manera:

- Tomamos el $1 \in \mathbb{N}$ y lo asignamos al primer natural de B, que podemos nombrar a_1, que no necesariamente será 1.
- Tomamos el $2 \in \mathbb{N}$ y lo asignamos al primer natural de B más grande que a_1 y lo llamamos a_2.
- Continuamos así con los siguientes naturales.

Si en algún momento agotamos todo B, entonces B es finito. Si no, queda definida una biyección $f : \mathbb{N} \to B$, donde $f(n) = a_n$.

Conjuntos intermedios

Si $C \subseteq B \subseteq A$ y tanto A como C son numerables, entonces B también es numerable.

Esto se sigue directamente del item anterior, ya que por un lado como B es subconjunto de A y A es numerable, B es finito o numerable. Pero como B contiene a C que no es finito, B no puede ser finito y resulta numerable.

Intersecciones

Si A_i con $i \in I$ es una colección de conjuntos numerables, entonces la intersección de todos ellos es a lo sumo numerable. Esto se sigue nuevamente del primer item ya que la intersección es un subconjunto de cualquiera de ellos;

$$\bigcap_{i \in I} A_i \subseteq A_{i_0}$$

Uniones finitas

Si $A_1, \dots A_n$ son n conjuntos numerables, la unión de ellos

$$\bigcup_{i=1}^{n} = A_1 \cup \cdots \cup A_n$$

es siempre numerable.

Observamos que para entender esto basta hacerlo para la unión de dos conjuntos, ya que la unión es asociativa. Así podemos hacer $A_1 \cup A_2$ que será numerable y luego unirle A_3; esta unión será entonces numerable y podemos unirle A_4 y continuar así hasta terminar con los n conjuntos.

Sean A y B dos conjuntos numerables. Para *numerar* a la unión $A \cup B$ procedemos así.

- Al $1 \in \mathbb{N}$ le asignamos el primer elemento de A.
- Al 2 le hacemos corresponder el primer elemento de B.
- Al 3 lo envíamos al segundo elemento de A.
- Al 4 lo mandamos al segundo elemento de B.
- Y en general, asignamos los impares a los elementos de A y los pares a los elementos de B.

Formalmente si $f : \mathbb{N} \to A$ y $g : \mathbb{N} \to B$ son las biyecciones que numeran a A y a B, definimos $h : \mathbb{N} \to A \cup B$ por

$$h(n) = \begin{cases} f(k), & \text{si } n = 2k-1 \\ g(k), & \text{si } n = 2k \end{cases}$$

La función h es una biyección y con la cual numeramos a la unión $A \cup B$.

Productos cartesianos finitos

Al igual que en el caso de la unión, basta mostrar que el producto cartesiano de dos conjuntos numerables es numerable. Dados A y B numerables numeramos el producto cartesiano $A \times B$ "por diagonales" como muestra el dibujo.

——— DIBUJO ———

Para escrbir formalmente la biyección descripa en el dibujo observamos que en cada diagonal la suma de la fila y la columna de sus elementos es constante. En la primera diagonal, que tiene un solo elemento, esta suma es igual a 2; en la siguiente igual a 3 y en la próxima igual a 4.

Para definir formalmente esta función, conviene definir en primer lugar su inversa, es decir una biyección $h : A \times B \to \mathbb{N}$. Si $f : \mathbb{N} \to A$ y $g : \mathbb{N} \to B$ son las biyecciones que numeran a A y a B respectivamente, definimos h como sigue. Dado (a, b) consideramos sus respectivos órdenes, es decir $i = f^{-1}(a)$ y $j = g^{-1}(b)$; esto nos indica que (a, b) está en la diagonal $i + j - 1$ y en ella ocupa el lugar j. Así

$$h(a, b) = 1 + 2 + \cdots + (i + j - 2) + j$$

Los primeros sumandos corresponden a las primeras diagonales y su suma representa todos los elementos de esas diagonales; el último sumando j, es la posición que ocupa (a, b) en su diagonal.

——- DIBUJO ———

$\mathbb{Q}$ es numerable

Los números racionales tienen numerador y denominador; el numerador es un entero cualquiera y el denominador puede elegirse natural. Un mismo racional puede expresarse usando distintos pares numerador / denominador. Es decir, los racionales se pueden ver como un subconjunto del producto cartesiano de enteros por naturales:

$$\mathbb{Q} \subseteq \mathbb{Z} \times \mathbb{N}$$

Como $\mathbb{Z}$ y $\mathbb{N}$ son numerables, $\mathbb{Z} \times \mathbb{N}$ es numerable. Además como $\mathbb{Q}$ contiene a $\mathbb{N}$, podemos ver a $\mathbb{Q}$ como conjunto intermedio entre dos numerables y por lo tanto resulta que $\mathbb{Q}$ es numerable.

El dibujo muestra, a modo de ejemplo, como se pueden numerar los racionales positivos.

—— DIBUJO ——

3.4. Ejercicios y problemas

Ejercicios

Ejercicio 3.1. Definir 2 funciones distintas con dominio $A = \{x, y, z\}$ y codominio $B = \{11, 12, 13, 14, 15\}$.

Ejercicio 3.2. Sea $f : \mathbb{N} \to \mathbb{Z}$ definida por $f(n) = 9 - n^2$.

(1) Calcular la imagen por f de los primeros 10 naturales.

(2) Determinar la preimagen por f del conjunto $\{-5, -4, \ldots, 0, 1, \ldots 5\}$.

(3) ¿Es f suryectiva?

Ejercicio 3.3. Sean a_n y b_n las sucesiones dadas por $a_n = n + (-1)^n$ y $b_n = 2n + 1$.

(1) Hacer un dibujo de ambas sucesiones en un mismo gráfico.

(2) Decir si son inyectivas o suryectivas.

(3) Calcular las composiciones $a_n \circ b_n$ y $b_n \circ a_n$.

(4) Evaluar las composiciones anteriores para $n = 1 \ldots 25$.

Ejercicio 3.4. Considerar la función L que a una palabra le asigna la primera letra del abecedario que aparece en esa palabra. Por ejemplo, $L(\text{oblongo}) = \text{b}$, $L(\text{trompo}) = \text{m}$ y $L(\text{fin}) = \text{f}$.

(1) Elegir un conjunto A de palabras tales que la imagen de A por L sea el conjunto de las vocales.

(2) Elegir un conjunto A de 8 palabras tales que la imagen de A por L sea el conjunto de las vocales.

(3) ¿Puede exhibir una palabra p tal que $L(p) =$ u?

(4) Encuentre 3 verduras tales que sus nombres no sean asignados por L todos a la letra a.

Ejercicio 3.5. ¿Cuántos multiplos de 3 hay entre 7 y 37?. Si la respuesta es n, exhibir explícitamente una biyección entre $[\![1, n]\!]$ y este conjunto. ¿Podría dar una segunda biyección distinta de la anterior?

Ejercicio 3.6. Sean $A = \{a, b, c, \ldots, k\}$ y $B = \{F_1, F_2, \ldots, F_7\}$. Definir en cada caso funciones $f : A \to B$ y $g : B \to A$ tales que:

(a) $f \circ g$ sea sobreyectiva.

(b) La imagen de $g \circ f$ tenga 7 elementos.

(c) La imagen de g tenga 3 elementos, la imagen de f tenga 5 elementos y la imagen de $g \circ f$ sea igual a la imagen de g.

(d) g sea inyectiva y la preimagen de $\{a, b, c\}$ por $g \circ f$ sea el conjunto $\{h, k\}$.

Problemas

Problema 3.7. Definir funciones $f : \mathbb{Z} \to \mathbb{N}$ satisfaciendo las siguientes condiciones:

(1) Suryectiva y no inyectiva.

(2) Inyectiva y no suryectiva.

(3) Inyectiva y $Im(f) = \{n \in \mathbb{N} : \ n \geq 10\}$.

(4) Suryectiva y tal que la preimagen de cualquier natural par tenga dos elementos.

Problema 3.8. Sea $f : \mathbb{Z} \to \mathbb{N}_0$ la función valor absoluto.

(1) ¿Existe $g : \mathbb{N}_0 \to \mathbb{Z}$ tal que $f \circ g = Id$?

(2) ¿Existe $g : \mathbb{N}_0 \to \mathbb{Z}$ tal que $g \circ f = Id$?

(3) Si $F(m) = f(m + 21)$, ¿existe $g : \mathbb{N}_0 \to \mathbb{Z}$ tal que $F \circ g = Id$?

Problema 3.9. Definir una función $f : \mathbb{N} \to \mathbb{N}$ tal que para todo $n \in \mathbb{N}$ la preimagen por f del singulete $\{n\}$ tenga cardinal n. Es decir, tal que el natural n sea alcanzado n veces.

Problema 3.10.

Parte II

Números y aritmética

En esta parte estudiaremos varios conjuntos de números y su aritmética. Estudiaremos los naturales, los enteros, los racionales o fraccionarios, los números reales y los números complejos.

Exploramos las propiedades de estos conjuntos de números y los fundamentos de su aritmética, por un lado con el objetivo de poder calcular con ellos de manera segura y así poderlos usar como herramientas para resolver problemas, y por otro lado para abstraer estructuras subyacentes que luego aparecen en otros conjuntos numéricos de la matemática.

Comenzaremos estudiando los números reales, y no por ejemplo los naturales a pesar de ser más simples, pues tienen una estructura más rica y sofisticada.

En nuestro estudio nos concentraremos en explicar y comprender cómo se comportan y en entender aspectos estructurales más que en intentar explicar qué son.

Adoptaremos dos puntos vista que convivirán en paralelo en la exposición y que se enriquecen el uno al otro.

(1) Punto de vista PRAGMÁTICO. Aceptando que conocemos los números naturales, los enteros, los racionales y los reales con sus operaciones de suma y producto y el orden usual, estudiamos sus propiedades y su aritmética a partir de un conjunto pequeño de propiedades que llamamos *básicas*.

(2) Punto de vista AXIOMÁTICO. Trabajamos sobre un conjunto abstracto con una suma, un producto y un orden, que podría ser otro que el de los números reales, asumiendo que satisfacen ciertas propiedades que llamamos *axiomas*. Desde este punto de vista no nos interesa la naturaleza de los elementos del conjunto estuadiado.

Vale la pena decir que cuando estudiamos un objeto concreto desde un punto de vista pragmático, lo que aprendemos se refiere a ese objeto. Mientras que si estudiamos ese mismo objeto desde un punto de vista axiómatico, abstrayendo sus propiedades fundamentales, lo que aprendemos es también válido para cualquier otro objeto con esas mismas propiedades.

Muchas veces la naturaleza de los objetos estudiados y el conocimiento que tengamos de ellos contribuye significativamente a descubrir verdades sobre ellos. Otras, el abstraer algunas de sus propiedades prescindidendo de su naturaleza permite ver con mayor claridad las verdades que los rigen. La experiencia muestra que la combinación de estos dos puntos de vistas facilita y enriquece el conocimiento matemático.

Capítulo 4

Números reales y su aritmética

4.1. Conjuntos numéricos

Denotaremos con $\mathbb{R}$ al conjunto de números reales. A los subconjuntos de racionales, enteros y naturales los denotaremos respectivamente $\mathbb{Q}$, $\mathbb{Z}$ y $\mathbb{N}$. Sabemos que

$$\mathbb{N} \subsetneq \mathbb{Z} \subsetneq \mathbb{Q} \subsetneq \mathbb{R} \tag{4.1}$$

y recordamos que:

$$\begin{aligned} \mathbb{N} &= \{1, 2, 3, \ldots\} \\ \mathbb{Z} &= \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\} \\ \mathbb{Q} &= \left\{ \frac{a}{b} : a, b \in \mathbb{Z}, b \neq 0 \right\} \end{aligned} \tag{4.2}$$

Éstos no son los únicos subconjuntos interesantes de números reales que hay, ni los únicos que se consideran y resultan útiles a la matemática. Entre $\mathbb{Q}$ y $\mathbb{R}$ hay una enorme variedad de conjuntos con propiedades aritméticas muy similares a las de $\mathbb{Q}$ y $\mathbb{R}$. Uno de éstos es

$$\mathbb{Q}(\sqrt{2}) = \{a + \sqrt{2}\, b : a, b \in \mathbb{Q}\} \tag{4.3}$$

donde $\sqrt{2}$ es la raíz cuadrada de 2 (el único real positivo que al cuadrado es igual a 2).

Nota. Otros subconjuntos de números que aparecen naturalmente en la matemática son, por ejemplo, los números irracionales y los números primos.

- Los irracionales son por definición el complemento del conjunto de racionales (al que denotamos $\mathbb{Q}^c$), es decir aquellos números que no pueden escribirse como cociente de dos enteros. Luego

  $$\mathbb{R} = \mathbb{Q} \cup \mathbb{Q}^c$$

  (donde la unión es disjunta) y un número real cualquiera es racional o irracional, pero nunca ambas cosas a la vez. Por ejemplo, los números $\sqrt{2}$ usado en (4.3) y π son números irracional, luego no pueden escribirse como cociente de dos enteros. Ahora, $7/3$ es cociente de dos enteros, luego es un número racional y por lo tanto no es irracional.

- Un número natural, distinto de 1, es primo si sus únicos divisores positivos son él mismo y 1. Por ejemplo, 3 es primo pues sus únicos divisores positivos son 3 y 1, mientras que 10 no es pirmo pues entre sus divisores positivos está el 5, que es distinto de 1 y distinto de 10. Notamos que el 1 no es primo. Es común denotar por $\mathbb{P}$ al conjunto de números primos.

A diferencia de los otros conjuntos de números mencionados, $\mathbb{Q}^c$ y $\mathbb{P}$ no son cerrados por la suma y el producto de números reales. Es decir, suma y producto de irracionales (resp. primos) no es necesariamente irracional (resp. primo). Por ejemplo, π y $3-\pi$ son irracionales, pero su suma $\pi + (3-\pi) = 3$ no es irracional (es racional). Además π y $\frac{2}{\pi}$ son irracionales, pero su producto $\pi \cdot \frac{2}{\pi} = 2$ no es irracional (es racional). Para el caso de los primos tenemos por ejemplo que $5 + 7 = 12$, donde 5 y 7 son primos, pero su suma no lo es, y su producto tampoco. (Encontrar ejemplos de dos primos que multiplicados no den un primo, debería ser muy fácil. ¿Porqué?) Por lo tanto, estos conjuntos no tienen una estructura aritmética como los otros.

Vale aclarar que hemos mostrado que la suma y el producto no son cerrados ni para los irracionales ni para los primo. Sin embargo, esto no implica que la suma o el producto de dos irracionales sea **siempre** racional. De hecho, $\sqrt{2} + \sqrt{2} = 2\sqrt{2}$ y $\sqrt{2}\sqrt{3} = \sqrt{6}$ son irracionales. Tampoco es cierto que la suma de dos primos nunca sea un primo, por ejemplo $2 + 3 = 5$. (Ya nos referimos con una pregunta a la situación con el producto de dos primos.)

En este capítulo estudiamos las propiedades aritméticas de los números reales combinando dos puntos de vista, uno PRAGMÁTICO y uno AXIOMÁTICO.

Aceptamos que los números reales existen y son como los conocemos. Reconocemos sus propiedades básicas, como por ejemplo que la suma y el producto son asociativos y conmutativos, o que el 0 es elemento neutro para la suma y el 1 es identidad para el producto.

Desde lo axiomático, planteamos estas propiedades observadas como *axiomas* para un conjunto de números abstracto que no conocemos. Estos axiomas son las propiedades exigidas o deseadas para ese conjunto de números (quizá inexistente).

Todas las verdades que enunciemos y probemos sobre la aritmética de los números reales, se seguirán del conjunto de propiedades básicas observadas (punto de vista prágmatico) o axiomas (punto de vista axiomático) y no dependerán de la naturaleza de los números reales. Es por esto que estas verdades de los números reales serán también verdades de la aritmética de todos los conjuntos de números que satisfagan esos axiomas, es decir que los tengan como propiedades. Esto no es un hecho menor, ya que muchas verdades se siguen de un conjunto pequeño de propiedades o axiomas y hay muchos conjuntos de números, muy distintos, que las comparten.

Por ejemplo, las propiedades básicas de la suma y el producto de números reales son compartidas por los números racionales y los complejos, y también por ciertos conjuntos finitos de números, entre muchos otros. Por lo tanto, todas las propiedades y verdades de los reales que se prueban usando solamente las propiedades de la suma y el producto valen también para los racionales, los complejos y para todos los conjuntos de números que satisfacen los axiomas de la suma y el producto de los reales.

Cuantos más axiomas se exigen, menor es la cantidad de conjuntos de números que los satisfacen a todos. Por ejemplo, si a los axiomas de suma y producto de los reales agregamos los axiomas de orden de los reales, los números complejos se quedan afuera, pues no satisfacen esos axiomas de orden. Si agregamos el axioma de completitud (y no los de orden), los racionales se quedan afuera, y los complejos adentro.

Es importante mencionar que hay una lista de axiomas que los números reales satisfacen, que hace que todos los conjuntos que se pudieran construir con esas propiedades resultarán todos *equivalentes* entre sí y equivalentes al conjunto de números reales. Es decir, esta lista caracteriza a los números reales y por esto se la conoce como "axiomas de los números reales".

4.1.1. Sobre la construcción de los números reales

¿Qué son los números reales? En este momento no es importante contestar esta pregunta, ya que estamos aceptando que los números reales existen y que los conocemos. Queremos aprender a calcular y a trabajar con ellos, por lo cual no interesa tanto su naturaleza, sino cómo se comportan. Sin embargo vamos a decir dos palabras sobre su naturaleza.

Los números reales pueden construirse de distintas maneras. A cada realización concreta que se construye se lo llama *modelo* de lo números reales. Cuando cada uno de nosotros piensa en los números reales, piensa en algún modelo particular que le resulta comprensible o le es familiar. Algunos piensan al conjunto de números reales como una recta e interpretan a las operaciones de suma y producto y al orden en ese contexto. Otros, prefieren ver a los números reales "escritos" en notación decimal, con coma y hasta infinitos dígitos a la derecha y así realizados entienden la suma y el producto y comprenden cuándo un número es mayor que otro.

Varias de las construcciones más conocidas se realizan a partir de los números racionales; como por ejemplo la construcción por *cortaduras de Dedekind* o la *completación de Cantor*. Otras construcciones conocidas son la *geométrica* (sobre la recta) y la de las *expansiones decimales*, ya mencionadas antes.

En todos los casos, no sólo se construyen los "números", sino que también se definen las operaciones de suma y producto, como así también el orden.

Para nuestros fines, es útil pensar a los reales como el último eslabón de una serie de construcciones que empieza con los naturales con la suma y el producto que aprendemos después de aprender a contar y con la noción de mayor usual, que luego sigue con los enteros, con los racionales y finalmente termina con los reales (ver (4.1)). En cada paso se extienden las operaciones de suma y producto del paso anterior y se extiende el orden. Los primeros pasos resultan intuitivos, aunque requieren de cierto formalismo y detalles técnicos. El último paso es más profundo y requiere una abstracción considerablemente mayor además de un formalismo complejo.

La construcción descripta se basa en la existencia de los números naturales, que aceptamos sin cuestionamientos. De todos modos vale la pena decir que también es posible construir los naturales, usando la teoría de conjuntos. En este caso, los "axiomas de los números naturales" son los *Axiomas de Peano*.

Las construcciones explícitas de los números y las pruebas formales de las propiedades pertenecen a los fundamentos de la matemática y escapan al alcance de este libro.

4.1.2. La suma, el producto y el orden de los números reales

Una *operación binaria* en un conjunto A, es una función del producto cartesiano $A \times A$ en A. En el conjunto $\mathbb{R}$ de números reales hay definidas dos operaciones binarias, una *suma* y un *producto*.

$$+ : \mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R}, \qquad \cdot : \mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R}$$

donde "$+$" denota a la suma y "$\cdot$" al producto.

Como ya dijimos, estas operaciones extienden las correspondientres de los números racionales. En particular, la suma y el producto de dos números racionales es siempre racional. En términos de funciones, esto se expresa diciendo que la restricción de la suma y el producto a $\mathbb{Q}$ son la suma y el producto definido en $\mathbb{Q}$. Lo mismo ocurre con las restricciones a $\mathbb{Z}$ y a $\mathbb{N}$. En símbolos,

$$\begin{aligned} +_{|\mathbb{Q}\times\mathbb{Q}} &: \mathbb{Q} \times \mathbb{Q} \longrightarrow \mathbb{Q} & \cdot_{|\mathbb{Q}\times\mathbb{Q}} &: \mathbb{Q} \times \mathbb{Q} \longrightarrow \mathbb{Q} \\ +_{|\mathbb{Z}\times\mathbb{Z}} &: \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z} & \cdot_{|\mathbb{Z}\times\mathbb{Z}} &: \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z} \\ +_{|\mathbb{N}\times\mathbb{N}} &: \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N} & \cdot_{|\mathbb{N}\times\mathbb{N}} &: \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N} \end{aligned}$$

Notación (para la suma y el producto)**.** Para indicar la suma de dos números a y b, siendo "$+$" el nombre de la función suma, deberíamos escribir $+(a, b)$. En su lugar escribimos $a + b$. Análogamente para indicar el producto de dos números a y b, siendo "$\cdot$" el nombre de la función producto, deberíamos escribir $\cdot(a, b)$. En su lugar escribimos $a \cdot b$. Es usual escribir también $a \times b$ o simplemente ab en vez de $a \cdot b$.

Observación. Notamos que si $a = b$, entonces los pares ordenados (x, a) y (x, b) son iguales y luego las funciones suma y producto valen lo mismo evaluadas en (x, a) y (x, b). Es decir, $x + a = x + b$ y $x \cdot a = x \cdot b$. En resumen, tenemos

$$a = b \quad \Rightarrow \quad (x, a) = (x, b) \quad \Rightarrow \quad \begin{cases} x + a = x + b \\ x \cdot a = x \cdot b \end{cases}$$

para todo $x \in \mathbb{R}$.

El orden de los números reales, dado por la relación "es menor que" denotada por $<$, es una estructura adicional que junto con las operaciones de suma y producto hacen de los números reales un ambiente muy interesante para hacer matemática, con una aritmética muy rica. Los subconjuntos de racionales, enteros y naturales también están ordenados por el mismo orden que los reales.

Nota. La relación "es menor que" de los reales ($<$) no es una relación de orden en el sentido de la Sección 3.1.2; en cambio la relación "es menor o igual que" ($\leq$) sí lo es.

4.2. Los axiomas de los números reales

En esta sección presentamos la lista completa de axiomas que caracterizan a los números reales. Todos salvo quizá el de completitud, son propiedades básicas bien conocidas de los números reales.

A partir de estas propiedades deduciremos de manera ordenada y rigurosa otras muchas propiedades aritméticas de $\mathbb{R}$. Esto ayudará a entender mejor y con fundamentos sólidos a los números reales y servirá de base para luego entender la aritmética de otros conjuntos de números.

Presentamos los axiomas que caracterizan a los números reales divididos en tres grupos, como axiomas para un conjunto de números R con una suma '$+$', un producto '$\cdot$' y un orden '$<$' dados [*]. En el primer grupo están los axiomas que caracterizan a un *cuerpo*; estos axiomas se refieren exclusivamente a las operaciones de suma y producto. Luego aparecen en un segundo grupo los axiomas que combinados con los anteriores caracterizan a un *cuerpo ordenado*. Finalmente aparece un último axioma, el de completitud, que en este caso está enunciado en términos del orden $<$ presente en R y que junto con todos los anteriores caracteriza a un *cuerpo ordenado completo*. Resulta que hay un único cuerpo ordenado completo: $\mathbb{R}$.

Una vez introducidos todos estos axiomas hacemos algunas observaciones sobre sus enunciados y comenzamos a deducir sistemáticamente otras propiedades aritméticas de cualquier cuerpo y de cualquier cuerpo ordenado.

Axiomas de cuerpo

I. De la suma

- *Asociatividad:* $(x + y) + z = x + (y + z)$ para todo $x, y, z \in R$.
- *Conmutatividad:* $x + y = y + x$ para todo $x, y \in R$.
- *Existencia de neutro*[**]*:* existe un $a \in R$ tal que $a + x = x$ para todo $x \in R$.
- *Existencia de opuesto:* para todo $x \in R$ existe un $x' \in \mathbb{R}$ tal que $x + x' = a$.

II. Del producto

- *Asociatividad:* $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ para todo $x, y, z \in R$.
- *Conmutatividad:* $x \cdot y = y \cdot x$ para todo $x, y \in R$.
- *Existencia de identidad*[***]*:* existe un $b \in R$ tal que $b \cdot x = x$ para todo $x \in R$.
- *Existencia de inverso:* para todo $x \in R$, $x \neq a$, existe $x' \in \mathbb{R}$ tal que $x \cdot x' = b$.

III. De compatibilidad de la suma con el producto

- *Distributividad:* $x \cdot (y + z) = x \cdot y + x \cdot z$ para todo $x, y, z \in R$.

Axiomas de cuerpo ordenado

IV. Del orden

[*] Este R no es a priori el de números reales. Con todos los axiomas exigidos podría no existir ninguno.

- *Tricotomía:* para todo $x, y \in R$ se tiene una y sólo una de las siguientes:

$$x < y, \qquad x = y \qquad \text{ó} \qquad y < x$$

- *Transitividad:* para todo $x, y, z \in R$ si $x < y$ e $y < z$, entonces $x < z$. Es decir

$$x < y \quad \wedge \quad y < z \qquad \Rightarrow \qquad x < z$$

V. De compatibilidad del orden con la suma y el producto

- *Consistencia con la suma:* si $x < y$, entonces

$$x + z < y + z \text{ para todo } z \in R.$$

- *Consistencia con el producto:* si $x < y$, entonces

$$c \cdot x < c \cdot y \text{ para todo } c > a.$$

Axiomas de cuerpo ordenado completo

VI. De completitud

- Todo subconjunto acotado superiormente, tiene una cota superior mínima.

Observación. Un conjunto $A \subseteq R$ es acotado superiormente si existe un $M \in R$ tal que para todo $x \in A$ se tiene que $x \leq M$. Un tal M es una cota superior; en general si A es acotado superiormente hay muchas cotas superiores distintas. Una cota superior mínima, en una cota superior M tal que si N es otra cota superior, entonces $M \leq N$.

Nota. En este libro no haremos uso ni nos referiremos de ahora en más a la completitud. Sin emabargo queremos decir que el axioma de completitud puede enunciarse en otros términos sin recurrir al orden. Por ejemplo, usando un valor absoluto o una distancia. Así los números complejos resultan un cuerpo completo aunque no ordenado.

En diferentes textos estos axiomas pueden aparecer con enunciados ligeramente distintos. Por ejemplo, a veces además de la existencia de un elemento neutro y de la existencia de una identidad exigen también unicidad. O también se exige que la identidad sea distinta del elemento neutro. Las siguientes observaciones muestran que estas cosas se siguen de los axiomas tal como los enunciamos. Además también muestran cómo otras propiedades báscias se siguen directamente de ellos.

[**] De los axiomas precedentes para la suma se sigue que si existe un neutro, es único, como lo veremos en seguida. Esto da sentido a los axiomas que siguen e involucran a a.

[***] De los axiomas precedentes para el producto se sigue que si existe una identidad, es única, como lo veremos en seguida. Esto da sentido a los axiomas que siguen e involucran a b.

Observaciones. De los axiomas se deducen los siguientes hechos básicos.

(1) UNICIDAD DEL NEUTRO.

Existe un único elemento neutro para la suma: si a y a' son elementos neutros, entonces $a = a + a'$ y $a' = a' + a$; luego $a = a + a' = a' + a = a'$, es decir $a = a'$.

(2) UNICIDAD DE LA IDENTIDAD.

Existe una única identidad para el producto: si b y b' son identidades, entonces $b = b \cdot b'$ y $b' = b' \cdot b$; luego $b = b \cdot b' = b' \cdot b = b'$, es decir $b = b'$.

Notación. Siendo los elementos neutro e identidad únicos, los llamaremos 0 y 1 respectivamente. Luego, para todo $x \in R$ valen

$$x + 0 = x = 0 + x \qquad \text{y} \qquad x \cdot 1 = x = 1 \cdot x$$

(3) $0 + 0 = 0$.

Si para todo $x \in R$ se tiene que $x + 0 = x$, en particular si $x = 0$ resulta que $0 + 0 = 0$.

(4) $1 \cdot 1 = 1$.

Si para todo $x \in R$ se tiene que $1 \cdot x = x$, en particular si $x = 1$ resulta que $1 \cdot 1 = 1$.

(5) UNICIDAD DEL OPUESTO.

Si x' y x'' son opuestos de x, entonces como $x + x' = 0$ y $x + x'' = 0$, tenemos que $x + x' = x + x''$. Sumando a ambos miembros un opuesto de x, por ejemplo x', podemos deducir que $x' = x''$:

$$\begin{aligned} x + x' = x + x'' &\Rightarrow x' + (x + x') = x' + (x + x'') \\ &\Rightarrow (x' + x) + x' = (x' + x) + x'' \\ &\Rightarrow 0 + x' = 0 + x'' \\ &\Rightarrow x' = x''. \end{aligned}$$

(6) UNICIDAD DEL INVERSO.

Si x' y x'' son inversos de x, entonces, como $x \cdot x' = 1$ y $x \cdot x'' = 1$, tenemos que $x \cdot x' = x \cdot x''$. Multiplicando a ambos miembros por un inverso de x, por ejemplo x', podemos deducir que $x' = x''$:

$$\begin{aligned} x \cdot x' = x \cdot x'' &\Rightarrow x' \cdot (x \cdot x') = x' \cdot (x \cdot x'') \\ &\Rightarrow (x' \cdot x) \cdot x' = (x' \cdot x) \cdot x'' \\ &\Rightarrow 1 \cdot x' = 1 \cdot x'' \\ &\Rightarrow x' = x''. \end{aligned}$$

Notación. Siendo el opuesto de x único, lo llamamos $-x$ y siendo el inverso de x (si $x \neq 0$) también único, lo llamamos x^{-1}. Luego, para todo $x \in R$ valen

$$x + (-x) = 0 = (-x) + x \qquad \text{y} \qquad x x^{-1} = 1 = x^{-1} x$$

Para el inverso a veces también se usa la notación fraccionaria $\frac{1}{x}$ ó $1/x$. Es decir, por convención tenemos que

$$x^{-1} = \frac{1}{x} = 1/x$$

(7) $-0 = 0$.

El opuesto de 0 es -0 y éste es igual a 0; es decir $-0 = 0$. En efecto, como $0 + 0 = 0$, se sigue que 0 es un opuesto de 0; por unicidad del opuesto debe ser $0 = -0$.

(8) $1^{-1} = 1$.

El inverso de 1 es 1^{-1} y éste es igual a 1; es decir $1^{-1} = 1$. En efecto, como $1 \cdot 1 = 1$, se sigue que 1 es un inverso de 1; por unicidad del inverso debe ser $1^{-1} = 1$.

(9) $1 \neq 0$ (si R tiene al menos 2 elementos).

La Proposición 4.1, que probaremos más abajo, establece que $x \cdot 0 = 0$ para todo $x \in \mathbb{R}$. De esto se sigue que el neutro y la identidad son distintos, es decir que $1 \neq 0$. En efecto, si $1 = 0$ y $x \in R$ cualquiera, entonces $x = x \cdot 1 = x \cdot 0 = 0$ y luego $x = 0$. Es decir, todos los elementos de R son iguales a 0 o dicho de otro modo, el único elemento de R es 0. Luego, si el conjunto R considerado tiene al menos dos elementos, entonces $1 \neq 0$.

Nota. En virtud de la última observación, de ahora en más, siempre que consideremos un cuerpo R asumiremos que tiene por lo menos 2 elementos.

Sobre los puntos de vista axiomático y pragmático

Existe un único cuerpo, ordenado y completo: $\mathbb{R}$.

Ya dijimos esto. Dado que es así, ¿porqué trabajar entonces axiomáticamente y no directamente en $\mathbb{R}$ de manera pragmática? Un aspecto muy importante del trabajo axiomático es que, todo lo que probemos usando ciertos axiomas será también válido para cualquier conjunto de números que satisfaga estos axiomas, es decir que entre sus propiedades estén las descriptas por esos axiomas. La realidad es que hay muchísimos conjuntos de números y muchísimos otros conjuntos formados por otros objetos matemáticos que satisfacen sólo algunos de todos estos axiomas. El trabajo axiomático abstrae y nos permite concentrar en las estructuras subyacentes que comparten ciertos objetos matemáticos y demostrar sus verdades de manera unificada.

Los siguientes son ejemplos de distintos conjuntos de números que satisfacen algunos de los axiomas enunciados, pero no necesariamente todos.

Ejemplos.

(1) Los enteros, $\mathbb{Z}$, satisfacen los Axiomas I–III, salvo la existencia de inversos para el producto. En efecto, solo ± 1 son inversibles en $\mathbb{Z}$. Por ejemplo, el 2 no tiene inverso en $\mathbb{Z}$ ya que no existe ningún $a \in \mathbb{Z}$ que cumpla $2a = 1$. Decimos entonces que $\mathbb{Z}$ es un *anillo* (conmutativo con unidad). Además, los enteros están ordenados con $<$ y satisfacen los Axiomas IV–V.

(2) Los racionales, $\mathbb{Q}$, satisfacen todos los Axiomas I–V. Es así que $\mathbb{Q}$ es otro *cuerpo ordenado*, distinto de $\mathbb{R}$. Por otra parte, $\mathbb{Q}$ no satisface el Axioma VI, por lo cual $\mathbb{Q}$ *no es completo*. Por ejemplo, el conjunto $\{x \in \mathbb{Q} : x < \sqrt{2}\} \subset \mathbb{Q}$ es acotado superiormente por (el racional) $1,42 = 142/10$, pero no tiene una cota superior mínima en $\mathbb{Q}$.

(3) Sea $\mathbb{C} = \{a + bi : a, b \in \mathbb{R}\}$ el conjunto de números complejos, que estudiaremos más adelante en el Capítulo 7, donde $i \notin \mathbb{R}$ con $i^2 = -1$. El conjunto $\mathbb{C}$ no tiene (ni puede tener) un orden compatible con su suma y su producto (ver §4.6). Sin embargo si satisface los Axiomas I, II, III, V y VI (aunque enunciado de otra forma). Por esto $\mathbb{C}$ es un cuerpo completo (no ordenado).

(4) Más adelante en el libro se presentan ciertos conjuntos finitos de números, denotados $\mathbb{Z}_p$, que satisfacen los Axiomas I–III para cada p primo (ver Capítulo 9). Éstos son ejemplos de *cuerpos finitos*. El más sencillo de tales cuerpos tiene sólo 2 elementos: $\mathbb{Z}_2 = \{0, 1\}$. El 0 es el neutro de la suma y el 1 la identidad del producto que están definidos por:

$$0 + 0 = 0, \quad 0 + 1 = 1 + 0 = 1, \quad 1 + 1 = 0 \quad \text{(la novedad!)}$$

$$0 \cdot 0 = 0, \quad 0 \cdot 1 = 1 \cdot 0 = 0, \quad 1 \cdot 1 = 1$$

Es muy fácil chequear que $\mathbb{Z}_2$ satisface todos los Axiomas I–III. ◊

Ejemplo †. El que sigue es quizá un ejemplo un poco más novedoso aún.

El conjunto $\mathbb{Q}(\sqrt{2})$ definido en (4.3), con las operaciones de $\mathbb{R}$, i.e.

$$(a + b\sqrt{2}) + (a' + b'\sqrt{2}) = (a + a') + (b + b')\sqrt{2},$$
$$(a + b\sqrt{2})(a' + b'\sqrt{2}) = (aa' + 2bb') + (ab' + a'b)\sqrt{2},$$

satisface todos los Axiomas I-III. Notar que $\mathbb{Q} \subsetneq \mathbb{Q}(\sqrt{2})$ ya que $\sqrt{2} \notin \mathbb{Q}$. Es claro que el neutro y la identidad son

$$0 = 0 + 0\sqrt{2} \qquad \text{y} \qquad 1 = 1 + 0\sqrt{2}$$

es decir el $0, 1$ de $\mathbb{R}$ pertenecen a $\mathbb{Q}(\sqrt{2})$ y también son el neutro y la identidad allí. Dejamos al lector reflexionar sobre el porqué las operaciones de suma y producto así definidas son asociativas, conmutativas y el producto es distributivo respecto de la suma (Ayuda: todo esto se sigue por particularización). Además es claro que el opuesto de $x = a + b\sqrt{2}$ es

$$-x = -a + (-b)\sqrt{2}$$

Veamos que todo $x \neq 0$ tiene inverso. Sea $x = a+b\sqrt{2}$, con a o b distintos de 0. Buscamos un $x' = a' + b'\sqrt{2}$ tal que $xx' = 1$, es decir $(a + b\sqrt{2})(a' + b'\sqrt{2}) = 1$. O sea, queremos que se cumpla

$$aa' + 2bb' = 1 \qquad \text{y} \qquad ab' + a'b = 0.$$

¿Tiene este sistema solución? Un truquito que nos servirá ahora y más adelante es el siguiente. Definamos $\bar{x} = a - b\sqrt{2} = a + (-b)\sqrt{2}$. Notemos que

$$x \cdot \bar{x} = (a + b\sqrt{2})(a - b\sqrt{2}) = a^2 - 2b^2.$$

Observar que este número es no nulo, asumiendo que $x \neq 0$. En efecto, si $a^2 - 2b^2 = 0$ entonces $a^2 = 2b^2$ de donde $2 = (\frac{a}{b})^2$ y así $\sqrt{2} = \frac{a}{b}$. Absurdo, pues sabemos que $\sqrt{2}$ es irracional. Luego, podemos dividir por este número y tenemos

$$\frac{x\bar{x}}{a^2 - 2b^2} = x \cdot \frac{\bar{x}}{a^2 - 2b^2} = 1.$$

O sea, el segundo factor $\bar{x}/(a^2 - 2b^2)$ funciona como inverso del primero. Luego

$$x^{-1} = \frac{\bar{x}}{a^2 - 2b^2} = \frac{a}{a^2 - 2b^2} + \frac{(-b)}{a^2 - 2b^2}\sqrt{2} \in \mathbb{Q}(\sqrt{2}).$$

Así resulta que $\mathbb{Q}(\sqrt{2})$ es un cuerpo y se tiene que $\mathbb{Q} \subsetneq \mathbb{Q}(\sqrt{2}) \subsetneq \mathbb{R}$.

Notar que el conjunto

$$\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\} \subsetneq \mathbb{Q}(\sqrt{2})$$

satisface los Axiomas I-III, salvo que no es cierto que todo elemento no nulo tenga inverso. Luego, no es un cuerpo (sólo resulta anillo conmutativo con unidad). Este conjunto hace las veces de los enteros dentro del cuerpo $\mathbb{Q}(\sqrt{2})$.

En realidad, para cualquier $n \in \mathbb{N}$ podemos definir el cuerpo

$$\mathbb{Q}(\sqrt{n}) = \{a + b\sqrt{n} : a, b \in \mathbb{R}\}$$

con similares características a $\mathbb{Q}(\sqrt{2})$. Notemos que si n es un cuadrado, digamos $n = m^2$ entonces es claro que $\mathbb{Q}(\sqrt{n}) = \mathbb{Q}(m) = \mathbb{Q}$. Por ejemplo, $\mathbb{Q}(\sqrt{4}) = \mathbb{Q}$. Por lo tanto interesan aquellos casos en los que n no es un cuadrado. Estos son los llamados cuerpos cuadráticos. ◊

4.3. Algunas propiedades aritméticas de los números reales

De ahora en más trabajaremos con el conjunto de los números reales $\mathbb{R}$, como modelo de cuerpo o de cuerpo ordenado. Todo lo que demostremos será válido también para otros cuerpos o cuerpos ordenados ya que las demostraciones se basan en los Axiomas I–V. Muchos de los resultados que probaremos son propiedades de los reales bien conocidas. De ahora en más serán propiedades bien conocidas de todos los cuerpos o cuerpos ordenados según corresponda.

En este libro no usamos el Axioma VI de completitud. Sus consecuencias se estudian principalmente en *Análisis Matemático*. Sin embargo, recordamos que este axioma es muy fuerte, ya que distingue a $\mathbb{Q}$ de $\mathbb{R}$, por ejemplo.

Nota. La suma está definida para un par de números dados. Para "sumar 3 números x, y, z", debemos hacerlo en etapas y en algún orden. En el orden dado primero sumamos $x+y$ y luego sumamos z, es decir hacemos $(x+y)+z$. Dado que la suma es conmutativa y asociativa, el orden en que sean dados x, y, z no altera la suma final. En efecto

$$(x+y)+z = (y+x)+z = (x+z)+y = (z+x)+y = (y+z)+x = (z+y)+x$$

Por esto, convenimos en escribir $x+y+z$, sin paréntesis, para representar a la "suma de los 3 números x, y, z".

Análogamente convenimos en escrbir xyz para representar el "producto de los 3 números x, y, z".

La siguiente propiedad es llamada propiedad absorvente del 0.

Proposición 4.1. *Para todo número real x, vale $x0 = 0$.*

Demostración. Tenemos que $x0 = x(0+0) = x0 + x0$. Sumando a ambos miembros el opuesto de $x0$, tenemos obtenemos que

$$0 = -x0 + x0 = -x0 + (x0 + x0) = (-x0 + x0) + x0 = 0 + x0 = x0$$

como queríamos ver. □

Notamos que en la demostración de esta proposición solamente usamos los axiomas de la suma y la distributividad del producto. Usamos que $0+0=0$ y que $x0$ tiene opuesto. No usamos la existencia de inversos multiplicativos, no usamos el orden, ni mucho menos la completitud.

Observación. De la proposición anterior se sigue que el inverso de x, de un x no nulo, es también no nulo. En efecto, si $x^{-1} = 0$, entonces $1 = xx^{-1} = x0 = 0$ lo cual es absurdo. (Recordemos que no admitimos cuerpos de un único elemento y en este caso siempre $1 \neq 0$.)

El siguiente teorema establece cuatro propiedades fundamentales, de las cuales deduciremos directamente muchas de las propiedades aritméticas más familiares de los reales.

Teorema 4.2. *En el conjunto de los números reales valen las siguientes propiedades.*

(a) Propiedad cancelativa de la suma: si $x+y = x+z$, entonces $y = z$.

(b) Para todo par $x, y \in \mathbb{R}$, existe un único a tal que $x + a = y$.

(c) Propiedad cancelativa del producto: si $xy = xz$ y $x \neq 0$, entonces $y = z$.

(d) Para todo par $x, y \in \mathbb{R}$, con $x \neq 0$, existe un único a tal que $ax = y$.

Demostración.

(a) Se sigue sumando a ambos miembros el opuesto de x:

$$x+y = x+z \quad \Rightarrow \quad -x+x+y = -x+x+z \quad \Rightarrow \quad 0+y = 0+z \quad \Rightarrow \quad y = z$$

(b) Existencia: consideremos $a = y + (-x)$. Luego

$$x + a = x + (y + (-x)) = (x + (-x)) + y = 0 + y = y$$

Unicidad: supongamos que a y b son tales que $x + a = y$ y $x + b = y$. Se sigue entonces que $x + a = x + b$ y luego por (a) resulta que $a = b$.

(c) Se sigue multiplicando ambos miembros por el inverso de x (que existe pues $x \neq 0$):

$$xy = xz \quad \Rightarrow \quad x^{-1}xy = x^{-1}xz \quad \Rightarrow \quad 1y = 1z \quad \Rightarrow \quad y = z$$

(d) Existencia: consideremos $a = yx^{-1}$. Luego

$$ax = (yx^{-1})x = y(xx^{-1}) = y1 = y$$

Unicidad: supongamos que a y b son tales que $ax = y$ y $bx = y$. Se sigue entonces que $ax = bx$ y que $xa = xb$ y luego por (c) resulta que $a = b$.

La demostración está completa. □

La hipótesis $x \neq 0$ en las dos últimas propiedades del Teorema 4.2 es esencial. Si $x = 0$, ambas son falsas. Por ejemplo, $0 \cdot 2 = 0 \cdot 3$ y sin embargo $2 \neq 3$; no podemos cancelar el 0. Esto mismo dice que 2 y 3 son 2 soluciones distintas de la ecuación $0 \cdot a = 0$.

La unicidad de la solución de la ecuación $x + a = y$ implica en particular, tomando $y = 0$, la unicidad del opuesto de x. Y la unicidad de la solución de la ecuación $xa = y$ con $x \neq 0$ implica en particular, tomando $y = 1$, la unicidad del inverso.

Notación. Dados $x, y \in \mathbb{R}$, al número $x + (-y)$ se lo denota por simplicidad $x - y$ y se lo llama *resta* de x e y y se lee "x menos y". Además, si $y \neq 0$, al número xy^{-1} se lo denota también $\dfrac{x}{y}$ y se lo llama *cociente* de x e y y se lee "x sobre y".

Hacemos notar que la "resta" y el "cociente", a diferencia de la suma y el producto, no son operaciones que se restringen bien a los enteros o a los naturales. Más precisamente, si $n, m \in \mathbb{N}$, $n - m$ puede no estar en $\mathbb{N}$ y si $a, b \in \mathbb{Z}$, a/b puede no estar en $\mathbb{Z}$. Por ejemplo, $2 - 5 \notin \mathbb{N}$ y $\dfrac{2}{3} \notin \mathbb{Z}$.

El siguiente corolario resume varias propiedades de los opuestos y de los inversos.

Corolario 4.3. *En el conjunto de los números reales valen las siguientes propiedades:*

(a) $-(-x) = x$.

(b) $-(x + y) = (-x) + (-y)$.

(c) $-(xy) = (-x)y = x(-y)$.

(d) $(-1)x = -x$.

(e) $(-x)(-y) = xy$.

(f) $(x^{-1})^{-1} = x$.

(g) $(xy)^{-1} = x^{-1}y^{-1}$.

(h) $(-1)^{-1} = -1$.

(i) $(-x)^{-1} = -x^{-1}$.

Demostración. Todas estas propiedades se siguen de las unicidades de los puntos (b) y (d) del Teorema 4.2.

(a) Tanto $a = x$ como $a = -(-x)$ son ambos solución de la ecuación $-x + a = 0$. Luego son iguales.

(b) Tenemos que $(-x)+(-y)+(x+y) = (-x+x)+(-y+y) = 0$ (usando conmutatividad y asociatividad). Es decir $a = (-x) + (-y)$ satisface la ecuación $a + (x + y) = 0$, que también es satisfecha por $a = -(x + y)$. Luego son iguales.

(c) Tenemos que $(-x)y + xy = (-x + x)y = 0y = 0$ y análogamente que $x(-y) + xy = x(-y + y) = x0 = 0$. Luego $(-x)y$, $x(-y)$ y $-(xy)$ son todos opuestos de xy y son todos iguales.

(d) Como $x + (-1)x = 1x + (-1)x = (1 - 1)x = 0x = 0$, se sigue que $(-1)x$ es opuesto de x y así es igual a $-x$.

(e) Ambos xy y $(-x)(-y)$ son opuestos de $-(xy)$. En efecto $(-x)(-y)-(xy) = (-x)(-y)+(-x)y = (-x)(-y + y) = (-x)0 = 0$. Por lo tanto, son iguales.

(f) Como $x \cdot x^{-1} = 1$, se sigue que x es el inverso de x^{-1}. Es decir $x = (x^{-1})^{-1}$.

(g) Tenemos que $(xy)(x^{-1}y^{-1}) = xx^{-1}yy^{-1} = 1 \cdot 1 = 1$ (usando asociatividad y conmutatividad). Luego, por unicidad del inverso, $(xy)^{-1} = x^{-1}y^{-1}$.

(h) Como $(-1)(-1) = 1$ (ver (f)), se sigue que -1 es el inverso de -1, es decir $(-1)^{-1} = -1$.

(i) Como $-x^{-1}(-x) = x^{-1}x = 1$, se sigue que el inverso de $-x$ es $-x^{-1}$, como queríamos probar.

La demostración está completa. □

La siguiente es otra propiedad importante de los números reales, y es que el producto de números no nulos es no nulo.

Proposición 4.4. *Para todo par de números reales x e y vale que:*

$$xy = 0 \quad \Leftrightarrow \quad x = 0 \quad \acute{o} \quad y = 0$$

o equivalentemente

$$xy \neq 0 \quad \Leftrightarrow \quad x \neq 0 \quad e \quad y \neq 0$$

Demostración. Supongamos que $xy = 0$. Si $x = 0$, ya está. Supongamos entonces que $x \neq 0$. Multiplicando la igualdad $xy = 0$ por el inverso de x, obtenemos que $x^{-1}(xy) = x^{-1}0 = 0$. Siendo $x^{-1}(xy) = (x^{-1}x)y = 1y = y$, se sigue que $y = 0$. La recíproca se sigue de la Proposición 4.1. □

Dado $x \in \mathbb{R}$, al producto de un número x con sí mismo, $x \cdot x$, lo denotamos x^2 y lo llamamos el *cuadrado* de x.

Corolario 4.5. *Para todo $x \in \mathbb{R}$ vale que:*

(a) $x^2 = 0 \quad \Leftrightarrow \quad x = 0.$

(b) $x^2 = 1 \quad \Leftrightarrow \quad x = 1 \ \text{ó} \ x = -1.$

(c) $x^{-1} = x \quad \Leftrightarrow \quad x = 1 \ \text{ó} \ x = -1.$

Demostración. El item (a) se sigue directamente de la proposición anterior con $y = x$. Y en (b) y (c) las recíprocas ($\Leftarrow$) son obvias.

Para terminar de probar (b) supongamos que $x^2 = 1$. Luego $x^2 - 1 = 0$ y por la propiedad distributiva, tenemos que $x^2 - 1 = (x-1)(x+1) = 0$. Por la proposición anterior $x - 1 = 0$ ó $x + 1 = 0$, de donde se sigue que $x = 1$ ó $x = -1$, lo cual prueba (b).

Finalmente, si $x^{-1} = x$, multiplicando ambos miembros por x tenemos que $x^2 = 1$ y luego por (b) $x = 1$ ó $x = -1$, de donde sigue (c). □

Notar que los incisos (b) y (c) del corolario anterior son equivalentes, ya que podemos pasar de $x^2 = 1$ a $x^{-1} = x$ y viceversa, multiplicando por x^{-1} o por x, respectivamente. Como notación, es común escribir $x = \pm 1$ para abreviar $x = 1$ ó $x = -1$. Usaremos esto cuando sea conveniente.

Ya hemos probado varias propiedades aritméticas de los reales. Con éstas ya es posible contestar preguntas y resolver problemas como los que se plentean a continuación.

Es muy instructivo intentar resolver los siguientes problemas por uno mismo antes de mirar las soluciones.

Problemas.

(1) ¿Es cierto que si $a^2 = b^2$, entonces $a = b$?

(2) Si $a^2 = b^2$, ¿se sigue que $a^3 = b^3$?

(3) Resolver la ecuación $x^3 - 2x = 7x$.

(4) Calcular $-\big(-(\pi + \pi^{-1} - 1) + \frac{1-\pi}{\pi}\big)$.

(5) ¿Cuáles son todos los números reales x tales que $(x - a)^2 - 1 = 0$ para un a dado?

(6) Simplificar la expresión del número $\dfrac{a}{a-b} + \dfrac{b}{b-a}$.

(7) ¿Es $-(a - (-a + 1))$ inversible para todo a?

(8) ¿Es cierto que $x + x = x \Leftrightarrow x = 0$?

(9) ¿Cuántos pares distintos de números reales a y b hay tales que $(a+b)^2 = a^2 + b^2$? ¿Y para un a dado?

Soluciones.

(1) No. No es cierto, ya que por ejemplo $3^2 = 9 = (-3)^2$. Más generalmente sabemos (se sigue del Corolario 4.3) que para todo x, $(-x)^2 = x^2$, pero $-x \neq x$, salvo para $x = 0$.

(2) No. Por ejemplo, $3^2 = (-3)^2$, sin embargo $3^3 = 27$ y $(-3)^3 = -27$.

(3) Resolver esta ecuación significa decidir si tiene o no solución; y, en caso afirmativo, si es posible darlas a todas. Una solución es un número real a que satisface la ecuación, es decir tal que $a^3 - 2a = 7a$. (Por ejemplo, 2 no es solución ya que $2^3 - 2 \cdot 2 = 4$ y $7 \cdot 2 = 14$.) Podemos proceder como sigue.

$$x^3 - 2x = 7x \quad \Leftrightarrow \quad x^3 - 2x - 7x = 0 \quad \Leftrightarrow \quad x(x^2 - 9) = 0$$

Esto muestra que las soluciones de la ecuación que nos interesa son exactamente las mismas que las de la última ecuación. La proposición anterior implica que las soluciones de ésta son las soluciones de la ecuación $x = 0$ más las de la ecuación $x^2 - 9 = 0$. La primera, evidentemente, tiene una única solución: $x = 0$. La segunda ecuación es equivalente a la ecuación $x^2 = 9$. Sus soluciones son $x = 3$ y $x = -3$. Por lo tanto concluimos que la ecuación original tiene exactamente 3 soluciones: $0, 3$ y -3.

(4) Tenemos que

$$\begin{aligned} -\big(-(\pi + \pi^{-1} - 1) + \frac{1-\pi}{\pi}\big) &= (\pi + \pi^{-1} - 1) - (1-\pi)\pi^{-1} \\ &= \pi + \pi^{-1} - 1 - (\pi^{-1} - 1) \\ &= \pi + \pi^{-1} - 1 - \pi^{-1} + 1 \\ &= \pi \end{aligned}$$

(5) Dado a, $(x-a)^2 = 1$ si y sólo si $x - a = \pm 1$ (ver Corolario 4.5); es decir $x = a \pm 1$.

(6) Tenemos que

$$\begin{aligned} \frac{a}{a-b} + \frac{b}{b-a} &= a(a-b)^{-1} + b(b-a)^{-1} \\ &= a(a-b)^{-1} + b(-(a-b))^{-1} \\ &= a(a-b)^{-1} + b(-(a-b)^{-1}) \\ &= a(a-b)^{-1} - b(a-b)^{-1} \\ &= (a-b)(a-b)^{-1} \\ &= 1 \end{aligned}$$

(7) Tenemos que $-(a-(-a+1)) = -(a+a-1) = 1 - 2a$. Como $1 - 2a = 0$ si y sólo si $a = 1/2$ (ver Teorema 4.2), resulta que $-(a-(-a+1))$ es inversible para todo $a \neq 1/2$.

(8) Si es cierto. Si $x = 0$, entonces es obvio que $2x = 0 = x$. Si $x + x = x$, sumando $-x$ a ambos miembros resulta $x = 0$.

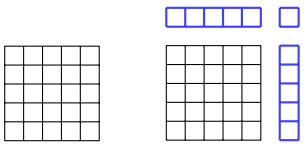
(9) Si tomamos $a = 0$, la identidad se satisface claramente para todo b. Luego hay infitios pares que la satisfacen. Si a es dado y $a \neq 0$, entonces como $(a+b)^2 = (a+b)(a+b) = a^2 + 2ab + b^2$ debe ser $2ab = 0$; siendo $a \neq 0$ debe ser $b = 0$. Por lo tanto para una a dado, $a \neq 0$ hay un único b, $b = 0$, tal que el par a, b satisface la identidad planteada. Luego, si $a, b \neq 0$, entonces $(a + b)^2 \neq a^2 + b^2$.

Problema.

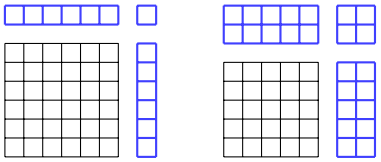
Supongamos que tenemos una cuadrícula o grilla, como un tablero de ajedrez, pero de tamaño $k \times k$, con $k \in \mathbb{N}$. ¿Cuántos cuadraditos más hacen falta para pasar a una grilla de $(k+1) \times (k+1)$ cuadraditos? ¿Y cuántos más para pasar a una de $(k+2) \times (k+2)$? Y en general, si $n > k$, ¿cuántos cuadraditos hay que agregar para pasar de una grilla $k \times k$ a una $n \times n$?

Solución.

Comencemos haciendo un caso particular, para que resulte más sencillo. Supongamos que $k = 5$, es decir, queremos ampliar la grilla de 5×5 cuadraditos a una de 6×6 y luego a una de 7×7. En el primer caso,



necesitamos $2 \cdot 5 + 1 = 11$ cuadraditos más. En el segundo caso, podemos hacerlo en dos etapas o en un solo paso



Se necesitan $(2 \cdot 5 + 1) + (2 \cdot 6 + 1) = 11 + 13 = 24$ cuadritos más (además de los 25 originales), si ampliamos en uno la grilla 6×6 o, equivalentemente, $2(2 \cdot 5) + 4 = 24$ si ampliamos en 2 la grilla 5×5 directamente.

Ahora atacamos el problema en el caso de un k cualquiera, haciendo uso de los diagramas anteriores. En el primer caso, para pasar de una grilla de $k \times k$ a una de $(k+1) \times (k+1)$ es claro que necesitamos agregar $k + 1 + k = 2k + 1$ cuadraditos.

En el segundo caso, para pasar a una grilla de $(k+2) \times (k+2)$, necesitamos $2k+1$ para la primer ampliación y $2(k + 1) + 1$ para la segunda. Luego, necesitamos

$$(2k + 1) + (2(k + 1) + 1) = 2k + 1 + 2k + 3 = 4k + 4 = 4(k + 1)$$

cuadraditos en total.

Análogamente, podríamos hacer una sola ampliación y en ese caso necesitamos

$$2(2k) + 4 = 4k + 4 = 4(k + 1),$$

cuadraditos, que corresponden a la descomposición de la derecha en el gráfico anterior.

Finalmente chequeamos que

$$(k + 1)^2 = k^2 + 2k + 1 \qquad \text{y que} \qquad (k + 2)^2 = k^2 + 4k + 4$$

Es decir, hemos deducido, a partir de los gráficos, las identidades $(k+1)^2 = k^2 + (2k+1)$ y $(k + 2)^2 = k^2 + (4k + 4)$, donde las expresiones entre paréntesis en la parte derecha de las igualdades representan lo que falta para pasar de un cuadrado a otro mas grande, en cada caso.

El caso general, i.e. pasar de una grilla $k \times k$ a una $n \times n$, resulta claro después de lo hecho. Hay que agregar

$$2k(n - k) + (n - k)^2 = (n - k)(2k + (n - k)) = (n - k)(n - k) = n^2 - k^2$$

cuadraditos. Es fácil chequear que $k^2 + 2k(n - k) + (n - k)^2 = n^2$. ◊

La siguiente proposición resume algunas identidades, del tipo de la aparecida en el problema anterior, que son útiles aprender a reconocer. Su demostración es directa y es un muy buen ejercicio desarrollarla completamente; hacerla ayuda a recordar estas identidades.

Notación. Al producto de x con sí mismo 3 veces xxx lo llamamos *cubo* de x y escribimos x^3. Es decir $x^3 = xxx$. Notemos además que $x^3 = x^2x$.

Proposición 4.6. *Para todo $x, y, z \in \mathbb{R}$ valen las siguientes expresiones:*

(a) $(x \pm y)^2 = x^2 \pm 2xy + y^2$.

(b) $(x \pm y)^3 = x^3 \pm 3x^2y + 3xy^2 \pm y^3$.

(c) $x^2 - y^2 = (x - y)(x + y)$.

(d) $x^3 - y^3 = (x - y)(x^2 + xy + y^2)$.

(e) $(x + y + z)^2 = x^2 + y^2 + z^2 + 2(xy + yz + xz)$.

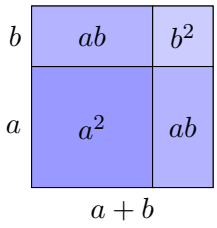
Demostración. En todos los casos, basta usar las definiciones de cuadrado o cubo según corresponda y las propiedades distributiva y asociativa. □

Algunas de estas identidades tienen nombres conocidos: (a) *cuadrado de un binomio*; (c) *diferencia de cuadrados* y (e) *cuadrado de un trinomio*.

Representaciones gráficas

Algunas de las identidades de arriba (como muchas otras) pueden ser interpretadas geométricamente de un modo sencillo pero bonito.

- Por ejemplo, el diagrama

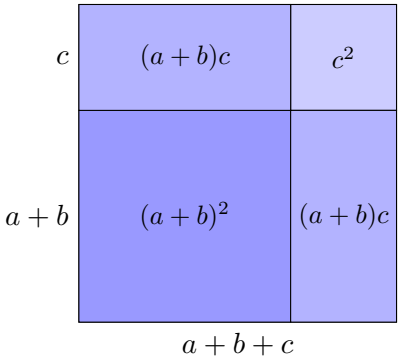


representa el cuadrado del binomio

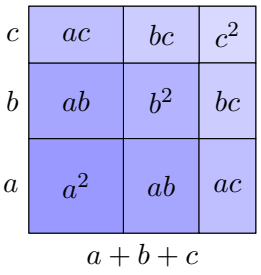
$$(a+b)^2 = a^2 + 2ab + b^2 = a^2 + b(2a+b),$$

pero también lo implica.

- Del mismo modo, el cuadrado de un trinomio se obtiene de



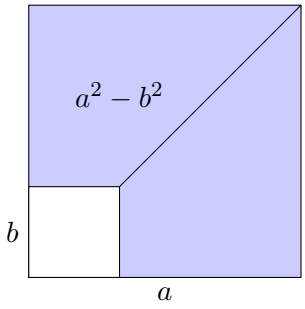
O sea,



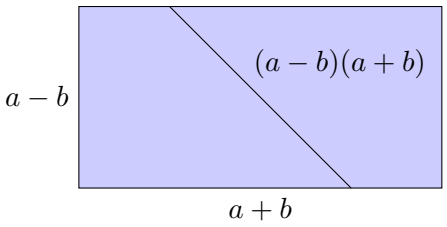
de donde se sigue que

$$(a+b+c)^2 = (a+b)^2 + 2(a+b)c + c^2 = a^2 + b^2 + c^2 + 2(ab+bc+ac).$$

- El caso de la diferencia de cuadrados es más interesante aún. Podemos suponer que $a > b$. En ese caso, consideramos un cuadrado de lado a, y dentro de éste uno mas pequeño de lado b en una esquina, más la diagonal uniendo los vértices de ambos cuadrados.



El área sombreada es $a^2 - b^2$. Notar que con los 2 trapecios se puede formar un rectángulo de lados $a - b$ y $a + b$ como sigue



Luego,

$$a^2 - b^2 = (a - b)(a + b).$$

4.4. El orden de $\mathbb{R}$

Pasamos ahora a estudiar propiedades de los números reales relacionadas con el orden. Como antes, el punto de partida son los axiomas y a partir de allí estableceremos la validez de nuevas propiedades. Está claro que podemos usar todas las propiedades de la suma y el producto que ya probamos. Antes de continuar definimos, usando el orden, la noción de positividad para los números reales.

Definición. Un número real $x \neq 0$ es *positivo* si $0 < x$ y es *negativo* si $x < 0$.

Decir que a es menor que b es lo mismo que decir que b es mayor que a. Aunque parezca obvio, a veces es conveniente enfatizar este hecho. Por eso se usa también el signo mayor "$>$", definido justamente así:

$$b > a \qquad \Leftrightarrow \qquad a < b$$

Por ejemplo, si x es positivo, podems escribir $x > 0$ o $0 < x$. El signo $\geq$ se define en términos de $\leq$ de la misma manera.

Comenzamos con una propiedad muy básica: el 1, identidad para el producto, es un número positivo. ¿Hay que probar esto?

Desde el punto de vista pragmático, no. Si asumimos que hemos construido los reales partiendo de los naturales pasando por los enteros, en ese momento habremos definido el orden de los enteros y en ese momento habremos observado que $0 < 1$.

Ahora desde lo axiomático no es una propiedad de un conjunto númerico concreto y por lo tanto si debemos probarlo. En este sentido todas las propiedades que van siendo descubiertas y demostradas sirven de ayuda para construir efectivamente algún modelo que satisfaga todos los axiomas. De esto se sigue que en cualquier modelo de un cuerpo ordenado que construyamos, deberemos definir el orden de manera tal que la identidad para el producto sea mayor que el elemento neutro de la suma.

Proposición 4.7. $0 < 1$.

Demostración. Procederemos por el absurdo. Ya hemos observado que $0 \neq 1$. Supongamos que $1 < 0$. Sumando -1 a ambos miembros, por la consistencia del orden con la suma, resulta que $0 < -1$. Luego, por la consistencia del orden con el producto (tomando $c = -1$ (ver en §4.2 los Axiomas de cuerpo ordenado)) se sigue que $(-1)1 < (-1)0$, es decir $-1 < 0$. (Esto ya contradice que $0 < -1$ y podríamos terminar acá.) Sumando 1 a ambos miembros resulta que $0 < 1$, lo que contradice nuestra primera suposición (por tricotomía). Luego, conlcuimos que $0 < 1$. □

Proposición 4.8. *En el conjunto de los números reales valen las siguientes propiedades:*

(a) $x > 0 \quad \Leftrightarrow \quad -x < 0.$

(b) $x > 0 \quad \Leftrightarrow \quad x^{-1} > 0.$

(c) $x < y \quad \Leftrightarrow \quad -x > -y.$

(d) $x < y \ \wedge \ u < v \quad \Rightarrow \quad x + u < y + v.$

(e) $x < y \ \wedge \ z < 0 \quad \Rightarrow \quad xz > yz.$

(f) Regla de los signos:

- $x > 0 \ \wedge \ y > 0 \quad \Rightarrow \quad xy > 0.$
- $x > 0 \ \wedge \ y < 0 \quad \Rightarrow \quad xy < 0.$
- $x < 0 \ \wedge \ y < 0 \quad \Rightarrow \quad xy > 0.$

Demostración.

(a) Si $0 < x$, entonces sumando $-x$ a ambos miembros obtenemos que $-x < 0$. Recíprocamente si $-x < 0$, entonces sumando x a ambos miembros obtenemos que $0 < x$.

(b) Si $x > 0$ sabemos que x tiene inverso x^{-1} y éste es distinto de 0. Luego $x^{-1} > 0$ ó $x^{-1} < 0$. Supongamos que $x^{-1} < 0$. Entonces, multiplicando $x > 0$ por x^{-1} resulta que $xx^{-1} < 0$, es decir $1 < 0$. Esto es absurdo, luego $x^{-1} > 0$.

Ahora si $x^{-1} > 0$, entonces su inverso es también positivo como acabamos de probar. Es decir $(x^{-1})^{-1} > 0$ y por lo tanto $x > 0$.

(c) Se sigue de las siguientes equivalencias:

$$x < y \ \Leftrightarrow \ x - x < y - x \ \Leftrightarrow \ 0 < y - x \ \Leftrightarrow \ -y < -y + y - x \ \Leftrightarrow \ -y < -x$$

(d) Por un lado tenemos que $x < y \Rightarrow x + u < y + u$ y por otro lado tenemos que $u < v \Rightarrow y + u < y + v$. Es decir $x + u < y + u$ y $y + u < y + v$, luego por transitividad se sigue que $x + u < y + v$.

(e) Como $z < 0$, entonces por (a) $-z > 0$ y luego $(-z)x < (-z)y$, es decir $-zx < -zy$. Luego por (c) resulta que $zy < zx$.

(f) La regla de los signos se sigue directamente de la consistencia del orden con el producto y del inciso anterior.

□

Nota. El inciso (a) de la proposición anterior se sigue del inciso (c) y también se sigue del inciso (e). ¿Cómo?

Proposición 4.9. *Para todo $x, y \in \mathbb{R}$ valen las siguientes propiedades:*

(a) $x^2 \geq 0 \ \wedge \ x \neq 0 \quad \Leftrightarrow \quad x^2 > 0.$

(b) $x^2 + y^2 = 0 \quad \Leftrightarrow \quad x = 0 \ \wedge \ y = 0.$

(c) $0 < x < y \quad \Rightarrow \quad x^2 < y^2.$

(d) $x < y < 0 \quad \Rightarrow \quad x^2 > y^2.$

Demostración.

(a) Sabemos que $x^2 = 0$ si y sólo si $x = 0$.

($\Rightarrow$) Si $x^2 \geq 0$ y $x \neq 0$, entonces $x^2 \geq 0$ y $x^2 \neq 0$ y por tricotomía $x^2 > 0$.

($\Leftarrow$) Si $x^2 > 0$ en particular $x^2 \neq 0$, luego $x^2 \geq 0$ y $x \neq 0$.

(b) $x^2 + y^2 = 0$ si y sólo si $x^2 = -y^2$.

($\Rightarrow$) Si $x, y \neq 0$, entonces $0 < x^2$ y $-y^2 < 0$ lo cual contradice el hecho de ser $x^2 = -y^2$. Si $y = 0$, entonces $x^2 + y^2 = x^2 = 0$ y luego $x = 0$. Análogamente, si $y = 0$ se sigue que $x = 0$.

($\Leftarrow$) La recíproca es inmediata.

(c) Por consistencia del orden con el producto, multiplicando la desigualdad $x < y$ respectivamente por $x > 0$ e $y > 0$, tenemos que $x^2 = xx < xy$ y que $xy < yy = y^2$. Por transitividad, se sigue que $x^2 < y^2$.

(d) Por la regla de los signos, multiplicando la desigualdad $x < y$ respectivamente por $x < 0$ e $y < 0$, tenemos que $x^2 = xx > xy$ y que $xy > yy = y^2$. Por transitividad, se sigue que $x^2 > y^2$.

La prueba está completa. □

Problemas.

(1) ¿Para qué valores de x es $(x+2)(x-1)$ positivo y para cuáles negativo?

(2) Si $a, b > 0$, entonces $\left(\frac{1}{a} + \frac{1}{b}\right)(a+b) \geq 2$.

(3) ¿Existe algún α tal que $\frac{1}{1+\alpha} = 1 + \frac{1}{\alpha}$?

(4) Si $a + b = 1$, entonces $a^2 + b^2 \geq \frac{1}{2}$.

(5) Mostrar que el promedio entre a y b, $\frac{a+b}{2}$, está entre a y b y equidistante de ambos.

(6) Para todo par de reales positivos a y b, vale que $\frac{a}{b} \geq 4 - \frac{4b}{a}$.

(7) Si $a > 0$, entonces $a + \frac{1}{a} \geq 2$.

(8) Si $a < 0$, entonces $a + \frac{1}{a} \leq -2$.

Es mejor ignorar las soluciones hasta haber intentado resolver los problemas por uno mismo varias veces. Mejor aún es ignorar las soluciones hasta pasado un tiempo luego de haber resuelto los problemas.

Soluciones.

(1) De acuerdo a la regla de los signos, $(x+2)(x-1)$ es positivo cuando $x+2$ y $x-1$ son simultaneamente positivos o son simultaneamente negativos. Es claro que $x + 2 > 0$ si y sólo si $x > -2$ y $x - 1 > 0$ si y sólo si $x > 1$. Y por lo tanto $x + 2 < 0$ si y sólo si $x < -2$ y $x - 1 < 0$ si y sólo si $x < 1$. Por lo tanto $(x+2)(x-1)$ es positivo para $x > 1$ o $x < -2$ y es negativo para $-2 < x < 1$. Notamos que $(x+2)(x-1)$ es 0 si $x = -2$ o $x = 1$.

(2) Tenemos que

$$\begin{aligned}\left(\tfrac{1}{a} + \tfrac{1}{b}\right)(a+b) &= (a^{-1} + b^{-1})(a+b) \\ &= a^{-1}a + a^{-1}b + b^{-1}a + b^{-1}b = 1 + a^{-1}b + b^{-1}a + 1.\end{aligned}$$

Como $a, b > 0$, entonces $a^{-1}b > 0$ y $b^{-1}a > 0$. Luego

$$1 + a^{-1}b + b^{-1}a + 1 > 2.$$

(3) Como $1 + \frac{1}{\alpha} = (1+\alpha)\alpha^{-1}$, se sigue que α satisface la identidad planteada si y sólo si $\alpha = (1+\alpha)^2$. En particular tenemos que $\alpha > 0$. Ahora $(1+\alpha)^2 = 1 + 2\alpha + \alpha^2$, luego $\alpha = (1+\alpha)^2$ si y sólo si $1 + \alpha + \alpha^2 = 0$. Pero $1 + \alpha + \alpha^2 = 0$ si y sólo si $\alpha = -1 - \alpha^2$. Se sigue en particular que $\alpha < 0$, lo que contradice que $\alpha > 0$. Concluimos entonces que no existe un tal α.

(4) Supongamos que $a + b = 1$. Como $a^2 + b^2 + 2ab \geq 0$, entonces $a^2 + b^2 \geq -2ab = -2a(1-a)$. Por otro lado $0 \leq (a - \frac{1}{2})^2 = a^2 - a + \frac{1}{4}$. Luego $a(a-1) = a^2 - a \geq -\frac{1}{4}$ y $-2a(1-a) \geq \frac{1}{2}$. Conlcuimos que $a^2 + b^2 \geq \frac{1}{2}$.

(5) Notamos primero que si $a = b$, entonces $\frac{a+b}{2} = a = b$. Podemos suponer entonces que, cambiando los nombres si es necesario, $a < b$. Se sigue que $a + b < 2b$ y luego que $\frac{a+b}{2} < b$. Similarmente se sigue que $2a < a + b$ y que $a < \frac{a+b}{2}$. Además $\frac{a+b}{2} - a = \frac{b-a}{2}$ y $b - \frac{a+b}{2} = \frac{b-a}{2}$.

(6) Tenemos que $(b - \frac{a}{2})^2 \geq 0$. Como $(b - \frac{a}{2})^2 = b^2 - ab + \frac{a^2}{4}$, se sigue que $b^2 - ab \geq -\frac{a^2}{4}$ y luego que $4b - 4a \geq -\frac{a^2}{b}$ y luego que $4\frac{b}{a} - 4 \geq -\frac{a}{b}$. De aquí lo que se quería probar.

(7) Tenemos que $(a - 1)^2 \geq 0$. Se sigue que $a^2 - 2a + 1 \geq 0$ y luego que $a^2 + 1 \geq 2a$. Si $a > 0$, se deduce que $a + \frac{1}{a} \geq 2$.

(8) Tenemos que $(a + 1)^2 \geq 0$. Se sigue que $a^2 + 2a + 1 \geq 0$ y luego que $a^2 + 1 \geq -2a$. Si $a < 0$, se deduce que $a + \frac{1}{a} \leq -2$.

Valor absoluto

El *valor absoluto* de un número real a, denotado por $|a|$, se define como a si a es positivo y como $-a$ si a es negativo y $|a| = 0$ si $a = 0$. Es decir la función valor absoluto

$$|\cdot| : \mathbb{R} \to \mathbb{R}_{\geq 0}$$

está definida por

$$|a| = \begin{cases} a, & \text{si } a \geq 0 \\ -a, & \text{si } a < 0 \end{cases}$$

Por ejemplo $|0| = 0$, $|1| = 1$ y $|-1| = 1$.

Las siguientes propiedades son inmediatas de la definición:

- $|a| = 0$ si y sólo si $a = 0$.
- $|-a| = |a|$.
- $|ab| = |a||b|$.
- $-|r| \leq r \leq |r|$
- $|a - b| = |b - a|$.
- $|\frac{a}{b}| = \frac{|a|}{|b|}$.
- $|a^{-1}| = |a|^{-1}$.
- $|a^2| = |a|^2$.
- $|a^3| = |a|^3$.

Además, vale la *desigualdad triangular*

$$|a + b| \leq |a| + |b|$$

y esta otra desigualdad

$$|a - b| \geq \big||a| - |b|\big|.$$

4.5. Aritmética racional y fraccionaria

Los números racionales se representan como una fracción de la forma $\frac{p}{q}$ donde p y q son enteros cualesqueira con $q \neq 0$. Un racional puede representarse de varias maneras distintas. Por ejemplo,

$$\frac{2}{3} = \frac{4}{6} = \frac{-2}{-3}$$

su opuesto

$$-\frac{2}{3} = \frac{-2}{3} = \frac{-4}{6} = \frac{2}{-3}$$

y su inverso

$$\frac{3}{2} = \frac{-3}{-2} = \frac{6}{4}$$

La suma y el producto de números racionales se definen usando esta representación por las fórmulas que aprendemos en la escuela. Si a/b y c/d son dos racionales dados, entonces

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+cb}{bd} \quad \text{y} \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

A continuación queremos ver a los números racionales como números reales y discutir brevemente algunos aspectos de la notación de fracción, que ya introdujimos en los números reales. Recordemos que dados dos reales x, y con $y \neq 0$ llamamos cociente de x por y y escribimos $\frac{x}{y}$ al número real xy^{-1}.

Dados dos enteros a, b con $b \neq 0$ la notación $\frac{a}{b}$ tiene dos interpretaciones, que podrían ser distintas. (Esto no sería bueno). Queremos mostrar que éstas coinciden en todo.

- Primero. Si pensamos a $\frac{a}{b}$ como un racional, éste se puede representar también como el racional $\frac{c}{d}$. Sabemos que

  $$\frac{a}{b} = \frac{c}{d} \Leftrightarrow ad = bc$$

  Si pensamos a $\frac{a}{b}$ y a $\frac{c}{d}$ como fracciones, es decir $\frac{a}{b} = ab^{-1}$ y $\frac{c}{d} = cd^{-1}$, tenemos que

  $$ab^{-1} = cd^{-1} \Leftrightarrow ad = bc$$

  Por lo tanto ambas notaciones son consistentes para representar a un número racional.

- Segundo.

A continuación mostramos las conocidas fórmulas para la suma y el producto de números racionales y otras identidades útiles para hacer aritmética usando esta representación de los números racionales.

Una vez más decimos que la fracción $\frac{a}{b}$ es una notación para el número ab^{-1} y por lo tanto uno puede elegir la forma que le resulte más conveniente en cada situación. En

un contexto donde la notación de fracciones es natural, como en el conjunto de números racionales por ejemplo, resulta útil conocer algunas identidades aritméticas expresadas en términos de fracciones.

- Producto

$$\frac{a}{b}\cdot\frac{c}{d}=\frac{ac}{bd}$$

En efecto,

$$\frac{a}{b}\cdot\frac{c}{d}=ab^{-1}cd^{-1}=acb^{-1}d^{-1}=ac(bd)^{-1}=\frac{ac}{bd}.$$

- Suma

$$\frac{a}{b}+\frac{c}{d}=\frac{ad+cb}{bd}$$

Tenemos,

$$\frac{a}{b}+\frac{c}{d} \quad = \quad ab^{-1}+cd^{-1}=ab^{-1}d^{-1}d+cd^{-1}b^{-1}b=(ad+cd)d^{-1}b^{-1}=\frac{ad+cb}{bd}.$$

- Opuesto

El opuesto de $\frac{a}{b}$ es

$$-\frac{a}{b}=\frac{-a}{b}=\frac{a}{-b}$$

Notar que

$$\frac{a}{b}+\frac{-a}{b}=\frac{a+(-a)}{b}=\frac{0}{b}=0.$$

Luego $\dfrac{-a}{b}$ es el opuesto de $\dfrac{a}{b}$. Además

$$\frac{-a}{b}=(-a)b^{-1}=a(-b^{-1})=a(-b)^{-1}=\frac{a}{-b}.$$

- Inverso

El inverso de $\frac{a}{b}$ es

$$\left(\frac{a}{b}\right)^{-1}=\frac{1}{\frac{a}{b}}=\frac{b}{a}$$

En efecto,

$$\frac{1}{\frac{a}{b}}=\frac{1}{ab^{-1}}=(ab^{-1})^{-1}=a^{-1}(b^{-1})^{-1}=a^{-1}b=\frac{b}{a}.$$

Ejemplo. Tratemos de simplificar la expresión $\dfrac{-1}{1+\frac{1}{a}}\cdot(1+a)$. Usando fracciones tenemos

$$\frac{-1}{1+\frac{1}{a}}\cdot(1+a)=\frac{-1}{\frac{a+1}{a}}\cdot(a+1)=\frac{-a}{a+1}\cdot(a+1)=-a$$

Ahora, usando la notación con exponentes tenemos

$$\begin{aligned}\frac{-1}{1+\frac{1}{a}}\cdot(1+a) &= (-1)(1+a^{-1})^{-1}(a+1) = (-aa^{-1})(1+a^{-1})^{-1}(a+1)\\ &= -a\big(a(1+a^{-1})\big)^{-1}(a+1) = -a(a+1)^{-1}(a+1) = -a\end{aligned}$$

y obviamente obtenemos el mismo resultado. ◊

Observación. Recordemos que $\frac{a}{b}$ es una notación para ab^{-1}, siendo a y b reales cualesquiera con la única restricción de ser $b \neq 0$. Así, las identidades que mostramos más arriba entre "fracciones" son válidas no sólo para racionales sino para fracciones de cualquier tipo.

4.6. Cuerpos, cuerpos ordenados y cuerpos completos †

Si de la lista completa de axiomas de los números reales, consideramos sólo algunos de ellos, entonces aparecen otros conjuntos de números, distintos de los reales, que los satisfacen.

Un primer ejemplo de esto, es el de los números racionales, que satisfacen todos los axiomas de los reales salvo el de completitud. Otro ejemplo es el de los números complejos, que satisfacen todos los axiomas de los reales salvo los del orden. (En este caso, hay que enunciar de otro modo el axioma de completitud, usando el valor absoluto en vez del orden.)

Dado un conjunto de números con una suma y un producto, y posiblemente con un orden, según sea el conjunto de axiomas que satisface recibe distintos títulos.

Un *cuerpo* es aquel conjunto de números que sartisface los axiomas de la suma y el producto de los números reales. Algunos ejemplos de cuerpos son $\mathbb{R}$, $\mathbb{Q}$ y $\mathbb{C}$; también hay cuerpos finitos y hay una infinidad de ellos entre $\mathbb{Q}$ y $\mathbb{R}$.

Un *cuerpo ordenado* es aquel conjunto de números que sartisface los axiomas de la suma y el producto de los números reales y los del orden. Algunos ejemplos de cuerpos ordenados son $\mathbb{R}$ y $\mathbb{Q}$. Los números complejos $\mathbb{C}$ no son un cuerpo ordenado. (Vimos que en un cuerpo ordenado como $\mathbb{R}$, los cuadrados son positivos. Luego i^2 debería ser positivo; pero $i^2 = -1$ que debe ser negativo pues la identidad 1 debe ser positiva.)

Un *cuerpo completo* es aquel conjunto de números que satisface los axiomas de la suma y el producto de los números reales y el axioma de completitud (convenientemente enunciado). Ejemplos de cuerpos completos son $\mathbb{R}$ y $\mathbb{C}$. En cambio $\mathbb{Q}$ no es un cuerpo completo.

Un *cuerpo ordenado y completo* es aquel conjunto de números que satisface todos los axiomas de los números reales. Un ejemplo es $\mathbb{R}$ y como ya dijimos es el único ejemplo! (salvo equivalentes).

Finalmente queremos hacer notar que si consideramos un conjunto pequeño de axiomas aparecen otros conjuntos de números muy distintos que los satisfacen. Por ejemplo, si solo consideramos los axiomas de la suma y del producto, salvo el de existencia de inversos, entonces el conjunto de los enteros los satisface.

El siguiente cuadro resume los ejemplos comentados.

	cuerpo	ordenado	completo
$\mathbb{Q}$	✓	✓	✗
$\mathbb{R}$	✓	✓	✓
$\mathbb{C}$	✓	✗	✓

4.7. Ejercicios y problemas

Fragmento de "Arithmetic", de Carl Sandburg (EEUU, 1878-1967)

Arithmetic is where the answer is right and everything is nice and you can look out of the window and see the blue sky - or the answer is wrong and you have to start over and try again and see how it comes out this time.

Ejercicios

Ejercicio 4.1. Calcular en varios pasos observando las propiedades que justifican cada paso:

(1) $\Big((3\sqrt{3}) - 4\sqrt{3}) + (2\sqrt{3}) - 3\sqrt{3}) + (\sqrt{3}) - 2\sqrt{3})\Big)^2$

(2) $\dfrac{1}{(1-\pi)^{-1}} + \dfrac{1}{(2-\pi)^{-1}} + \dfrac{1}{(3-\pi)^{-1}}$

(3) $\left(\dfrac{1}{(\sqrt{2}+1)} + \dfrac{1}{(\sqrt{2}+1)^2} + \dfrac{1}{(\sqrt{2}+1)^3}\right)^{-1} (\sqrt{2}+2)$

Ejercicio 4.2. Dados $a, b \in \mathbb{R}$, encontar expresiones más simples de los siguientes números reales.

(1) $-a^{-1} + \big(-(-a)^{-1}\big) + \Big(-\big(-(-a)\big)^{-1}\Big)$

(2) $\dfrac{ba}{\Big(1+1/a\Big)^{-1}} \times \left(\dfrac{a}{b}\right)^{-1} a$

(3)

Ejercicio 4.3. Sabiendo que $3 < \pi < 4$ determinar si el siguiente número es positivo o negativo:

$$4(1-\pi) + \frac{1-\pi}{\pi} + (\pi - 1)\Big(\pi + \frac{4}{3}\Big)$$

Ejercicio 4.4. Decir, justificando, si las siguientes afirmaciones son verdaderas o falsas.

(1) Para todo $a \neq 0$, si $1 + a$ es positivo, entonces $1 - a$ es negativo.

(2) Existen al menos 3 números reales distintos a tales que $1 + a$ es positivo y $1 - a$ es negativo.

(3) No hay ningún número real T tal que $T^2 - 1$ es negativo y $2T + 1 > 2$.

Ejercicio 4.5. Escribir al número 1 como:

(1) Producto de 3 números distintos, al menos uno negativo.

(2) Suma de 3 números, al menos uno mayor que 2.

(3) Suma de 3 productos en los que al menos un factor sea un natural primo.

Ejercicio 4.6. Justificar a partir de las propiedades básicas de los reales la validez de las siguientes afirmaciones (bien sabidas).

(1) $0 + 0 = 0$ y $1 \cdot 1 = 1$.

(2) $a = b \Leftrightarrow a - b = 0$.

(3) $1 = 1^{-1}$ y $-1 = (-1)^{-1}$.

Ejercicio 4.7. Justificar a partir de las propiedades básicas de los reales la validez de las siguientes afirmaciones (bien sabidas). Recordar que si $b \neq 0$, $\frac{a}{b}$ denota al número real ab^{-1}.

(1) $\dfrac{b}{1} = b$.

(2) Si $b \neq 0 \neq d$, entonces $\dfrac{a}{b} = \dfrac{c}{d} \Leftrightarrow ad = bc$.

(3) Si $b \neq 0 \neq d \Rightarrow \left(\dfrac{b}{d}\right)^{-1} = \dfrac{d}{b}$.

(4) Si $b \neq 0 \neq d \Rightarrow \dfrac{a}{\frac{b}{d}} = \dfrac{ad}{b}$.

(5) Si $0 < a$ y $0 < b$, entonces $a < b \Leftrightarrow b^{-1} < a^{-1}$.

(6) $a + a = 0 \Rightarrow a = 0$.

(7) $a \neq 0 \Rightarrow a^2 > 0$.

Ejercicio 4.8. Decidir si las siguientes afirmaciones son verdaderas o falsas y justificar.

(1) $x^2 = x$, $\forall x \in \mathbb{R}$.

(2) $x^2 = x$ para algún $x \in \mathbb{R}$.

(3) Si a y b son reales, $a < b \Leftrightarrow a^2 < b^2$.

(4) $(a + b)^2 = a^2 + b^2$, $\forall a, b \in \mathbb{R}$.

Ejercicio 4.9. Hallar varios pares de números a, b que verifiquen la siguiente desigualdad y varios pares que no la verifiquen. (Ayuda: buscar probando)

$$\left(a + \frac{1}{a}\right)\left(b + \frac{1}{b}\right) > ab.$$

Ejercicio 4.10. Dados $a, b, c \in \mathbb{R}$ probar que siempre vale que:

(1) Si $b \neq 0 \Rightarrow -\dfrac{a}{b} = \dfrac{-a}{b} = \dfrac{a}{-b}$ y $\dfrac{-a}{-b} = \dfrac{a}{b}$.

(2) Si $b \neq 0 \neq d \Rightarrow \dfrac{a}{b} \pm \dfrac{c}{d} = \dfrac{ad \pm bc}{bd}$.

(3) Si $b, c, d \neq 0 \Rightarrow \dfrac{a/b}{c/d} = \dfrac{ad}{bc}$.

(4) Si $b \neq 0 \neq d$ y $\dfrac{a}{b} = \dfrac{c}{d} \Rightarrow \dfrac{a \pm b}{b} = \dfrac{c \pm d}{d}$.

Observación: Como a, b, c son reales cualesquiera, no necesariamente enteros, las fracciones que aparecen no son necesariamente números racionales. Las propiedades probadas generalizan las correspondientes de la aritmética racional.

Ejercicio 4.11. Analizar la veracidad de las siguientes proposiciones.

(1) $a \in \mathbb{R}$, $a > 0 \Leftrightarrow a^3 > 0$.

(2) $a, b \in \mathbb{R}$, $a^2 = b^2 \Rightarrow a^3 = b^3$.

(3) $a \in \mathbb{R}$, $a^2 \leq 1$ entonces $-1 \leq a \leq 1$.

Problemas

Problema 4.12. Probar las siguientes afirmaciones justificando cada pasos e identificando el método de prueba utilizado.

(1) Si $a \neq b \Rightarrow a^2 + b^2 > 0$.

(2) Si $0 < a$ y $0 < b$ entonces $a < b \Leftrightarrow a^2 < b^2$.

(3) No existe un número real x tal que $x^2 + 1 = 0$.

Problema 4.13. Analizar la veracidad de las siguientes afirmaciones.

(1) $\exists x$, $3x + -2 = -4x + 1$.

(2) $\exists x$, $x^2 + x + 1 = 0$.

(3) $\forall x$, $x^2 + 3x + 1 = 0$.

(4) $(\exists x)$: $x = -x$.

(5) $(\forall x)$: $\exists y$, $x = y^2$.

Problema 4.14. Analizar la validez de la siguiente demostración.

> *Teorema:* *Si* $a \in \mathbb{R}$ *entonces* $a = 0$.
> *Demostración:* $a^2 = a^2 \Rightarrow a^2 - a^2 = a^2 - a^2 \Rightarrow (a - a)(a + a) = a(a - a) \Rightarrow a + a = a \Rightarrow a = 0$.

Problema 4.15. Probar lo siguiente.

(I) Si $a, b \in \mathbb{R}_{>0}$, entonces $\frac{a}{b} \geq 4 - \frac{4b}{a}$

(II) Si $a, b, c, d \in \mathbb{R}$, entonces $(ab + cd)^2 \leq (a^2 + c^2)(b^2 + d^2)$.

(III) Si $x, y, z \in \mathbb{R}_{>0}$, entonces $(x + y + z)(\frac{1}{x} + \frac{1}{y} + \frac{1}{z}) \geq 9$.

(IV) Si $x, y \in \mathbb{R}$ son positivos, con $x < 1 < y$, entonces $xy + 1 < x + y$.

Problema 4.16. Probar lo siguiente.

(I) Dados $x, y, \alpha \in \mathbb{R}$, $x < y$, vale $x < \alpha x + (1 - \alpha)y < y$ si y sólo si $0 < \alpha < 1$.

(II) Si además $x < z < y$, entonces existe $\alpha \in \mathbb{R}$, $0 < \alpha < 1$, tal que $z = \alpha x + (1 - \alpha)y$.

Problema 4.17. Decidir si la desigualdad

$$\frac{a^2 + b^2}{2} \geq \left(\frac{a + b}{2}\right)^2$$

es válida en los siguientes casos:

(I) $a, b \geq 0$, (II) $a, b < 0$, (III) $a < 0 < b$.

Problema 4.18. Sabiendo que $\sqrt{2}$ es irracional, mostrar que:

(a) Existen pares de números irracionles cuyo producto no es irracional.

(b) $1 + \sqrt{2}$ y $1 - \sqrt{2}$ son irracionales.

(c) Existen pares de números irracionales cuya suma no es irracional.

(d) $\sqrt{2}/2$ es irracional.

(e) Existen irracionales cuya suma es irracional.

(f) $\sqrt{\sqrt{2}}$ es irracional.

(g) Existen irracionales cuyo producto es irracional.

Problema 4.19. Probar las siguientes afirmaciones justificando los pasos que realiza e identificar el método de prueba que utiliza.

(I) Si $0 \neq a \in \mathbb{R} \Rightarrow a^2 + \frac{1}{a^2} \geq 2$. Probar que vale la igualdad si y sólo si $a = 1$ o $a = -1$.

(II) No existe ningún $z \in \mathbb{R}$ tal que $x \leq z \ \forall x \in \mathbb{R}$.

(III) Si $a, b \in \mathbb{R}$, $a, b > 0$ y $ab = 1$, entonces $a + b \geq 2$. Probar que vale la igualdad si y sólo si $a = b = 1$.

Problema 4.20. Decidir si las siguientes afirmaciones son verdaderas o falsas.

(I) Existen $a, b \in \mathbb{R}$ tales que $\frac{1}{a+b} = \frac{1}{a} + \frac{1}{b}$.

(II) $(\frac{1}{a}-1)(\frac{1}{b}-1)=1\ \forall a,b>0$ tal que $a+b=1$.

(III) $x^2=x$ para exactamente un $x\in\mathbb{R}$.

(IV) $(a+b)^2\geq a^2+b^2$, $\forall a,b\in\mathbb{R}$.

(V) Existe $a,b\in\mathbb{R}$ tales que $(a+b)^2=a^2+b^2$.

(VI) $a,b\in\mathbb{R}$, $(a+b)^2=a^2+b^2\Leftrightarrow a=0$ ó $b=0$.

(VII) Existe $a\in\mathbb{R}$ tal que $1-\frac{1}{1+\frac{1}{a}}=\frac{1}{a}$.

Problema 4.21. Analizar la veracidad de las siguientes afirmaciones.

(I) $(\exists x)$: $x^3+6x^2+11x+6=(x+3)(x+1)$.

(II) $(\forall x>0)$: $\exists y$ tal que $0<y<x$.

(III) $\forall x$, $\exists y\neq x$ tal que $x^2=y^2$.

(IV) $\exists! x$: $x^2+3x+2=0$.

Problema 4.22. Probar lo siguiente.

(I) Si $a,b\in\mathbb{R}_{>0}$, entonces $\frac{a^3}{b^3}-\frac{a^2}{b^2}-\frac{a}{b}+1\geq 0$.

(II) Si $a\neq 0\neq b$ y $a+b=1$, entonces $(\frac{1}{a}-1)(\frac{1}{b}-1)=1$.

(III) Sean $a,b,c\in\mathbb{R}$ positivos. Si $a+b+c=1$, entonces $(\frac{1}{a}-1)(\frac{1}{b}-1)(\frac{1}{c}-1)\geq 8$.

(IV) Si $x,y,z\in\mathbb{R}$ positivos tales que $xyz=1$, entonces $x+z+y\geq 3$ (Ayuda: $x=y=z=1$ o uno de ellos es mayor que 1 y otro menor que 1.)

Problema 4.23. Un subconjunto A de los números reales se dice *convexo* si para todo par de elementos $x,y\in A$, $x<y$, y todo $z\in\mathbb{R}$ tal que $x<z<y$ se tiene $z\in A$.

Decidir si los siguientes subconjuntos de $\mathbb{R}$ son convexos:

(I) $\{x\in\mathbb{R}: x^3<4\}$.

(II) $\{x\in\mathbb{R}: x^2<12\}$.

(III) $\{x\in\mathbb{R}: x^2>12\}$.

(IV) $\{x\in\mathbb{R}: x^3<x\}$.

Capítulo 5

Números naturales y el principio de inducción

"Dios hizo los naturales; el resto es obra de los hombres"
Leopold Kronecker, matemático prusiano (1823 – 1891)

5.1. Números naturales

Los números naturales son los números que usamos para contar:

$$\mathbb{N} = \{1, 2, 3, 4, 5, \ldots\}$$

Todos sabemos sumar y multiplicar naturales y dados dos sabemos cuál es más grande.

5.1.1. Los axiomas de Peano

Los números naturales tienen una propidad fundamental: existe la noción de "siguiente" o "sucesor". Todo natural tiene un sucesor, el sucesor de n es $n + 1$. Además se tiene que:

- El 1 no es sucesor de nadie, y es el único natural así.
- Dos naturales distintos tienen sucesores distintos.
- Si K es un subconjunto de $\mathbb{N}$ que contiene al 1, tal que el sucesor de cualquier elemento de K está en K, entonces $K = \mathbb{N}$.

Las dos primeras son muy claras. La tercera requiere algo de reflexión.

Éstas son propiedades básicas de los naturales tal como los concemos. Ahora bien, estas propiedades *caracterizan* al conjunto de números naturales, tal como los axiomas de los reales (§4.2) caracterizan a los reales. Es decir, si imponemos estos axiomas a un conjunto N de números con una noción de sucesor, el conjunto N será (equivalente a) el de los números naturales.

AXIOMAS DE LOS NÚMEROS NATURALES

N1. Existe un único elemento en N, que llamamos 1, que no es el sucesor de ningún otro elemento.

N2. Dos elementos distintos de N tienen sucesores distintos.

N3. Si K es un subconjunto de N que contiene al 1, tal que el sucesor de cualquier elemento de K está en K, entonces $K = N$.

Nota. Éstos son los *axiomas de Peano*.

Observación. Podemos pensar en la *función sucesor* $s : \mathbb{N} \to \mathbb{N}$ que a cada $n \in \mathbb{N}$ le asigna su sucesor. En términos de s, el axioma N1 dice que no existe $n \in \mathbb{N}$ tal que $1 = s(n)$, es decir $1 \notin \mathrm{Im}\,(s)$, mientras que el axioma N2 dice que s es una función inyectiva.

La suma en $\mathbb{N}$ se define a partir de la función s empezando con:

$$n + 1 = s(n)$$

Ahora

$$n + 2 = (n + 1) + 1 = s(n + 1) = s(s(n)) = s^2(n)$$

En general, tenemos que

$$n + m = \underbrace{s(s(\cdots(s}_{n-\text{veces}}(n))\cdots)) = s^n(m)$$

Notar que $s^n(m) = s^m(n)$ y que como $s(n) + 1 = s(s(n)) = s(n + 1)$ tenemos

$$s(n + m) = s(n) + m = s(m) + n = s(n + m) = s(n) + s(m) - 1$$

5.1.2. Los naturales y los reales

Recordamos que los reales se construyen a partir de los naturales y que la suma y el producto de reales también se construyen extendiendo las operaciones de los naturales

A continuación mostramos cómo una propiedad de los naturales como subconjunto de los reales se sigue directamente de las propiedades del sucesor. Es un primer ejemplo de muchas demostraciones que haremos de la misma índole. De hecho, este método tiene nombre: inducción matemática.

Mostramos que todos los naturales, como números reales, son todos positivos. Dado que esto no tiene nada de novedoso, el hecho de que hagamos una prueba de ello puede resultar confuso. Vale la pena pensarlo de la siguiente manera.

¿Cómo debemos definir el orden de los números reales, para que resulte un cuerpo ordenado? En el contexto de cuerpo ordenado, vimos que $0 < 1$; es decir que la identidad del producto debe ser positiva. Ahora nos preguntamos si el resto de los naturales deberán ser todos positivos o si podrían haber algunos negativos. La respuesta es no. Deben ser todos positivos; no hay ninguna otra eleción posible.

Comencemos con un argumento simple, aunque no suficientemente riguroso. Ya hemos probado que $1 > 0$; luego, el sucesor de 1, $2 = 1 + 1 > 1 + 0 = 1 > 0$; ahora $3 = 2 + 1 > 1+0 = 1 > 0$. Así sucesivamente podríamos mostrar que todos los naturales son positivos. Este argumento es intuitivamente correcto, aunque a priori tiene una deficiencia. A partir de haber probado que 1, 2 y 3 son positivos deducimos que todos los naturales lo son.

Pregunta. ¿Cómo probamos esto de manera rigurosa para todos los naturales?

Respuesta. Usando el axioma N3.

Proposición 5.1. *Si $n \in \mathbb{N}$, entonces $n > 0$.*

Demostración. Consideremos el subconjunto de números reales K de todos los naturales positivos:

$$K = \{n \in \mathbb{N} : n > 0\}$$

Queremos ver que $K = \mathbb{N}$. Para esto usamos el tercero de los axiomas de los números naturales.

Como $1 > 0$, entonces $1 \in K$. Además si $n \in K$, es decir si $n > 0$, su sucesor $n + 1 > 0 + 1 = 1 > 0$, y por lo tanto $s(n) = n + 1 \in K$. Se sigue entonces que $K = \mathbb{N}$ como queríamos. □

Corolario 5.2. *Si $n \in \mathbb{N}$, entonces, su opuesto, $-n \notin \mathbb{N}$.*

Demostración. Si $n \in \mathbb{N}$, $n > 0$; luego $0 = n + (-n) > 0 + (-n) = -n$, es decir $-n < 0$ y por lo tanto $-n \notin \mathbb{N}$. □

El conjunto de números enteros, $\mathbb{Z}$, está formado por los naturales, sus opuestos y el cero,

$$\mathbb{Z} = -\mathbb{N} \cup \{0\} \cup \mathbb{N}$$

donde

$$-\mathbb{N} = \{-n : n \in \mathbb{N}\} = \{m : -m \in \mathbb{N}\}$$

El conjunto de los enteros tiene una estructura aritmética más rica que el de los naturales. El opuesto de un entero es un entero, mientras que el de un natural no lo es. Así, la suma de un entero a más el opuesto de otro b, es siempre otro entero. Es decir,

$$a, b \in \mathbb{Z} \quad \Rightarrow \quad a - b \in \mathbb{Z}$$

En general, a la suma de un número real x más el opuesto de otro y, se la llama *resta* de x e y. Así, hemos observado que la resta de enteros es entera. Esto no es cierto para los naturales; es decir, la resta de dos naturales puede no ser natural. Precisamente tenemos la siguiente proposición.

Proposición 5.3. *Dados $a, b \in \mathbb{N}$, $a - b \in \mathbb{N}$ si y sólo si $a > b$.*

Demostración. Si $a - b \in \mathbb{N}$, entonces $a - b > 0$ y luego $a > b$. Recíprocamente, si $a > b$, entonces $a - b > 0$ y como $a - b \in \mathbb{Z}$ concluimos que $a - b \in \mathbb{N}$. □

5.2. Inducción matemática

El *principio de inducción* es un método de prueba muy poderoso usado en toda la matemática. Se aplica a familias infinitas (indexadas por $\mathbb{N}$) de enunciados dados en forma de lista. En esta sección veremos el principio básico y algunas de sus variantes mas usadas, como la inducción corrida y la inducción fuerte entre otras.

5.2.1. El principio básico

La idea detrás de la inducción es la de mostrar que la validez de cada enunciado de la lista se sigue de la validez del anterior. Así, sólo basta disparar el proceso en el punto de partida para desencadenar una reacción en cadena que probará la validez de todos los enunciados de la lista. Por ejemplo, para probar que:

$$\forall n \in \mathbb{N},\ 2^n > n$$

el principio de inducción es muy adecuado. Para un número natural dado, como $n = 1$, la proposición dice que $2 = 2^1 > 1$ y para $n = 5$ dice que $32 = 2^5 > 5$. En cada caso podríamos hacer una prueba particular, pero esto no es suficiente si queremos probarla "para todo n".

Sin saberlo, ya hemos hecho una prueba "por inducción" cuando probamos que todo natural es positivo. Esa prueba se basó en el tercero de los axiomas de los naturales y éste es el que permite formular el siguiente teorema.

Teorema 5.4 (Principio de inducción)**.**
Sea $P(n)$ una función proposicional, con $n \in \mathbb{N}$. Si valen

(I) *$P(1)$ es verdadera y,*

(II) *asumiendo que $P(k)$ es verdadera para un $k \in \mathbb{N}$ arbitrario se deduce que $P(k+1)$ es verdadera,*

entonces $P(n)$ es verdadera para todo $n \in \mathbb{N}$.

Demostración. Consideremos el conjunto

$$H = \{n \in \mathbb{N} : P(n) \text{ es verdadera}\}$$

Por definición, $H \subseteq \mathbb{N}$. Basta entonces probar que H satisface el axioma N3 y así $H = \mathbb{N}$, se donde se sigue que $P(n)$ es verdadera para todo $n \in \mathbb{N}$.

Ahora

(I) $1 \in H$, pues $P(1)$ es verdadera por hipótesis;

(II) Si $k \in H$, es decir que $P(k)$ es verdadera, entonces de la segunda hipótesis se sigue que $P(k+1)$ es verdadera y por lo tanto $k+1 \in H$.

Luego $H = \mathbb{N}$ como queríamos ver. □

La conclusión del teorema dice que *todas* las (infinitas) proposiciones $P(n)$, con n un natural, son verdaderas. Sin el principio de inducción, para probar tal cosa, habría que encontrar una demostración para cada instancia o una demostración independiente de n.

Esta herramienta es efectiva pues reduce en general el trabajo a realizar ya que para probar una instancia dada, digamos $P(k+1)$, podemos asumir la validez de $P(k)$, que muchas veces es algo muy cercano a lo que se desea probar. Este paso de una demostración por inducción, se llama *paso inductivo* y $P(k)$ es la *hipótesis inductiva*. No debemos olvidar que para completar, o mejor dicho para empezar, una prueba por inducción debemos probar separadamente la primera instancia de P, es decir $P(1)$. Este es el *paso inicial*.

Veamos como funciona.

Ejemplo. *Para todo n natural, $2^n > n$.*
Demostración. Es fácil ver que para los primeros naturales esto es cierto y no es difícil convencerce de la validez de la afirmación.

n	1	2	3	4	5	6	7	8	9	10
2^n	2	4	8	16	32	64	128	256	512	1024

Sin embargo, para que sea aceptada como verdad matemática, debe ser demostrada rigurosamente, más alla de todos los indicios a su favor. Hagamos una prueba por inducción.

- Paso inicial: $P(1)$ es verdadera, ya que si $n = 1$, $2^n = 2^1 = 2 > 1 = n$.

- Paso inductivo: Asumimos que $P(k)$ es verdadera, es decir que $2^k > k$ y demostramos a partir de ésto que $P(k+1)$ es también verdadera; es decir que $2^{k+1} > k+1$. Tenemos que $2^{k+1} = 2 \cdot 2^k$ y, por hipótesis inductiva, se sigue que $2 \cdot 2^k > 2 \cdot k = k + k$; como $k \geq 1$ resulta que $k + k \geq k + 1$. Por lo tanto

$$2^{k+1} = 2 \cdot 2^k > 2 \cdot k = k + k \geq k + 1$$

como queríamos probar. Luego, como vale $P(1)$ y, dado cualquier $k \in \mathbb{N}$, $P(k)$ verdadero implica $P(k+1)$ verdadero, se tiene que $P(n)$ es verdadero para todo $n \in \mathbb{N}$. ◊

Ahora veamos un ejemplo tomado "prestado" del análisis, para quienes ya conocen el concepto de derivada de funciones.

Ejemplo. Sea $f(x) = \operatorname{sen}(x)$. Veamos que la fórmula para la derivada n-ésima de f está dada por

$$f^{(n)}(x) = \operatorname{sen}\left(x + \tfrac{n\pi}{2}\right)$$

Sea $P(n)$ la fórmula que queremos probar $f^{(n)}(x) = \operatorname{sen}(x + \frac{n\pi}{2})$.

- Paso inicial: Para el paso inicial tenemos que $f'(x) = \operatorname{sen}'(x) = \cos(x)$. Y la fórmula nos da

$$(1)(x) = \operatorname{sen}(x + \tfrac{\pi}{2}) = \operatorname{sen}(x)\cos(\tfrac{\pi}{2}) + \cos(x)\operatorname{sen}(\tfrac{\pi}{2}) = \cos(x)$$

donde hemos usado la fórmula del seno de una suma y que $\cos(\frac{\pi}{2}) = 0$ y $\operatorname{sen}(\frac{\pi}{2}) = 1$.

- Paso inductivo: Para el paso inductivo, supongamos que vale $P(k)$, i.e. $f^{(k)}(x) = \operatorname{sen}(x + \frac{k\pi}{2})$, para $k \in \mathbb{N}$ y veamos que vale $P(k+1)$, i.e $f^{(k+1)}(x) = \operatorname{sen}(x + \frac{(k+1)\pi}{2})$. Por un lado, usando que la derivada $(k+1)$-ésima de $f(x)$ es la derivada de $f^{(k)}(x)$ y la hipótesis inductiva, tenemos

$$f^{(k+1)}(x) = (f^{(k)}(x))' = \operatorname{sen}(x + \tfrac{k\pi}{2})' = \cos(x + \tfrac{k\pi}{2})$$

Por otra parte, usando la fórmula para el coseno de una suma,

$$\begin{aligned} \operatorname{sen}(x + \tfrac{(k+1)\pi}{2}) &= \operatorname{sen}((x + \tfrac{k\pi}{2}) + \tfrac{\pi}{2}) \\ &= \operatorname{sen}(x + \tfrac{k\pi}{2})\cos(\tfrac{\pi}{2}) + \cos(x + \tfrac{k\pi}{2})\operatorname{sen}(\tfrac{\pi}{2}) = \operatorname{sen}(x + \tfrac{k\pi}{2}) \end{aligned}$$

Luego, el paso inductivo vale y por lo tanto la fórmula para la derivada también. ◊

Nota. Una buena forma de pensar en la inducción es a través de la siguiente alegoría. Pensemos que tenemos infinitas fichas de dominó, tantas como números naturales. Pensemos que cada una de las propiedades $P(n)$ representa una ficha de dominó D_n, y que todas están colocadas en fila a la misma distancia, menor que la altura de las fichas. Pensemos que probar que $P(n)$ "vale" equivale a que la ficha correspondiente a D_n se "cae". Luego, probar que $P(n)$ vale para todo n, es equivalente a ver que todas las fichas se caen.

En estas condiciones, para asegurarnos de tirar todas las fichas de dominó, necesitamos dos cosas:

- que si se cae una se caiga la siguiente (es decir, $P(k)$ verdadero implica $P(k+1)$ verdadero);
- que se caiga la primera ($P(1)$ verdadero) y dispare la caída en cadena del todo el resto.

La primera condición sobre los dominós es el paso inductivo y la segunda condición es el paso inicial.

Cómo evitar errores comunes en el uso de la inducción

En las pruebas por inducción es imprescindible llevar a cabo la prueba del paso inicial y la prueba del paso inductivo. Además, hay que asegurarse que el argumento usado en el paso inductivo, efectivamente es válido para cualquier $k \in \mathbb{N}$. Hay afirmaciones falsas, que dependen de n, para las cuales vale o bien la primera instancia o bien el paso inductivo (pero no ambas!).

- Por ejemplo, consideremos las afirmaciones

$$\begin{aligned} P(n) &: n-1 \text{ es positivo para todo } n \in \mathbb{N}; \\ Q(n) &: n^2 = n^3 \text{ para todo } n \in \mathbb{N}. \end{aligned}$$

Evidentemente ambas son falsas. Sin embargo, para P el paso inductivo funciona pues $n-1>0$ implica que $n=(n-1)+1>1>0$; y, para Q, la primera instancia funciona pues $1^2=1^3$.

En muchas pruebas por inducción el paso inicial es sencillo y la dificultad está en el paso inductivo. Esto no quiere decir que si el paso inductivo es díficil y uno logra probarlo, esto sea suficiente.

- Consideremos ahora la siguiente afirmación que da una fórmula para la suma de los primeros n naturales.

$$R(n) \ : \ 1+2+3+\cdots+n = \tfrac{1}{8}(2n+1)^2$$

Paso inductivo: Supongamos que $R(k)$ vale para $k \in \mathbb{N}$ y veamos que $R(k+1)$ también vale. Calculemos entonces $R(k+1)$. Por hipótesis inductiva

$$1+2+3+\cdots+k+(k+1) = \tfrac{1}{8}(2k+1)^2+(k+1)$$

Luego queremos ver que

$$\tfrac{1}{8}(2k+1)^2+(k+1) = \tfrac{1}{8}(2(k+1)+1)^2$$

Ahora, por un lado tenemos que

$$\tfrac{1}{8}(2k+1)^2+(k+1) = \tfrac{1}{8}(4k^2+4k+1)+(k+1) = \tfrac{1}{8}(4k^2+12k+9)$$

y por otro lado tenemos que

$$\tfrac{1}{8}(2(k+1)+1)^2 = \tfrac{1}{8}(2k+3)^2 = \tfrac{1}{8}(4k^2+12k+9)$$

Por lo tanto hemos probado el paso inductivo.

A pesar de haber superado el paso inductivo, la afirmación el falsa. Por ejemplo la suma $1+2+3=6$ y la fórmula evaluada en $n=3$ da $\frac{1}{8}(2\cdot 3+1)^2 = \frac{49}{8} = 6+\frac{1}{8}$. El paso inicial sin embargo no vale, pues $R(1)$ es $1=\frac{9}{8}$, que es falso. (Si valiera, entonces la afirmación debería ser cierta!) Amazing!

- Analicemos ahora la siguiente afirmación, para la cual el primer caso es evidentemente verdadero.

$$S(n) \ : \ \text{En cualquier grupo de } n \text{ personas, todas son de la misma altura.}$$

Veamos que para todo conjunto de n personas, todas tienen la misma altura h. Si $n=1$, ésto es claro. Ahora supongamos que esto es cierto para todo conjunto de k personas y demostrémoslo para todo conjunto de $k+1$ personas. Dado uno de éstos, retiramos a una persona cualquiera, quedando un conjunto de k. Por hipótesis inducitva, estas k personas son todas de la misma altura. Pero esto vale para cualquier conjunto de k personas. Luego, si consideramos un nuevo conjunto de k personas, intercambiando a la persona que retiramos con una cualquiera de las k personas del primer conjunto, concluimos que la persona retirada al principio también tiene altura h, igual que el resto, con lo cuál ¡todas tienen la misma altura!

Siendo la afirmación falsa, la prueba es incorrecta. ¿Dónde está el error?

5.2.2. Inducción corrida

Veamos a continuación un ejemplo parecido a uno ya visto, que aunque similar a este, no permite el uso del principio de inducción tal como lo conocemos. Sin embargo se observa que ambos ejemplos comparten algo fundamental que nos conducirá a enunciar un principio de inducción más amplio.

Ejemplo. Consideremos el enunciado: *Para todo n natural*, $2^n > 2n + 1$.

No es difícil ver que esto no es cierto. Para $n = 1$ y para $n = 2$ se afirma que $2 > 3$ y que $4 > 5$ respectivamente. Sin embargo, para $n = 3$ es cierto, ya que se afirma que $8 > 7$. La siguiente tabla muestra que, a partir de 3, aparentemente es cierto.

n	1	2	3	4	5	6	7	8	9	10
$2n+1$	3	5	7	9	11	13	15	17	19	21
2^n	2	4	8	16	32	64	128	256	512	1024

No es posible hacer una demostración de lo afirmado, ya que es falso. Si hubiéramos intentado una prueba por inducción, no hubiéramos superado el primer paso, ya que para $n = 1$ la afirmación es falsa.

Sin embargo y a pesar de esto, intentemos el paso inductivo. Es decir supongamos que $2^k > 2k+1$ y deduzcamos que $2^{k+1} > 2(k+1)+1$. Tenemos que $2^{k+1} = 2 \cdot 2^k$ y por hipótesis inductiva se sigue que $2 \cdot 2^k > 2(2k + 1) = 4k + 2$. Ahora $4k + 2 = 2(k + 1) + 1 + 2k - 1$, luego como $2k - 1 \geq 0$ para todo k natural, se sigue $4k + 2 \geq 2(k + 1) + 1$ y por lo tanto $2^{k+1} > 2(k + 1) + 1$. ◊

En este ejemplo hemos probado el paso inductivo pero no el primer paso. Ahora, dado que si $n = 3$ la afirmación es válida, podríamos tomar a 3 como primer caso y gracias al paso inductivo deducir que para $n = 4$ la afirmación es válida, y luego para $n = 5$, etc.

El siguiente teorema describe una versión más general del Principio de Inducción en la cual el paso inicial no es necesariamente aquel en el que $n = 1$, sino otro natural cualquiera o aún un entero negativo o el 0.

Teorema 5.5 (Principio de inducción corrida)**.**
Sea $P(n)$ una función proposicional, con $n \in \mathbb{Z}$ y sea $N \in \mathbb{Z}$. Si valen

(I) *$P(N)$ es verdadera y,*

(II) *asumiendo que $P(k)$ es verdadera se deduce que $P(k+1)$ es verdadera, para un $k \in \mathbb{Z}$ arbitrario con $k \geq N$,*

entonces $P(n)$ es verdadera para todo $n \in \mathbb{Z}$ con $n \geq N$.

Demostración. Sea

$$H = \{n \in \mathbb{N} : \ P(N - 1 + n) \text{ es verdadera}\}$$

Por definición, $H \subseteq \mathbb{N}$. Si probamos que H satisface el axioma N3 resultará que $H = \mathbb{N}$ y, por ende, que $P(N-1+n)$ es verdadera para todo $n \in \mathbb{N}$. Equivalentemente, probaremos que $P(k)$ es verdadera para todo $k \geq N$, $k \in \mathbb{Z}$.

Ahora

(I) $1 \in H$, pues $P(N-1+1) = P(N)$ es verdadera por hipótesis;

(II) Si $k \in H$, es decir que $P(N-1+k)$ es verdadera, entonces de la segunda hipótesis se sigue que $P(N-1+k+1) = P(N-1+(k+1))$ es verdadera y así $k+1 \in H$.

Luego se cumple el axioma N3 y por lo tanto $H = \mathbb{N}$, como queríamos. □

Los siguientes problemas son ejemplos en los que el Principio de Inducción corrido se aplica con éxito.

Problemas.

(1) ¿Es cierto que $2^{n+1} > n^2 + n + 2$ para todo n natural? ¿Es cierto a partir de algún n?.

(2) Probar que $n^2 + n \geq 42$ si $n \geq 6$ ó $n \leq -7$.

(3) Mostrar que
$$(1+h)^n \geq \tfrac{1}{2} n(n-1)h^2$$
para todo natural $n \geq 2$ y para todo real $h \geq 2$.

Soluciones.

(1) Para $n = 1$ tenemos $2^{1+1} = 4 = 1^2 + 1 + 2$. Para $n = 2$ tenemos $2^{2+1} = 8 = 2^2 + 2 + 2$. Para $n = 3$ tenemos $2^{3+1} = 16 > 3^2 + 3 + 2 = 14$. Veamos si es cierto que vale para todo $n \geq 3$. Usaremos por tanto el principio de inducción corrido con $N = 3$. Sea $k \geq 3$ arbitrario y supongamos que vale $2^{k+1} > k^2 + k + 2$. Queremos ver que entonces también vale la desigualdad para $k+1$, esto es
$$2^{k+2} > (k+1)^2 + (k+1) + 2 = k^2 + 2k + 1 + k + 3 = k^2 + 3k + 4$$
Por hipótesis inductiva tenemos
$$\begin{aligned} 2^{k+2} = 2 \cdot 2^{k+1} &> 2(k^2 + k + 2) = 2k^2 + 2k + 4 \\ &= k^2 + k^2 + 2k + 4 > k^2 + 3k + 4 \end{aligned}$$
donde hemos usado que $k^2 > k$ pues $k \geq 3$ (esto a su vez puede ser probado por inducción corrida, lo dejamos como ejercicio). Luego, $2^{n+1} > n^2 + n + 2$ para todo $n \geq 3$.

(2) Podemos pensar esto como 2 problemas. Sea $P(n)$ a función proposicional $n^2 + n \geq 42$ con $n \in \mathbb{N}$. Queremos ver que $P(n)$ es verdadero para todo natural $n \geq 6$ y para todo natural $n \leq -7$. En el primer caso, podemos usar inducción corrida, con $N = 6$. El paso inicial vale pues $6^2 + 6 = 42$. El paso inductivo es fácil también. Supongamos que $k^2 + k \geq 42$ para un $k \geq 6$ entonces
$$(k+1)^2 + k + 1 = (k^2 + k) + 2(k+1) \geq 42 + 2(k+1) \geq 42$$

pues $k > 0$.

Para el segundo caso, es decir $P(n)$ para $n \leq -7$ no podemos aplicar inducción tal como lo sabemos, pues necitamos $n \geq N$ para algún N. Para esto, multiplicando por -1 la desigualdad, llegamos a $-n \geq 7$. Haciendo el cambio de variable

$$m = -n$$

tenemos la desigualdad en la forma deseada $m \geq 7$ y tomamos a $N = 7$ para la inducción corrida. Sin embargo, aun nos resta hacer el cambio de variable en la función proposicional, que queremos enunciarla en términos de m. Como $n = -m$, $n^2 + n = (-m)^2 + (-m) = m^2 - m$. Luego, probar que $P(n)$ dada por $n^2 + n \geq 42$, vale para todo $n \leq -7$ es equivalente a probar que

$$Q(m): \quad m^2 - m \geq 42, \quad \forall m \geq 7.$$

Ahora sí, usando inducción corrida con $N = 7$, el paso inicial se cumple pues $7^2 - 7 = 42$ y asumiendo que $k^2 - k \geq 42$ para $k \geq 7$ tenemos, por hipótesis inductiva que $(k+1)^2 - (k+1) = k^2 + k > k^2 - k \geq 42$.

Luego, por el principio de inducción, $P(n)$ vale para todo $n \geq 6$ y $Q(m)$ vale para todo $m \geq 7$, es decir, $P(n)$ vale para todo natural con $n \geq 6$ y $n \leq -7$.

(3) El paso inicial con $N = 2$ vale, pues $(1+h)^2 = h^2 + 2h + 1$ y $\frac{1}{2}2(2-1)h^2 = h^2$ y $h > 0$. Supongamos que vale $(1+h)^k \geq \frac{1}{2}k(k-1)h^2$, para $k \geq 2$. Queremos ver que entonces también vale $(1+h)^{k+1} \geq \frac{1}{2}k(k+1)h^2$. Usando la hipótesis inductiva, tenemos que

$$(1+h)^{k+1} = (1+h)^k(1+h) \geq \tfrac{1}{2}k(k-1)h^2(1+h)$$

Luego, queremos ver si $12k(k-1)h^2(1+h) \geq \frac{1}{2}k(k+1)h^2$, es decir, si

$$(k-1)(1+h) = (k-1)h + k - 1 \geq k + 1$$

o sea si $(k-1)h \geq 2$. Como esto último vale para todo $k \geq 2$ y $h \geq 2$, vemos que el paso inductivo se cumple y por lo tanto hemos terminado.

Nota. Más adelante veremos (ver binomio de Newton, §12.2) que

$$(1+h)^n = 1 + nh + \tfrac{1}{2}n(n-1)h^2 + \circledast$$

donde $\circledast$ son términos de la forma $a_k(n)\, h^k$ para $3 \leq k \leq n$. Usando esto es directo probar por inducción que el enunciado vale para todo $n \in \mathbb{N}$ y para todo $h \geq 0$.

5.2.3. Inducción fuerte

Comencemos con un ejemplo. Imaginemos que existen billetes de \$4. [*]

Pregunta. ¿Es posible pagar cualquier cantidad usando solo billetes de \$4 y \$5?

[*] Bueno, esto es mucho menos grave que "supongamos un caballo totalmente esférico deslizando por una montaña piramidal sin rozamiento", como hay que asumir por ahí en otras ciencias.

Está claro que los montos chicos resultan difíciles. No podemos pagar 1, 2 y 3. Si podemos 4 y 5, pero no 6 ni 7. Ahora 8, 9 y 10 si, pero de nuevo 11 no. Sigamos un poco más:

12 = 4+4+4	17 = 4+4+4+5
13 = 4+4+5	18 = 4+4+5+5
14 = 4+5+5	19 = 4+5+5+5
15 = 5+5+5	20 = 5+5+5+5
16 = 4+4+4+4	21 = 4+4+4+4+5

Parece que funcionará siempre bien, ¿o no? Para estar seguros necesitamos entender cómo hacer que funcione siempre. Podríamos intentar una prueba por inducción. Sin embargo, no está claro cómo escribir a $n+1$ como suma de cuatros y cincos sabiendo cómo hacerlo con n.

En cambio es más claro que para escribir al 18 como suma de cuatros y cincos es más útil ir para atrás hasta el 14 y sumarle un cuatro más o ir hasta el 13 y sumarle un cinco más. Así tenemos que

$$18 = 14 + 4 = (4 + 5 + 5) + 4 \qquad \text{ó} \qquad 18 = 13 + 5 = (4 + 4 + 5) + 5.$$

Entonces, para escribir $n+1$ como suma de cuatros y cincos consideramos

$$(n + 1) - 4 = n - 3\,,$$

que ya sabemos escribir como suma de cuatros y cincos y le agregamos un 4 más. Esto funciona perfectamente a partir de $n = 15$.

Hemos probado lo que queríamos de manera inductiva, haciendo uso de que conocemos para $n-3$ lo que queremos probar para $n+1$. Está claro que esto difiere de lo que aprendimos como método inductivo, en el que hacemos uso de que conocemos para n lo que queremos probar para $n+1$. Sin embargo, esto también funciona.

El siguiente teorema asegura que lo que hemos hecho es correcto. Establece un principio de inducción más amplio, que incluye al anterior. Su demostración necesita del *principio de buena ordenación* que discutiremos en la Sección 5.7. En esa sección probaremos este teorema.

Teorema 5.6 (Principio de inducción fuerte)**.**
Sea $P(n)$ una función proposicional, con $n \in \mathbb{N}$. Si

(I) *$P(1)$ es verdadera y,*

(II) *asumiendo que $P(1), P(2), \ldots, P(k)$ son verdaderas para un $k \in \mathbb{N}$ arbitrario se deduce que $P(k+1)$ es verdadera,*

entonces $P(n)$ es verdadera para todo $n \in \mathbb{N}$.

Este resultado nos pone a disposición un método de prueba más potente que el anterior ya que al momento de probar el paso inductivo la hipótesis inductiva es mucho

más amplia. Podemos asumir como hipótesis inductiva, no sólo $P(k)$ sino además todas las instancias anteriores. En el ejemplo anterior resultó conveniente usar como hipótesis inductiva sólo $P(k-3)$.

Veamos otro ejemplo en el cuál la inducción fuerte es lo que necesitamos.

Ejemplo. Sea $r \in \mathbb{R}$ tal que $r + \frac{1}{r} \in \mathbb{Z}$. Probar que el número

$$R_n = r^n + \frac{1}{r^n} \in \mathbb{Z} \qquad \text{para todo } n \in \mathbb{N}.$$

Primero observemos que existen números r tales que $r + \frac{1}{r}$ resulta entero. Por ejemplo $r = 1$ ó $r = 2 + \sqrt{3}$ son algunos de ellos (chequear).

Usemos el principio de inducción fuerte.

- Paso inicial: Si $n = 1$, $R_1 = r + \frac{1}{r}$ es entero pues así fue elegido r.
- Paso inductivo: Supongamos que $r^k + \frac{1}{r^k} \in \mathbb{Z}$ para todo $k = 1, 2, \ldots, n$. Queremos deducir que $r^{k+1} + \frac{1}{r^{k+1}}$ es también entero. Tenemos que

$$\begin{aligned} R_{k+1} &= r^{k+1} + \frac{1}{r^{k+1}} = r^k \cdot r + \frac{1}{r^k} \cdot \frac{1}{r} \\ &= \left(r^k + \frac{1}{r^k}\right)\left(r + \frac{1}{r}\right) - r^k \cdot \frac{1}{r} - \frac{1}{r^k} \cdot r \\ &= \left(r^k + \frac{1}{r^k}\right)\left(r + \frac{1}{r}\right) - \left(r^{k-1} + \frac{1}{r^{k-1}}\right) = R_k R_1 - R_{k-1}. \end{aligned}$$

Ahora, por hipótesis inductiva (fuerte) el miembro de la derecha es entero, ya que R_1, R_{k-1} y R_k son enteros por hipótesis. Luego R_n es entero para todo natural n. ◊

En el ejemplo, hemos usado que valen $P(1)$, $P(k-1)$ y $P(k)$ simultáneamente, para probar que $P(k+1)$ también vale.

5.2.4. Inducción generalizada †

Los enunciados de la forma "para todo $n \in \mathbb{N}$, vale $P(n)$" son los enunciados arquetípicos para ser probados por inducción. Vimos que enunciados de la forma "para todo $n \in \mathbb{N}$ con $n \geq N$, vale $P(n)$" también pueden ser probados por inducción.

Queremos ahora explicar como el mismo principio de inducción se aplica para probar enunciados que a primera vista lucen más generales que el enunciado típico. Por ejemplo, imaginemos un enunciado como el que sigue:

- *"Probar que para todo número real x de la forma $\cos(k\pi/4)$, con k múltiplo positivo de 3, la función f satisface que $f(x) = 0$."*

A pesar de aparecer un x real, la función coseno y una función f el enunciado es de la forma:

- *"Para todo k múltiplo postivo de 3, vale $P(k)$"*, donde $P(k)$ es "si x de la forma $\cos(k\pi/4)$, la función f satisface que $f(x) = 0$."

Los múltiplos positivos de 3 no son todos los naturales, sin embargo hay un primer múltiplo positivo de 3, el 3, y hay un siguiente, el 6. Y dado uno cualquiera, digamos $3m$,

también hay un siguiente, $3(m+1)$. De hecho todos los múltiplos positivos de 3 son de la forma $3m$ para algún natural m.

Reescribamos una vez más la proposción inicial.

• "*Para todo* $m \in \mathbb{N}$, *vale* $Q(m)$", donde ahora $Q(m)$ es "si $x = \cos(3m\pi/4)$, la función f satisface que $f(x) = 0$".

La proposición inicial así escrita puede ser probada por inducción.

Preguntas.

(1) ¿Qué hicimos?

(2) ¿Porqué fue posible?

(3) ¿Hay un enunciado general para aprender?

Respuestas.

(1) Lo que hicimos fue reescribir la proposición original llevándola a la forma "para todo $n \in \mathbb{N}$, vale $P(n)$".

(2) Esto fue posible pues los infinitos enunciados a probar estaban dados como una lista rotulada por los naturales. Es decir, hay un primer enunciado, un segundo enunciado, un tercero, un cuarto, un quinto, etcétecra.

(3) Podremos hacer lo mismo en todos los casos en los que el dominio de variable k de la función porposicional $P(k)$ se pueda listar, con un primer elemento, un segundo elemento, un tercero, etcétera. Basta notar que una lista como éstas no es más que una sucesión.

El enunciado general es el siguiente.

Teorema 5.7 (Principio de inducción generalizado)**.**
Sea $P(a)$ *una función proposicional, con* $a \in Im(a_n)$*, donde* a_n *es una sucesión dada. Si*

(I) $P(a_1)$ *es verdadera y,*

(II) *asumiendo que* $P(a_n)$ *es verdadera para un* a_n *arbitrario se deduce que* $P(a_{n+1})$ *es verdadera,*

entonces $P(a)$ *es verdadera para todo* $a \in Im(a_n)$*.*

Demostración. Sea A el subconjunto de los naturales $A = \{n \in \mathbb{N} : P(a_n) \text{ es verdadera}\}$. Veamos que $A = \mathbb{N}$ y así se sigue que $P(a_n)$ es verdadera para todo $n \in \mathbb{N}$ como debemos probar.

Como $P(a_1)$ es verdadera, se sigue que $1 \in A$. Además si $n \in A$, $P(a_n)$ es verdadera. Luego por hipótesis $P(a_{n+1})$ es verdadera, de donde se sigue que $n+1 \in A$. Ahora el axioma N3 implica que $A = \mathbb{N}$ y la prueba está completa. □

Ejemplos. Los siguientes son ejemplos de proposiciones de la forma "$P(x)$, para todo $x \in A$" que podrían ser atacadas con el Principio de Inducción (generalizada). Sólo hacemos hincapié en el dominio A de la variable de la función proposicional P.

(1) Todos los enteros $m \geq 199$ terminados en 99 (en notación decimal), satisfacen la propiedad P.

(2) Si $n \geq 4$ es un múltiplo de 3 mas 1, entonces vale que ...

(3) Los números de Fermat [**] satisfacen ...

Observación. Algunos casos particulares de inducción generalizada tienen nombre propio.

- El principio de inducción corrida (Teorema 5.5) se sigue directamente de éste más general tomando $a_n = (n-1) + N$.
- La "inducción para atrás" es otro caso de inducción generalizada en la que $a_n = -n$.
- También podemos considerar la inducción para atrás corrida, con $a_n = -n-(N-1)$. En este caso los índices comienzan en $-N$ y continuan hacia atrás: $-N, -N-1, -N-2, \ldots$.

Nota. También podemos extender el principio de inducción fuerte a uno fuerte y generalizado de manera análoga a lo que hicimos.

Inducción de Cauchy †

Existen un sinnúmero de maneras de aplicar el principio de inducción. Sólo a modo de mostrar hasta donde podemos llegar presentamos un caso de inducción segmentada. Quizá el ejemplo más conocido es el siguiente: la *inducción de Cauchy*.

Supongamos que tenemos que probar que $P(n)$ es verdadera para todo $n \in \mathbb{N}$. Pero en vez de tener las hipótesis inductivas usuales, tenemos las siguiemtes:

(I) $P(1)$ es verdadera.

(II) Si $P(n)$ es verdadera, entonces $P(2n)$ es verdadera.

(III) Si $P(m+1)$ es verdadera, entonces $P(m)$ es verdadera.

Resulta entonces que $P(n)$ es en efecto verdadera para todo $n \in \mathbb{N}$

Es el momento apropiado para que cada uno recorra, con lápiz y papel, los naturales corroborando cómo deducir la verdad de P en cada una de esas instancias. Comenzando con 1 sabemos que $P(1)$ es verdadera por hipótesis y luego se sigue que $P(2)$ y $P(4)$ son verdaderas; a partir de $P(4)$ deducimos $P(3)$ y podemos también obtener $P(6)$, para luego deducir $P(5)$. ¿Convencidos? Quizá sea buena idea avanzar un poco más. Pero primero una pausa...

[**] Los números de Fermat son los naturales de la forma $F_n = 2^{2^n} + 1$.

Ahora sí. Para probar esto formalmente podemos usar Inducción fuerte. Es decir, basta que mostremos que las dos hipótesis de la inducción fuerte se satisfacen para $P(n)$ y así el principio de inducción fuerte nos asegura que $P(n)$ es verdadera para todo $n \in \mathbb{N}$ Recordemos éstas dos hipótesis:

- $P(1)$ es verdadera.
- Si $P(k)$ es verdadera para $1 \leq k \leq n-1$, entonces $P(n)$ es verdadera.

La primera de éstas ya fue asumida como hipótesis (I). Para verificar la segunda analizamos la paridad de n. Si n es par, $\frac{n}{2}$ es entero y $1 \leq \frac{n}{2} \leq n$, luego $P(\frac{n}{2})$ es verdadera y por (II) $P(n)$ resulta verdadera como queremos. Si en cambio n es impar, $n+1$ es par y $\frac{n+1}{2} \leq n$ y así $P(\frac{n+1}{2})$ es verdadera por hipótesis. Luego, por (II), $P(n+1)$ es verdadera y por (III), $P(n)$ es verdadera como queríamos.

Ejemplo. Aca poner la cota media aritmetica vs media geometrica

5.2.5. Inducción doble ‡

El principio de inducción también permite probar enunciados en los que aparecen dos variables naturales. Consideremos, por ejemplo, la siguiente proposición:

$$2^{n+1}(m-1) > nm, \text{ para todo par } n, m \in \mathbb{N} \text{ con } m > 1.$$

En caso de ser verdadera, es posible probar esta proposicón por inducción. Como no hay sólo una variable, es necesario replantear el problema adecuadamente. Antes de mostrar como hacerlo, nos convenzamos de que es cierto. Primero probemos algunos pares n, m.

n	m	$2^{n+1}(m-1)$	nm	
2	2	8	4	✓
3	5	64	15	✓
7	4	192	28	✓
10	2	512	20	✓
1	15	56	15	✓
11	11	40.960	121	✓
9	32	31.744	288	✓

Parece que funciona bien.

Ahora probemos algunos pares más, pero de manera más organizada. Por ejemplo, elijamos un n y para ese n elijamos varios m distintos. Luego cambiemos el n y volvamos a elegir varios m distintos.

n	m	$2^{n+1}(m-1)$	nm	
2	2	8	4	✓
2	5	32	10	✓
2	8	56	16	✓
2	15	112	30	✓
2	21	160	42	✓
5	9	512	45	✓
5	10	576	50	✓
5	11	640	55	✓
5	12	704	60	✓
5	13	768	65	✓
5	14	832	70	✓
5	15	896	75	✓

Sigue funcionando bien. Podríamos seguir experimentando, sin embargo quizá ya sea suficiente para observar que para un n fijo, el comportamiento de $2^{n+1}(m-1)$ y nm es claro. Luego quizá sea fácil de probar esto por inducción.

Elijamos y fijemos entonces un n, digamos n_0. Y probemos, por inducción (corrida) en m que

$$2^{n_0+1}(m-1) > n_0 m, \text{ para todo } m > 1.$$

Si hacemos esto, como n_0 es arbitrario habremos probado la proposición para todo n y para todo m ($m > 1$).

- Si $m = 2$, debemos mostrar que $2^{n_0+1} > 2n_0$. Esto es equivalente a $2^{n_0}2 > 2n_0$ y también a $2^{n_0} > n_0$, hecho que ya probamos inmediatamente después de enunciar el principio de inducción en 5.2.1.
- Supongamos ahora que $2^{n_0+1}(m-1) > n_0 m$ y veamos que podes deducir que $2^{n_0+1}(m+1-1) > n_0(m+1)$ también vale. Como $2^{n_0+1} > n_0$ (como ya vimos), se sigue que

$$2^{n_0+1}(m-1) + 2^{n_0+1} > n_0 m + n_0$$

es decir

$$2^{n_0+1}m > n_0(m+1)$$

como queríamos.

Hemos terminado nuestra tarea.

Observación. En vez de fijar un n y hacer inducción en m, también se puede elegir y fijar un m_0 y hacer inducción en n. Puede ser que una de estas estrategias sea más conveniente que la otra.

Nota. En este caso que hemos desarrolado, una vez elegido n_0 pudimos probar la correspondiente proposición por inducción en m sin ninguna restricción sobre n_0. Esto fue posible pues apelamos a un resultado que ya conocíamos; sabíamos que $2^{n_0} > n_0$ para todo n_0. Si no hubiéramos sabido esto, en las dos instancias del proceso inductivo sobre m deberíamos haber usado la inducción sobre n. Más precisamente.

- Para $m = 2$, debemos probar que $2^{n_0+1} > 2n_0$ cualquiera sea n_0, es decir debemos probar que $2^{n+1} > 2n$ para todo n y esto lo hacemos por inducción en n.
- En el paso inductivo sobre m debemos probar que cualquiera sea n_0,

$$2^{n_0+1}(m-1) > n_0 m \quad \Rightarrow \quad 2^{n_0+1}m > n_0(m+1)$$

Ee decir debemos porbar que, si $m > 2$,

$$2^{n+1}(m-1) > nm \quad \Rightarrow \quad 2^{n+1}m > n(m+1)$$

para todo n. Esto también lo hacemos por inducción en n.

Proposición 5.8. *Aca induccion doble enunciada como las otras.*

Demostración. □

***

5.3. Definiciones recursivas

Iterar una operación o un proceso es una situación frecuente en todas las ciencias. Es común hacerlo en matemática y es fundamental en computación, por ejemplo. Detrás de esto están los números naturales. Un proceso iterativo es un proceso inductivo: para hacer una operación o proceso $n+1$ veces hay que hacerlo n veces primero y luego una vez más.

5.3.1. Sumatoria y productoria

En aritmética, podemos querer sumar o multiplicar muchos números, no sólo dos. Supongamos que tenemos n números reales $x_1, x_2, \ldots, x_n$. Podemos denotar a su suma como

$$x_1 + x_2 + x_3 + \cdots + x_n$$

y a su producto como

$$x_1 \cdot x_2 \cdot x_3 \cdots x_n.$$

Ahora, ¿cómo se suman y multiplican efectivamente estos n números? ¿Cómo entendemos lo que hemos escrito? Si tenemos que sumar tres números x_1, x_2 y x_3, escribimos

$$x_1 + x_2 + x_3$$

*** r: aca faltaria poner algunas estrategias como en [Johnson]

y entendemos, como ya dijimos, que sumamos dos de ellos y al resultado le sumamos el tercero, sin importarnos el orden en que lo hagamos, pues dadas la conmutatividad y asociatividad el resultado es siempre el mismo. Más formal sería escribir

$$(x_1 + x_2) + x_3.$$

Dado esto, podemos interpretar los puntos suspensivos en las definiciones más arriba cómo indicación implícita de lo que debemos hacer. Comenzar sumando $x_1 + x_2$ y luego sumar x_3, etcétera. Estamos frente a una definición recursiva o inductiva, en este caso implícita. A veces, esto es suficiente.

De todos modos, mostramos cómo definir formalmente esto con una definición recursiva explícita. Para esto introducimos primero nueva notación:

$$\sum_{i=1}^{n} x_i = x_1 + x_2 + x_3 + \cdots + x_n \tag{5.1}$$

$$\prod_{i=1}^{n} x_i = x_1 \cdot x_2 \cdot x_3 \cdots x_n \tag{5.2}$$

El símbolo $\sum$ se llama *sumatoria* y el símbolo $\prod$ se llama *productoria*[*]. Además $\sum_{i=1}^{n} x_i$ se lee "la suma de los equis-i, para i desde 1 hasta n" y $\prod_{i=1}^{n} x_i$ se lee "el producto de los equis-i, para i desde 1 hasta n". Esta notación para sumas y productos es simple y económica por lo que resulta útil y es entonces muy usada.

Definición. Dados n números reales $x_1, x_2, \ldots, x_n$ se definen recursivamente

$$\sum_{i=1}^{1} x_i = x_1 \qquad \text{y} \qquad \sum_{i=1}^{n} x_i = \Big(\sum_{i=1}^{n-1} x_i\Big) + x_n, \quad \forall n \geq 2$$

$$\prod_{i=1}^{1} x_i = x_1 \qquad \text{y} \qquad \prod_{i=1}^{n} x_i = \Big(\prod_{i=1}^{n-1} x_i\Big) \cdot x_n, \quad \forall n \geq 2$$

En la Sección 5.5 estudiamos en detalle las propiedades de la sumatoria y la productoria.

5.3.2. El factorial

El *factorial* de n es el producto de todos los naturales menores o iguales que n, es decir

$$n! = n \cdot (n-1) \cdot (n-2) \cdots 3 \cdot 2 \cdot 1$$

[*] Σ es la mayúscula de la letra griega sigma σ , que equivale a una "s" romana, por "suma"; y $\prod$ es la mayúscula de la letra griega pi π, que equivale a una "p", por "producto".

Por ejemplo

$$\begin{aligned}
1! &= 1,\\
2! &= 2\cdot 1 = 2\cdot 1! = 2\\
3! &= 3\cdot 2\cdot 1 = 3\cdot 2! = 6\\
4! &= 4\cdot 3\cdot 2\cdot 1 = 4\cdot 3! = 24\\
5! &= 5\cdot 4\cdot 3\cdot 2\cdot 1 = 5\cdot 4! = 120\\
6! &= 6\cdot 5\cdot 4\cdot 3\cdot 2\cdot 1 = 6\cdot 5! = 720\\
7! &= 7\cdot 6\cdot 5\cdot 4\cdot 3\cdot 2\cdot 1 = 7\cdot 6! = 5040\\
8! &= 8\cdot 7\cdot 6\cdot 5\cdot 4\cdot 3\cdot 2\cdot 1 = 8\cdot 7! = 40320
\end{aligned}$$

La definición recursiva formal es la siguiente:

Definición. Para todo $n\in\mathbb{N}$ se define el *factorial* de n, denotado $n!$, recursivamente por:

$$1! = 1 \qquad \text{y} \qquad (n+1)! = (n+1)n! \quad \text{para } n\geq 2.$$

Es conveniente definir $0! = 1$ (más adelante veremos porqué).

El doble factorial †

Muchas veces es útil usar el doble factorial para simplificar ciertas expresiones. El *doble factorial* (o *semifactorial*) de n, denotado $n!!$, es el producto de todos los naturales entre 1 y n, pero de la misma paridad que n; es decir

$$n!! = n(n-2)(n-4)\cdots \tag{5.3}$$

Si n es par, se tiene

$$n!! = \prod_{i=1}^{n/2}(2i) = n(n-2)\cdots 4\cdot 2$$

mientras que para n impar, se tiene

$$n!! = \prod_{i=1}^{(n+1)/2}(2i-1) = n(n-2)\cdots 3\cdot 1$$

Por ejemplo

$$7!! = 7\cdot 5\cdot 3\cdot 1, \qquad 8!! = 8\cdot 6\cdot 4\cdot 2$$

El factorial y el semifactorial están obviamente relacionados. Por ejemplo,

$$7!! = 7\cdot 5\cdot 3\cdot 1 = \frac{7!}{6!!}$$

y

$$8!! = 8\cdot 6\cdot 4\cdot 2 = (2\cdot 4)(2\cdot 3)(2\cdot 2)(2\cdot 1) = 2^4\cdot 4!$$

En general, es claro que si $n = 2k$ se tiene

$$(2k)!! = 2^k \cdot k!$$

y si n es impar se tiene

$$n!! = \frac{n!}{(n-1)!!}$$

Luego, si $n = 2k+1$, entonces vale

$$(2k+1)!! = \frac{(2k+1)!}{2^k \cdot k!}$$

de donde podemos escribir potencias de 2 en términos de factoriales y semifactoriales $2^k = (2k+1)!/(2k+1)!!k!$

5.3.3. La potenciación

Dado un número real a, podemos multiplicarlo por el mismo obteniendo como resultado $a \cdot a$; si al resultado lo multiplicamos de nuevo por a obtenemos $a \cdot a \cdot a$. Podemos continuar multipicando sucesivamente por a, n veces, para obtener la *potencia n-ésima* de a,

$$a^n = \underbrace{a \cdot a \cdots a}_{n}$$

La definición recursiva formal es la que sigue.

Definición. Dado un $a \in \mathbb{R}$, para todo $n \in \mathbb{N}$ se define la potencia n-ésima de a, denotada a^n, recursivamente por:

$$a^1 = a \qquad \text{y} \qquad a^{n+1} = a^n \cdot a \quad \text{para } n \geq 2.$$

Propiedades de las potencias

Para todo $x, y \in \mathbb{R}$ y $m, n \in \mathbb{N}$ valen

$$\begin{aligned} x^{m+n} &= x^m \cdot x^n \\ x^{mn} &= (x^m)^n = (x^n)^m \\ (xy)^n &= x^n \cdot y^n \end{aligned}$$

Es muy instructivo hacer la prueba de estas identidades por inducción y lo dejamos como ejercicio.

5.4. Sucesiones definidas por recurrencia

Una *sucesión* de números reales es una función de $\mathbb{N}$ en $\mathbb{R}$, digamos

$$a : \mathbb{N} \to \mathbb{R}$$

Dada una sucesión a, en general denotamos a_n en vez de $a(n)$ a la imagen de n por a y también denotamos $\{a_n\}_{n\in\mathbb{N}}$ en vez de $a : \mathbb{N} \to \mathbb{R}$ (es decir, identificamos la función con su imagen).

Hay sucesiones que se definen, cómo tantas otras funciones, por medio de alguna fórmula. Por ejemplo, $a_n = 2n^2 + 1$.

Hay otras que se definen de forma recursiva o inductiva. En este caso, un valor dado de la sucesión se define en término de los valores anteriores, por lo general el anterior o los dos anteriores. En símbolos,

$$a_n = f(a_1, a_2, \ldots, a_{n-1})$$

donde f es una cierta función que depende de $a_1, \ldots, a_{n-1}$. Por ejemplo, si cada término de la sucesión depende del anterior, si conocemos el primer valor de la sucesión, la conocemos toda.

El término a_n, que depende de $a_1, \ldots, a_{n-1}$, se llama *término general* de la sucesión y a_1 se llama *término inicial*.

Muchas veces, dada una sucesión definida recursivamente es posible hallar una fórmula cerrada para el término general n-ésimo (es decir, una expresión de a_n que dependa de n y no de los términos anteriores a_i, $1 \leq i \leq n-1$). Esto siempre es deseable por motivos obvios. Para calcular el n-ésimo término de la sucesióon, a_n, es preferible tener una fórmula que dependa de n, que tener que calcular a_1, con este a_2, con este a_3 y así hasta a_{n-1} para finalmente poder calcular a_n.

Ejemplos.

(1) $a_1 = 1$ y $a_n = a_{n-1} + 2$ para todo $n \geq 2$.

A partir de la recurrencia que la define y sabiendo que $a_1 = 1$, podemos calcular sucesivamente:

$$a_2 = a_1 + 2 = 1 + 2 = 3, \qquad a_3 = a_2 + 2 = 3 + 2 = 5,$$
$$a_4 = a_3 + 2 = 5 + 2 = 7, \qquad a_5 = a_4 + 2 = 7 + 2 = 9,$$

etcétera. Es claro que la sucesión $\{a_n\}$ es la sucesión de naturales impares, o sea

$$a_n = 2n - 1, \qquad n \geq 1$$

(compruebe esto por inducción).

(2) $b_1 = 1$ y $b_n = 2b_{n-1}$ para todo $n \geq 2$.

Es fácil calcular los primeros valores de la sucesión $\{b_n\}$:

$$b_2 = 2 \cdot 1 = 2, \qquad a_3 = 2 \cdot 2 = 4, \qquad a_4 = 2 \cdot 4 = 8, \qquad a_5 = 2 \cdot 8 = 16,$$

etcétera. A partir de estos resultados podemos arriesgar que la sucesión $\{b_n\}$ es la de las potencias de 2, comenzando con $1 = 2^0$. Más precisamente parece ser

$$b_n = 2^{n-1}$$

(compruebe esto por inducción).

(3) $c_1 = 0$ y $c_n = 2c_{n-1} + 1$ para todo $n \geq 2$.

Los primeros valores de esta sucesión son:

$$c_2 = 2 \cdot 0 + 1 = 1, \qquad c_3 = 2 \cdot 1 + 1 = 3, \qquad c_4 = 2 \cdot 3 + 1 = 7,$$
$$c_5 = 2 \cdot 7 + 1 = 15, \qquad c_6 = 2 \cdot 15 + 1 = 31, \qquad c_7 = 2 \cdot 31 + 1 = 63,$$

etcétera. Aunque quizá no sean suficientes los valores calculados, conjeturamos que $c_n = 2^{n-1} - 1$.

(4) $d_1 = 1$ y $d_n = d_{n-1} + n$ para todo $n \geq 2$.

Los primeros valores de d son:

$$d_2 = 1 + 2 = 3, \qquad d_3 = 3 + 3 = 6, \qquad d_4 = 6 + 4 = 10, \qquad d_5 = 10 + 5 = 15,$$

etcétera. En este caso no es tan fácil proponer una fórmula para d_n. Calcular más valores de d_n puede ayudar.

$$d_6 = 15 + 6 = 21, \quad d_7 = 21 + 7 = 28, \quad d_8 = 28 + 8 = 36, \quad d_9 = 36 + 9 = 45,$$

etcétera. Nosotros arriesgamos que $d_n = \frac{n(n+1)}{2}$.

(5) $e_1 = 1$ y $e_n = ne_{n-1}$ para todo $n \geq 2$.

La sucesión e_n comienza así:

$$e_2 = 2 \cdot 1 = 2; \quad e_3 = 3 \cdot 2 = 6; \quad e_4 = 4 \cdot 6 = 24; \quad e_5 = 5 \cdot 24 = 120; \quad etc.$$

Notamos que también podemos escribir:

$$e_2 = 2 \cdot 1; \quad e_3 = 3 \cdot 2 \cdot 1; \quad e_4 = 4 \cdot 3 \cdot 2 \cdot 1; \quad e_5 = 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1; \quad etc.$$

Esta última es la sucesión de los números factoriales, $\{e_n\} = \{n!\}$.

Observación. Si a la sucesión a_n le cambiamos el primer valor, es decir redefinimos a_1, toda la sucesión cambia, aun manteniendo la misma relación de recurrencia para el resto de sus valores. Si en vez tomar $a_1 = 1$, fijamos $a_1 = 2$, obtenemos la sucesión de naturales pares. Y si tomamos $a_1 = 3$, obtenemos la sucesión de naturales impares mayores que 2.

En el caso de la sucesión b_n, si fijamos $b_1 = 0$, resulta que $b_n = 0$ para todo n. En cambio de tomamos $b_1 = 2$, resulta que $b_n = 2^n$ para todo n. Esta última afirmación, tan clara, requeriría una demostración y una por inducción parace ser adecuada. Dejamos este caso como ejercicio para el lector.

En los casos de las sucesiones c_n y d_n hemos afirmado que:

- $c_n = 2^{n-1} - 1$.
- $d_n = \frac{n(n+1)}{2}$.

Probemos esto por inducción.

- Sucesión $\{c_n\}$.

Por definición $c_1 = 0$ y $2^0 - 1 = 0$. Luego la fórmula evaluada en $n = 1$ es igual a c_1. Ahora $c_{n+1} = 2c_n + 1$ y por hipótesis inductiva resulta

$$c_{k+1} = 2c_k + 1 = 2(2^{k-1} - 1) + 1 = 2^k - 2 + 1 = 2^k - 1$$

Así la fórmula evaluada en $k + 1$ coincide con c_{k+1}. Por lo tanto $c_n = 2^{n-1} - 1$ para todo $n \in \mathbb{N}$.

- Sucesión $\{d_n\}$.

Por definición $d_1 = 1$ y $1 \cdot (1 + 1)/1 = 1$. Luego la fórmula evaluada en $n = 1$ es igual a d_1. Ahora $d_{n+1} = d_n + (n + 1)$ y por hipótesis inductiva resulta

$$d_{k+1} = \tfrac{1}{2}k(k + 1) + (k + 1) = (k + 1)(\tfrac{k}{2} + 1) = \tfrac{1}{2}(k + 1)(k + 2)$$

Por lo tanto $d_n = \frac{n(n+1)}{2}$ para todo $n \in \mathbb{N}$.

Ejemplo (Torres de Hanoi)**.** Este es un juego de mesa clásico, solitario, inventado por el matemático Eduard Lucas en 1883 (también se lo conoce como torres de Brahma o torres de Lucas). Consta de 3 clavijas y de n discos de distintos tamaños. En la posición inicial, todos los discos se encuentran en la misma clavija, ordenados de mayor (disco n) a menor (disco 1) desde abajo. En la figura se muestra un juego con 7 discos.

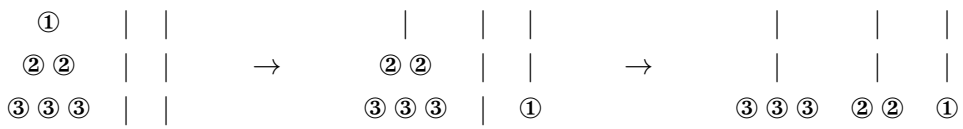
El juego consiste en mover la pila de n discos de una clavija a otra cualquiera sujeto a las siguientes reglas:

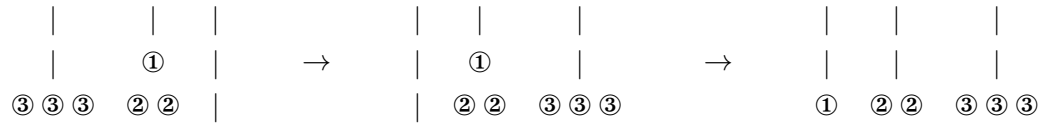
(1) Se puede mover de a un disco por vez (el superior de alguna pila),

(2) Ningún disco puede ser colocado sobre otro de menor tamaño (diámetro).

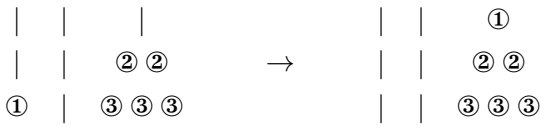
Pregunta. ¿Cuál es el número mínimo de movimientos, digamos T_n, necesarios para resolver el juego con n discos?

Estudiemos los casos más simples, para los primeros valores de n. Es fácil chequear que $T_0 = 0$, $T_1 = 1$, $T_2 = 3$ y $T_3 = 7$. Por ejemplo, para el caso de 3 discos, la secuencia sería





y finalmente



Pero, ¿cuánto vale T_n? Para responder esto, primero obtendremos una recurrencia. En algún momento, deberemos mover el dico n. Para mover el disco n, necesitamos mover primero la torre de $n-1$ discos a alguna clavija. Sabemos que el mínimo número de movidas para lograr esto es T_{n-1}. Luego tenemos una movida para llevar el disco n de la clavija en que se encuentra a la que esta libre y, finalmente, otras T_{n-1} movidas para llevar la torre de $n-1$ discos a la posición final arriba del disco n. En total, hemos visto que

$$T_n = 2T_{n-1} + 1 \tag{5.4}$$

De esta manera, tenemos los que los primeros valores de T_n son

n	0	1	2	3	4	5	6	7
T_n	0	1	3	7	15	31	63	127

Pareciera ser que

$$T_n = 2^n - 1$$

Ahora podemos probar esto por inducción usando la recurrencia anterior (5.4). En efecto, el paso inicial ya vimos que vale y el paso inductivo es ahora obvio

$$T_{n+1} = 2T_n + 1 = 2(2^n - 1) + 1 = 2^{n+1} - 1$$

De este modo probamos que el juego con n discos puede ser resuelto en $2^n - 1$ pasos. ◊

Nota. el acertijo de Reve es una variación de las torres de Hanoi, con las mismas reglas, pero usando 4 clavijas (propuesta por Henry Dudeney en 1907). El número mínimo de movidas para resolver el acertijo con n-discos es… ¡desconocido! aunque se conjetura que este número es

$$R(n) = \left(\sum_{i=1}^{k} i\, 2^{i-1}\right) - \left(\tfrac{k(k+1)}{2} - n\right) 2^{k-1}$$

donde k es el menor entero tal que $n \leq \frac{k(k+1)}{2}$.

Otras sucesiones recursivas

Consideremos la sucesión $\{a_n\}$ definida por:

$$a_1 = 3, \qquad a_2 = 5, \qquad a_n = 3a_{n-1} - 2a_{n-2} \quad \forall n \geq 3$$

Esta sucesión está definida por recurrencia en un sentido más amplio que las que consideramos antes. En este caso la definición del término a_n involucra los dos términos anteriores a_{n-1} y a_{n-2}, y no sólo el inmediato anterior, a_{n-1}, como antes.

Tenemos

$$\begin{aligned}
a_3 &= 3a_2 - 2a_1 = 3 \cdot 5 - 2 \cdot 3 = 15 - 6 = 9 \\
a_4 &= 3a_3 - 2a_2 = 3 \cdot 9 - 2 \cdot 5 = 27 - 10 = 17 \\
a_5 &= 3a_4 - 2a_3 = 3 \cdot 17 - 2 \cdot 9 = 51 - 18 = 33 \\
a_6 &= 3a_5 - 2a_4 = 3 \cdot 33 - 2 \cdot 17 = 99 - 34 = 65 \\
a_7 &= 3a_6 - 2a_5 = 3 \cdot 65 - 2 \cdot 33 = 195 - 66 = 129
\end{aligned}$$

Mirando los términos de a_n que calculamos, podemos conjeturar una fórmula:

$$a_n = 2^n + 1, \quad \text{para todo } n. \tag{5.5}$$

Pregunta. ¿cómo probamos que esto es cierto?

Respuesta. ¡Por inducción!

- Para $n = 1$ tenemos que $a_n = a_1 = 3$ y $2^n + 1 = 2^1 + 1 = 3$. El primer paso está cumplido.
- Supongamos ahora que $a_k = 2^k + 1$ y tratemos de ver que entonces $a_{k+1} = 2^{k+1} + 1$. Tenemos que, por definición de a_n, $a_{k+1} = 3a_k - 2a_{k-1}$. La hipótesis inductiva nos dice cuánto es a_k, pero no cuánto es a_{k-1}. La prueba por inducción se trabó.

  Volvamos al principio. Pudimos calcular a_3; es cierto que para ello necesitamos además de a_2 también a_1. Y para calcular a_4 usamos no sólo a_3 sino también a_2. Esto mismo ocurrió en todos los casos; simpre necesitamos los dos valores previos, y siempre los teníamos ya calculados.

  Retomemos nuestra prueba por inducción volviendo a calcular a_{k+1}, pero esta vez aceptemos que ya tenemos calculado los dos valores previos y que ambos satisfacen la fórmula (5.5). Este es exactamente el contexto de la inducción fuerte. En este caso:

$$\begin{aligned}
a_{k+1} &= 3a_k - 2a_{k-1} \\
&= 3(2^k + 1) - 2(2^{k-1} + 1) \\
&= 3 \cdot 2^k + 3 - 2^k - 2 \\
&= 2 \cdot 2^k + 1 = 2^{k+1} + 1
\end{aligned}$$

  BINGO !! Asumiendo una doble hipótesis inductiva, completamos el paso inductivo. Esto permite desencadenar el proceso en cadena, una vez que arranque. Para arrancar, necesitamos saber que los dos primeros términos satisfacen la fórmula (5.5). Esto es así en este caso. Por lo tanto, gracias al principio de inducción fuerte, hemos terminado.

Sucesiones definidas por recursión doble

Consideremos la siguiente función F de dos variables naturales definida recursivamente por una recursión doble:

$$\begin{aligned} F(1,1) &= 2 \\ F(m+1,n) &= F(m,n) + 2(m+n) \\ F(m,n+1) &= F(m,n) + 2(m+n-1) \end{aligned}$$

5.5. Propiedades de la sumatoria y la productoria

En la Sección 5.3 definimos la sumatoria y la productoria. Ahora en esta sección mostramos varias de sus propiedades que permiten hacer un uso eficiente de ellas. Para ello es necesario aprender a manipularlas como objetos en sí mismas.

En las definiciones recursivas

$$\sum_{i=1}^{n} x_i = \Big(\sum_{i=1}^{n-1} x_i\Big) + x_n \qquad\qquad \prod_{i=1}^{n} x_i = \Big(\prod_{i=1}^{n-1} x_i\Big) \cdot x_n$$

aparecen separados el último sumando y el último factor. A veces es útil separar el primer sumando o el primer factor y escribir

$$\sum_{i=1}^{n} x_i = x_1 + \sum_{i=2}^{n} x_i \qquad\qquad \prod_{i=1}^{n} x_i = x_1 \cdot \prod_{i=2}^{n} x_i$$

Otras veces conviene separar un término cualquiera, por ejemplo el j-ésimo,

$$\sum_{i=1}^{n} x_i = x_j + \sum_{\substack{i=1 \\ i\neq j}}^{n} x_i \qquad\qquad \prod_{i=1}^{n} x_i = x_j \cdot \prod_{\substack{i=1 \\ i\neq j}}^{n} x_i$$

En algunos casos particulares, es posible calcular explícitamente y dar un resultado conciso para la suma o el producto de los números $x_1, x_2, \ldots, x_n$ dados. Por ejemplo, si $x_1 = x_2 = \cdots = x_n = a$, entonces

$$\sum_{i=1}^{n} x_i = na \qquad \text{y} \qquad \prod_{i=1}^{n} x_i = a^n$$

En particular, $\sum_{i=1}^{n} 1 = n$ y $\prod_{i=1}^{n} 1 = 1$. Si $x_1 = 1$, $x_2 = 2$, …, $x_n = n$, entonces

$$\sum_{i=1}^{n} x_i = 1 + 2 + \cdots + n \qquad \text{y} \qquad \prod_{i=1}^{n} x_i = 1 \cdot 2 \cdots n = n!$$

Con más generalidad podemos sumar o multiplicar una cantidad finita de números indexada por un conjunto distinto del conjunto $\{1, 2, \ldots, n\}$. Por ejemplo, sea $I = \{*, \alpha, b\}$

y sean $x_* = 2$, $x_\alpha = \frac{1}{2}$ y $x_b = -1$. Entonces para escribir la suma de estos 3 números, escribimos

$$\sum_{i\in I} x_i = x_* + x_\alpha + x_b = 2 + \tfrac{1}{2} - 1 = \tfrac{3}{2}$$

y para escribir su producto escribimos

$$\prod_{i\in I} x_i = x_* \cdot x_\alpha \cdot x_b = 2 \cdot \tfrac{1}{2} \cdot (-1) = -1$$

En general, si I es un conjunto **finito** y para cada $i \in I$ tenemos $x_i \in \mathbb{R}$, escribimos

$$\begin{aligned} \sum_{i\in I} x_i &= \text{suma de todos los } x_i \text{ con } i \in I \\ \prod_{i\in I} x_i &= \text{producto de todos los } x_i \text{ con } i \in I \end{aligned}$$

También podemos sumar o multiplicar todos los elementos de un conjunto finito de números reales dado, sin necesidad de que éste esté indexado. Si $X \subseteq \mathbb{R}$ es finito, escribimos

$$\begin{aligned} \sum_{x\in X} x &= \text{suma de todos los elementos de } X \\ \prod_{x\in X} x &= \text{producto de todos los elementos de } X \end{aligned}$$

El orden en que hagamos la suma o el producto es irrelevante. La asociatividad y conmutatividad de la suma y el producto aseguran esto. Sin embargo, una demostración formal de este hecho es más engorrosa de lo que uno imagina a primera vista.

Convención. Si $X = \varnothing$, convenimos que

$$\sum_{x\in X} x = 0 \qquad \text{y} \qquad \prod_{x\in X} x = 1$$

En particular si $I = \varnothing$, $\sum_{i\in I} x_i = 0$ y $\prod_{i\in I} x_i = 1$.

Si $I = \{1, 2, \ldots, n\}$, tenemos que

$$\sum_{i=1}^{n} x_i = \sum_{i\in I} x_i \qquad\qquad \prod_{i=1}^{n} x_i = \prod_{i\in I} x_i$$

Extendemos estas definiciones para el caso en que

$$I = [\![a, b]\!] := \{i \in \mathbb{Z} : \ a \le i \le b\}$$

definiendo

$$\sum_{i=a}^{b} x_i = \sum_{i\in I} x_i = \sum_{i\in[\![a,b]\!]} x_i$$
$$\prod_{i=a}^{b} x_i = \prod_{i\in I} x_i = \prod_{i\in[\![a,b]\!]} x_i$$

En este caso, a y b son los *índices de sumación*.

Convenimos también que si $b < a$, entonces $\sum_{i=a}^{b} x_i = 0$ y $\prod_{i=a}^{b} x_i = 1$ (de hecho, esto coincide con lo dicho previamente ya que en este caso $[\![a,b]\!] = \varnothing$).

5.5.1. Propiedades básicas

Algunas propiedades básicas de la sumatoria y la productoria que se siguen directamente de la definición y que usaremos frecuentemente son:

- $\sum_{i\in I} x_i = \sum_{j\in I} x_j$ y $\prod_{i\in I} x_i = \prod_{j\in I} x_j$.
- $\sum_{i\in I} 1 = |I|$ y $\prod_{i\in I} 1 = 1$.
- Si $|I| = n$, entonces $\sum_{i\in I} x = nx$ y $\prod_{i\in I} x = x^n$.
- $\sum_{i\in I} ax_i + by_i = a\sum_{i\in I} x_i + b\sum_{i\in I} y_i$.
- $\prod_{i\in I} x_i y_i = \prod_{i\in I} x_i \prod_{i\in I} y_i$.

Los números x_i a sumar no son en general arbitrarios, por el contrario la mayoría de la veces vienen dados por alguna fórmula que depende del índice de sumación i. Por ejemplo:

- Si $x_i = i$, entonces
$$\sum_{i=1}^{n} x_i = \sum_{i=1}^{n} i$$
es la suma de los naturales entre 1 y n.
- Si $x_i = i^2$, entonces
$$\sum_{i=1}^{n} x_i = \sum_{i=1}^{n} i^2$$
es la suma de los cuadrados de los naturales entre 1 y n.

Ahora, si queremos describir usando el símbolo de sumatoria la suma de los primeros n impares, debemos encontrar una fórmula que describa los impares entre 1 y n. Esto no es difícil y hay más de una manera de hacerlo:

$$\sum_{i=1}^{n} 2i-1 = \sum_{i=0}^{n-1} 2i+1 = \text{suma de los primeros } n \text{ impares.}$$

5.5.2. Cambios de variable

Dados un conjunto finito de índices I y un conjunto de números reales indexados por I, digamos $\{x_i \in \mathbb{R} : i \in I\}$, la suma $\sum_{i\in I} x_i$ se puede hacer de muchas maneras. Para cada *parametrización* del conjunto I corresponde una forma de hacer la suma. Parametrizar el conjunto I es dar una biyección de otro conjunto J en I, digamos σ. Siendo $\sigma : J \to I$ una biyección se sigue que J e I tienen el mismo cardinal. Luego, tenemos

$$\sum_{i\in I} x_i = \sum_{j\in J} x_{\sigma(j)}$$

En la práctica muchas veces se elije J como el conjunto $\{1, 2, \ldots, n\}$, con $n = |I|$. En este caso escribimos

$$\sum_{i=1}^{n} x_i = \sum_{j=1}^{n} x_{\sigma(j)}.$$

Estos cambios también se llaman *cambio de variables* y son muy comunes.

Ejemplos. Veamos algunos de los cambios de variables mas usuales.

(1) $\displaystyle\sum_{i=1}^{n} x_i = \sum_{j=0}^{n-1} x_{j+1}.$

En este caso $\sigma(j) = j + 1$. Cambian los índices de sumación porque cambian los conjuntos ya que $\sigma : J \to I$ con $J = \{1, 2, \ldots, n\}$ e $I = \{0, 1, \ldots, n-1\}$.

(2) $\displaystyle\sum_{i=0}^{n} x_i = \sum_{j=1}^{n+1} x_{j-1}.$

Aquí $\sigma(j) = j - 1$ donde $\sigma : J \to I$ con $J = \{0, 1, \ldots, n-1\}$ e $I = \{1, 2, \ldots, n\}$.

(3) $\displaystyle\sum_{i=1}^{n} x_i = \sum_{j=1}^{n} x_{n+1-j}.$

En este caso $\sigma(j) = n - j + 1$ con $J = I = \{1, 2, \ldots, n\}$, pero ha sido parametrizado de mayor a menor, siendo el primer sumando x_n, el segundo x_{n-1} y el último x_1. Es decir $\displaystyle\sum_{i=1}^{n} x_i = x_1 + x_2 + \cdots + x_n$ mientras que $\displaystyle\sum_{i=1}^{n} x_{n+1-j} = x_n + x_{n-1} + \cdots + x_1$. ◊

5.5.3. Sumas y productos dobles

Una situación que se encuentra usualmente es la de sumar o multiplicar sobre un conjunto de números que está descripto o parametrizado usando más de un índice.

Por ejemplo, cuando el conjunto de índices A es el producto de dos conjuntos $I \times J$ y tenemos una familia de números reales indexados por A, digamos $\{x_{i,j} : (i,j) \in I \times J\}$ y nos interesa calcular

$$\sum_{I\times J} x_{i,j} \qquad \text{ó} \qquad \prod_{I\times J} x_{i,j}$$

Otro caso de interés es cuando uno de los índices depende linealmente del otro, por ejemplo

$$A = \{(i,j) : a \leq i \leq b, 0 \leq j \leq i\}$$

• Sumas y productos rectangulares

Analicemos con cuidado el siguiente ejemplo de *suma rectangular* y *producto rectangular*. Supongamos que

$$A = \{(i,j) :\ 1 \leq i \leq 8,\ 1 \leq j \leq 5\}$$

y consideremos la colección de números $x_{i,j} = i$ con $(i,j) \in A$. El conjunto A es el producto cartesiano

$$A = [\![1,8]\!] \times [\![1,5]\!]$$

y el conjunto de números $\{x_{i,j}\}$ es

——— DIBUJO ———-

Son en total 40 números; ni tantos ni tan pocos para sumarlos y multiplicarlos a todos. Cada uno puede hacerlo como más le guste. La suma y el producto de todos ellos es

$$\sum_{(i,j)\in A} x_{i,j} = \qquad\qquad \prod_{(i,j)\in A} x_{i,j} =$$

Veamos como hacer esta suma y este producto de manera sistemática, para poder aplicarlo a otros casos similares. El quid para hacer estas operaciones de manera eficiente y práctica está en cómo organizamos la suma o el producto, en qué orden hacemos las operaciones. De las muchas maneras de hacerlo hay algunas más convenientes que otras. Los dibujos muestran dos maneras, muy naturales, de organizar la suma y el producto.

——— DIBUJO ———

En este caso sumamos o multiplicamos los términos de cada columna y luego sumamos o multiplicamos estos resultados parciales. Como en cada columna los números son iguales resulta muy fácil hacer las sumas o productos y todo se reduce la suma o producto final.

——— Dibujo ———-

En este caso sumamos o multiplicamos los términos de cada fila y luego sumamos o multiplicamos estos resultados parciales. Como las filas son todas iguales los resultados parciales son todos iguales y la suma o producto final es muy fácil de calcular. Así hay una sola suma o producto no trivial.

Para escribir esto debemos hacer exactamente lo que dijimos en cada caso.

• Por columnas

En el primer caso comenzamos considerando las columnas; una columna de A es el subconjunto de puntos con una misma primera coordenada. La primera columna de A es

$$\text{primera columna} = A^1 = \{(i,j) \in A : \ i = 1\} = \{(1,j) : \ 1 \leq j \leq 5\}$$

y la quinta columna de A es

$$\text{quinta columna} = A^5 = \{(i,j) \in A : \ i = 5\} = \{(5,j) : \ 1 \leq j \leq 5\}$$

En este caso sumamos cada una de las columnas, desde la primera hasta la octava, esto es

$$\sum_{j=1}^{5} x_{1,j} = 5 \times 1 = 5, \quad \sum_{j=1}^{5} x_{2,j} = 5 \times 2 = 10, \quad \ldots \quad \sum_{j=1}^{5} x_{8,j} = 5 \times 8 = 40$$

y luego sumamos todos estas sumas parciales:

$$\sum_{i=1}^{8} \sum_{j=1}^{5} x_{i,j} = 5 + 10 + 15 + 20 + 25 + 30 + 35 + 40 = 180$$

Así resulta que

$$\sum_{(i,j)\in A} x_{i,j} = \sum_{i=1}^{8} \sum_{j=1}^{5} x_{i,j} = 180$$

Análogamente

$$\begin{aligned} \prod_{(i,j)\in A} x_{i,j} = \prod_{i=1}^{8} \prod_{j=1}^{5} x_{i,j} &= 1^5 \times 2^5 \times 3^5 \times 4^5 \times 5^5 \times 6^5 \times 7^5 \times 8^5 \\ &= 1 \times 32 \times 243 \times 1024 \times 1875 \times 7776 \times 17367 \times 32768 \\ &= \end{aligned}$$

• Por filas

En el segundo caso comenzamos considerando las filas; una fila de A es el subconjunto de puntos con una misma segunda coordenada. La primera fila de A es

$$\text{primera fila} = \{(i,j) \in A : \ j = 1\} = \{(i,1) : \ 1 \leq i \leq 8\}$$

y la tercera fila de A es

$$\text{tercera fila} = \{(i,j) \in A : \ j = 3\} = \{(i,3) : \ 1 \leq i \leq 8\}$$

En este caso sumamos cada una de las filas, desde la primera hasta la quinta, esto es

$$\sum_{i=1}^{8} x_{i,1} = 1{+}2{+}\cdots{+}8 = 36, \quad \sum_{i=1}^{8} x_{i,2} = 1{+}2{+}\cdots{+}8 = 36, \quad \ldots \quad \sum_{i=1}^{8} x_{i,5} = 1{+}2{+}\cdots{+}8 = 36$$

y luego sumamos todos estas sumas parciales:

$$\sum_{j=1}^{5}\sum_{i=1}^{8} x_{i,j} = 36 \times 5 = 180$$

Así resulta, como ya sabemos, que

$$\sum_{(i,j)\in A} x_{i,j} = \sum_{j=1}^{5}\sum_{i=1}^{8} x_{i,j} = 180$$

Análogamente

$$\begin{aligned}\prod_{(i,j)\in A} x_{i,j} = \prod_{j=1}^{5}\prod_{i=1}^{8} x_{i,j} &= (1\times 2\times\cdots\times 8)^5 = \\ &= 40320^5 =\end{aligned}$$

En general, dada una colección finita de números $\{x_{i,j} : (i,j) \in I \times J\}$ indexada por un producto cartesiano $I \times J$, es decir un rectángulo, la suma y el producto de ellos se puede hacer de cualquiera de las dos formas anteriores; comenzando por columnas o por filas. Es decir

$$\sum_{(i,j)\in I\times J} x_{i,j} = \sum_{i\in I}\sum_{j\in J} x_{i,j} = \sum_{j\in J}\sum_{i\in J} x_{i,j}$$

y también

$$\prod_{(i,j)\in I\times J} x_{i,j} = \prod_{i\in I}\prod_{j\in J} x_{i,j} = \prod_{j\in J}\prod_{i\in J} x_{i,j}$$

En particular, si la naturaleza de $x_{i,j}$ es tal que la dependencia en i y la dependencia en j pueden ser separadas, digamos que

$$x_{i,j} = f(i)g(j)$$

donde f, g son ciertas funciones, entonces

$$\sum_{I\times J} x_{i,j} = \sum_{i\in I} f(i)\sum_{j\in J} g(j) = \sum_{j\in J} g(j)\sum_{i\in I} f(i)$$

y lo mismo para el producto.

Ejemplo. Sean $x_1, x_2, \ldots, x_{105}$ números reales dados y sean $y_{i,j} = (-1)^j x_i$ con $33 \le i \le 1048$ y $1 \le j \le 105$. ¿Cuánto vale la suma de todos los $y_{i,j}$, es decir

$$\sum_{(i,j)\in I\times J} y_{i,j}$$

con $I = [\![33, 1048]\!]$ y $J = [\![1, 105]\!]$?

Para evaluar la suma comenzamos sumando por columnas; así

$$\sum_{(i,j)\in I\times J} y_{i,j} = \sum_{i\in I}\sum_{j\in J}(-1)^j x_i = \sum_{i\in I} x_i \sum_{j\in J}(-1)^j$$

Ahora la suma $\sum_{j\in J}(-1)^j$ es una suma de 1's y -1's y como J tiene $1048-33+1=1016$ elementos, esta suma es igual a 0, siempre. Luego tenemos que

$$\sum_{(i,j)\in I\times J} y_{i,j} \quad = \quad \sum_{i\in I} x_i \sum_{j\in J}(-1)^j = \sum_{i\in I} x_i \cdot 0 = \sum_{i\in I} 0 = 0$$

Notar que la suma no pendende de los x_i's y notar también que si comenzaramos sumando por filas nos encontraríamos con la suma de todos los x_i's, que no conocemos pues ni siquiera conocemos a los x_i's! ◊

• SUMAS Y PRODUCTOS TRIANGULARES

Analizamos ahora un caso de sumas y productos dobles en el que el conjunto de índices, o dominio de la suma o el producto, es un triángulo en vez de un rectángulo como en el caso anterior.

Veamos como sumar y multiplicar los números del dibujo

——- DIBUJO——-

El triángulo tiene 8 números en la base o primera fila y 8 en la altura o primera columna. En total hay 36 números que sumar y multiplicar.

El conjunto de índices, que no es un prodcuto cartesiano, es

$$A = \{(i,j) :\ 1\le i\le 8,\ 1\le j\le i\}$$

y la suma y el producto que queremos calcular son

$$\sum_A x_{i,j} \qquad\qquad \sum_A x_{i,j}$$

donde $x_{i,j}=j$. Entonces tenemos que

$$\sum_A x_{i,j} = \sum_{i=1}^{8}\sum_{j=1}^{i} j \qquad \text{y} \qquad \prod_A x_{i,j} = \prod_{i=1}^{8}\prod_{j=1}^{i} j$$

Las sumas y productos parciales, con índice j, son las sumas y productos de las columnas.

—- DIBUJO —- Resulta que

$$\sum_A x_{i,j} = \sum_{i=1}^{8}\sum_{j=1}^{i} j = \qquad \text{y} \qquad \prod_A x_{i,j} = \prod_{i=1}^{8}\prod_{j=1}^{i} j =$$

Ahora también podemos hacer estas operaciones comenzando por filas.

5.6. Identidades con sumas y sumas sumables

Una vez que hemos entendido como escribir ciertas sumas, ahora nos toca sumar. Esto es encontrar fórmulas que den el resultado final de sumas largas, con n sumandos. A pesar de que en general esto no es posible, hay algunos casos importantes que aparecen naturalemnte en los que sí es posible. En esta sección estudiamos estos casos.

5.6.1. Suma de enteros consecutivos

Comenzamos sumando los primeros n naturales. Esto es, queremos conocer el resultado de la suma

$$\sum_{i=1}^{n} i = 1 + 2 + 3 + \cdots + n$$

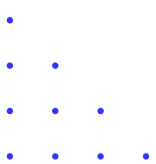
para todo n, si es posible. Una buena respuesta satisfactoria es una fórmula en términos de n. Hagamos algunos cálculos.

- $n = 1 \longrightarrow \sum_{i=1}^{1} i = 1.$
- $n = 2 \longrightarrow \sum_{i=1}^{2} i = 1 + 2 = 3.$
- $n = 3 \longrightarrow \sum_{i=1}^{3} i = 1 + 2 + 3 = 6.$
- $n = 4 \longrightarrow \sum_{i=1}^{4} i = 1 + 2 + 3 + 4 = 10.$
- $n = 5 \longrightarrow \sum_{i=1}^{5} i = 1 + 2 + 3 + 4 + 5 = 15.$

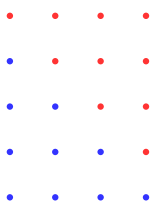
¿Hay alguna fórmula que describa estos resultados? ¿La podremos encontrar? Ambas preguntas tienen respuesta afirmativa. Mientras que disponemos de la inducción como herramienta para probar que una tal fórmula es correcta, no disponemos de un método para encontrarla. A continuación mostramos dos maneras ingeniosas de encontrar la respuesta, que luego no tendremos problemas en probar por inducción.

- Gráficamente

La suma $1 + 2 + 3 + 4$ puede representarse gráficamente como

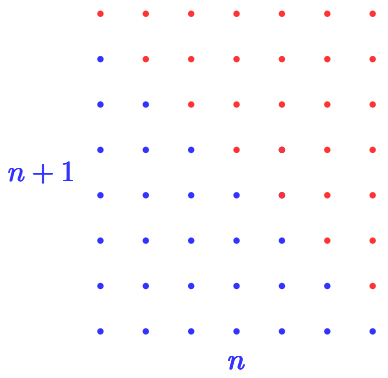


Para contar esta cantidad de puntos agregamos un "triángulo" del mismo tipo arriba de modo de obtener un rectángulo de 4×5 puntos



Luego, el número de puntos azules (triángulo inferior 4×4) es igual a la mitad del número total de puntos, o sea $\frac{4\cdot 5}{2} = 10$.

En general, para calcular $1+2+3+\cdots+n$ hacemos lo mismo.



Luego, conjeturamos que $1+2+\cdots+(n-1)+n = \frac{1}{2}n(n+1)$.

- A là Gauss

Para calcular la suma $1+2+3+4+5+6+7+8+9+10$ de los primeros 10 naturales, podemos hacer lo siguiente

$$(1+10)+(2+9)+(3+8)+(4+7)+(5+6)$$

Es decir, organizar la suma total en una suma de parejas, todas con igual suma parcial. Para saber el resultado sólo hay que saber cuántas parejas hay, o sea, cuántas sumas de la forma

$$i+(10-i+1)$$

hay. En este caso, son 5 (la primera es $1+10$ y la última es $5+6$) Como conclusión resulta que la suma buscada es igual a $11\times 5 = 55$.

Si hacemos lo mismo para calcular la suma $1+2+\cdots+n$, el resultado es igual a la suma de cada pareja, en este caso $n+1$, por la cantidad de parejas. Si n es par hay $\frac{n}{2}$ parejas y entonces resulta que

$$1+2+\cdots+n = (n+1)\cdot\tfrac{n}{2} = \tfrac{n(n+1)}{2}$$

Ahora si n es impar, no podemos formar parejas con todos los sumandos; el sumando central no tiene compañero. Este es $(n+1)/2$. Con el resto de los sumando se forman $(n-1)/2$ parejas. Así resulta que

$$1+2+\cdots+n = \tfrac{(n+1)(n-1)}{2} + \tfrac{n+1}{2} = \tfrac{(n+1)(n-1)+(n+1)}{2} = \tfrac{n(n+1)}{2}$$

Observamos que ya sea n par o impar la fórmula obtenida es la misma. Esta a su vez coincide con la obtenida graficamente.

Nota histórica. Cuenta la leyenda, que en el año 1787, cuando Carl Friedrich Gauss tenía apenas 10 años, un alboroto en el aula del colegio provocó que el maestro J. B. Büttner enojado, pidiera a los alumnos que sumaran todos los números del 1 al 100, creyendo que el castigo sería tenerlos a todos un buen rato ocupados.

Al rato nomás, Gauss se levantó del pupitre, y le entregó el resultado de la suma al profesor: 5050. El profesor, asombrado y seguramente creyendo que su alumno había puesto un número arbitrariamente, se dispuso él mismo a hacer la interminable suma. Al cabo de un buen rato, comprobó que el resultado de "Carlitos" era correcto.

¿Como hizo Gauss para resolver la suma en tan pocos minutos? Para hacer la suma $1+2+3+4+5+6+\cdots+97+98+99+100$ observó primero la secuencia de números. Hábilmente se dió cuenta de que la suma del primero con el último, el segundo con el penúltimo, y así sucesivamente, era siempre la misma:

$$1+100 = 2+99 = 3+98 = \cdots = 49+52 = 50+51 = 101.$$

Luego, como entre el número 1 y el 100 hay 50 pares de números, solo restaba multiplicar por 50 el resultado obtenido $50 \cdot 101 = 5050$. Bazinga!

En internet se pueden encontrar innumerables versiones distintas recopiladas de la literatura de esta interesante anécdota con sus respectivas citas.

Proposición 5.9. *Para todo $n \in \mathbb{N}$,*

$$\sum_{i=1}^{n} i = \tfrac{n(n+1)}{2}$$

Demostración. La haremos por inducción. Sea $P(n)$ la fórmula $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$.

- Paso inicial: Si $n = 1$, $\sum_{i=1}^{1} i = 1$ y $\frac{1(1+1)}{2} = 1$, luego coinciden.
- Paso inductivo: Supongamos ahora que $\sum_{i=1}^{k} i = \frac{k(k+1)}{2}$ (o sea, $P(k)$ es verdadero).

Queremos ver que $\sum_{i=1}^{k+1} i = \frac{(k+1)(k+2)}{2} = \frac{1}{2}(k^2+2k+2)$ (o sea, $P(k+1)$ es verdadero). Luego tenemos que

$$\sum_{i=1}^{k+1} i = \Big(\sum_{i=1}^{k} i\Big) + (k+1)$$

Por hipótesis inductiva,

$$\sum_{i=1}^{k+1} i = \tfrac{1}{2}k(k+1) + (k+1) = \tfrac{1}{2}\{k(k+1) + 2(k+1)\} = \tfrac{(k+1)(k+2)}{2}$$

Por lo tanto $\sum_{i=1}^{n+1} i = \frac{(k+1)(k+2)}{2}$ y la proposición queda probada. □

Nota. El *n-ésimo número triangular* se define como $T_n = \frac{n(n+1)}{2}$. Hemos visto que estos números aparecen como el término general de la sucesión definida recursivamente por

$d_1 = 1$ y $d_n = d_{n-1} + n$ para $n \geq 2$. También vimos que la suma de los primeros n naturales está dada por estos números. Es decir, tenemos que

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2} = T_n = d_n$$

Está claro ahora que si queremos conocer la suma de los primeros 36 naturales, la respuesta es $\sum_{i=1}^{36} i = \frac{1}{2}(36 \cdot 37) = 18 \cdot 37 = 666$. Y la de los primeros 1000 naturales es igual a $\frac{1}{2}(1000 \cdot 1001) = 500 \cdot 1001 = 500.500$.

Ahora, ¿cuál es la suma de los naturales desde el 32 hasta el 100 inclusive? ¿Necesitamos encontrar y probar nuevas fórmulas para sumas que comiencen en 32? Y si luego quiseramos conocer la suma de todos los enteros comenzando en -12 y hasta 51 inclusive, ¿cómo haríamos? La buena noticia es que la fórmula que hemos probado es suficiente para responder a todas estas preguntas.

Ejemplos.

(1) La suma de todos los naturales de 32 a 100 inclusive. Aquí restamos

$$\sum_{i=32}^{100} i = \sum_{i=1}^{100} i - \sum_{j=1}^{31} j = \frac{100 \cdot 101}{2} - \frac{31 \cdot 32}{2} = 5050 - 496 = 4554$$

(2) La suma de todos los enteros de -12 a 51 inclusive se calcula así

$$\begin{aligned} \sum_{i=-12}^{51} i &= \sum_{i=-12}^{-1} i + \sum_{j=1}^{51} j = \sum_{i=1}^{12} (-i) + \sum_{j=1}^{51} j = \sum_{j=1}^{51} j - \sum_{i=1}^{12} i \\ &= \frac{50 \cdot 51}{2} - \frac{12 \cdot 13}{2} = 25 \cdot 51 - 6 \cdot 13 = 1326 - 78 = 1248 \end{aligned}$$

Aquí hemos sumado y hemos hecho cambio de variable. ◊

En general para la suma de cualquier conjunto de enteros consecutivos se tiene la siguiente proposición.

Proposición 5.10. *Sean $a, b \in \mathbb{Z}$ con $a < b$. Entonces*

$$\sum_{i=a}^{b} i = \tfrac{1}{2}(b+a)(b-a+1) \tag{5.6}$$

Demostración. Hay que considerar los 3 casos posibles: (i) $0 < a < b$, (ii) $a < 0 < b$ y (iii) $a < b < 0$.

(i) Si $0 < a < b$ entonces

$$\begin{aligned}\sum_{i=a}^{b} i &= \sum_{i=1}^{b} i - \sum_{i=1}^{a-1} i = \tfrac{b(b+1)}{2} - \tfrac{(a-1)a}{2} \\ &= \tfrac{1}{2}(b^2 + b - a^2 - a) \\ &= \tfrac{1}{2}\big((b-a)(b+a) + (b+a)\big) \\ &= \tfrac{1}{2}(b+a)(b-a+1)\end{aligned}$$

(ii) Si $a < 0 < b$ entonces

$$\begin{aligned}\sum_{i=a}^{b} i &= \sum_{i=-|a|}^{-1} i + \sum_{i=1}^{b} i = \sum_{i=1}^{|a|}(-i) + \sum_{i=1}^{b} i = \sum_{i=1}^{b} i - \sum_{i=1}^{|a|} i \\ &= \tfrac{1}{2}b(b+1) - \tfrac{1}{2}|a|(|a|+1) = \tfrac{1}{2}(b-|a|)(b+|a|+1)\end{aligned}$$

Como $a < 0$ se tiene $|a| = -a$ y por lo tanto vale (5.6).

(iii) Finalmente, si $a < b < 0$ entonces

$$\sum_{i=a}^{b} i = \sum_{i=-|a|}^{-|b|} i = -\sum_{i=|b|}^{|a|} i$$

Como $0 < |b| < |a|$, estamos en el primer caso y por lo tanto

$$\sum_{i=a}^{b} i = -\tfrac{1}{2}(|a| - |b|)(|b| + |a| + 1) = \tfrac{1}{2}(|b| - |a|)(|b| + |a| + 1)$$

De aquí sale (5.6), y la prueba está terminada. □

Chequeamos los ejemplos anteriores, ahora usando la fórmula (5.6):

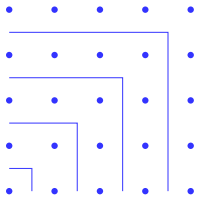
$$\sum_{i=32}^{100} i = \tfrac{132\cdot 69}{2} = 66 \cdot 69 = 4554, \qquad \text{y} \qquad \sum_{i=-12}^{51} i = \tfrac{39\cdot 64}{2} = 32 \cdot 39 = 1248$$

5.6.2. La suma de los impares

Ya sabemos sumar enteros consecutivos, ¿podremos sumar, por ejemplo, los naturales impares?

$$1 + 3 + 5 + 7 + \cdots + (2n-3) + (2n-1) = ??$$

El siguiente artilugio gráfico permite encontrar la respuesta correcta. Armando el cuadrado



es directo ver que

$$\begin{aligned}
1+3 &= 4 = 2^2\\
1+3+5 &= 9 = 3^2\\
1+3+5+7 &= 16 = 4^2\\
1+3+5+7+9 &= 25 = 5^2
\end{aligned}$$

Uno intuye y conjetura entonces que

$$1+3+5+\cdots+(2n-1) = \sum_{j=1}^{n} 2j-1 = n^2 \tag{5.7}$$

lo cual puede probarse por inducción.

Otra manera de encontrar la respuesta es manipulando la sumatoria correspondiente y usando lo que ya sabemos.

$$\sum_{i=1}^{n} 2i-1 = 2\sum_{i=1}^{n} i - \sum_{i=1}^{n} 1 = 2\cdot\frac{n(n+1)}{2} - n = n^2$$

En otras palabras, n^2 es igual a la suma de los n primeros impares y recíprocamente.

La sucesión de naturales impares que hemos sumado es un ejemplo de progresión aritmética, que estudiaremos más adelante.

5.6.3. Las sumas de los cuadrados y de los cubos

Comenzamos estudiando la suma de los cuadrados de los naturales.

$$\sum_{i=1}^{n} i^2 = ??$$

Hagamos algunos cálculos.

- $n=1 \longrightarrow \sum_{i=1}^{1} i^2 = 1.$
- $n=2 \longrightarrow \sum_{i=1}^{2} i^2 = 1+4 = 5.$
- $n=3 \longrightarrow \sum_{i=1}^{3} i^2 = 1+4+9 = 14.$
- $n=4 \longrightarrow \sum_{i=1}^{4} i^2 = 1+4+9+16 = 30.$
- $n=5 \longrightarrow \sum_{i=1}^{5} i^2 = 1+4+9+16+25 = 55.$

De nuevo, ¿hay alguna fórmula que describa estos resultados?, ¿la podremos encontrar? Las respuestas a ambas es de nuevo afirmativa. Sin embargo, ninguna de las formas que nos llevaron a encontrar una fórmula en el caso anterior funcionan en este caso. Lo que sí resulta efectivo es una nueva forma de hacer la suma del caso anterior que si es posbile aplicar a este caso.

- Caso anterior: Para hacer la suma $\sum_{i=1}^{n} i$ consideramos el cuadrado de $i+1$,

$$(i+1)^2 = i^2 + 2i + 1$$

luego usando las propiedades de la sumatoria resulta que

$$\sum_{i=1}^{n}(i+1)^2 = \sum_{i=1}^{n} i^2 + 2\sum_{i=1}^{n} i + \sum_{i=1}^{n} 1$$

En esta identidad aparece la suma que nos interesa, aunque puede parecer inútil ya que también aparecen dos sumas de cuadrados que no sabemos evaluar. Sin embargo, estas dos sumas de cuadrados son muy parecidas ya que tienen casi los mismos sumandos. En efecto la primera es la suma de los cuadrados comenzando en 2 y hasta $(n+1)^2$, $2^2+3^3+\cdots+n^2+(n+1)^2$, mientras que la segunda es la suma de los cuadrados comenzando en 1 y hasta n^2, $1+2^2+3^2\cdots+n^2$. Así, al restarlas se hará el milagro. En efecto,

$$\sum_{i=1}^{n}(i+1)^2 - \sum_{i=1}^{n} i^2 = (n+1)^2 - 1$$

Esto se suele llamar *suma telescópica*. Luego, de esto, y de la identendiad anterior se sigue que

$$2\sum_{i=1}^{n} i = \sum_{i=1}^{n}(i+1)^2 - \sum_{i=1}^{n} i^2 - n = (n+1)^2 - 1 - n = n^2 + n$$

Por lo tanto,

$$\sum_{i=1}^{n} i = \frac{(n+1)n}{2}$$

Notar que hemos dado una nueva demostración de este hecho, usando la suma de cuadrados $\sum_{i=1}^{n} i^2$ de forma auxiliar, sin necesidad de saber cuánto es el valor exacto de esa suma. Lo bueno es que esta idea puede ser utilizada para calcular sumas similares.

- Caso nuevo: Para hacer la suma $\sum_{i=1}^{n} i^2$ consideramos el cubo de $i+1$,

$$(i+1)^3 = i^3 + 3i^2 + 3i + 1$$

luego usando las propiedades de la sumatoria resulta que

$$\sum_{i=1}^{n}(i+1)^3 = \sum_{i=1}^{n} i^3 + \sum_{i=1}^{n} 3i^2 + \sum_{i=1}^{n} 3i + \sum_{i=1}^{n} 1$$

Despejando la suma que nos interesa y usando sumas telescópicas, se sigue que

$$3\sum_{i=1}^{n} i^2 = \Big(\sum_{i=1}^{n}(i+1)^3 - \sum_{i=1}^{n} i^3\Big) - 3\sum_{i=1}^{n} i - \sum_{i=1}^{n} 1$$

Luego,

$$\begin{aligned} 3\sum_{i=1}^{n} i^2 &= (n+1)^3 - 1 - \tfrac{3}{2}n(n+1) - n = (n+1)\{(n+1)^2 - \tfrac{3}{2}n - 1\} \\ &= (n+1)\{n^2 + 2n - \tfrac{3}{2}n\} = n(n+1)\{n+2-\tfrac{3}{2}\} = \tfrac{1}{2}n(n+1)(2n+1), \end{aligned}$$

y por lo tanto

$$\sum_{i=1}^{n} i^2 = \tfrac{1}{6}n(n+1)(2n+1) \tag{5.8}$$

Nota. La suma $\sum_{i=1}^{n} a_i$ se dice *telescópica* si los términos son de la forma $a_i = b_i - b_{i+1}$ con $b_1, b_2, \ldots, b_{n+1}$. En este caso, tenemos

$$\sum_{i=1}^{n} a_n = (b_1 - b_2) + (b_2 - b_3) + \cdots + (b_{n-2} - b_{n-1}) + (b_{n-1} - b_n) = b_1 - b_{n+1}$$

es decir, los términos se cancelan y sólo queda el aporte del primero y del último

Hacemos notar que para sumar los primeros n naturales resultó muy efectivo considerar los cuadrados, y que luego para sumar los cuadrados fue efectivo considerar los cubos. Este no es un fenómeno extraño en matemática; más de una vez para resolver un problema hay que salirse del marco natural del mismo, para encontrar su solución en un entorno más grande.

La siguiente proposición resume lo que hicimos y establece resultados para otras sumas nuevas.

Proposición 5.11. *Para todo $n \in \mathbb{N}$ se tiene que:*

(a) $\displaystyle\sum_{i=1}^{n} i = \tfrac{1}{2}n(n+1)$,

(b) $\displaystyle\sum_{i=1}^{n} i^2 = \tfrac{1}{6}n(n+1)(2n+1)$,

(c) $\displaystyle\sum_{i=1}^{n} i^3 = \tfrac{1}{4}n^2(n+1)^2$,

(d) $\displaystyle\sum_{i=1}^{n} i^4 = \tfrac{1}{30}n(n+1)(2n+1)(3n^2+3n-1)$.

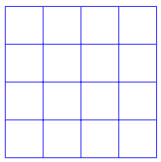
Los dos primeros items ya fueron probados y las demostración del tercero (resp. cuarto) es análoga a la dada para la suma de los cuadrados, comenzando por considerar la cuarta (resp. quinta) potencia de $i+1$. Dejamos estas cuentas como ejercicio para el lector.

Notar que podemos escribir estas sumas de potencias en términos de sumas de potencias mas chicas:

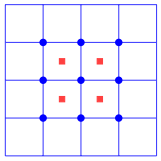
$$\begin{aligned}
\sum_{i=1}^{n} i^2 &= \tfrac{1}{3}(2n+1)\Big(\sum_{i=1}^{n} i\Big) \\
\sum_{i=1}^{n} i^3 &= \Big(\tfrac{n(n+1)}{2}\Big)^2 = \Big(\sum_{i=1}^{n} i\Big)^2 \\
\sum_{i=1}^{n} i^4 &= \tfrac{1}{5}(3n^2+3n-1)\Big(\sum_{i=1}^{n} i^2\Big) = \tfrac{1}{5}(6\Big(\sum_{i=1}^{n} i\Big)-1)\Big(\sum_{i=1}^{n} i^2\Big)
\end{aligned} \tag{5.9}$$

Veamos ahora un ejemplito práctico, con una de esas preguntas que suelen aparecer en revistas de juegos para el verano o en programas baratos de madrugada.

Ejemplo. ¿Cuántos cuadrados hay en la siguiente grilla 4×4?



Tenemos que contar todos los cuadrados 1×1, 2×2, 3×3 y 4×4. Claramente hay 4^2 cuadrados 1×1 y uno solo 4×4. Marcamos con puntos redondos los centros de los cuadrados 2×2 y con puntos cuadrados* los cuadrados 3×3.



Luego, el número de cuadrados es

$$1+4+9+16 = 1^2+2^2+3^2+4^2 = 30$$

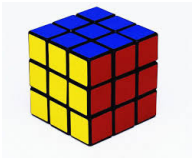
De aquí es fácil inferir que el número total de cuadrados en una grilla $n \times n$ es

$$1+2^2+\cdots+n^2 = \tfrac{1}{6}n(n+1)(2n+1)$$

por (5.8). Por ejemplo, el número total de cuadrados presentes en un tablero de ajedrez (8×8) es $\sum_{i=1}^{8} i^2 = \frac{1}{6}\cdot 8\cdot 9\cdot 17 = 3\cdot 4\cdot 17 = 4\cdot 51 = 204$ y en uno de damas (10×10) es $\sum_{i=1}^{10} i^2 = \frac{1}{6}10\cdot 11\cdot 21 = 5\cdot 7\cdot 11 = 385$. También, podríamos haber hecho $(1^2+\cdots+8^2)+9^2+10^2 = 204+81+100 = 385$, usando el resultado previo. ◊

*Este truquito nos fue sugerido por Luca Podestá (7).

Notar que el argumento usado en el ejemplo vale en otras dimensiones. Es decir, podemos interpretar a la suma $\sum_{i=1}^{n} i$ como el número total de segmentos que hay en una regla numerada del 0 a n. Del mismo modo, podemos interpretar a la suma $\sum_{i=1}^{n} i^3$ como el número total de cubitos unitarios que hay en un cubo $n \times n \times n$ (es decir, formado por n^3 cubitos unitarios). Por ejempplo, para el cubito $3 \times 3 \times 3$, tenemos $\sum_{i=1}^{3} i^3 = 1+8+27 = 36$



cubitos en total. Por favor, compruebe todo esto por su cuenta ya que es muy lindo y produce esa extraña sensación en el alma.

Problema.

Encontrar una fórmula para la suma de las primeras n potencias de orden k. Es decir, hallar una fórmula para

$$S_{k,n} = \sum_{i=1}^{n} i^k$$

5.6.4. La suma de potencias

Hemos estado estudiando la suma de números, cuadrados y cubos consecutivos. Ahora nos interesa estudiar una variante de esto. Fijamos un número real a y queremos calcular la suma de todas sus potencias consecutivas.

Proposición 5.12. *Sea $a \in \mathbb{R}$ no nulo y $a \neq 1$. Entonces para todo $n \in \mathbb{N}$,*

$$\sum_{i=0}^{n} a^i = 1 + a + a^2 + \cdots + a^n = \frac{a^{n+1} - 1}{a - 1} \tag{5.10}$$

Demostración. (Por inducción) Para $n = 1$ el miembro de la izquierda es igual a $1 + a$ y el de la derecha es igual a $\frac{a^2-1}{a-1} = a + 1$. Luego coinciden.

Queremos ver que $\sum_{i=0}^{n+1} a^i = \frac{a^{n+2}-1}{a-1}$. Ahora, $\sum_{i=0}^{n+1} a^i = \left(\sum_{i=0}^{n} a^i\right) + a^{n+1}$ y por hipótesis inductiva tenemos que

$$\begin{aligned} \sum_{i=0}^{n+1} a^i &= \frac{a^{n+1} - 1}{a - 1} + a^{n+1} = \frac{a^{n+1} - 1 + (a-1)a^{n+1}}{a - 1} \\ &= \frac{a^{n+1} - 1 + a^{n+2} - a^{n+1}}{a - 1} = \frac{a^{n+2} - 1}{a - 1} \end{aligned}$$

y, por principio de inducción, la demostración está completa. □

Si $a = 1$ no vale (5.10), pero la suma $\sum_{i=1}^{n} a^i = n$ es trivial en ese caso.

5.6.5. Progresiones aritméticas †

Ya sabemos calcular sumas tales como $1+2+\cdots+135$ o como $(-2)+(-1)+0+1+2+3+\cdots+106+107$ y otras del mismo tipo. Con lo que sabemos podemos sumar cualquier progresión aritmética.

Recordamos que una *sucesión* de números reales es una función de $\mathbb{N}$ en $\mathbb{R}$. Dada una sucesión a, en general denotamos a_n en vez de $a(n)$ a la imagen de n por a y también denotamos $\{a_n\}_{n\in\mathbb{N}}$ en vez de $a:\mathbb{N}\to\mathbb{R}$.

Definición. Un *progresión aritmética* es una sucesión tal que la diferencia de dos valores consecutivos es constante. Esta constante es el *paso* de la progresión.

Si $\{a_n\}_{n\in\mathbb{N}}$ es aritmética, entonces, por definición, $a_{n+1}-a_n=c$ para todo $n\geq 1$, para algún c. Notemos que esto define recursivamente a a_n, ya que

$$a_{n+1}=a_n+c$$

Luego $a_2=a_1+c$, $a_3=a_2+c=a_1+2c$, $a_4=a_3+c=a_1+3c$ y en general

$$a_n=a_1+(n-1)c$$

Recíprocamente si $a_n=a_1+(n-1)c$, entonces

$$a_{n+1}-a_n=(a_1+nc)-(a_1+(n-1)c)=c$$

lo que muestra que a_n es aritmética, de paso c. hemos probado la siguiente caracterización de las sucesiones aritméticas.

Proposición 5.13. *Una sucesión $\{a_n\}_{n\in\mathbb{N}}$ es aritmética si y sólo si existen $b,c\in\mathbb{R}$ tales que para todo $n\in\mathbb{N}$ vale*

$$a_n=b+(n-1)c$$

Decimos que la sucesión comienza en b, pues este es el valor de a_1, y es de paso c. Por ejemplo, la sucesión de los números naturales es una progresión aritmética de paso $c=1$ que comienza en 1, y las sucesiones de naturales impares y de naturales pares son progresiones aritméticas de paso $c=2$ que comienzan en 1 y en 2 respectivamente.

Ejemplos. Otros ejemplos son estos:

- $a_n=5+(n-1)3$: $\quad 5,\ 8,\ 11,\ 14,\ 17,\ 20,\ \ldots$
- $b_n=-\frac{1}{2}+(n-1)\frac{3}{2}$: $\quad -\frac{1}{2},\ 1,\ \frac{5}{2},\ 4,\ \frac{11}{2},\ 7,\ \ldots$
- $c_n=2\pi+(n-1)(-\frac{\pi}{2})$: $\quad 2\pi,\ \frac{3}{2}\pi,\ \pi,\ \frac{1}{2}\pi,\ 0,\ -\frac{1}{2}\pi,\ -\pi,\ \ldots$

En el primer caso b y c son enteros, en el segundo caso ambos son racionales, y en el tercero ambos son irracionales. ◊

En la Proposición 5.9 aprendimos a sumar los términos de la sucesión de naturales (que es aritmética de paso 1 con inicio en 1) comenzando en 1 hasta un n arbitrario y luego vimos que podíamos también sumar cualquier sucesión de enteros desde un a hasta un b cualesquiera.

Veamos ahora que más generalmente, con la misma Proposición 5.9, podemos sumar los términos de cualquier *progresión aritmética* entre dos puntos cualesquiera. A modo de ejemplo tomemos las progresiones aritméticas consideradas más arriba y las sumamos hasta N.

- $a_n = 5 + (n-1)3$.

$$\begin{aligned}\sum_{n=1}^{N} a_n &= \sum_{n=1}^{N} 5 + (n-1)3 = 5\sum_{n=1}^{N} 1 + 3\sum_{n=1}^{N}(n-1) = 5N + 3\sum_{n=1}^{N-1} n \\ &= 5N + 3\cdot\tfrac{(N-1)N}{2} = \tfrac{3}{2}N^2 + \tfrac{7}{2}N = \tfrac{1}{2}N(3N+7)\end{aligned}$$

  Por ejemplo, si $N = 5$ tenemos que

$$5 + 8 + 11 + 14 + 17 = \tfrac{1}{2}5(15+7) = 55$$

- $b_n = -\frac{1}{2} + (n-1)\frac{3}{2}$.

$$\begin{aligned}\sum_{n=1}^{N} b_n &= \sum_{n=1}^{N} -\tfrac{1}{2} + (n-1)\tfrac{3}{2} = -\tfrac{1}{2}\sum_{n=1}^{N} 1 + \tfrac{3}{2}\sum_{n=1}^{N-1} n \\ &= -\tfrac{N}{2} + \tfrac{3}{2}\tfrac{(N-1)N}{2} = \tfrac{3}{4}N^2 - \tfrac{5}{4}N = \tfrac{1}{4}N(3N-5)\end{aligned}$$

  Por ejemplo, si $N = 5$ tenemos que

$$-\tfrac{1}{2} + 1 + \tfrac{5}{2} + 4 + \tfrac{11}{2} = \tfrac{1}{4}5(15-5) = \tfrac{25}{2}$$

- $c_n = 2\pi + (n-1)(-\frac{\pi}{2})$.

$$\begin{aligned}\sum_{n=1}^{N} c_n &= \sum_{n=1}^{N} 2\pi - (n-1)\tfrac{\pi}{2} = 2\pi\sum_{n=1}^{N} 1 - \tfrac{\pi}{2}\sum_{n=1}^{N}(n-1) \\ &= 2\pi N - \tfrac{\pi}{2}\sum_{n=1}^{N-1} n = 2\pi N - \tfrac{\pi}{2}\tfrac{(N-1)N}{2} = \tfrac{\pi}{4}N(9-N)\pi\end{aligned}$$

  Por ejemplo, si $N = 7$ tenemos que

$$2\pi + \tfrac{3}{2}\pi + \pi + \tfrac{1}{2}\pi + 0 - \tfrac{1}{2}\pi - \pi = \tfrac{\pi}{4}7(9-7) = \tfrac{7}{2}\pi$$

Como ha quedado claro en estos ejemplos, ni el paso ni el primer punto de la progresión aritmética a sumar son relavantes para afectuar al suma. Por lo tanto podemos escribir la suma de una progresión aritmética general.

Proposición 5.14. *Sea a_n la progresión aritmética $a_n = b+(n-1)c$, con $b, c \in \mathbb{R}$. Entonces, la suma de los primeros N términos de la progresión es*

$$\sum_{n=1}^{N} a_n = N\big(b + \tfrac{1}{2}(N-1)c\big) = \tfrac{1}{2}cN^2 + (b - \tfrac{1}{2}c)N$$

Demostración. Tenemos,

$$\sum_{n=1}^{n} a_n = \sum_{n=1}^{N} b + (n-1)c = bN + c\sum_{n=1}^{N-1} n = bN + \tfrac{1}{2}c(N-1)N$$

de donde la proposición sigue directamente. □

También podemos hacer sumas un poquito mas generales.

Corolario 5.15. *Si $a, b \in \mathbb{Z}$ con $a < b$ y $\alpha, \beta \in \mathbb{R}$, entonces*

$$\sum_{j=a}^{b} \alpha j + \beta = \big(\tfrac{1}{2}\alpha(b+a) + \beta\big)(b-a+1) \tag{5.11}$$

Demostración. Sale de $\sum_{j=a}^{b} \alpha j + \beta = \alpha(\sum_{i=a}^{b} i) + \beta(b-a+1)$, usando la Proposición 5.10. □

Observación. La proposición anterior también sale escribiendo

$$\sum_{n=1}^{N} b + (n-1)c = \sum_{n=1}^{N} cn + (b-c)$$

y usando el Corolario 5.15 con $\alpha = c$, $\beta = b - c$, $a = 1$, $b = N$.

5.6.6. Progresiones geométricas †

Las progresiones aritméticas son sucesiones definidas recursivamente en las que un término se obtiene del anterior sumando una cantidad fija, llamada paso. Las *progresiones geométricas* son la versión multiplicativa de las anteriores. Están definidas recursivamente y en este caso un término se obtiene del anterior multiplicándolo por una cantidad fija, en este caso llamada razón.

Definición. Un *progresión geométrica* es una sucesión tal que el cociente de dos valores consecutivos es constante. Esta constante es la *razón* de la progresión.

Está implícito en la definición que ningún término de una progresión geométrica puede ser 0.

Si $\{b_n\}_{n\in\mathbb{N}}$ es geométrica, entonces $b_{n+1}/b_n = c$ para todo $n \geq 1$, para algún $c \in \mathbb{R}$. Notemos que esto define recursivamente a b_n, ya que

$$b_{n+1} = b_n c$$

Luego $b_2 = b_1c$, $b_3 = b_2c = b_1c^2$, $b_4 = b_3c = b_1c^3$ y en general $b_n = b_1c^{n-1}$. Recíprocamente, si $b_n = b_1c^{n-1}$, entonces

$$b_{n+1}/b_n = b_1c^n/b_1c^{n-1} = c$$

lo que muestra que b_n es geométrica de razón c. Tenemos entonces la siguiente caracterización de las progresiones geométricas.

Proposición 5.16. *Una sucesión $\{b_n\}_{n\in\mathbb{N}}$ es geométrica si y sólo si existen $b, c \in \mathbb{R}$, no nulos, tales que*

$$b_n = bc^{n-1}$$

para todo $n \in \mathbb{N}$.

Las progresiones geométricas, son una de las pocas sucesiones que es posible sumar (los infinitos términos!). La siguiente proposición muestra como sumar los primeros términos de una progresión geométrica de razón a y que comienza en 1. O sea,

$$b_n = a^n, \qquad b_0 = 1$$

(a veces, como ahora, permitimos que una sucesión comience en $n = 0$). Notamos que si la razón es 1, entonces la progresión es constante y ya sabemos sumar sus términos. Convenimos que, para todo $a \in \mathbb{R}$, $a \neq 0$, $a^0 = 1$.

Es inmediato calcular la suma de una progresión geométrica. Si c_n es una progresión geométrica no constante de razón a ($a \neq 1$) que comienza en b, es decir $c_n = ba^{n-1}$, se tiene que

$$\sum_{i=1}^{n} c_n = \sum_{i=1}^{n} ba^{n-1} = b\sum_{i=0}^{n-1} a^i = b\frac{a^n - 1}{a - 1}$$

donde hemos usado la suma de potencias (5.10).

Veamos algunos ejemplos particulares.

Ejemplos.

(1) La suma de las potencias de 2 es casi una potencia de 2. En efecto,

$$\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$$

(2) La suma de las potencias de $\frac{1}{2}$ es casi 1. Más precisamente,

$$\begin{aligned}\sum_{i=1}^{n} \left(\tfrac{1}{2}\right)^i &= \sum_{i=0}^{n} \left(\tfrac{1}{2}\right)^i - 1 = \frac{(\frac{1}{2})^{n+1} - 1}{\frac{1}{2} - 1} - 1 \\ &= \frac{1 - (\frac{1}{2})^{n+1}}{\frac{1}{2}} - 1 = 2 - (\tfrac{1}{2})^n - 1 = 1 - (\tfrac{1}{2})^n\end{aligned}$$

(3) También podemos calcular la suma alternada de potencias de un número dado. Si $a \in \mathbb{R}$, $a \neq -1$, la suma

$$1 - a + a^2 - a^3 + a^4 - \cdots + (-1)^n a$$

es la suma de la progresión geométrica de razón $-a$ que empieza en 1. Así

$$1 - a + a^2 - a^3 + a^4 - \cdots + (-1)^n a = \sum_{i=0}^{n} (-a)^i = \frac{(-a)^{n+1} - 1}{-a - 1} = (-1)^n \frac{a^{n+1} + 1}{a + 1}$$

Nota histórica (La leyenda del ajedrez)**.** Cuenta la leyenda que el brahmán Lahur Sessa, inventor del ajedrez también conocido como Sissa Ben Dahir, escuchó que el Rey Iadava estaba triste por la muerte de su hijo. Éste fue a ofrecerle al Rey el juego de ajedrez como entretenimiento para olvidar sus penas. El rey quedó tan satisfecho con el juego, que luego quiso agradecer al joven otorgándole lo que este pidiera.

Sessa lo único que pidió fue trigo. ¡Sí! Pidió que el rey le diera un grano de trigo por la primera casilla del tablero, el doble por la segunda, el doble de la anterior por la tercera, y así sucesivamente hasta llegar a la casilla número 64. Es decir, $2^0+2^1+2^2+\cdots+2^{63}$ granos de trigo. Iadava, al oir el extraño e ínfimo pedido del joven, lanzó una sonora carcajada y, tras burlarse de su modestia, ordenó que se le diera lo que había solicitado. Al cabo de algunas horas los algebristas más hábiles del reino le informaron al Soberano que se necesitarían:

$$2^0 + 2^1 + 2^2 + \cdots + 2^{63} = 2^{64} - 1 = 18.446.744.073.709.551.615$$

granos de trigo!!

Concluyeron los algebristas y geómetras más sabios, que la cantidad de trigo que debe entregarse a Lahur Sissa equivalía a una montaña que teniendo como base la ciudad de Taligana, fuese 100 veces más alta que el Himalaya. La India entera, sembrados todos sus campos y destruídas todas sus ciudades, no bastaría para producir durante un siglo la cantidad de granos calculada.

5.7. Conjuntos inductivos y buena ordenación †

5.7.1. Conjuntos inductivos

Lo que sigue, sobre conjuntos inductivos, ayuda a comprender mejor los axiomas de los números naturales y el principio de inducción.

Definición. Un subconjunto $H \subseteq \mathbb{R}$ se dice *inductivo* si satisface que:

(i) $1 \in H$.

(ii) $h \in H \Rightarrow h + 1 \in H$.

Un subconjunto de números reales es inductivo si tiene al 1 y al sucesor de cualquiera de sus elementos. El primer ejemplo de conjunto inductivo es $\mathbb{N}$.

Ejemplos (Conjuntos inductivos)**.** Los siguientes conjuntos son inductivos.

(1) $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Z}$.

(2) $\mathbb{Q}(\sqrt{2})$.

(3) $\mathbb{Z}_{\geq -9} = \{a \in \mathbb{Z} : a \geq -9\} = \{-9, -8, -7, \dots, -1, 0, 1, 2, 3, 4, \dots\}$.

(4) $\frac{1}{2}\mathbb{Z} = \{\frac{a}{2} : a \in \mathbb{Z}\} = \{\dots, -\frac{3}{2}, -1, -\frac{1}{2}, 0, \frac{1}{2}, 1, \frac{3}{2}, 2, \dots\}$.

(5) $X = \bigcup_{n\in\mathbb{N}} (n - \epsilon, n + \epsilon)$ con $0 \leq \epsilon < 1$.

Ejemplos (Conjuntos no inductivos)**.** Los siguientes conjuntos no son inductivos.

(1) $A = \{n \in \mathbb{N} : n \geq 2\}$.

(2) $B = \{z \in \mathbb{Z} : z \leq 99\}$.

(3) $C = \mathbb{Z} - \{4\}$.

(4) Ningún conjunto finito puede ser inductivo

(5) H^c, si H es inductivo.

Explicar por qué los distintos conjuntos de los ejemplos son o no inductivos no es difícil. Es muy recomendable pensar el porqué, hasta poder dar algún argumento conciso y contundente. Dejamos esto como ejercicio. Otro buen ejercicio es mostrar ejemplos, si es posible, de conjuntos A con las siguientes propiedades.

(1) A es inductivo y $a \in A$ es tal que $A - \{a\}$ no lo es.

(2) A es inductivo y $a \in A$ es tal que $A - \{a\}$ sigue siendo inductivo.

(3) A es inductivo, pero $A - \{a\}$ no lo es cualquiera sea a.

(4) A es inductivo y $A - \{a\}$ también, cualquiera sea a.

Nota. con esta definición, el tercer axioma de los números naturales toma la siguiente forma.

> **N3.** *Si K es un subconjunto inductivo de $\mathbb{N}$ entonces $K = \mathbb{N}$.*

Es decir, ¡$\mathbb{N}$ no tiene subconjuntos inductivos propios!

Nos preguntamos ahora sobre la intersección y la unión de conjuntos inductivos. Si A y B son dos conjuntos inductivos, ¿es $A \cap B$ inductivo?; ¿es $A \cup B$ inductivo? No es difícil responder a estas preguntas afirmativamente. En primer lugar es claro que el 1 pertenece tanto a la intersección como a la unión. Por otro lado, si un número pertenece a la intersección, está en ambos y luego su sucesor está en ambos, es decir en la intersección. Ahora, si un número está en la unión, está en uno de ellos y luego su sucesor está en ese mismo conjunto, y en particular en la unión.

Con más generalidad vale el siguiente resultado.

Proposición 5.17. *La intersección arbitraria y la unión arbitraria de conjuntos inductivos, son conjuntos inductivos.*

Demostración. Dada $\mathcal{F}$ una familia de conjuntos inductivos, sean U y V respectivamente la intersección y la unión de todos los conjuntos de $\mathcal{F}$. Podemos denotar $U = \bigcap_{A\in\mathcal{F}} A$ y $V = \bigcup_{A\in\mathcal{F}} A$.

Primero, como todos los conjuntos de $\mathcal{F}$ son inductivos, todos contienen al 1. Luego $1 \in U$ y $1 \in V$.

Además, si $x \in U$, entonces x pertenece a todos los conjuntos de $\mathcal{F}$. Luego, como son todos inductivos $x + 1$ pertenece a todos ellos y así $x + 1 \in U$. Resultando U inductivo.

Por último, si $x \in V$, x está en alguno de los conjutos A de $\mathcal{F}$; siendo éste inductivo contiene a $x + 1$. Luego $x + 1 \in V$ y V es inductivo. □

5.7.2. Buena ordenación e inducción fuerte

Posiblemente a esta altura ya resulte intuitivo, que todo conjunto inductivo contiene a los naturales. Aunque resulte claro necesitamos deducirlo a partir de lo que sabemos. Para esto resulta útil introducir el concepto de *buena ordenación*.

Definición. Un subconjunto $H \subseteq \mathbb{R}$ tiene *primer elemento* h, si

(i) $h \in H$,

(ii) $h \leq k$ para todo $k \in H$.

Un subconjunto $K \subseteq \mathbb{R}$ se dice *bien ordenado*, si todo subconjunto $H \subseteq K$, no vacío, tiene primer elemento.

Presentamos ahora el *principio de buena ordenación*. Usaremos la siguiente notación $[\![1, n]\!] = \{1, 2, \ldots, n\}$, que ya fue definida en (3.6).

Teorema 5.18 (Principio de buena ordenación)**.** $\mathbb{N}$ *es bien ordenado.*

Demostración. Procedemos por el absurdo. Debemos probar que todo subconjunto $H \subseteq \mathbb{N}$, no vacío, tiene primer elemento. Supongamos que hay un $H \subseteq \mathbb{N}$, no vacío, sin primer elemento y sea H' su complemento en $\mathbb{N}$, es decir $H' = \mathbb{N} - H$. Como H es no vacío, H' no es igual a $\mathbb{N}$. Consideremos ahora el conjunto

$$K = \{n \in \mathbb{N} : [\![1, n]\!] \subseteq H'\}$$

Tenemos que $1 \in K$ dado que $\{1\} \subseteq H'$, pues $1 \notin H$, ya que de lo contrario sería el primer elemento de H. Además, si $h \in K$, entonces ninguno de los elementos de $\{1, 2, \ldots, h\}$ están H; luego $h + 1$ tampoco está H, pues de lo contrario sería su primer elemento. Así hemos probado que K es un subconjunto inductivo de $\mathbb{N}$ y por lo tanto $K = \mathbb{N}$. De esto se deduce que $H' = \mathbb{N}$ y H es vacío, lo que contradice nuestra suposición. □

Ahora sí podemos probar lo que queríamos.

Proposición 5.19. *Si $H \subseteq \mathbb{R}$ es inductivo, entonces $\mathbb{N} \subseteq H$.*

Demostración. Razonamos por el absurdo. Supongamos que $\mathbb{N} \not\subseteq H$ y sea $K = \{n \in \mathbb{N} : n \notin H\}$. Por ser K no vacío. Sea m su primer elemento; $m \neq 1$, pues $1 \in H$ por ser inductivo. Luego $m - 1 \in \mathbb{N}$ y $m - 1 \notin K$. Así $m - 1 \in H$ y por ser H inductivo, su sucesor, $m \in H$. Esto contradice el hecho de ser m elemento de K. Por lo tanto K es vacío y $\mathbb{N} \subseteq H$. □

Como corolario obtenemos una caracterización del subconjunto de los naturales.

Corolario 5.20. *$\mathbb{N}$ es el menor de todos los conjuntos inductivos de $\mathbb{R}$. Es decir, está contenido en todo conjunto inductivo y no contiene propiamente a ningún otro conjunto inductivo.*

Ahora si estamos en condiciones de dar la prueba del Principio de Inducción Fuerte, establecido en el Teorema 5.6. Recordemos su enunciado.

Teorema. *Sea $P(n)$ una función proposicional, con $n \in \mathbb{N}$. Si*

(I) *$P(1)$ es verdadera y,*

(II) *asumiendo que $P(1), P(2), \ldots, P(k)$ son verdaderas para un $k \in \mathbb{N}$ arbitrario se deduce que $P(k+1)$ es verdadera,*

entonces $P(n)$ es verdadera para todo $n \in \mathbb{N}$.

Demostración. Sea

$$H = \{n \in \mathbb{N} : P(n) \text{ es verdadera}\}$$

Supongamos que $H \subsetneq N$ y sea $H' = \mathbb{N} - H \neq \varnothing$. Sea k' el primer elemento de H'. Notamos que $k' > 1$, pues $1 \in H$ por hipótesis. Se sigue que si $k < k'$, entonces $k \notin H'$, es decir $k \in H$. Así tenemos que $1, \ldots, k' - 1$ están todos en H; es decir $P(1), \ldots, P(k' - 1)$ son todas verdaderas. Luego, por hipótesis, $P(k')$ es también verdadera y así $k' \in H$, lo cuál contradice el hecho de estar k' en H', el complemento de H. El absurdo s proviene de suponer que $H \neq \mathbb{N}$. Luego $H = \mathbb{N}$ y la prueba está completa. □

5.8. Ejercicios y problemas

Natural numbers are better for your health. Anónimo.

Ejercicios

Ejercicio 5.1. En cada una de las siguientes situaciones, decidir para qué valores de $n \in \mathbb{N}$ podemos asegurar que vale $P(n)$:

(a) $P(1)$ es verdadera y $P(n) \Rightarrow P(n+2)$ para todo $n \in \mathbb{N}$.

(b) $P(1)$ es verdadera y $P(n) \Rightarrow P(2n)$ para todo $n \in \mathbb{N}$.

(c) $P(1)$ y $P(2)$ son verdaderas, y $P(n) \Rightarrow P(n+2)$ para todo $n \in \mathbb{N}$.

(d) $P(1)$ es verdadera y $P(n) \Rightarrow P(n+2), P(n+3)$ para todo $n \in \mathbb{N}$.

(e) $P(1)$ es verdadera y $P(n) \Rightarrow P(n+1)$ para todo $n \geq 2$.

Ejercicio 5.2. Probar por inducción que valen las siguientes afirmaciones:

(a) $n+1 \leq 2^n \leq (n+1)!$ para todo $n \in \mathbb{N}$.

(b) $n^3 \leq 3^n$ para todo $n \in \mathbb{N}$.

(c) $1 + 2^n \leq 3^n$ para todo $n \in \mathbb{N}$.

(d) Existe $n_0 \in \mathbb{N}$ tal que $n^2 \geq 11n + 3$ para todo $n \geq n_0$.

Ejercicio 5.3. Explicitar las siguientes sumas y productos escribiendo todos los sumandos y luego calcular.

(a) $\sum_{r=0}^{4} r$.

(b) $\sum_{i=-2}^{5} i^2 - 2i + 1$.

(c) $\prod_{j=-3}^{3} \cos(j\pi)(j^2 - 4)$.

(d) $\prod_{i=1}^{5} i$.

(e) $\sum_{k=-3}^{-1} \frac{1}{k(k-1)}$.

(f) $\sum_{p=3}^{7} \frac{2p}{1-p^2}$.

(g) $\prod_{n=2}^{7} \frac{n}{n-1}$.

Ejercicio 5.4. Para cada de las siguientes sumas escribir explícitamente los primeros 3 y los últimos 3 sumandos.

(a) $\sum_{i=0}^{2014} \frac{i-14}{1+i}$.

(b) $\sum_{i=1}^{k} 2(i+1)$.

(c) $\sum_{i=-k}^{k} i^2 + 1$.

(d) $\sum_{i=-j+1}^{2j} i/2 + j$.

Ejercicio 5.5. Probar las siguientes identidades:

(a) $\sum_{i=-n}^{n} i^3 = 0.$

(b) $\sum_{i=0}^{n} 2^{2i+1} = 2 + 2\sum_{i=1}^{n} 4^i.$

(c) $\sum_{i=1}^{n}(-1)^n = \begin{cases} 0, & n \text{ par,} \\ -1, & n \text{ impar.} \end{cases}$

(d) $\sum_{i=0}^{n}(-1)^n = \begin{cases} 1, & n \text{ par,} \\ 0, & n \text{ impar.} \end{cases}$

Ejercicio 5.6. Para cada de las siguientes sumas escribir explícitamente los primeros 3 y los últimos 3 sumandos.

(a) $\sum_{i=-78}^{1112} i + 1.$

(b) $\sum_{i=q}^{p} i + 1.$

(c) $\sum_{i=q^2}^{p^2} i + 1.$

(d) $\sum_{i=q+1}^{2p-13} i + 1.$

Ejercicio 5.7. Demostrar por inducción que valen las siguientes identidades, para todo $n \in \mathbb{N}$:

(a) $\sum_{k=1}^{n}(2k-1)^2 = \frac{n(4n^2-1)}{3}.$

(b) $\prod_{i=1}^{n} \frac{i+1}{i} = n + 1.$

(c) $\sum_{k=1}^{n} k(k+1) = \frac{n(n+1)(n+2)}{3}.$

(d) $\sum_{j=1}^{n} \frac{1}{(2j-1)(2j+1)} = \frac{n}{2n+1}.$

(e) $\prod_{k=1}^{n}\left(1 - \frac{1}{(k+1)^2}\right) = \frac{n+2}{2n+2}.$

(f) $\sum_{k=1}^{n} \frac{1}{k(k+1)(k+2)} = \frac{n(n+3)}{4(n+1)(n+2)}.$

(g) $\sum_{k=1}^{n} k^5 + \sum_{k=1}^{n} k^7 = 2(\sum_{k=1}^{n} k)^4.$

Ejercicio 5.8. Para cada una de las siguientes sucesiones definidas por recurrencia, escribir explícitamente sus primeros 20 términos.

(a) $a_n = 3 + a_{n-1}$ y $a_1 = \pi$.

(b) $b_n = 4b_{n-1} + 1$ y $b_0 = 0$.

(c) $u_n = u_{n-1} + n$ y $u_2 = 3$.

(d) $w_n = w_{n-1} - w_{n-2}$ y $w_1 = 1$, $w_2 = 2$.

Ejercicio 5.9. Decidir cuáles de los siguientes conjuntos son inductivos.

(a) $\mathbb{N} \cup \{1/2\}$.

(b) $\mathbb{N} \cup \{0\}$.

(c) $\{1\} \cup \{2\} \cup \{x \in \mathbb{R} : x \geq 3\}$.

(d) $\{1\} \cup \{x \in \mathbb{Q} : x \geq 2\}$.

Ejercicio 5.10. Las siguientes proposiciones no son válidas para todo natural n. Intente realizar una prueba por inducción e indique qué paso puede realizarse correctamente y qué paso no puede realizarse:

(a) $n = n^2$.

(b) $n = n + 1$.

(c) $3^n = 3^{n+2}$.

(d) $3^{3n} = 3^{n+2}$.

Ejercicio 5.11. Usando inducción, probar que valen las siguientes afirmaciones:

(I) $2n + 1 \leq 2^n$ para todo $n \geq 3$.

(II) $6^n > 4^n + 1$ para todo $n \in \mathbb{N}$.

(III) $2^n > n^2$ para todo $n \geq 5$.

Ejercicio 5.12. Calcular las siguientes sumas:

(a) $\sum_{j=1}^{1023} j$.

(b) $\sum_{j=11}^{269} 3j - 1$.

(c) $\sum_{i=0}^{177} i^2 - 3i + 1$.

(d) $\sum_{k=-34}^{134} k^2 + k/2$.

Ejercicio 5.13. Calcular las siguientes sumas:

(a) $\sum_{j=0}^{102} (1/2)^j$.

(b) $\sum_{j=0}^{269} 3^j - 1$.

(c) $\sum_{i=1}^{106} (1/3)^i$.

(d) $\sum_{k=-66}^{66} 2^k + 1$.

Ejercicio 5.14. Utilizando las propiedades de sumatoria, decidir la validez de las siguientes identidades:

(a) $\sum_{i=1}^{n+1} (n + 1 - i) = 2(n + 1) + \sum_{i=1}^{n} (n + i)$.

(b) $\sum_{i=1}^{2^{n+1}} (3i - 1) = 3 \cdot 2^{n+1} - 1 + \sum_{i=1}^{2^n} (3i - 1)$.

Problemas

Problema 5.15. Probar que:

(a) La suma de los ángulos interiores de todo polígono convexo de n lados es $(n - 2)\pi$.

(b) Todo polígono convexo de n lados tiene $\frac{n(n-3)}{2}$ diagonales.

Problema 5.16. Probar por inducción que valen las siguientes afirmaciones:

(a) Si $a \geq -1$, entonces $(1 + a)^n \geq 1 + na$, para todo $n \in \mathbb{N}$.

Problema 5.17. Dados n números naturales $a_1, \ldots, a_n$ tales que cada uno de ellos se escribe como la suma de dos cuadrados, probar que $a_1 \cdots a_n$ también se escribe como suma de dos cuadrados.

Problema 5.18. Dado $\alpha \in \mathbb{R}$ tal que $\operatorname{sen}\alpha \neq 0$, probar que para todo $n \in \mathbb{N}$ se verifica:

$$\cos(\alpha)\ \cos(2\alpha)\ \cos(4\alpha)\cdots\cos(2^{n-1}\alpha) = \frac{\operatorname{sen}(2^n\alpha)}{2^n \operatorname{sen}\alpha}.$$

Problema 5.19. Sea $r \in \mathbb{R}$ tal que $r + \frac{1}{r} \in \mathbb{Z}$. Probar que $r^n + \frac{1}{r^n} \in \mathbb{Z}$, para todo $n \in \mathbb{N}$.
NOTA: La condición $r + \frac{1}{r} \in \mathbb{Z}$ se traduce en que r es solución de la ecuación $r^2 - ar + 1 = 0$, para algún $a \in \mathbb{Z}$. Para ello, es necesario que $|a| \geq 2$. Algunos ejemplos son $r = \frac{3+\sqrt{5}}{2}$, $r = \frac{4+\sqrt{12}}{2} = 2 + \sqrt{3}$, etc. Puede probar con alguno de estos ejemplos antes de considerar el caso general.

Problema 5.20. La *sucesión de Fibonacci* se define recursivamente de la siguiente manera:

$$u_1 = u_2 = 1, \qquad u_n = u_{n-1} + u_{n-2} \quad n \geq 3.$$

Así, sus primeros términos son $1, 1, 2, 3, 5, 8, 13$. Demostrar por inducción que el término general de la sucesión está dado por la siguiente fórmula:

$$u_n = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right].$$

AYUDA: Usar que $\frac{1\pm\sqrt{5}}{2}$ son las soluciones de la ecuación cuadrática $x^2 - x - 1 = 0$.

Sea $\{u_n\}_{n\in\mathbb{N}}$ la sucesión definida recursivamente por $u_0 = 5$, $u_1 = 6$, $u_2 = 14$, $u_n = 2u_{n-1} + u_{n-2} - 2u_{n-3}$ si $n \geq 3$. Probar que $u_n = 3 \cdot 2^n + 1 + (-1)^n$.

Problema 5.21. Sucesiones recursivas.

(a) Sea $\{u_n\}_{n\in\mathbb{N}}$ la sucesión definida recursivamente por $u_1 = 3$, $u_2 = 5$ y, si $n \geq 3$, $u_n = 3u_{n-1} - 2u_{n-2}$. Probar que $u_n = 2^n + 1$.

(b) Sea $\{u_n\}_{n\in\mathbb{N}}$ la sucesión definida recursivamente por $u_1 = 9$, $u_2 = 33$, $u_n = 7u_{n-1} - 10u_{n-2}$ si $n \geq 3$. Probar que $u_n = 2^{n+1} + 5^n$.

Problema 5.22. Encuentre el error en los siguientes argumentos de inducción.

(a) Demostraremos que $5n + 3$ es múltiplo de 5 para todo $n \in \mathbb{N}$.

Supongamos que $5k + 3$ es múltiplo de 5, para $k \in \mathbb{N}$. Entonces existe $p \in \mathbb{N}$ tal que $5k + 3 = 5p$. Probemos entonces que $5(k + 1) + 3$ es múltiplo de 5. Notar que

$$5(k + 1) + 3 = (5k + 5) + 3 = (5k + 3) + 5 = 5p + 5 = 5(p + 1);$$

entonces $5(k + 1) + 3$ es múltiplo de 5. Por lo tanto, por el principio de inducción, demostramos que $5n + 3$ es múltiplo de 5, para todo $n \in \mathbb{N}$.

(b) Sea $a \in \mathbb{R}$, con $a \neq 0$. Vamos a demostrar que para todo entero no negativo n, $a^n = 1$. Como $a^0 = 1$ por definición, la proposición es verdadera para $n = 0$. Supongamos que para un entero k, $a^m = 1$ para $0 \leq m \leq k$. Entonces,

$$a^{k+1} = \frac{a^k a^k}{a^{k-1}} = \frac{1 \cdot 1}{1} = 1.$$

Por lo tanto, el principio de inducción fuerte implica que $a^n = 1$ para todo entero no negativo n.

Problema 5.23. Sea $n \in \mathbb{N}$. Encontrar una fórmula que exprese el número de puntos de intersección de n rectas en el plano tales que:

- cualesquiera dos de ellas no son paralelas, y
- no hay tres rectas que pasen por un mismo punto.

Problema 5.24. Usando inducción, probar que valen las siguientes afirmaciones:

(a) Si $a_1, \ldots, a_n > 0$, entonces $\left(\sum_{i=1}^{n} a_i\right)\left(\sum_{i=1}^{n} \frac{1}{a_i}\right) \geq n^2$.

(b) Si $a_1, \ldots, a_n \in \mathbb{R}$, entonces $\sum_{i=1}^{n} a_i^2 \leq \left(\sum_{i=1}^{n} |a_i|\right)^2$.

Problema 5.25. Demostrar por inducción que valen las siguientes identidades, para todo $n \in \mathbb{N}$:

(a) $\sum_{k=1}^{n} k^3 = \left(\frac{n(n+1)}{2}\right)^2$.

(b) $\sum_{i=1}^{n} i^4 = \frac{n(n+1)(2n+1)(3n^2+3n-1)}{30}$.

(c) $\sum_{k=0}^{n} a + kb = \frac{(n+1)(2a+nb)}{2}$.

(d) $\sum_{j=1}^{n} (j-1)j(j+1) = \frac{n(n+1)(n^2+n-2)}{4}$.

(e) $\sum_{k=1}^{n} k \cdot k! = (n+1)! - 1$.

Problema 5.26. Sea $\{a_n\}$ una sucesión que satisface la siguiente propiedad: para todo $n \in \mathbb{N}$, $a_{n+1} = 2a_n + 1$. Probar que $a_n + 1 = 2^{n-1}(a_1 + 1)$ para todo $n \in \mathbb{N}$.

Problema 5.27. Probar que para todo $n \in \mathbb{N}$:

$$\sum_{i=1}^{n} (-1)^{i-1} i^2 = (-1)^{n-1} \left(\sum_{i=1}^{n} i\right).$$

Sugerencia: probar por separado los casos n par y n impar, cada uno por inducción.

Problema 5.28. Sea $\{u_n\}$ la sucesión de Fibonacci. Probar que para todo n y m se verifica lo siguiente:

(a) $u_{n+1}^2 - u_n u_{n+2} = (-1)^n$.

(b) $u_{n+m} = u_{m-1}u_n + u_m u_{n+1}$.

Problema 5.29. Consideremos una sucesión $\{u_n\}$ definida recursivamente por:

$$u_1 = x, \qquad u_2 = y, \qquad u_{n+1} = au_n + bu_{n-1},\ n \geq 2,$$

donde x, y, a, b son números reales.

Sean α, β las raíces de la ecuación $t^2 - at - b = 0$; asumimos que son distintas. Si

$$c = \frac{y - \beta x}{(\alpha - \beta)\alpha}, \qquad d = \frac{y - \alpha x}{(\beta - \alpha)\beta},$$

probar inductivamente que $u_n = c\alpha^n + d\beta^n$.

Problema 5.30. Decidir la veracidad de las siguientes proposiones:

(a) Todo conjunto infinito de $\mathbb{N}$ que contenga al 1 es inductivo.

(b) Existen subconjuntos finitos de $\mathbb{N}$ que son inductivos.

(c) El conjunto vacío es inductivo.

(d) El conjunto $\{x \in \mathbb{R} : x < 0\}$ es disjunto con $\mathbb{N}$.

Capítulo 6

Aritmética entera

" ¿Porqué sumar números primos?
Los números primos están hechos para ser multiplicados, no sumados"
Lev Landau, matemático ruso (1908 – 1968)

En este capítulo iniciamos el estudio de la artimética de los números enteros denotados por $\mathbb{Z}$. Sabemos que $\mathbb{Z}$ es unión del conjunto de naturales $\mathbb{N}$, sus opuestos $-\mathbb{N}$ y el 0. Es decir,

$$\mathbb{Z} = -\mathbb{N} \cup \{0\} \cup -\mathbb{N},$$

donde $-\mathbb{N} = \{m \in \mathbb{R} : \ -m \in \mathbb{N}\}$. Recordemos que la suma y el producto de números reales extienden a la suma y el producto de enteros. Formalmente esto es:

$$+|_{\mathbb{Z}\times\mathbb{Z}} : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \quad \text{y} \quad \cdot|_{\mathbb{Z}\times\mathbb{Z}} : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}.$$

Vamos a considerar a los enteros como un conjunto de números con una suma y un producto propios y estudiaremos su artimética prescindiendo en general de los reales. De todas formas, como resulta práctico aprovechar lo que sabemos de los reales para estudiar los enteros, no nos olvidaremos de esto.

Cabe recordar, que ya tomamos una actitud similar cuando estudiamos, aunque rápidamente, la artimética de los racionales. Es ese caso también pensamos a $\mathbb{Q}$ como un conjunto de números con una suma y un producto, prescindiendo de los reales. En el caso de $\mathbb{Q}$ observamos que tiene las mismas propiedades aritméticas que $\mathbb{R}$ respecto de la suma y el producto, y aún las mismas respecto del orden. Por lo tanto no se distinguen por su artimética.

El caso de los enteros $\mathbb{Z}$ resulta mucho más interesante, ya que $\mathbb{Z}$ no tiene las mismas propiedades básicas que tienen $\mathbb{R}$ y $\mathbb{Q}$. La diferencia fundamental proviene del hecho de que en $\mathbb{Z}$ no hay inversos multiplicativos.

Entre las propiedades básicas de la suma y el producto que comparten $\mathbb{Z}$ y $\mathbb{R}$ están la asociatividad y conmutatividad de ambas y la propiedad distributiva; éstas valen en $\mathbb{Z}$ por particularización de las correspondientes para $\mathbb{R}$. Además también en $\mathbb{Z}$ hay un elemento neutro para la suma, el 0, y una identidad para el producto, el 1. Esto es inmediato ya que 0 y 1 tienen esos roles en el ámbito más grande de los números reales. Debemos preguntarnos por la unicidad de éstos. Esto no se sigue de la unicidad del neutro y de la

identidad en $\mathbb{R}$. Ser elemento neutro en $\mathbb{Z}$ es más fácil, ya que $\mathbb{Z} \subsetneq \mathbb{R}$; ser neutro en $\mathbb{Z}$ no implica ser neutro en $\mathbb{R}$ y por lo tanto podría haber más de un neutro en $\mathbb{Z}$. Además cada entero tiene un opuesto entero, que resulta único pues dicho tiene un único opuesto real.

Proposición 6.1. *La suma y el producto de números enteros tienen las siguientes propiedades.*

(a) La suma es asociativa y conmutativa.

(b) El producto es asociativo y conmutativo.

(c) El producto y la suma satisfacen la propiedad distributiva.

(d) El 0 es el único elemento neutro para la suma.

(e) El 1 es la única identidad para el producto.

(f) Cada entero tiene un único opuesto entero.

Demostración.

(a) Para todo para de números reales a, b se tiene que $a + b = b + a$. En particular si a, b son enteros. Cualesquiera sean $a, b, c \in \mathbb{R}$, se tiene que $(a + b) + c = a + (b + c)$. En particular si a, b, c son enteros.

(b) Análoga a la del inciso anterior.

(c) Cualesquiera sean $a, b, c \in \mathbb{R}$, se tiene que $a(b+c) = ab+ac$. En particular si a, b, c son enteros.

(d) Siendo el 0 entero, es elemento neutro para la suma de enteros, pues $0 + a = a$ para todo $a \in \mathbb{R}$, y luego en particular si $a \in \mathbb{Z}$. Supongamos que $0'$ es otro entero que es elemento neutro para la suma; entonces por un lado $0 + 0' = 0$ y por otro $0 + 0' = 0'$ y por lo tanto $0 = 0'$.

(e) Siendo el 1 entero, es identidad para el producto de enteros, pues $1 \cdot a = a$ para todo $a \in \mathbb{R}$, y luego en particular si $a \in \mathbb{Z}$. Si $1'$ es otro entero que es identidad para el producto, tenemos que por un lado $1 \cdot 1' = 1$ y por otro que $1 \cdot 1' = 1'$; luego $1 = 1'$.

(f) Dado un entero a, su opuesto real $-a$ es entero, luego a tiene un opuesto entero. Si tuviera otro opuesto entero, éste sería también otro opuesto real. Por lo tanto a tiene un único opuesto entero.

La prueba está completa. □

Una de las propiedades básicas de $\mathbb{R}$ es la existencia de inversos, que luego probamos son únicos. Esto no ocurre en $\mathbb{Z}$ y ésta es la diferencia fundamental entre $\mathbb{R}$ y $\mathbb{Z}$.

Ejemplo. El número entero 2, no tiene inverso en $\mathbb{Z}$. Si lo tuviera, éste sería un inverso de 2 en $\mathbb{R}$; pero como en $\mathbb{R}$ el 2 tiene un único inverso, $\frac{1}{2}$, y éste no es entero, se sigue que 2 no tiene inverso entero. El 2 no es un caso raro, por el contrario, ningún entero, salvo 1 y -1, tiene inverso en $\mathbb{Z}$.

Proposición 6.2. *Los únicos números enteros que tienen inverso entero son* 1 *y* -1.

Demostración. Sea a un entero con inverso entero. Está claro que $a \neq 0$. El inverso entero de a es en particular un inverso real de a, luego debe ser a^{-1}. Por lo tanto $a^{-1} \in \mathbb{Z}$.

Supongamos primero que $a \in \mathbb{N}$; así $1 \leq a$ y luego $0 < a^{-1} \leq 1$. Siendo a^{-1} entero, se tiene que $a^{-1} = 1$. Ahora, si $a \in -\mathbb{N}$, entonces $-a \in \mathbb{N}$ y $-a^{-1} = 1$, de donde se sigue que $a = -1$. □

A pesar de que los enteros no poseen inversos (salvo ± 1), a veces sucede que dados dos enteros a y b, ba^{-1} si es entero, donde a^{-1} es el inverso en $\mathbb{R}$ de a (que es racional). Por ejemplo, si $b = 6$ y $a = 3$, entonces $ba^{-1} = 6 \cdot \frac{1}{3} = 2$. Entender este fenómeno más profundamente nos lleva a estudiar la *divisibilidad* de enteros.

6.1. Divisibilidad

En $\mathbb{R}$, como todo $a \neq 0$ tiene inverso, la ecuación

$$b = ax$$

(con $a, b \in \mathbb{R}$, $a \neq 0$) tiene solución (única) $x = ba^{-1}$. Esta misma ecuación en $\mathbb{Z}$, es decir con $a, b \in \mathbb{Z}$, $a \neq 0$, no siempre tiene solución; ya vimos que la ecuación $2x = 1$ no tiene solución en $\mathbb{Z}$. (La única posibilidad es la única solución real de esta ecuación que es igual a $1/2$.) Pero también vimos que la ecuación $3x = 6$, si tiene solución entera $x = 2$. Esta situación es la que resulta importante destacar y estudiar. La situación en la que a y b son tales que la ecuación $ax = b$ tiene solución entera.

Definición. Dados dos enteros a y b, decimos que "a *divide a* b" o que "b *es divisible por* a" si existe un número entero c tal que

$$b = ac.$$

En este caso también decimos que "a es *divisor* de b" o que "b es *múltiplo* de a".

Si a divide a b escribimos $a \mid b$ y si a no divide a b escribimos $a \nmid b$.

Observación. Si $a \mid b$, es decir si a es divisor de b, existe c tal que $b = ac$. Luego c es también un divisor de b.

Ejemplos.

(1) $3 \mid 12$, pues $12 = 3 \cdot 4$. Es decir, 3 es divisor de 12 y luego 4 es otro divisor de 12.

(2) $12 \nmid 3$, pues no existe ningún entero c tal que $3 = c \cdot 12$. Hay un único real c así y es $c = 1/4$ que no entero.

(3) $6 \mid 18$, pues $18 = 6 \cdot 3$. Luego también vale que $18 = (-6) \cdot (-3)$ y que $-18 = (-6) \cdot 3$ y $-18 = 6 \cdot (-3)$. De esto se sigue que

$$6 \mid 18, \qquad -6 \mid 18, \qquad -6 \mid -18, \qquad 6 \mid -18,$$

$$3 \mid 18, \qquad -3 \mid 18, \qquad 3 \mid -18, \qquad -3 \mid -18.$$

(4) Cualquiera sea a, como $a = 1 \cdot a$, se tiene que $1 \mid a$ y que $a \mid a$. Y luego como en el inciso anterior se sigue que $1 \mid \pm a$, $-1 \mid \pm a$, $a \mid \pm a$ y que $-a \mid \pm a$.

(5) Si $a \mid 1$, entonces existe c entero tal que $1 = ac$; es decir a tiene inverso en $\mathbb{Z}$, por lo tanto $a = \pm 1$.

(6) ¿Qué enteros dividen a 0? ¿Se puede dividir por 0, o mejor dicho a qué enteros divide 0? Para que un entero a divida a 0, $a \mid 0$, debe existir un c tal $0 = a \cdot c$. Si elegimos $c = 0$ resulta que $0 = a \cdot c$. Por lo tanto todos los enteros dividen a 0.

Supongamos ahora que $0 \mid a$. Es decir $a = 0 \cdot c$ para algún c. Pero, cualquiera sea c, $0 \cdot c = 0$. Luego, $0 \mid a$ es sólo posible para $a = 0$. Es decir $0 \mid 0$ y $0 \nmid a$ si $a \neq 0$. ◊

En los ejemplos hemos discutido algunas propiedades básicas de la divisibilidad que resumimos en la siguiente proposición. El lector puede escribir una prueba completa siguiendo los argumentos de los ejemplos.

Proposición 6.3. *Para todo $a, b \in \mathbb{Z}$, valen las siguientes propiedades.*

(a) $1 \mid \pm a$ *y* $-1 \mid \pm a$.

(b) $a \mid \pm a$ *y* $-a \mid \pm a$.

(c) $a \mid b \Leftrightarrow a \mid \pm b$ *y* $-a \mid \pm b$.

(d) $a \mid 0$.

(e) $0 \mid a \Leftrightarrow a = 0$.

(Notar que en los puntos (a), (b) y (c) hay cuatro posibilidades.)

Antes de continuar destacamos una propiedad importante de los enteros que tiene que ver con el 0 y la divisibilidad. Ya sabemos que cualquiera sea a, $a \mid 0$, pues $0 \cdot a = 0$.

Pregunta. ¿Es posible que exista $b \neq 0$ tal que $ba = 0$ aún si $a \neq 0$?

Respuesta. No, no es posible.

En efecto, si $ba = 0$ y $a \neq 0$, entonces multiplicando por el inverso real de a, tenemos que $b = baa^{-1} = 0a^{-1} = 0$. Es decir, $ab = 0$ si y solo si $a = 0$ o $b = 0$ (comparar con la Proposición 4.4.) El hecho de que no haya enteros distintos de 0 que multiplicados den 0, se resume diciendo que no hay *divisores de 0*. Hemos probado la siguiente proposición.

Proposición 6.4. *Los enteros no tienen divisores de cero.*

Corolario 6.5. *Si $ab = ac$ y $a \neq 0$, entonces $b = c$. En particular si $a = ab$, entonces $b = 1$.*

Demostración. Si $ab = ac$, entonces $0 = ab - ac = a(b - c)$. Como $a \neq 0$, se sigue que $b - c = 0$ o equivalentemente $b = c$.

Si $a = ab$, entonces $a \cdot 1 = ab$ de donde se sigue que $1 = b$. □

La siguiente proposición establece otras propiedades de la divisibilidad que usaremos frecuentemente en lo que sigue.

Proposición 6.6. *Sean $a, b, c \in \mathbb{Z}$ todos no nulos. Entonces valen las siguientes propiedades.*

(a) Si $a \mid b$ y $b \mid c$, entonces $a \mid c$.

(b) Si $a \mid b$ y $b \mid a$, entonces $a = b$ o $a = -b$.

(c) Si $a \mid b$ y $a \mid c$, entonces $a \mid b \pm c$.

(d) Si $a \mid b \pm c$ y $a \mid b$, entonces $a \mid c$.

(e) Si $a \mid b$, entonces $a \mid bc$.

Demostración.

(a) Si $a \mid b$ y $b \mid c$, existen m, n tale que $b = am$ y $c = bn$. Luego tenemos que $c = bn = a(mn)$, de donde se sigue que $a \mid c$.

(b) Si $a \mid b$ y $b \mid a$, existen m, n tales que $b = am$ y $a = bn$. Luego $b = am = b(nm)$ de donde se sigue que $nm = 1$. Como n y m son enteros, $n = \pm 1$ y $m = \pm 1$, de donde se sigue que $b = a$ o $b = -a$.

(c) Si $a \mid b$ y $a \mid c$, existen m, n tales que $b = ma$ y $c = na$. Entonces $b \pm c = ma \pm na = (m \pm n)a$ de donde se sigue que $a \mid b \pm c$.

(d) Si $a \mid b \pm c$ y $a \mid b$, entonces por el inciso anterior $a \mid b \pm c - b$, es decir $a \mid \pm c$ y luego $a \mid c$.

(e) Si $a \mid b$ entonces existe m tal que $b = ma$. Luego $bc = (ma)c = a(mc)$ de donde se sigue que $a \mid bc$.

La demostración está completa. □

Observación. La probado también vale en los casos en que a, b o c son nulos. La demostración es siempre directa, aunque hay varios casos que considerar. Por ejemplo, en el primer inciso si $a = 0$, entonces $b = 0$ y $c = 0$, luego $a \mid c$. Y en el último, si $b = 0$, entonces $bc = 0$ y $a \mid bc$ cualquiera sea a.

6.1.1. Los conjuntos de divisores

Sea $\mathrm{Div}(n)$ el *conjunto de divisores* de un entero n, es decir

$$\mathrm{Div}(n) = \{d \in \mathbb{Z} : d \mid n\}.$$

Las Proposiciones 6.3 y 6.6 dicen varias cosas sobre los conjuntos de divisores [*]. Para todo $a, b, n \in \mathbb{Z}$ se tiene que:

- $\{1, -1, n, -n\} \subseteq \mathrm{Div}(n)$.
- $\mathrm{Div}(1) = \{1, -1\}$.

[*] No confundir el conjunto de divisores de un entero, aún del 0, con la noción de no tener los enteros divisores de cero en el sentido de la Proposición 6.4.

- $\mathrm{Div}(0) = \mathbb{Z}$.
- $a \in \mathrm{Div}(n) \quad \Leftrightarrow \quad -a \in \mathrm{Div}(n)$.
- $\mathrm{Div}(n) = \mathrm{Div}(-n)$.
- $a \mid b \quad \Leftrightarrow \quad \mathrm{Div}(a) \subseteq \mathrm{Div}(b)$ y la igualdad se tiene si y sólo si $a = \pm b$.

Observación. Se sigue entonces que para estudiar el conjunto de divisores de un n, cuando sea conveniente podemos suponer que $n \in \mathbb{N}$ y podemos también estudiar sólo sus divisores positivos.

Una idea intuitiva que tenemos es la de que un divisor de a es "más chico" que a y luego a sólo puede tener una cantidad finita de divisores. Esto se base en el hecho de que el producto de dos naturales es más grande que cada uno de los factores. Sin embargo está claro que no es cierto para el producto de enteros. Por ejemplo, $-1 = 1 \cdot (-1)$ pero $-1 \not\geq 1$. Es decir $1 \mid -1$, pero 1 no es más chico que -1.

A pesar de esto, hay algo de cierto en la idea de que un divisor de a es "más chico" que a y sí es cierto que a sólo puede tener una cantidad finita de divisores.

La función valor absoluto de los enteros $|\ | : \mathbb{Z} \to \mathbb{Z}_{\geq 0}$, está definida por

$$|a| = \begin{cases} a, & \text{si } a \geq 0; \\ -a, & \text{si } a < 0. \end{cases}$$

En particular $|a| = 0$ si y sólo si $a = 0$. Se sigue de la regla de los signos del producto en $\mathbb{R}$ que $|ab| = |a||b|$.

Lema 6.7. *Si $b \neq 0$ y $a \mid b$, entonces $|a| \leq |b|$.*

Demostración. Si $a \mid b$, entonces existe c tal que $b = ac$ y luego $|b| = |a||c|$. Como $b \neq 0$, entonces $c \neq 0$ y $a \neq 0$, y así $|c| \geq 1$ y $|a| \geq 1$. Se sigue que $|b| = |a||c| \geq |a| \cdot 1 = |a|$. □

De este resultado, se sigue que un entero no nulo tiene una cantidad finita de divisores.

Proposición 6.8. *Sea $n \in \mathbb{Z}$, $n \neq 0$. El conjunto de divisores de n es finito. Más aún,*

$$\mathrm{Div}(n) \subseteq [\![-n, n]\!].$$

Demostración. Si a es un divisor de n, entonces por el lema anterior $|a| \leq |n|$. Los enteros con módulo menor o igual que $|n|$ son todos los de $[\![-n, n]\!]$. Luego $a \in [\![-n, n]\!]$. □

Nota. La idea intuitiva de que un divisor a de un entero b es "más chico" que b es correcta si la noción de "más chico" está dada por el valor absoluto. Es decir, a es "más chico" que b si $|a| \leq |b|$.

Ejemplos.

(1) $\mathrm{Div}(5) = \{\pm 1, \pm 5\}$.

(2) $\mathrm{Div}(6) = \{\pm 1, \pm 2, \pm 3, \pm 6\}$.

(3) $\mathrm{Div}(12) = \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12\} = \mathrm{Div}(-12)$.

(4) Como $6 \mid 12$, entonces $\mathrm{Div}(6) \subseteq \mathrm{Div}(12)$. En este caso, $\mathrm{Div}(12) - \mathrm{Div}(6) = \{\pm 4, \pm 12\}$.

6.1.2. Los números primos

Todo entero $b \neq 0$, y distinto de 1 y de -1, tiene por lo menos 4 cuatro divisores distintos: 1, -1, b y $-b$; dos positivos y dos negativos (cuidado! $-b$ no es necesariamente negativo). Éstos son los *divisores triviales*. Algunos enteros tienen además otros divisores; éstos se llaman *divisores propios*.

Hay enteros que no tienen divisores propios, sólo tienen los obvios, como por ejemplo el 2, el 3, el 17 y el 47, y luego también el -2, el -3, el -17 y el -47. En cambio el 4, el 12, el 36 y el 100 tiene divisores propios.

Definición. Un entero p se dice *primo*, si es positivo y tiene exactamente cuatro divisores, es decir

$$\mathrm{Div}(p) = \{\pm 1, \pm p\}.$$

Un entero se dice *compuesto* si no es primo.

Observaciones.

(1) El 1 no es primo (pues tiene sólo 2 divisores).

(2) El 0 no es primo (pues tiene infinitos divisores).

(3) Si p y q son primos distintos, entonces $p \nmid q$ y $q \nmid p$. Dicho de otra forma, si p y q son primos y $p \mid q$ entonces $p = q$.

Los números primos son sumamente importantes no sólo en aritmética y en el álgebra en general, sino en toda la matemática. Denotaremos por $\mathbb{P}$ al conjunto de números primos.

Damos a continuación la lista de los primeros números primos, los menores que 100.

Los primos menores que 100

2	3	5	7	11
13	17	19	23	29
31	37	41	43	47
53	59	61	67	71
73	79	83	89	97

Todos los números naturales pueden construirse a partir de una única pieza fundamental si la herramienta es la suma. Con el 1 y la suma construimos todos los naturales. Ahora, si la herramienta es el producto la situación es distinta. Con el 2 podemos construir el 2, el 4, el 8, el 16 y todas la potencias de 2 pero ningún otro natural. Lo mismo sucede si se nos permite usar un sola pieza. Como no pudimos construir el 3, lo agreguemos como pieza permitida. Ahora, con el 2 y con el 3, podemos construir (usando el producto):

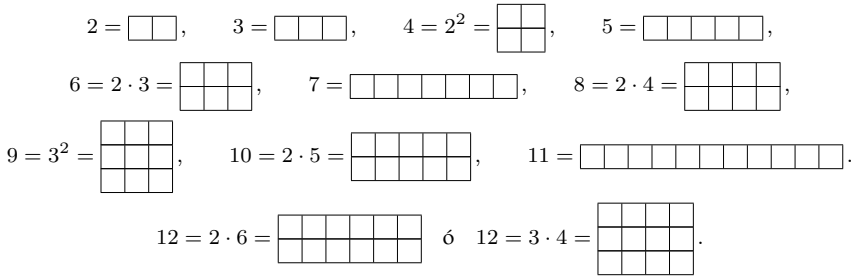
$$2, \qquad 3, \qquad 2^2 = 4, \qquad 2 \cdot 3 = 6, \qquad 2^3 = 8, \qquad 3^2 = 9,$$

$$2^2 \cdot 3 = 12, \qquad 2^4 = 16, \qquad 2 \cdot 3^2 = 18, \ldots$$

Está claro que no construiremos todos. No pudimos construir el 5, el 7 ni el 10. Necesitamos más piezas. La próxima a agregar debería ser el 5, el primer natural que no pudimos construir con el 2 y el 3; luego quizá debamos agregar el 7. De todas formas no debemos apurarnos. Por ejemplo, no deberíamos agregar el 10, hasta ver si lo podemos construir con las nuevas piezas agregadas. De hecho esto es lo que sucede ya que $2 \cdot 5 = 10$.

Una observación importante es que los números primos no se pueden construir multiplicando otros. La única manera de escribir a un primo p como producto de dos números (positivos) es $p = 1 \cdot p$. Luego, debemos incluirlos a todos como piezas para construir naturales.

Hay una forma muy bonita de pensar a los enteros gráficamente, como rectángulos formados por cuadraditos unidad. Por ejemplo, para los primeros naturales tenemos



De este modo, es claro que los números primos corresponden exactamente con aquellos números que sólo pueden ser representados como una sola fila. Luego, 2, 3, 5, 7 y 11 son primos (ya sabemos).

La pregunta que surge naturalmente es la siguiente:

Pregunta. ¿Son suficientes los números primos?

Respuesta. Sí. Todo natural se puede escribir como producto de números primos.

Tomemos un entero positivo b cualquiera; éste pueder ser primo o no. Si es primo, sus únicos divisores positivos son 1 y b. Si no lo es, hay por lo menos un divisor positivo propio $c \neq 1, b$ y luego también otro divisor propio d con $b = cd$ y $1 < c < b$, $1 < d < b$. Tanto c como d pueden ser primos o no. Si alguno no es primo, tiene un divisor propio y se factoriza como producto de dos naturales menores. Si continuamos este proceso de factorización, como los factores son cada vez más chicos y siempre mayores que 1, en algún momento tendremos una factorización de b como producto de factores todos primos. Más adelante escribiremos una demostración inductiva completa de este hecho.

Nota. Esto es una parte del Teorema Fundamental de la Aritmética (TFA), la existencia de una tal factorización; la otra parte afirma que ésta es única (salvo el orden de los factores). Probar la unicidad es más difícil y requiere algún resultado extra sobre números primos que probaremos más adelante.

Hay muchas preguntas naturales que uno puede hacerse sobre los números primos, aunque en realidad la mayoría son muy difíciles.

- ¿Cómo son los primos?
- ¿Cúales son? ¿Se conocen todos los primos?
- ¿Cuántos números primos hay?
- ¿Los podemos describir, hay alguna fórmula para esto?
- Dado un entero cualquiera, muy grande, ¿se puede decidir si es primo o no?
- Dado un número compuesto, ¿cómo encontrar sus factores primos?

La criba de Eratóstenes

Eratóstenes concibió allá por el año 255 a.C este método sistemático para encontrar todos los números primos entre el 2 y un natural n dado [**]. El método consiste en:

(1) Escribir en una cuadrícula todos los naturales desde el 2 hasta el n.

(2) Marcamos el 2 que es primo y a continuación tachamos todos los múltplos de 2 que, siendo múltiplos de un natural distinto de 1, no son primos.

(3) El primer natural despúes del 2 que sobrevivió sin tachar es el 3; lo marcamos como primo.

(4) Ahora tachamos todos los múltiplos de 3 y al terminar marcamos como primo al primer natual mayor que 3 sin tachar: el 5.

(5) Continuamos de la misma manera hasta agotar la cuadrícula.

El criterio de la raíz

A continuación mostramos todos los primos menores que 1000. Son exactamente nnn.

Terminamos esta sección considerando 10 problemas sobre divisibilidad.

Problemas.

(1) ¿Es cierto que si $a \mid bc$, entonces $a \mid b$ ó $a \mid c$?

(2) Determinar todos los divisores de 60.

(3) ¿Es 29 primo? ¿Y 517?

[**] Cribar: Separar las partes menudas de las gruesas de una materia. Seleccionar o elegir lo que interesa. Criba: Utensilio consistente en una lámina agujereada o una tela sujeta a un aro de madera, que se emplea para separar granos de distintos tamaños o cosas similares.

Cuadro 6.1: Los primeros 100 primos

2	3	5	7	11	13	17	19	23	29	31	37	41	43	47
53	59	61	67	71	73	79	83	89	97	101	103	107	109	113
127	131	137	139	149	151	157	163	167	173	179	181	191	193	197
199	211	223	227	229	233	239	241	251	257	263	269	271	277	281
283	293	307	311	313	317	331	337	347	349	353	359	367	373	379
383	389	397	401	409	419	421	431	433	439	443	449	457	461	463
467	479	487	491	499	503	509	521	523	541					

(4) Mostrar que $4^n - 1$ es divisible por 3 para todo $n \in \mathbb{N}$.

(5) ¿V o F: $n \mid 3^n + 1$, para todo $n \in \mathbb{N}$?

(6) ¿Cuál es el menor natural que es divisible por 6 y por 15?

(7) ¿Existe algún entero que tenga exactamente 8 divisores positivos? ¿Y alguno con exactamente 5?

(8) Si $m, n \in \mathbb{N}$ y $m \leq n$, entonces $m \mid n!$.

(9) ¿Es $3^{2n+1} + 2^{n+2}$ múltiplo de 7, $\forall n \in \mathbb{N}$?

(10) Dados $0 \leq a, b, c \leq 9$ sea x el número abc escrito en notación decimal. Mostrar que $9 \mid abc - (a + b + c)$.

Soluciones.

(1) Para simplificar la situación pensemos que a, b y c son todos naturales. Consideremos una situación fácil en la que $a \mid bc$, supongamos por ejemplo que $a = bc$. ¿Deberá ser que $a \mid b$ ó $a \mid c$? Si la respuesta fuera si, en particular tendríamos que $a \geq b$ ó $a \geq c$. Siendo $a = bc$ esto no es general posible. Todo esto nos hace sospechar que la respuesta es NO. Un ejemplo basta. Tomemos $a = 6 = 2 \times 3$, $b = 2$ y $c = 3$. Listo.

(2) Sabemos que basta determinar los divisores positivos. Si $a \mid 60$, $60 = a \cdot b$ para algún b y así b también es divisor de 60. Es decir los divisores de 60 (y de cualquier entero) están apareados. Por ejemplo, $1 \mid 60$ pues $60 = 1 \cdot 60$; luego 1 y 60 están apareados. Continuemos $2 \mid 60$, pues $60 = 2 \mid 30$ y así 30 es otro divisor de 60. Notemos que a medida el primer divisor crece, el segundo decrece. Tenemos que $3 \mid 60$ y $4 \mid 60$, ya que $60 = 3 \cdot 20$ y $60 = 4 \cdot 15$. Por lo pronto ya tenemos que $\{1, 60, 2, 30, 3, 20, 4, 15\}$ son todos divisores positivos de 60. Continuemos. $5 \mid 60$ y $6 \mid 60$ pues $60 = 5 \cdot 12 = 6 \cdot 10$. Ahora, 7, 8 y 9 no son divisores de 60. El 10 si es divisor, pero ya apareció junto con el 6. Además no es necesario seguir revisando si los mayores que 10 son divisores pues los que si lo son ya aparecieron apareados con otro divisor menor que 10. Hemos terminado. Concluimos que

$$\mathrm{Div}(60) = \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 5, \pm 6, \pm 10, \pm 12, \pm 15, \pm 20, \pm 30, \pm 60\}$$

(3) Busquemos divisores positivos de 29, distintos de 1 y 29. Si encontramos, 29 no es primo. Si no encontramos, 29 es primo. El 2 no divide a 29, ni el 3, ni el 4, ni el 5, pues 29 no está la tabla de ninguno de estos números. No es necesario continuar revisando el 6 (o los mayores) que ya de ser divisor estaría apareado con otro divisor necesariamente menor (que ya revisamos) pues $6 \times 6 = 36 > 29$. Conclusión: 29 es primo.

Para analizar el 517 procedemos de la misma manera que con el 29 observando que deberíamos revisar hasta el 22, pues $23 \times 23 = 529$. Empecemos. El 2 no divide a 517; luego podemos inmediatamente descartar como divisor al 4 ya que $2 \mid 4$ y sería entonces divisor de 517. Con el mismo argumento descartamos al 4, al 6 y a todos los pares. El 3 no divide a 517 pues $172 \times 3 = 516$ y $173 \times 3 = 519$, y luego 6 tampoco, ni 9, ni 12, ni 15, ni 18, ni 21. El 5 no divide a 517 y por lo tanto tampoco el 10, el 15 o el 20. El 7 no divide a 517, pues $73 \times 7 = 511$ y $74 \times 7 = 518$ y así tampoco el 14 ni el 21. Nos quedan por revisar el 11, el 13, el 17 y el 19. Ahora, el 11 si divide a 517, pues si hacemos la divisón que aprendimos en la escuela resulta que $517 = 11 \times 47$ Conclusión: 517 no es primo.

(4) Estamos ante un enunciado típico para intentar probarlo por inducción. Si $n = 1$, $4^n - 1 = 3$ y como $3 \mid 3$ la afirmación para $n = 1$ es verdadera. Ahora, supongamos que $3 \mid 4^{n-1} - 1$ e intentemos deducir que $3 \mid 4^n - 1$. Para esto reescribimos $4^n - 1$ convenientemente de la forma:

$$4^n - 1 = 4 \times 4^{n-1} - 1 = (3 + 1) \times 4^{n-1} - 1 = 3 \times 4^{n-1} + 4^{n-1} - 1$$

Así escrito $4^n - 1$ es la suma de dos sumandos ambos divisibles por 3, luego $4^n - 1$ es divisible por 3. (El segundo sumando el divisible por 3 por hipótesis inductiva.) El Principio de Inducción asegura que $4^n - 1$ es divisible por 3 para todo $n \in \mathbb{N}$.

(5) A diferencia del problema anterior, en este caso debemos decidir en primer lugar si el enunciado es verdadero o falso. Si sospechamos que es verdadero intentaremos prbarlo por inducción como hicimos con el anterior. Para poder formarnos una idea empecemos a probar con los primeros naturales.

$$\begin{aligned} n = 1 \Rightarrow 3^n + 1 = 4 \quad &\text{y} \quad 1 \mid 4 \quad 3 \\ n = 2 \Rightarrow 3^n + 1 = 10 \quad &\text{y} \quad 2 \mid 10 \quad 3 \\ n = 3 \Rightarrow 3^n + 1 = 28 \quad &\text{y} \quad 3 \nmid 28 \end{aligned}$$

Listo, nada más que hacer. La afirmación es falsa.

(6) Los naturales que son divisibles por 6 son sus múltiplos (positivos): 6, 12, 18, 24, 30, 36, etc. Aquellos divisibles por 15 son: 15, 30, 45, 60, etc. Mirando estas dos listas vemos que el menor natural que aparece en ambas es el 30. Luego es 30 el menor natural que divisible por 6 y por 15.

(7) Sabemos que si d es un divisor de a, entonces todos los divisores de d son también divisores de a. Buscamos un número a con no demasiados divisores, con exactamente 8 divisores positivos. Por lo tanto parece conveniente construir el número a a partir de algunos pocos divisores d que tengan ellos mismos muy pocos divisores. Podemos entonces comenzar con números primos. Veamos que construimos con el 2 y el 3.

Además de 2 y 3, tenemos $6 = 2 \times 3$, tenemos $12 = 2 \times 2 \times 3$ y tenemos $18 = 2 \times 3 \times 3$. Ahora 6 tiene 4 divisores positivos, 12 tiene 6 al igual que 18. Consideremos entonces $36 = 2 \times 2 \times 3 \times 3$. Pero 36 tiene 9 divisores positivos; nos pasamos. Intentemos con 3 primos distintos y consideremos $30 = 2 \times 3 \times 5$. Excelente, 30 tiene 8 divisores positivos.

Otra manera de buscar que no intentamos puede ser la de considerar un único primo. Por ejemplo consideremos 2, $4 = 2^2$, $8 = 2^3$, $16 = 2^4$ etc. Los divisores positivos de estos números son fáciles. Los de 4 son: 1, 2, 4. Los de 8 son: 1, 2, 4, 8. Los de 16 son: 1, 2, 4, 8, 16. Parece sencillo encontrar una potencia de 2 con 8 divisores positivos: $2^7 = 128$ es la respuesta. Más aún, así podemos construir un número con la cantidad de divisores positivos que queramos, pues 2^n tiene $n + 1$ divisores positivos.

En particular podemos entonces construir con un solo primo un número con exactamente 5 divisores positivos. Pero ahora, ¿habrá alguno construido con 2 primos? La respuesta es no; de la misma forma que el 6 tiene 4 y ya el 12 y el 18 tienen 6, todos los números construidos con 2 primos distintos tienen la misma cantidad de divisores. Esto quedará totalmente claro más adelante.

(8) Esto no es difícil. Recordemos que

$$n! = 1 \cdot 2 \cdot 3 \cdots (n-2) \cdot (n-1) \cdot n$$

es decir es el producto de todos los naturales menoreos o iguales que n. Como $m \geq n$, m está entre los factores y así $m \mid n!$.

(9) No es difícil verificar que las primeras instancias de esta afirmación, para n pequeño, son ciertas. En particular si $n = 1$ se afirma que $7 \mid 35$. Por esto intentamos probar la afirmación por inducción. Corroborado el caso $n = 1$ hacemos el paso inducctivo. Escribimos

$$3^{2(n+1)+1} + 2^{(n+1)+2} = 3^{2n+1}3^2 + 2^{n+2}2 =$$

y restamos y sumamos $3^{2n+1}2$ para obtener

$$= 3^{2n+1}3^2 - 3^{2n+1}2 + 3^{2n+1}2 + 2^{n+2}2 = 3^{2n+1}(3^2 - 2) + 2(3^{2n+1} + 2^{n+2})$$

Los dos sumandos de la última expresión son divisibles por 7; el primero pues $3^2 - 2 = 7$ y el segundo por hipótesis inductiva. Por lo tanto la afirmación es válida para todo $n \in \mathbb{N}$.

(10) El número abc escrito en notación decimal es el número

$$a \times 100 + b \times 10 + c$$

Ahora

$$a \times 100 + b \times 10 + c = a \times 99 + a + b \times 9 + b + c = (a \times 99 + b \times 9) + (a + b + c)$$

de donde se sigue que

$$abc - (a + b + c) = a \times 99 + b \times 9 = (a \times 11 + b) \times 9$$

y así $9 \mid abc - (a + b + c)$ como queríamos probar.

6.2. El algoritmo de la división

Hemos introducido ya las nociones "ser divisor de", "ser múltiplo de" y "ser primo". Estas nociones forman parte de los cimientos de toda la artimética y del álgebra.

Es importante recordar que las nociones "ser divisor de" y "ser múltiplo de" son en realidad una sóla. En efecto, a es divisor de b si y sólo si b es múltiplo de a. Esto es así pues así lo definimos. Por lo tanto todo enunciado, propiedad o resultado sobre divisores se corresponde con uno de múltiplos y viceversa.

6.2.1. Conjuntos de múltiplos

Dado un entero a, un múltiplo de a es un entero m para el cual exsite un entero c con $m = ac$. Recíprocamente, si c es cualquier entero, entonces $m = ac$ es un múltiplo de a. Se sigue entonces que los múltiplos de a, si $a \neq 0$, son infinitos. Más aún, hay una biyección natural con los enteros.

Dado $a \in \mathbb{Z}$, consideramos el *conjunto de múltiplos de* a, que denotamos por I_a. Tenemos

$$I_a = \{m : \ m \text{ es múltiplo de } a\} = \{ac : \ c \in \mathbb{Z}\}.$$

La biyección entre entre el conjunto de los enteros e I_a está dada por

$$\mu_a : \mathbb{Z} \to I_a, \qquad k \mapsto ka,$$

es decir $\mu_a(k) = ak$.

Es claro que $I_0 = \{0\}$ e $I_1 = \mathbb{Z}$, y como todo múltiplo de a es múltiplo de $-a$ y viceversa, se tiene que

$$I_a = I_{-a}.$$

Los conjuntos de múltiplos tienen una estructura interesante dada por las propiedades fundamentales contenidas en la proposición que sigue. Entre ellas que la suma y el producto de múltiplos de a son múltiplos de a.

Proposición 6.9. *Dado un entero a, el conjunto de sus múltiplos, I_a, tiene las siguientes propiedades:*

(a) $0 \in I_a$.

(b) Si $m, n \in I_a$, *entonces* $m + n \in I_a$.

(c) Si $m \in I_a$ *y* $n \in \mathbb{Z}$, *entonces* $mn \in I_a$.

Demostración.

(a) Como $0 = a0$, entonces $0 \in I_a$.

(b) Si $m, n \in I_a$, entonces existen $c, c' \in \mathbb{Z}$ tales que $m = ca$ y $n = c'a$. Luego, $m + n = ca + c'a = (c + c')a$ y por lo tanto $m + n \in I_a$.

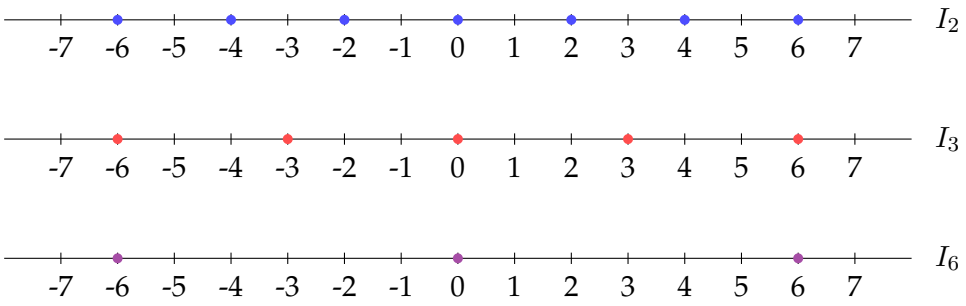
(c) Si $m \in I_a$, entonces existe $c \in \mathbb{Z}$ tal que $m = ca$. Luego, $mn = (ca)n = (cn)a$ y así $mn \in I_a$.

La prueba está completa. □

Observación. Las tres propiedades enunciadas en la proposición están contenidas en las Proposiciones 6.3 y 6.6. La primera propiedad es el inciso (d) de la Proposición 6.3 y las segunda y tercera son los incisos (c) y (e) de la Proposición 6.6.

Nota. Un poco más adelante estaremos en condiciones de mostrar que estas propiedades caracterizan a los conjuntos de múltiplos [*]. Es decir, si $A \subseteq \mathbb{Z}$ tiene estas 3 propiedades, entonces existe un $a \in \mathbb{Z}$ tal que $A = I_a$. Más aún, existe un único $a \geq 0$ tal que $A = I_a$.

Ejemplo. Tomemos $a = 2, 3, 6$ y comparemos los distintos conjuntos I_a que resultan. Es claro que $I_6 \subsetneq I_2$ y que $I_6 \subsetneq I_3$. Además $I_6 = I_3 \cap I_2$. Por otro lado, si b es tal que $I_3 \subseteq I_b$, entonces $b = 3$ o $b = 1$; es decir no hay ningún conjunto de múltiplos entre I_3 y $\mathbb{Z}$.



Lema 6.10. *Dados enteros a y b, $a \mid b$ si y sólo si $I_b \subseteq I_a$.*

Demostración. Si $a \mid b$, b es múltiplo de a (por definición de múltiplo). Luego, si c es múltiplo de b, es también múltiplo de a (ver Proposición 6.6). Para todo $c \in I_b$, $c \in I_a$ y así resulta que $I_b \subseteq I_a$.

Recíprocamente, si $I_b \subseteq I_a$, entonces en particular $b \in I_a$. Es decir b es múltiplo de a, o sea $a \mid b$. □

Observaciones.

(1) Como los divisores de un a dado son finitos, entonces toda sucesión $I_a \subseteq I_{a_1} \subseteq I_{a_2} \subseteq \ldots$ se estabiliza, es decir, a partir de algun momento los conjuntos son iguales; esto es hay un j para el cual se tiene que $I_{a_i} = I_{a_{i+1}}$ para todo $i \geq j$. Por ejemplo, si $a = 60$, tenemos que

$$I_{60} \subseteq I_{20} \subseteq I_4 \subseteq I_2 \subseteq I_2 \subseteq I_2 \subseteq \ldots$$

o también

$$I_{60} \subseteq I_{30} \subseteq I_6 \subseteq I_3 \subseteq I_3 \subseteq I_3 \subseteq \ldots$$

[*]Para el lector curioso: I_a es lo que se llama un *ideal* del *anillo* $\mathbb{Z}$.

(2) Dado a existen sucesiones infinitas que nunca se estabilizan $I_a \supsetneq I_{a_1} \supsetneq I_{a_2} \supsetneq \dots$. Por ejemplo,

$$I_2 \supsetneq I_4 \supsetneq I_8 \supsetneq I_{16} \supsetneq I_{32} \supsetneq I_{64} \supsetneq \dots$$

o también

$$I_3 \supsetneq I_6 \supsetneq I_{18} \supsetneq I_{36} \supsetneq I_{72} \supsetneq I_{144} \supsetneq \dots$$

6.2.2. La división entera

Dado un b, no nulo, el conjunto de sus múltiplos tiene una estructura muy rica. Dos múltiplos de b se pueden sumar y multiplicar como ya vimos y cada múltiplo tiene un opuesto. Esto permite hacer aritmética con los múltiplos de b.

Dados dos enteros a y b puede suceder que a sea múltiplo de b o que no lo sea. Si lo es, entonces $a = qb$, para algún q. ¿Qué podemos hacer o decir si no lo es? Podemos aproximar a a por un múltiplo de b. En este caso tendremos

$$a = \text{aproximación} + \text{error}.$$

Cuanto mejor sea la aproximación menor será el error.

—— DIBUJO (con b positivo) ——

Si a no es múltiplo de b, entonces está entre dos múltiplos consecutivos. Cualquiera de éstos dos es una buena aproximación, ya que el error (en valor absoluto) es menor que el mismo b. Más aún la diferencia entre a y el menor de estos dos múltiplo de b es positiva y es menor que b. Esto nos permite expresar a a como un múltiplo de b más una corrección (pequeña) positiva y menor que b.

Dados a y $b > 0$, si a no es múltiplo de b, existen un q y un $0 < r < b$ tales que

$$a = qb + r.$$

Notemos que si a si es múltiplo de b, entonces $r = 0$. Luego podemos afirmar que dados a y $b > 0$, existen q y $0 \leq r < b$ tales que

$$a = qb + r.$$

También observamos que si $b < 0$, podemos proceder como antes con $-b$ en lugar de b y afirmar que existen q y $0 \leq r < -b$ tales que

$$a = qb + r.$$

Todo esto se puede expresar de manera unificada diciendo que dados a y $b \neq 0$, existen enteros q y r tales que

$$a = qb + r, \qquad 0 \leq r < |b|.$$

Esta expresión de a en términos de b es la *división entera* de a por b, o de a dividido b. Luego de algunos ejemplos daremos una prueba formal y completa de este hecho.

Ejemplo. Calculemos la división entera de $a = 26$ por $b = 7$ (y las variantes con signos) usando el conjunto de múltiplos I_b

$$I_b = \{\dots, -35, -28, -21, -14, -7, 0, 7, 14, 21, 28, 35, \dots\}$$

(1) Dados $a = 26$ y $b = 7$, como $21 \leq a \leq 28$ se tiene que $26 = 3 \times 7 + 5$.

(2) Para $a = -26$ y $b = 7$, como $-28 \leq a \leq -21$ se tiene que $-26 = (-4) \times 7 + 2$.

(3) Dados $a = 26$ y $b = -7$, como $21 \leq a \leq 28$ escribimos $26 = (-3) \times (-7) + 5$.

(4) Por último, si $a = -26$ y $b = -7$, de $-28 \leq a \leq -21$ resulta que $-26 = 4 \times (-7) + 2$.

Una vez fijado el criterio para elegir la corrección r entre a y algún múltiplo de b, tanto q como r quedan unívocamente determinados.

Notación. q es el *cociente* de la división de a por b y r es el *resto* de esa división.

El lema y el teorema que siguen por un lado establecen la existencia y unicidad del cociente y del resto y por otro sus demostraciones muestran cómo calcularlos. Para la existencia del cociente y el resto es fundamental el hecho de que $\mathbb{N}$ es bien ordenado (ver Teorema 5.18).

Lema 6.11. *Dados dos enteros positivos a y b, existen enteros q y r, con $0 \leq r < b$, tales que $a = qb + r$. Más aún, q y r son únicos en estas condiciones.*

Demostración. Sea $H = \{n \in \mathbb{N} : nb > a\}$. H es no vacío, pues $a + 1 \in H$; en efecto $a + 1 > a$ y como $b > 0$, se tiene que $(a + 1)b > a$. Sea h el primer elemento de H y sea $q = h - 1$. Por ser h el primer elemento, se sigue que $q \notin H$, es decir $qb \leq a < hb = (q + 1)b = qb + b$. Luego si $r = a - qb$, tenemos que $a = qb + r$ y además que $0 \leq r$ y $r < b$ como queremos. Por último, supongamos que $a = qb + r = q'b + r'$ con $0 \leq r, r' < b$. Entonces $(q - q')b = r' - r$, es decir $r' - r$ es un múltiplo de b. Como $0 \leq r' < b$ y $0 \leq r < b$, tenemos que $0 \geq -r > -b$ y luego que $-b < r' - r < b$. Siendo 0 el único múltiplo de b en estas condiciones resulta que $r' - r = 0$, es decir $r' = r$ y luego, dado que $b \neq 0$, resulta también que $q' = q$. □

Teorema 6.12. *Dados a y b enteros cualesquiera con $b \neq 0$, existen enteros q y r con $0 \leq r < |b|$ tales que $a = qb + r$. Más aún, en estas condiciones q y r son únicos.*

Demostración. La unicidad de q y r se sigue de la misma manera que en el lema anterior.

Para la existencia notamos primero que si $a = 0$, $q = 0$ y $r = 0$ satisfacen que $a = qb + r$; luego consideramos por separado los 4 casos que resultan según sean a y b positivos o negativos, observando que el caso $a > 0$ y $b > 0$ ya fue considerado en el lema anterior. En los 3 casos restantes recurrimos al primero.

- $a > 0$ y $b < 0$: dividimos a por $-b$; así existen q' y $0 \leq r < -b = |b|$ tales que $a = q'(-b) + r$. Reescribiendo $a = (-q)b + r$ vemos que $q = q'$ y r son los buscados.
- $a < 0$ y $b < 0$: como $-b > 0$ dividimos $-a$ por $-b$; así existen q' y $0 \leq r' < -b$ tales que $-a = q'(-b) + r'$, es decir $a = q'b - r'$. Si $r' = 0$ elegimos $q = q'$ y $r = r' = 0$. Si $0 < r' < -b$, tenemos que $a = q'b - r'$ con $b < -r' < 0$. Sumando y restando b resulta que $a = q'b + b - b - r' = (q' + 1)b + (-b - r')$ con $0 < -b - r' < -b = |b|$. Luego elegimos $q = q' + 1$ y $r = -b - r'$.

- $a < 0$ y $b > 0$: dividimos $-a$ por b; así existen q' y $0 \leq r' < b$ tales que $-a = q'b + r'$, es decir $a = -q'b - r'$. Si $r' = 0$ elegimos $q = -q'$ y $r = r' = 0$. Si $0 < r' < b$, es decir si $-b < -r' < 0$, sumamos y restamos b para obtener que $a = -q'b - b + b - r' = (-q' - 1)b + (b - r')$. Como $0 < b - r' < b$ elegimos $q = -q' - 1$ y $r = b - r'$.

La prueba está completa.

□

Antes de hacer varias divisiones enteras en los ejemplos que siguen, pensemos un minuto sobre cómo proceder. La demostración del lema muestra que, en el caso en que $a > 0$ y $b > 0$, el cociente q es tal que qb es el menor de los múltiplos de b que son mayores o iguales que a. Para encontrarlo podemos comenzar inspeccionando los primeros múltiplos de b e ir avanzando hasta encontrar el primer múltiplo de b que supera a a; en ese caso el múltiplo buscado es el inmediato anterior. La demostración del teorema muestra que cualesquieran sean a y b, no necesariamente positivos, podemos hacer la división entera de a por b empezando con la división entera de $|a|$ por $|b|$. Notemos que también en el caso general podemos encontrar el cociente comenzando con los múltiplos pequeños de b y avanzar en una u otra dirección según sea el caso hasta encontrar el múltiplo adecuado. Pasemos a los ejemplos.

Ejemplos. Dividir 103 por ± 7 y -103 por ± 7.

(1) Los primeros 4 múltiplos positivos de 7 son: 7, 14, 21, 28. Conocemos algunos múltiplo más grandes como el décimo y el úndecimo: 70, 77. Continuemos a partir de ahí hasta superar a 103:

$$70,\ 77,\ 84,\ 91,\ 98,\ 105$$

El múltiplo que nos interesa es 98, el decimo cuarto múltiplo de 7. Así el cociente es $q = 14$ y el resto es $r = 103 - q \times 7 = 103 - 98 = 5$. Terminamos

$$103 = 14 \times 7 + 5$$

(2) Para dividir 103 por -7 miramos lo que ya sabemos: $103 = 14 \times 7 + 5$. Debemos hacer aparecer el -7. Por lo tanto escribimos

$$103 = (-14) \times (-7) + 5$$

(3) Para dividir -103 por 7 empezamos con $103 = 14 \times 7 + 5$. Luego $-103 = (-14) \times 7 - 5$. Debemos hacer una corrección, pues -5 no es un resto posible. Para esto sumamos y restamos 7. Así $-103 = (-14) \times 7 - 7 + 7 - 5 = (-15) \times 7 + 2$. Listo

$$-103 = (-15) \times 7 + 2$$

(4) Para dividir -103 por -7 empezamos con $103 = 14\times 7+5$. Luego $-103 = 14\times(-7)-5$. Como antes sumamos y restamos 7 para obtener $-103 = 14 \times (-7) - 7 + 7 - 5 = 15 \times (-7) + 2$. Conclusión

$$-103 = 15 \times (-7) + 2$$

Ejemplos. Más ejemplos en los que hacemos la división entera directamente. Dividir 58 por -8, -37 por 5 y -46 por -6.

(1) Como $-8 < 58$ consideramos los múltiplos mayores que -8 empezando por -8, 0, $8 = (-1) \times (-8)$, $16 = (-2) \times (-8)$, etc.:

$$-8,\ 0,\ 8,\ 16,\ 24,\ 32,\ 40,\ 48,\ 56,\ 64$$

El múltiplo buscado es 56. Así

$$58 = (-7) \times (-8) + 2$$

(2) Como $-37 < 5$ consideramos los múltiplos de 5 menores que 5 empezando por 5, 0, $-5 = (-1) \times 5$, $-10 = (-2) \times 5$, etc.:

$$5,\ 0,\ -5,\ -10,\ -15,\ -20,\ -25,\ -30,\ -35,\ -40$$

El múltiplo buscado es -40 pues $-40 < -37 < -35$. Así

$$-37 = (-8) \times 5 + 3$$

(3) Como $-46 < -6$ consideramos los múltiplos de -6 menores que -6 empezando por -6, $-12 = 2 \times (-6)$, $-18 = 3 \times (-6)$, etc.:

$$-6,\ -12,\ -18,\ -24,\ -30,\ -36,\ -42,\ -48$$

El múltiplo buscado es -48 pues $-48 < -46 < -42$. Así

$$-46 = 8 \times (-6) + 2$$

Ejemplos. En los ejemplos anteriores hemos dividido un número grande, en valor absoluto, por otro más chico, en valor absoluto. Y es esta la situación que nos representamos en la mente cuando pensamos en dividir. Pero, ¿cómo se divide un número chico por uno grande? De la misma forma en que se dividen dos números cualesquiera.

(1) Dividamos 5 por 17. ¿Cuál es el múltiplo de 17 menor que 5 y más próximo a 5? Es el 0. Luego

$$5 = 0 \times 17 + 5$$

(2) Dividamos -3 por 17. En este caso el múltiplo de 17 menor que -3 más próximo a -3 es -17. Por lo tanto

$$-3 = (-1) \times 17 + 14$$

Las siguientes preguntas muestran a la división entera como una herramienta útil para atacar problemas que involucran enteros.

Problemas.

(1) ¿Existe algún natural n tal que $n^2 + 1$ sea divisible por 25?

(2) ¿Existe algún natural n tal que $n^2 + 1$ sea divisible por 4?

(3) Exhibir varios pares de naturales consecutivos cuyo producto no sea divisible por 6.

(4) Mostrar que el producto de 3 naturales consecutivos es siempre divisible por 6.

(5) ¿Tiene la ecuación $2n^2 - 1 = 3(m + 1)$ alguna solución entera?

Soluciones.

(1) Buscamos un n tal que $n^2 + 1$ sea múltiplo de 25, es decir tal que n^2 sea un múltiplo de 25 menos 1. Listemos los primeros múltiplo de 25:

$$25,\ 50,\ 75,\ 100,\ 125,\ 150$$

y todos estos les restemos 1:

$$24,\ 49,\ 74,\ 99,\ 124,\ 149$$

¿Hay entre éstos alguno que sea un natural al cuadrado? Si, por suerte si: $49 = 7^2$. Por lo tanto elegimos $n = 7$. ¿Habrá otro?

(2) La pregunta es muy similar a la anterior. ¿Tendremos la misma suerte? Listemos directamente los primeros múltiplos de 4 menos 1:

$$3,\ 7,\ 11,\ 15,\ 19,\ 23,\ 27,\ 31,\ 35,\ 39,\ 43,\ 47,\ 51,\ 55$$

Nada hasta ahora. Algunos más:

$$59,\ 63,\ 67,\ 71,\ 75,\ 79,\ 83,\ 87,\ 91,\ 95,\ 99$$

No hay suerte. Quizá no haya un tal n. Intentemos demostrar que no hay ningún natural así. La división por 4 está presente en el enunciado mismo de la pregunta. Esto nos lleva a considerar la división entera de n por 4. Es decir, consideramos todas las posibilidades para n dividido por 4, que son 4, dado que hay 4 resto posibles: 0, 1, 2, 3. Procedemos caso por caso.

- $n = 4m$. Luego $n^2 + 1 = 16m^2 + 1 = 4 \cdot (4m) + 1$. Esta expresión es la división entera de $n^2 + 1$ por 4; como el resto es 1, $n^2 + 1$ no es divisible por 4 en este caso.

- $n = 4m + 1$. Luego $n^2 + 1 = 16m^2 + 8m + 1 + 1 = 4 \cdot (4m^2 + 2m) + 2$. Se sigue que en este caso $n^2 + 1$ tampoco es divisible por 4.
- $n = 4m + 2$. Luego $n^2 + 1 = 16m^2 + 16m + 4 + 1 = 4 \cdot (4m^2 + 4m + 1) + 1$. No divisble por 4.
- $n = 4m + 3$. Luego $n^2 + 1 = 16m^2 + 24m + 9 + 1 = 16m^2 + 24m + 8 + 2 = 4 \cdot (4m^2 + 6m + 2) + 2$. No divisible por 4.

En todos los casos posibles para n resultó que $n^2 + 1$ tiene resto 1 o 2 en la división por 4. Por lo tanto no existe un n como el buscado.

(3) Comenzamos calculando.

n	$n+1$	$n(n+1)$	
1	2	2	✓
2	3	6	✗
3	4	12	✗
4	5	20	✓
5	6	30	✗
6	7	42	✗
7	8	56	✓
8	9	72	✗
9	10	90	✗

Sin mucho esfuerzo hemos encontrado ya 3 pares como los buscados. Al mismo tiempo vemos que hay muchos pares de naturales consecutivos cuyo producto si es divisible por 6. ¿Será posible describir cuáles son?

(4) Observamos primero que si un número es divisible por 2 y por 3, entonces es divisible por 6. (Recordamos que esto no se puede generalizar: $4 \mid 12$ y $6 \mid 12$, sin embargo $24 \nmid 12$.) En efecto, si $2 \mid n$ y $3 \mid n$, entonces $n = 2a$ y $n = 3b$. Así tenemos que $2a = 3b = 2b + b$, de donde se sigue que $2 \mid 2b + b$ y como $2 \mid 2b$ entonces $2 \mid b$. Es decir $b = 2c$ y luego $n = 3b = 3(2c) = 6c$.

Veamos ahora que el producto de tres naturales consecutivos $n(n + 1)(n + 2)$ es divisible por 2 y por 3.

- Si n es par, es decir si $n = 2m$, el prodcuto $n(n + 1)(n + 2) = 2m(n + 1)(n + 2)$ es par. Si n es impar, es decri si $n = 2m + 1$, el producto $n(n + 1)(n + 2) = n(2m + 2)(n + 2) = 2n(m + 1)(n + 2)$ es par.
- Dividimos n por 3 y llamamos p al producto $n(n + 1)(n + 2)$. Si $n = 3m$, el producto p es múltiplo de 3 oues el primer factor es múltiplo de 3. Si $n = 3m + 1$, el tercer factor de p es múltiplo de 3 y luego p es múltiplo de 3. Si $n = 3m + 2$, el segundo factor de p es múltiplo de 3 y así p es múltiplo de 3.

(5) Podemos probar suerte un rato buscando pares de enteros n, m que satisfagan la ecuación propuesta (de hecho es muy bueno que cada uno lo haga). Al mismo tiempo podemos intentar probar que no hay solución alguna.

El miembro derecho de la ecuación en cuestión es divisible por 3, cualquiera sea m. Luego si el miembro izquierdo no es nunca divible por 3, la ecuación no tiene solución. Veamos que es así.

- Si $n = 3m$, entonces
$$2n^2 - 1 = 2 \cdot 9m^2 - 1 = 3 \cdot 6m^2 - 3 + 3 - 1 = 3 \cdot (6m^2 - 1) + 2.$$
- Si $n = 3m + 1$, entonces
$$2n^2 - 1 = 2 \cdot (9m^2 + 6m + 1) - 1 = 18m^2 + 12m + 2 - 1 = 3 \cdot (6m^2 + 4m) + 1.$$
- Si $n = 3m + 2$, entonces
$$\begin{aligned} 2n^2 - 1 = 2 \cdot (9m^2 + 12m + 4) - 1 &= 18m^2 + 24m + 8 - 1 \\ &= 18m^2 + 24m + 6 + 1 = 3 \cdot (6m^2 + 8m + 2) + 1. \end{aligned}$$

En todos los casos, el resto en la división por 3 de $2n^2 - 1$ es distinto de 0.

6.3. Números primos y factorización

Ya observamos que todo entero positivo se puede expresar como producto de números primos. El proceso de factorización comienza encontrando divisores propios del número dado y luego divisores de los divisores, etc.

El número $a = 8.701.110$ no es primo; 10 es uno de sus divisores y 55 es otro. Si comenzamos dividiendo por 10 y luego continuamos dividiendo algunos de los factores que aparecen podemos obtener, por ejemplo,

$$\begin{aligned} 8.701.110 &= 10 \times 870.111 = 10 \times 51 \times 17.061 \\ &= 10 \times 51 \times 47 \times 363 \\ &= 10 \times 51 \times 47 \times 11 \times 33 \end{aligned}$$

o también

$$\begin{aligned} 8.701.110 &= 10 \times 870.111 = 10 \times 3 \times 290.037 \\ &= 10 \times 3 \times 17 \times 17.061 \\ &= 10 \times 3 \times 17 \times 121 \times 141 \\ &= 10 \times 3 \times 17 \times 121 \times 141 \end{aligned}$$

Si comenzamos dividiendo por 55 y luego continuamos dividiendo algunos de los factores que aparecen podemos obtener, por ejemplo,

$$\begin{aligned} 8.701.110 &= 55 \times 158.202 = 55 \times 2 \times 79.101 \\ &= 55 \times 2 \times 11 \times 7.191 \\ &= 55 \times 2 \times 11 \times 17 \times 423 \\ &= 55 \times 2 \times 11 \times 17 \times 3 \times 141 \end{aligned}$$

o también

$$\begin{aligned} 8.701.110 &= 55 \times 158.202 = 55 \times 94 \times 1.683 \\ &= 55 \times 94 \times 9 \times 187 \\ &= 55 \times 94 \times 9 \times 11 \times 17 \end{aligned}$$

Todas estas factorizaciones son distintas, aunque algunos factores aparecen en más de una. Ahora como no todos los factores son primos, podemos seguir dividiendo.

$$\begin{aligned} 8.701.110 &= 10 \times 870.111 = 10 \times 51 \times 17.061 \\ &= 10 \times 51 \times 47 \times 363 \\ &= 10 \times 51 \times 47 \times 11 \times 33 \\ &= 2 \times 5 \times 3 \times 17 \times 47 \times 11 \times 3 \times 11 \end{aligned}$$

$$\begin{aligned} 8.701.110 &= 10 \times 870.111 = 10 \times 3 \times 290.037 \\ &= 10 \times 3 \times 17 \times 17.061 \\ &= 10 \times 3 \times 17 \times 121 \times 141 \\ &= 10 \times 3 \times 17 \times 121 \times 141 \\ &= 2 \times 5 \times 3 \times 17 \times 11 \times 11 \times 3 \times 47 \end{aligned}$$

$$\begin{aligned} 8.701.110 &= 55 \times 158.202 = 55 \times 2 \times 79.101 \\ &= 55 \times 2 \times 11 \times 7.191 \\ &= 55 \times 2 \times 11 \times 17 \times 423 \\ &= 55 \times 2 \times 11 \times 17 \times 3 \times 141 \\ &= 5 \times 11 \times 2 \times 11 \times 17 \times 3 \times 3 \times 47 \end{aligned}$$

$$\begin{aligned} 8.701.110 &= 55 \times 158.202 = 55 \times 94 \times 1.683 \\ &= 55 \times 94 \times 9 \times 187 \\ &= 55 \times 94 \times 9 \times 11 \times 17 \\ &= 5 \times 11 \times 2 \times 47 \times 3 \times 3 \times 11 \times 17 \end{aligned}$$

Notablemente en estas factorizaciones aparecen exactamente los mismos factores, aunque no en el mismo orden; pero dada la conmutatividad del producto podemos reordenar los factores para que todas estas factorizaciones sean idénticas. Está claro que ahora sí todos los factores son primos.

Esta lista de primos asociada a $8.701.110$ es como su ADN. Desde luego no hay nada especial en este número. Todos los naturales tiene su ADN que los identifica univocamente.

Teorema 6.13 (Teorema fundamental de la aritmética)**.** *Todo número natural n distinto de 1 es el producto de números primos. Los factores de esta factorización están unívocamente determinados por n y en particular esta factorización resulta única, salvo el orden en que aparecen los factores.*

Ye hemos bosquejado la prueba de la existencia de una tal factorización, que ahora escribimos formalmente. Destacamos que para probar unicidad de la misma, necesitamos una propiedad fundametal de los números primos que presentamos en la próxima sección.

Lema 6.14. *Todo número natural, distinto de 1, es divisible por un primo.*

Demostración. (Por inducción) El 2 es primo y luego 2 es divisible por un primo. Supongamos ahora que todo natural $k \leq n$ es divisible por un primo y veamos que todo natural $k \leq n+1$ es también divisible por un primo. Se tiene que $n+1$ puede ser primo o no. Si es primo, es divisible por un primo, luego todos los $k \leq n+1$ son divisibles por un primo. Si no los es, entonces tiene al menos un divisor propio, esto es existen $c, d \in \mathbb{N}$, con $n+1 = cd$ y $c, d < n+1$. Siendo $c, d \leq n$, por hipótesis inductiva se sigue que c (y también d) es divisible por un primo p; como $p \mid c$ y $c \mid n+1$, entonces $p \mid n+1$. □

Proposición 6.15 (Existencia en el **TFA**). *Todo número natural admite una factorización como producto de números primos.*

Demostración. □

Como hemos visto la existencia de la factorización de un natural como producto de primos, se sigue fácilmente del Lema 6.14 que asegura que todo natural es divisible por al menos un primo, cosa que es inmediata de la definición de número primo como vimos.

De este hecho elemental, se sigue la existencia de muchos números primos. Esto no quiere decir que conozcamos muchos primos, ni que podamos describirlos. Estos son algunos de los misterios más antiguos y fascinantes de la matemática.

Teorema 6.16 (Euclides). *Existen infinitos números primos.*

Demostración. Supongamos que hay un número finito de números primos, digamos $p_1, \ldots, p_n$. Consideremos el número

$$N = p_1 p_2 \cdots p_n + 1.$$

Como $N > 1$, N tiene un divisor primo p. Luego, $p = p_i$ para algún $1 \leq i \leq n$. Luego p divide a N y a $N-1$, de donde p divide a 1, absurdo. □

Existen más de 150 pruebas de esta hecho en la literatura, aunque algunas pruebas no son tan elementales como la de Euclides. Nosotros damos nuestra propia prueba.

Demostración alternativa. Supongamos que el conjunto de números primos $\mathbb{P}$ fuera finito y sea $p_1 = 2 \leq p_2 = 3 \leq p_3 = 5 \leq \cdots \leq p_n$ todos ellos. Consideremos los números

$$N^+ = p_1 \cdots p_{n-1} + 1, \qquad N^- = p_1 \cdots p_{n-1} - 1.$$

Podemos asumir que $n \geq 3$, pues sabemos que 2, 3 y 5 son primos. Los números $N^{\pm} \geq 2$ tienen un divisor primo, que no puede ser ninguno de los primos $p_1, \ldots, p_{n-1}$. Así, la única posibilidad es que $p = p_n$ y, por lo tanto, $p_n \mid N^+ - N^- = 2$. De este modo $p_1 = \cdots = p_n = 2$. Luego, si $\mathbb{P}$ es finito entonces $\mathbb{P} = \{2\}$. Pero 3 es un primo distinto de 2, una contradicción. Luego, $\mathbb{P}$ es infinito. □

6.4. El máximo común divisor

Dados dos enteros a y b, alguno de ellos no nulo, el conjunto de divisores comunes, es un conjunto no vacío y finito. Esto es así ya que el conjunto de divisores de cualquier entero no nulo contiene al 1 y es finito. El mayor de estos divisores comunes tiene un rol destacado en la aritmética entera. En esta sección aprenderemos a calcularlo y presentaremos sus propiedades fundamentales.

Ejemplos. Determinamos por inspección el mcd en varios casos. Como 1 es siempre divisor común basta considerar los divisores positivos comunes.

	divisores positivos	divisores comunes	mcd
$a = 12$ $b = -30$	$\{1, 2, 3, 4, 6, 12\}$ $\{1, 2, 3, 5, 6, 10, 15, 30\}$	$\{1, 2, 3, 6\}$	6
$a = 15$ $b = 28$	$\{1, 3, 5, 15\}$ $\{1, 2, 4, 7, 14, 28\}$	$\{1\}$	1
$a = -8$ $b = 24$	$\{1, 2, 4, 8\}$ $\{1, 2, 3, 4, 6, 8, 12, 24\}$	$\{1, 2, 4, 8\}$	8

Definición. Dados dos enteros a y b no simultáneamente nulos, el *máximo común divisor* de a y b, es el mayor de los divisores comunes de a y b.

Notación. El máximo común divisor de a y b se denota por (a, b) o también por $\text{mcd}(a, b)$.

Luego, podemos escribir

$$(a, b) = \text{máx}\{\text{Div}(a) \cap \text{Div}(b)\}.$$

Definición. Dos enteros se dicen *coprimos*, si $(a, b) = 1$.

Entre las propiedades básicas del mcd, inmediatas de su definición, se tienen:

- $(a, b) \geq 1$.
- $(a, b) = (b, a)$.
- $(1, a) = 1$ y $(0, b) = |b|$.
- $(a, b) = (|a|, |b|)$ y en particular $(a, b) = (-a, b) = (a, -b) = (-a, -b)$.

Dados dos enteros a y b, no simultáneamente nulos, se tiene que

$$\frac{a}{(a, b)} \quad \text{y} \quad \frac{b}{(a, b)}$$

son enteros (y resultan coprimos, como veremos más adelante).

6.4.1. Combinaciones lineales enteras

Una propiedad muy útil del $\mathrm{mcd}(a,b)$ es la de escribirse como *combinación lineal entera* de a y b. Es decir, $d=(a,b)$ se puede escribir como

$$d = ma + nb,$$

para algunos enteros m y n.

Por un lado está claro que todo entero $e = ra + sb$ es un múltiplo de $d = (a,b)$ ya que como $d \mid a$ y $d \mid b$, luego $d \mid ra$ y $d \mid sb$ y finalmente $d \mid e$. Ahora no todo $e = ra + sb$ es divisor común de a y b; por ejemplo $e = (-5)\times 2 + 5 \times 3 = 5$ y 5 no es divisor de 2 ni de 3. Sin embargo, el menor natural e que se puede escribir de la forma $e = ma + nb$ si es un divisor común de a y b y notablemente es el mayor de ellos, es decir es el igual al $\mathrm{mcd}(a,b)$. Por ejemplo $1 = (-1)\times 2 + 1 \times 3 = (2,3)$. Es bueno notar que un mismo e puede escribirse de distintas formas como combinación lineal entera de dos enteros a y b dados.

Ejemplos.

(1) $(2,3) = 1 = (-1)\times 2 + 1 \times 3 = (2,3) = (-2)\times 4 + 3 \times 3 = 11 \times 2 + (-7) \times 3.$

(2) $(33, 105) = 3 = 6 \times 105 - 19 \times 33 = -5 \times 105 + 16 \times 33.$

Proposición 6.17. *Dados dos enteros a y b, no simultáneamente nulos, el $\mathrm{mcd}(a,b)$ es el menor natural que se escribe como combinación lineal entera de a y b.*

Demostración. Sea $e = ma + nb$ el menor natural que es combinación lineal entera de a y b. Veamos primero que e es un divisor común de a y b. Dividiendo a y b por e, existen (únicos) enteros p, q, r, s tales que

$$\begin{aligned} a &= qe + r, \qquad 0 \le r < e, \\ b &= pe + s, \qquad 0 \le s < e. \end{aligned}$$

Si $r \neq 0$,

$$\begin{aligned} r &= a - qe \\ &= a - q(ma + nb) \\ &= a - qma - qnb \\ &= (1 - qm)a - qnb, \end{aligned}$$

lo que contradice el hecho de ser e la menor combinación lineal entera de a y b. Luego, $r = 0$. Análogamente, sale que $s = 0$ y así $e \mid a$ y $e \mid b$.

Además, e es el mayor de los divisores comunes de a y b ya que si $f \mid a$ y $f \mid b$, entonces $f \mid e$ y $f \le e$. Por lo tanto $e = \mathrm{mcd}(a,b)$. □

Esta proposición tiene varias consecuencias importantes de distinta índole.

Consecuencia 1: Sobre un número dividiendo a un producto de dos números.

Sabemos que, en general, si a divide a un producto bc no es cierto que a divide a alguno de los factores. Sin embargo, si a es coprimo con uno estos factores, digamos b, entonces sí podemos asegurar que a divide al otro factor c.

Corolario 6.18. *Si $a \mid bc$ con a y b coprimos, entonces $a \mid c$.*

Demostración. Como $(a, b) = 1$ entonces existen $r, s \in \mathbb{Z}$ tales que $1 = ra + sb$. Multiplicando por c tenemos $c = rac + sbc$. Ahora, como $a \mid bc$, $bc = at$ para algún entero t. Luego

$$c = rac + s(at) = a(rc + st)$$

de donde se sigue que $a \mid c$. □

Consecuencia 2: Sobre cómo mostrar que dos números son coprimos.

Si dados a y b logramos escribir al 1 como combinación lineal entera de a y b, es decir $1 = ma + nb$ para ciertos enteros m, n, entonces a y b son coprimos, ya que 1 es el menor de todos los naturales. De este hecho se sigue el siguiente corolario.

Corolario 6.19. *Dados $a, b \in \mathbb{Z}$, no simultáneamente nulos, $\frac{a}{(a,b)}$ y $\frac{b}{(a,b)}$ son coprimos.*

Demostración. Sean $r, s \in \mathbb{Z}$ tales que $(a, b) = ra + sb$. Luego

$$1 = r\frac{a}{(a,b)} + s\frac{b}{(a,b)}.$$

Se sigue lo que queríamos probar. □

Consecuencia 3: Sobre el cálculo efectivo del mcd.

Una consecuencia más de la Proposición 6.17, es el siguiente resultado que muchas veces facilita el cálculo del mcd.

Proposición 6.20. *Sean a y b enteros dados, no simultáneamente nulos. Entonces, para cualquier entero m, $(a, b) = (a, b + ma)$.*

Demostración. Sea $d = (a, b)$. Entonces existen r, s tales que $d = ra + sb$. Ahora sea $r' = r - sm$. Tenemos que

$$r'a + s(b + ma) = (r - sm)a + sb + sma = ra - sma + sb + sma = ra + sb = d.$$

Es decir, d es una combinación lineal entera de a y $b + ma$. Además, es la menor, pues es en particular una combinación lineal de a y b. □

Consecuencia 4: Otra caracterización del mcd.

En algunos textos el mcd se define de otro manera, equivalente a la que dimos en estas notas. Esa definición es la que está contenida en la siguiente proposición.

Proposición 6.21. *Sean a y b enteros no simultáneamente nulos y sea $d = (a, b)$. Entonces d satisface:*

(a) $d \mid a$ y $d \mid b$;

(b) si d' es otro entero tal que $d' \mid a$ y $d' \mid b$, entonces $d' \mid d$.

Recíprocamente, si d es natural y satisface estas dos propiedades, entonces $d = (a, b)$.

Demostración. Siendo d divisor común de a y b, se tiene en particular que $d \mid a$ y $d \mid b$. Además como $d = ma + nb$, si $d' \mid a$ y $d' \mid b$, entonces $d' \mid ma + nb$, es decir $d' \mid d$.

Ahora si d satisface (a) se sigue que es un divisor común de a y b y si satisface (b) se sigue que $d = |d| \geq |d'| \geq d'$ para cualquier otro divisor común d'. Luego es el mayor de los divisores comunes de a y b, es decir $d = (a, b)$. □

6.4.2. El algoritmo de Euclides

Euclides (300 AC) propuso el siguiente algoritmo para calcular el mcd de dos naturales a y b sin necesidad de conocer todos los divisores de a y b. Este algoritmo se basa en el siguiente hecho.

Proposición 6.22. *Dados a, b enteros cualesquiera, no simultáneamente nulos, sean $a = qb + r$ la división entera de a por b. Entonces $(a, b) = (b, r)$.*

Demostración. Por la Proposición 6.20 $(a, b) = (b, a) = (b, a - qb) = (b, r)$. □

Dado esto, para calcular el mcd de a y b (ambos positivos) dividimos el más grande, digamos a, por le más chico, b, y tenemos que $(a, b) = (b, r)$, donde r es el resto. Ahora, $a \leq b$ y $r \leq b$, por lo tanto hemos cambiado el par a, b por otro más chico. Iterando esto encontraremos un par muy pequeño al que podamos calcularle el mcd fácilmente.

Ejemplo. Veamos cómo funciona para $a = 30855$ y $b = 20475$.

- Dividimos 30855 por 20475: $30855 = 1 \times 20475 + 10380$. Luego $d = (20475, 10380)$.
- Dividimos 20475 por 10380: $20475 = 1 \times 10380 + 10095$. Luego $d = (10380, 10095)$.
- Dividimos 10380 por 10095: $10380 = 1 \times 10095 + 285$. Luego $d = (10095, 285)$.
- Dividimos 10095 por 285: $10095 = 35 \times 285 + 120$. Luego $d = (285, 45)$.
- Dividimos 285 por 120: $285 = 2 \times 120 + 45$. Luego $d = (120, 45)$.
- Dividimos 120 por 45: $120 = 2 \times 45 + 30$. Luego $d = (45, 30)$.
- Divimos 45 por 30: $45 = 1 \times 30 + 15$. Luego $d = (30, 15)$.
- Dividimos 30 por 15: $30 = 2 \times 15 + 0$. Luego $d = (15, 0) = 15$.

Este algoritmo requiere hacer la división entera de dos naturales. Para esto conocemos un algortimo que aprendimos en la escuela que es más eficiente que el de buscar entre los múltiplos de uno de ellos uno que se aproxime al otro. Puede suceder que sea necesario hacer muchos pasos antes de terminar con el mcd. Sin embargo, es sistemático y siempre termina con el mcd.

Escribimos ahora el algoritmo descripto en el ejemplo para ser aplicado a cualquier par a y b de enteros no simultáneamente nulos.

ALGORITMO DE EUCLIDES

PASO 1. Podemos suponer que $a, b \geq 0$, tomando $|a|$ y $|b|$ y podemos suponer que $a \geq b$.

PASO 2. Si $a = b$, entonces $(a, b) = a$. FIN

PASO 3. Si $b = 0$, entonces $(a, b) = a$. FIN

PASO 4. Sean $a' = a$ y $b' = b$. Dividimos a' por b': $a' = q \times b' + r$. Si $r = 0$, entonces $(a, b) = (a', b') = b'$. FIN

PASO 5. Se repite el paso anterior con $a' = b'$ y $b' = r$ hasta terminar

6.5. El Teorema fundamental de la aritmética

Del primer corolario de la Proposición 6.17 se sigue una propiedad fundamental de los números primos: si un primo divide al producto de dos enteros, entonces divide al menos a uno de ellos. Es decir, si p es primo, entonces

$$p \mid ab \qquad \Rightarrow \qquad p \mid a \quad \text{ó} \quad p \mid b.$$

Esto no es cierto si p no es primo; $6 \mid 2{,}3$, sin embargo $6 \nmid 2$ y $6 \nmid 3$.

Proposición 6.23. *Dados dos enteros a y b y un primo p, si $p \mid ab$, entonces $p \mid a$ ó $p \mid b$.*

Demostración. Supongamos que $p \nmid a$ y veamos que entonces $p \mid b$. Como $p \nmid a$ y p es primo, $\mcd(a, p) = 1$, luego por el Corolario 6.18 existen m y n tales que $1 = ma + np$, de donde se sigue que $b = bma + bnp$. Como $p \mid ab$, $p \mid bma$ y además $p \mid bnp$, luego $p \mid b$. □

Esta proposición es fundamental para probar la unicidad en la descomposición como producto de primos de cualquier entero.

Teorema 6.24 (Teorema Fundamental de la Aritmética)**.** *Todo número entero no nulo distinto de 1 ó -1 es el producto de números primos si es positivo y es el producto de -1 por un producto de números primos si es negativo. Los distintos factores primos que aparecen y sus multiplicidades son únicos. Es decir, la factorización mencionada es única salvo el orden de sus factores.*

Demostración. Basta suponer que a es natural.

EXISTENCIA: Se sigue directamente de la Proposición 6.15.

UNICIDAD: Sean $a = p_1 \dots p_r$ y $a = q_1 \dots q_s$ dos factorizaciones de a como producto de números primos, con $r, s \geq 1$. Debemos mostrar que $r = s$ y que para cada $1 \leq i \leq r$ existe un $1 \leq j_i \leq s$ tal que $p_i = q_{j_i}$ donde $j_i \neq j_k$ si $i \neq k$. Hacemos esto por inducción

en el mayor de los naturales r y s, que podemos suponer sin pérdida de generalidad que es r.

Paso 1: Si $r = 1$, entonces $a = p_1$ y $a = q_1$, luego $r = s$ y $p_1 = q_1$.

Paso 2: Supongamos que $r = n + 1$. Así $a = p_1 \dots p_n p_{n+1}$ y $a = q_1 \dots q_s$ con $s \leq n + 1$. Ahora, $p_{n+1} \mid a$, luego por el Lema 6.14 $p_{n+1} \mid q_j$ para algún $1 \leq j \leq n + 1$. Siendo ambos primos, se sigue que son iguales, es decir $p_{n+1} = q_j$. Si $j \neq s$, permutamos en la segunda factorización q_j con q_s, y así resulta que $p_{n+1} = q_s$. Por la propiedad cancelativa se sigue que

$$a' = p_1 \cdots p_n = q_1 \cdots q_{s-1}.$$

Tenemos ahora dos factorizaciones de a' como producto de números primos, una con n factores y otra con $s - 1$ factores, con $n \geq s - 1$. Por lo tanto, por hipótesis inductiva, se sigue que $n = s - 1$ y que para cada $1 \leq i \leq n$ existe un $1 \leq j_i \leq s$ tal que $p_i = q_{j_i}$, donde $j_i \neq j_k$ si $i \neq k$. De esto se sigue que $n + 1 = s$ y que para cada $1 \leq i \leq n + 1$ existe un $1 \leq j_i \leq s$ tal que $p_i = q_{j_i}$ donde $j_i \neq j_k$ si $i \neq k$. □

El TFA tiene consecuencias profundas en la aritmética entera y también, por ejemplo, en la estructura y aritmética de los reales, como muestran los siguientes problemas.

Problemas.

(1) Probar que el número real $\sqrt{2}$ es irracional.

(2) ¿Es posible caracterizar a los naturales n tales que $\sqrt{n}$ es racional?

(3) Si n es un natural tal que $28 \mid n$ y $45 \mid n$, entonces $n \geq 1000$.

(4) Hallar todas las soluciones enteras de la ecuación $2n = 3m - 2$.

Soluciones.

(1) Supongamos, por el absurdo, que $\sqrt{2}$ es un número racional; así $\sqrt{2} = n/m$ para ciertos naturales n, m. Luego $\sqrt{2}m = n$ y $2m^2 = n^2$. Es decir n y m satisfacen la ecuación entera.

$$2m^2 = n^2.$$

Pero esta ecuación no tiene soluciones enteras. Esto es consecuencia directa del TFA. En efecto en la factorización prima de $2m^2$ el 2 aparece al menos con multiplicidad 1, dependiendo si aparece o no en la factorización de m. Si la multiplicidad del 2 en m es i, entonces la multiplicidad del 2 en m^2 es $2i$. Por lo tanto la multiplicidad del 2 en $2m^2$ es siempre impar. Sin embargo la multiplicidad del 2 en n^2 es siempre par.

(2) Si podemos decir exactamente cuáles son los naturales n tales que $\sqrt{n}$ es racional, repitiendo el argumento usado con el 2. Supongamos que $sqrtn = a/b$, para ciertos naturales a, b. Entonces,

$$n \cdot b^2 = a^2.$$

Si p es un primo que aparece en la factorizacón prima de n, debe aparecer en la factorización prima de a^2; es ésta última a parece con multiplicidad par. Luego aparece

también en b^2. Como en b^2 aparece con multiplicidad par, se sigue que en n aparece con multiplicidad par. Así es necesario que todas las multiplicidades de los primos de la factorización de n sean pares. Ahora, ésto es también suficiente para que $\sqrt{n}$ sea racional, más aún, naturtal!

Podemos concluir entonces que $\sqrt{n}$ es natural o irracional y es natural si y sólo si es un cuadrado perfecto.

(3) Como $28 = 2^2 \cdot 7$, $45 = 3^2 \cdot 5$ y $n = 28a$ y $n = 45b$, en la factorización prima de n aparecen 2^2, 7, 3^2 y 5. Es decir $n = 2^2 \cdot 7 \cdot 3^2 \cdot 5 \cdot m$ para algún natural m. Como $2^2 \cdot 7 \cdot 3^2 \cdot 5 = 1260$ se sigue que $n \geq 1260$ y en particular $n \geq 1000$.

(4) La ecuación $2n = 3m - 2$ es equivalente a la ecuación $2(n+1) = 3m$. Cualquier solución de ésta satisface que $2 \mid m$ y $3 \mid n+1$. Así $m = 2a$, $n + 1 = 3b$ y la ecuación se reescribe como $2 \cdot 3b = 3 \cdot 2a$, es decir $6b = 6a$. Todas las soluciones de esta última son $a = b$. Luego todas la soluciones de la ecuación original son de la forma

$$m = 2a \quad \text{y} \quad n = 3a - 1$$

donde a es un entero cualquiera.

6.6. El mínimo común múltiplo

Dados dos enteros a y b no nulos, los conjuntos de sus múltiplos, I_a e I_b, son infinitos. Siempre tienen intersección no vacía, ya que $ab \in I_a \cap I_b$ y como si $m \in I_a \cap I_b$ entonces $-m \in I_a \cap I_b$, esta intersección tiene elementos positivos, es decir siempre hay múltiplos naturales comunes. Por el PBO (principio de buena ordenación), existe un menor múltiplo común de a y b. Si alguno, a o b, es igual a cero entonces $I_a \cap I_b = \{0\}$.

Definición. Dados dos enteros a y b, el *mínimo común múltiplo* de a y b es el menor entero no negativo que es múltiplo de ambos.

Notación. Denotamos al mínimo común múltiplo de a y b por $[a, b]$ o $\mathrm{mcm}(a, b)$.

Entre las propiedades básicas del mcm, inmediatas de su definición, se tienen:

- $[a, b] = [b, a]$.
- $[1, b] = |b|$ y $[0, b] = 0$.
- $[a, b] = [|a|, |b|]$ y en particular $[a, b] = [-a, b] = [a, -b] = [-a, -b]$.

Proposición 6.25. *Si k es un múltiplo común de a y b y $a, b \neq 0$, entonces $[a, b] \mid k$.*

Demostración. Dividiendo k por $[a, b]$ se tiene que $k = q[a, b] + r$, con $0 \leq r < [a, b]$. Ahora como $a \mid k$ y $a \mid [a, b]$, entonces $a \mid r$ y análogamente $b \mid [a, b]$, luego r es un múltiplo común de a y b menor que $[a, b]$, esto implica que $r = 0$ y que $[a, b] \mid k$. □

Teorema 6.26. *Si a y b son enteros no negativos no simultáneamente nulos entonces*

$$ab = (a, b)[a, b].$$

Demostración. Veamos que el número $\dfrac{ab}{(a,b)}$ es un múltiplo común de a y b y que divide a todo otro múltiplo común; luego es el mínimo común múltiplo de a y b.

Como $(a,b) \mid a$ y $(a,b) \mid b$, tenemos que

$$\frac{ab}{(a,b)} = a\frac{b}{(a,b)} = b\frac{a}{(a,b)},$$

y así $\dfrac{ab}{(a,b)}$ es un múltiplo común de a y b.

Ahora, sea m un múltiplo común positivo de a y b. Es decir $m = ra = sb$ con $r, s \in \mathbb{N}$. Luego

$$r\frac{a}{(a,b)} = s\frac{b}{(a,b)}.$$

Como $\frac{a}{(a,b)}$ y $\frac{b}{(a,b)}$ son coprimos, $\frac{b}{(a,b)}$ divide a r (Proposición 6.18). Por lo tanto, $r = t\frac{b}{(a,b)}$ y luego

$$m = ra = t\frac{ab}{(a,b)}.$$

La prueba está completa. □

6.7. El TFA, divisores, mcd y mcm

Dado un $a \in \mathbb{N}$, $a \neq 1$, se tiene que $a = p_1^{i_1} \dots p_r^{i_r}$, donde $p_1, \dots, p_r$ son todos los primos distintos que aparecen en la (única) factorización de a como producto de primos y los naturales $i_1, \dots, i_r$ son sus multiplicidades (también únicas). Análogamente, dado un $b \in \mathbb{N}$, $b \neq 1$, $b = q_1^{j_1} \dots q_s^{j_s}$ donde $q_1, \dots q_s$ son todos los primos distintos que aparecen en la factorización de b como producto de primos y $j_1, \dots, j_s$ sus multiplicidades. Cuando necesitamos trabajar simultáneamente con las factorizaciones de dos números, como las de a y b, es conveniente unificarlas de algún modo. Una manera efectiva de hacer esto, es considerar todos los primos distintos que aparecen en alguna de las dos factorizaciones, digamos $P_1, P_2, \dots, P_k$, y permitir a las multiplicidades de estos primos ser 0. Así, si uno de lo primos P_i no aparece en la factorización de a su multiplicidad en a es 0; como $P_i^0 = 1$ esto no produce ningún problema.

Ejemplos.

(1) $a = 18 = 2^1 \cdot 3^2$ y $b = 20 = 2^2 \cdot 5$. Los primos que aparecen en alguna de las factorizaciones de estos dos númeors son 2, 3 y 5. Luego escribimos ambas usando estos 3 primos. Así $a = 18 = 2^1 \cdot 3^2 \cdot 5^0$ y $b = 20 = 2^2 \cdot 3^0 \cdot 5^1$. Las multiplicidades son en el primer caso 1, 2 y 0 y en el segundo caso son 2, 0 y 1.

(2) A continuación mostramos las factorizaciones de varios naturales en las que aparecen los primos 2, 3, 5 o 7.

	2	3	5	7	
20	2	0	1	0	$2^2 \cdot 3^0 \cdot 5^1 \cdot 7^0$
315	0	2	1	1	$2^0 \cdot 3^2 \cdot 5^1 \cdot 7^1$
350	1	0	2	1	$2^1 \cdot 3^0 \cdot 5^2 \cdot 7^1$
4410	1	2	1	2	$2^1 \cdot 3^2 \cdot 5^1 \cdot 7^2$

El hecho se ser a divisor de b, se puede expresar de manera simple en términos de estas listas de primos y multiplicidades. También el $\mathrm{mcd}(a,b)$ y el $\mathrm{mcm}(a,b)$ se calculan de manera simple a partir de estas listas.

Proposición 6.27. *Dados dos naturales a y b, con $a = p_1^{i_1} p_2^{i_2} \dots p_r^{i_r}$ y $b = p_1^{j_1} p_2^{j_2} \dots p_r^{j_r}$ sus factorizaciones primas, entonces $a \mid b$ si y sólo si $i_k \le j_k$ para todo $k = 1 \dots r$. Es decir, $a \mid b$ si y sólo si los primos en la factorización de a aparecen menor o igual número de veces que en b. Por lo tanto el conjunto de divisores de a es*

$$\mathrm{Div}(a) = \{\pm p_1^{e_1} \cdots p_r^{e_r} : 0 \le e_k \le i_k,\ k = 1, \dots, r\}$$

Demostración. FALTA. □

Una aplicación directa de esta proposición es que podemos escribir todos los divisores de un a dado a partir de su factorización. Si $a = p_1^{i_1} p_2^{i_2} \dots p_r^{i_r}$, para escribir un divisor de a debemos elegir las multiplicidades que querramos para los primos $p_1, \dots, p_r$, recordando que éstas deben ser menores, o la sumo iguales, que las multiplicidades $i_1, \dots, i_r$. Por ejemplo si

$$a = p_1^3 p_2^2 p_3^5,$$

algunos divisores (propios) de a son

$$d = p_1^1 p_2^2 p_3^0 = p_1 p_2^2, \quad e = p_1^3 p_2 p_3^4, \quad f = p_1^0 p_2^0 p_3^1 = p_3.$$

Para cada primo p_k tenemos $i_k + 1$ elecciones para la multiplicidad de ese primo en el divisor. Esto nos permite contar la cantidad total de divisores (positivos), propios y no, de a.

Corolario 6.28. *Si p es primo, entonces p^n tiene $n+1$ divisores positivos: $1, p, p^2, p^3, \dots, p^{n-1}, p^n$.*

Más generalmente, tenemos lo siguiente.

Corolario 6.29. *Si $a = p_1^{i_1} \dots p_r^{i_r}$ es la factorización prima de a, donde $p_1, \dots, p_r$ son todos primos distintos y $i_1, \dots, i_r$ son naturales, tiene exactamente $(i_1+1)(i_2+1)\dots(i_r+1)$ divisores positivos.*

Demostración. El resultado es intuitivamente claro. La prueba la veremos más adelante como aplicación de las técnicas de conteo (ver Ejemplo en §11.1.2). □

Ejemplos.

(1) El número $105 = 3 \times 5 \times 7$ tiene exactamente 8 divisores positivos: 1, 3, 5, 7, 3×5, 3×7, 5×7 y 105.

(2) El número $1575 = 3^2 \times 5^2 \times 7$ tiene exactamente 18 divisores positivos. éstos son todos de la forma

$$d = 3^i \times 5^j \times 7^k, \qquad 0 \leq i \leq 2, \quad 0 \leq j \leq 2, \quad 0 \leq k \leq 1.$$

La siguiente tabla muestra todas las posibilidades para las multiplicidades de 3, 5 y 7 en la factorización de los diviosres de 1575 y el correspondiente divisor.

i	0	0	0	0	0	0	1	1	1	1	1	1	2	2	2	2	2	2
j	0	0	1	1	2	2	0	0	1	1	2	2	0	0	1	1	2	2
k	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
d	1	7	5	35	25	175	3	21	15	105	75	525	9	63	45	315	225	1575

Proposición 6.30. *Dados dos naturales a y b, con $a = p_1^{i_1} p_2^{i_2} \dots p_r^{i_r}$ y $b = p_1^{j_1} p_2^{j_2} \dots p_r^{j_r}$ sus factorizaciones primas, entonces se tiene que:*

(a) El $\operatorname{mcd}(a,b)$ es el producto de los primos de sus factorizaciones, con la menor de las multiplicidades con la que aparecen en ellas. Es decir,

$$(a,b) = p_1^{\min(i_1,j_1)} p_2^{\min(i_2,j_2)} \dots p_r^{\min(i_r,j_r)}.$$

(b) El $\operatorname{mcm}(a,b)$ es el producto de los primos de sus factorizaciones, con la mayor de las multiplicidades con la que aparecen en ellas. Es decir,

$$[a,b] = p_1^{\max(i_1,j_1)} p_2^{\max(i_2,j_2)} \dots p_r^{\max(i_r,j_r)}.$$

Demostración. FALTA □

Corolario 6.31. *Si $a \mid c$, $b \mid c$ y $(a,b) = 1$, entonces $ab \mid c$.*

6.7.1. La función φ de Euler †

La función φ de Euler, es la *función aritmética*, que cuenta la cantidad de coprimos positivos de un natural dado. Precisamente, $\varphi : \mathbb{N} \to \mathbb{N}$,

$$\varphi(n) = |\{m \in \mathbb{N} : \ (m,n) = 1\}|.$$

Se sigue directamente de la definición de φ que $\varphi(1) = 1$ y que $\varphi(p) = p - 1$si p es primo ya que todos los naturales $1, 2, \dots, p-1$ son copirmos con p. Una propiedad fundamental y no evidente de φ es el hecho de ser una función aritmética multiplicativa, aunque no fuertemente multiplicativa.

Proposición 6.32. *La función aritmética de Euler φ, es multiplicativa, esto es*

$$\varphi(mn) = \varphi(m)\varphi(n),$$

si m y n son coprimos.

A esta altura no estamos en condiciones de dar una demostración de este hecho. Más adelante, cuando estudiemos aritmética modular, derivaremos una demostración de este hecho.

Observación. La función φ no es fuertemente multiplicativa, esto es, no es cierto que $\varphi(mn) = \varphi(m)\varphi(n)$ cualesquiera sean m y n. Por ejemplo $\varphi(4) = 2$, sin embargo $\varphi(2)\varphi(2) = 1 \times 1 = 1$.

Proposición 6.33. *Si $n = p^k$ donde p es primo y k un natural, entonces*

$$\varphi(n) = p^k - p^{k-1}.$$

Si $n = p_1^{i_1} \dots p_r^{i_r}$, donde $p_1, \dots, p_r$ son todos primos distintos y $i_1, \dots, i_r$ son naturales, entonces

$$\varphi(n) = n \prod_{j=1}^{r} \left(1 - \frac{1}{p_j}\right).$$

Demostración. Los enteros que no son coprimos con p^k son los de la forma pm con $1 \leq m \leq p^{k-1}$. Éstos son en total p^{k-1}. Luego la cantidad de coprimos con p^k es $p^k - p^{k-1}$.

Como φ es multiplicativa, entonces

$$\varphi(n) = \varphi(p_1^{i_1}) \dots \varphi(p_r^{i_r})$$

Además $\varphi(p_j^{i_j}) = p_j^{i_j} - p_j^{i_j - 1} = p_j^{i_j}\left(1 - \frac{1}{p_j}\right)$. Luego se sigue que

$$\varphi(n) = \prod_{j=1}^{r} p_j^{i_j}\left(1 - \frac{1}{p_j}\right) = n \prod_{j=1}^{r}\left(1 - \frac{1}{p_j}\right)$$

□

6.8. Representación decimal y desarrollos s-ádicos

El sistema de notación decimal que aprendemos en la escuela primaria para representar a los números naturales y enteros, y también a los racionales, utiliza 10 símbolos. A pesar de no ser caprichosa la elección del 10, también son posibles otras elecciones.

6.8.1. Representación decimal de enteros

El número 20376 es distinto del número 32607 a pesar de estar ambos escritos con exactamente los mismos símbolos: 0, 2, 3, 7 y 6. Las dos listas de símbolos tienen un significado preciso. La primera representa al número

$$2 \times 10^4 + 0 \times 10^3 + 3 \times 10^2 + 7 \times 10^1 + 6 \times 10^0,$$

mientras que la segunda representa al número

$$3 \times 10^4 + 2 \times 10^3 + 6 \times 10^2 + 0 \times 10^1 + 7 \times 10^0.$$

Una propiedad fundamental de este sistema, es la de no permitir confusiones, es decir no hay dos listas de símbolos que representen el mismo número.

En general, un natural cualquiera a se escribe de manera única como:

$$a = 10^s a_s + 10^{s-1} a_{s-1} + \cdots + 10^2 a_2 + 10 a_1 + 10^0 a_0,$$

con todos los dígitos $0 \leq a_s, \ldots, a_0 \leq 9$. La expresión decimal de a es entonces

$$a = (a_s a_{s-1} \cdots a_2 a_1 a_0)_{10}.$$

La expresión decimal de $-a$ (entero negativo) es

$$-a = -(a_s a_{s-1} \cdots a_2 a_1 a_0)_{10}.$$

Nota (Tengo un sistema mejor!)**.** Consideremos por un momento el siguiente sistema para representar números naturales. Convenimos que la lista de dígitos $a_4 a_3 a_2 a_1$ representa al número $a_4 \times 4 + a_3 \times 3 + a_2 \times 2 + a_1$. Así el 2301 representa al $2 + 3 \times 3 + 1 =$ dieciocho, que escrito en notación decimal es: 18. Pero ahora observamos que el 3200 representa al $3 \times 4 + 2 \times 3$ que es también el dieciocho y observamos que también el 600 representa al dieciocho. Este sistema no es bueno. Un mismo número tiene múltiples representaciones.

Pregunta. ¿Cómo y porqué funciona el sistema de representación decimal?

Respuesta. Sea a un natural dado. Para encontrar su expresión decimal, comenzamo dividendo a por 10:

$$a = 10q_0 + r_0, \quad 0 \leq r_0 \leq 9.$$

Luego $a - r_0$ es divisible por 10 y $(a - r_0)/10 = q_0$. Dividamos ahora q_0 por 10:

$$q_0 = 10q_1 + r_1, \quad 0 \leq r_1 \leq 9.$$

Combinando estas dos expresiones, para a y para q_0, obtenemos:

$$\begin{aligned} a &= 10q_0 + r_0 \\ &= 10(10q_1 + r_1) + r_0 \\ &= 10^2 q_1 + 10^1 r_1 + 10^0 r_0. \end{aligned}$$

Sigamos, dividiendo q_1 por 10 (si es $q_1 \geq 10$).

$$q_1 = 10q_2 + r_2, \quad 0 \leq r_2 \leq 9.$$

Reemplazando en la última expresión de a, tenemos:

$$\begin{aligned} a &= 10q_0 + r_0 \\ &= 10(10q_1 + r_1) + r_0 \\ &= 10^2 q_1 + 10^1 r_1 + 10^0 r_0 \\ &= 10^2(10q_2 + r_2) + 10^1 r_1 + 10^0 r_0 \\ &= 10^3 q_2 + 10^2 r_2 + 10^1 r_1 + 10^0 r_0. \end{aligned}$$

Si $q_2 < 10$, entonces su divisón por 10 es simplemente $q_2 = 10 \cdot 0 + r_3$ con $r_3 = q_2$. Así resulta que

$$a = 10^3 r_2 + 10^2 r_2 + 10^1 r_1 + 10^0 r_0,$$

con $0 \leq r_3, r_2, r_1, r_0 \leq 9$.

A partir de a y haciendo divisiones sucesivas por 10 encontramos los dígitos de la expresión decimal de a. Estos dígitos son únicos pues son restos de la división por 10; el primero es el resto de dividir a a, dado, por 10. El segundo es el resto de dividir a $a - q_0$, con q_0 el único cociente de la división anterior, por 10. Etcétera.

Ejemplo. Tenemos al sistema de representación decimal tan incorporado, que (casi) no nos es posible referirnos a un número natural sin recurrir a ella. Un ejemplo se hace entonces imposible.

Notación. Siendo la expresión decimal la más usual, no se escribe el subíndice 10 salvo que por alguna razón especial sea necesario.

Nota. La expresión decimal de un a y un b como

$$a = 10^s a_s + 10^{s-1} a_{s-1} + \cdots + 10^2 a_2 + 10 a_1 + 10^0 a_0,$$
$$b = 10^t b_t + 10^{t-1} b_{t-1} + \cdots + 10^2 b_2 + 10 b_1 + 10^0 b_0,$$

es útil para entender y explicar los algorítmos de suma y multiplicación que aprendemos en la escuela primaria.

- Suma. Recordemos que para sumar dos números naturales, dadas su expresiones decimales, se ubican uno debajko del otro alineando a la derecha sus últimos dígitos. Luego se suman los últimos dígitos y si el redultado es 10 o mayor se coloca sólo el último dígito y hay que "llevarse" 1, para el momento se sumar los segundos dígitos; este proceso se itera hasta terminar.
- Producto.

6.8.2. El sistema de representación binaria

"Existen 10 clases de personas, las que saben binarios y las que no."

Si en vez de elegir al 10 y los dígitos $0, 1, 2, \ldots, 9$ para representar a los naturales elegimos al 2 y los dígitos $0, 1$, entonces estamos frente al sistema binario de representación.

Pregunta. ¿Cómo y porqué funciona?

Respuesta. De la misma manera y por la misma razón que funciona el sistema decimal. Dado un número natural cualquiera a, sucesivas divisiones por 2 calculan los dígitos (únicos) de la representación binaria de a.

En general, un natural cualquiera a se escribe de manera única como:

$$a = 2^s a_s + 2^{s-1} a_{s-1} + \cdots + 2^2 a_2 + 2 a_1 + 2^0 a_0,$$

con todos los dígitos $0 \leq a_s, \ldots, a_0 \leq 1$. La expresión binaria de a es entonces

$$a = (a_s a_{s-1} \cdots a_2 a_1 a_0)_2.$$

Ejemplo. Ahora si, tomemos el número 37 (escrito en notación decimal) y calculemos su expresión binaria.

$$37 = 2 \cdot 18 + 1,$$

luego el último dígito es 1. Ahora

$$18 = 2 \cdot 9 + 0,$$

luego el segundo dígito (desde la derecha) es 0. Ahora

$$9 = 2 \cdot 4 + 1,$$

$$4 = 2 \cdot 2 + 0,$$

$$2 = 2 \cdot 1 + 0,$$

y

$$1 = 2 \cdot 0 + 1.$$

Por lo cual los siguientes cuatro dígitos son (de derecha a izquierda): 1, 0, 0 y 1. Así resulta que

$$(37)_{10} = (100101)_2.$$

A partir de esta expresión binaria podemos recuperar la expresión decimal usual haciendo:

$$(100101)_2 = 1 \cdot 2^5 + 0 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0 = 32 + 4 + 1 = 37.$$

Las potencias de 2 son tan relevantes para el sistema binario como lo son las potencias de 10 para el sistema decimal. Recordemos la primeras potencias de 2:

$$2^0 = 1, \quad 2^1 = 2, \quad 2^2 = 4, \quad 2^3 = 8, \quad 2^4 = 16, \quad 2^5 = 32,$$

$$2^6 = 64, \quad 2^7 = 128, \quad 2^8 = 256, \quad 2^9 = 512, \quad 2^{10} = 1024.$$

Con estas 11 potencias podemos escribir, en sistema binario, todos los naturales hasta el

$$(11111111111)_2 = 2^{10} + 2^9 + \cdots + 2^2 + 2 + 1 = 2^{11} - 1 = (2047)_{10}.$$

Observación. En el sistema decimal, el número más grande que se puede escribir con 11 dígitos, es decir con las 11 primeras potencias de 10 es

$$99999999999 = 10^{11} - 1.$$

Usando las potencias que de 2 que ya tenemos escritas escribamos, sin hacer las divisiones, algunos naturales menores que 2047 en sistema binario.

- 83: $83 = 64 + 16 + 2 + 1$, luego $(83)_2 = 1010011$.
- 107: $107 = 64 + 32 + 8 + 2 + 1$, luego $(107)_2 = 1101011$.
- 1366: $1024 + 256 + 128 + 32 + 4 + 2$, luego $(1366)_2 = 10110100110$.
- 512: $512 = 512$, luego $(512)_2 = 1000000000$.

6.8.3. Los sistemas de representación s-ádicos †

6.9. Ejercicios y problemas

¿Cuál es el mayor número primo conocido? Sabemos que existen infinitos números primos pero sólo se conocen explícitamente una cantidad finita de ellos. El mayor de todos es el número de Mersenne $2^{43112609} - 1$ que tiene 12.978.189 de dígitos. Este fue descubierto en el año 2008 gracias a GIMPS[*]*, un proyecto de computadoras en red que se dedica a buscar números primos grandes. Por el descubrimiento GIMPS obtuvo el premio ofrecido por la EFF de $u\$s$ 100.000. Aún se haya vacante el premio de $u\$s$ 250.000 a quien descubra el primer número primo con más de 1.000.000.000 de dígitos*[**]*.*

Ejercicios

Ejercicio 6.1. Sean a un entero negativo y b un entero positivo. Determinar cuáles de los siguientes enteros son positivos, cuáles son iguales a 0 y cuáles son negativos.

(1)

Ejercicio 6.2. Decidir y demostrar cuáles de los siguientes naturales son primos y cuáles no.

(1)

Ejercicio 6.3. Factorizar como producto de primos por ± 1 a los siguientes enteros.

(1)

Ejercicio 6.4. Calcular el cociente y el resto de la división de a por b en los casos:

(1) $a = 133$, $b = -14$. (2) $a = 13$, $b = 111$.

Ejercicio 6.5. Decidir cuáles de las siguientes afirmaciones son verdaderas $\forall a, b, c \in \mathbb{Z}$.

(1) $ab \mid c \Longrightarrow a \mid c$ y $b \mid c$.
(2) $4 \mid a^2 \Longrightarrow 2 \mid a$.
(3) $2 \mid ab \Longrightarrow 2 \mid a$ ó $2 \mid b$.
(4) $9 \mid ab \Longrightarrow 9 \mid a$ ó $9 \mid b$.
(5) $a \mid b + c \Longrightarrow a \mid b$ ó $a \mid c$.
(6) $a \mid c$ y $b \mid c \Longrightarrow ab \mid c$.
(7) $a \mid b \Longrightarrow a \leq b$.
(8) $a \mid b \Longrightarrow a \leq \mid b \mid$.
(9) $a \mid b + a^2 \Longrightarrow a \mid b$.

Ejercicio 6.6. Probar que para todo $n \in \mathbb{Z}$, $n^2 + 2$ no es divisible por 4.

Ejercicio 6.7. Probar que:

(1) La suma de dos pares, es par.

[*] `http://www.mersenne.org/`
[**] `https://www.eff.org/awards/coop`

(2) La suma de dos impares, es par.

(3) La suma de un par mas un impar, es impar.

(4) El producto de dos pares es par.

(5) El producto de dos impares, es impar.

(6) El prodcuto de un par por un impar, es par.

Ejercicio 6.8.

(1) Probar que la suma de 7 enteros consecutivos siempre es divisible por 7.

(2) Probar que el producto de 7 enteros consecutivos siempre es divisible por 7.

(3) ¿Es la suma de 8 enteros consecutivos simepre divisible por 8?

(4) ¿Es la suma de 8 enteros consecutivos alguna vez divisible por 8?

(5) ¿Es el producto de 8 enteros consecutivos simepre divisible por 8?

(6) ¿Es el producto de 8 enteros consecutivos alguna vez divisible por 8?

Ejercicio 6.9. Probar por inducción que las siguientes afirmaciones son verdaderas para todo n natural.

(1) $8 \mid 5^{2n} + 7$.

(2) $15 \mid 2^{4n} - 1$.

(3) $5 \mid 3^{3n+1} + 2^{n+1}$.

(4) $24 \mid 2 \cdot 7^n + 3 \cdot 5^n - 5$.

Ejercicio 6.10. Calcular el mínimo común múltiplo y el máximo común divisor de los siguientes pares de números.

(1) $a = 12$, $b = 15$.

(2) $a = 11$, $b = 13$.

(3) $a = 140$, $b = 150$.

(4) $a = 3^2 \cdot 5^2$, $b = 2^2 \cdot 11$.

(5) $a = 2 \cdot 3 \cdot 5$, $b = 2 \cdot 5 \cdot 7$.

Ejercicio 6.11. Mostrar que 725 y 441 son coprimos y encontrar enteros m y n tales que $1 = m \cdot 725 + n \cdot 441$.

Ejercicio 6.12. (1) Probar que si $(a, 4) = 2$ y $(b, 4) = 2$ entonces $(a + b, 4) = 4$.

(2) Probar que si $(a, b) = 1$ entonces $(a + b, a - b) = 1$ ó 2.

Ejercicio 6.13. Probar que $\sqrt{6}$ es irracional.

Ejercicio 6.14. Decidir si existen enteros n y m tales que:

(1) $m^4 = 27$.

(2) $m^2 = 12n^2$.

(3) $m^3 = 47n^3$.

Ejercicio 6.15. Un entero se dice *"libre de cuadrados"* si no es divisible por el cuadrado de ningún entero distinto de 1. Probar que:

(1) Si n es libre de cuadrados entonces n se escribe como producto de primos, todos distintos.

(2) Todo número entero se escribe como producto de un cuadrado y un entero libre de cuadrados.

Ejercicio 6.16. Expresar 1810, 1816 y 1972 en las bases $s = 3, 5, 7, 11$.

Ejercicio 6.17. Expresar en base 10 los siguientes enteros.

(I) $(1503)_6$ (III) $(1111)_{12}$ (V) $(12121)_3$

(II) $(1111)_2$ (IV) $(123)_4$ (VI) $(1111)_5$

Ejercicio 6.18. Sabiendo que el resto de la división de un entero a por 6 es 2, calcular el resto de:

(1) la división de a por 3.

(2) la división de a por 2.

(3) la división de $a^2 - 3a$ por 6.

(4) la división de $2a^2 + a - 1$ por 3.

Ejercicio 6.19. Si n es un entero impar, probar que $n^4 + 4n^2 + 11$ es divisible por 16.

Ejercicio 6.20. (1) Listar los 5 naturales que en la división por 5 tienen cociente y resto iguales.

(2) Dado un natural a, listar todos los números que al dividirlos por a tienen cociente igual al resto.

Ejercicio 6.21. Sea $n = 132$.

(1) Mostrar que no es posible escribir a n como suma de 2 naturales consecutivos.

(2) Escribir a n como suma de 3 naturales consecutivos.

(3) Determinar todos los posibles r tales que n se puede escribir como suma de r naturales consecutivos, y escribirlo así en esos casos.

(4) Determinar todas las formas de escribir a n como suma de 2 naturales, no necesariamente consecutivos.

Ejercicio 6.22. Probar que las siguientes afirmaciones son verdaderas para todo $n \in \mathbb{N}$.

(I) $99 \mid 10^{2n} + 197$

(II) $9 \mid 7 \cdot 5^{2n} + 2^{4n+1}$

(III) $56 \mid 13^{2n} + 28n^2 - 84n - 1$

(IV) $256 \mid 7^{2n} + 208n - 1$

Ejercicio 6.23. En cada uno de los siguientes casos calcular el máximo común divisor entre a y b y escribirlo como combinación lineal entera de a y b.

(1) $a = 2532$, $b = 63$.

(2) $a = 5335$, $b = 110$.

(3) $a = 131$, $b = 23$.

Ejercicio 6.24. Sean $a, b \in \mathbb{Z}$. Sabiendo que el resto de dividir a a por b es 27 y que el resto de dividir a b por 27 es 21, calcular (a, b).

Ejercicio 6.25. Sean a y b enteros coprimos. Probar que:

(I) $(a \cdot c, b) = (b, c)$ para todo entero c.

(II) a^m y b^n son coprimos, para todo $m, n \in \mathbb{N}$.

(III) $a + b$ y $a \cdot b$ son coprimos.

Ejercicio 6.26. Sean a y b enteros coprimos. Probar que:

(I) $(2a + b, a + 2b) = 1$ ó 3

(II) $(a + b, a^2 + b^2) = 1$ ó 2.

(III) $(a + b, a^2 - ab + b^2) = 1$ ó 3.

Ejercicio 6.27. Sea $n \in \mathbb{N}$. Probar que:

(I) $(2^n + 7^n, 2^n - 7^n) = 1$

(II) $(2^n + 5^{n+1}, 2^{n+1} + 5^n) = 3$ ó 9.

(III) $(3^n + 5^{n+1}, 3^{n+1} + 5^n) = 2$ ó 14.

Ejercicio 6.28. Sea $n \in \mathbb{N}$. Probar que:

(I) si $n \neq 1$ y $n \mid (n-1)! + 1$ entonces n es primo.

(II) si $2^n - 1$ es primo entonces n es primo.

(III) si $2^n + 1$ es primo entonces n es una potencia de 2.

Ejercicio 6.29. Probar que $1 + \frac{1}{2} + \frac{1}{3} + ... + \frac{1}{n}$ no es entero, para todo n natural.

Ejercicio 6.30. Hallar el menor múltiplo de 168 que es un cuadrado.

Ejercicio 6.31. Probar que, para todo natural n, $2^{2^n} - 1$ es divisible por al menos n primos distintos.

Ejercicio 6.32. Encontrar una sucesión de cien números naturales consecutivos tales que todos sean compuestos. Generalizar a una sucesión de n naturales consecutivos.

Ejercicio 6.33. ¿Cuál es la mayor potencia de 3 que divide a $100!$? ¿En cuántos ceros termina el desarrollo decimal de $100!$?

Ejercicio 6.34. Determinar todos los $p \in \mathbb{N}$ tales que p, $p + 2$, $p + 6$, $p + 8$, $p + 12$ y $p + 14$ sean todos primos.

Problemas

Problema 6.35. Sean a y b enteros positivos. Si la división de a por b tiene cociente q y resto r, hallar el cociente y el resto de ...

(1) ... dividir a por $-b$. (2) ... dividir $-a$ por b. (3) ... dividir $-a$ por $-b$.

Problema 6.36. Calcular el cociente y el resto de la división de a por b en los casos:

(1) $a = 3b + 7$, $b \neq 0$.

(2) $a = b^2 - 6$, $b \neq 0$.

(3) $a = n^2 + 5$, $b = n + 2$, $n \in \mathbb{N}$

(4) $a = n + 3$, $b = n^2 + 1$, $n \in \mathbb{N}$.

Problema 6.37 (†)**.** Sea n un número natural. Probar que en todo conjunto de $n+2$ números enteros hay dos tales que su suma o su diferencia es divisible por $2n$. Probar también que el resultado no es cierto si se toman $n + 1$ enteros.

Problema 6.38. Probar que para todo a impar, $a^2 + (a + 2)^2 + (a + 4)^2 + 1$ es divisible por 12.

Problema 6.39. Probar que $\frac{(3n)!}{(3!)^n}$ es entero, para todo n natural.

Problema 6.40. Probar que si d es un divisor común de a y b, ambos no nulos, entonces

$$\text{(i)}\frac{(a,b)}{d} = \left(\frac{a}{d}, \frac{b}{d}\right) \qquad \text{(ii)}\frac{[a,b]}{d} = \left[\frac{a}{d}, \frac{b}{d}\right] \qquad \text{(iii)}\left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right) = 1$$

Problema 6.41. Probar que si $(a, b) = 1$ y $n + 2$ es un número primo, entonces $(a + b, a^2 + b^2 - nab) = 1$ ó $n + 2$.

Problema 6.42. Demostrar que $\forall n \in \mathbb{Z}, n > 2$, existe p primo tal que $n < p < n!$. (Ayuda: pensar qué primos dividen a $n! - 1$.)

Problema 6.43. Hallar todos los $n \in \mathbb{N}$ para los cuales el resto de la división de $n^3 + 4n + 5$ por $n^2 + 1$ es $n - 1$.

Problema 6.44. Sabiendo que el resto de la división de un entero a por 18 es 5, calcular el resto de ...

(I) ... la división de $a^2 - 3a + 11$ por 18.

(II) ... la división de a por 3.

(III) ... la división de $4a + 1$ por 9.

(IV) ... la división de $a^2 + 7$ por 36.

(V) ... la división de $7a^2 + 12$ por 28

(VI) ... la división de $1 - 3a$ por 27.

Problema 6.45. Probar que, para todo $n > 1$, $n^{n-1} - 1$ es divisible por $(n - 1)^2$.

Problema 6.46. En cada uno de los siguientes casos calcular el máximo común divisor entre a y b y escribirlo como combinación lineal entera de a y b.

(1) $a = n^2 + 1$, $b = n + 2$, $n \in \mathbb{N}$.

Capítulo 7

Números complejos

"La única razón por la que nos gustan los números complejos es que no nos gustan los números reales."
Berndt Sturmfels, matemático alemán (1962 –)

Hemos estudiado hasta aquí, y con bastante profundidad, a los números reales y a varios de sus subconjuntos relevantes de números como los naturales y enteros y los racionales. Ahora estudiaremos un conjunto nuevo de números, más grande que el de los reales. Los números complejos.

7.1. ¿Qué son?

Los números complejos se pueden presentar de varias maneras, pero en el fondo son un par ordenado de números reales. Dos números reales donde distinguimos el primero y el segundo. Podemos identificar a los números complejos con los pares ordenados

$$(a, b), \qquad a, b \in \mathbb{R}$$

y decir que como conjunto no son otra cosa que el producto cartesiano

$$\mathbb{R} \times \mathbb{R}$$

Ahora bien, denotar a un número complejo como par ordenado no resulta totalmente satisfactorio sobre todo a la hora de hacer aritmética de manera práctica y eficiente. Una mejor notación para el número complejo asociado al par ordenado (a, b) es

$$a + bi$$

donde, por el momento, tanto i como el signo $+$ son sólo símbolos que distinguen los roles de los dos números reales a y b. El primero de ellos, a, es la *parte real* y el segundo, b, es la *parte imaginaria* del número complejo $a + bi$. Usualmente se denotan por Re e Im respectivamente. Es decir

$$\mathrm{Re}(a + bi) = a \qquad \text{y} \qquad \mathrm{Im}(a + bi) = b$$

El conjunto de todos los números complejo se denota por $\mathbb{C}$. Así tenemos que

$$\mathbb{C} = \{a + bi : \ a, b \in \mathbb{R}\}$$

Ya sabemos qué son los números complejos, conocemos su naturaleza. De ahora en más no será siempre necesario mostrar toda la intimidad de un número complejo exhibiéndolo de la forma $a + bi$, con sus partes real e imaginaria al desnudo. Podemos nombrar a un número complejo con la letra z o la w; también puede ser α un número complejo cuando así lo querramos. Y cuando sea necesario revelar su intimidad, bastará examinar sus partes real e imaginaria. Así si $\mathrm{Re}(z) = a$ y $\mathrm{Im}(z) = b$, entonces

$$z = a + bi$$

Si la parte imaginaria de un número complejo z es nula, en vez de escribir $z = a + 0i$ simplemente escribimos $z = a$ y de manera análoga si la parte imaginaria de z es nula, escribimos $z = bi$ en vez de escribir $z = 0 + bi$. Los complejos sin parte imaginaria, son reales. Más precisamente pensamos a los números reales incluidos en los complejos, $\mathbb{R} \subseteq \mathbb{C}$, vía la identificación

$$a \mapsto a + 0i$$

Los complejos sin parte real son los *imaginarios puros*. El imaginario puro $1i$ se denota simplemente i y es la *unidad imaginaria*.

Ejemplos. Algunos números complejos concretos.

(1) $2 + 3i$ tiene parte real igual a 2 y parte imaginaria igual a 3.

(2) $2 - 3i$ es otra manera de escribir al número complejo $2 + (-3)i$, cuya parte imaginaria es igual a -3.

(3) Si $\mathrm{Re}(z) = -\sqrt{2}$ y $\mathrm{Im}(z) = -\frac{1}{2}$, entonces $z = -\sqrt{2} - \frac{1}{2}i$.

(4) Los números complejos $z_n = \frac{2}{n}i$ con $n \in \mathbb{N}$ son todos imaginarios puros.

(5) Los complejos $w_n = (-1)^n\pi$ con $n \in \mathbb{N}$ son todos reales.

Representación gráfica

La naturaleza de los números complejos, el hecho de ser pares ordenados de números reales, permite de manera natural graficarlos en el plano por medio de coordenadas, donde el eje horizontal representa a la parte real y el eje vertical a la parte imaginaria.

———— DIBUJO ————-

Nota. Esto no es otra cosa que una representación gráfica del producto cartesiano $\mathbb{R} \times \mathbb{R}$.

7.2. Suma y producto

Para darle vida a los números complejos es necesario poder hacer algo con ellos. Como todos los conjuntos de números que conocemos, los complejos se pueden sumar y multiplicar.

Por un momento pensemos e intententemos responder a la siguiente

PREGUNTA: ¿Cómo están definidas la suma y el producto?

Dado que los complejos son pares ordenados de números reales, podrían éstos sumarse y multiplicarse coordenada a coordenada.

——— DIBUJO ———

Si fuera así, tendríamos por ejemplo que $(2+3i)+(-1+2i) = 1+5i$ y $(2+3i).(-1+2i) = -2+6i$. La suma resulataría asociativa, conmutativa, el $0+0i$ sería su elemento neutro y $-a-bi$ el opuesto de $a+bi$. El producto también sería asociativo y conmutativo y el $1+i$ sería la identidad. Sin embargo no todos los complejos distintos de $0+0i$ tendrían inverso; por ejemplo, el número $0+i$ no tendría inverso, pues $(0+i).(a+bi) = 0+bi$ que nunca será igual al $1+i$. El producto de números complejos es más soficticado.

IMPORTANTE: los complejos no se multiplican coordenada a coordenada.

La suma de complejos

La suma de números complejos si está definida coordenada a coordenada. Así, por definición,

$$(a+bi)+(c+di) = (a+c)+(b+d)i \tag{7.1}$$

La suma de complejos que estamos definiendo con el signo $+$ (en azul) está definida en términos de la suma de números reales con el signo $+$ (en rojo). Los otros signos $+$ (en negro) son los que usamos, hasta ahora sólo como símbolos, para escribir a los números complejos. Sin embargo resulta que todos estos símbolos $+$ tienen ahora el sentido unificado de suma de complejos. En efecto, si tomamos el número real a y el número imaginario puro bi y los sumamos con la suma que acabamos de definir tenemos que

$$a+bi = (a+0i)+(0+bi) = (a+0)+(0+b)i = a+bi$$

Además si a y b son dos reales, la suma de ellos como complejos es

$$a+b = (a+0i)+(b+0i) = (a+b)+(0+0)i = a+b;$$

de donde se sigue que la suma de complejos extiende a la suma de reales.

Observaciones. La suma de complejos tiene las mismas propiedades aritméticas que la suma de reales y que la suma de enteros.

(1) Es asociativa y conmutativa. Esto se sigue directamente de la definición (7.1) y el hecho que la suma de reales es asociativa y conmutativa.

(2) El número complejo $0+0i$, que denotamos simplemente 0, es elemento neutro.

(3) Todo número complejo $z = a+bi$ tiene un opuesto, que denotamos $-z$, donde $-z = -a+(-b)i$. Como $(-b)i$ es el opuesto de bi lo denotamos $-bi$ y como $-a+(-b)i$ es la suma (compleja) de $-a$ y $-bi$ escribimos $-z = -a-bi$.

(4) Estas propiedades son exactamente las propiedades básicas de la suma de los reales. Por lo tanto, la aritmética de la suma de los complejos es idéntica a la de los reales. Todos los resultados que sabemos para la suma de reales valen ahora automáticamente para la suma de complejos.

A pesar de no estar probablemente tan familiarizados con los complejos como con los reales, a la ahora de hacer aritmética con la suma de complejos no debemos sentir ni hacer ninguna diferencia.

Ejemplos. Sean $z = 1 + 2i$, $w = -1 + 2i$ y $v = 1 - 2i$.

(1) $z + w = 4i$ un imaginario puro; $z + v = 2$ un número real.

(2) $-(2v - z + w) = -(v - z + v + w) = -(v - z) = -v + z = 4i$.

(3) ¿Tiene la ecuación $X + z = w - v$ solución? ¿Tiene muchas? Tal como en el caso de los reales esta ecuación tiene una única solución:

$$X = w - v - z = -3 + 2i$$

(4) ¿Cuál es el opuesto de $-v$ y el de $2z - 3w + v$? El opuesto de $-v$ es v y el de $2z - 3w + v$ es $-2z + 3w - v$ que puede escribirse como $-6 + 4i$.

La suma de complejos es fácil de entender gráficamente, en el plano. Está dada por la regla del paralelogramo.

———— DIBUJO ————————

El producto de complejos

Ya dijimos que el producto de complejos no está definido coordenada a coordenada y observamos que si así fuera no todos los complejos distintos de 0 tendrían inverso multiplicativo; ésta es una propiedad muy relevante que sería bueno tener, además de preservar la asociatividad, conmutatividad y el resto de las propiedades del producto de los reales por ejemplo.

Antes de definir formalmente el producto de dos números complejos $a + bi$ y $c + di$, hagamos el siguiente ensayo. Supongamos que tenemos definido el producto con las mismas propiedades de los números reales y que además extienda al producto de los reales. Es decir, si multiplicamos dos reales pensados como complejos el resultado sea el mismo que si los multiplicamos como reales. Veamos que sucede entonces:

$$\begin{aligned}(a + bi).(c + di) &= a.(c + di) + bi.(c + di) \\ &= a.c + a.(di) + (bi).c + (bi).(di) \\ &= ac + (ad)i + (bc)i + (bd)i.i\end{aligned}$$

De la última expresión se sigue que el producto sólo depende de cuánto vale $i.i$, es decir i^2. Una vez definido esto, el producto queda totalmente determinado.

Nota. Está claro que podríamos definir $i.i$ de muchas maneras, aunque algunas podrían no ser del todo satisfactorias. Por ejemplo, si definiéramos $i.i = 0$, tendríamos nuevamente complejos no nulos sin inverso.

El producto de los números complejos queda determinado definiendo

$$i.i = -1$$

Así resulta, continuando el ensayo de más arriba, que

$$\begin{aligned}(a+bi).(c+di) &= a.(c+di) + bi.(c+di)\\ &= a.c + a.(di) + (bi).c + (bi).(di)\\ &= ac + (ad)i + (bc)i + (bd)i.i\\ &= ac + (ad+bc)i - bd\\ &= (ac-bd) + (ad+bc)i\end{aligned}$$

Resumiendo tenemos que

$$(a+bi).(c+di) = (ac-bd) + (ad+bc)i \tag{7.2}$$

Ejemplos. Sean $z = 1-2i$, $w = 1+2i$ y $v = 1/\sqrt{2} + 1/\sqrt{2}i$.

(1) $z(1+i) = (1-2i)(1+i) = (1+2) + (1-2)i = 3 - i$.

(2) $zw = (1-2i)(1+2i) = (1+4) + (2-2)i = 5$.

(3) Si $\lambda \in \mathbb{R}$, entonces $\lambda z = (\lambda + 0i)(1-2i) = (\lambda + 0{,}2) + (-\lambda 2 - 0{,}2) = \lambda - \lambda 2i$.

(4) $iv = (0+i)(1/\sqrt{2} + 1/\sqrt{2}i) = (0 - 1/\sqrt{2}) + (0 + 1/\sqrt{2})i = 1/\sqrt{2} + (1/\sqrt{2})i$.

(5) $v^2 = (1/\sqrt{2} + 1/\sqrt{2}i)(1/\sqrt{2} + 1/\sqrt{2}i) = (1/2 - 1/2) + (1/2 + 1/2)i = i$. Es decir v es una raiz cuadrada de i.

(6) z también tiene raiz cuadrada. Consideremos $u = a + bi$ y calculemos

$$(a+bi)(a+bi) = (a^2 - b^2) + 2abi$$

Buscamos a y b tales que $a^2 - b^2 = 1$ y $2ab = -2$. De la segunda se sigue que $b = -1/a$ y luego tenemos que $a^2 - 1/a^2 = 1$; se sigue que $a^4 - 1 = a^2$ o $a^4 - a^2 - 1 = 0$. Poniendo $x = a^2$ resulta la ecuación cuadrática $x^2 - x - 1 = 0$ cuyuas soluciones son $x = \frac{1+\sqrt{5}}{2}$ y $x = \frac{1-\sqrt{5}}{2}$. Siendo solo la primera positiva elejimos $a = \sqrt{\frac{1+\sqrt{5}}{2}}$ y luego $b = -1/a$. Hemos encontrado una raiz cuadrada de z y como su opuesto también es raiz cuadrada de z, hemos encontrado 2.

Observaciones. El producto así definido tiene las mismas propiedades básicas que el producto de los reales. Para mostrar la existencia de inversos debemos trabajar un poquito más. Discutimos ahora brevemente sobre las otras propiedades.

(1) La conmutatividad del producto es clara de (7.2) dado que el producto de los reales es conmutativo.

(2) El 1 es identidad para el producto.

(3) La asociatividad del producto se sigue directamente calculando $z(vw)$ y $(zv)w$. Solo requiere algunos minutos y varios renglones.

(4) Una propiedad importante es la distributividad del producto respecto de la suma. Al igual que en el caso de la asociatividad, basta calcular directamente $z(v+w)$ y $zv+zw$ para observar que son iguales. Este caso requiera algunos renglones más que el anterior.

Nota. ¿Porqué se eligió definir $i.i=-1$? La razón es que así la ecuación $x^2+1=0$ que no tiene solución real, sí la tiene en los complejos. i es una solución!; $-i$ es otra (y de hecho son las dos únicas soluciones).

Algunos cálculos con el producto

Para familiarizarnos con el producto de complejos, menos trasparente y más novedoso que la suma, hacemos ahora algunos cálculos interesantes.

- Las potencias de i.

  Mostramos ahora un fenómeno nuevo, algo que no sucede en los números reales, debido desde luego a la unidad imaginaria i. Calculemos las potencias de i.

i^0	i^1	i^2	i^3	i^4	i^5	i^6	i^7	i^8	i^9	i^{10}
1	i	-1	$-i$	1	i	-1	$-i$	1	i	-1

  Los resultados se repiten cíclicamente: 1, i, -1, $-i$. Cualquiera sea el natural n, i^n toma uno de estos 4 valores. Por ejemplo

$$i^{123}=i^{120}i^3=1.(-i)=-i$$

- La multiplicación por i en el plano.

  Tomemos un complejo z cualquiera, $z=a+bi$, y lo multipliquemos por i:

$$zi=(a+bi)i=ai-b=-b+ai$$

  El siguiente dibujo muestra que los segmentos desde el origen a z y a zi son perpendiculares; es decir zi se obtiene de a paritr de z rotándolo 90 grados en sentido antihorario. Esto es así pues los triángulos rojo y azul son congruentes.

  ———- DIBUJO ————

  Si continuamos y multiplicamos a zi por i, obetenemos zi^2 que es el rotado de zi 90 grados, o lo mismo que z rotado 180 grados. Multiplicando a z por i^3 o a zi^i por i logramos rotar otros 90 grados más y multiplicando por $i^4=1$ volvemos al principio. Así, multiplicando sucesivamente por i, i^2, etc logramos hacer girar el molino en sentido antihorario de a 90 grados.

  — recuadrar —

  La multiplicación pot i, como transformación del plano, es la rotación de 90 grados en sentido antihorario.

- Las potencias de un número complejo.

  Ya estudiamos las pontencias de i. Investiguemos ahora las potencias de $1+i$; los cálculos no son difíciles. Los resultados son:

$(1+i)^1$	$(1+i)^2$	$(1+i)^3$	$(1+i)^4$	$(1+i)^5$
$1+i$	$2i$	$2^{3/2}(-1+i)$	$2^2(-1+0i)$	$2^{5/2}(-1-i)$

$(1+i)^6$	$(1+i)^7$	$(1+i)^8$	$(1+i)^9$	$(1+i)^{10}$
$2^3(0-i)$	$2^{7/2}(1-i)$	$2^4(1+0i)$	$2^{9/2}(1+i)$	$2^5(0+i)$

  Observamos que los resultados no se repiten ciclicamente como en el caso de i, pero es por poco. En la tabla se ve que, salvo un múltiplo real positivo, el complejo $1+i$ se repite en la octava potencia y a partir de ahí si aparece un fenómeno cíclico. Si en la tabla omitimos los múltiplos reales positivos vemos que aparecen 8 complejos distintos que a partir de la octava potencia se repiten. Estos son:

$$1+i, \quad i, \quad -1+i, \quad -1, \quad -1-i, \quad -i, \quad 1-i, \quad 1$$

  El dibujo exhibe lo que vimos.

  ——— DIBUJO ———-

- Raíces cuadradas de reales negativos.

  Ya sabemos que i es una raiz cuadrada de -1 y $-i$ es otra. ¿Tienen todos los reales negativos una raíz cuadrada compleja? La respeusta es sí, y es fácil encontrala usando la unidad imaginaria i. Si a es un real cualquiera, el cuadrado de ai es $-a^2$. Por lo tanto si queremos una raíz cuadrada de -2 por ejemplo, tomamos $a=\sqrt{2}$, y luego $(ai)^2=-2$. En general, una raíz cuadrada de un real negativo $-b$, es $\sqrt{b}i$.

7.3. La conjugación y el módulo

La conjugación y el módulo son dos funciones básicas definidas en los complejos, la primera llegando a los mismos complejos y la segunda llegando a los reales.

- La conjugación $^- : \mathbb{C} \to \mathbb{C}$ está definida por

$$\overline{a+bi} = a-bi.$$

- El módulo $|\ | : \mathbb{C} \to \mathbb{R}$ está definido por

$$|a+bi| = \sqrt{a^2+b^2}.$$

Resulta útil entender el efecto de la conjugación como función del plano en sí mismo vía la identificación $(a,b) \leftrightarrow a+bi$ de los puntos del plano con los números complejos e interpretar geométricamente al módulo

———— DIBUJO ————-

La conjugación resulta ser la reflexión del plano respecto al eje de las abscisas, y el módulo la distancia al orgien (Pitágoras).

En particular se sigue que cualqueira sea z se tiene que

$$|\overline{z}| = |z|$$

La conjugación y el módulo están relacionadas de manera interesante.

Proposición 7.1. *Para todo $z \in \mathbb{C}$ se tiene que*

$$z\overline{z} = |z|^2.$$

Demostración. Si $z = a + bi$, entonces $\overline{z} = a - bi$. Luego

$$z\overline{z} = (a + bi)(a - bi) = (a^2 + b^2) + (-ab + ba)i = a^2 + b^2 = |z|^2$$

□

De está proposición se sigue ahora de manera más o menos directa la existencia de inversos multiplicativos para los complejos no nulos. En efecto, si $z \neq 0$, entonces su módulo es real y no nulo; luego tiene inverso $1/|z|$. Como $z\overline{z} = |z|^2$, tenemos que

$$\frac{z\overline{z}}{|z|^2} = 1,$$

de donde se sigue que $\overline{z}/|z|^2$ es un inverso de z. De la misma manera que probamos que en los reales el inverso de cada número es único, éste es único también. Así denotamos

$$z^{-1} = \frac{\overline{z}}{|z|^2}$$

Las proposiciones que siguen reúnen algunas propiedades básicas de la conjugación y el módulo que es muy bueno conocer pues ayudan a calcular y hacer aritmética con los complejos de manera eficiente.

Proposición 7.2. *Sean z y w números complejos cualesquiera. Se tiene que:*

(a) $\overline{\overline{z}} = z$.

(b) $\overline{z} = z$ *si y sólo si* $z \in \mathbb{R}$. *En particular* $\overline{|z|} = |z|$.

(c) $\mathrm{Re}(z) = \frac{z+\overline{z}}{2}$ *y* $\mathrm{Im}(z) = \frac{z-\overline{z}}{2i}$.

(d) $\overline{z + w} = \overline{z} + \overline{w}$.

(e) $\overline{zw} = \overline{z}\,\overline{w}$.

(f) $\overline{z^{-1}} = \overline{z}^1$.

Demostración. Todos los items se siguen directamente calculando. Suponemos que $z = a + bi$ y $w = c + di$.

(1) Como $\overline{z} = a - bi$, luego $\overline{\overline{z}} = a + bi = z$.

(2) Como $\overline{z} = a - bi$, se sigue que $\overline{z} = z$ si y sólo si $-b = b$, es decir si $b = 0$ o $z \in \mathbb{R}$.

(3) Tenemos que $z + \overline{z} = (a + bi) + (a - bi) = 2a$ y que $z - \overline{z} = (a + bi) - (a - bi) = 2bi$ de donde se sigue el resultado.

(4) Como $z + w = (a + c) + (b + d)i$, $\overline{(z + w)} = (a + c) - (b + d)i$. Por otro lado $\overline{z} + \overline{w} = (a - bi) + (c - di) = (a + c) - (b + d)i$.

(5) Como $zw = (ac - bd) + (ad + bc)i$, $\overline{zw} = (ac - bd) - (ad + bc)i$. Por otro lado $\overline{zw} = (a - bi)(c - di) = (ac - bd) + (-ad - bc)i = (ac - bd) - (ad + bc)i$.

(6) Como $z^{-1} = \overline{z}/|z|^2$ y $|z|$ es real, se sigue por el item anterior que $\overline{z^{-1}} = z/|z|^2$. Por otro lado $\overline{z}^{-1} = \overline{\overline{z}}/|\overline{z}|^2 = z/|z|^2$.

□

Proposición 7.3. *Sean z y w números complejos cualesquiera. Se tiene que:*

(a) $|z| = 0$ *si y sólo si* $z = 0$.

(b) $|zw| = |z||w|$.

(c) $|z + w| \leq |z| + |w|$.

Demostración. Sólo el tercer item no es inmediato.

(1) Si $z = a + bi$, $|z| = \sqrt{a^2 + b^2}$. Ahora $\sqrt{a^2 + b^2} = 0$ si y sólo si $a^2 + b^2 = 0$ si y sólo si $a = 0$ y $b = 0$.

(2) Basta probar que $|zw|^2 = |z|^2|w|^2$ pues los números involucrados son todos positivos. Si $z = a + bi$ y $w = c + di$, entonces

$$|zw|^2 = (ac-bd)^2+(ad+bc)^2 = (ac)^2+(bd)^2-2abcd+(ad)^2+(bc)^2+2abcd = (ac)^2+(bd)^2+(ad)^2+(bc)^2.$$

Por otro lado

$$|z|^2|w|^2 = (a^2 + b^2)(c^2 + d^2) = (ac)^2 + (ad)^2 + (bc)^2 + (bd)^2.$$

(3)

□

Ejemplos. Sean $z = 1 + i$ y $w = 2 - i$.

(1) $|z(-w)| =$

(2) $\overline{|z^2|} =$

(3) $z^1 + w^1 =$

(4) Si $zx + w = 0$, entonces $x =$

(5) $|\overline{(zw^2)^{-1}}| =$

7.4. Coordenadas polares

Hasta ahora y según hemos definido, para identificar a un número complejo debemos conocer sus partes real e imaginaria. Éstas lo determinan univocamente.

Ahora, ésta no es la única manera de identificar a un número complejo. Para entender esto recurrimos a la identificación de los complejos con el plano. El siguiente dibujo muestra de manera clara como se puede identificar a un complejo conociendo su distiancia al origen y el ángulo que forma con el eje positivo de las abscisas. Esta forma de identificación es conocida como FORMA POLAR.

——— DIBUJO ———

La distancia al origen de un complejo es su módulo y el "ángulo" referido más arriba es su *argumento*.

Veamos como hacemos esto sistemáticamente. Luego veremos como a veces es más útil la forma polar que la *forma cartesiana*; por ejemplo, el producto se entiende mejor en la forma polar.

Una primera cosa importante es observar que dado un complejo z ($z \neq 0$), el complejo $z/|z|$ tiene el mismo argumento que z y su módulo es 1. Por lo tanto los complejos de módulo 1 resultan relevantes.

Los complejos de módulo 1

Sea w un complejo con $|w| = 1$, esto es un punto del plano en la circunsferencia unidad. Del conocimiento básico de las funciones trigonométricas sabemos que estos puntos son de la forma

$$(\cos(\theta), \operatorname{sen}(\theta))$$

donde θ es el ángulo destacado en el dibujo, o el argumento de w.

————— DIBUJO —————

Luego, podemos escribir

$$w = \cos(\theta) + \operatorname{sen}(\theta)i$$

Es importante recordar que el ángulo θ no está univocamente determinado, sin embargo dos posibles ángulos difieren en 2π y hay un único si $\theta \in [0, 2\pi)$.

Hay una notación especial para los complejos de módulo 1, que resulta muy útil para hacer aritmética con el producto y que ayuda a interpretar el producto en el plano.

Notación. Dado $\theta \in \mathbb{R}$, definimos

$$e^{i\theta} = \cos(\theta) + \operatorname{sen}(\theta)i.$$

Ahora, volvamos al principio y tomemos un z cualquiera $z \neq 0$ y consideremos

$$w = \frac{z}{|z|}$$

de módulo 1. Luego tenemos queda

$$w = e^{i\theta}$$

para algún θ. Si tomamos $\rho = |z|$, de la definición de w se sigue que

$$z = \rho e^{i\theta} \tag{7.3}$$

Ésta es la *forma polar* de z, en la que se ven explíciatmente su módulo y su argumento (en vez de sus partes real e imaginaria).

El producto y la forma polar

La forma polar es particularmente adecuada para entender el producto de números complejos. Como antes, resulta importante considerar primero a los complejos de módulo 1. Tomemos $e^{i\theta}$ y $e^{i\phi}$ y calculemos el producto de ellos:

$$\begin{aligned} e^{i\theta}e^{i\phi} &= (\cos(\theta) + \operatorname{sen}(\theta)i)(\cos(\phi) + \operatorname{sen}(\phi)i) \\ &= \Big((\cos(\theta)\cos(\phi) - \operatorname{sen}(\theta)\operatorname{sen}(\phi)\Big) + \Big(\cos(\theta)\operatorname{sen}(\phi) + \operatorname{sen}(\theta)\cos(\phi)\Big)i \end{aligned}$$

En este punto es crucial reconocer las fórmulas del "coseno de la suma" y del "seno de la suma". [*] Estas fórmulas dicen que la parte real del producto que hemos calculado es

$$\Big((\cos(\theta)\cos(\phi) - \operatorname{sen}(\theta)\operatorname{sen}(\phi)\Big) = \cos(\theta + \phi)$$

y la parte imaginaria es

$$\Big(\cos(\theta)\operatorname{sen}(\phi) + \operatorname{sen}(\theta)\cos(\phi)\Big) = \operatorname{sen}(\theta + \phi)$$

Es decir, el producto es $\cos(\theta + \phi) + \operatorname{sen}(\theta + \phi)i$. Concluimos entonces que

$$e^{i\theta}e^{i\phi} = e^{i(\theta+\phi)} \tag{7.4}$$

———————— DIBUJO ————————-

Ahora que ya entendemos cómo se múltiplican los complejos de módulo 1 es fácil entender cómo se multiplican dos complejos cualesquiera. Dados z y w complejos cualesquiera, distintos de 0, considermos sus formas polares

$$z = |z|e^{i\theta} \qquad \text{y} \qquad w = |w|e^{i\phi}$$

y multiplicamos:

$$\begin{aligned} zw &= |z|e^{i\theta}|w|e^{i\phi} && (7.5) \\ &= |zw|e^{i(\theta+\phi)} && (7.6) \end{aligned}$$

—- recuadrar —- destacar —-

Esta fórmula dice que para multiplicar dos complejos en forma polar hay que multiplicar sus módulos y sumar sus argumentos.

[*] xxx

7.5. Raíces de la unidad y fórmula de De Moivre

Raíces n-ésimas

Fórmula de De Moivre

7.6. Conjuntos y transformaciones del plano

El dibujo muestra en azul a los complejos de módulo 1; éstos son todos los puntos de la circunsferecnia de radio 1 y centro en el origen del plano. Ese conjunto es

$$S = \{z \in \mathbb{C} : \ |z| = 1\}$$

Los puntos en el interior del círculo son los del conjunto

$$E = \{z \in \mathbb{C} : \ |z| < 1\}$$

y los del exterior

$$F = \{z \in \mathbb{C} : \ |z| > 1\}$$

Claramente todo el plano es la unión disjunta

$$\mathbb{C} = E \cup S \cup F$$

—— DIBUJO ——

El círculo $D = \{z : \ |z| \leq 1\} = S \cup E$ es el *círculo o disco unidad*.

En este momento la descripción y comprensión de ciertos conjuntos del plano y algunas transformaciones geométricas es muy instrutiva para aprender la aritmética de los complejos, ya que requiere cierta habilidad en la manipulación de los complejos.

A continuación trabajamos con varios tipos distintos de conjuntos, como círculos, rectas y semiplanos y varias transformaciones geométricas como traslaciones, rotaciones y reflexiones.

Círculos

A partir del círculo unidad D, es posible obtener cualquier otro por medio de dos operaciones geométricas: las expansiones y contracciones, y las traslaciones.

———- DIBUJO ————-

El círculo del medio es D expandido por un factor $3/2$. Y el tercer círculo es este último trasladado por el punto $(2, 1)$.

Mientras que el círculo unidad está descripto como

$$D = \{z : \ |z| \leq 1\}$$

el círculo $B(r)$ con centro en el origen y radio r se puede describir como

$$B(r) = \{z : \ |z| \leq r\}$$

Ahora si $B_p(r)$ es el círculo con centro p y radio r, $B_p(r)$ es el trasldado por p de $B(r)$. Es decir

$$\begin{aligned} B_p(r) &= \{z : z = w + p \text{ con } w \in B(r)\} \\ &= \{z : z - p \in B(r)\} \\ &= \{z : |z - p| \leq r\} \end{aligned}$$

La circunsferencia de cenro p y radio r es el *borde* deeste círculo y está descrita como

$$\partial B_p(r) = \{z : |z - p| = r\}$$

El interior y el exterior de $B_p(r)$ son respectivamente

$$B_p^<(r) = \{z : |z - p| < r\} \qquad \text{y} \qquad B_p^>(r) = \{z : |z - p| > r\}$$

Ejemplos. En el dibujo hay tres circunsferencias. Más abajo están descriptas como vimos.

——- DIBUJO ———-

(1) La primera tiene centro en el origen y radio $2/5$. Luego es $C_1 = \{z : |z| = 2/5\}$.

(2) La segunda tiene centro en $(2, 1)$ y radio 1. Luego es $C_2 = \{z : |z - (2 + i)| = 1\}$.

(3) La tercera tiene centro en $(-2, 2)$ y radio $3/2$. Luego es $C_3 = \{z : |z-(-2+2i)| = 3/2\}$.

Ejemplos. En estos dibujos se ven dos conjuntos asociados a círculos. Más abajo están descriptos.

————— DIBUJO ———

(1) En el dibujo de la derecha se ve destacada la circunsferencia de centro $(1, 1)$ y radio 2 junto con su exterior. Este conjunto es

$$A = \{z : |z - (1 + i)| \geq 2\}$$

(2) En el dibujo de la izquierda se ve destacado el interior de la circunsferenca de centro $(2, -1)$ y radio $3/4$. Este conjunto es

$$B = \{z : |z - (2 - i)| < 3/4\}$$

Rectas y semiplanos

Las rectas verticales y las rectas horizontales son muy fáciles de describir. Para identificar a una recta vertical basta decir en qué punto corta al eje real, es decir cuál es la parte real de sus puntos. Análogamente una recta horizontal queda determinada por la parte imaginaria de todos sus puntos.

——— DIBUJO ———

El dibujo muestra a las rectas

$$R_1 = \{z \in \mathbb{C} : \operatorname{Re}(z) = 3/4\}, \qquad R_2 = \{z \in \mathbb{C} : \operatorname{Re}(z) = -\sqrt{2}\}$$

$$S_1 = \{z \in \mathbb{C} : \operatorname{Im}(z) = 2\}, \qquad S_2 = \{z \in \mathbb{C} : \operatorname{Im}(z) = -1\}$$

Las rectas que pasan por el origen pueden describirse como el conjunto de todos los múltiplos reales de uno cualquiera de sus puntos (no nulos). Si R es la recta que queremos describir, tomamos uno de sus puntos, digamos $v \neq 0$ y así

$$R = \{z : \ z = tv, \text{ con } t \in \mathbb{R}\}$$

Ésta es una descripción paramétrica de R y el parámetro t recorre a R. Los t positivos recorren la semirecta de R que contiene a v y los negativo la semirecta opuesta.

—— DIBUJO ——

Otra manera de describir a estas rectas es pensarlas como rotadas de la recta real (la recta horizontal por el origen). La recta real se puede describir por la ecuación

$$\operatorname{Im}(z) = 0$$

Si R es la recta a describir y la multiplicamos adecuadamente podemos llevarla a coincidir con la recta real, que ya sabemos describir. Si $v \in R$, entonces los puntos de R tienen todos el mismo argumento que v, digamos θ, y como el argumento de $\overline{v}$ es $-\theta$, resulta que

$$\overline{v}R = \{\overline{v}z : \ z \in R\}$$

es la recta real. Así, si $v \in R$, la ecuación

$$\operatorname{Im}(\overline{v}z) = 0$$

describe a la recta R. Esto es, el conjunto de todos los z que la satisfacen es exactamente R.

$$R = \{z : \operatorname{Im}(\overline{v}z) = 0\}$$

Cada una de estas rectas determina dos semiplanos. En el caso de la recta real, el semiplano superior es

$$\text{semiplano superior} = \{z : \operatorname{Im}(z) > 0\}$$

y el semiplano inferior es

$$\text{semiplano inferior} = \{z : \operatorname{Im}(z) < 0\}$$

Análogamente los semiplanos determinados por R son

$$\{z : \operatorname{Im}(\overline{v}z) > 0\} \qquad \text{y} \qquad \{z : \operatorname{Im}(\overline{v}z) < 0\}$$

Para poder identificar cuál es cuál hay que pensar en la rotación determinada por la multiplicación por v, que lleva la recta R a la recta real y los semiplanos determinados por R

a los semiplanos determinados por la recta real. Otra manera de hacerlo es tomar un punto z_0 en uno de los semiplanos y evaluar $\mathrm{Im}(\overline{v}z_0)$. El resultado será positivo o negativo, nunca 0, y ese signo identifica a todo el semiplano en el que está z_0.

———— DIBUJO ————

Nos quedan por describir todas las rectas que no son verticales, horizontales o pasan por el origen. Pero esto no es difícil, ya que dada una recta cualquiera siempre podemos trasladarla para hacerla pasar por el origen, es decir podemos llevarla a una que ya sabemos describir.

———- DIBUJO ————

Si S no pasa por el origen y $w \in S$, entonces

$$R = S - v = \{z - v : \ z \in S\}$$

es una recta que si pasa por el origen y $S = R + v$. Ahora si z es otro punto (distinto) de S, $w - v \in R$ y $w - v \neq 0$; luego S queda descripta por la ecuación

$$\mathrm{Im}((\overline{w - v})(z - v)) = 0$$

Los semiplanos que determina esta recta están dados por

$$\{z : \mathrm{Im}((\overline{w - v})(z - v)) > 0\} \qquad \text{y} \qquad \{z : \mathrm{Im}((\overline{w - v})(z - v)) < 0\}$$

y para identificarlos basta elegir un punto z_0 en el semiplano de interés y evaluar $\mathrm{Im}((\overline{w - v})(z_0 - v))$.

———— DIBUJO ————

Ejemplos. En cada caso determinamos la ecuación que describe a la recta R presentada y al semiplano elegido.

(1) R_1 es la recta por el origen que forma un ángulo de 45 grados con el eje de los reales positivos. El semiplano elegido es el que contiene a los reales negativos.

—— DIBUJO ——

(2) R_2 es la recta que pasa por lo puntos $(3, 1)$ y $(0, 2)$ y el semiplano elegido es el de la derecha.

—— DIBUJO ——-

Sectores angulares

Un sector angular como el del dibujo más abajo puede describirse de dos maneras naturales.

- Usando la función argumento.
- Intersecando dos semiplanos.

—— DIBUJO ——

En este caso por un lado

$$S = \{z : \ 0 \leq \mathrm{Arg}(z) \leq \pi/4\}$$

y por otro también

$$S = \{z : \ \mathrm{Im}(z) \geq 0 \text{ y } \mathrm{Im}((1-i)z) \leq 0\}$$

Si el sector angular a describir tiene su vértice en v_0 y no en el origen, para describirlo usando la función argumento, hay pensar en el trasladado, por $-v_0$, que si tiene su vértice en el orgigen. El sector angular general

—— DIBUJO ——-

queda descripto por

$$\{z : \ \alpha \leq \mathrm{Arg}(z - v_0) \leq \alpha + \theta\}$$

Ejemplo. Describimos el sector angular

—— DIBUJO ——

usando la función argumento y como intersección de dos semiplanos.

-
-

Conjuntos construidos a partir de los anteriores

Problemas.

(1) Caracterizar el conjunto del dibujo (los bordes no perteneces a él).
—— DIBUJO (sandwich de huevo) ———-

(2) Considerar las rectas por el origen que pasan una por el punto $(2, 1)$ y la otra por el punto $(-2, 1)$. Colorear "el moño" y caracterizarlo como conjunto del plano.

(3) Considerar dos círculos A y B, el primero de centro $(2, 2)$ y radio 1 y el otro de centro $(1, 2)$ y radio $3/2$. Colorear "la medialuna". Escribir usando la operaciones de conjuntos a la medialuna (con sus bordes) en términos de los conjuntos A y B. Caracterizar la medialuna usando la aritmética de los complejos.

Soluciones. (1)

(2)

(3)

7.7. Polinomios y el Teorema Fundamental del Algebra †

7.8. Ejercicios y problemas

Ejercicios

Ejercicio 7.1.

Problemas

Problema 7.2.

Parte III

Aritmética modular

Capítulo 8

Congruencias de enteros

🕔 + 🕘 = 🕐

Imaginemos las siguiente situación:

> Son las 17hs y acabo de tomar el remedio, la próxima dosis me toca en 8 horas, a la 1 de la mañana. No me tengo que olvidar. Sí, está bien ¡17+8=1!

o esta otra

> Son las 15hs y salimos de viaje rumbo a la Patagonia. Tenemos 27 horas de viaje por delante. ¿Llegaremos a tomar la leche? A ver... $15 + 27 = 15 + 3$, sí, llegaremos cerca de las 6 de la tarde.

Está claro que ni $17 + 8 = 1$ ni $15 + 27 = 18$ es la suma de enteros. Sin embargo es la suma del reloj, la suma en la aritmética del reloj de 24 horas (o de 12 horas si usamos la notacion am y pm). En esta nueva aritmética, el resultado da siempre algo entre 0 y 23, pues los múltiplos de 24 son despreciables.

Siguiendo con la analogía, en este capítulo aprenderemos la aritmética del reloj, pero para relojes arbitrarios de m horas, donde m es cualquier entero (esto nos servirá sin duda para cualquier planeta que visitemos).

8.1. La congruencia de enteros

Comenzamos con la definición de congruencia entre enteros.

Definición. Dados a, b, m enteros con $m > 0$, decimos que a *es congruente a* b *módulo* m si m divide a la diferencia de a y b. En este caso, escribimos $a \equiv b \pmod{m}$. En símbolos,

$$a \equiv b \pmod{m} \qquad \Leftrightarrow \qquad m \mid a - b$$

El entero m se llama el *módulo* de la congruencia. Si a no es congruente a b módulo m, es decir, si $m \nmid a - b$, entonces decimos que a y b son *incongruentes* módulo m y escribimos $a \not\equiv b \pmod{m}$ en este caso.

Luego, por definición,

$$a \equiv b \pmod{m} \qquad \Leftrightarrow \qquad b = km + a \quad \text{para algún } k \in \mathbb{Z}$$

Notación. Para abreviar, a veces escribiremos $a \equiv b \ (m)$ o incluso $a \equiv_m b$. Cuando el módulo m esté implícito, o ya haya sido explicitado y no haya lugar a dudas, escribiremos simplemente $a \equiv b$. En este capítulo y los siguientes m denotará un módulo y asumiremos pues que $m > 0$.

Por ejemplo, es claro que $7 \equiv 1 \pmod 2$, $5 \equiv 17 \pmod{12}$ y $150 \equiv 30 \pmod{60}$. Menos obvio resulta que $9876 \equiv 237 \pmod{17}$ y $9876 \equiv 237 \pmod{567}$. En efecto, $9876 - 237 = 9639 = 17 \cdot 567$.

De la definición, tenemos que $a \equiv 0 \pmod m$ si y sólo si $m \mid a$. Luego,

$$a \equiv b \pmod m \quad \Leftrightarrow \quad a - b \equiv 0 \pmod m$$

Veamos que la congruencia es naturalmente una relación de equivalencia en los enteros.

Proposición 8.1. *Dado $m \in \mathbb{N}$, la relación de congruencia módulo m define una relación de equivalencia en $\mathbb{Z}$. Es decir, valen*

(a) $a \equiv a \pmod m$.

(b) $a \equiv b \pmod m$ *si y sólo si* $b \equiv a \pmod m$.

(c) $a \equiv b \pmod m$ *y* $b \equiv c \pmod m$ *implican* $a \equiv c \pmod m$.

Demostración. Sigue directamente de las siguientes propiedades de divisibilidad.
(a) $m \mid 0$.
(b) Si $m \mid a - b$ entonces $m \mid b - a$.
(c) Si $m \mid a - b$ y $m \mid b - c$ entonces $m \mid (a - b) + (b - c) = a - c$. □

Nota histórica. Carl F. Gauss (1777-1855), conocido como el *Príncipe de las Matemáticas*, introdujo la noción de congruencia módulo un entero en su obra cumbre *Disquisitiones Arithmeticae* de 1801, cuando contaba con tan sólo 24 años. Debido a la Proposición anterior, utilizó el símbolo $\equiv$ por su parecido con el símbolo $=$ de igualdad.

8.1.1. Clases de congruencia

Como la congruencia módulo un entero m es una relación de equivalencia, se sigue entonces que el conjunto de números enteros queda partido como unión (disjunta) de las clases de equivalencia (ver Proposición 3.1). Estas clases se llaman *clases de congruencia módulo* m. La clase de congruencia módulo m de un entero a es

$$[a]_m = \{b \in \mathbb{Z} \,:\, b \equiv a \pmod m\} \tag{8.1}$$

Cuando m esté sobreentendido, la denotaremos simplemente por $[a]$.

De las definiciones, es claro que

- $a \equiv b \pmod{m} \quad \Leftrightarrow \quad [a]_m = [b]_m$
- $x \equiv y \pmod{m} \quad \Leftrightarrow \quad x, y \in [a]_m$

para todo $a, x, y, m \in \mathbb{Z}$.

Ejemplo. Los enteros 17, 112 y -18 son todos congruentes a 2 módulo 5 y por lo tanto pertencen a la misma clase de equivalencia módulo 5. Luego, tenemos $17, 112, -18 \in [2]_5$ y $[17]_5 = [112]_5 = [-18]_5 = [2]_5$.

Veamos que sólo hay m clases distintas de congruencia módulo m. En efecto,

$$[a + m]_m = [a]_m$$

para todo $a \in \mathbb{Z}$. Además, como $0, 1, \ldots, m-1$ (resp. $1, 2, \ldots, m$) son enteros incongruentes entre sí módulo m, las clases $[0]_m, [1]_m, \ldots, [m-1]_m$ (resp. $[1]_m, [2]_m, \ldots, [m]_m$) son todas disjuntas. Por lo tanto tenemos

$$\mathbb{Z} = [0]_m \cup [1]_m \cup \cdots \cup [m-1]_m = [1]_m \cup [2]_m \cup \cdots \cup [m]_m \tag{8.2}$$

Notar que

$$[0]_m = \{a \in \mathbb{Z} : a \equiv 0 \pmod{m}\} = \{a \in \mathbb{Z} : m \mid a\} = \mu_m$$

es decir, la clase del 0 módulo m está formada por todos los múltiplos de m. ¿Qué representan las otras clases de congruencia? ¿Cómo podemos describirlas?

Ejemplos. Tenemos $\mathbb{Z} = [0]_2 \cup [1]_2$ y $\mathbb{Z} = [0]_3 \cup [1]_3 \cup [2]_3$.

(1) Como la clase del 0 módulo 2 corresponde a los pares (múltiplos de 2), entonces $[1]_2$ debe ser la clase de los impares.

(2) La clase $[0]_3$ son los múltiplos de 3, a $[1]_3$ lo forman los números que difieren en 1 de un múltiplo de 3 y $[2]_3$ son los enteros que difieren en 2 de un múltiplo de 3. ◊

Observación. Si $m = 1$, todos los enteros son congruentes entre sí módulo m. Es decir, hay una sola clase módulo $m = 1$, la clase de los múltiplos de 1, o sea todos los enteros. En símbolos $\mathbb{Z} = [0]_1$.

En el siguiente Capítulo haremos aritmética con estas clases de congruencia. Es decir, operaremos con las clases ¡cómo si fueran números! Veremos que estos nuevos 'números' tienen propiedades muy interesantes. Cuando nos acustumbremos a ellos seremos capaces de darnos cuenta de su poder de síntesis para realizar cálculos.

8.1.2. Restos de la división entera

Ahora veremos cómo interpretar a los números congruentes entre sí módulo un entero m a través de la división entera, algo que tal vez ya debería ser intuitivamente claro.

Comencemos con un ejemplo sencillo. Supongamos que el módulo es $m = 7$. Luego, $10 = 7 + 3$ y 3 están relacionados. También lo están $17 = 2 \cdot 7 + 3$, $24 = 3 \cdot 7 + 3$ y $-25 = (-4) \cdot 7 + 3$. Todos estos números estan relacionados entre sí, y vemos que todos tienen resto 3 al dividir por 7. En efecto, todos los números de la forma $a = k \cdot 7 + 3$ con $k \in \mathbb{Z}$ son congruentes a 3 módulo 7. Este es un hecho general. Veamos primero un resultado auxiliar.

Lema 8.2. *Si $a \equiv b \pmod m$ y $0 \leq |b-a| < m$ entonces $a = b$.*

Demostración. Tenemos que $b - a = km$ para algún entero k. Como $0 \leq |b-a| < m$, la única posibilidad es que $k = 0$, o sea $|b-a| = 0$. Luego, $a = b$. □

Proposición 8.3. *Dos enteros son congruentes módulo m si y sólo si tienen el mismo resto en la división por m. En símbolos, dados $a, b \in \mathbb{Z}$ vale*

$$a \equiv b \pmod m \qquad \Leftrightarrow \qquad a = q_1 m + r \quad y \quad b = q_2 m + r$$

donde $q_1, q_2, r \in \mathbb{Z}$ con $0 \leq r < m$.

Demostración. Dividiendo a y b por m tenemos que $a = q_1 m + r_1$ y $b = q_2 m + r_2$ con $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ y $0 \leq r_1, r_2 < m$.

Si $a \equiv b \pmod m$ entonces $m \mid a - b$. Por otra parte, $a - b = (q_1 - q_2)m + (r_1 - r_2)$. Como m divide a $a - b$ entonces m divide a $r_1 - r_2$. Luego, $r_1 - r_2 \equiv 0 \pmod m$. Como $0 \leq |r_1 - r_2| < m$, por el Lema 8.2 tenemos que $r_1 = r_2$.

Recíprocamente, si a y b son dos enteros con el mismo resto en la división por m, entonces $r_1 = r_2$ y $a - b = m(q_1 - q_2)$ de donde m divide a $a - b$, es decir $a \equiv b \pmod m$. □

Notación. Cuando m está sobreentendido, el resto r de la división de a por m se suele denotar por $\bar{a}$, y se llama la reducción de a módulo m. En símbolos, si

$$a = qm + r \quad \text{con} \quad 0 \leq r < m$$

entonces

$$\bar{a} = a \mod m = r \tag{8.3}$$

Esto permite caracterizar las clases de congruencia en (8.2). Ahora es claro que

$$[r]_m = \{a \in \mathbb{Z} : a = qm + r \text{ para algún } q \in \mathbb{Z}\} = m\mathbb{Z} + r$$

para cada $0 \leq r < m$. Por ejemplo, si $m = 7$ entonces

$$\begin{aligned}
[0]_7 &= \{a \in \mathbb{Z} : a = 7m + 0 \text{ con } q \in \mathbb{Z}\} = \{\ldots, -7, 0, 7, 14, \ldots\} \\
[1]_7 &= \{a \in \mathbb{Z} : a = 7m + 1 \text{ con } q \in \mathbb{Z}\} = \{\ldots, -6, 1, 8, 15, \ldots\} \\
[2]_7 &= \{a \in \mathbb{Z} : a = 7m + 2 \text{ con } q \in \mathbb{Z}\} = \{\ldots, -5, 2, 9, 16, \ldots\} \\
[3]_7 &= \{a \in \mathbb{Z} : a = 7m + 3 \text{ con } q \in \mathbb{Z}\} = \{\ldots, -4, 3, 10, 17, \ldots\} \\
[4]_7 &= \{a \in \mathbb{Z} : a = 7m + 4 \text{ con } q \in \mathbb{Z}\} = \{\ldots, -3, 4, 11, 18, \ldots\} \\
[5]_7 &= \{a \in \mathbb{Z} : a = 7m + 5 \text{ con } q \in \mathbb{Z}\} = \{\ldots, -2, 5, 12, 19, \ldots\} \\
[6]_7 &= \{a \in \mathbb{Z} : a = 7m + 6 \text{ con } q \in \mathbb{Z}\} = \{\ldots, -1, 6, 13, 20, \ldots\}
\end{aligned}$$

Observación. Dado $m \in \mathbb{N}$, todas las clases de equivalencia de congruencia módulo m tienen un único representante mayor o igual que 0 y menor estricto que m. Es decir, para todo $a \in \mathbb{Z}$, exsite un único r con $0 \leq r < m$ tal que $a \equiv r \pmod m$. Este r es el resto de la división de a por m.

8.2. Propiedades básicas

Veremos ahora una serie de propiedades elementales de las congruencias, que nos serán de suma utilidad en lo que sigue.

8.2.1. Linealidad

Comenzamos viendo que la relación de congruencia se porta bien con las sumas y productos bajo un mismo módulo. Es claro que si

$$a \equiv b \pmod{m} \qquad \text{y} \qquad c \in \mathbb{Z}$$

entonces

$$a + c \equiv b + c \pmod{m} \qquad \text{y} \qquad ac \equiv bc \pmod{m}$$

Esto sale directamente de la definición de congruencia y las propiedades de divisibilidad. Lo interesante es que estas propiedades se preservan si en lugar de usar el mismo c usamos dos enteros c, c' congruentes entre sí.

Proposición 8.4. *Sean $a, b, c, c', m \in \mathbb{Z}$ con $m > 0$. Si $a \equiv b \pmod{m}$ y $c \equiv c' \pmod{m}$, entonces*

$$a + c \equiv b + c' \pmod{m} \qquad y \qquad ac \equiv bc' \pmod{m}$$

Demostración. Como $a \equiv b \pmod{m}$ y $c \equiv c' \pmod{m}$, entonces $m \mid a - b$ y $m \mid c - c'$. Luego $m \mid (a - b) + (c - c') = (a + c) - (b + c')$, de donde se sigue que $a + c \equiv b + c' \pmod{m}$.

Notar que $ac - bc' = c(a - b) - b(c' - c)$. Luego, como $m \mid a - b$ y $m \mid c - c'$ tenemos que $m \mid ac - bc'$, de donde sale que $ac \equiv bc' \pmod{m}$. □

Dado $m \in \mathbb{N}$, ya hemos observado que ser congruente a 0 módulo m, es ser un múltiplo de m. Luego, si a y b son múltiplos de m, $a \equiv 0\,(m)$ y $b \equiv 0\,(m)$, entonces la Proposición 8.4 dice que $a+b \equiv 0\,(m)$, es decir, que $a+b$ es múltiplo de m. Por supuesto, esto ya lo sabemos desde que estudiamos múltiplos y divisores de números enteros.

Ejemplo. Sea $m = 5$. Si $a = 23$ y $b = 62$, su suma es $a + b = 85$ y su producto es $ab = 1446$. Como $a \equiv 3 \pmod{5}$ y $b \equiv 2 \pmod{5}$, entonces debe ser $a + b \equiv 3 + 2 \equiv 0 \pmod{5}$ y $ab \equiv 2 \cdot 3 \equiv 1 \pmod{5}$. En efecto, $85 \equiv 0 \pmod{5}$ y $1446 \equiv 1 \pmod{5}$.

Las propiedades de la proposición anterior pueden ser iteradas y combinadas entre sí. Sea

$$f(x) = c_n x^n + c_{n-1} x^{n-1} + \cdots + c_2 x^2 + c_1 x + c_0 \tag{8.4}$$

donde $c_0, c_1, \ldots, c_n \in \mathbb{Z}$ con $c_n \neq 0$ y x es un símbolo. Tal $f(x)$ se dice un polinomio con coeficientes enteros o *polinomio entero*[*]. y se lo denota $f(x) \in \mathbb{Z}[x]$. Si $a \in \mathbb{Z}$, tenemos la expresión polinómica en a

$$f(a) = c_n a^n + c_{n-1} a^{n-1} + \cdots + c_2 a^2 + c_1 a + c_0 \in \mathbb{Z}$$

que es también un entero. Decimos que $f(a)$ es el polinomio $f(x)$ evaluado en a.

[*] algo de esto ya vimos en el capítulo de números complejos y lo estudiaremos en algún detalle en el Capítulo **??**

Corolario 8.5. *Si* $a \equiv b \pmod m$ *y* $\alpha \equiv \beta \pmod m$ *entonces:*

(a) $ax + by \equiv \alpha x + \beta y \pmod m$ *para todo* $x, y \in \mathbb{Z}$.

(b) $a^n \equiv b^n \pmod m$ *para todo* $n \in \mathbb{N}$.

(c) $f(a) \equiv f(b) \pmod m$ *para todo* $f(x) \in \mathbb{Z}[x]$ *como en* (8.4).

Demostración. El resultado sale de forma inmediata usando la Proposición 8.4 repetidas veces. Haremos el item (b) y dejamos los demás como ejercicio para el lector. Hacemos inducción en n. Tenemos $a \equiv a \pmod m$ y supongamos que $a^j \equiv b^j \pmod m$. Tomando $c = a$ y $c' = b$ en la proposición, tenemos $a^{j+1} \equiv b^{j+1} \pmod m$, y luego $a^n \equiv b^n \pmod m$ para todo natural n. □

Ejemplo. Recordemos los números de Fermat, que son los de la forma $F_n = 2^{2^n} + 1$ con $n \in \mathbb{N}_0$. Ya en el primer capítulo, mencionamos que $F_0, \ldots, F_4$ son primos y que Euler probó que $F_5 = 2^{32} + 1$ es compuesto mostrando que $641 \mid F_5$. Una forma fácil de probar esto es usando congruencias. Estudiaremos las potencias de 2 módulo 641. Tenemos

$$2^2 = 4, \quad 2^4 = 16, \quad 2^8 = 256, \qquad 2^{16} = 65536 \equiv 154 \pmod{641}$$

Luego,

$$2^{32} \equiv (154)^2 = 23716 \equiv 640 \equiv -1 \pmod{641}$$

Por lo tanto, $F_5 = 2^{32} + 1 \equiv 0 \pmod{641}$, es decir F_5 es compuesto. ◊

8.2.2. Reducción del módulo

En general, los factores comunes no nulos de ambos miembros de un congruencia no se pueden simplificar. Por ejemplo, consideremos $48 \equiv 18 \pmod{10}$. Ambos miembros son divisibles por 6, pero no es cierto que $8 \equiv 3 \pmod{10}$. Sin embargo, dividiendo por 2 obtenemos $24 \equiv 9 \pmod 5$, que si es correcto. Esto último, si es un hecho general. Es decir, un factor común se puede simplificar a ambos miembros de la congruencia si el módulo es divisible por el mismo factor, pagando el precio de dividir el módulo por este factor también. Esto simplifica mucho la congruencia.

Proposición 8.6. *Si* $c > 0$ *entonces*

$$a \equiv b \pmod m \qquad \textit{si y sólo si} \qquad ac \equiv bc \pmod{mc}$$

Demostración. Sale directo por la propiedad $m \mid a - b$ si y sólo si $cm \mid c(a - b)$. Necesitamos que $c \neq 0$ para poder simplificar y que $c > 0$ para que $mc > 0$, o sea, un módulo válido. □

Cuando el módulo no es divisible por el factor común, aún es posible simplificar la congruencia de alguna manera. La siguiente proposición da cuenta de ello.

Proposición 8.7 (Ley de simplificación)**.** *Si* $ac \equiv bc \pmod m$ *y* $d = (m, c)$ *entonces*

$$a \equiv b \pmod{\tfrac{m}{d}}$$

En particular, si $c = p$ *es primo y* $p \nmid m$*, entonces* $a \equiv b \pmod m$.

En otras palabras, un factor común se puede simplificar si el módulo es divible por el máximo común divisor entre ambos. En particular, un factor común primo, coprimo con el módulo, siempre puede ser simplificado.

Demostración. Por hipótesis, $m \mid c(a-b)$ de donde $\frac{m}{d} \mid \frac{c}{d}(a-b)$. Como $(\frac{m}{d}, \frac{c}{d}) = 1$ tenemos que $\frac{m}{d}$ debe dividir a $a-b$ y por lo tanto $a \equiv b \pmod{\frac{m}{d}}$ como queríamos ver. □

8.2.3. Otras propiedades

Divisibilidad

Veamos que dada una congruencia, si un entero divide a un miembro y divide al módulo entonces divide al otro miembro.

Proposición 8.8. *Supongamos que* $a \equiv b \pmod{m}$. *Si* $d \mid a$ *y* $d \mid m$ *entonces* $d \mid b$.

Demostración. Basta suponer que $d > 0$. Por transitividad, como $d \mid m$ y $m \mid a-b$ entonces $d \mid a-b$, o sea $a \equiv b \pmod{d}$. Como $a \mid d$ entonces $a \equiv 0 \pmod{d}$ de donde $b \equiv 0 \pmod{d}$.

Otra forma. Tenemos $b = km + a$ para algún entero k. Como $d \mid m$ y $d \mid a$ entonces $d \mid b$. □

Ahora veamos que números congruentes tienen el mismo máximo común divisor con el módulo.

Proposición 8.9. *Si* $a \equiv b \pmod{m}$ *entonces* $(a, m) = (b, m)$.

Demostración. Sea $d = (a, m)$ y $e = (b, m)$. Como $d \mid a$ y $d \mid m$, por la proposición anterior, $d \mid b$ y por lo tanto $d \mid e$. Análogamente, $e \mid b$, $e \mid m$, luego $e \mid a$ y por lo tanto $e \mid d$. Así, $d = e$ como queríamos ver. □

Producto de módulos

Proposición 8.10. *Supongamos que* $a \equiv b \pmod{m}$ *y* $a \equiv b \pmod{n}$. *Si* $(m, n) = 1$ *entonces* $a \equiv b \pmod{mn}$.

Demostración. Tenemos $m \mid a-b$ y $n \mid a-b$ y como $(m, n) = 1$ entonces $mn \mid a-b$. □

Luego, para módulos primos esto siempre vale.

Corolario 8.11. *Si* $a \equiv b \pmod{p}$ *y* $a \equiv b \pmod{q}$ *con* p, q *primos entonces* $a \equiv b \pmod{pq}$.

Ejemplo. Como $34-4 = 30$, tenemos que $34 \equiv 4$ módulo $2, 3, 5, 6, 10, 15$ y 30. Sin embargo, $34 \equiv 4 \pmod{3}$ y $34 \equiv 4 \pmod{6}$ no implican que $34 \equiv 4 \pmod{18}$. El problema está en que 3 y 6 no son coprimos.

8.3. Aplicaciones de congruencias

8.3.1. Aplicaciones a la aritmética entera: cálculos con potencias

Veremos aquí como usar congruencias en algunos problemas aritméticos. Las congruencias son un método muy potente de cálculo, ya que suelen reducir cómputos largos y difíciles a algunas pocas cuentas. Aquí conviene pensar que tenemos un número N muy grande, por lo general dado en término de potencias de números o sumas de potencias. Imaginemos entonces que tenemos un número

$$N = c^e \tag{8.5}$$

donde c y e son enteros conocidos. Por ejemplo, $N = 13^{195}$ ó $N = 72^{1249^{356}}$. Más generalmente, podemos considerar números de la forma

$$N = c_1^{e_1} + \cdots + c_k^{e_k}$$

Veremos a continuación cómo:

(a) calcular restos de la división de N por un entero;

(b) calcular las últimas cifras de N (unidades, decenas, etc);

(c) determinar si N es divisible o no por un entero dado.

Las reglas de divisibilidad son otra aplicación importante, que veremos en la siguiente sección. Otra aplicación de las congruencias realmente útil en la práctica, es en criptografía. Este es el arte de encriptar datos de forma segura (mantenerlos ocultos, seguros de la mirada de extraños). El algoritmo del famoso método RSA se basa en el uso apropiado de congruencias.

Potencias

La clave para todas estas aplicaciones mencionadas arriba es saber calcular congruencias de potencias. Muchas veces, las potencias de un número dado, digamos a^k, $k \in \mathbb{N}$, al mirarlas módulo un entero m toman expresiones sencillas y pueden por lo general ser mas o menos bien descriptas. Esto ayuda en las cuentas que queramos hacer.

Veamos con un ejemplo la forma de proceder en general. El truco es encontrar una potencia k de a tal que a^k sea pequeño o fácil de operar (en lo posible, $a^k \equiv 0, \pm 1, \pm 2$ módulo m).

Ejemplo. Estudiemos las potencias de 2 módulo los primeros enteros. Veamos $2^k \pmod m$ para $3 \leq m \leq 10$, y calculemos cuánto es $N = 2^{2015}$ módulo m.

- $m = 3$. Tenemos

$$\begin{aligned} 2^0 &= 1 \equiv 1 \pmod 3 \\ 2^1 &= 2 \equiv 2 \pmod 3 \\ 2^2 &= 4 \equiv 1 \pmod 3 \\ 2^3 &= 8 \equiv 2 \pmod 3 \end{aligned}$$

Es claro que en general tenemos

$$\begin{aligned} 2^{2k} &\equiv 1 \pmod 3 \\ 2^{2k+1} &\equiv 2 \pmod 3 \end{aligned} \tag{8.6}$$

para todo $k \in \mathbb{N}$. Luego $N \equiv 2 \pmod 3$.

- $m = 4, 8$. Tenemos $2^0 = 1 \pmod 4$, $2^1 = 2 \pmod 4$, $2^2 = 4 \equiv 0 \pmod 4$. Luego

$$2^k \equiv 0 \pmod 4 \qquad k \geq 2$$

Similarmente,

$$2^k \equiv 0 \pmod 8 \qquad k \geq 3$$

Luego $N \equiv 0 \pmod 4$ y $N \equiv 0 \pmod 8$.

- $m = 5$. Tenemos

$$\begin{aligned} 2^0 = 1 &\equiv 1 \pmod 5 & 2^2 = 4 &\equiv 4 \pmod 5 \\ 2^1 = 2 &\equiv 2 \pmod 5 & 2^3 = 8 &\equiv 3 \pmod 5 \end{aligned}$$

Luego, $2^4 = 2 \cdot 3 \equiv 1 \pmod 5$ y por lo tanto es claro que a partir de aquí se repiten las congruencias y tenemos

$$\begin{aligned} 2^{4k} &\equiv 1 \pmod 5 \\ 2^{4k+1} &\equiv 2 \pmod 5 \\ 2^{4k+2} &\equiv 4 \pmod 5 \\ 2^{4k+3} &\equiv 3 \pmod 5 \end{aligned} \tag{8.7}$$

para todo $k \in \mathbb{N}$. Luego $N = 2^{4 \cdot 503 + 3} \equiv 3 \pmod 5$.

- $m = 6$. Tenemos $2^0 = 1 \equiv 1 \pmod 6$ y

$$\begin{aligned} 2^1 = 2 &\equiv 2 \pmod 6 & 2^3 = 8 &\equiv 2 \pmod 6 \\ 2^2 = 4 &\equiv 4 \pmod 6 & 2^4 = 16 &\equiv 4 \pmod 6 \end{aligned}$$

Luego, es claro que

$$\begin{aligned} 2^{2k} &\equiv 4 \pmod 6 \\ 2^{2k+1} &\equiv 2 \pmod 6 \end{aligned}$$

para todo $k \in \mathbb{N}$. Luego $N \equiv 2 \pmod 6$. Notar que esto también sale a partir del caso $m = 3$. En efecto, usando la Proposición 8.6 con $c = 2$ en (8.6) se obtienen las congruencias de arriba.

- $m = 7$. Aquí, como $2^3 \equiv 1 \pmod 7$, hay 3 clases de congruencias, dadas por

$$\begin{aligned} 2^{3k} &\equiv 1 \pmod 7 \\ 2^{3k+1} &\equiv 2 \pmod 7 \\ 2^{3k+2} &\equiv 4 \pmod 7 \end{aligned}$$

para todo $k \in \mathbb{N}$. Notar que también sale de (8.6), usando la Proposición 8.6 con $c = 2$. Luego $N = 2^{3 \cdot 671 + 2} \equiv 4 \pmod 7$.

- $m = 9$. Como $2^3 = 8 \equiv -1 \pmod 9$, tenemos que $2^6 \equiv 1 \pmod 9$ y que $2^4 \equiv -2 \pmod 9$ y $2^5 \equiv -4 \pmod 9$. Luego,

$$\begin{aligned} 2^1 &= 2 \equiv 2 \pmod 9 & 2^4 &= 16 \equiv -2 \equiv 7 \pmod 9 \\ 2^2 &= 4 \equiv 4 \pmod 9 & 2^5 &= 32 \equiv -4 \equiv 5 \pmod 9 \\ 2^3 &= 8 \equiv -1 \pmod 9 & 2^6 &= 64 \equiv -8 \equiv 1 \pmod 9 \end{aligned}$$

  Luego, es claro que

$$\begin{aligned} 2^{6k} &\equiv 1 \pmod 6 & 2^{6k+3} &\equiv 8 \pmod 6 \\ 2^{6k+1} &\equiv 2 \pmod 6 & 2^{6k+4} &\equiv 7 \pmod 6 \\ 2^{6k+2} &\equiv 4 \pmod 6 & 2^{6k+5} &\equiv 5 \pmod 6 \end{aligned}$$

  para todo $k \in \mathbb{N}$. Luego $N = 2^{6\cdot 335+5} \equiv 5 \pmod 9$.

- $m = 10$. Sale como en los casos anteriores, notando que como $2^5 \equiv 2 \pmod{10}$, comienza a repetirse. Podemos nuevamente usar el caso $m = 5$. A partir de (8.7), y usando la Proposición 8.6 con $c = 2$, tenemos

$$\begin{aligned} 2^{4k} &\equiv 2 \pmod{10} \\ 2^{4k+1} &\equiv 4 \pmod{10} \\ 2^{4k+2} &\equiv 8 \pmod{10} \\ 2^{4k+3} &\equiv 6 \pmod{10} \end{aligned}$$

  Luego $N = 2^{4\cdot 503+3} \equiv 6 \pmod{10}$. ◊

Particularmente importante será el estudio de las potencias de 10 módulo un entero m. Esto lo haremos cuando veamos las reglas de divisibilidad.

Observación. Sea $\bar{c} = c \mod m$ la reducción de c módulo m, es decir, el menor entero positivo r tal que $c \equiv r \pmod m$. Notar que como

$$\overline{c^e} \equiv \bar{c}^e \pmod m$$

siempre podemos reducir la base N módulo m de modo de reducir el problema al caso en que $N < m$.

Por ejemplo, para calcular $123^{17} \pmod{10}$ basta notar que $123 = 120 + 3 \equiv 3 \pmod{10}$. Luego,

$$123^{17} \equiv 3^{17} \pmod{10}$$

que es mucho mas sencillo de calcular.

Veamos ahora un resultado bastante curioso que permite reducir ciertas sumas de potencias módulo 6, cuando los exponentes son números de Fermat $F_k = 2^{2^k} + 1$, $k \in \mathbb{N}_0$.

Proposición 8.12. *Si $e_1, \ldots, e_r$ son números de Fermat entonces*

$$n_1^{e_1} + \cdots + n_r^{e_r} \equiv n_1 + \cdots + n_r \pmod 6$$

Demostración. La prueba se basa en la identidad $x^3 - x = x(x^2-1) = x(x-1)(x+1)$ y en el hecho de que si $x \in \mathbb{Z}$ entonces $6 \mid x(x-1)(x+1)$ por ser 3 enteros consecutivos.

Sea

$$n := n_1 + \cdots + n_r$$

Supongamos primero que los e_i son todos iguales a 3 (i.e., $e_i = F_0$). Tenemos que

$$\begin{aligned} n_1^3 + \cdots + n_r^3 &= (n_1^3 - n_1) + \cdots + (n_r^3 - n_r) + n \\ &= n_1(n_1-1)(n_1+1) + \cdots + n_r(n_r-1)(n_r+1) + n \end{aligned}$$

Como 6 divide a cada término $n_i(n_i-1)(n_i+1)$, tenemos que $n_1^3 + \cdots + n_r^3 \equiv n \pmod 6$.

En general, usamos que

$$x^{F_k} - x = x(x^{2^{2^k}} - 1) = x(x^{2^{2^k-1}} - 1)(x^{2^{2^k-1}} + 1)$$

Si seguimos factorizando los factores de la forma $x^{2^j} - 1$ llegamos a la expresión

$$x^{F_k} - x = x(x-1)(x+1)(x^2+1)(x^4+1)\cdots(x^{2^{2^k-1}} + 1)$$

que es divisible por 6. O sea

$$x^{F_k} \equiv x \pmod 6$$

Luego, es claro que

$$n_1^{e_1} + \cdots + n_1^{e_r} \equiv n \pmod 6$$

para todo $k_1, \ldots, k_r \in \mathbb{N}_0$, donde $e_1, \ldots, e_r$ son números de Fermat. □

Ejemplo. Típicamente, usamos esto para expresiones con potencias que involucran los exponentes 3, 5, 17 y 255. Por ejemplo:

(1) $12^{17} + 7^5 + 11^{255} + 123^3 \equiv 12 + 7 + 11 + 123 = 153 \equiv 3 \pmod 6$.

(2) $1^3 + 2^3 + 3^3 + 4^3 + 5^3 \equiv 1 + 2 + 3 + 4 + 5 \equiv 3 \pmod 6$. Más generalmente,

$$\sum_{i=0}^{n} i^{F_{j_i}} \equiv 1 + 2 + 3 + \cdots + n = \tfrac{n(n+1)}{2}$$

Luego, $6 \mid 1^{F_{j_0}} + 2^{F_{j_1}} + 3^{F_{j_2}} + \cdots + n^{F_{j_n}}$ si n es de la forma $n = 24k$ ó $n = 24k - 1$.

(3) $1^5 + 2^5 + 4^5 + 8^5 + 16^5 \equiv 1 + 2 + 4 + 8 + 16 = 31 \equiv 1 \pmod 6$. Más generalmente, tenemos

$$\begin{aligned} \sum_{i=0}^{r} (2^i)^{F_{j_i}} &= 1^{F_{j_0}} + 2^{F_{j_1}} + (2^2)^{F_{j_2}} + (2^3)^{F_{j_3}} + \cdots + (2^r)^{F_{j_r}} \\ &\equiv 1 + 2 + 2^2 + 2^3 + \cdots + 2^r = 2^{r+1} - 1 \equiv \begin{cases} 1 \pmod 6 & \text{si } r \text{ es par,} \\ 3 \pmod 6 & \text{si } r \text{ es impar.} \end{cases} \end{aligned}$$

Muchos otros ejemplos interesantes de este tipo pueden ser provistos por el lector. ◊

Restos de la división entera

Ya sabemos que encontrar el resto r de la división entera de N por m, es equivalente a encontrar un r tal que $N \equiv r \pmod{m}$ con $0 \leq r < m$.

Casos particulares importantes son cuando $m = 10$ y $r = 0$. Si $m = 10$, el resto de la división por m no es otra cosa que el dígito de la unidad de N. Por otro lado, si $r = 0$ entonces N es divisible por m.

Ejemplo. Calculemos el resto de dividir $N = 10^{135}$ por 7.

- Directamente: como $10^2 \equiv 3^2 \equiv 2 \pmod{7}$, tenemos que $10^3 = 10 \cdot 10^2 \equiv 3 \cdot 2 = 6 \equiv -1 \pmod{7}$ de donde $10^6 = (10^3)^2 \equiv (-1)^2 = 1 \pmod{7}$. Como $135 = 6 \cdot 22 + 3$ tenemos
$$10^{135} = 10^{6 \cdot 22 + 3} = (10^6)^{22} \cdot 10^3 \equiv 1 \cdot 6 \equiv 6 \pmod{7}$$
- Reduciendo la base: tenemos $10^{135} \equiv 3^{135} \pmod{7}$. Notar que $3^2 \equiv 2 \pmod{7}$, luego $3^3 \equiv 6 \equiv -1 \pmod{7}$ y por lo tanto $3^6 \equiv 1 \pmod{7}$. Luego,
$$3^{135} = 3^{6 \cdot 22 + 6} = (3^6)^{22} \cdot 3^3 \equiv 1 \cdot 6 \equiv 6 \pmod{7}$$
y así $10^{135} \equiv 6 \pmod{7}$. ◊

Las cuentas no siempre son tan fáciles o directas como lo muestra el siguiente ejemplo.

Ejemplo. ¿Cuál es el resto de dividir $N = 3^{64}$ por 31? Para empezar, notar que tenemos $3^3 = 27 \equiv -4 \pmod{31}$. Como queremos usar esto, escribimos $64 = 3 \cdot 21 + 1$ y tenemos

$$3^{64} = (3^3)^{21} \cdot 3 \equiv (-4)^{21} \cdot 3 \equiv -2^{42} \cdot 3 \pmod{31}$$

Ahora, el problema se reduce a estudiar las potencias de 2 módulo 31. Como $2^5 = 32 \equiv 1 \pmod{31}$, usando $42 = 5 \cdot 8 + 2$ llegamos a que

$$3^{64} \equiv -2^{5 \cdot 8 + 2} \cdot 3 = -(2^5)^8 \cdot 2^2 \cdot 3 \equiv -12 \equiv 19 \pmod{31}$$

Luego, el resto de dividir 3^{64} por 31 es 19. ◊

En general se trata de saber qué trucos usar y cuando, y sin duda esto lo da la práctica.

Las cifras de un número grande

Sea $N = c^e$ como en (8.5) ¿En qué dígitos termina N? Por ejemplo, ¿cuáles son las últimas 3 cifras de N? Nos estamos preguntando por las unidades, decenas y centenas de N dado como en (8.5). Es decir, si

$$N = a_r \cdots a_2 a_1 a_0$$

debemos determinar a_0, a_1 y a_2. Por notación decimal, sabemos que esto significa

$$N = a_r 10^r + a_{r-1} 10^{r-1} + \cdots + a_2 10^2 + a_1 10 + a_0 \tag{8.8}$$

donde $0 \leq a_0, a_1, \ldots, a_r \leq 9$.

Para determinar a_0 basta calcular $N \pmod{10}$, pues tomando congruencia módulo 10 en la expresión (8.8) tenemos $N \equiv a_0 \pmod{10}$, por Corolario 8.5. Para determinar a_1, basta calcular $N \pmod{100}$, pues tomando congruencia módulo 100 en (8.8), tenemos $N \equiv a_1 10 + a_0 \pmod{100}$. Para determinar a_2 tomamos congruencia módulo 1000. Está claro cuál es la forma de proceder en general. El único inconveniente es que las cuentas se van complicando paulatinamente al aumentar el k del a_k que queremos determinar.

Más generalmente, para $N = c_1^{e_1} + \cdots + c_k^{e_k}$ tomamos congruencia módulo 10^k si lo que queremos es determinar los últimos $(k+1)$-dígitos de N, es decir la cadena $a_k \cdots a_1 a_0$ si $N = a_r \cdots a_{k+1} a_k \cdots a_1 a_0$, y utilizamos el Corolario 8.5.

Ejemplo. Calculemos los 3 últimos dígitos de $N = 5897^{12}$. En primer lugar, sabemos que $5897^{12} \equiv 7^{12} \pmod{10}$. Luego, las unidades, decenas y centenas de N son las mismas que las correspondientes de 7^{12}.

Tenemos que $7^2 = 49 \equiv 9 \equiv -1 \pmod{10}$, luego $7^4 \equiv 9^2 = 81 \equiv 1 \pmod{10}$. De este modo tenemos que

$$7^{12} = 7^4 \cdot 7^4 \cdot 7^4 = (7^4)^3 \equiv 1^3 = 1 \pmod{10}$$

Por ende, el dígito de unidades de 7^{12} es 1.

Ahora, $7^4 = 49^2 = 2401 \equiv 1 \pmod{100}$. Luego,

$$7^{12} = (7^4)^3 \equiv 1 \pmod{100}$$

De este modo, la cifra de las decenas de 7^{12} es 0 y N termina en 01.

Finalmente, tenemos que $7^4 = 2401 \equiv 401 \pmod{1000}$. Luego,

$$7^{12} = (7^4)^2 \cdot 7^4 \equiv 401^2 \cdot 401 = 160801 \cdot 401 \equiv 801 \cdot 401 = 321201 \equiv 201 \pmod{1000}$$

De esta manera 7^{12}, y por lo tanto N, termina en 201. ◊

Divisibilidad

Decir que un número N es divisible por d es lo mismo que ver que N es congruente a 0 módulo d. En símbolos,

$$d \mid N \qquad \Leftrightarrow \qquad N \equiv 0 \pmod{d}$$

Sin embargo, si N es como en (8.5), es mucho más fácil calcular la congruencia, sin necesidad de calcular toda la potencia.

Ejemplo. ¿Es $N = 5^{2013} + 7^{2013}$ divisible por 6? Responderemos la pregunta sin calcular las potencias explícitamente. Tomemos $m = 6$ y veamos si N es congruente a 0 o no módulo 6. Por un lado sabemos que $7 \equiv 1 \pmod{6}$ y luego por la Proposición 8.4,

$$7^k \equiv 1 \pmod{6}$$

para cualquier $k \in \mathbb{N}$. Por otro lado $5 \equiv -1 \pmod{6}$ y así $5^2 \equiv 1 \pmod{6}$ (esto también sigue directamente ya que $5^2 = 25$), luego la Proposición 8.4 implica que $(5^2)^k \equiv 1 \pmod{6}$, o sea

$$5^{2k} \equiv 1 \pmod{6}$$

para cualquier $k \in \mathbb{N}$. De todo esto se sigue que

$$5^{2013} + 7^{2013} = (5^{2012} \cdot 5) + 1 \equiv 1 \cdot 5 + 1 \equiv 0 \pmod 6$$

Concluimos que $6 \mid 5^{2013} + 7^{2013}$. ◊

Ejemplo. Veamos que $5n^3 + 7n^5$ es múltiplo de 12 para todo n. Ya sabemos que este tipo de problema puede resolverse por inducción. Sin embargo, las congruencias también son muy útiles en este caso. Notar que, como $(12k + i)^3 \equiv i^3 \pmod{12}$, basta analizar las potencias n^3 módulo 12 para $1 \leq n \leq 11$, y lo mismo para n^5.

En general obtendríamos 2 listas con las congruencias de $n^3 \pmod{12}$ y de $n^5 \pmod{12}$. Sin embargo, en este caso sucede algo curioso. Como $12 - k \equiv k \pmod{12}$ tenemos que

$$\begin{aligned} 1^2 \equiv 11^2 \equiv 1 \pmod{12} \\ 2^2 \equiv 10^2 \equiv 4 \pmod{12} \\ 3^2 \equiv 9^2 \equiv 9 \pmod{12} \\ 4^2 \equiv 8^2 \equiv 4 \pmod{12} \\ 5^2 \equiv 7^2 \equiv 1 \pmod{12} \end{aligned}$$

y $6^2 \equiv 0 \pmod{12}$.

De aquí se deduce que

$$n^5 \equiv n^3 \pmod{12} \tag{8.9}$$

(el lector debería chequear esto). Sólo a modo de curiosidad damos el las congruencias

$$\begin{aligned} 1^5 \equiv 1^3 \equiv 1 \pmod{12} \\ 2^5 \equiv 2^3 \equiv 8 \pmod{12} \\ 3^5 \equiv 3^3 \equiv 3 \pmod{12} \\ 4^5 \equiv 4^3 \equiv 4 \pmod{12} \\ 5^5 \equiv 5^3 \equiv 5 \pmod{12} \end{aligned}$$

Es claro que (8.9) inmediatamente implica que

$$12 \mid 5n^3 + 7n^5$$

pues $5n^3 + 7n^5 \equiv (5 + 7)n^3 \equiv 0 \pmod{12}$. ◊

8.3.2. Aplicaciones a la vida cotidiana †

Digresión. Es claro que en nuestra vida cotidiana usamos congruencias inconscientemente. Sin embargo, la costumbre hace que hagamos las cuentas de forma correcta y que su aritmética no nos parezca rara. Veamos algunos ejemplos de situaciones y los módulos correspondientes que usamos:

- Relojes: usamos módulo 12 ó 24 para las horas, módulo 60 para los minutos y segundos. Si estamos cronometrando algo, también usamos módulo 10 para las décimas de segundo, módulo 100 para las centésimas, etcétera.
- Fechas: usamos módulo 7 para los días de la semana y módulo 12 para los meses del año. Por ejemplo, si es martes y debemos pagar una boleta que se vence dentro de 10 días, sabemos que hay que contar 3 días a partir del martes, o sea miercoles, jueves y viernes. Luego, de aca a 2 viernes a mas tardar deberíamos pagar nuestra boleta para que no se venza. Si estamos en abril (mes 4) y sabemos que en 18 meses nos entregan la casa, esta será en el mes 4+6=10, o sea en octubre del próximo año. Usamos módulo 4 para calcular años bisiestos. Otro ejemplo de este tipo es el horóscopo chino que cambia de signo cada 12 años.
- Compras de almacén: usamos congruencias cuando pedimos por docenas (huevos, facturas), o por cuartos o medios quilos (pan, criollos, quesos, etc).
- Ángulos: cuando trabajamos con los ángulos de la geometría plana y los medimos en grados, estamos usando congruencias módulo 360 para los grados y módulo 60 para los minutos y segundos. Son muy usados en la práctica en navegación y en astronomía. También en las latitudes y longitudes de una localización geográfica usa ángulos.

Claramente, aplicamos congruencias en situaciones donde hay una cierta *periodicidad*, y esta puede ser medida de forma *discreta* (es decir, no continua).

Fórmula para el día de la semana a partir de la fecha

Existe una curiosa fórmula (aunque no es curioso que la fórmula exista) para saber, dada una fecha, de qué día de la semana se trata. Toda fecha, como 1 de enero de 2001, define 4 enteros n, m, a, b como sigue. Sea n el número que corresponde al día del mes ($n = 1$ en nuestro ejemplo). Sea m el número del mes contando desde marzo. O sea, $m = 1$ para marzo, $m = 2$ para abril, ..., $m = 10$ para diciembre, $m = 11$ para enero y $m = 12$ para febrero. Esto peculiar elección se debe a que en los años bisiestos un día extra es añadido a febrero (además es coherente con el lenguaje, ya que setiembre, octubre, noviembre y diciembre, claramente aluden a séptimo, octavo, noveno y décimo). Representemos a los años por ac donde c son las centenas (últimas dos cifras) y a el resto ($a = 20$ y $c = 01$ en nuestro ejemplo). Por último, sea d el día de la semana, con $d = 0$ para domingo, $d = 1$ para lunes, y así hasta $d = 6$ para el sábado.

Proposición 8.13 (Día de la semana a partir de la fecha)**.** *En las notaciones previas, para cualquier fecha $n/m/ac$, a partir del 15 de octubre de 1582 dC, el día de la semana que le corresponde es*

$$d = n + [2{,}6m - 0{,}2] + c + [c/4] + [a/4] - 2a - (1 + b)[m/11] \pmod 7$$

donde $[\,\cdot\,]$ denota la función parte entera y ponemos $b = 1$ si el año es bisiesto y $b = 0$ si no.

La fórmula vale a partir del 15 de octubre de 1582, que es cuando se adoptó el calendario gregoriano actualmente en uso. Recordar que los años bisiestos son aquellos que son

divisibles por 4, salvo los que son divisibles por 100, que entonces son bisiestos si además son divisibles por 400. Por ejemplo, 1984 y 2000 son bisiestos, pero 1900 y 2100 no lo son.

Ejemplo. Calculemos que día cayó el 'barrilete cósmico', es decir el día de los goles de Diego Maradona a los ingleses. Todos sabemos (o deberíamos) que ese día fue el 22 de junio de 1986. Luego, tenemos $n = 22$, $m = 4$, $a = 19$ y $c = 86$. Además $b = 0$. Por la fórmula tenemos

$$\begin{aligned} d &= 22 + [2, 6 \cdot 4 - 0, 2] + 86 + [86/4] + [19/4] - 2 \cdot 19 - (1 + 0)[4/11] \\ &= 22 + 10 + 86 + 21 + 4 - 38 = 105 = 7 \cdot 15 \equiv 0 \pmod 7 \end{aligned}$$

Luego $d = 0$, es decir fue un domingo! ◊

Demostración. La prueba es una curiosa aplicación del principio de inducción hacia atrás. Veremos que la fórmula es correcta viendo que: **(i)** si es correcta para una fecha, entonces también es correcta para la fecha del día siguiente y para la del día previo, y **(ii)** que en efecto es correcta para una fecha cualquiera del calendario, a partir de 1582. (Si usamos el 15 de octubre de 1582 como punto de partida entonces sale con la inducción normal.)

Para ver el punto (i), veremos que si la fórmula vale para una fecha dada entonces también vale para el día siguiente. Haremos un estudio caso por caso. En todos los casos debemos ver que al cambiar los valores de n, m, a, c y b de la fecha por n', m', a', c' y b' de la fecha del día siguiente, cambia el valor de $d \pmod 7$ por el de $d + 1 \pmod 7$.

Recordemos que los meses de 31 días son enero, marzo, mayo, julio, agosto, octubre y diciembre (que corresponden a 11, 1, 3, 5, 6 y 8), los de 30 días son abril, junio, setiembre y noviembre (2, 4, 7 y 9), y febrero tiene 28*.

(a) cambio de día, pero no de mes ni de año (por ejemplo, 9 de julio de 1816). En este caso es claro que sólo cambia n por $n + 1$ y por lo tanto d por $d + 1$ módulo 7.

(b) cambio de mes, de 31 días, sin cambio de año (por ejemplo 31 de enero de 2000). Tenemos $n = 31$, $n' = 1$, $m \in \{1, 3, 5, 6, 8, 10\}$, $m' = m + 1$, $a = a'$ y $c' = c$.

(c) cambio de mes, de 30 días, sin cambio de año (por ejemplo 30 de abril de 2000). Tenemos $n = 30$, $n' = 1$, $m \in \{2, 4, 7, 9\}$, $m' = m + 1$, $a = a'$ y $c' = c$.

(d) cambio de mes, de 29 días (29 de febrero de cualquier año bisiesto). Tenemos $n = 29$ con $b = 1$, $n' = 1$ $m = 12$, $m' = 1$, $a = a'$ y $c' = c + 1$.

(e) cambio de mes, de 28 días (28 de febrero de un año no bisiesto). Tenemos $n = 28$ con $b = 0$, $n' = 1$ $m = 12$, $m' = 1$, $a = a'$ y $c' = c + 1$.

(f) cambio de año sin cambio de siglo (por ejemplo, 31 de diciembre de 2013) Tenemos $n = 31$, $n' = 1$ $m = 10$, $m' = 11$, $a = a'$ y $c' = c + 1$.

(g) cambio de año con cambio de siglo (por ejemplo, 31 de diciembre de 1999) Tenemos $n = 31$, $n' = 1$ $m = 10$, $m' = 11$, $a' = a + 1$ y $c = 99$ y $c' = 0$.

*recordar el versito de la primaria *treinta días trae noviembre / con abril, julio y septiembre / de veintiocho sólo hay uno / y los demás, de treinta y uno.*

Para ver que la fórmula es válida para el día precedente se procede de manera similar, y lo dejamos como ejercicio para el lector.

El punto (ii) ya lo verificamos en el ejemplo anterior, luego la fórmula es válida para toda fecha posterior al 15 de octubre de 1582. □

8.4. Reglas de divisibilidad

8.4.1. Reglas de divisibilidad y la notación decimal

Las reglas de divisibilidad dicen cuándo un número dado es divisible por otro en términos de su representación decimal. Dado $a \in \mathbb{N}$ consideramos su representación decimal, $a = (a_r a_{r-1} \dots a_1 a_0)_{10}$, y dado un $m \in \mathbb{N}$ queremos condiciones sobre los dígitos de a, $a_0, a_1, \dots, a_r$ que indiquen si a es divisible por m o no. Las condiciones buscadas las deduciremos de la identidad $a \equiv 0 \pmod{m}$ que dice exactamente que $m \mid a$.

En general, la expresión $a = (a_r \dots a_1 a_0)_{10}$ es una abreviatura de

$$a = a_r 10^r + \cdots + a_1 10 + a_0 \tag{8.10}$$

Si queremos estudiar cuando $m \mid a$, tomando congruencia módulo m arriba tenemos

$$a \equiv a_r 10^r + \cdots + a_1 10 + a_0 \pmod{m} \tag{8.11}$$

y a partir de aquí deducimos condiciones para los $a_0, \dots, a_n$, de modo tal de asegurar que $a \equiv 0 \pmod{m}$. Para esto será de vital importancia estudiar las potencias de diez

$$10, 10^2, \dots, 10^r \pmod{m}$$

involucradas.

Por ejemplo, para decidir cuándo a es divisible por 10, tomamos $m = 10$ y tenemos que $a \equiv a_r 10^r + \cdots + a_1 10 + a_0 \equiv a_0 \pmod{10}$. Dado que $0 \leq a_0 < 9$, entonces

$$a_0 \equiv 0 \pmod{10} \qquad \Leftrightarrow \qquad a_0 = 0$$

Por lo tanto, a es divisible por 10 si y sólo si $a_0 = 0$, es decir a "termina en 0".

Observación. Notar que por la Proposición 8.10 solo bastará dar reglas de divisibilidad para *potencias de primos*, pues si a es divisible por p^r y es divisible por q^s entonces es divisible por $p^r q^s$, donde p, q son primos distintos. En general, se tiene que *si*

$$m = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$$

es la factorización prima de m, entonces un entero cualquiera a es divisible por m si a es divisible por todos y cada uno de los $p_i^{r_i}$, $1 \leq i \leq k$.

Por ejemplo, un entero n es:

- divisible por 6, si es divisible por 2 y por 3;
- divisible por 12, si es divisible por 3 y por 4 (pero no por 2 y por 6);

- divisible por 14, si es divisible por 2 y por 7;
- divisible por 15, si es divisible por 3 y por 5;
- divisible por 18, si es divisible por 2 y por 9 (pero no por 3 y por 6);
- divisible por 20, si es divisible por 4 y por 5 (pero no por 2 y por 10);

Del mismo modo, m es divisible por 21, si es divisible por 3 y por 7; es divisible por 22, si es divisible por 2 y por 11; es divisible por 24, si es divisible por 3 y por 8 (pero no por 4 y por 6); es divisible por 28, si es divisible por 4 y por 7 (pero no por 2 y por 14); es divisible por 30, si es divisible por 2, por 3 y por 5.

8.4.2. Reglas de divisibilidad

Reglas básicas de divisibilidad

Proposición 8.14 (divisibilidad por 2, 5 y 10)**.** *Sea $a \in \mathbb{Z}$.*

(a) a es divisible por 2 si su dígito de unidades es par (i.e., $0, 2, 4, 6$ u 8).

(b) a es divisible por 5 si su dígito de unidades es 0 ó 5.

(c) a es divisible por 10 si su dígito de unidades es 0.

Demostración. En todos los casos partimos de las expresiones (8.10) y (8.11).
(a) Divisibilidad por 2. Aquí $m = 2$ y como $10 \equiv 0 \pmod 2$ tenemos $a \equiv a_0 \pmod 2$. Ahora, $a_0 \equiv 0 \pmod 2$ si y sólo si es par, es decir si y sólo si $a_0 = 0, 2, 4, 6, 8$.
(b) Divisibilidad por 5. Como $10 \equiv 0 \pmod 5$ tenemos $a \equiv a_0 \pmod 5$ y $a_0 \equiv 0 \pmod 5$ si y sólo si $a_0 = 0, 5$.
(c) Divisibilidad por 10. Ya vimos esto directamente. Usando lo anterior, para que n sea divisible por 10 debe ser divisible por 2 (dígito de unidades par) y por 5 (dígito de unidades 0 ó 5), luego, el dígito de unidades debe ser 0. □

Proposición 8.15 (divisibilidad por 3, 9 y 11)**.** *Sea $a \in \mathbb{Z}$ con $a = (a_r \cdots a_1 a_0)_{10}$.*

(a) a es divisible por 3 si la suma de sus dígitos $a_0 + \cdots + a_r$ es divisible por 3.

(b) a es divisible por 9 si la suma de sus dígitos $a_0 + \cdots + a_r$ es divisible por 9.

(c) a es divisible por 11 si la suma alternada de sus dígitos, comenzando desde las unidades, $a_0 - a_1 + a_2 - \cdots + (-1)^r a_r$ es divisible por 11.

Demostración. Como antes, partimos de las expresiones (8.10) y (8.11).
(a) Divisibilidad por 3. Como $10 \equiv 1 \pmod 3$ tenemos que $10^k \equiv 1 \pmod 3$ para todo k. Luego

$$a \equiv a_r + \cdots + a_2 + a_1 + a_0 \pmod 3$$

Así, a es divisible por 3 si y sólo si la suma de sus dígitos es divisible por 3.

(b) Divisibilidad por 9. La prueba es idéntica a la anterior, cambiando 3 por 9.

(c) Divisibilidad por 11. Notar que $10 \equiv -1 \pmod{11}$. Luego $10^2 \equiv 1 \pmod{10}$. Es claro que las potencias de 10 son congruentes a 1 ó -1 según la paridad de la potencia. Es decir,

$$10^{2k} \equiv 1 \pmod{11}, \qquad 10^{2k+1} \equiv -1 \pmod{11}$$

para todo $k \in \mathbb{N}$. Luego,

$$a \equiv a_0 - a_1 + a_2 - a_3 + \cdots + (-1)^r a_r \pmod{11}$$

de donde a e divisible por 11 si y sólo si la suma alternada de sus dígitos (empezando desde las unidades con signo positivo) es divisible por 11. □

Ejemplo. ¿Es 3.737.868 divisible por 3? ¿y por 9? La suma de sus dígitos es 42, cuyos dígitos suman 6. Como 6 es divisible por 3, 42 también los es y así 3.737.868 resulta divisible por 3. Como 6 no es divisible por 9, tampoco lo es 42 y por lo tanto, 3.737.868 no es divisible por 9. Notar que hemos tenido que usar la regla 2 veces. ◊

Ejemplo. El número 121 es divisible por 11, ya que $1 - 2 + 1 = 0$ es divisible por 11. El número 12321 no es divisible por 11 pues $1 - 2 + 3 - 4 + 5 = 3$ no es divisible por 11. Análogamente, el número 1234321 es divisible por 11, pero 123454321 no lo es. ◊

Ejemplo. Los siguiente son ejemplos de números divisibles por 11:

(1) 11, 1111, y en general $1111\cdots1111$ con una cantidad par de unos.

(2) Los números capicúas $a_0a_1\cdots a_ka_k\cdots a_1a_0$ con un número par de dígitos como por ejemplo 135278872531.

(3) Los números de la forma $a_ra_r\cdots a_2a_2a_1a_1a_0a_0$ como por ejemplo 337722110099. ◊

Proposición 8.16 (divisibilidad por 4 y 8)**.** *Sea $a \in \mathbb{Z}$.*

(a) a es divisible por 4 si el número formado por sus 2 últimos dígitos es divisible por 4. Un criterio para esto es que 2 veces las decenas mas las unidades sea divisible por 4. En particular, a es divisible por 4 si termina en a_1a_0 con: (i) a_1 par y $a_0 \in \{0, 4, 8\}$ o (ii) a_1 impar y $a_1 \in \{2, 6\}$.

(b) a es divisible por 8 si el número formado por sus 3 últimas cifras es divisible por 8. Un criterio para esto es que 4 veces las centenas mas 2 veces las decenas mas las unidades sea divisible por 8. En particular, a es divisible por 8 si termina en $a_2a_1a_0$ con: (i) a_2 par y a_1a_0 es divisible por 8 ó (ii) a_2 impar y a_1a_0 divisible por 4.

Demostración. Partimos de (8.10) y (8.11).

(a) Divisibilidad por 4. Tenemos $10 \equiv 2 \pmod{4}$ y $10^2 \equiv 0 \pmod{4}$, luego $10^k \equiv 0 \pmod{4}$ para todo $k \geq 2$. Esto dice que a es divisible por 4 si el número formado por sus 2 últimos dígitos es divisible por 4. Más aún, tenemos

$$a \equiv 2a_1 + a_0 \pmod{4}$$

De aquí se deduce que si a_1 es par, $4 \mid 2a_1$ y por lo tanto $a \equiv 0 \pmod 4$ si y sólo si $4 \mid a_0$. Por otro lado, si a_1 es impar, entonces $2a_1 \equiv 2 \pmod 4$ y así $a \equiv 0 \pmod 4$ si $a_0 \equiv 2 \pmod 4$, o sea $a_0 = 2$ o $a_0 = 6$.

(b) Divisibilidad por 8. Tenemos $10 \equiv 2 \pmod 8$, $100 \equiv 4 \pmod 8$ y $10^k \equiv 0 \pmod 8$ para todo $k \geq 3$. Luego, a es divisible por 8 si el número formado por sus 3 últimos dígitos es divisible por 8 y tenemos

$$a \equiv 4a_2 + 2a_1 + a_0 \pmod 8$$

Si a_2 es par entonces $a_2 = 2k$ y $a \equiv 2a_1 + a_0 \pmod 8$. Si a_2 es impar entonces $a_2 = 2k + 1$ y $a \equiv 4 + 2a_1 + a_0 \pmod 8$. De aquí se deduce la última afirmación del enunciado. □

Ejemplo. El número 1728 es divisible por 4, pues 28 es múltiplo de 4; y es divisible por 8, pues $4 \cdot 7 + 2 \cdot 2 + 8 = 40$ lo es. El número 1492 es divisible por 4, pues 92 lo es; pero no es divisible por 8, pues $4 \cdot 4 + 2 \cdot 9 + 2 = 36$ no lo es. ◊

Las reglas de divisibilidad por 7 y 13 son parecidas a las del 11, sólo que aquí las sumas alternadas se hacen con ciertos "pesos" (alternativamente en bloques de 3 dígitos).

Proposición 8.17 (divisibilidad por 7). *Un entero a es divisible por 7 si la suma pesada de sus dígitos con pesos sucesivos $1, 3, 2, -1, -3, -2$, comenzando desde las unidades, es divisible por 7. Más precisamente, si $a = (a_r \cdots a_1 a_0)_{10}$, entonces a es divisible por 7 si y sólo si*

$$\sum_{k=0}^{[r/6]} -2a_{6k+5} - 3a_{6k+4} - a_{6k+3} + 2a_{6k+2} + 3a_{6k+1} + a_{6k} \equiv 0 \pmod 7 \qquad (8.12)$$

Demostración. Notar que $10 \equiv 3 \pmod 7$, $10^2 \equiv 2 \pmod 7$, $10^3 \equiv 6 \pmod 7$, $10^4 \equiv 4 \pmod 7$, $10^5 \equiv 5 \pmod 7$ y $10^6 \equiv 1 \pmod 7$. Luego, para todo k se tiene $10^{6k} \equiv 1 \pmod 7$ y por lo tanto

$$\begin{aligned} 10^{6k} &\equiv 1 \pmod 7 & 10^{6k+3} &\equiv -1 \pmod 7 \\ 10^{6k+1} &\equiv 3 \pmod 7 & 10^{6k+4} &\equiv -3 \pmod 7 \\ 10^{6k+2} &\equiv 2 \pmod 7 & 10^{6k+5} &\equiv -2 \pmod 7 \end{aligned}$$

Así, por (8.10) y (8.11) tenemos

$$a \equiv a_0 + 3a_1 + 2a_2 - a_3 - 3a_4 - 2a_5 + a_6 + 3a_7 + 2a_8 - a_9 \cdots \pmod 7$$

Por lo tanto, vale (8.12) y el resultado sigue. □

Una forma equivalente, pero que puede resultar mas simple, es que un entero a es divisible por 7 si y sólo si la suma alternada de sus dígitos tomados de a bloques de 3, comenzando por las unidades, es divisible por 7 (Ejercicio). Esto reduce el problema a divisibilidad por 7 para números de 3 cifras o menos.

Ejemplo. ¿Es $a = 1612871918$ divisible por 7? Aplicando el criterio de la Proposicion 8.17 tenemos que

$$\begin{aligned} a &\equiv 1\cdot 8 + 3\cdot 1 + 2\cdot 9 - 1\cdot 1 - 3\cdot 7 - 2\cdot 8 + 1\cdot 2 + 3\cdot 1 + 2\cdot 1 - 1\cdot 6 - 2\cdot 1 \\ &= 8 + 3 + 18 - 1 - 21 - 16 + 12 + 3 + 2 - 6 - 2 = 0 \pmod 7 \end{aligned}$$

por lo que $7 \mid 1612871918$.

Usando el criterio alternativo, hacemos $918 - 871 + 612 - 1 = 658 = 7 \cdot 94$. ◊

Existen algunos otros métodos para la divisibilidad por 7. Damos aquí dos métodos algorítmicos que pueden ser muy prácticos.

- *Multiplicar por 3 el primer dígito*: se basa en que $10x + y \equiv 3x + y \pmod 7$ y el hecho de que es fácil determinar cuando un entero de 2 cifras es divisible por 7. La idea es usar esta regla con los dígitos de un número, aplicándola sucesivamente a pares consecutivos de dígitos.

  Por ejemplo, supongamos que queremos ver si 7371 es divisible o no por 7. Comenzamos con el 73 y hacemos $3 \cdot 7 + 3 = 24 \equiv 3 \pmod 7$. Luego tenemos que $7371 \equiv 371 \pmod 7$. Ahora tomamos el 37 y tenemos $3 \cdot 3 + 7 = 16 \equiv 2 \pmod 7$. Luego $7371 \equiv 371 \equiv 21 \pmod 7$, que por supuesto es divisible por 7. Luego 7371 es divisible por 7.

  ¿Porqué funciona? Por que vamos reduciendo el número original por otros cada vez menores pero que tienen todos el mismo resto al dividir por 7.

- *Restar el doble del último dígito al resto de los dígitos*: Notar que $10x + y$ es divisible por 7 si y sólo si $x - 2y$ es divisible por 7. En efecto, como $10 \cdot 5 \equiv 10 \cdot (-2) \equiv 1 \pmod 7$, si ponemos $z = 10x + y$, tenemos $-2z \equiv x - 2y \pmod 7$, y por lo tanto, z es divisible por 7 si y sólo si $x - 2y$ es divisible por 7.

  Como en el caso anterior se aplica esto repetidas veces tantas como sea necesario. Tomamos como y la unidad del número y como x el resto de los dígitos.

  Por ejemplo, para el 7371 hacemos $737 - 2 \cdot 1 = 735$. Ahora, hacemos $73 - 2 \cdot 5 = 63$. Como 63 es divisible por 7, también lo es 7371.

El caso de la divisibilidad por 13 es muy similar al caso de la divisibilidad por 7.

Proposición 8.18 (divisibilidad por 13). *Un entero a es divisible por 13 si la suma pesada de sus dígitos con pesos sucesivos $1, -3, -4, -1, 3, 4$, comenzando desde las unidades, es divisible por 13. Más precisamente, si $a = (a_r \cdots a_1 a_0)_{10}$, entonces a es divisible por 13 si y sólo si*

$$\sum_{k=0}^{[r/6]} 4a_{6k+5} + 3a_{6k+4} - a_{6k+3} - 4a_{6k+2} - 3a_{6k+1} + a_{6k} \equiv 0 \pmod{13} \tag{8.13}$$

Demostración. Notar que $10 \equiv -3 \pmod{13}$, $10^2 \equiv 9 \equiv -4 \pmod{13}$, $10^3 \equiv 12 \equiv -1 \pmod{13}$, $10^4 \equiv 3 \pmod{13}$, $10^5 \equiv 4 \pmod{13}$ y $10^6 \equiv 1 \pmod{13}$. Luego, para todo k se

tiene

$$\begin{aligned} 10^{6k} &\equiv 1 \pmod{13} & 10^{6k+3} &\equiv -1 \pmod{13} \\ 10^{6k+1} &\equiv -3 \pmod{13} & 10^{6k+4} &\equiv 3 \pmod{13} \\ 10^{6k+2} &\equiv -4 \pmod{13} & 10^{6k+5} &\equiv 4 \pmod{13} \end{aligned}$$

Así, por (8.10) y (8.11) se tiene

$$a \equiv a_0 - 3a_1 - 4a_2 - a_3 + 3a_4 + 4a_5 + 3a_6 - 3a_7 - 4a_8 - a_9 \cdots \pmod{13}$$

que es lo mismo que (8.13). □

Equivalentemente, un entero a es divisible por 13 si y sólo si la suma alternada de sus dígitos tomados de a bloques de 3, comenzando por las unidades con signo menos, es divisible por 13 (Ejercicio). Esto reduce el problema a divisibilidad por 13 para números de 3 cifras o menos. Por ejemplo, el número 348309 es divisible por 13 ya que $348 - 309 = 39$.

Ejemplo. Intentemos factorizar el número $a = 1729$.

Es inmediato que a no es divisible por 2, por 3 ni por 5. Con respecto al 7 tenemos $9 + 3 \cdot 2 + 2 \cdot 7 - 1 = 28$ y por lo tanto $7 \mid 1729$. Luego, $1729 = 7 \cdot 247$. Ahora, es claro que 247 no es divisible por los primos $2, 3, 5, 7$ y 11. Usando el criterio de divisibilidad por 13, tenemos $247 = 7 - 3 \cdot 4 - 4 \cdot 2 = 7 - 12 - 8 = -13 \equiv 0 \pmod{13}$. Luego, 1729 es divisible por 13 y tenemos que $1729 = 7 \cdot 13 \cdot 19$, con lo cual concluimos la factorización. ◊

Nota histórica. En 1917, Hardy el matemático mas famoso de la época, fué a visitar a genio indio Ramanujan al hospital. Cuenta la anécdota que Hardy le mencióno a Ramanujan que había ido a verlo en un taxi cuyo número era 1729, y que le parecía un número "medio pavo", que no tenía ninguna propiedad interesante. Acto seguido, Ramanujan le constesto: "para nada, es un número muy interesante! De hecho, es el menor número que se puede escribir como suma de 2 cubos (positivos) de dos formas distintas". En efecto

$$1729 = 1^3 + 12^3 = 9^3 + 10^3.$$

Pero esto no es todo. Luego de esto, Hardy preguntó naturalmente si conocía algún número que fuera expresable como suma de dos potencias cuartas en más de una forma. Ramanujan contestó que no tenía un ejemplo obvio a mano, pero que el primer número que cumpliera esto debía ser grande. Hardy no mencionó, aunque probablemente supiera, que Euler había encontrado (más de 100 años antes) una familia infinita de tales números, el primero de los cuales es 635.318.657. Luego de un momento de meditación, Ramanujan respondió:

$$635.318.657 = 133^4 + 134^4 = 158^4 + 59^4.$$

Cuando Hardy le contó a su colega Littlewood el episodio del hospital, este dijo "cada número positivo es uno de los amigos personales de Ramanujan".

Nota. Con las ideas que ya usamos, es posible determinar reglas de divisibilidad para números mayores. El lector está invitado a pensar (ver Ejercicios) en las reglas para las potencias primas menores que 50 no vistas aun, o sea divisibilidad por p^k con p primo con $16 < p^k < 50$.

8.4.3. Reglas de divisibilidad y representaciones s-ádicas †

Las reglas de divisibilidad que hemos visto, se basan en la notación decimal. Sin embargo, cambiando la base, pero manteniendo la misma idea, es posible hallar reglas de divisibilidad en otras bases. Las bases distintas de 10 más usadas son 2, 8 y 16, por cuestiones que tienen que ver con bits y computadoras, pero también resultan de interés 3, 12 y 60 por ejemplo. Por ser números chicos, pueden ser útiles además las bases 3, 5, 7 y 11.

A continuación daremos algunas reglas de divisibilidad en base 2, 3 y 5.

Divisibilidad en base 2

Recordemos que la notación binaria para un entero a es

$$a = 2^n a_n + 2^{n-2} a_{n-1} + \cdots + 2^2 a_2 + 2a_1 + a_0$$

para algún n, con $0 \leq a_0, \ldots, a_n \leq 1$.

Usaremos las cuentas que ya hicimos en el Ejemplo de la página 255. Solo damos la lista de reglas de divisibilidad, ya que el método es similar al usado en base 10.

Reglas básicas de divisibilidad en base 2:

• **por 2**: tenemos que $a \equiv a_0 \pmod 2$. Luego, *a es divisible por 2 si a termina en 0.*

• **por 3**: como $2^{2k} \equiv 1$ y $2^{2k+1} \equiv 2 \pmod 3$, vale $a \equiv a_0 + 2a_1 + a_2 + 2a_3 + \cdots \pmod 3$. Es decir, $a \equiv \sum_k a_{2k} + 2_{2k+1} \pmod 3$. Luego, *$a$ es divisible por 3 si la suma de los dígitos con pesos 1 y 2 comenzando desde las unidades es divisible por 3.* Por ejemplo $(1111)_2$ es divisible por 3 pues $1 + 2 + 1 + 2 = 6$.

• **por 4**: como $a \equiv 2a_1 + a_0 \pmod 4$, *$a$ es divisible por 4 si a termina en 00.*

• **por 5**: tenemos $a \equiv a_0 + 2a_1 + 4a_2 + 3a_3 + a_4 + 2a_5 + 4a_6 + 3a_7 + \cdots \pmod 5$, luego *$a$ es divisible por 5 si $\sum_k a_{4k} + 2a_{4k+1} + 4a_{4k+2} + 3a_{4k+3}$ es divisible por 5.* Por ejemplo, los números binarios formados por sucesivos bloques de la forma 0000, 0101, 1010 y 1111 son divibles por 5. Esta regla es más complicada que en base 10.

• **por 7**: Tenemos $a \equiv \sum_k a_{3k} + 2a_{3k+1} + 4a_{3k+2} \pmod 7$. Luego *$a$ es divisible por 7 si la suma de los dígitos binarios con pesos $1, 2$ y 4 comenzando desde las unidades es divisible por 7.* Por ejemplo, 1110111000 es dibisible por 7 (notar que las ternas 000 y 111 tomadas en bloques de 3 pueden ser descartados). Esta regla es más sencilla que en base 10.

• **por 8**: a es divisible por 8 si $4a_2 + 2a_1 + a_0$ es divisible por 8. La única posibilidad es que $a_0 = a_1 = a_2 = 0$, luego *a es divisible por 8 si a termina en 000.*

• **por 11**: Esta regla es mas complicada que en base 10: *a es divisible por 11 si la suma de los dígitos con pesos $1, 2, 4, 8, 5, -1, -2, -4, -8, -5$ es divisible por 11.*

En general, a es divisible por 2^k si a termina en $\underbrace{0 \ldots 0}_{k}$.

Divisibilidad en base 3

En notación ternaria un entero a se escribe

$$a = 3^n a_n + 3^{n-2} a_{n-1} + \cdots + 3^2 a_2 + 3a_1 + a_0$$

para algún n, con $0 \leq a_0, \ldots, a_n \leq 2$.

Reglas básicas de divisibilidad en base 3:

Es claro que a es divisible por 3, $9 = 3^2$, $27 = 3^3$ si a termina en 0, 00 y 000, respectivamente.

• **por 2**: como $a \equiv \sum_k a_k \pmod 2$, *$a$ es divisible por 2 si la suma de sus dígitos es divisible por 2*.

• **por 4 y por 8**: $a \equiv \sum_k a_{2k} + 3a_{2k+1} \pmod 4, \pmod 8$, luego *$a$ es divisible por 4 ó por 8 si la suma de sus dígitos con pesos $1, 3$ comenzando desde las unidades es divisible por 4 o por 8*.

• **por 5**: $a \equiv \sum_k a_{4k} + 3a_{4k+1} + 4a_{4k+2} + 2a_{4k+3} \pmod 5$, luego *$a$ es divisible por 5 si la suma de sus dígitos con pesos $1, 3, 4$ y 2 comenzando desde las unidades es divisible por 5*.

• **por 7**: $a \equiv \sum_k a_{6k} + 3a_{6k+1} + 2a_{6k+2} - a_{6k+3} - 3a_{6k+4} - 2a_{6k+5} \pmod 7$, luego *$a$ es divisible por 7 si la suma de sus dígitos con pesos $1, 3, 2, -1, -3, -2$ comenzando desde las unidades es divisible por 7*. Esta regla ¡es la misma que en base 10! (aunque es mucho más fácil sumar sólo con los dígitos 0, 1 y 2).

• **por 11**: $a \equiv \sum_k a_{5k} + 3a_{5k+1} - 2a_{5k+2} + 5a_{5k+3} - 4a_{5k+4} \pmod{11}$, luego *$a$ es divisible por 11 si la suma de sus dígitos con pesos $1, 3, -2, 5, -4$ comenzando desde las unidades es divisible por 11*.

Divisibilidad en base 5

En base 5, un entero a se escribe

$$a = 5^n a_n + 5^{n-2} a_{n-1} + \cdots + 5^2 a_2 + 5a_1 + a_0$$

para algún n, con $0 \leq a_0, \ldots, a_n \leq 4$.

Reglas de divisibilidad:

• **por 2**: como $a \equiv \sum_k a_k \pmod 2$, *$a$ es divisible por 2 si la suma de sus dígitos es divisible por 2* (igual a la del 2 en base 3).

• **por 3**: como $5^{2k} \equiv 1$ y $5^{2k+1} \equiv 2 \pmod 3$, vale $a \equiv a_0 + 2a_1 + a_2 + 2a_3 + \cdots \pmod 3$. Es decir, $a \equiv \sum_k a_{2k} + 2_{2k+1} \pmod 3$. Luego, *$a$ es divisible por 3 si la suma de los dígitos con pesos 1 y 2 comenzando desde las unidades es divisible por 3.*

• **por 4**: como $a \equiv \sum_k a_k \pmod 4$, *$a$ es divisible por 4 si la suma de sus dígitos es divisible por 4*.

• **por 5**: como $a \equiv a_0 \pmod 5$, *a es divisible por 5 si a termina en 0*.

• **por 7**: $a \equiv \sum_k a_{6k} - 2a_{6k+1} - 3a_{6k+2} - a_{6k+3} + 2a_{6k+4} + a_{6k+5} \pmod 7$, luego *$a$ es divisible por 7 si la suma de sus dígitos con pesos $1, -2, -3, -1, 2, 3$ comenzando desde las unidades es divisible por 7*. Es

• **por 8**: como $5^k \equiv 1 \pmod 8$ para todo $k \geq 2$, luego *a es divisible por 8 si $a_0 + 5a_1 + a_2 + a_3 + \cdots$ es divisible pr 8*.

• **por 11**: como $a \equiv \sum_k a_{5k} + 5a_{5k+1} + 3a_{5k+2} + 4a_{5k+3} - 2a_{5k+4} \pmod{11}$, luego *$a$ es divisible por 11 si la suma de sus dígitos con pesos $1, 5, 3, 4, -2$, comenzando desde las unidades es divisible por 11*.

Como el método es el mismo, el lector interesado podrá por su cuenta encontrar reglas de divisibilidad por n en base b, con n y b de su agrado. Esto es muy formativo y por consiguiente lo estimulamos a intentarlo. ¿Se anima a dar las reglas básicas en sistema octal y hexadecimal (bases 8 y 16 respectivamente)?

Claro está que algunas reglas son más simples en una base que en otra. Para sacarle provecho, conviene conocer las reglas básicas en algunas bases chicas y saber pasar un número de una base a otra.

8.5. Los Teoremas de Fermat, Euler y Wilson

En esta sección veremos 3 teoremas muy famosos sobre congruencias, los teoremas de Fermat, de Euler (o Euler-Fermat) y de Wilson. Necesitaremos el siguiente hecho que, aunque elemental, resultará muy importante.

Lema 8.19. *Sea a un entero no nulo. Existe $a^* \in \mathbb{Z} \setminus \{0\}$ tal que*

$$aa^* \equiv 1 \pmod{m} \tag{8.14}$$

si y sólo si $(a, m) = 1$. Además, la clase de congruencia de a^* es única. Es decir, si a' es otro entero no nulo que tal que $aa' \equiv 1 \pmod{m}$ entoces $a' \equiv a^* \pmod{m}$.

Demostración. Si $aa^* \equiv 1 \pmod{m}$ entonces $aa^* - 1 = km$ para algún $k \in \mathbb{Z}$. Luego, $1 = aa^* + km$ de donde sale que a y m son coprimos.

Si a y m son coprimos, existen $r, s \in \mathbb{Z}$ tales que $ra + sm = 1$. Luego $ar \equiv 1 \pmod{b}$. Tomar $b = a^*$.

Para ver que dos enteros que cumplen (8.14) son congruentes, multiplicamos $aa^* \equiv 1 \pmod{m}$ por a'. Luego, $a'(aa^*) \equiv a' \pmod{m}$. Como $a'(aa^*) = (aa')a^* \equiv a^* \pmod{m}$ se deduce que $a^* \equiv a' \pmod{m}$, como queríamos ver. □

8.5.1. Los teoremas de Fermat y Euler-Fermat

El siguiente es conocido como el *pequeño teorema de Fermat*.

Teorema 8.20 (Fermat). *Si p es un número primo y $a \in \mathbb{Z}$ entonces*

$$a^p \equiv a \pmod{p} \tag{8.15}$$

Si además $p \nmid a$, es decir si a y p son coprimos, entonces vale

$$a^{p-1} \equiv 1 \pmod{p} \tag{8.16}$$

Nota. No daremos la demostración de este resultado (¡al igual que Fermat!, ver la siguiente nota histórica), ya que el Teorema de Fermat saldrá como caso particular del Teorema de Euler (ver Teorema 8.24).

Por ejemplo, el teorema asegura que

$$2^{19} \equiv 2 \pmod{19}, \qquad 5^{17} \equiv 5 \pmod{17} \qquad \text{ó} \qquad 105^6 \equiv 1 \pmod{7}$$

Observaciones.

(1) Notar que (8.16) no vale si $p \mid a$, pues en ese caso tendríamos $0 \equiv 1 \pmod{p}$.

(2) Los dos enunciados del teorema son equivalentes. Claramente, (8.15) se obtiene de (8.16) multiplicando por a. Para ver la recíproca usamos el Lema 8.19. Sea a^* en entero tal que $aa^* \equiv 1 \pmod{m}$. Multiplicando (8.15) por a^* tenemos $a^p a^* = a^{p-1}(aa^*) \equiv aa^* \pmod{m}$ de donde sale que $a^{p-1} \equiv 1 \pmod{m}$.

(3) La recíproca del teorema de Fermat no vale, es decir, que valga $a^{p-1} \equiv 1 \pmod{p}$ no implica que p sea primo. Por ejemplo, $2^{340} \equiv 1 \pmod{341}$ pero $341 = 11 \cdot 31$ no es primo.

(4) Existen números compuestos n tales que $a^{n-1} \equiv 1 \pmod{n}$ para todo $(a, n) = 1$. A dichos números se los conoce como *números de Carmichael*.

Corolario 8.21. *Sea $a \in \mathbb{Z}$ y p primo. Entonces*

$$a^{(p^n)} \equiv a \pmod{p}$$

para todo $n \in \mathbb{N}$. Si $(a, p) = 1$ entonces $a^{(p^n-1)} \equiv 1 \pmod{p}$.

Demostración. Hacemos inducción en n. Si $n = 1$, el resultado vale trivialmente (Teorema de Fermat). Supongamos que vale $a^{(p^k)} \equiv a \pmod{p}$ para un natural k. Luego,

$$a^{(p^{k+1})} = (a^{p^k})^p \equiv a^p \equiv a \pmod{p}$$

donde primero usamos la hipótesis inductiva y luego el paso inicial (Teorema de Fermat). Luego $a^{(p^n)} \equiv a \pmod{p}$ para todo $n \in \mathbb{N}$.

La segunda afirmación del enunciado puede probarse igualmente usando inducción. Más simple es lo siguiente. Vimos que $a^{(p^n)} - a = a(a^{(p^n-1)} - 1) \equiv 0 \pmod{p}$. Como $(a, p) = 1$, se sigue que $a^{(p^n-1)} - 1 \equiv 0 \pmod{p}$. □

Nota histórica. Pierre de Fermat reveló el enunciado del teorema por primera vez en una carta a Bernhard Frénicle de Bessy, fechada el 18 de Octubre de 1640. Sin embargo no acompañó el enunciado con una prueba, si no que lo hizo con las palabras "te enviaría la prueba, si no temiera que fuera tan larga". La primer prueba escrita del pequeño teorema de Fermat fue dada por Euler en 1736 (¡casi 100 años después!). Sin embargo, se sabe que Leibniz dejó un manuscrito no publicado, con prácticamente la misma prueba, que data de antes de 1683. Por este motivo, sería mas justo llamar al pequeño teorema de Fermat como el teorema de Fermat-Leibniz-Euler.

El Teorema de Fermat se suele usar en combinación con el siguiente resultado.

Proposición 8.22. *Supongamos que $a^r \equiv 1 \pmod{p}$ con $r \in \mathbb{Z}$ y p primo. Si $d = (r, p-1)$ entonces $a^d \equiv 1 \pmod{p}$.*

Demostración. Existen enteros x, y tales que $d = rx + (p-1)y$. Luego,

$$a^d = (a^r)^x (a^{p-1})^y \equiv 1 \pmod{p}$$

como queríamos. □

Por ejemplo, tenemos $2^{16} \equiv 1 \pmod 5$, y como $d = (8,4) = 4$ entonces también vale $2^4 \equiv 1 \pmod 5$.

En particular, la última proposición implica que si r es el menor entero positivo tal que $a^r \equiv 1 \pmod p$ entonces $r \mid p-1$. El entero r que satisface esta propiedad se llama el *orden de a módulo p* y se denota $\mathrm{ord}_p(a)$. Luego, si queremos calcular el orden de a módulo p, los candidatos a mirar son los divisores de $p-1$.

Ejemplo. Supangamos que queremos calcular el orden de 2 módulo $7, 11$ y 13. Sabemos por Fermat que $2^6 \equiv 1 \pmod 7$. Los divisores no triviales de 6 son 2 y 3. Como $2^2 \not\equiv 1 \pmod 7$ y $2^3 \equiv 1 \pmod 7$ entonces $\mathrm{ord}_7(2) = 3$. Para $p = 11$, miramos los divisores de 10. Ni 2^2 ni 2^5 son congruentes a 1 módulo 11. Luego, el orden $\mathrm{ord}_{11}(2) = 10$. Del mismo modo, el lector puede chequear que $2^2, 2^3, 2^4, 2^6 \not\equiv 1 \pmod{13}$ y entonces, por Fermat, $\mathrm{ord}_{13}(2) = 12$. ◊

Aplicación: cálculos de restos de potencias grandes

Podemos usar el teorema para reducir drásticamente una potencia grande módulo un primo p. En general, si queremos calcular a^e módulo un primo p, primero dividimos por $p-1$ y luego usamos Fermat. Si $e = q(p-1)+r$ con q y r el cociente y el resto de dividir por $p-1$ respectivamente, entonces

$$a^e = a^{q(p-1)+r} = (a^{p-1})^q \cdot a^r \equiv a^r \pmod p \tag{8.17}$$

Seguramente, haya que continuar reduciendo a^r, pero éste ya es un número muchísimo más chico que a^e. Por ejemplo, $2^{1492} = 2^{12\cdot 124+4} \equiv 2^4 \equiv 3 \pmod{13}$.

Ejemplo. Calculemos el resto de $3^{20231814311}$ al dividir por 17. Notemos que $20231814311 = 1264488394 \cdot 16 + 7$. Luego, por (8.17)

$$3^{20231814311} \equiv 3^7 \equiv 11 \pmod{17}$$

donde el último paso es muy sencillo, y procedemos como siempre estudiando las potencias de 3: $3^3 \equiv 10$, $3^4 \equiv 13$, $3^5 \equiv 5$ y $3^6 \equiv -2$ módulo 17. ¡Qué sencillo! ◊

8.5.2. Sistemas residuales y teorema de Euler

Sistemas residuales completos y reducidos

Definición. Un conjunto de m representantes, uno de cada una de las m clases de congruencia módulo m, se llama un *sistema **completo** de restos módulo m*. Un *sistema **reducido** de restos módulo m* es un conjunto de $\varphi(m)$ enteros incongruentes módulo m, cada uno coprimo con m. Alternativamente, también diremos *sistema residual completo* y *sistema residual reducido* módulo m.

Ejemplos.

(1) Claramente, $\{0, 1, \ldots, m-1\}$ y $\{1, 2, \ldots, m\}$ son sistemas completos de restos módulo m ($\{0, 1, \ldots, m-1\}$ es llamado *sistema residual **estándar*** módulo m). También son sistemas residuales completos módulo m

$$\{1, m+2, 2m+3, 3m+4, \ldots, m^2\} \quad \text{y} \quad \{m+1, m^2+2, m^3+3, \ldots, m^m+m\}$$

(2) Un sistema residual reducido módulo 8 es $\{1,3,5,7\}$. Un sistema residual reducido módulo 24 es $\{1,5,7,11,13,17,19,23\}$.

(3) Si p es primo, $\{1,2,\dots,p-1\}$ es un sistema residual completo módulo m, que también es reducido.

(4) En algunos casos es conveniente usar tanto números positivos como negativos. Si m es par, digamos $m=2k$, entonces

$$\{-\tfrac{m}{2}+1,-\tfrac{m}{2}+2,\dots,-1,0,1,\dots,\tfrac{m}{2}\}=\{-k+1,-k+2,\dots,-1,0,1,\dots,k\}$$

es un sistema residual completo módulo m. Si m es impar, digamos $m=2k+1$, entonces

$$\{-\tfrac{(m-1)}{2},-\tfrac{(m-1)}{2}+1,\dots,-1,0,1,\dots,\tfrac{m-1}{2}\}=\{-k,-k+1,\dots,-1,0,1,\dots,k\}$$

es un sistema residual completo módulo m. Por ejemplo, $\{-4,\dots,5\}$ es un sistema residual completo módulo 10 y $\{-5,\dots,5\}$ lo es módulo 11. ◊

Proposición 8.23. *Supongamos que* $(k,m)=1$.

(a) Si $\{a_1,\dots,a_m\}$ *es un sistema completo de restos módulo* m*, también lo es* $\{ka_1,\dots,ka_m\}$.

(b) Si $\{a_1,a_2,\dots,a_{\varphi(m)}\}$ *es un sistema reducido de restos módulo* m*, entonces también lo es* $\{ka_1,ka_2,\dots,ka_{\varphi(m)}\}$.

Demostración.
(a) Si $ka_i\equiv ka_j \pmod m$ entonces $a_i\equiv a_j \pmod m$ pues $(k,m)=1$. Luego, el conjunto $\{ka_1,ka_2,\dots,ka_m\}$ es un sistema completo de restos módulo m.

(b) Ningún par de números ka_i es congruente módulo m. Como $(a_i,m)=1=(k,m)$ entonces $(ka_i,m)=1$ para todo i, luego $\{ka_1,ka_2,\dots,ka_{\varphi(m)}\}$ es un sistema reducido de restos módulo m. □

Pregunta. Si $\{a_1,\dots,a_m\}$ y $\{b_1,\dots,b_m\}$ son sistemas residuales completos módulo m. ¿Es $\{a_1b_1,\dots,a_mb_m\}$ un sistema residual completo módulo m? ¿Si m es primo?

El teorema de Euler-Fermat

La siguiente es una generalización natural del teorema de Fermat.

Teorema 8.24 (Euler-Fermat). *Si* $(a,m)=1$*, entonces*

$$a^{\varphi(m)}\equiv 1 \pmod m$$

Si a y m no son coprimos el teorema no vale. Por ejemplo, $2^{\varphi(10)}=2^4\equiv 6 \pmod{10}$.

Demostración. Sea $\{b_1, b_2, \ldots, b_{\varphi(m)}\}$ un sistema residual reducido módulo m. Como a es coprimo con m, resulta que $\{ab_1, ab_2, \ldots, ab_{\varphi(m)}\}$ es un sistema residual reducido, por la Porposición 8.23. Luego, el producto de todos los enteros del primer sistema reducido es congruente al producto de los enteros del segundo sistema reducido

$$(ab_1)(ab_2)\cdots(ab_{\varphi(m)}) \equiv b_1 b_2 \cdots b_{\varphi(m)} \pmod{m}$$

es decir

$$a^{\varphi(m)} b_1 \cdots b_{\varphi(m)} \equiv b_1 \cdots b_{\varphi(m)} \pmod{m}$$

Cancelando los b_i's (pues son coprimos con m) tenemos $a^{\varphi(m)} \equiv 1 \pmod{m}$. □

Nota. Si $m = p$ es primo, entonces $\varphi(p) = p - 1$. Luego, se obtiene el teorema de Fermat clásico, $a^{p-1} \equiv 1 \pmod{p}$, que de este modo queda automáticamente demostrado.

Usando repetidas veces el teorema de Euler, para todo k tenemos

$$a^{(\varphi(m)^k)} \equiv (a^{\varphi(m)})^k \equiv 1 \pmod{m}$$

Ejemplo. Determinemos los últimos 2 dígitos de 1993^{1993}. Hay que calcular $1993^{1993} \pmod{100}$. Como $\varphi(100) = \varphi(4)\varphi(25) = 2 \cdot 20 = 40$, dividimos 1993 por 40 y tenemos $1993 = 40q + 33$ para algún q. Luego,

$$1993^{1993} \equiv 93^{40q+33} = (93^{40})^q 93^{33} \equiv 93^{33} \pmod{100}$$

donde usamos el Teorema de Euler para $93^{40} \equiv 1 \pmod{100}$.

Notemos que $93 \equiv -7 \pmod{100}$, luego $93^{33} \equiv (-1)^{33} 7^{33} \pmod{100}$. Ahora, $7^2 = 49$, $7^3 = 343 \equiv 43 \pmod{100}$, $7^4 = 301 \equiv 1 \pmod{100}$. Luego, $7^{33} = (7^4)^8 \cdot 7 \equiv 7 \pmod{100}$. Por lo tanto, $19993^{1993} \equiv -7 \equiv 93 \pmod{100}$. Es decir, 1993^{1993} termina en 93. ◊

Ejemplo. Veamos que si

$$n \text{ impar} \qquad \Rightarrow \qquad n \mid 2^{n!} - 1.$$

En particular, para los primeros valores de n tenemos

$$\begin{aligned} 3 &\mid 2^{3!} - 1 = 2^6 - 1 \\ 5 &\mid 2^{5!} - 1 = 2^{120} - 1 \\ 7 &\mid 2^{7!} - 1 = 2^{5040} - 1 \\ 9 &\mid 2^{9!} - 1 = 2^{362880} - 1 \end{aligned}$$

En efecto, por el Teorema de Euler-Fermat, $n \mid 2^{\varphi(n)} - 1$. Como $\varphi(n) < n$, entonces $n = \varphi(n) \cdot k$ para algún k. Luego,

$$2^{n!} - 1 = (2^{\varphi(n)} - 1)(2^{\varphi(n)(k-1)} + 2^{\varphi(n)(k-2)} + \cdots + 2^{\varphi(n)2} + 1)$$

Luego, n también divide a $2^{n!} - 1$. ◊

Observación. El Teorema de Euler-Fermat da una forma fácil y efectiva de calcular el entero a^* del Lema 8.19, cuando a y m son coprimos. Como $a^{\varphi(m)-1} a \equiv 1 \pmod{m}$, podemos tomar

$$a^* = a^{\varphi(m)-1} \tag{8.18}$$

Esto resultará muy útil en los próximos capítulos, por ejemplo para resolver ecuaciones lineales en congruencias.

8.5.3. El Torema de Wilson

Es claro que p divide a $p! + p = p((p-1)! + 1)$. El siguiente resultado asegura que p también divide al factor $(p-1)! + 1$.

Teorema 8.25 (Wilson). *Si p es primo, entonces*

$$(p-1)! \equiv -1 \pmod{p} \tag{8.19}$$

Además, $(p-2)! \equiv 1 \pmod{p}$.

Luego, (8.19) es equivalente a

$$p^2 \mid p! + p \tag{8.20}$$

Demostración. Si $p = 2$ ó $p = 3$ el resultado es trivial. Supongamos entonces que $p \geq 5$. Como $(p-1)! = 1 \cdot 2 \cdot 3 \cdots (p-2)(p-1)$ y $p - 1 \equiv -1 \pmod{p}$, basta probar que $(p-2)! = 2 \cdot 3 \cdots (p-2) \equiv 1 \pmod{m}$.

Por el Lema 8.19, para cada entero a con $1 \leq a \leq p-1$ existe un único entero a^* tal que $aa^* \equiv 1 \pmod{p}$ y $1 \leq a^* \leq p-1$. Diremos que a^* es el *inverso* de a módulo p. Luego, por unicidad, si $a_1 \neq a_2$ entonces $a_1^* \neq a_2^*$.

Veamos que cada factor a de $(p-2)!$ y su inverso a^* son distintos. Supongamos entonces que hay un $a \in [2, p-2]$ tal que $a^* = a$. Luego, vale que $a^2 \equiv 1 \pmod{p}$, o sea

$$(a-1)(a+1) = a^2 - 1 \equiv 0 \pmod{p}$$

Luego $a - 1 \equiv 0 \pmod{p}$ ó $a + 1 \equiv 0 \pmod{p}$, es decir $a = 1$ ó $a = p-1$, lo cual es absurdo.

Luego, si $p = 2q + 1$, tenemos

$$(p-2)! = 1 \cdot (a_1 a_1^*) \cdots (a_q a_q^*) \equiv 1 \pmod{p}$$

de donde, multiplicando por $p - 1$, se deduce que $(p-1)! \equiv p - 1 \equiv -1 \pmod{p}$.

Finalmente, como $(p-1)! = (p-1)(p-2)!$ y $p - 1 \equiv -1 \pmod{p}$ se deduce que $(p-2)! \equiv 1 \pmod{p}$. □

Ilustramos la demostración con un ejemplo. Consideremos $p = 11$. Reordenando convenientemente tenemos

$$10! = (1 \cdot 10)[(2 \cdot 6)(3 \cdot 4)(5 \cdot 9)(7 \cdot 8)] \equiv (-1)(1 \cdot 1 \cdot 1 \cdot 1) = -1 \pmod{11}$$

La prueba muestra que esto se puede hacer para cualquier primo p.

Corolario 8.26. *Si $p = 2q + 1$ es un primo impar entonces*

$$(q!)^2 \equiv (-1)^{q+1} \pmod{p} \tag{8.21}$$

Demostración. Partiendo del teorema de Wilson $1 \cdot 2 \cdot 3 \cdots (p-2)(p-1) \equiv -1 \pmod{p}$ podemos escribir

$$1(p-1)2(p-2) \cdots q(p-q) \equiv 1(-1)2(-2) \cdots q(-q) \pmod{p}$$

De aquí tenemos

$$(-1)^q \prod_{j=1}^{q} j^2 \equiv -1 \pmod{p}$$

de donde sigue (8.21). □

Ejemplo. Consideremos los primos $29 = 2 \cdot 14 + 1$ y $47 = 2 \cdot 23 + 1$. Luego, por (8.19) tenemos $28! \equiv -1 \pmod{29}$ y $46! \equiv -1 \pmod{47}$. Además, por (8.21) también valen $(14!)^2 \equiv (-1)^{15} = -1 \pmod{29}$ y $(23!)^2 \equiv (-1)^{24} = 1 \pmod{47}$. ◊

Vimos que $10! \equiv -1 \pmod{11}$. Una consecuencia directa de esto es que el producto de 10 enteros consecutivos cualquiera (no solo los 10 primeros) es congruente a -1 módulo 11, si ninguno es divisible por 11 (obviamente el producto es congruente a 0 módulo 11 si algún entero es divisible por 11). En efecto, reduciendo el conjunto $\{k+1, \ldots, k+10\}$ módulo 11 se tiene el sistema reducido $\{1, 2, \ldots, 10\}$ (ó $\{0, 1, \ldots, 9\}$, dependiendo del caso). Por ejemplo,

$$23 \cdot 24 \cdot 25 \cdots 31 \cdot 32 \equiv 1 \cdot 2 \cdot 3 \cdots 9 \cdot 10 \equiv -1 \pmod{11}$$

Lo visto se generaliza de manera obvia a cualquier primo p. Consideremos $(p-1)$ enteros consecutivos $k+1, \ldots, k+p-1$, ninguno de los cuales es divisible por p. Entonces

$$\prod_{j=1}^{p-1} (k+j) = (k+1)(k+2)\cdots(k+p-1) \equiv -1 \pmod{p}$$

Con la misma idea, esto se puede generalizar aun más tomando $(p-1)$ enteros, uno en cada clase de congruencia módulo p (no necesariamente enteros consecutivos).

Corolario 8.27. *Sea p primo y para cada $1 \leq i \leq p-1$ sea k_i un entero en la clase de congruencia de i módulo p, es decir $k_i \in [i]_p$. Entonces*

$$\prod_{i=1}^{p-1} k_i = k_1 k_2 \cdots k_{p-1} \equiv -1 \pmod{p} \tag{8.22}$$

Demostración. El conjunto $\{k_1, k_2 \ldots, k_{p-1}\}$ es congruente a $\{1, 2, \ldots, p-1\}$ módulo p. Luego $k_1 \cdot k_2 \cdots k_{p-1} \equiv 1 \cdot 2 \cdots p-1 \equiv -1 \pmod{p}$, como queríamos ver. □

Por ejemplo, $\{1, 13, 25, 37, 49, 61, 73, 85, 97, 109\} \equiv \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\} \pmod{11}$, luego

$$1 \cdot 13 \cdot 25 \cdot 37 \cdot 49 \cdot 61 \cdot 73 \cdot 85 \cdot 97 \cdot 109 \equiv 1 \cdot 2 \cdots 10 = 10! \equiv -1 \pmod{11}$$

Ejemplo. Sea p primo y sean $\{a_1, \ldots, a_p\}$, $\{b_1, \ldots, b_p\}$ sistemas residuales completos módulo p. ¿Es $\{a_1 b_1, \ldots, a_p b_p\}$ un sistema residual completo módulo p? Veamos que si p es impar entonces esto no puede pasar.

Sin pérdida de generalidad podemos suponer que $a_p \equiv b_p \equiv 0 \pmod{p}$. Ahora bien, si $\{a_1 b_1, \ldots, a_p b_p\}$ fuera un sistema residual completo módulo p, entonces por (8.22), tendríamos

$$-1 \equiv \prod_{i=1}^{p-1} a_i b_i \equiv \prod_{i=1}^{p-1} a_i \prod_{i=1}^{p-1} b_i \equiv (-1)(-1) = 1 \pmod{p}$$

lo cual sólo vale para $p = 2$, y por lo tanto es absurdo si p es impar. ◊

Veamos algunas ejemplos del uso del Teorema de Wilson.

Ejemplo. Veamos que $437 \mid 18! + 1$. Primero notemos que $437 = 19 \times 23$, ambos primos. Basta ver que

$$18! \equiv -1 \pmod{19}, \quad \pmod{23}$$

La primera identidad vale directamente por el Teorema de Wilson y además $22! \equiv -1 \pmod{23}$. Ahora

$$22! = 18! \cdot 19 \cdot 20 \cdot 21 \cdot 22 \equiv 18! \cdot (-1)(-2)(-3)(-4) = 18!24 \equiv 18! \pmod{23}$$

de donde $18! \equiv -1 \pmod{23}$. Luego 437 divide a $18! + 1$. ◊

Ejemplo. Sea $a \in \mathbb{N}$ tal que

$$1 + \tfrac{1}{2} + \tfrac{1}{3} + \cdots + \tfrac{1}{23} = \tfrac{a}{23!}$$

Encontrar a módulo 13. Escribimos

$$a = 23! + \tfrac{23!}{2} + \cdots + \tfrac{23!}{23}$$

Claramente, todos los términos $23!/k$ son divisibles por 13 salvo $23!/13$. Luego,

$$a \equiv \tfrac{23!}{13} = (1 \cdot 2 \cdots 12) \times (14 \cdot 15 \cdots 23) \equiv 12! \times (1 \cdot 2 \cdots 10) \equiv 12!10! \pmod{13}$$

Por el Teorema de Wilson tenemos que $12! \equiv -1 \pmod{13}$ y que $11! \equiv 1 \pmod{13}$. Como $11 \cdot 10! = 11! \equiv 1 \equiv 66 \pmod{13}$ tenemos que $10! \equiv 6 \pmod{13}$. Finalmente, llegamos a que $a \equiv 12!10! \equiv (-1)6 \equiv 7 \pmod{13}$. ◊

Nota histórica. El enunciado del Teorema de Wilson apareció publicado por primera vez en 1770, en el trabajo *Meditationes Algebraicae* del matemático inglés Edward Waring, en el cual aparecían varios resultados novedosos para la época. El resultado se debe a un alumno suyo llamado John Wilson aunque, similarmente a Fermat con su pequeño teorema, ninguno de los dos aportó una prueba. Wilson y Waring creían que la falta de una notación adecuada era lo que hacía el resultado difícil de probar. Al leer el pasaje en el libro, Gauss pronunció su rotundo comentario "nociones versus notaciones". Efectivamente, al poco tiempo, en 1771, Lagrange presentó la primera demostración de este hecho, donde además observó que la recíproca del teorema también era válida.

Como en el caso del pequeño teorema de Fermat, hay evidencia que de Leibniz estaba al tanto de esta propiedad, pero nunca publicó una prueba. Más curioso resulta el hecho de que Abu Ali al-Hasan ibn al-Haytham (ca. 950 - 1040, matemático, físico y astrónomo, considerado por muchos como el creador del método científico), más conocido como Alhazén o Alhacén, mucho tiempo antes, cerca del año 1000, resolvió ciertos problemas que involucraban (las hoy llamadas) congruencias utilizando el resultado conocido como el Teorema de Wilson. Por este motivo, sería mas justo llamarlo el Teorema de Alhacén-Leibniz-Wilson-Lagrange.

Como acabamos de mencionar, la recíproca del Teorema de Wilson también vale.

Proposición 8.28 (Lagrange). *Si* $(n-1)! \equiv -1 \pmod{n}$ *entonces* n *es primo.*

Demostración. Supongamos que n no es primo. Entonces n tiene un divisor d no trivial, i.e. $1 < d < n$. Además $d \mid (n-1)!$ pues $d \leq n-1$. Por hipótesis, $n \mid (n-1)!+1$ y; como $d \mid n$, por transitividad tenemos $d \mid (n-1)!+1$. Luego $d \mid 1$, lo cual es absurdo. Luego n es primo. □

Como consecuencia del Teorema de Wilson y su recíproco, tenemos que

$$(n-1)! \equiv -1 \pmod{n} \qquad \Leftrightarrow \qquad n \text{ es primo.}$$

Es decir, tenemos lo que se llama un *test de primalidad*; esto es, un criterio para decidir si un entero n dado es primo o no. El problema de este métodos es que resulta de escaso valor práctico, ya que es muy complicado calcular $(n-1)!$ para n grande y todavía reducirlo módulo p. Sin embargo, para valores pequeños de n esto funciona y podemos ponerlo en práctica con la ayuda de computadoras. Ilustramos con los primeros valores de n.

n	$(n-1)!$	$(n-1)! \pmod{n}$	primo
2	1	1	✓
3	2	2	✓
4	6	2	✗
5	24	4	✓
6	120	0	✗
7	720	6	✓
8	5040	0	✗
9	40320	0	✗
10	362880	0	✗

Observación. El teorema de Wilson implica el Teorema de Fermat. En efecto, sea a un entero coprimo con p primo. Veamos que $\{a, 2a, 3a, \ldots, (p-1)a\}$ es un sistema reducido módulo p equivalente al sistema reducido estándar $\{1, 2, 3, \ldots, p-1\}$. En efecto, si $aj \equiv ak \pmod{p}$ con $1 \leq j, k \leq p-1$, entonces $p \mid a(j-k)$. Como p es coprimo con a debe dividir a $j-k$, luego $j = k$. Así,

$$a \cdot 2a \cdot 3a \cdots (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) = (p-1)! \equiv -1 \pmod{p}$$

y por otra parte

$$a \cdot 2a \cdot 3a \cdots (p-1)a = a^{p-1}(p-1)! \equiv -a^{p-1} \pmod{p}$$

donde hemos usado el teorema de Wilson 2 veces. Luego, $-a^{p-1} \equiv -1 \pmod{p}$, es decir $a^{p-1} \equiv 1 \pmod{p}$, como queríamos ver.

Recíprocamente, es posible probar el Teorema de Wilson usando el Teorema de Euler-Fermat y el Teorema Chino del resto (que veremos mas adelante) o también usando números combinatorios (que veremos más adelante) y el Teorema de Fermat. Dejamos la demostración de este hecho para más adelante (ver ???).

Aplicación: mezclado de cartas

(ver book of numbers o el de edwards)

Riffle shuffle algo

Monge shuffle algo

8.6. Ejercicios

Andrew Wiles presentó en 1993 una demostración para el 'Último Teorema de Fermat' (conjeturado por Pierre Fermat en 1637). Sin embargo, esta tenía un error que él mismo pudo corregir dos años más tarde. Así describe Andrew Wiles su trabajo:

> *"Uno entra en la primera habitación de una mansión y está en la oscuridad. En una oscuridad completa. Vas tropezando y golpeando los muebles, pero poco a poco aprendes dónde está cada elemento del mobiliario. Al fin, tras seis meses más o menos, encuentras el interruptor de la luz y de repente todo está iluminado. Puedes ver exactamente dónde estás. Entonces vas a la siguiente habitación y te pasas otros seis meses en las tinieblas. Así, cada uno de estos progresos, aunque a veces son muy rápidos y se realizan en un solo día o dos, son la culminación de meses precedentes de tropezones en la oscuridad, sin los que el avance sería imposible."*

Ejercicio 8.1. Hallar el resto en la división por 5 y por 7 de los siguientes números:

(I) $\sum_{i=1}^{8} i^8$. (II) $3 \cdot 11 \cdot 17 \cdot 71 \cdot 101$. (III) $\sum_{i=1}^{30} 6^i$.

Ejercicio 8.2. (I) Hallar el resto de la división de $1^5 + 2^5 + 3^5 + \cdots + 100^5$ por 4.

(II) Probar que $111^{333} + 333^{111}$ es divisible por 7.

(III) Hallar la cifra de las unidades y la de las decenas del número 7^{15}.

Ejercicio 8.3. (I) Hallar el resto de la división de 2^{51833} por 31.

(II) Hallar el resto de la división de $43 \cdot 2^{163} + 11 \cdot 5^{221} + 61^{999}$ por 31.

(III) Probar que $2^{5n} \equiv 1 \pmod{31}$ para todo $n \in \mathbb{N}$.

(IV) Sea $k \in \mathbb{N}$ tal que $2^k \equiv 39 \pmod{31}$. Hallar el resto de la división de k por 5.

Ejercicio 8.4. Sean a, b y c números enteros, ninguno divisible por 3. Probar que $a^2 + b^2 + c^2 \equiv 0 \pmod{3}$.

Ejercicio 8.5. (I) Probar las reglas de divisibilidad por 2, 3, 4, 5, 8, 9 y 11.

(II) Decir por cuáles de los números 2, 3, 4, 5, 8, 9 y 11 son divisibles los siguientes números:

$$12342, \quad 5176, \quad 314573, \quad 899.$$

Ejercicio 8.6. Resolver las siguientes ecuaciones:

(I) $2x \equiv -21 \pmod 8$. (II) $2x \equiv -12 \pmod 7$. (III) $3x \equiv 5 \pmod 4$.

Ejercicio 8.7. Resolver la ecuación $221x \equiv 85 \pmod{340}$. Hallar las soluciones x tales que $0 \leq x < 340$.

Ejercicio 8.8. (I) Determinar si existe algún entero x que satisfaga simultáneamente:

a) $x \equiv 1 \pmod 6$, $x \equiv 2 \pmod{20}$ y $x \equiv 3 \pmod 9$.
b) $x \equiv 1 \pmod{12}$, $x \equiv 7 \pmod{10}$ y $x \equiv 4 \pmod{20}$.

En caso afirmativo, hallar dichos enteros.

(II) Sabiendo que los restos de la división de un entero a por 3, 5 y 8 son 2, 3 y 5 respectivamente, hallar el resto de la división de a por 120.

Ejercicio 8.9. ¿Existen 21 enteros positivos consecutivos tales que cada uno de ellos es divisible por al menos uno de los siguientes números: 2, 3, 5, 7, 11, 13?

Ejercicio 8.10. La producción diaria de huevos en una granja es inferior a 75. Cierto día el recolector informó que la cantidad de huevos recogidos era tal que contando de a 3 sobraban 2, contando de a 5 sobraban 4 y contando de a 7 sobraban 5. El capataz, dijo que eso era imposible. ¿Quién tenía razón? Justificar.

Ejercicio 8.11. Probar que para cada entero positivo n, existen n enteros positivos consecutivos tales que ninguno de ellos es libre de cuadrados.

Ejercicio 8.12. (I) Calcular $\phi(m)$ para $m = 11, 12, 35, 61, 105, 1001$.

(II) ¿Es 10 inversible módulo 61? ¿y módulo 105? En caso afirmativo, hallar su inverso.

(III) Determinar los inversibles módulo m, para $m = 11, 12$. Para cada uno de ellos, hallar su inverso.

(IV) Probar que si $(a, 1001) = 1$ entonces 1001 divide a $a^{720} - 1$.

Ejercicio 8.13. (I) Probar que $(-13)^{n+1} \equiv (-13)^n + (-13)^{n-1} \pmod{181}$ para todo $n \in \mathbb{N}$.

(II) Probar que 13 divide a $11^{12n+6} + 1$ para todo $n \in \mathbb{N}$.

Ejercicio 8.14. (I) Hallar el resto de la división de $3 \cdot 7^{135} + 24^{78} + 11^{222}$ por 70.

(II) Hallar el resto de la división de 3^{385} por 400.

(III) Hallar el resto de la división de 2^{2^n} por 13 para cada $n \in \mathbb{N}$.

Ejercicio 8.15. (I) Hallar todos los $a \in \mathbb{Z}$ tales que $539 \mid 3^{253}a + 5^{44}$.

(II) Hallar todos los $n \in \mathbb{N}$ tales que $3^n \equiv 53 \pmod{77}$.

Ejercicio 8.16. Decidir si existe un conjunto S formado por 2013 enteros positivos tales que:

- Los elementos de S son relativamente primos de a pares.
- La suma de cualesquiera k elementos en S es compuesta, para todo $k \geq 2$.

Ejercicios complementarios

Ejercicio 8.17. Sean $a, b, m \in \mathbb{Z}$ todos divisibles por cierto $d > 0$. Probar que la ecuación $ax \equiv b \pmod{m}$ tiene solución si y sólo si la tiene

$$\frac{a}{d}\, x \equiv \frac{b}{d} \left(\mod \frac{m}{d} \right).$$

Ejercicio 8.18. (I) Sea $a \in \mathbb{Z}$ tal que $a \equiv 22 \pmod{14}$. Hallar el resto de dividir a a por 2, 7 y 14.

(II) Sea $a \in \mathbb{Z}$ tal que $a \equiv 13 \pmod{5}$. Hallar el resto de dividir a $33a^3 + 3a^2 - 197a + 2$ por 5.

(III) Hallar, para cada $n \in \mathbb{N}$, el resto de la división de $\sum_{i=1}^{n} (-1)^i\, i!$ por 36.

Ejercicio 8.19. Encontrar el resto en la división de a por b en los siguientes casos:

(I) $a = 11^{13} \cdot 13^8$, $b = 12$.

(II) $a = 4^{1000}$, $b = 7$.

(III) $a = 123^{456}$, $b = 31$.

(IV) $a = 7^{83}$, $b = 10$.

Ejercicio 8.20. Sean a, m y n enteros positivos. Probar que $(a^n - 1, a^m - 1) = a^{(n,m)} - 1$.

Ejercicio 8.21. Sabiendo que $1001 = 7 \cdot 11 \cdot 13$, deducir criterios de divisibilidad por 7, 11 y 13.

Ejercicio 8.22. Sea p un primo impar. Probar que:

(I) $1^{p-1} + 2^{p-1} + \cdots + (p-1)^{p-1} \equiv -1 \pmod{p}$.

(II) $1^p + 2^p + \cdots + (p-1)^p \equiv 0 \pmod{p}$.

Ejercicio 8.23. Hallar todos los x que satisfacen:

(I) $x^2 \equiv 1 \pmod{4}$.

(II) $x^2 \equiv x \pmod{12}$.

(III) $x^2 \equiv 2 \pmod{3}$.

(IV) $x^2 \equiv 0 \pmod{12}$.

(V) $x^4 \equiv 1 \pmod{16}$.

(VI) $3x \equiv 1 \pmod{5}$.

Ejercicio 8.24. Hallar todos los enteros que satisfacen simultáneamente:

(I) $x \equiv 1 \pmod{3}$, $x \equiv 1 \pmod{5}$ y $x \equiv 1 \pmod{7}$.

(II) $x \equiv 2 \pmod{3}$, $x \equiv 3 \pmod{5}$ y $x \equiv 5 \pmod{2}$.

Ejercicio 8.25. Hallar un entero a entre 60 y 90 tal que el resto de la división de $2a$ por 3 sea 1 y el resto de la división de $7a$ por 10 sea 8.

Ejercicio 8.26. (I) Hallar el resto de la división de $5! \cdot 25!$ por 31.

(II) Hallar el residuo de la división de 70! por 5183.

Ejercicio 8.27. Una banda de 17 piratas robó una bolsa con monedas de oro de un barco enemigo. Cuando intentaron repartir las monedas en partes iguales, sobraban 3 monedas. En medio de la discusión sobre cómo proceder con la distribución uno de los piratas murió. Al intentar nuevamente dividir las monedas en partes iguales, sobraban 10 monedas. Una nueva discusión terminó con la muerte de otro pirata. Finalmente volvió la paz al barco cuando intentaron dividir las monedas en partes iguales y lo lograron. ¿Cuál es el mínimo número de monedas que robaron?

Ejercicio 8.28. Si p y q son dos primos distintos, probar que $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$.

Ejercicio 8.29. Hallar todos los primos p, q tales que pq divide a $(5^p - 2^p)(5^q - 2^q)$.

Ejercicio 8.30. Probar que si $n \geq 6$ no es primo, entonces $(n-1)! \equiv 0 \pmod{n}$.

Ejercicio 8.31. ¿Para qué valores de n es $10^n - 1$ divisible por 11?

Capítulo 9

Enteros modulares

9.1. Los enteros modulares

Ahora, dado un $m \in \mathbb{N}$, haremos aritmética con las clases de equivalencia de la congruencia módulo m. Esto requiere un grado de abstracción mayor. Hasta ahora hemos hecho aritmética con números cuya naturaleza comprendemos. En cambio ahora haremos aritmética con conjuntos formados por números, las clases de congruencia. Sumaremos y multiplicaremos estas clases que darán como resultado otra clase. Encontraremos interesantes particularidades artiméticas que dependerán en muchos casos del m elegido. Por ejemplo, habrá clases que tengan inverso multiplicativo y otras que no.

Recordamos que dado $m \in \mathbb{N}$, con $[a]_m$ denotamos a la clase de todos los enteros congruentes con a módulo m y con $\overline{a}$ la reducción de a módulo m, es decir su resto al dividir por m.

Definición. Dado $m \in \mathbb{N}$, definimos $\mathbb{Z}_m$ como el conjunto de clases de equivalencia de la relación de congruencia módulo m. Así,

$$\mathbb{Z}_m = \{[0], [1], \ldots, [m-1]\}$$

A los elementos de $\mathbb{Z}_m$ se los llama *enteros modulares* módulo m y $\mathbb{Z}_m$ es el *anillo de enteros modulares* módulo m.

Para poder hacer aritmética, necesitamos definir sumas y productos en $\mathbb{Z}_m$. Definiremos las operaciones

$$+ : \mathbb{Z}_m \times \mathbb{Z}_m \to \mathbb{Z}_m \qquad \text{y} \qquad \cdot : \mathbb{Z}_m \times \mathbb{Z}_m \to \mathbb{Z}_m,$$

a partir de la suma y el producto de enteros, como sigue.

- La suma de dos clases es la clase de la suma de dos representantes, uno de cada clase.
- El producto de dos clases es la clase del producto de dos representantes, uno de cada clase.

En símbolos:

$$[a] + [b] = [a + b] \qquad \text{y} \qquad [a] \cdot [b] = [a \cdot b] \tag{9.1}$$

Buena definición

Estas definiciones necesitan de la elección de representantes de las clases a sumar o multiplicar, por lo tanto hay que verificar que independientemente de cual sea la elección de representantes, el resultado es el mismo. Es necesario mostrar que las definiciones dadas no son ambiguas.

La buena definición de la suma y el producto de clases se sigue de la Proposición 8.4. En efecto, supongamos que a y a' son representantes de la misma clase y que b y b' son representantes de una misma clase, es decir $a \equiv a'$ y $b \equiv b'$. De la Proposición 8.4 se sigue que

$$a + b \equiv a' + b' \qquad \text{y} \qquad ab \equiv a'b'$$

y por lo tanto

$$[a] + [b] = [a + b] = [a' + b'] = [a'] + [b']$$
$$[a] \cdot [b] = [a \cdot b'] = [a' \cdot b'] = [a'] \cdot [b']$$

Además, podemos definir un producto entre enteros y clases, es decir $\cdot : \mathbb{Z} \times \mathbb{Z}_m \to \mathbb{Z}_m$, de la siguiente manera. Si $k \in \mathbb{Z}$, definimos $k[a]$ como la suma de la clase $[a]$ con si misma k veces. Luego,

$$k[a] := \underbrace{[a] + \cdots + [a]}_{k-\text{veces}} = \underbrace{[a + \cdots + a]}_{k-\text{veces}} = [ka]$$

Ejemplo. sea $m = 6$.

(1) Para calcular la suma de las clases $[3]$ y $[4]$, sumamos $3 + 4 = 7$ y el resultado es entonces la clase del 7, $[7]$; como $7 \equiv 1 \mod 6$, $[7] = [1]$ y podemos decir que

$$[3] + [4] = [1]$$

También es cierto que $[3] + [4] = [7]$ y aún que $[3] + [4] = [13]$ pues 1, 7 y 13 son todos equivalentes módulo 6.

(2) Para calcular el producto de las clases $[3]$ y $[4]$, multiplicamos $3 \times 4 = 12$ y el resultado es entonces la clase del 12, $[12]$; como $12 \equiv 0 \mod 6$, podemos decir que

$$[3] \cdot [4] = [0]$$

También podemos decir que $[3] \cdot [4] = [12]$ y aún que $[3] \cdot [4] = [18]$ pues 0, 12 y 18 son todos equivalentes módulo 6.

(3) La suma de $[4]$ con sí mismo 5 veces, es

$$[4] + [4] + [4] + [4] + [4] = [4 + 4 + 4 + 4 + 4] = [20] = [2]$$

es decir, $5[4] = [5 \cdot 4] = [2]$. ◊

En la aritmética modular hay algunas propiedades que valen cualquiera sea el m considerado.

- De la definición de la suma es inmediato que $[0]$ es un elemento neutro, ya que cualquiera sea a se tiene que

$$[a] + [0] = [0] + [a] = [a]$$

- De la definición del producto es inmediato que $[1]$ es una identidad, ya que para todo a vale

$$[a] \cdot [1] = [1] \cdot [a] = [a]$$

- Cualquiera sea a, tenemos

$$[a] + [m - a] = [a + (m - a)] = [m] = [0]$$

Es decir, la clase $[m - a] = [-a]$ es opuesta de la clase $[a]$. Así, $[a]$ tiene un opuesto, que resulta único (veremos), que se denota $-[a]$. O sea,

$$-[a] = [-a]$$

- Al igual que sucede en los enteros, la identidad $[1]$ y el opuesto de la identidad $[-1] = [m - 1]$ tienen inverso multiplicativo: ellos mismos. En efecto,

$$[1] \cdot [1] = [1 \cdot 1] = [1]$$

y

$$[-1] \cdot [-1] = [(-1) \cdot (-1)] = [1]$$

Estos inversos resultan únicos (veremos) y ponemos

$$[1]^{-1} = [1] \qquad \text{y} \qquad [-1]^{-1} = [-1] = -[1]$$

Pregunta. ¿Son los elementos neutros y los opuestos de $\mathbb{Z}_m$ únicos como en $\mathbb{Z}$?

A pesar de compartir algunas propiedades básicas con la aritmética de los enteros, hay diferencias que dan lugar a fenómenos nuevos.

Ejemplos.

(1) En $\mathbb{Z}_{14}$, $[3][5] = [1]$, pues $3 \cdot 5 = 15 \equiv 1 \pmod 1 4$. Es decir, tanto 3 como 5 tienen inverso multiplicativo en $\mathbb{Z}_{14}$, distintos de 1 y -1. De hecho $[3]^{-1} = [5]$ y $[5]^{-1} = [3]$

(2) En $\mathbb{Z}_8$, $[4][6] = [0]$ pues, $4 \cdot 6 = 24 \equiv 0 \pmod 8$. Es decir, en $\mathbb{Z}_8$ hay dos clases no nulas cuyo producto da 0. En particular, estas clases no tienen inverso.

(3) $\mathbb{Z}_3$ tiene 3 elementos, $[0]$, $[1]$ y $[2]$. Se tiene que $[2][2] = [1]$ y así todo elemento no nulo de $\mathbb{Z}_3$ tiene inverso multiplicativo. Propiedad ésta que $\mathbb{Z}$ no tiene, pero que si tienen $\mathbb{R}$ y $\mathbb{Q}$. ◊

9.2. Tablas de suma y producto

Como $\mathbb{Z}_m$ es finito, podemos mostrar las tablas de la suma y el producto completas. En ellas, muchas de las propiedades de cada $\mathbb{Z}_m$ en particular quedan a la vista. Veamos los primeros casos, es decir $2 \leq m \leq 9$.

De ahora en mas, por simpleza y practicidad, escribiremos $\boldsymbol{a}$ en lugar de $[a]$. Es decir,

$$\mathbb{Z}_n = \{\mathbf{0}, \mathbf{1}, \mathbf{2}, \ldots, \boldsymbol{n-1}\}$$

9.2.1. $\mathbb{Z}_2$

$+$	$\mathbf{0}$	$\mathbf{1}$
$\mathbf{0}$	$\mathbf{0}$	$\mathbf{1}$
$\mathbf{1}$	$\mathbf{1}$	$\mathbf{0}$

$\cdot$	$\mathbf{0}$	$\mathbf{1}$
$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$
$\mathbf{1}$	$\mathbf{0}$	$\mathbf{1}$

9.2.2. $\mathbb{Z}_3$

$+$	$\mathbf{0}$	$\mathbf{1}$	$\mathbf{2}$
$\mathbf{0}$	$\mathbf{0}$	$\mathbf{1}$	$\mathbf{2}$
$\mathbf{1}$	$\mathbf{1}$	$\mathbf{2}$	$\mathbf{0}$
$\mathbf{2}$	$\mathbf{2}$	$\mathbf{0}$	$\mathbf{1}$

$\cdot$	$\mathbf{0}$	$\mathbf{1}$	$\mathbf{2}$
$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$
$\mathbf{1}$	$\mathbf{0}$	$\mathbf{1}$	$\mathbf{2}$
$\mathbf{2}$	$\mathbf{0}$	$\mathbf{2}$	$\mathbf{1}$

9.2.3. $\mathbb{Z}_4$

$+$	$\mathbf{0}$	$\mathbf{1}$	$\mathbf{2}$	$\mathbf{3}$
$\mathbf{0}$	$\mathbf{0}$	$\mathbf{1}$	$\mathbf{2}$	$\mathbf{3}$
$\mathbf{1}$	$\mathbf{1}$	$\mathbf{2}$	$\mathbf{3}$	$\mathbf{0}$
$\mathbf{2}$	$\mathbf{2}$	$\mathbf{3}$	$\mathbf{0}$	$\mathbf{1}$
$\mathbf{3}$	$\mathbf{3}$	$\mathbf{0}$	$\mathbf{1}$	$\mathbf{2}$

$\cdot$	$\mathbf{0}$	$\mathbf{1}$	$\mathbf{2}$	$\mathbf{3}$
$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$
$\mathbf{1}$	$\mathbf{0}$	$\mathbf{1}$	$\mathbf{2}$	$\mathbf{3}$
$\mathbf{2}$	$\mathbf{0}$	$\mathbf{2}$	$\mathbf{0}$	$\mathbf{2}$
$\mathbf{3}$	$\mathbf{0}$	$\mathbf{3}$	$\mathbf{2}$	$\mathbf{1}$

9.2.4. $\mathbb{Z}_5$

$+$	$\mathbf{0}$	$\mathbf{1}$	$\mathbf{2}$	$\mathbf{3}$	$\mathbf{4}$
$\mathbf{0}$	$\mathbf{0}$	$\mathbf{1}$	$\mathbf{2}$	$\mathbf{3}$	$\mathbf{4}$
$\mathbf{1}$	$\mathbf{1}$	$\mathbf{2}$	$\mathbf{3}$	$\mathbf{4}$	$\mathbf{0}$
$\mathbf{2}$	$\mathbf{2}$	$\mathbf{3}$	$\mathbf{4}$	$\mathbf{0}$	$\mathbf{1}$
$\mathbf{3}$	$\mathbf{3}$	$\mathbf{4}$	$\mathbf{0}$	$\mathbf{1}$	$\mathbf{2}$
$\mathbf{4}$	$\mathbf{4}$	$\mathbf{0}$	$\mathbf{1}$	$\mathbf{2}$	$\mathbf{3}$

$\cdot$	$\mathbf{0}$	$\mathbf{1}$	$\mathbf{2}$	$\mathbf{3}$	$\mathbf{4}$
$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$
$\mathbf{1}$	$\mathbf{0}$	$\mathbf{1}$	$\mathbf{2}$	$\mathbf{3}$	$\mathbf{4}$
$\mathbf{2}$	$\mathbf{0}$	$\mathbf{2}$	$\mathbf{4}$	$\mathbf{1}$	$\mathbf{3}$
$\mathbf{3}$	$\mathbf{0}$	$\mathbf{3}$	$\mathbf{1}$	$\mathbf{4}$	$\mathbf{2}$
$\mathbf{4}$	$\mathbf{0}$	$\mathbf{4}$	$\mathbf{3}$	$\mathbf{2}$	$\mathbf{1}$

9.2.5. $\mathbb{Z}_6$

$+$	**0**	**1**	**2**	**3**	**4**	**5**
0	**0**	**1**	**2**	**3**	**4**	**5**
1	**1**	**2**	**3**	**4**	**5**	**0**
2	**2**	**3**	**4**	**5**	**0**	**1**
3	**3**	**4**	**5**	**0**	**1**	**2**
4	**4**	**5**	**0**	**1**	**2**	**3**
5	**5**	**0**	**1**	**2**	**3**	**4**

$\cdot$	**0**	**1**	**2**	**3**	**4**	**5**
0	**0**	**0**	**0**	**0**	**0**	**0**
1	**0**	**1**	**2**	**3**	**4**	**5**
2	**0**	**2**	**4**	**0**	**2**	**4**
3	**0**	**3**	**0**	**3**	**0**	**3**
4	**0**	**4**	**2**	**0**	**4**	**2**
5	**0**	**5**	**4**	**3**	**2**	**1**

9.2.6. $\mathbb{Z}_7$

$+$	**0**	**1**	**2**	**3**	**4**	**5**	**6**
0	**0**	**1**	**2**	**3**	**4**	**5**	**6**
1	**1**	**2**	**3**	**4**	**5**	**6**	**0**
2	**2**	**3**	**4**	**5**	**6**	**0**	**1**
3	**3**	**4**	**5**	**6**	**0**	**1**	**2**
4	**4**	**5**	**6**	**0**	**1**	**2**	**3**
5	**5**	**6**	**0**	**1**	**2**	**3**	**4**
6	**6**	**0**	**1**	**2**	**3**	**4**	**5**

$\cdot$	**0**	**1**	**2**	**3**	**4**	**5**	**6**
0	**0**	**0**	**0**	**0**	**0**	**0**	**0**
1	**0**	**1**	**2**	**3**	**4**	**5**	**6**
2	**0**	**2**	**4**	**6**	**1**	**3**	**5**
3	**0**	**3**	**6**	**2**	**5**	**1**	**4**
4	**0**	**4**	**1**	**5**	**2**	**6**	**3**
5	**0**	**5**	**3**	**1**	**6**	**4**	**2**
6	**0**	**6**	**5**	**4**	**3**	**2**	**1**

9.2.7. $\mathbb{Z}_8$

$+$	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
0	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
1	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**0**
2	**2**	**3**	**4**	**5**	**6**	**7**	**0**	**1**
3	**3**	**4**	**5**	**6**	**7**	**0**	**1**	**2**
4	**4**	**5**	**6**	**7**	**0**	**1**	**2**	**3**
5	**5**	**6**	**7**	**0**	**1**	**2**	**3**	**4**
6	**6**	**7**	**0**	**1**	**2**	**3**	**4**	**5**
7	**7**	**0**	**1**	**2**	**3**	**4**	**5**	**6**

$\cdot$	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
0	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**
1	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
2	**0**	**2**	**4**	**6**	**0**	**2**	**4**	**6**
3	**0**	**3**	**6**	**1**	**4**	**7**	**2**	**5**
4	**0**	**4**	**0**	**4**	**0**	**4**	**0**	**4**
5	**0**	**5**	**2**	**7**	**4**	**1**	**6**	**3**
6	**0**	**6**	**4**	**2**	**0**	**6**	**4**	**2**
7	**6**	**7**	**6**	**5**	**4**	**3**	**2**	**1**

9.2.8. $\mathbb{Z}_9$

$+$	0	1	2	3	4	5	6	7	8
0	0	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8	0
2	2	3	4	5	6	7	8	0	1
3	3	4	5	6	7	8	0	1	2
4	4	5	6	7	8	0	1	2	3
5	5	6	7	8	0	1	2	3	4
6	6	7	8	0	1	2	3	4	5
7	7	8	0	1	2	3	4	5	6
8	8	0	1	2	3	4	5	6	7

$\cdot$	0	1	2	3	4	5	6	7	8
0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8
2	0	2	4	6	8	1	3	5	7
3	0	3	6	0	3	6	0	3	6
4	0	4	8	3	7	2	6	1	5
5	0	5	1	6	2	7	3	8	4
6	0	6	3	0	6	3	0	6	3
7	0	7	5	3	1	8	6	4	2
8	0	8	7	6	5	4	3	2	1

Observaciones. Mirando las tablas precedentes se observa lo siguiente.

(1) Por la conmutatividad de las operaciones, las tablas son simétricas respecto de las diagonales principales.

(2) En las tablas de la suma, cada número aparece una sola vez en cada fila y en cada columna, corridos cíclicamente.

(3) En la tabla de productos de $\mathbb{Z}_m$, la fila (columna) $m-k$ es reversa de la fila (columna) k (salvo el 0).

(4) En la tabla de los productos de $\mathbb{Z}_m$, en la diagonal principal aparecen los cuadrados módulo m.

(5) En la tabla de los productos, salvo por la fila (columna) nula, los ceros aparecen en las filas (columnas) k con $k \mid m$. Dicho de otro modo, si $(k, m) = 1$ entonces las entradas de la fila (columna) k son todas no nulas.

(6) En la tabla del producto de $\mathbb{Z}_m$, no aparece el 0 (salvo en la primera fila y columna) si y sólo si el m es primo.

(7) En las tablas de la suma y el producto de $\mathbb{Z}_m$, todas las filas y columnas suman cero si el m es primo. ¿Vale la recíproca?

Pregunta para pensar. ¿Son estos hechos válidos en general? ¿Algunos, todos? En el caso afirmativo ¿se anima el lector a probar alguno de ellos?

9.3. Aritmética modular

Ya estamos en condiciones para hacer aritmética en $\mathbb{Z}_m$. Sin embargo, antes de continuar, creemos que es bueno hacer una pausa para reflexionar sobre esto y hacerlo en paralelo con la aritmética de los enteros que nos es más familiar.

En este caso tenemos ahora un conjunto finito de m elementos, $\mathbb{Z}_m$, en el cual tenemos definidas dos operaciones, una suma y un producto. Notablemente éstas satisfacen las mismas propiedades básicas que la suma y el producto de enteros y luego comparten todas las propiedades que se derivan de ellas. Desde ya que los enteros y los enteros módulo m son conjuntos de números muy distintos, sin embargo comparten cierta estructura artimética.

PROPIEDADES BÁSICAS DE LA ARITMÉTICA MODULAR.

Para todo m, dados $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c} \in \mathbb{Z}_m$, valen

- De la suma:
  - Asociatividad:
    $$\boldsymbol{a} + (\boldsymbol{b} + \boldsymbol{c}) = (\boldsymbol{a} + \boldsymbol{b}) + \boldsymbol{c} = \boldsymbol{a} + \boldsymbol{b} + \boldsymbol{c}$$
  - Conmutatividad:
    $$\boldsymbol{a} + \boldsymbol{b} = \boldsymbol{b} + \boldsymbol{a}$$
  - Existencia de un único neutro:
    $$\boldsymbol{a} + \mathbf{0} = \mathbf{0} + \boldsymbol{a} = \boldsymbol{a}$$
    Si además $\boldsymbol{a} + \mathbf{0'} = \mathbf{0'} + \boldsymbol{a} = \boldsymbol{a}$ entonces $\mathbf{0} = \mathbf{0'}$.
  - Existencia de opuestos únicos: se tiene
    $$\boldsymbol{a} + (-\boldsymbol{a}) = \mathbf{0}$$
    Además, si $\boldsymbol{a} + \boldsymbol{a'} = \mathbf{0}$ entonces $\boldsymbol{a'} = -\boldsymbol{a}$. La clase $-\boldsymbol{a}$ se dice el *opuesto* de $\boldsymbol{a}$.
- Del producto:
  - Asociatividad:
    $$\boldsymbol{a} \cdot (\boldsymbol{b} \cdot \boldsymbol{c}) = (\boldsymbol{a} \cdot \boldsymbol{b}) \cdot \boldsymbol{c} = \boldsymbol{a} \cdot \boldsymbol{b} \cdot \boldsymbol{c}$$
  - Conmutatividad:
    $$\boldsymbol{a} \cdot \boldsymbol{b} = \boldsymbol{b} \cdot \boldsymbol{a}$$
  - Existencia de una única identidad:
    $$\boldsymbol{a} \cdot \mathbf{1} = \mathbf{1} \cdot \boldsymbol{a} = \boldsymbol{a}$$
    y si $\boldsymbol{a} \cdot \mathbf{1'} = \mathbf{1'} \cdot \boldsymbol{a} = \boldsymbol{a}$ entonces $\mathbf{1'} = \mathbf{1}$.

- Distributividad del producto con la suma:

$$\boldsymbol{a}\cdot(\boldsymbol{b}+\boldsymbol{c})=\boldsymbol{a}\cdot\boldsymbol{b}+\boldsymbol{a}\cdot\boldsymbol{c}$$

La validez de las propiedades anteriores son consecuencias directas de la definición de clase $\boldsymbol{a}=[a]$ y de las propiedades de la suma y el producto de enteros. En efecto, tenemos:

Asociatividad de la suma

$$\begin{aligned}\boldsymbol{a}+(\boldsymbol{b}+\boldsymbol{c}) &= [a]+([b]+[c])=[a]+[b+c]=[a+(b+c)]\\ &= [(a+b)+c]=[a+b]+[c]=([a]+[b])+[c]=\boldsymbol{a}+(\boldsymbol{b}+\boldsymbol{c})\end{aligned}$$

Conmutatividad de la suma:

$$\boldsymbol{a}+\boldsymbol{b}=[a]+[b]=[a+b]=[b+a]=[b]+[a]=\boldsymbol{b}+\boldsymbol{a}$$

Asociatividad del producto:

$$\begin{aligned}\boldsymbol{a}(\boldsymbol{bc}) &= [a]\cdot([b]\cdot[c])=[a]\cdot[b\cdot c]=[a\cdot(b\cdot c)]\\ &= [(a\cdot b)\cdot c]=[a\cdot b]\cdot[c]=([a]\cdot[b])\cdot[c]=(\boldsymbol{ab})\boldsymbol{c}\end{aligned}$$

Conmutatividad del producto:

$$\boldsymbol{ab}=[a]\cdot[b]=[a\cdot b]=[b\cdot a]=[b]\cdot[a]=\boldsymbol{ba}$$

El opuesto permite definir resta de clases

$$\boldsymbol{a}-\boldsymbol{b}:=\boldsymbol{a}+(-\boldsymbol{b})$$

En la otra notación, tenemos

$$[a]-[b]=[a]+(-[b])=[a]+[-b]=[a-b]$$

es decir, la diferencia de las clases es la clase de la diferencia.

Nota. Estas propiedades son las mismas que satisfacen los enteros con la suma y el producto de enteros. A los conjuntos con 2 operaciones (llamadas suma y producto) que cumplen las propiedades de arriba se los llaman anillos (conmutativos con unidad). Luego, tanto $\mathbb{Z}$ como $\mathbb{Z}_m$ son *anillos* (conmutativos con unidad).

De las propiedades vistas, se deduce que por ejemplo valen las expresiones

$$(\boldsymbol{a}+\boldsymbol{b})^2=\boldsymbol{a}^2+2\boldsymbol{ab}+\boldsymbol{b}^2$$
$$(\boldsymbol{a}^2-\boldsymbol{b}^2)=(\boldsymbol{a}-\boldsymbol{b})(\boldsymbol{a}+\boldsymbol{b})$$

y por supuesto, las potencias mayores se definen recursivamente

$$\boldsymbol{a}^k=\boldsymbol{a}\boldsymbol{a}^{k-1}\qquad k\in\mathbb{N}$$

Hacer cuentas con suma, producto y opuestos en $\mathbb{Z}_m$ es entonces formalmente igual que hacer cuentas en $\mathbb{Z}$.

Ejemplo. Calculemos, en $\mathbb{Z}_{12}$, la siguiente expresión

$$x = \mathbf{5}^2 - 2(\mathbf{4} + \mathbf{9}) - 5(\mathbf{3} - \mathbf{7})$$

Hay muchas maneras de hacer esto. Una forma es hacer todas las cuentas y reducir modulo 12 al final:

$$x = \mathbf{25} - 2 \cdot \mathbf{13} - 5(\mathbf{-4}) = \mathbf{25} - \mathbf{26} + \mathbf{20} = \mathbf{19} = \mathbf{7}$$

Otra forma es is reduciendo en cada paso:

$$x = \mathbf{1} - 2 \cdot \mathbf{1} + \mathbf{20} = \mathbf{1} - \mathbf{2} + \mathbf{8} = \mathbf{7}$$

Una forma mas, distribuyendo todo primero y despues operando:

$$x = \mathbf{25} - \mathbf{8} - \mathbf{-18} - \mathbf{15} + \mathbf{35} = \mathbf{1} + \mathbf{4} + \mathbf{6} + \mathbf{9} - \mathbf{1} = \mathbf{7}$$

Uno trata de ir eligiendo los representantes de las clases que mas le convengan, no hay una regla fija para esto. ◊

Como lo hicimos para enteros, podemos calcular algunas sumas sencillas para enteros modulares.

Proposición 9.1. *Si p es primo, entonces*

$$\sum_{[k]\in\mathbb{Z}_p} [k] = \sum_{[k]\in\mathbb{Z}_p} [k]^2 = \sum_{[k]\in\mathbb{Z}_p} [k]^3 = 0$$

Más generalmente, para m cualquiera vale

$$\begin{aligned} \sum_{[k]\in\mathbb{Z}_m} [k] &= \begin{cases} [k] & \text{si } n = 2k \text{ es par,} \\ [0] & \text{si } m \text{ es impar.} \end{cases} \\ \sum_{[k]\in\mathbb{Z}_m} [k]^3 &= \begin{cases} [k^2] & \text{si } n = 2k \text{ es par,} \\ [0] & \text{si } m \text{ es impar.} \end{cases} \end{aligned} \tag{9.2}$$

Demostración. Usando la Proposición 5.11 y (5.9), tenemos que.. □

A pesar de que $\mathbb{Z}$ y $\mathbb{Z}_m$ son ambos anillos (con las mismas propiedades básicas), no comparten todas sus propiedades. Para empezar, los conjuntos $\mathbb{Z}_m$ son finitos. Además, ya hemos observado, por ejemplo que para algunos m en $\mathbb{Z}_m$ hay pares de números no nulos cuyo producto es 0, cosa que no acurre en $\mathbb{Z}$. En $\mathbb{Z}$ si $ab = 0$ podemos deducir que $a = 0$ ó $b = 0$; esto no es posible en $\mathbb{Z}_m$. También hemos visto que para algunos m, hay números distintos de 1 y -1 con inverso multiplicativo, cosa que tampoco ocurre en $\mathbb{Z}$.

9.4. Unidades y divisores de cero en $\mathbb{Z}_m$

Ya hemos visto que no todo elemento $[a] \in \mathbb{Z}_m$ tiene inverso (en breve veremos un criterio para saber cuando esto ocurre). Sin embargo, como es de esperar, si un entero modular es inversible, entonces su inverso es único.

En efecto, supongamos que $[a]$ es inversible y que tiene dos inversos, digamos $[a']$ y $[a'']$. O sea, $[a][a'] = [1]$ y $[a][a''] = [1]$ con $[a'], [a''] \in \mathbb{Z}_m$ y $[a'], [a''] \neq [0]$. Luego, multiplicando la primera igualdad por $[a'']$ tenemos

$$[a'']([a][a']) = ([a''][a])[a'] = [1][a'] = [a']$$

Esto también se deduce del Lema 8.19 Al inverso de $[a]$ se lo denota $[a]^{-1}$.

Esto permite definir la división en $\mathbb{Z}_m$ por elementos inversibles*. Si $[b]$ es inversible en $\mathbb{Z}_m$, entonces

$$[a]/[b] := [a] \cdot [b]^{-1}$$

Por ejemplo, $[4][7] = [1]$ en en $\mathbb{Z}_9$, y así $[7] = [4]^{-1}$.

Al conjunto de clases no nulas de $\mathbb{Z}_m$ lo denotaremos con $\mathbb{Z}_m^\times$, es decir

$$\mathbb{Z}_m^\times = \mathbb{Z}_m \setminus \{[0]\} = \{[1], [2], \ldots, [m-1]\}$$

Definición. Sea $m \in \mathbb{N}$, $m \geq 2$, y sea $[a] \in \mathbb{Z}_m^\times$. Entonces

- $[a]$ es una *unidad* si existe un $[b] \in \mathbb{Z}_m^*$ tal que $[a] \cdot [b] = [1]$.
- $[a]$ es un *divisor de cero* si existe un $[b] \in \mathbb{Z}_m^*$ tal que $[a] \cdot [b] = [0]$.

Nota. Es costumbre en álgebra, llamar unidades a elementos inversibles de un anillo (conjunto con suma y producto, como $\mathbb{Z}$ y $\mathbb{Z}_m$).

Debería quedar claro de las mismas definiciones, que estas son excluyentes entre sí. Es decir, una unidad no puede ser un divisor de cero y recíprocamente. En efecto, supogamos que $[a]$ es a la vez unidad y divisor de cero en $\mathbb{Z}_m$. Entonces, existen $[b], [c]$ no nulos en $\mathbb{Z}_m$ tales que $[a]\cdot[b] = [1]$ y $[a]\cdot[c] = [0]$. Multiplicando la segunda identidad por $[b]$ tendríamos $[c] = [b] \cdot [a] \cdot [c] = [b] \cdot [0] = [0]$, lo cual es absurdo.

Observaciones. $\mathbb{Z}$ y $\mathbb{R}$ son en cierto sentido opuestos.

(1) En $\mathbb{Z}$, todo entero resulta divisor de 0, ya que $a \cdot 0 = 0$, y sólo hay 2 unidades 1 y -1.

(2) $\mathbb{R}$ no tiene divisores de 0 no nulos y todo real no nulo es unidad.

Ejemplos.

(1) $[2]$ es divisor de cero en $\mathbb{Z}_{2m}$ para todo m, pues $[2][m] = [0]$. En particular en $\mathbb{Z}_{2^r}$ para cualquier $r \geq 2$, pues $[2][2^{r-1}] = [0]$. En general, si p es primo, $[p]$ es divisor de cero en $\mathbb{Z}_{p^r}$, $r \geq 2$.

*Un viejo profe decía que si un elemento no es inversible entonces es inservible.

(2) $[m-1]$ es unidad en $\mathbb{Z}_m$ ¡para todo m! En efecto, $[m-1]^2 = [-1]^2 = [1]$.

(3) Dado a fijo, $[a]$ es divisor de 0 en $\mathbb{Z}_{am}$ para todo m e inversible en todo $\mathbb{Z}_n$ con n coprimo con a.

Pregunta para pensar. ¿Cuándo $a^2 = 1$ en $\mathbb{Z}_m$? Es decir, ¿cuándo a es su propio inverso? Vimos que 1 y $m-1$ cumplen esto. Además, por la prueba del Teorema de Wilson, si $m = p$ es primo entonces 1 y $p-1$ son los únicos elementos con esta propiedad. ¿Qué pasa en general?

El Lema 8.19, escrito en términos de congruencias, da la condición necesaria y suficiente para la existencia de inversos módulo m. Poniendolo en términos de clases en $\mathbb{Z}_m$ tenemos lo siguiente.

Proposición 9.2. *$[a]$ en $\mathbb{Z}_m^*$ tiene inverso multiplicativo si y sólo si $(a, m) = 1$. Luego, $[a]$ es divisor de cero si y sólo si $(a, m) > 1$.*

Definición. Un conjunto A con 2 operaciones $+$ y $\cdot$ (llamadas suma y producto), con neutros 0 y 1 respectivamente, que sean asociativas, conmutativas, y que distribuyan entre sí, se dice un *anillo (conmutativo con unidad)*. A es un *cuerpo* si todo elemento no nulo de A es inversible respecto del producto, es decir, para todo $a \in A, a \neq 0$ existe $a^{-1} \in A$ tal que $aa^{-1} = 1$.

Por ejemplo, $\mathbb{Z}$, $\mathbb{Q}$ y $\mathbb{R}$ son anillos; pero $\mathbb{Z}$ no es cuerpo y $\mathbb{Q}$ y $\mathbb{R}$ si lo son. Los enteros modulares $\mathbb{Z}_m$ son otro ejemplo de anillo. Nos preguntamos si existen m para los cuales $\mathbb{Z}_m$ resulte un cuerpo. Es decir, ¿existe m tal que todo $[a] \in \mathbb{Z}_m$ no nulo tiene inverso $[a]^{-1}$?

Es claro que si m no es primo, digamos $m = kn$ entonces $[k][n] = [m] = [0]$. Luego, $[k]$ y $[n]$ son divisores de 0, y por lo tanto no son unidades. Es decir, si m no es primo, $\mathbb{Z}_m$ no puede ser un cuerpo. La Proposición anterior nos da la respuesta.

Corolario 9.3. *$\mathbb{Z}_p$ es cuerpo si y sólo si p es primo.*

Nota. Esto dice que existen cuerpos finitos. Conjuntos finitos con sumas y productos, donde se puede dividir por todo elemento no nulo. Existen otros cuerpos finitos, muchos mas además de los $\mathbb{Z}_p$ con p primo. De hecho, para cada primo p y cada $k \geq 1$ existe un cuerpo finito con $q = p^k$ elementos. Estos cuerpos se denotan $\mathbb{F}_q$.

Ejemplo. Sea

$$\mathbb{F}_4 = \{0, 1, \omega, \omega^2\}$$

donde ω es una raíz del polinomio $x^2 + x + 1$, o sea $\omega = e^{\frac{2\pi i}{3}} \in \mathbb{C}$. Definamos la suma y el producto en $\mathbb{F}_4$ mediante las siguientes tablas

$+$	0	1	ω	ω^2
0	0	1	ω	ω^2
1	1	1	ω	ω^2
ω	ω	ω^2	0	1
ω^2	ω^2	ω	1	0

$\cdot$	0	1	ω	ω^2
0	0	0	0	0
1	0	1	ω	ω^2
ω	0	ω	ω^2	1
ω^2	0	ω^2	1	ω

El lector puede chequear que las operaciones están bien definidas, satisfacen las propiedades asociativa, conmutativa y distributiva, y además, todo elemento no nulo tiene inverso. Luego $\mathbb{F}_4$ es un cuerpo. Como se construye en general un cuerpo de p^k elementos está mas allá del alcance de este libro. ◊

Como calcular inversos

Si $(a, m) = 1$ sabemos que $[a]$ tiene inverso en $\mathbb{Z}_m$, pero ¿quién es $[a]^{-1}$? Veamos algunas formas de calcularlo.

- INSPECCIÓN: Vamos probando los productos $[a][2]$, $[a][3]$, $[a][4]$, hasta que eventualmente, $[a][b] = 1$. Luego $[b] = [a]^{-1}$. Por ejemplo, busquemos el inverso de 5 en $\mathbb{Z}_{12}$. $[5][2] = [10]$, $[5][3] = [3]$, $[5][4] = [8]$, $[5][5] = 1$. Luego $[5]^{-1} = [5]$.
- TABLAS: si tenemos la tabla del producto a disposición, por ejemplo para m pequeños, entonces es automático. En la fila de a buscamos el 1 en dicha fila. Luego, el número que etiqueta la columna (digamos b) es el inverso de a, pues $[a][b] = [1]$. Por ejemplo, el inverso de $[2]$ en $\mathbb{Z}_9$ es $[5]$.
- POTENCIAS: vamos calculando las potencias de $[a]$, o sea $[a^2], [a^3], [a^4], \ldots$ hasta que $[a^k] = [1]$ para algún k. Luego $[a^{k-1}] = [a]^{-1}$. Rehagamos los ejemplos anteriores. En $\mathbb{Z}_{12}$, $[5^2] = [1]$ y así $[5]^{-1} = [5]$. En $\mathbb{Z}_9$, $[2^2] = [4]$, $[2^3] = [8]$, $[2^4] = [7]$, $[2^5] = [5]$, $[2^6] = [1]$. Luego, $[2]^{-1} = [2^5] = [5]$.
- EULER-FERMAT: El Teorema 8.24, de Euler-Fermat, nos da una potencia k tal que $[a^k] = [a]^{-1}$. En efecto, como $a^{\varphi(m)} \equiv 1 \pmod{m}$, entonces $[a][a^{\varphi(m)-1}] = [1]$ en $\mathbb{Z}_m$. O sea,

  $$[a^{\varphi(m)-1}] = [a]^{-1}$$

  ($k = \varphi(m) - 1$). Por ejemplo, en $\mathbb{Z}_{12}$, $[5^{\varphi(12)-1}] = [5^3] = [5^2][5] = [5]$ es el inverso de $[5]$. Notar que la potencia k que da este método no tiene que ser la menor, pero al menos sólo se hace una sola cuenta (no como en el caso anterior en que uno no sabe quien será el k y debe ir calculando todas las potencias previas).

La ventaja de usar Euler-Fermat para el cálculo de inversos es que el mismo exponente sirve para todos los inversibles en $\mathbb{Z}_m$. Es decir, supongamos que $\mathbb{Z}_m^* = \{[a_1], [a_2], \ldots, [a_{\varphi(m)}]\}$ entonces

$$[a_i]^{-1} = [a_i^{\phi(m)-1}] \qquad 1 \le i \le \varphi(m)$$

9.4.1. El grupo de unidades $\mathbb{Z}_m^*$

El conjunto de unidades se denota por $\mathcal{U}(\mathbb{Z}_m)$ o bien por $\mathbb{Z}_m^*$. Luego, tenemos

$$\mathbb{Z}_m^* = \{[a] : 0 \le a < m, (a, m) = 1\}$$

De aquí es claro que

$$\#\mathbb{Z}_m^* = \varphi(m)$$

Este conjunto es *cerrado* por el producto (aunque no por la suma). Es decir, producto de unidades es unidad, pero suma de unidades en general no es unidad. En efecto, supongamos que $a, b \in \mathbb{Z}_m^*$. El inverso de $[a][b]$ es $[a^{-1}b^{-1}]$ pues

$$[a][b][a^{-1}b^{-1}] = [a][b][b]^{-1}[a]^{-1} = [a][a]^{-1}$$

Es decir, el inverso del producto es el producto de los inversos. Se dice que $(\mathbb{Z}_m^*, \cdot)$ es un grupo multiplicativo y se habla entonces del grupo de unidades.

Por simpleza, en lo que sigue escribiremos a en lugar de $[a]$.

Observaciones.

(1) Es claro que si p es primo,

$$\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$$

(2) Si $m = 2^r$ entonces las unidades de $\mathbb{Z}_m$ son todos los impares. Es decir,

$$\mathbb{Z}_{2^r}^* = \{1, 3, 5, \ldots, 2^r - 3, 2^r - 1\}$$

para todo $r \geq 2$.

Calculemos los grupos de unidades de $\mathbb{Z}_m$ para m pequeños. Aquí damos $\mathbb{Z}_m^*$ para los m no primos menores que 20 y algunos ejemplos mas grandes.

m	$\mathbb{Z}_m^*$	$\varphi(m)$
4	$\{1, 3\}$	2
6	$\{1, 5\}$	2
8	$\{1, 3, 5, 7\}$	4
9	$\{1, 2, 4, 5, 7, 8\}$	6
10	$\{1, 3, 7, 9\}$	4
12	$\{1, 5, 7, 11\}$	4
14	$\{1, 3, 5, 9, 11, 13\}$	6
15	$\{1, 2, 4, 7, 8, 11, 13, 14\}$	8
16	$\{1, 3, 5, 7, 9, 11, 13, 15\}$	8
18	$\{1, 5, 7, 11, 13, 17\}$	6
20	$\{1, 3, 7, 9, 11, 13, 17, 19\}$	8

TABLAS DE MULTIPLICAR EN $\mathcal{U}(\mathbb{Z}_m)$

$(\mathbb{Z}_4^*, \cdot)$	**1**	**3**
1	**1**	**3**
3	**3**	**1**

$(\mathbb{Z}_6^*, \cdot)$	**1**	**5**
1	**1**	**5**
5	**5**	**1**

$(\mathbb{Z}_8^*, \cdot)$	**1**	**3**	**5**	**7**
1	**1**	**3**	**5**	**7**
3	**3**	**1**	**7**	**5**
5	**5**	**7**	**1**	**3**
7	**7**	**5**	**3**	**1**

$(\mathbb{Z}_{10}^*, \cdot)$	**1**	**3**	**7**	**9**
1	**1**	**3**	**7**	**9**
3	**3**	**9**	**1**	**7**
7	**7**	**1**	**9**	**3**
9	**9**	**7**	**3**	**1**

$(\mathbb{Z}_{12}^*, \cdot)$	**1**	**5**	**7**	**11**
1	**1**	**5**	**7**	**11**
5	**5**	**1**	**11**	**7**
7	**7**	**11**	**1**	**5**
11	**11**	**7**	**5**	**1**

$(\mathbb{Z}_9^*, \cdot)$	**1**	**2**	**4**	**5**	**7**	**8**
1	**1**	**2**	**4**	**5**	**7**	**8**
2	**2**	**4**	**8**	**1**	**5**	**7**
4	**4**	**8**	**7**	**2**	**1**	**5**
5	**5**	**1**	**2**	**7**	**8**	**4**
7	**7**	**5**	**1**	**8**	**4**	**2**
8	**8**	**7**	**5**	**4**	**2**	**1**

$(\mathbb{Z}_{14}^*, \cdot)$	**1**	**3**	**5**	**9**	**11**	**13**
1	**1**	**3**	**5**	**9**	**11**	**13**
3	**3**	**9**	**1**	**13**	**5**	**11**
5	**5**	**1**	**11**	**3**	**13**	**9**
9	**9**	**13**	**3**	**11**	**1**	**5**
11	**11**	**5**	**13**	**1**	**9**	**3**
13	**13**	**11**	**9**	**5**	**3**	**1**

$(\mathbb{Z}_{15}^*, \cdot)$	**1**	**2**	**4**	**7**	**8**	**11**	**13**	**14**
1	**1**	**2**	**4**	**7**	**8**	**11**	**13**	**14**
2	**2**	**4**	**8**	**14**	**1**	**7**	**11**	**13**
4	**4**	**8**	**1**	**13**	**2**	**14**	**7**	**11**
7	**7**	**14**	**13**	**4**	**11**	**2**	**1**	**8**
8	**8**	**1**	**2**	**11**	**4**	**13**	**14**	**7**
11	**11**	**7**	**14**	**2**	**13**	**1**	**8**	**4**
13	**13**	**11**	**7**	**1**	**14**	**8**	**4**	**2**
14	**14**	**13**	**11**	**8**	**7**	**4**	**2**	**1**

$(\mathbb{Z}_{16}^*, \cdot)$	**1**	**3**	**5**	**7**	**9**	**11**	**13**	**15**
1	**1**	**3**	**5**	**7**	**9**	**11**	**13**	**15**
3	**3**	**9**	**15**	**5**	**11**	**1**	**7**	**13**
5	**5**	**15**	**9**	**3**	**13**	**7**	**1**	**11**
7	**7**	**5**	**3**	**1**	**15**	**13**	**11**	**9**
9	**9**	**11**	**13**	**15**	**1**	**3**	**5**	**7**
11	**11**	**1**	**7**	**13**	**3**	**9**	**15**	**5**
13	**13**	**7**	**1**	**11**	**5**	**15**	**9**	**3**
15	**15**	**13**	**11**	**9**	**7**	**5**	**3**	**1**

$(\mathbb{Z}_{18}^*, \cdot)$	**1**	**5**	**7**	**11**	**13**	**17**
1	**1**	**5**	**7**	**11**	**13**	**17**
5	**5**	**7**	**17**	**1**	**11**	**13**
7	**7**	**17**	**13**	**5**	**1**	**11**
11	**11**	**1**	**5**	**13**	**17**	**7**
13	**13**	**11**	**1**	**17**	**7**	**5**
17	**17**	**13**	**11**	**7**	**5**	**1**

$(\mathbb{Z}_{20}^*, \cdot)$	**1**	**3**	**7**	**9**	**11**	**13**	**17**	**19**
1	**1**	**3**	**7**	**9**	**11**	**13**	**17**	**19**
3	**3**	**9**	**1**	**7**	**13**	**19**	**11**	**17**
7	**7**	**1**	**9**	**3**	**17**	**11**	**19**	**13**
9	**9**	**7**	**3**	**1**	**19**	**17**	**13**	**11**
11	**11**	**13**	**17**	**19**	**1**	**3**	**7**	**9**
13	**13**	**19**	**11**	**17**	**3**	**9**	**1**	**7**
17	**17**	**11**	**19**	**13**	**7**	**1**	**9**	**3**
19	**19**	**17**	**13**	**11**	**9**	**7**	**3**	**1**

Ejemplo. Como $60 = 2^2 \cdot 3 \cdot 5$ tenemos $\varphi(60) = 2 \cdot 2 \cdot 4 = 16$. Luego $\#\mathbb{Z}_{60}^* = 16$ y

$$\mathbb{Z}_{60}^* = \{1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 37, 41, 43, 47, 59\}$$

9.5. Ejercicios

a

Capítulo 10

Ecuaciones en congruencias

Dado un polinomio $f(x)$ con coeficientes enteros consideramos la ecuación módulo m

$$f(x) \equiv 0 \mod m. \tag{10.1}$$

Una solución es un entero x_0 tal que el entero $f(x_0)$ que resulta de evaluar el polinomio $f(x)$ en x_0, satisface que $f(x_0) \equiv 0\ (m)$.

Dado que si $x_0 \equiv y_0$, entonces $f(x_0) \equiv f(y_0)$, se sigue que si (10.1) tiene una solución, tiene infinitas. Convenimos en que si x_0 e y_0 son soluciones y $x_0 \equiv y_0$, entonces las consideramos como una solo solución. Así resolver la ecuación (10.1) es encontrar todas sus soluciones en un conjunto de representantes módulo m, como por ejemplo $\{0, 1, 2, \ldots, m-1\}$.

Ejemplos.

(1) La ecuación $2x \equiv 3\ (4)$ o equivalentemente $2x - 3 \equiv 0\ (4)$, no tiene ninguna solución. $2x - 3$ es siempre un número impar, luego nunca es divisible por 4.

(2) La ecuación $x^2 \equiv 1\ (8)$ tiene exactamente 4 soluciones.

La clase más simple de ecuaciones de este tipo, son las *ecuaciones lineales* de congrueencia, aquellas donde el polinomio $f(x)$ es de grado 1, es decir $f(x) = ax + b'$, que da lugar a la ecuación $ax + b' \equiv 0$ o equivalentemente a la ecuaicón

$$ax \equiv b \mod m,$$

donde $b = -b'$.

10.1. Ecuaciones lineales

10.1.1. Una variable

Mostraremos que éstas siempre se pueden resolver, es decir siempre podemos decidir si tienen o no solución y en caso afirmativo decir cuántas. Antes de hacer esto enunciamos y probamos algunas propiedades más de la congruencia de enteros.

Proposición 10.1. *Si* $a \equiv b \mod m$, *entonces* $\mcd(a,m) = \mcd(b,m)$.

Demostración. Sean $d = (a,m)$ y $e = (b,m)$. Como $m \mid a-b$, y $d \mid a$ y $d \mid m$, entonces $d \mid b$. Luego $d \mid e$. Análogamente, se sigue que $e \mid d$ y por lo tanto $d = e$. □

Proposición 10.2 (Propiedad cancelativa)**.** *Si* $ac \equiv bc \mod m$ *y* $d = (m,c)$, *entonces*

$$a \equiv b \mod \frac{m}{d}.$$

En particular si $(m,c) = 1$, *resulta que* $a \equiv b \mod m$.

Demostración. Tenemos que $m \mid c(a-b)$; luego $\frac{m}{d} \mid \frac{c}{d}(a-b)$. Ahora, como $\frac{m}{d}$ y $\frac{c}{d}$ son coprimos, se sigue que $\frac{m}{d} \mid (a-b)$. □

Proposición 10.3. *Si* $a \equiv b \mod m$, $a \equiv b \mod n$ *y* $(m.n) = 1$, *entonces* $a \equiv b \mod mn$.

Demostración. Tanto m como n dividen a la diferecnia $a-b$; siendo m y n coprimos se sigue que el producto mn divide a $a-b$. □

Proposición 10.4. *Si* $d \mid a$, $d \mid b$ *y* $d \mid m$, *entonces la ecuación* $ax \equiv b \mod m$ *tiene solución si y sólo si la ecuación* $\frac{a}{d}x \equiv \frac{b}{d} \mod \frac{m}{d}$ *tiene solución.*

Demostración. Supongamos que existe c tal $ac \equiv b \mod m$, esto es $m \mid ac-b$. Luego $\frac{m}{d} \mid \frac{ac-b}{d} = \frac{a}{d}c - \frac{b}{d}$. Es decir c satisface que $\frac{a}{d}c \equiv \frac{b}{d} \mod \frac{m}{d}$.

Recíprocamente, si c es tal que $\frac{a}{d}c \equiv \frac{b}{d} \mod \frac{m}{d}$, entonces $\frac{m}{d} \mid \frac{a}{d}c - \frac{b}{d} = \frac{ac-b}{d}$, de donde se sigue que $m \mid ac-b$, es decir $ac \equiv b \mod m$. □

....

Teorema 10.5. *Consideremos la ecuación lineal de congruencia*

$$ax \equiv b \mod m. \tag{10.2}$$

(a) Si $(a,m) = 1$, *entonces la ecuación (10.2) tiene una única solución.*

(b) Si $(a,m) = d$, *entonces la ecuación (10.2) tiene solución si y sólo si* $d \mid b$. *Si* $(a,m) = d$ *y* $d \mid b$, *entonces la ecuación (10.2) tiene exactamente* d *soluciones; éstas son:*

$$t, t + \frac{m}{d}, t + 2\frac{m}{d}, \ldots, t + (d-1)\frac{m}{d}$$

donde t *es la única solución de la ecuación*

$$\frac{a}{d}x \equiv \frac{b}{d} \mod \frac{m}{d}.$$

Demostración. (a) Como a y m son coprimos, entonces $a, 2a, 3a, \ldots, ma$ son todos no congruentes dos a dos módulo m. Así son un conjunto de representates de todas las clases de congruencia módulo m. Luego $b \equiv ia$ para un único $1 \leq i \leq m$.

(b) Si hay una solución x_0, $m \mid ax_0 - b$. Como $d \mid a$ y $d \mid m$, entonces $d \mid b$. Recíprocamente, si $d \mid b$ consideramos la ecuación $\frac{a}{d}x \equiv \frac{b}{d} \mod \frac{m}{d}$. Como $\frac{a}{d}$ y $\frac{b}{d}$ son coprimos, ésta última ecuación tiene solución x_0. Ahora x_0 es también solución de la original.

(c) Los d números enteros de la forma $t + i\frac{m}{d}$ con $i = 0 \dots d-1$ son claramente soluciones de la última ecuación (que por convención consideramos iguales como soluciones de la ecuación de congruencia por ser equivalentes módulo $\frac{m}{d}$). Luego todos éstos son también soluciones de la ecuación (10.2). Pero ahora son todos no equivalentes módulo m, pues si $m \mid t + i\frac{m}{d} - t - j\frac{m}{d}$, entonces $m \mid (i-j)\frac{m}{d}$ y luego $d \mid (i-j)$, lo que implica que $i = j$. Tenemos así d soluciones distintas de la ecuación (10.2).

Por otro lado si x_0 es solución de (10.2), entonces $ax_0 \equiv b \equiv at \mod m$, y luego $x_0 \equiv t \mod \frac{m}{d}$. Es decir $x_0 = t + k\frac{m}{d}$. Pero $k \equiv r \mod d$, para algún $0 \leq r < d$. Se sigue que $km \equiv rm \mod dm$ y por lo tanto $k\frac{m}{d} \equiv r\frac{m}{d} \mod m$. Finalmente, tenemos que $x_0 \equiv t + r\frac{m}{d} \mod m$, y resulta que x_0 es una de las soluciones anteriores, mostrando que esas son todas.

□

Observación. Notar que la existencia y unicidad de una solución en el caso en que $(a, m) = 1$, se sigue también directamente de la existencia de un inverso multiplicativo para a en $\mathbb{Z}_m$. En efecto, si c es tal que $ac \equiv 1$, entonces $acb \equiv b$. Desde otro punto de vista, $ax \equiv b$ implica, multiplicando por c, que $x \equiv cb$. Este el mismo argumento que usamos para resolver las ecuaciones lineales en $\mathbb{R}$.

10.1.2. 2 y 3 variables

10.2. El teorema chino del resto

a

10.3. Sistemas de ecuaciones lineales

a

10.4. Ejercicios

a

Parte IV

Combinatoria

Capítulo 11

Principios de conteo

"Hay 3 clases de personas, las que saben contar y las que no"

"No todo lo que puede ser contado cuenta y no todo lo que cuenta puede ser contado"
Albert Einstein, físico alemán (1879 – 1955)

Si le preguntáramos a un nene pequeño cuántos asientos hay en un cine, es posible que este comience a contarlos uno por uno. Si el niño es algo mayor es probable que cuente solo el número de filas, n, y el número de asientos por filas, m, y que deduzca que el número de asientos es nm.

Muchos problemas en matemática involucran "contar" objetos de alguna clase o con ciertas propiedades determinadas. Algunas preguntas que surgen naturalmente son:

- ¿De cuántas formas se puede realizar una determinada acción?
- ¿Cuántos elementos tiene un cierto conjunto?
- ¿Cuántos subconjuntos con ciertas propiedades se pueden obtener a partir de un conjunto dado?
- ¿De cuántas formas se pueden elegir ciertos elementos de un conjunto?
- ¿De cuántas formas se pueden ordenar estos elementos?
- ¿De cuántas formas se pueden clasificar objetos dados en categorías? o equivalentemente, ¿cuántas formas se pueden distribuir bolas en cajas?

Queremos estudiar modos sistemáticos y prácticos de contar, como el usado en el caso del cine, según distintas situaciones particulares bastante comunes que se dan en la realidad.

El arte de contar sin enumerar, es decir de calcular el número de casos que nos interesa sin hacer una lista concreta, es una parte central de la combinatoria. Ésta es un area de la matemática que ha tenido un gran desarrollo en el siglo pasado y que interactua con otras muchas áreas de la matemática como por ejemplo la matemática discreta, la teoría

de grafos, la geometría finita, la teoría de códigos y también fuertemente con la ciencia de la computación.

Comenzaremos aprendiendo herramientas e intentando desarrollar habilidades de conteo, intuitivamente y a través de ejemplos. Mas adelante, en el Capítulo **??**, veremos los fundamentos rigurosos que sustentan lo anterior.

A continuación damos un breve resumen de lo que aprenderemos en este capítulo y los siguientes.

ASPECTOS COMBINATORIOS

- PRINCIPIOS COMBINATORIOS: de adición, de multiplicación, del complemento, de la inyección y la biyección, del palomar y de inclusión/exclusión.
- ACCIONES COMBINATORIAS: "elegir", "ordenar" y "distribuir" objetos de cierta manera (permutaciones, combinaciones y arreglos, selecciones con y sin repetición, distribuciones).
- NÚMEROS COMBINATORIOS. Binomio de Newton e identidades combinatorias con coeficientes binomiales. Otros números que sirven para contar.

En este capítulo, daremos algunos métodos de conteo que sirvan para responder las preguntas planteadas más arriba, en una gran variedad de casos. Veremos algunos principios básicos de conteo, pero que son de amplia aplicación.

11.1. Principios básicos de conteo

Describimos a continuación 3 principios básicos que son muy naturales y por lo tanto fáciles de incorporar. Estos son:

- *Principio de adición.*
- *Principio de multiplicación.*
- *Principio del complemento.*

Muchas de las estrategias para contar una determinda clase de objetos consiste en combinar de alguna manera estos 3 principios con alguno de estos dos:

- *Principio de inyección.*
- *Principio de biyección.*

Presentamos a continuación dichos principios sin pruebas. Más adelante daremos las demostraciones formales de todos estos hechos.

11.1.1. El principio de adición

Este principio afirma lo siguiente.

PRINCIPIO DE ADICIÓN (**PA**). *Si una acción A se puede realizar de n formas distintas y otra acción B se puede realizar de m formas distintas, siendo A y B excluyentes (si se hace A no se hace B y vicecersa), entonces la cantidad de formas posibles de realizar la acción A ó B es $n+m$.*

Ejemplo. Quiero ver una película. En la tele hay 8 canales de películas y en el complejo de cines cerca de casa hay 5 películas en cartelera. ¿Cuántas películas tengo para elegir? Hay en total 8+5=13 películas para elegir. ◊

Formalmente, en términos de conjuntos, este principio se enuncia como sigue.

PRINCIPIO DE ADICIÓN II (**PA**). *Si A y B son conjuntos finitos disjuntos, entonces*

$$|A \cup B| = |A| + |B|$$

En el caso de 3 acciones mutuamente excluyentes el principio queda así. Si A, B y C son conjuntos mutuamente disjuntos (o disjuntos 2 a 2), es decir $A \cap B = \varnothing$, $B \cap C = \varnothing$ y $C \cap A = \varnothing$, entonces

$$|A \cup B \cup C| = |A| + |B| + |C|$$

Ejemplos. (turísticos)

(1) Quiero viajar de Córdoba a Buenos Aires. Considerando distintos horarios, rutas y empresas hay 3 formas de viajar en avión, 5 formas de ir en colectivo y 2 formas de ir en tren. Como cada medio de transporte es excluyente, hay $3+5+2=10$ formas de viajar.

(2) En un bar, quiero comer algo dulce. Hay helados (casatta, almendrado, bombón escocés y bombón suizo) y tortas (tiramisú, selva negra, imperial ruso). Luego, tengo $4+3=7$ opciones. ◊

Más generalemente, tenemos.

Teorema 11.1 (PA). *Si $A_1, A_2, \ldots, A_n$ son conjuntos disjuntos 2 a 2, o sea $A_i \cap A_j = \varnothing$ para todo $1 \leq i, j \leq n$ con $i \neq j$, entonces*

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = |A_1| + |A_2| + \cdots + |A_n|$$

Como una aplicación mas interesante veamos el siguiente ejemplo.

Ejemplo. Encontrar el número de pares de enteros (x, y) tales que $x^2 + y^2 \leq 4$. Queremos calcular en cardinal del conjunto

$$A = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} : x^2 + y^2 \leq 4\}$$

Dividimos el problema en casos disjuntos; o sea, queremos encontrar los pares de enteros (x, y) tal que $x^2 + y^2 = i$ con $i = 0, 1, 2, 3, 4$. Es decir,

$$A = \bigcup_{i=0}^{4} A_i \qquad \text{donde} \qquad A_i = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} : x^2 + y^2 = i\}.$$

Calculando, tenemos

$$A_0 = \{(0, 0)\} \qquad A_1 = \{(\pm 1, 0), (0, \pm 1)\}$$
$$A_2 = \{(1, \pm 1), (-1, \pm 1)\} \qquad A_3 = \varnothing \qquad A_4 = \{(\pm 2, 0), (0, \pm 2)\}$$

Luego, por el principio de adición,

$$|A| = \sum_{i=0}^{4} |A_i| = 1 + 4 + 4 + 0 + 4 = 13$$

Es decir, hay 13 pares de enteros cuyos cuadrados suman 4 o menos. ◊

11.1.2. El principio de multiplicación

Este principio dice que

> Principio de multiplicación (**PM**). *Si una acción A se puede realizar de n formas distintas y una acción B se puede realizar de m formas distintas, siendo A y B acciones independientes, entonces la cantidad de formas de realizar la acción A y B es nm.*

Ejemplos. (turísticos)

(1) Supongamos que queremos viajar de Salta a Mar del Plata, pasando por Tucumán y Córdoba. Si hay 3 formas de ir de Salta a Tucumán, 2 formas de ir de Tucumán a Córdoba y 3 formas de ir de Córdoba a Mar del Plata. ¿Cuántas formas hay de ir de Salta a Mar del Plata?

Aplicamos el principio de multiplicación 2 veces. Como las formas de viajar de Salta a Tucumán y de Tucumán a Córdoba son independientes, es decir la eleccion de la primera no determina para nada la elección de la segunda, entonces, por **PM** hay $3 \cdot 2 = 6$ formas de ir de Salta a Córdoba, pasando por Tucumán. Ahora, por **PM** nuevamente, hay $6 \cdot 4 = 24$ formas de ir de Salta a Mar del Plata pasando por Córdoba.

(2) En un restaurante quiero pedir un almuerzo con entrada, plato y postre. De entradas hay empanadas, humita o sopa. De plato principal hay locro, ravioles o milanesas. De postre hay flan, budín de pan o vigilante. Por el **PM** (aplicado 2 veces) hay $3 \cdot 3 \cdot 3 = 27$ menúes posibles, i.e. combinaciones de entradas, platos y postres. ◊

Veamos un ejemplo en el que el **PM** no se aplica.

Ejemplo. Nos preguntamos de cuántas formas podemos obtener suma 7 al tirar 2 dados. Si representamos la tirada por el par

$$(x, y) \quad \text{donde} \quad 1 \leq x, y \leq 6,$$

nos preguntamos cuantos pares hay que cumplan

$$x + y = 7$$

Ahora los eventos "que el primer dado salga x" y "que el segundo dado salga y" no son independientes, ya que si suman 7, el valor del segundo dado depende del primero, $y = 7 - x$ (y recíprocamente). Está claro que aquí no se aplica el **PM**. Como hay 6 posibles valores para x, hay 6 pares posibles $(1, 6), (2, 5), (3, 4), (4, 3), (5, 2), (6, 1)$. ◊

En términos de conjuntos, este principio se enuncia como sigue.

Principio de multiplicación II (**PM**). *Si A y B son conjuntos finitos, entonces*

$$|A \times B| = |A| \cdot |B|$$

Ejemplo. En el caso del menú del ejemplo anterior, tenemos $E = \{e, h, s\}$, $P = \{l, m, r\}$ y $C = \{b, f, v\}$. Luego,

$$E \times C = \{(e, l), (e, m), (e, r), (h, l), (h, m), (h, r), (s, l), (s, m), (s, r)\}$$

e identificando $(E \times C) \times P$ con $E \times C \times P$, vemos que

$$\begin{aligned}
&(e, l, b), (e, m, b), (e, r, b), (h, l, b), (h, m, b), (h, r, b), (s, l, b), (s, m, b), (s, r, b),\\
&(e, l, f), (e, m, f), (e, r, f), (h, l, f), (h, m, f), (h, r, f), (s, l, f), (s, m, f), (s, r, f),\\
&(e, l, v), (e, m, v), (e, r, v), (h, l, v), (h, m, v), (h, r, v), (s, l, v), (s, m, v), (s, r, v),
\end{aligned}$$

son todos los posibles menúes. ◊

Más generalemente, para cualquier número de conjuntos tenemos.

Teorema 11.2 (PM). *Si $A_1, A_2, \ldots, A_n$ son conjuntos entonces*

$$|A_1 \times A_2 \times \cdots \times A_n| = |A_1| \cdot |A_2| \cdots |A_n|$$

Ejemplo. Calcular el número máximo posible de patentes viejas y de patentes nuevas de los autos.

Las patentes viejas (anteriores a las actuales, hubieron otras antes) eran de la forma

$$X\, a_1 a_2 a_3 a_4 a_5 a_6$$

con X una letra (una por cada provincia incluyendo la capital) y los a_i dígitos. Es decir, $X \in \mathcal{A} = \{\text{A, B, C, } \ldots, \text{X, Y, Z}\} \setminus \{\text{I, Ñ, O}\}$ y $a_i \in \mathcal{D} = \{0, 1, \ldots, 8, 9\}$ para $i = 1, \ldots, 6$. Por la cantidad de autos, había dos casos especiales: Buenos Aires, con letra B, permitía un

(a) antigua

(b) nueva

Figura 11.1: patentes de automóviles argentinas

digito más a_0, con $0 \leq a_0 \leq 2$; y Capital Federal, con letra C, permitía un dígito a_0 más con $0 \leq a_0 \leq 1$.

Las patentes nuevas son de la forma

$$XYZ\,abc$$

con X, Y, Z letras en $\mathcal{A}$ y a, b, c dígitos.

Por el **PM**, el número total de patentes viejas posibles, que no son de Buenos Aires o Capital Federal, es

$$|(\mathcal{L} \smallsetminus \{B, C\}) \times (\mathcal{D} \times \mathcal{D} \times \mathcal{D} \times \mathcal{D} \times \mathcal{D} \times \mathcal{D})| = |\mathcal{L} \smallsetminus \{B, C\}| \times |\mathcal{D}|^6 = 22 \cdot 10^6 = 22.000.000$$

Si a esto le sumamos las $3.000.000$ de patentes de Buenos Aires mas los $2.000.000$ de patentes de Capital, esto da un total de $27.000.000$ de patentes.

Por otro lado, el número total de patentes nuevas posibles es

$$|(\mathcal{L} \times \mathcal{L} \times \mathcal{L}) \times (\mathcal{D} \times \mathcal{D} \times \mathcal{D})| = |\mathcal{L}|^3 \times |\mathcal{D}|^3 = 27^3 \cdot 10^3 = 19.683.000.$$

Sí, parece que hay menos que antes...* ◊

En muchos problemas (por lo general), ambos principios **PA** y **PM** deben ser usados conjuntamente para resolver un problema.

Ejemplo. Sea $X = \{1, 2, 3, \ldots, 9, 10\}$. Calcular el número de elementos del conjunto

$$S = \{(a, b, c) \ : \ a, b, c \in X,\ a < b,\ a < c\}$$

Para cada $a = k \in \{1, 2, \ldots, 9\}$ hay $10 - k$ elecciones para b y $10 - k$ elecciones para c. Luego, por **PM**, para cada k hay $(10 - k)^2$ elecciones para (k, b, c) con $k < b$, $k < c$. Ahora, como k toma los valores $1, 2, \ldots, 9$, por el **PA** tenemos

$$|S| = 9^2 + 8^2 + \cdots + 2^2 + 1^2.$$

Ya vimos como calcular esta suma de cuadrados en (5.8):

$$|S| = \sum_{k=1}^{n=9} k^2 = \tfrac{1}{6} n(n+1)(2n+1) = \tfrac{9 \cdot 10 \cdot 19}{6} = 185$$

Luego hay 185 ternas de dígitos, tales que el segundo y el tercero son ambos menores que el primero. ◊

*Este es un ejemplo trivial que muestra la falta que hacen los matemáticos en empresas y gobiernos.

Veamos la prueba del Corolario 6.29 que nos quedó pendiente.

Ejemplo (número de divisores de n)**.** Supongamos que $n = p_1^{i_1} \dots p_r^{i_r}$ es la factorización prima de n, donde $p_1, \dots, p_r$ son todos primos distintos y $i_1, \dots, i_r > 0$. En la Proposición 6.27 vimos que

$$\operatorname{Div}(n) = \{\pm p_1^{j_1} \cdots p_r^{j_r} : 0 \leq j_k \leq i_k, k = 1, \dots, r\}$$

Veamos que n tiene exactamente $2(i_1 + 1)(i_2 + 1) \dots (i_r + 1)$ divisores.

Para cada $1 \leq j \leq r$, sea $D_j = \operatorname{Div}^+(p_j^{i_j})$ el conjunto de divisores positivos de $p_j^{i_j}$. Notar que hay una biyección

$$\operatorname{Div}^+(n) \longleftrightarrow D_1 \times D_2 \times \cdots \times D_r$$

dada por

$$p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r} \longleftrightarrow (p_1^{e_1}, p_2^{e_2}, \dots, p_r^{e_r})$$

Luego, como $D_j = \{1, p_j, p_j^2, \dots, p_j^{i_j}\}$, por el **PM** se tiene que

$$|\operatorname{Div}^+(n)| = |D_1| \cdot |D_2| \cdots |D_r| = (i_1 + 1)(i_2 + 1) \cdots (i_r + 1)$$

Ahora, como $\operatorname{Div}(n) = \operatorname{Div}^+(n) \cup \operatorname{Div}^-(n)$ (unión disjunta), y $\#\operatorname{Div}^+(n) = \#\operatorname{Div}^-(n)$, por el **PA** y el ejemplo de más arriba tenemos

$$\#\operatorname{Div}(n) = 2\#\operatorname{Div}^+(n) = 2(i_1 + 1)(i_2 + 1) \cdots (i_r + 1)$$

como queríamos ver. ◊

11.1.3. El principio del complemento

Supongamos que queremos contar la cantidad de formas en que se puede realizar cierta acción (casos favorables). A veces es más fácil contar los casos en que no pasa lo que queremos (casos no favorables) y restarlos del total de casos posibles. Esto criterio tan sencillo se conoce como principio del complemento.

> Principio del complemento (**PC**). *Supongamos que hay n formas de realizar una determinada acción A y, de éstas, hay exactamente k que no cumplen con una propiedad P dada. Entonces, la cantidad de formas de realizar la acción A cumpliendo con la propiedad P es $n - k$.*

Típicamente, a este principio se lo usa cuando los casos que queremos contar, son evidentemente muchos comparados con el total de casos posibles. En ese caso conviene contar los casos que no nos interesan y restarlos del total.

Ejemplo (Dados)**.** Supongamos que se tiran 2 dados distintos (es decir que los podemos distinguir, digamos uno blanco y otro negro) obteniedo el par (x, y) con $1 \leq x, y \leq 6$, donde x representa el dado blanco e y el negro. Por ejemplo ⚀⚄ $= (2, 5)$. Notar que $(x, y) \neq (y, x)$.

¿Cuántos pares se pueden obtener que no sean "dobles"? Está claro que podemos enumerarlos a todos $(1,2),(1,3),\ldots,(1,6),(2,1),(2,3),\ldots,(2,6)$, etcétera. Pero lo más simple es contar el número de dobles (lo que no queremos) y restarlos del total. Hay 6 pares dobles

Por el **PM**, el número total de pares es $6 \cdot 6 = 36$. Luego, por el **PC** hay $36 - 6 = 30$ pares que no son dobles. ◊

En términos de conjuntos, este principio se enuncia como sigue.

Teorema 11.3 (PC). *Si $A \subseteq \mathcal{U}$ con $|\mathcal{U}| = n$ entonces $|A| = n - |A^c|$.*

Demostración. Como $\mathcal{U} = A \cup A^c$ y $A \cap A^c = \varnothing$, por el principio de adición tenemos $|\mathcal{U}| = |A| + |A^c|$, de donde $|A| = n - |A^c|$. □

11.1.4. Principios de Inyección y Biyección

Otros principios que son muy sencillos pero útiles son los principios de inyección y biyección

Proposición 11.4 (Principio de Inyección (**PI**)). *Si A y B son conjuntos finitos y existe una función inyectiva de A en B entonces $|A| \leq |B|$.*

La demostración de este principio la veremos más adelante (ver §11.8.1), aunque es intuitivamente clara. Para el caso en que los conjuntos son infinitos el resultado igual vale, ¡pero no es para nada trivial! Se lo conoce como el teorema de Cantor-Bernstein-Schröder.

Proposición 11.5 (Principio de Biyección (**PB**)). *Si A y B son conjuntos finitos y existe una biyección entre A y B entonces $|A| = |B|$.*

Demostración. Si $f : A \to B$ es una biyección, entonces tanto f como f^{-1} son inyectivas, y, por el **PI**, se tiene $|A| \leq |B|$ y $|B| \leq |A|$. □

Usaremos estos principios en reiteradas oportunidades en ejemplos venideros.

11.2. Acción básica: Ordenar

Dos problemas básicos y fundamentales son:

- Dados n objetos, ordenarlos.
- Dados n objetos, elegir k de ellos.

Las siguientes preguntas están relacionadas con estos problemas.

- ¿De cuántas formas se pueden ordenar n objetos?
- ¿De cuántas formas se pueden elegir k elementos de un conjunto de n elementos?

Es claro que si tenemos a mano todas las posibles ordenaciones de n objetos entonces podemos contarlos. La dificultad de obtener todas las ordenaciones crece muy rápido a medida que crece el n, como veremos en ejemplos sencillos. Lo que queremos es descubrir una manera de saber calcular el número de ordenaciones, sin tener que contarlas!

11.2.1. Ordenar en fila (listar)

Cuando uno describe un conjunto, no importa el orden en que sus elementos son listados. Sin embargo, en otros contextos, el orden es muy importante. Cuando esto ocurre, debemos saber dar los distintos órdenes y saber contar cuántos hay. En general cuando decimos ordenar queremos significar listar, dar una lista ordenada.

Ordenar (en fila) un conjunto finito es dar una lista (u ordenación) de sus elementos.

Ejemplo. Si $X = \{x_1, x_2, \ldots, x_7\}$, las siguientes son ejemplos de listas distintas de los elementos de X

$$L_1 = x_1, x_2, x_3, x_4, x_5, x_6, x_7 \qquad L_2 = x_7, x_6, x_5, x_4, x_3, x_2, x_1$$
$$L_3 = x_2, x_1, x_4, x_3, x_6, x_5, x_7 \qquad L_4 = x_4, x_1, x_7, x_5, x_2, x_6, x_3$$

Podemos pensar que la primer lista L_1 es lo mismo que tener una función $f_1 : I_7 \to X$ dada por

$$f_1(1) = x_1,\ f_1(2) = x_2,\ f_1(3) = x_3,\ f_1(4) = x_4,\ f_1(5) = x_5,\ f_1(6) = x_6,\ f_1(7) = x_7$$

Similarmente, L_2 se puede ver como la función $f_2 : I_7 \to X$ dada por

$$f_2(1) = x_7,\ f_2(2) = x_6,\ f_2(3) = x_5,\ f_2(4) = x_4,\ f_2(5) = x_3,\ f_2(6) = x_2,\ f_2(7) = x_1$$

Análogamente tenemos funciones $f_3, f_4 : I_7 \to X$ para L_3 y L_4. ◊

Ahora, si $X = \{x_1, x_2, \ldots, x_7\}$ es un n-conjunto, es decir un conjunto de n elementos, entonces una lista es algo de la forma

$$L = x_{i_1}, x_{i_2}, \ldots, x_{i_n} \tag{11.1}$$

donde los $x_{i_1}, x_{i_2}, \ldots, x_{i_n}$ son todos los elementos de X. Es decir, $x_{i_1}, x_{i_2}, \ldots, x_{i_n} \in X$ y $x_{i_j} \neq x_{i_k}$ para todo $1 \leq i_j, i_k \leq n$ con $j \neq k$. Por ejemplo,

$$L_1 = x_1, x_2, x_3, \ldots, x_{n-1}, x_n$$
$$L_2 = x_2, x_3, x_1, \ldots, x_{n-1}, x_n$$
$$L_3 = x_n, x_{n-1}, \ldots, x_3, x_2, x_1$$

son ejemplos de listas distintas. A la lista L como en (11.1) podemos asociarle la función biyectiva

$$f : I_n \to X$$

dada por

$$f(1) = x_{i_1}, \qquad f(2) = x_{i_2}, \qquad \cdots \qquad f(n) = x_{i_n}$$

Recíprocamente, a cada función biyectiva $f : I_n \to X$ podemos asociarle la lista

$$L_f = f(1), f(2), \ldots, f(n)$$

formada por sus imagenes ordenadas.

Luego, identificamos una lista ordenada de elementos de X con la imagen de una ordenación de X

$$f(1) = x_{i_1}, \quad f(2) = x_{i_2}, \quad \ldots, \quad f(n) = x_{i_n}$$

Dijimos que ordenar un conjunto finito es dar una lista de sus elementos. Más formalmente, es encontrar una "ordenación" para él.

Ejemplo. Comencemos tratando de ordenar conjuntos pequeños. Tomemos el conjunto $X = I_n = \{1, 2, \ldots, n\}$, para los primeros valores de n, y ordenamos sus elementos cuidando de hacerlo de todas las formas posibles.

- I_1. Para $n = 1$ hay una única forma: 1.
- I_2. Para $n = 2$ hay solo dos formas: 12 y 21.
- I_3. Para $n = 3$ hay 6 formas: 123, 132, 213, 231, 312, 321.
- I_4. Fijemos el 1 como primer elemento y listemos todos los órdenes que comienzan con 1; éstos los obtendremos con todos los órdenes posibles para los elementos del conjunto $\{2, 3, 4\}$. Luego, tenemos

  $$1234, \quad 1243, \quad 1324, \quad 1342, \quad 1423, \quad 1432.$$

  Ahora, repetimos el proceso tomando a 2 como primer elemento y ordenando $\{1, 3, 4\}$. Haciendo lo mismo con todos los posibles primeros elementos, finalemente obtenemos

1234	2134	3124	4123
1243	2143	3142	4132
1324	2314	3214	4213
1342	2341	3241	4231
1423	2413	3412	4312
1432	2431	3421	4321

  Luego, para $n = 4$ hay 24 formas de ordenar los elementos $1, 2, 3, 4$. Notar que, para estar seguros de que cubrimos todos los casos, usamos por lo general el orden del diccionario. ◊

A partir de los ejemplos previos, nos damos cuenta que podemos resolver el problema general de ordenar n elementos recursivamente.

MÉTODO GENERAL

Fijamos el primer elemento de la lista, para el cual hay n elecciones posibles, y ordenamos el conjunto de $n-1$ elementos restantes, el cual sabemos recursivamente que podemos ordenar de $(n-1)!$ formas distintas. Luego, por el princio de multiplicación, hay

$$n(n-1)! = n!$$

formas distintas de ordenar un n-conjunto.

Proposición 11.6. *Hay $n!$ formas distintas de ordenar los elementos de un n-conjunto, para cada $n \in \mathbb{N}$.*

Demostración. Por el principio de biyección, basta ver que hay $n!$ formas de ordenar los elementos del conjunto $I_n = \{1, 2, \dots, n\}$. Hacemos inducción en n. Hay una única forma de ordenar $I_1 = \{1\}$. Supongamos que hay $k!$ formas de listar los elementos de I_k, y veamos que entonces hay $(k+1)!$ formas de listar los elementos de I_{k+1}. Sea

$$x_1, x_2, \dots, x_{k+1}$$

una lista de elementos de I_{k+1}, es decir $x \in I_{k+1}$ con $x_i \neq x_j$ para todo $1 \leq i, j \leq k+1, i \neq j$. Supongamos que $x_1 = j$. Luego

$$\{x_2, x_3, \dots, x_{k+1}\} = I_{k+1} \setminus \{j\}$$

y este conjunto está claramente en biyección con I_k. Por ejemplo, tenemos la biyección $\psi : I_{k+1} \setminus \{j\} \to I_k$ definida por

$$\psi(i) = \begin{cases} i & i = 1, \dots, j-1 \\ i-1 & i = j+1, \dots, k+1 \end{cases}$$

Es decir,

$$\begin{aligned} 1 &\mapsto 1 \\ 2 &\mapsto 2 \\ &\vdots \\ j-1 &\mapsto j-1 \\ j+1 &\mapsto j \\ &\vdots \\ k+1 &\mapsto k \end{aligned}$$

Como $|I_{k+1} \setminus \{j\}| = |I_k| = k$, por el principio de biyección, hay $k!$ formas de ordenar a $I_{n+1} \setminus \{j\}$. Como hay $k+1$ elecciones posibles para x_1, por el principio de multiplicación, hay $(k+1)k! = (k+1)!$ formas de ordenar I_{k+1}. Luego, por inducción, hay $n!$ formas de ordenar I_n. □

Consideramos en los siguientes ejemplos algunas variaciones del problema de ordenar los elementos de un conjunto dado.

Ejemplo (anagramas)**.** ¿Cuántas palabras distintas (reales o no) se pueden formar con las letras de la palabra MURCIELAGO? Sea $X = \{\text{M,U,R,C,I,E,L,A,G,O}\}$. Como $|X| = 10$ hay $10! = 3.628.800$ posibles palabras.

Ejemplo (cartas)**.** ¿De cuántas formas puede quedar un mazo de cartas españolas luego de ser mezclado, con todas las cartas boca arriba (o todas boca abajo)? Hay 40 cartas, por lo tanto hay $40!$ mezcladas.

Ejemplo (sentadas)**.** ¿De cuántas formas distintas se pueden sentar en una fila 7 chicos y 6 chicas si...

(1) no les exigimos ninguna condición?

(2) los sexos deben estar intercalados (ningún par de chicos o chicas juntos)?

(3) las chicas deben estar todas juntas?

Respuestas:
(1) Hay 7+6=13 personas, por lo tanto $13! = 6.227.020.800$ formas de sentarlas en fila.

(2) Deben aparecer así

$$b_1\, g_1\, b_2\, g_2\, b_3\, g_3\, b_4\, g_4\, b_5\, g_5\, b_6\, g_6\, b_7$$

Hay $7!$ formas de ordenar a los chicos entre sí, $6!$ formas de ordenar a las chicas entre sí, y por **PM**, hay

$$7! \cdot 6! = 10 \cdot 9 \cdot 8 \cdot 7! = 10!$$

formas de sentarlos intercalados.

(3a) Las 6 chicas forman un bloque y luego podemos pensarlas como una sola persona. Hay $8!$ formas de sentar a los 7 chicos mas este bloque de chicas y hay $6!$ formas de ordenar a las chicas entre sí (dentro del bloque). Por **PM**, hay

$$8! \cdot 6! = 8 \cdot 10!$$

formas de sentarlos, con las chicas formando bloque.
(3b) Otra forma, muy similar, es la siguiente. Sentamos a los chicos primero (hay $7!$ formas) y para el bloque de chicas existen 8 lugares donde puede ser ubicado:

$$\square\, b_1\, \square\, b_2\, \square\, b_3\, \square\, b_4\, \square\, b_5\, \square\, b_6\, \square\, b_7\, \square$$

y luego ordenamos las chicas entre sí ($6!$ formas). Así, tenemos

$$8 \cdot 7! \cdot 6! = 8! \cdot 6! = 10!$$

formas de sentarlos con las chicas formando un bloque. ◊

Como aplicación sencilla, veamos "ordenar con repeticiones", algo que estudiaremos en breve en mas detalle.

Ejemplo (ordenar con repeticiones)**.** Nos preguntamos ahora como ordenar "conjuntos" donde hay elementos repetidos. Por ejemplo, ¿Cuántas palabras se pueden formar con las letras de la palabra BANANA*?

La clave está en distinguir a las letras repetidas, por ejemplo con colores o con subíndices, para poder contarlas y luego "indistinguirlas" para no contar repeticiones. Así, tenemos $A_1, A_2, A_3, B, N_1, N_2$. Hay 6! posibles palabras con estas letras. Ahora debemos volver a indistinguir las letras, ya que por ejemplo, las secuencias

$$BA_1N_1A_2N_2A_3 \quad \text{y} \quad BA_1N_2A_2N_1A_3$$

representan la misma palabra cuando consideremos como iguales a $N_1 = N_2$. Como hay 2! reordenaciones de las N's y 3! reordenaciones de las A's, y todas estas dan la misma palabra cuando use las letras B, A, N. Luego, podemos formar

$$\frac{6!}{3!\,2!} = \frac{6 \cdot 5 \cdot 4}{2} = 5 \cdot 4 \cdot 3 = 60$$

posibles palabras distintas con las letras de BANANA. ◊

Después que aprendamos a "elegir", veremos otra forma de resolver el ejemplo anterior y el resultado general sobre como ordenar con repeticiones (ver §11.6).

11.2.2. Ordenar en círculos (ciclar)

Veamos 2 variantes de "ordenar",

- *Ordenar en círculos o ciclar*.
- *Ordenar con repeticiones*.

Comencemos con un ejemplo práctico.

Ejemplo (mesa)**.** ¿De cuántas formas se pueden sentar 6 personas alrededor de una mesa circular? Sólo nos interesan las posiciones relativas entre las personas (es decir, quién está a la izquierda y a la derecha de quién). Veamos 2 formas de hacerlo. Sabemos que hay 6! formas de ordenarlas en fila.

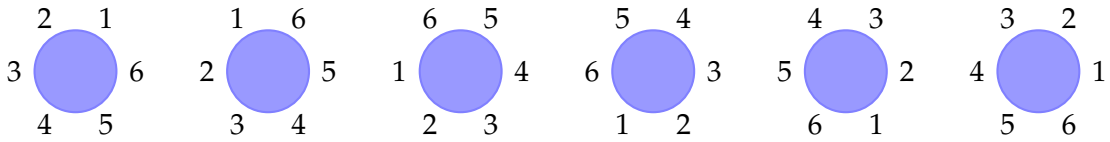
(1) Elegimos una persona, digamos la 6, y la sentamos en una posición fija. Los 5 asientos que quedan pueden pensarse como un fila, ya que los bordes no están unidos. Luego hay

$$5!$$

formas de sentar las 6 personas alrededor de la mesa. Por ejemplo, dos sentadas distintas posibles son

*notar que podríamos haber usado cualquier fruta que solo contenga la vocal "a" 3 veces, como por ejemplo ANANÁ, MANZANA, NARANJA, GRANADA o PAPAYA.

(2) Hay 6! formas de sentarlos. Pero cada posición es contada 6 veces, pues la 6 rotaciones de una misma posición inical son consideradas la misma "sentada" (i.e. las posiciones relativas son las mismas).



Luego hay

$$\frac{6!}{6} = 5!$$

formas de sentar a las 6 personas alrededor de la mesa. ◊

Dado un n-conjunto, *ordenar cíclicamente* (o *ciclar*) sus elementos es, intuitivamente, ordenarlos sobre un círculo y no sobre un segmento como en el caso de listas. Formalmente, ahora no existe un primer elemento de la lista, un segundo elemento de la lista, etcétera, como antes. Es decir, consideramos el último elemento de un orden lineal como si estuviera a la izquierda del primero (o el primero como si estuviera a la derecha del último). Por ejemplo, 123, 231 y 312 se consideran (cíclicamente) ordenaciones iguales del conjunto $\{1, 2, 3\}$. En este caso, dado $X = \{x_1, x_2, \ldots, x_n\}$, los órdenes lineales (distintos)

$$\begin{array}{lcccccccc}
L_1 & = & x_1 & x_2 & x_3 & \ldots & x_{n-2} & x_{n-1} & x_n \\
L_2 & = & x_2 & x_3 & x_4 & \ldots & x_{n-1} & x_n & x_1 \\
L_3 & = & x_3 & x_4 & x_5 & \ldots & x_n & x_1 & x_2 \\
\vdots & & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
L_{n-1} & = & x_{n-1} & x_n & x_1 & \ldots & x_{n-4} & x_{n-3} & x_{n-2} \\
L_n & = & x_n & x_1 & x_2 & \ldots & x_{n-3} & x_{n-2} & x_{n-1}
\end{array}$$

son considerados, por definición, como el *mismo* orden cíclico $C = (x_1, x_2, \ldots, x_n)$.

En el caso general, tenemos.

MÉTODO GENERAL I

Elegimos una persona y la sentamos en un lugar fijo de la mesa. Quedan $n-1$ personas para sentar en los $n-1$ lugares libres. Hay

$$(n-1)!$$

formas de ordenar a estas personas.

MÉTODO GENERAL II

Hay $n!$ formas de ordenar n personas. Como consideramos a las n posibles rotaciones cíclicas de una sentada dada como la misma, dividimos por n para no contar repeticiones. Luego, hay

$$\frac{n!}{n} = (n-1)!$$

formas distintas de sentar a las n personas en círculo.

Proposición 11.7. *Hay* $(n-1)!$ *formas de ordenar cíclicamente un* n*-conjunto, para cada* $n \in \mathbb{N}$.

Demostración. Hacemos inducción en n. El paso inicial es obvio, hay 1 solo orden cíclico de 1 elemento, que es igual a $(1-1)! = 0! = 1$.

Supongamos que k elementos pueden ordenarse cíclicamente de $(k-1)!$ formas distintas. Veamos que $k+1$ elememtos pueden ordenarse cíclicamente de $k!$ formas. Sean $1, 2, \ldots, k, k+1$ estos elementos. Pensemos que el elemento $k+1$ lo ponemos a la derecha del elemento i y que forman una sola entidad. Ahora tenemos k elementos que pueden ser ordenados cíclicamente de $(k-1)!$ formas. Y hay k elecciones distintas para el elemento i. Luego, por **PM** hay $k(k-1)! = k!$ formas ordenes cíclicos distintos con $k+1$ elementos. Por principio de inducción, el resultado sigue. □

Ejemplo (sentar chicos y chicas)**.** ¿De cuántas formas se pueden sentar a una mesa circular 5 chicos y 3 chicas si...

(1) ...el chico B_1 no debe estar al lado de la chica G_1?

(2) ...ninguna de las chicas son adyacentes (se sientan juntas)?

(1a) Una forma de hacerlo es sentar a todos menos la chica G_1. Hay $(7-1)! = 6!$ formas de hacerlo. Quedan 7 lugares donde sentar a la chica G_1, pero como no puede estar al lado de B_1 no podemos sentarla ni a su izquierda ni a su derecha. Esto deja 5 lugares posibles. Luego, por **PM**, hay

$$6! \cdot 5 = 720 \cdot 5 = 3.600$$

formas de sentarlos de la forma pedida.

(1b) Si usamos el principio del complemento, contamos de cuántas formas se pueden sentar B_1 y G_1 juntos y lo restamos del número total. Hay $(8-1)! = 7!$ formas de sentar a las 8 personas a la mesa. Pensamos a $\{B_1, G_1\}$ como una sola persona. Luego hay $(7-1)! = 6!$ formas de sentar a las 7 "personas" y ahora teniendo en cuenta el orden entre ellos, B_1G_1 y G_1B_1, tenemos $2 \cdot 6! = 1440$. Luego, hay

$$7! - 2 \cdot 6! = 5.040 - 1.440 = 3.600$$

formas de sentarlos. Notar que $7! - 2 \cdot 6! = (7-2)6! = 56!$ que fue la respuesta dada en (1a).

(2) Sentamos primero a los 5 chicos, hay $(5-1)! = 4!$ formas de hacerlo. La chica G_1 tiene 5 lugares. Como no pueden estar juntas, la chica G_2 tiene 4 lugares para sentarse y la chica G_3 tiene 3 lugares. Luego, hay

$$4! \cdot 5 \cdot 4 \cdot 3 = 1.440$$

formas de sentarse de la forma pedida. ◊

Ejemplo (sentar matrimonios)**.** ¿De cuántas formas se pueden sentar a una mesa n matrimonios si...

(1) ...hombres y mujeres deben alternarse?

(2) ...cada mujer está al lado de su marido? (sentada políticamente correcta).

(1) Los n hombres se pueden sentar de $(n-1)!$ formas. Las n mujeres se pueden sentar en los n lugares que quedan entre los hombres. Esto puede hacerse de $n!$ formas. Por **PM**, hay

$$n!\,(n-1)!$$

formas de sentar n matrimonios con los hombres y mujeres alternados.

(2) Primero sentamos a las parejas. Condiderando a cada pareja como una entidad, hay $(n-1)!$ formas de sentarlas. Como a cada pareja hay 2 formas de ordenarlas, tenemos

$$2^n\,(n-1)!$$

formas de sentar a n matrimonios con el hombre y la mujer uno al lado del otro. ◊

Nota. Un problema mucho mas difícil es el conocido como problema *"des menages"*. Se quiere determinar de cuántas formas se pueden sentar n matrimonios de manera que los hombres y las mujeres alternan y ningún hombre está al lado de su mujer (sentada políticamente incorrecta!). Este problema fue planteado por el matemático francés Francis Lucas (1842–1891).

11.3. Acción básica: Elegir

Ya estudiamos la acción combinatoria de ordenar elementos de un conjunto. Ahora estudiemos la acciones de elegir elementos de un conjunto. Comencemos con un número pequeño.

Pregunta. ¿De cuántas formas se pueden elegir 2 objetos de un total de 4? En otras palabras, dado el conjunto $I_4 = \{1,2,3,4\}$, ¿cuántos 2-subconjuntos tiene?

Respuesta. Veamos 3 formas distintas de responder esta pregunta.

(1) Listamos directamente todos los 2-subconjuntos $\{a,b\}$

{1,2}	{2,3}	{3,4}
{1,3}	{2,4}	
{1,4}		

Una forma de estar seguros de que no olvidamos ningún par es pensar que los ordenamos como en un diccionario, esto es siguiendo el orden lexicográfico (en la primer columna los que empiezan con 1 y dentro de esa columna ordenados de menor a mayor, en la segunda columna los que empiezan con 2 y dentro de esta ordenados de menor a mayor, etc.)

(2) Tomando todos los posibles pares ordenados (a, b)

12	21	31	41
13	23	32	42
14	24	34	43

Hay $4 \cdot 3 = 12$. Como los pares (a, b) y (b, a) ambos representan al conjunto $\{a, b\}$ (si nos olvidamos del orden), tenemos que el número de 2-subconjuntos es $\frac{12}{2} = 6$.

(3) Ahora tomamos todas las $4! = 24$ ordenaciones de I_4

1234	1324	1423
1243	1342	1432
2134	3124	4123
2143	3142	4132
2314	2413	3412
2341	2431	3421
3214	4213	4312
3241	4231	4321

Considero los 2 primeros elementos ab de cada lista $abcd$. Si nos fijamos aparecen $abcd$ y $abdc$. Ambas listas de 4 elementos me darán la misma lista de 2 elementos ab cuando descartemos los dos últimos posiciones. Luego, tenemos $\frac{4!}{2} = 12$ pares ordenados. Ahora estamos en el caso anterior. Como siempre están ab y ba, dividimos por 2 y obtenemos los seis 2-subconjuntos listados en (1).

Los métodos (2) y (3) parecen un poco absurdos, porque contamos repeticiones de más y luego dividimos para no contarlas... Sin embargo, en el caso general esto resultará más fácil, y de hecho es la forma adecuada de probarlo.

Definición. Definimos el número $\binom{n}{k}$ como la cantidad de subconjuntos de k elementos que tiene un conjunto de n elementos (o equivalentemente la cantidad de formas de elegir k elementos de un conjunto de n elementos). O sea,

$$\binom{n}{k} = \#\{A \subseteq X : |A| = k, |X| = n\} = \#\{A \subseteq I_n : |n| = k\} \tag{11.2}$$

Por definición tenemos $0 \leq k \leq n$. El número $\binom{n}{k}$ se llama *número combinatorio n en k* y se lee simplemente "n en k". Si $k < 0$ o $k > n$ definimos $\binom{n}{k} = 0$.

Tratemos de adivinar una fórmula para $\binom{n}{k}$, usando los argumentos vistos en el ejemplo.

MÉTODO GENERAL I

Sea X un n-conjunto y $\{x_1, x_2, \ldots, x_k\}$ un k-subconjunto de X. Hay n formas de elegir el elemento x_1, $n-1$ formas de elegir el elemento x_2, $n-2$ formas de elegir el elemento x_3, etcétera, y finalmente $n-(k-1) = n-k+1$ formas de elegir el elemento x_k. Por el **PM** hay

$$n(n-1)(n-2)\cdots(n-k)(n-k+1)$$

formas de elegir k elementos de X. Sin embargo, las $k!$ reordenaciones posibles de estos elementos representan el mismo conjunto. Luego, el número buscado es

$$\binom{n}{k} = \frac{n(n-1)\cdots(n-k+1)}{k!}$$

MÉTODO GENERAL II

La idea es hacer listas con los n elementos, dividirla en 2 bloques, el primero con k elementos y el segundo con $n-k$ elementos, y finalmente descartar los elementos del segundo bloque. Hay $n!$ formas de ordear los elementos de I_n. Dada una lista cualquiera

$$\underbrace{a_1 a_2 \ldots a_k}_{k} \mid \underbrace{a_{k+1} \ldots a_n}_{n-k}$$

y fijados los primeros k elementos de la lista, hay $(n-k)!$ reordenaciones de los elementos del segundo bloque. Luego, hay

$$\frac{n!}{(n-k)!}$$

listas ordenadas de k elementos (después de tirar los elementos del segundo bloque). Las $k!$ ordenaciones distintas de $a_1 \ldots a_k$ dan lugar al mismo conjunto; por lo tanto, hay

$$\binom{n}{k} = \frac{\frac{n!}{(n-k)!}}{k!} = \frac{n!}{k!(n-k)!}$$

formas de elegir k elementos de I_n.

Así, hemos probado el siguiente resultado.

Proposición 11.8. *Dado $n \in \mathbb{N}_0$, para todo $0 \leq k \leq n$ se tiene*

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n(n-1)\cdots(n-k+1)}{k!}$$

Demostración. Los métodos I y II vistos más arriba dan pruebas combinatorias de que $\binom{n}{k} = \frac{n(n-1)\cdots(n-k+1)}{k!}$ y $\binom{n}{k} = \frac{n!}{k!(n-k)!}$, respectivamente. □

Podemos chequear algebraicamente la igualdad

$$\frac{n!}{k!(n-k)!} = \frac{n(n-1)\cdots(n-(k-1))(n-k)!}{k!(n-k)!} = \frac{n(n-1)\cdots(n-k+1)}{k!}$$

Ejemplo. Hay 22 jugadores elegidos para armar una selección de futbol. Sabemos que hay 3 arqueros, 6 defensores, 8 volantes y 5 delanteros. ¿Cuántos equipos distintos se pueden formar...

(1) ... si no imponemos restricciones?

(2) ... si debemos elegir un capitán?

(3) ... si deben tener la disposición táctica 4-4-2? y la 4-3-3?[*] ¿De cuántas formas distintas se pueden "parar" en la cancha estos equipos?

Respuestas:

(1) Hay que elegir un arquero y 10 jugadores. Luego hay

$$\binom{3}{1}\binom{19}{10} = 3 \cdot \frac{19 \cdot 18 \cdots 11}{9 \cdot 8 \cdots 2} = 3 \cdot 19 \cdot 17 \cdot 13 \cdot 11 \cdot 2 = 277.134.$$

(2) A cada posible equipo lo distinguimos eligiendo un capitán. Luego, hay $3\binom{19}{10}11 = 3.048.474$ equipos con capitán.

(3) Hay que elegir un arquero, 4 defensores, 4 mediocampistas y 2 delanteros. Luego,

$$\binom{3}{1}\binom{6}{4}\binom{8}{4}\binom{5}{2} = 3\frac{6!}{4!2!}\frac{8!}{4!4!}\frac{5!}{2!3!} = 3 \cdot 15 \cdot 70 \cdot 10 = 31.500.$$

Además hay 2 formas de parar a los delanteros, y $4!$ de ordenar cada línea de 4, por lo que tenemos $2(4!)^2 = 1.152$ formas distintas de parar a cada elección de 11 jugadores, dando un total de $31.500 \times 1.152 = 36.288.000$ posibles equipos parados de la forma 4-4-2.

Similarmente para el 4-3-3 tenemos

$$3\binom{6}{4}\binom{8}{3}\binom{5}{3} = 3 \cdot 15 \cdot 56 \cdot 10 = 25.200$$

equipos y

$$4!(3!)^2 = 24 \cdot 36 = 864$$

formas de parar cada uno de estos equipos. Luego, hay $25.200 \times 864 = 21.772.800$ equipos posibles con esta disposición táctica.

Si además debemos elegir un capitán en cada caso, entonces debemos multiplicar por 11 los números obtenidos. ¡El "loco" Bielsa sabe esto, por supuesto!

11.4. Combinaciones, permutaciones y arreglos

Definiciones. Sean $k, n \in \mathbb{N}$, con $0 \leq k \leq n$.

Una *combinación* de k en n es una selección de k elementos de un conjunto de n. Denotamos por

$$C_{k,n} = \#\{\text{combinaciones de } k \text{ en } n\}$$

[*] ni falta hace mencionar que nosotros preferimos el esquema 4-3-1-2 con enganche, ese raro especimen en vías de extinción.

Aquí no importa el orden.

Un *arreglo* de k en n es una selección ordenada de k elementos de un conjunto de n. Denotamos por

$$A_{k,n} = \#\{\text{arreglos de } k \text{ en } n\}$$

Aquí si importa el orden. También se lo sabe llamar una k-permutación de n

Una *permutación* de n es un arreglo de n en n. Denotamos por

$$P_n = \#\{\text{permutaciones de } n\}$$

Notar que:

- el número de combinaciones de k en n es el número de k-subconjuntos de un n-conjunto;
- a una permutación de n se la puede pensar como una biyección de I_n en I_n.

Ejemplo. Sea $n = 5$ y $k = 3$. Las combinaciones de 3 en 5 de I_5 son

$$\{1,2,3\}, \quad \{1,2,4\}, \quad \{1,2,5\}, \quad \{1,3,4\}, \quad \{1,3,5\},$$
$$\{1,4,5\}, \quad \{2,3,4\}, \quad \{2,3,5\}, \quad \{2,4,5\}, \quad \{3,4,5\},$$

luego

$$C_{3,5} = 10 = \binom{5}{3}$$

Por otra parte, una combinación como $\{1,3,5\}$ da lugar a varios 3-arreglos distintos

$$(1,3,5), \quad (1,5,3), \quad (3,1,5), \quad (3,5,1), \quad (5,1,3), \quad (5,3,1).$$

Luego

$$A_{3,5} = 3! \cdot C_{3,5} = 3!\binom{5}{3} = \frac{5}{(5-3)!} = \frac{5 \cdot 4 \cdot 3 \cdot 2}{2} = 60$$

Finalmente, es claro que las permutaciones de 5 son 5!. ◊

Permutaciones cíclicas. A veces nos puede interesar ordenar objetos circularmente, no en fila, son los llamados *arreglos circulares*. Si tenemos n objetos y elegimos k de ellos y los arreglamos alrededor de un círculo, decimos que tenemos un *arreglo circular de k en n* o un *k-arreglo circular de n*. Al número total de tales arreglos lo denotamos por $Q_{k,n}$. Un n-arreglo circular de n es llamado una *permutación circular* de n. Por lo visto en el ejemplo la Sección §11.2.2, sabemos que el número de permutaciones cíclicas de n elementos, que denotaremos por Q_n, es

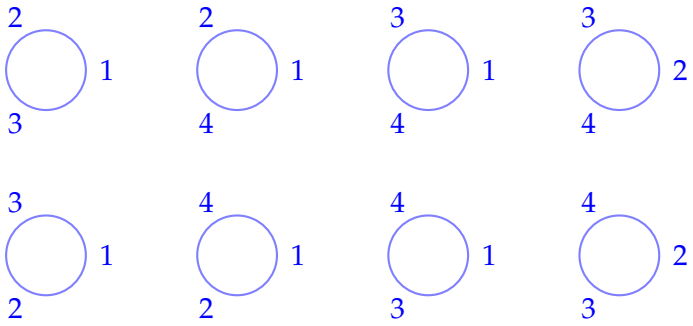
$$Q_n = \frac{n!}{n} = (n-1)!$$

El mismo argumento muestra que para cada $k \leq n$, el número de k-arreglos circulares de n es

$$Q_{k,n} = \frac{A_{k,n}}{k} = \frac{n!}{k(n-k)!}$$

Notar que $Q_{n,n} = Q_n$ como debe ser.

Por ejemplo, si $k = 3$ y $n = 4$, hay $Q_{3,4} = \frac{4!}{3} = 8$ arreglos circulares de 3 en 4. En I_4 son



que podemos representar así

$$(1,2,3),\quad (1,2,4),\quad (1,3,4),\quad (2,3,4),$$
$$(1,3,2),\quad (1,4,2),\quad (1,4,3),\quad (2,4,3).$$

(recorriendo el círculo en sentido antihorario).

Resumen. Resumiendo los resultados del capítulo hasta aquí, tenemos la siguiente tabla

Cuadro 11.1: Combinaciones, permutaciones y arreglos

	notación	variaciones	número
arreglos	$A_{k,n}$	$k!C_{k,n}$	$k!\binom{n}{k} = \frac{n!}{(n-k)!}$
combinaciones	$C_{k,n}$	$\frac{A_{k,n}}{k!}$	$\binom{n}{k} = \frac{n!}{k!(n-k)!}$
permutaciones	P_n	$A_{n,n}$	$n!$
arreglos circulares	$Q_{k,n}$	$\frac{1}{k}A_{k,n}$	$\frac{n!}{k(n-k)!}$
permutaciones cíclicas	Q_n	$Q_{n,n} = \frac{1}{n}P_n$	$(n-1)!$

Notar que un k-arreglo de n se obtiene de elegir un k-subconjunto y ordenar sus elementos. Recíprocamente, una k-combinación de n se obtiene a partir de un k-arreglo considerando como iguales todas las reordenaciones de sus elementos.

11.5. Aplicaciones

Muchos problemas generales de conteo se pueden resolver combinando las técnicas aprendidas hasta ahora. Esto es, usando los principios **PA**, **PM**, **PC**, **PI** y **PB**, y el hecho de que sabemos de cuántas formas se pueden elegir y ordenar determinados conjuntos.

11.5.1. Ejemplos variopintos

Veamos algunos ejemplos, combinando el uso de "elegir" y "ordenar" (equipos de fútbol, comités, sentadas en mesas, manos de póker).

Ejemplo: dominós En el dominó hay fichas con 2 números del 0 al 7. ¿Cuántas fichas de dominó hay? Por supuesto que podemos contarlas una por una, no son tantas. Pero hagámoslo de forma más elegante.

(1) Una forma es ordenarlos así,

$$\begin{array}{ccccccc}
(0,0) & & & & & & \\
(1,0) & (1,1) & & & & & \\
(2,0) & (2,1) & (2,2) & & & & \\
(3,0) & (3,1) & (3,2) & (3,3) & & & \\
(4,0) & (4,1) & (4,2) & (4,3) & (4,4) & & \\
(5,0) & (5,1) & (5,2) & (5,3) & (5,4) & (5,5) & \\
(6,0) & (6,1) & (6,2) & (6,3) & (6,4) & (6,5) & (6,6)
\end{array}$$

donde el par (x, y) con $0 \leq x \leq y \leq 6$ representa un dominó. Por ejemplo, $(3, 5) =$ ⚃⚅. Luego, hay

$$1 + 2 + 3 + \cdots + 7 = \tfrac{7\cdot 8}{2} = 28$$

(2) Una forma más fácil todavía es contar los pares que no son "dobles" más los que si lo son. Como hay 7 dobles, hay en total

$$\tbinom{7}{2} + 7 = \tfrac{7\cdot 6}{2} + 7 = 21 + 7 = 28$$

fichitas de dominó.

Ejemplo: comités. Queremos formas comités de entre un grupo de 7 mujeres y 6 hombres. ¿Cuántos comités distintos de 5 personas pueden formarse...

(1) ... sin restricciones?

(2) ... con 1 presidente y 2 secretarios?

(3) ... de 3 mujeres y 2 hombres?

(4) ... con por lo menos 3 mujeres?

(5) ... con al menos una mujer?

(6) ... si el temible Sr X debe estar si o si?

(7) ... con 2 hombres y el Sr X y la Sra X no pueden estar ambos en el comité?*

* se quieren evitar las tristemente célebres acaloradas discusiones entre los X's...

Respuestas:

(1) Elegimos 5 personas de un total de 13, luego hay

$$\binom{13}{5} = \frac{13!}{5!8!} = \frac{13 \cdot 12 \cdot 11 \cdot 10 \cdot 9}{5 \cdot 4 \cdot 3 \cdot 2} = 13 \cdot 11 \cdot 9 = 1.287$$

(2) Una forma es elegir primero el comité. Por (1) sabemos que se puede elegir de $\binom{13}{5}$ formas. Además, hay 5 formas de elegir un presidente y $\binom{4}{2}$ formas de elegir los secretarios de entre los que no son presidentes. Luego hay

$$5\binom{13}{5}\binom{4}{2} = 13 \cdot 11 \cdot 9 \cdot 5 \cdot 6 = 38.610$$

Otra forma es elegir primero al presidente de entre los 13. De los 12 que quedan, elegimos 2 secretarios y, de los 10 restantes, 2 personas cualquiera para completar. Luego, hay

$$\binom{13}{1}\binom{12}{2}\binom{10}{2} = 13 \cdot \frac{12 \cdot 11}{2} \cdot \frac{10 \cdot 9}{2} = 13 \cdot 11 \cdot 9 \cdot 6 \cdot 5$$

comités de la forma pedida.

Notar que el número de comités coincide en las dos formas de calcularla y que hay más comités que el total posible calculado en (1). Esto está bien, pues hemos distinguido los roles, al igual que con los capitanes en el ejemplo previo de los equipos de fútbol.

(3) Es calro que hay

$$\binom{7}{3}\binom{6}{2} = \frac{7 \cdot 6 \cdot 5}{3 \cdot 2} \cdot \frac{6 \cdot 5}{2} = 7 \cdot 5^2 \cdot 3 = 525$$

(4) Sumamos los comités con exactamente 3, 4 y 5 mujeres respectivamente. Luego, hay

$$\binom{7}{3}\binom{6}{2} + \binom{7}{4}\binom{6}{1} + \binom{7}{5} = 7 \cdot 5^2 \cdot 3 + 7 \cdot 6 \cdot 5 + 7 \cdot 3 = 756$$

(5) Al menos una mujer, significa que haya 1, 2, 3, 4 ó 5 mujeres. Por el **PC**, conviene contar el número de comités sin mujeres y restarlos del total. Luego, hay

$$\binom{13}{5} - \binom{7}{0}\binom{6}{5} = 1.287 - 6 = 1.281$$

(6) Como el Sr X debe estar, solo hay que elegir los 4 que faltan:

$$\binom{12}{4} = \frac{12 \cdot 11 \cdot 10 \cdot 9}{4 \cdot 3 \cdot 2} = 11 \cdot 9 \cdot 5 = 495$$

(7) Veamos 2 formas distintas:

(i) Usamos el **PA**. Contamos los 3 casos favorables por separado y luego sumamos:

(a) El Sr X está y la Sra X no: $\binom{6}{3}\binom{5}{1} = 20 \cdot 5 = 100$.

(b) La Sra X está y el Sr X no: $\binom{6}{2}\binom{5}{2} = 15 \cdot 10 = 150$.

(c) Ninguno está: $\binom{6}{3}\binom{5}{2} = 20 \cdot 10 = 200$.

Hay en total hay $175 + 315 + 200 = 450$ comités sin los controvertidos X's.

(ii) Ahora usamos el **PC**. Todos los comités de 3 mujeres y 2 hombres son $\binom{7}{3}\binom{6}{2} = 525$. El número de comités en que el Sr y Sra X están es: $\binom{6}{2}\binom{5}{1} = 15 \cdot 5 = 75$. Luego, hay $525 - 75 = 450$ comités apacibles.

Ejemplo: Bits. Pensemos en cadenas binarias de longitud n, es decir

$$a_1 a_2 \cdots a_n, \qquad a_i \in \{0, 1\}, \quad i = 1, \ldots, n$$

(si $n = 8$ se llaman bits y 8 bits forman un byte, i.e. $n = 64$). Nosotros llamaremos bits a cualquier n-cadena, por simplicidad.

Queremos contar bits bajo algunas condiciones. En general los números son autoexplicativos, por lo que haremos algún breve comentario sólo cuando sea necesario.

- # de bits sin restricciones = 2^n.
- # de bits con k posiciones prefijadas = 2^{n-k}.
- # de bits con exactamente k ceros = $\binom{n}{k}$.
- # de bits con a lo sumo k ceros = $\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{k}$.
- # de bits con por lo menos k ceros = $\binom{n}{k} + \binom{n}{k+1} + \cdots + \binom{n}{n}$.
- # de bits con igual número de 0's que 1's = $\begin{cases} \binom{n}{n/2} & \text{si } n \text{ es par,} \\ 0 & \text{si } n \text{ es impar.} \end{cases}$
- # de bits capicúas = $2^{\lceil n/2 \rceil}$.

  Primero digamos que un bit es capicúa si escrito en orden inverso se obtiene el mismo bit; es decir, si

  $$a_k = a_{n-k}, \qquad 1 \leq k \leq n.$$

  Si $n = 2m$, entonces basta considerar las primeras (o últimas) m posiciones (pues las otras m están determinadas) Luego hay 2^m capicúas. Si $n = 2m + 1$, la posición del medio, la $m + 1$, no se "refleja", y por lo tanto hay $2 \cdot 2^m = 2^{m+1}$.

  Para escribir ambos casos con una sola fórmula, usamos la función *techo*[**], donde si $x \in \mathbb{R}$, $\lceil x \rceil$ es igual al menor entero mayor o igual que x. Controlemos, si $n = 2m$ entonces $\lceil \frac{n}{2} \rceil = m$ y si $n = 2m + 1$ entonces $\lceil \frac{n}{2} \rceil = \lceil m + \frac{1}{2} \rceil = m + 1$.
- # de bits con un número par de 0's = 2^{n-1}.

  El número buscado es sin dudas

  $$\sum_{j \text{ par}} \binom{n}{2j}$$

[**] del inglés 'ceiling'

Más adelante veremos que este número es 2^{n-1} (será consecuencia del binomio de Newton). Un argumento distinto sería que, por simetría, hay tantos bits con cantidad par de ceros que con cantidad impar de ceros, luego el número buscado es la mitad del total $\frac{2^n}{2}$. ◊

Ejemplo: manos de póker. El póker se juega con un mazo francés de 52 cartas. Hay 13 valores $2, 3, \ldots, 10$, J, Q, K, A y 4 palos ♢, ♣, ♡, ♠. En la mano de póker se dan 5 cartas por jugador. Los distintos "juegos" que se pueden obtener son:

- *escalera real mayor* o *flor imperial* (royal flush): 5 cartas de valores consecutivos empezando desde el as y del mismo palo; e.g. A♡, K♡, Q♡, J♡, 10♡.
- *escalera real* o *escalera de color* (straight flush): 5 cartas de valores consecutivos y del mismo palo que no empiezan en as; e.g. 10♡, 9♡, 8♡, 7♡, 6♡.
- *escalera* (straight): 5 cartas de valores consecutivos sin importar el palo; e.g. 8♡, 7♣, 6♢, 5♡, 4♠.
- *color* (flush): 5 cartas del mismo palo, pero que no formen escalera; e.g. Q♠, 9♠, 7♠, 5♠, 2♠.
- *póker* (four of a kind): 4 cartas del mismo valor; e.g. J♡, J♣, J♢, J♠, 4♠.
- *full* (full house): 3 cartas del mismo valor y dos cartas del mismo valor (pierna + par); e.g. A♡, A♢, A♠, 7♡, 7♣.
- *trío* o *pierna* (three of a kind): 3 cartas del mismo valor y dos cartas de valores distintos; e.g. A♡, A♢, A♠, 7♡, 5♣.
- *par doble* (two pairs o pocket): 1 par de cartas del mismo valor y otro par de cartas del mismo valor, pero distinto al primero (2 pares que no formen poker); e.g. K♡, K♢, J♠, J♡, 8♣.
- *par*: 2 cartas de igual valor; e.g. 10♠, 10♡, Q♡, 7♢, 3♠.

Como no importa el orden, la cantidad de manos posibles es

$$\binom{52}{5} = \frac{52 \cdot 51 \cdot 50 \cdot 49 \cdot 48}{5!} = 2.598.960$$

Analicemos pues, cuantos juegos de cada tipo puede haber. Notar que los distintos juegos son excluyentes entre sí.

- Escalera real mayor: Debe ser A,K,Q,J,10 del mismo palo, luego sólo hay 4.
- Escalera real (no mayor): la escalera puede empezar en cualquiera de estos valores K,Q,J,$10, \ldots 5$ (A sirve de as o de 1) y hay 4 palos, luego hay $9\binom{4}{1} = 36$.
- Póker: son 4 cartas del mismo valor, y 13 valores posibles, luego hay $13 \cdot 48 = 624$.

- Full: son 3 cartas de un valor y 2 de otro, luego hay

$$13\binom{4}{3}12\binom{4}{2} = 13 \cdot 4 \cdot 12 \cdot 6 = 13 \cdot 48 \cdot 6 = 3.744$$

  Hay 6 veces "fulles" que "pókers".

- Color: son 5 cartas del mismo palo y, ojo, restamos las escaleras reales. Luego, hay

$$4\binom{13}{5} - 4 \cdot 10 = 4(13 \cdot 11 \cdot 9 - 10) = 5.108$$

- Escalera: 5 valores de cartas consecutivos, que no sean escalera real.

$$10 \cdot 4^5 - 4 \cdot 10 = 40(4^4 - 1) = 40 \cdot 255 = 10.200$$

- Pierna: 3 cartas del mismo valor, $aaabc$, luego hay

$$13\binom{4}{3}\binom{12}{2}4^2 = 13 \cdot 11 \cdot 6 \cdot 4^3 = 54.912$$

  Esto también es $13 \cdot 48 \cdot 88$, o sea 88 veces mas piernas que pókers y casi 15 veces mas piernas que fulles.

  También podemos contar de esta forma.

$$13\binom{4}{3}\binom{48}{2} - 13 \cdot 48 \cdot 6 = 13 \cdot 48(94 - 6) = 13 \cdot 48 \cdot 88$$

  Hay $13 \cdot 4$ formas de elegir un valor, digamos a, y los palos. De las 49 cartas que quedan no puedo elegir la a del palo que falta, por lo que en realidad me quedan 48 cartas. De éstas elijo 2 cualquiera, y restos los casos en que elegí dos del mismo valor, que en total me da una pierna.

- Par doble: 2 cartas de igual valor y 2 cartas de igual valor distinto del anterior, luego hay

$$\binom{13}{2}\binom{4}{2}^2(11 \cdot 4) = 13 \cdot 6^3 \cdot 44 = 123.552$$

  (elegimos los dos valores de los pares y luego la carta distinta).

- Par: 2 cartas del mismo rango, hay

$$13\binom{4}{2}\binom{12}{3}4^3 = 13 \cdot 12 \cdot 11 \cdot 10 \cdot 4^3 = 1.098.240$$

  Esto también es $13 \cdot 48 \cdot 88 \cdot 20$ es decir, $88 \cdot 20 = 1760$ veces mas que los pokers, un poco mas de 293 veces que los fulles y 20 veces mas que las piernas.

La suma de todos estos da $1.296.416$ casos. Si los restamos del total de manos vemos que hay $1.302.544$ manos en que no obtenemos ningún juego (por **PC**), que son aproximadamente la mitad.

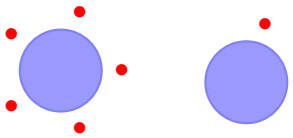
Ejemplo: 2 y 3 mesas. ¿De cuántas formas se pueden sentar 6 personas en 2 mesas si debe haber al menos una persona por mesa? ¿De cuántas formas se pueden sentar 6 personas en 3 mesas si debe haber al menos una persona por mesa?

- para 2 mesas, hay 3 casos: que en la primer mesa haya 5, 4 ó 3 personas y que en la segunda haya 1, 2 ó 3 personas, respectivamente. Consideramos los casos:

$$(i) \quad 5+1, \qquad (ii) \quad 4+2, \qquad (iii) \quad 3+3.$$

Usando lo que ya sabemos sobre como sentar a una mesa tenemos.

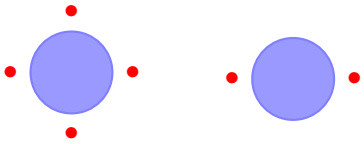
Caso (i):



Por **PM** hay

$$\binom{6}{5} 4!\, 0! = 6 \cdot 24 = 144$$

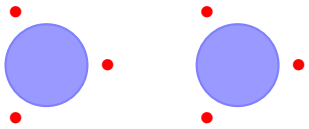
Caso (ii):



Por **PM** hay

$$\binom{6}{4} 3!\, 1! = 15 \cdot 6 = 90$$

Caso (iii):



Por **PM** hay

$$\tfrac{1}{2}\binom{6}{3} 2!\, 2! = 5 \cdot 4 \cdot 2 = 40$$

Notar que aquí tenemos que dividir por 2, ya que como las 2 mesas son de la misma cantidad de personas (3 y 3), la sentada a, b, c en la primera mesa y d, e, f en la segunda es considerada igual que la sentada d, e, f en la primera mesa y a, b, c en la segunda.

Finalmente, por **PA**, hay

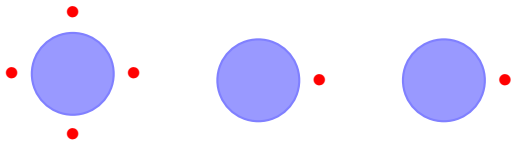
$$144 + 90 + 40 = 274$$

formas de sentar 6 personas en 2 mesas con al menos una persona por mesa.

- para 3 mesas, hay 3 casos

$$(i) \quad 4+1+1, \qquad (ii) \quad 3+2+1, \qquad (iii) \quad 2+2+2.$$

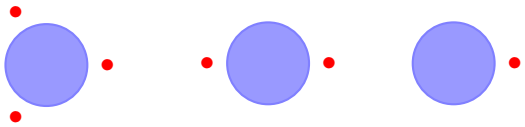
Caso (i):



Por **PM** hay

$$\tfrac{1}{2}\binom{6}{4}\binom{2}{1}3!0!0! = 90$$

Caso (ii):



Por **PM** hay

$$\binom{6}{3}\binom{3}{2}2!1! = 120$$

Caso (iii):

Por **PM** hay

$$\tfrac{1}{3!}\binom{6}{2}\binom{4}{2}1!1!1! = 15$$

Nuevamente, hemos tenido en cuenta las repeticiones. Por lo tanto, tuvimos que dividir por 2 en el primer caso porque hay dos mesas con 1 persona; y por 3! en el último caso, pues hay 3 mesas de 2 personas.

Finalmente, por **PA**, hay

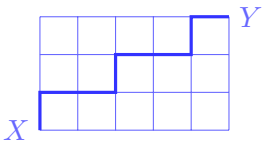
$$90 + 120 + 15 = 225$$

formas de sentar a 6 personas en 3 mesas con al menos una persona por mesa.

Pregunta. ¿De cuántas formas se pueden sentar n personas en k mesas si debe haber al menos una persona por mesa?

11.5.2. Caminos más cortos.

¿Cuántos caminos más cortos hay de X a Y, donde X es el borde inferior izquierdo e Y el borde superior derecho de una grilla 5×3? (pensar por ejemplo en un mapa urbano de 5×3 manzanas o 6×4 calles).



Sea

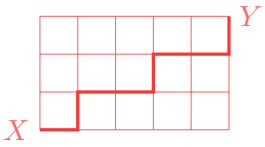
$$K = \{ \text{ caminos más cortos de } X \text{ a } Y \}$$

Cada camino en K consiste de 8 segmentos unidad contiguos, 5 horizontales y 3 verticales. Si denotamos por 0 a los segmentos horizontales y por 1 a los segmentos verticales, cada camino en K puede representarse de forma única por una 8-upla con cinco 0's y tres 1's. Sea B el conjunto de 8-uplas binarias con cinco 0's y tres 1's, es decir

$$B = \{(b_1, b_2, \ldots, b_8) \in \{0,1\}^8 \,:\, b_{i_j} = 1,\ 1 \le j \le 3;\ b_{i_k} = 0,\ 1 \le k \le 5\}$$

Luego, hay una biyección entre K y B.

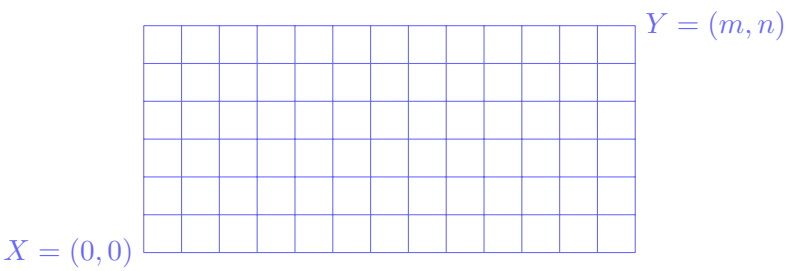
Por ejemplo, el camino dibujado arriba se corresponde de forma única con la 8-upla $(1,0,0,1,0,0,1,0)$. Recíprocamente, la 8-upla $(0,1,0,0,1,0,0,1)$ representa (sólo) el camino



Por el **PB**, tenemos

$$\#K = \#B = \binom{8}{3} = \frac{8!}{3!\,5!} = 8 \cdot 7 = 56$$

En general, supongamos que tenemos una grilla de $m \times n$ cuadros (o sea, $(m+1) \times (n+1)$ líneas).



Sea

$$K(m,n) = \{ \text{ caminos mas cortos de } (0,0) \text{ a } (m,n) \}$$

Identificamos a los caminos de $K(m,n)$ con las $(m+n)$-uplas binarias con exactamente m ceros (representando los segmentos horizontales) y exactamente n unos (representando los segmentos verticales). Luego, tenemos que

$$K_{m,n} = \#K(m,n) = \binom{m+n}{m} = \binom{m+n}{n} \tag{11.3}$$

O sea,

$$K_{m,n} = \frac{(m+n)!}{n!m!} = \frac{(m+n)\cdots(m+1)}{n!}$$

A partir de esta expresión, podemos obtener algunos resultados sencillos:

- $K_{m,n} = K_{n,m}$.
- $K_{m,0} = \binom{m}{0} = 1$.
- $K_{m,1} = \binom{m+1}{1} = m+1$.
- $K_{m,2} = \binom{m+2}{2} = \frac{1}{2}(m+2)(m+1)$.

Más interesantes son

$$K_{m,m} = \binom{2m}{m} = \frac{2m(2m-1)\cdots(m+2)(m+1)}{m(m-1)\cdots 2\cdot 1}$$
$$K_{2m,m} = \binom{3m}{m} = \frac{3m(3m-1)\cdots(2m+2)(2m+1)}{m(m-1)\cdots 2\cdot 1}$$

Esta última puede generalizarse para cualquier $k \geq 1$,

$$K_{km,m} = \binom{(k+1)m}{m} = \frac{((k+1)m)!}{(km)!m!} = \frac{((k+1)m)\cdots(km+2)(km+1)}{m(m-1)\cdots 2\cdot 1}$$

Este ejemplo satisface las 3 b's: bueno, bonito y barato!

11.5.3. Apareos

Sea X un conjunto con $2n$ elementos. Un *apareo* de X es una partición de X en 2-subconjuntos (conjuntos de pares). Una situación donde se dan los apareos es en los torneos de tenis o en las fases finales de campeonatos mundiales de fútbol, basquet, rugby, voley, hockey, etcétera. Hay 16 finalistas (octavos de final) y deben aparearse para jugar partidos elimatorios. Luego, los 8 que quedan (ganadores) vuelven a aparearse (cuartos de final), etcétera.

Por ejemplo, en el mundial de fútbol de Sudáfrica en 2010, los 8 equipos que llegaron a cuartos de final son: Alemania, Argentina, Brasil, España, Ghana, Holanda, Paraguay y Uruguay. Los cruces se dieron de la siguiente forma

Hol vs Bra	Uru vs Gha
Arg vs Ale	Par vs Esp

Podemos pensar entonces en el conjunto

$$F = \{\text{Ale, Arg, Bra, Esp, Gha, Hol, Par, Uru}\}$$

y en el apareo $\big\{\{\text{Hol}, \text{Bra}\}, \{\text{Uru}, \text{Gha}\}, \{\text{Arg}, \text{Ale}\}, \{\text{Par}, \text{Esp}\}\big\}$.

Queremos encontrar el número total de posibles apareos para un $2n$-conjunto X con $n \geq 1$. Damos a continuacion 3 formas de obtener este número.

(1) Sea x_1 un elemento cualquiera de X. Hay $2n-1$ formas de elegir un compañero x_1' para x_1. Ahora elegimos un elemento x_2 de X distinto de x_1, x_1'. Hay $2n-3$ formas de elegir un compañero x_2' para x_2. Iterando este proceso, vemos que habiendo elegido los pares $\{x_1, x_1'\}, \ldots, \{x_k, x_k'\}$, hay $2n-(2k-1)$ formas de elegir un compañero x_{k+1}' para un elemento $x_{k+1} \in X \smallsetminus \{x_1, x_1', \ldots, x_k, x_k'\}$. Por **PM** hay

$$(2n-1)(2n-3)\cdots 5 \cdot 3 \cdot 1 = (2n-1)!! \tag{11.4}$$

apareos posibles.

(2) Hacemos una lista con los n pares. Vemos que hay $\binom{2n}{2}$ formas de elegir el primer par, $\binom{2n-2}{2}$ formas de elegir el segundo par, $\binom{2n-4}{2}$ formas de elegir el tercer par, etc. Como el orden de los pares no nos interesa, el número total de apareos es

$$\frac{\binom{2n}{2}\binom{2n-2}{2}\cdots\binom{4}{2}\binom{2}{2}}{n!} \tag{11.5}$$

(3) Ordenamos los $2n$ elementos en una fila. Hay $(2n)!$ formas de hacer esto. Respetando ese orden, los agrupamos de 2 en 2 (lod 2 primeros un par, el tercero y cuarto otro par, etc). Como el orden de los n pares no interesa dividimos por $n!$ y como el orden de los elementos de cada uno de los pares no nos interesa, dividos por dos por cada par. Luego, el número de apareos es

$$\frac{(2n)!}{2^n\, n!} \tag{11.6}$$

Pareciera ser que obtuvimos 3 resultados distintos. No nos dejemos engañar por las apariencias y veamos que estas 3 expresiones son iguales. En primer lugar, cancelando telescópicamente vemos que (11.5) y (11.6) son iguales:

$$\frac{\binom{2n}{2}\binom{2n-2}{2}\cdots\binom{4}{2}\binom{2}{2}}{n!} = \frac{1}{n!}\cdot\frac{(2n)!}{2(2n-2)!}\cdot\frac{(2n-2)!}{2(2n-4)!}\cdot\frac{(2n-4)!}{2(2n-6)!}\cdots\frac{4!}{2\cdot 2!}\cdot\frac{2!}{2\cdot 0!} = \frac{(2n)!}{2^n\, n!}$$

Ahora escribiendo $(2n)!$ como el producto de los pares por el producto de los impares tenemos

$$\begin{aligned}(2n)! &= (2n)(2n-1)(2n-2)\cdots 4\cdot 3\cdot 2\\ &= \{(2n)(2n-2)(2n-4)\cdots 4\cdot 2\}\{(2n-1)(2n-3)(2n-5)\cdots 5\cdot 3\cdot 1\}\\ &= 2^n\{n(n-1)(n-2)\cdots 2\}\{(2n-1)(2n-3)(2n-5)\cdots 5\cdot 3\cdot 1\}\end{aligned}$$

de donde sale que (11.4) es igual a (11.6). Luego, hemos obtenido el siguiente resultado.

Proposición 11.9. *El número total de apareos de un $2n$-conjunto es*

$$\frac{(2n)!}{2^n\, n!} = \frac{1}{n!}\prod_{k=1}^{n}\tbinom{2k}{2} = \prod_{\substack{j=1\\ j\ impar}}^{2n-1}(2n-j) = (2n-1)!!$$

El símbolo $n!!$ denota el doble factorial de n definido en (5.3).

Ejemplo. Supongamos un torneo de fútbol con 32 equipos divididos en 8 zonas de 4 equipos cada una (como en los mundiales). Se clasifican los 2 primeros de cada zona y luego es por elimminación directa, es decir hay 8vos de final (16 equipos), 4tos de final (8 equipos), semifinal y final. Hay 32 campeones posibles, y hay $\binom{32}{2} = 16\cdot 31 = 496$ distintas finales posibles (a priori, antes del reparto de zonas). Nos preguntamos, ¿De cuántas formas distintas se puede llegar al campeón? Distingamos algunos casos.

• *Mundial Brasil 2014.* Aquí las zonas ya están determinadas por "sorteo" previo y las llaves y cruces predeterminadas según zonas y posiciones. En este caso, importa el orden en que clasifican en las zonas (para armar las llaves) y por lo tanto hay $(2\binom{4}{2})^8 = 12^8$ posibles formas en que pueden salir los 16 finalistas. De aquí en mas los cruces estan determinados (por ejemplo, 1ero grupo A vs 2do grupo B, etc). En 8vos de final hay 8 partidos y por lo tanto 2^8 formas distintas de obtener los 8 ganadores. En 4tos hay 4 partidos, por lo tanto 2^4 formas de obtener los 4 semifinalistas, luego 2^2 formas de obtener los 2 finalistas. Luego hay

$$(2\tbinom{4}{2})^8\, 2^8\, 2^4\, 2^2\, 2 = 12^8\, 2^{15} = 2^{31}\, 3^8 = 14.089.640.214.528$$

formas distintas de llegar al campeón!

• *Mundial con sorteo en los cruces.* Teniendo en cuenta los cruces, y usando la fórmula para los apareos, y el número es

$$\tbinom{4}{2}^8 \cdot \frac{16!}{2^8 8!}\cdot 2^8 \cdot \frac{8!}{2^4 4!}\cdot 2^4 \cdot \frac{4!}{2^2 2!}\cdot 2^2 \cdot 2$$

que calculando da

$$\begin{aligned} 6^8\, 2^{15}(15\cdot 13\cdots 3\cdot 1)(7\cdot 5\cdots 3\cdot 1)(3\cdot 1) &= 2^{31}\, 3^8(15\cdot 13\cdot 11\cdot 9\cdot 7^2\cdot 5^2\cdot 3^3) \\ &= 3.904.694.740.058.112.000 \end{aligned}$$

¡Casi 4 trillones! Este número es $638.512.875$ veces más grande que para el mundial sin sorteo.

• *Copa Famaf.* Aquí hay 32 equipos y las zonas y los cruces se sortean[***]. Notar que el número de formas de tener 8 zonas de 4 equipos es

$$\tbinom{32}{4}\tbinom{28}{4}\tbinom{24}{4}\tbinom{20}{4}\tbinom{16}{4}\tbinom{12}{4}\tbinom{8}{4}\tbinom{4}{4} = \tfrac{32!}{4!28!}\cdot\tfrac{28!}{4!24!}\cdot\tfrac{24!}{4!20!}\cdot\tfrac{20!}{4!16!}\cdot\tfrac{16!}{4!12!}\cdot\tfrac{12!}{4!8!}\cdot\tfrac{8!}{4!4!} = \tfrac{32!}{4!^8}$$

Este número es mayor que $2,39\times 10^{24}$, o sea mas de 2 cuatrillones!!

[***] aunque siempre gana el equipo de los matemáticos, por su gran despliegue y su fútbol exquisito.

A partir de aquí sigue como en el caso anterior y tenemos un total de

$$\frac{32!}{4!^8} \cdot 2^{31} \cdot 3^8 \cdot (15 \cdot 13 \cdot 11 \cdot 9 \cdot 7^2 \cdot 5^2 \cdot 3^3) > 2,15 \times 10^{46}$$

(más de 2 mil septillones...!?). ◊

11.5.4. Elegir distinguiendo (equipos con líderes)

Lo que sigue es una aplicación del método "elegir y ordenar". Se trata de elegir conjuntos distinguidos, es decir, nos preguntamos ¿de cuántas formas se pueden elegir k objetos de un total de n y luego, de entre estos, distinguir de alguna manera una cantidad m de ellos? Una forma práctica de pensar este problema es con equipos o comités.

Proposición 11.10. *Para toda tripla de enteros n, k, ℓ se tiene*

$$\binom{n}{k}\binom{k}{\ell} = \binom{n}{\ell}\binom{n-\ell}{k-\ell} \tag{11.7}$$

Demostración combinatoria. Podemos suponer que $0 \leq \ell \leq k \leq n$, de otra forma el resultado vale trivialmente. Contaremos un mismo número de dos formas distintas. Primero, notemos que podemos interpretar al número $\binom{n}{k}\binom{k}{\ell}$ como el número de formas de elegir un comité de k personas de un total de n y luego elegir ℓ líderes de entre éstas. Procediendo en el orden inverso, podemos elegir primero a los ℓ líderes de entre las n personas y completar el comité con $k-\ell$ personas de las $n-\ell$ que restan. Esto puede hacerse de $\binom{n}{\ell}\binom{n-\ell}{k-\ell}$ formas. Por lo tanto vale (11.7) □

Demostración algebraica. Por un lado tenemos

$$\binom{n}{k}\binom{k}{\ell} = \frac{n!}{k!(n-k)!} \cdot \frac{k!}{\ell!(k-\ell)!} = \frac{n!}{\ell!(n-k)!(k-\ell)!}$$

y por el otro

$$\binom{n}{\ell}\binom{n-\ell}{k-\ell} = \frac{n!}{\ell!(n-\ell)!} \cdot \frac{(n-\ell)!}{(k-\ell)!((n-\ell)-(k-\ell))!} = \frac{n!}{(n-k)!\ell!(k-\ell)!}$$

de donde la identidad sigue. □

En particular, si $\ell = 1$ tenemos

$$k\binom{n}{k} = n\binom{n-1}{k-1} \tag{11.8}$$

que se puede interpretar como el número de formas de elegir un comité con 1 presidente (o un equipo deportivo con un capitán, como ya hemos visto antes).

11.6. Acción básica: Ordenar con repeticiones

Volvamos al ejemplo de las bananas: ¿cuántas palabras se pueden formar con las letras de BANANA? Ahora que sabemos "elegir", podemos resolverlo de manera más sencilla. Hay $\binom{6}{3}$ formas de elegir los lugares para poner las A's; y de los 3 lugares que quedan, hay $\binom{3}{2}$ formas de elegir los 2 lugares para las N's. Por supuesto, el lugar para la B queda determinado (a la pobre no le queda opción). Luego, hay

$$\binom{6}{3}\binom{3}{2} = \frac{6!}{3!3!}\frac{3!}{2!1!} = \frac{6!}{3!2!} = 5\cdot 4\cdot 3 = 60$$

Generalizando el ejemplo anterior, podemos considerar el siguiente problema más general. Supongamos que tenemos n objetos de m clases distintas (por ejemplo m frutas distintas, siguiendo con el ejemplo frutal) y hay r_i objetos de la clase i para cada $i = 1, \dots, m$. Luego,

$$r_1 + r_2 + \cdots + r_m = n$$

Denotemos por

$$\binom{n}{r_1, r_2, \dots, r_m} = \begin{array}{c}\text{número de formas distintas de ordenar}\\ \text{los } n \text{ objetos de } m \text{ clases en una fila}\\ \text{donde hay } r_i \text{ objetos de clase } i\end{array} \tag{11.9}$$

Notemos que si $m = 1$ entonces $\binom{n}{r_1}$ es el número combinatorio que ya conocemos. Intentemos adivinar la fórmula para $\binom{n}{r_1,r_2,\dots,r_m}$, como hicimos previamente para $\binom{n}{k}$.

MÉTODO GENERAL I

Hay $\binom{n}{r_1}$ formas de elegir los lugares para los objetos de la clase r_1. Quedan $n - r_1$ lugares libres. Hay $\binom{n-r_1}{r_2}$ formas de elegir lugares para los objetos de la clase r_2. Luego, el número de formas de elegir los lugares para los objetos de la clase r_1 y r_2 es

$$\binom{n}{r_1}\binom{n-r_1}{r_2} = \frac{n!}{r_1!(n-r_1)!}\frac{(n-r_1)!}{r_2!(n-r_1-r_2)!} = \frac{n!}{r_1!r_2!(n-r_1-r_2)!}$$

Siguiendo así, hay $\binom{n-r_1-r_2}{r_3}$ formas de elegir lugares para los objetos de la clase r_3 y, en general, hay $\binom{n-r_1-r_2-\cdots-r_{k-1}}{r_k}$ formas de elegir lugares para los objetos de la clase r_k. Luego, es claro que el número buscado es

$$\binom{n}{r_1,\dots,r_m} = \binom{n}{r_1}\binom{n-r_1}{r_2}\binom{n-r_1-r_2}{r_3}\cdots\binom{n-r_1-r_2-\cdots r_{m-1}}{r_m}$$

y cancelando factores telescópicamente como en la identidad de arriba, finalmente llegamos a

$$\binom{n}{r_1,\dots,r_m} = \frac{n!}{r_1!\cdots r_m!}$$

ya que $(n - r_1 - \cdots r_m)! = 0! = 1$.

MÉTODO GENERAL II

Hay $n!$ formas de ordenar todos los objetos. Si tengo r_1 objetos a_1, r_2 objetos a_2, etcétera, los distinguimos

$$a_1^1, a_1^2, \dots, a_1^{r_1}, \qquad a_2^1, a_2^2, \dots, a_2^{r_2}, \qquad \dots, \qquad a_m^1, a_m^2, \dots, a_m^{r_m}$$

Para "desordenar", es decir para no contar repeticiones, dividimos por $r_i!$ para eliminar las repeticiones que vienen de las reordenaciones de los $a_i^1, a_i^2, \dots, a_i^{r_i}$ entre sí. Luego, hay

$$\binom{n}{r_1, \dots, r_m} = \frac{n!}{r_1! \cdots r_m!}$$

Proposición 11.11. *Para todo $n, r_1, \dots, r_m \in \mathbb{N}$ con $r_1 + r_2 + \cdots + r_m = n$ se tiene*

$$\binom{n}{r_1, \dots, r_m} = \prod_{j=1}^{m} \binom{n - r_1 - \cdots - r_j}{r_j} = \frac{n!}{r_1! \cdots r_m!} \tag{11.10}$$

Demostración. Por inducción en m. Supongamos que tenemos $k+1$ clases distintas de objetos. Pienso que tengo objetos de 2 clases, una clase formada por las viejas clases de tipo $1, 2, \dots, k$ y otra clase formado por los objetos de tipo $k+1$. Luego, tenemos

$$\binom{n}{r_1, \dots, r_{k+1}} = \binom{n}{r_1, \dots, r_k} \binom{n - (r_1 + \cdots + r_k)}{r_{k+1}}$$

y, por hipótesis inductiva, lo de arriba es igual a

$$\binom{n}{r_1} \binom{n - r_1}{r_2} \binom{n - r_1 - r_2}{r_3} \cdots \binom{n - r_1 - r_2 - \cdots - r_{m-1}}{r_m} = \frac{n!}{r_1! \cdots r_m!}$$

Y chau pichu. □

Notar que si $m = 2$ y $r_1 = k$, $r_2 = n - k$, entonces

$$\binom{n}{r_1, r_2} = \binom{n}{k}$$

Usando la proposición previa, es inmediato resolver el problema de cuántas palabras distintas se pueden formar con las letras de una palabra dada.

Ejemplo. (anagramas)

(1) BANANA. Hay 6 letras, 3 A's, 2 N's y una B. Luego se pueden formar

$$\binom{6}{3, 2, 1} = \frac{6!}{3!2!1!} = 60$$

palabras distintas, como ya sabíamos.

(2) OTORRINOLARINGOLOGO. Hay 19 letras: 6 O's, 3 R's, 2 I's, N's, L's y G's, una T y una A. Luego, hay

$$\binom{19}{6, 3, 2, 2, 2, 1, 1} = \frac{19!}{6!3!2!2!2!2!1!1!} = \frac{19!}{6!3!2^4} = 1.759.911.753.600$$

posibles anagramas de otorrinolaringólogo (ignorando el acento). ◊

11.7. Acción básica: Distribuir

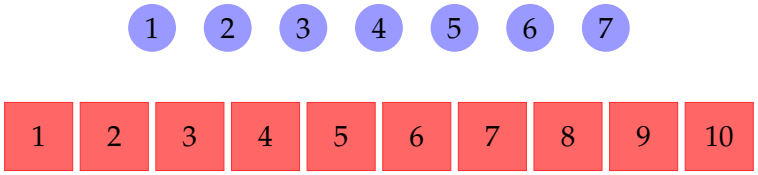
Queremos contar ahora el número de formas de distribuir r objetos en n categorías. Para fijar ideas, será conviene pensar por ejemplo que queremos

distribuir r bolitas en n cajas,

bajo ciertas condiciones adicionales. Tanto las bolas como las cajas pueden ser todas iguales (indistinguibles) o distintas (ordenadas, coloreadas, marcadas, diferentes tamaños, etc). En esta sección sólo nos ocuparemos del caso de cajas distintas. Más adelante diremos algo sobre el caso de cajas iguales.

11.7.1. Bolas y cajas distintas.

Distribuir r bolas distintas en n cajas distintas. Podemos pensar en bolas numeradas $b_1, b_2, \ldots, b_r$ y cajas numeradas $c_1, c_2, \ldots, c_n$. Por ejemplo, si $k = 7$ y $n = 10$ tenemos



(a) A lo sumo una bola por caja. Supongamos que en cada caja se puede poner como mucho 1 bola (luego $r \leq n$).

Una forma: hay n posibilidades para la primer bola (puedo colocarla en cualquiera de las n cajas). Luego quedan $n-1$ lugares para la segunda, etc. Por el principio de multiplicación, resulta

$$n(n-1)(n-2)\cdots(n-(r-1)) = n(n-1)(n-2)\cdots(n-r+1)$$

Otra forma: elegir r cajas de las n donde poner las bolitas y luego considerar los $r!$ órdenes distintos que hay para cada elección de las cajas, o sea $r!\binom{n}{r}$.

Luego, hay

$$\binom{n}{r} r! = n(n-1)(n-2)\cdots(n-r+1) = \frac{n!}{(n-r)!}$$

formas de distribuir las bolas de la forma buscada.

(b) Sin restricciones en las cajas. Luego, cada caja puede contener n bolas. Hay n posibilidades para la primer bola, n para la segunda, etc. Por **PM** el número de formas es

$$\underbrace{n \cdot n \cdots n}_{r-\text{ veces}} = n^r$$

(c) Cualquier número de bolas por caja, pero importa el orden. La primera bola b_1 tiene n posibilidades. Sea c_1 la caja elegida para la bola b_1. La segunda bola b_2 tiene $n-1$ cajas distintas o puede ir en la caja c_1 pero a la izquierda o a la derecha de de b_1. Luego hay

$$(n-1) + 2 = n + 1$$

posibilidades. Para la bola b_3, si b_1 y b_2 están en cajas distintas, entonces hay

$$(n-2)+4 = n+2$$

posibilidades, mientras que si b_1 y b_2 están en la misma caja entonces hay

$$(n-1)+3 = n+2$$

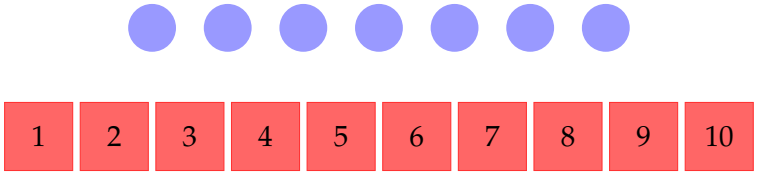
posibilidades. En ambos casos tenemos $n+2$ posibilidades para b_3. En general, tenemos $n+(j-1)$ posibilidades para la bola b_j. Luego, por **PM**, hay

$$n(n+1)(n+2)\cdots(n+(r-1)) = \frac{(n-1+r)!}{(n-1)!}$$

de distribuir las bolas de la manera deseada.

11.7.2. Bolas iguales en cajas distintas.

Ahora queremos distribuir r bolas iguales en n cajas distintas bajo ciertas condiciones. Por ejemplo, si $k = 7$ y $n = 10$ tenemos

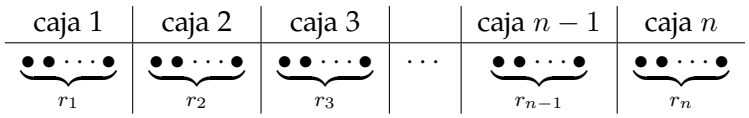


(a) A lo sumo 1 bola por caja. Esto solo puede pasar si s $r \leq n$. Hay una correspondencia 1-1 entre las formas de distribuir las bolas y de elegir r cajas para poner 1 bola en cada una. Luego hay

$$\binom{n}{r}$$

formas.

(b) Sin restricciones en el número de bolas. Pensamos que ponemos r_1 bolas en la caja 1, r_2 bolas en la caja 2, etc, hasta que ponemos r_n bolas en la caja n, como en la figura



de modo que

$$r_1 + r_2 + \cdots + r_n = n, \qquad r_1, r_2, \ldots, r_n \geq 0$$

Y acá viene la magia. Representamos a cada una de estas distribuciones con una lista de 0's y 1's. Los 0's corresponden a las bolas y los 1's corresponden a las $n-1$ líneas verticales que separan a las bolas de las distintas cajas. O sea, por el principio de biyección, el número

de formas de repartir r bolas en n cajas sin restricciones es igual al número de $r+(n-1)$ uplas de 0's y 1's con exactamente r ceros y $n-1$ unos, que es simplemente

$$\binom{r+n-1}{r} = \binom{r+n-1}{n-1}$$

o sea

$$\frac{(r+n-1)!}{r!(n-1)!} = \frac{(r+n-1)\cdots(n+1)n}{r!}$$

No se puede hacer mas fácil!

(c) Cada caja contiene por lo menos 1 bola. Luego $r \geq n$. Coloquemos 1 bola en cada caja (hay una sola forma de hacer esto!). Ahora colocamos las $r-n$ bolas que sobran en las n cajas sin restricciones. Por el **PM** y el caso anterior, hay

$$\binom{(r-n)+n-1}{r-n} = \binom{r-1}{r-n} = \binom{r-1}{n-1}$$

formas de colocar r bolas en n cajas sin que haya ninguna vacía.

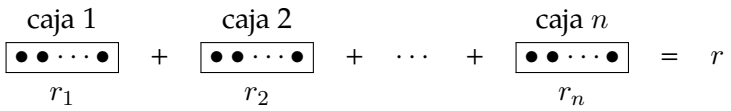
Como aplicación, veamos un ejemplo interesante sobre soluciones enteras de una ecuación lineal.

Ejemplo (Soluciones enteras)**.** Si $r \geq 0$ y $n \geq 1$, ¿cuántas soluciones enteras tiene la ecuación

$$x_1 + x_2 + \cdots + x_n = r$$

con $x_1, x_2, \ldots, x_n \geq 0$?

Toda solución entera no negativa $(r_1, r_2, \ldots, r_n)$ de la ecuación de arriba corresponde a distribuir r objetos idénticos en n cajas distintas como sigue



Por el **PB** y 11.7.2(b), el número deseado es

$$\binom{r+n-1}{r}$$

11.8. Funciones y conteo

11.8.1. Funciones, cardinal y principios básicos

Recordemos que una función $f : X \to Y$ se dice inyectiva si $f(x) \neq f(y)$ para $x \neq y$...

Recordemos también que decimos que un conjunto (finito) X tiene cardinal n, con $n \in \mathbb{N}_0$ si existe una biyección entre X e $I_n = \{1, 2, \ldots, n\}$. En este caso escribimos $|X| = n$. También se suele usar la notación $\#X = n$. Nosotros usaremos indistintamente ambas.

Por conveniencia, si $0 \leq m \leq n$, denotamos por

$$[\![m, n]\!] = \{k \in \mathbb{N} : m \leq k \leq n\} = \{m, m+1, \ldots, n-1, n\} = I_n \setminus I_{m-1}$$

al intervalo de números naturales entre m y n inclusive. En particular, $[\![1, n]\!] = I_n$.

Nuestra meta es mostrar que el concepto de cardinal de un conjunto, es decir, el número de elementos (si este conjunto es finito), está bien definido. Es decir que si un conjunto tiene cardinal n y cardinal m entonces $n = m$. En otras palabras, un conjunto no puede tener dos cardinales distintos.

Veamos un resultado que es intuitivamente claro, aunque hay que probarlo, y que tendrá consecuencias importantes.

Teorema 11.12. *Sea $m, n \in \mathbb{N}$. Si $n > m$, no existe una función inyectiva del intervalo $[\![1, n]\!]$ en el intervalo $[\![1, m]\!]$. Es decir, si $f : [\![1, n]\!] \to [\![1, m]\!]$, f no es inyectiva.*

Demostración. Sea

$$H = \{n \in \mathbb{N} : \exists m \in \mathbb{N} \text{ y } f : [\![1, n]\!] \to [\![1, m]\!] \text{ tal que } m < n \text{ y } f \text{ es inyectiva}\}.$$

Queremos ver que $H = \varnothing$. Supongamos que $H \neq \varnothing$. Por el principio de buena ordenación, existe un primer elemento $h \in H$ de H. Por definición de H, existe una función inyectiva

$$f : [\![1, h]\!] \to [\![1, m]\!]$$

con $m < h$. Si $m = 1$ entonces f no es biyectiva. Si $1 < h < m$ hay dos posibilidades:

$$f(h) = m \qquad \text{ó} \qquad f(h) = c \quad \text{con} \quad c < m.$$

– Si $f(h) = m$ entonces podemos restringir f al intervalo $[\![1, h-1]\!]$ y tenemos la función

$$f : [\![1, h-1]\!] \to [\![1, m-1]\!]$$

que es inyectiva. Luego, $h - 1 \in H$. Pero esto es absurdo pues h es el primer elemento de H.

– Ahora, si $f(h) = c < m$, nos fabricaremos una nueva función inyectiva $f^* : [\![1, h]\!] \to [\![1, m]\!]$ con $f^*(h) = m$ y el argumento es como antes. Para ello, componemos f con la función biyectiva $g : [\![1, m]\!] \to [\![1, m]\!]$ dada por

$$g(c) = m, \quad g(m) = c \quad \text{y} \quad g(x) = x, \ x \neq c, m.$$

Luego, la función $f^* = g \circ f : [\![1, h]\!] \to [\![1, m]\!]$ satisface

$$f^*(h) = g(f(h)) = g(c) = m$$

y f^* es inyectiva, por ser composición de funciones inyectivas. Ahora, si restringimos f^* al intervalo $[\![1, h-1]\!]$, tenemos que $f^* : [\![1, h-1]\!] \to [\![1, m-1]\!]$ continúa siendo inyectiva. Luego, $h - 1 \in H$, y esto es absurdo pues h es el primer elemento de H.

De esta manera, $H = \varnothing$ y esto prueba el teorema. □

Corolario 11.13. *Si $m, n \in \mathbb{N}$ y $n \neq m$ entonces no existe una función biyectiva de $[\![1, n]\!]$ en $[\![1, m]\!]$. En otras palabras, si $f : [\![1, n]\!] \to [\![1, m]\!]$ es biyectiva, entonces $n = m$.*

Demostración. Como f es biyectiva, tanto f como f^{-1} son inyectivas, y por el teorema anterior, f inyectiva implica $n \leq m$ y similarmente, f^{-1} inyectiva implica $m \leq n$. Luego $n = m$. □

Este resultado asegura que el cardinal de un conjunto finito está bien definido. Aclaremos esto. Supongamos que tenemos que $|X| = n$ y $|X| = m$. Esto quiere decir que existen funciones biyectivas $f : X \to [\![1, n]\!]$ y $g : X \to [\![1, m]\!]$. Luego, la composición $h = g \circ f : [\![1, n]\!] \to [\![1, m]\!]$ es biyectiva. Por el coralario anterior, tal función no puede existir si $n \neq m$. Así, $n = m$. Es decir, el número de elementos de un conjunto finito es un número bien determinado.

Corolario 11.14. *Sea $f : [\![1, n]\!] \to [\![1, n]\!]$. Entonces f es inyectiva si y sólo si f es sobreyectiva.*

Demostración. FALTA.. □

Ahora estamos en condiciones de probar los principios de adición y multiplicación del Capítulo 11.

Teorema 11.15 (principio de adición)**.** *Si $A_1, A_2, \ldots, A_n$ son conjuntos disjuntos 2 a 2, o sea $A_i \cap A_j = \varnothing$ para todo $1 \leq i, j \leq n$ con $i \neq j$, entonces*

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = |A_1| + |A_2| + \cdots + |A_n|.$$

Demostración. Veamos que si A y B son conjuntos finitos disjuntos entonces

$$|A \cup B| = |A| + |B|.$$

Supongamos que $|A| = n$ y $|B| = m$. Luego, existen funciones biyectivas $f : [\![1, n]\!] \to A$ y $g : [\![1, m]\!] \to B$. Basta ver que existe una función biyectiva $h : [\![1, n + m]\!] \to A \cup B$. Notar que

$$[\![1, n + m]\!] = [\![1, n]\!] \cup [\![n + 1, n + m]\!]$$

y que la función $k : [\![n + 1, n + m]\!] \to [\![1, m]\!]$ definida por $k(x) = x - n$ es claramente biyectiva, con inversa $k^{-1}(x) = x + n$. Luego, la función $h : [\![1, n]\!] \cup [\![n + 1, n + m]\!] \to A \cup B$ definida por

$$h(x) = \begin{cases} f(x) & \text{si } x \in [\![1, n]\!] \\ g(k(x)) & \text{si } x \in [\![n + 1, n + m]\!] \end{cases}$$

es biyectiva por construcción, pues A y B son disjuntos.

El caso general sale por inducción y los dejamos como ejercicio. □

Teorema 11.16 (principio de multiplicación)**.** *Si $A_1, A_2, \ldots, A_n$ son conjuntos finitos entonces*

$$|A_1 \times A_2 \times \cdots \times A_n| = |A_1| \cdot |A_2| \cdots |A_n|.$$

Demostración. Veamos que $|A \times B| = |A| \times |B|$. Si $|A| = n$ y $|B| = m$, existen funciones biyectivas $f : [\![1, n]\!] \to A$ y $g : [\![1, m]\!] \to B$. Luego, podemos escribir $A = \{a_1, a_2, \ldots, a_n\}$ y $B = \{b_1, b_2, \ldots, b_m\}$ donde $a_i = f(i)$ para $1 \leq i \leq n$ y $b_j = g(j)$ para $1 \leq j \leq m$. Tenemos que

$$A \times B = (A \times \{b_1\}) \cup (A \times \{b_2\}) \cup \cdots \cup (A \times \{b_m\})$$

y la unión es disjunta. Para cada j, se tiene $A \times \{b_j\} = \{(a_1, b_j), (a_2, b_j), \ldots, (a_n, b_j)\}$ y por lo tanto $|A \times \{b_j\}| = |A| = n$. Para cada $1 \leq j \leq m$, la biyeccion entre $A \times \{b_j\}$ y A está dada por $(a, b_j) \mapsto a$. Luego, por el principio de adición, tenemos

$$|A \times B| = |A \times \{b_1\}| + |A \times \{b_2\}| + \cdots + |A \times \{b_m\}| = m \cdot n = |A| \cdot |B|$$

como se quería ver. El caso general sale por inducción y lo dejamos como ejercicio. □

11.8.2. El principio del palomar

El Corolario 11.14 suele llamarse *principio de los casilleros* o *principio del palomar* (por "pigeonhole principle" en inglés) o también *principio de la cajonera de Dirichlet*.

Parafraseando el enunciado de dicho resultado, tenemos

PRINCIPIO DEL PALOMAR. *Si n objetos son distribuidos en m casillas y $n > m$ entonces hay al menos una casilla que contiene al menos 2 objetos.*

Ejemplo.

(1)

(2)

(3) En la ciudad de Córdoba (y en cualquier ciudad con más de un millón de habitantes) hay por lo menos 2 personas con el mismo número de pelos en la cabeza.

◊

Ejemplo. En todo conjunto de n personas, con $n \geq 2$, hay (por lo menos) 2 personas con el mismo número de amigos.

Sea $X = \{x_1, \ldots, x_n\}$ un conjunto de n-personas. Suponemos que si x_i es amiga de x_j entonces x_j es amiga de x_i, para toda $1 \leq i, j, \leq n$ (en particular, si $i = j$, toda persona es amiga de si misma) y lo denotamos por $x_i \sim x_j$. Sea f la función que cuenta el número de amigos de cada persona en X, es decir

$$f : X \to \{1, 2, \ldots, n\}$$

definida por

$$f(x_i) = \#\{j \in I_n : x_j \sim x_i\}.$$

Si alguien tiene n amigos, entonces es amigo de todas las personas de X. Luego, no puede haber una persona con un único amigo (el mismo!). De esta manera, 1 y n no pueden estar ambas en $\mathrm{Im}(f)$. Luego,

$$|\operatorname{Im} f| < n \qquad \text{y} \qquad |X| = n.$$

Por el PP, existen $x_i, x_j \in X$ con $i \neq j$, tales que $f(x_i) = f(x_j)$. Es decir, hay 2 personas en X con el mismo número de amigos ($2 \leq f(x_i) \leq n - 1$). ◊

Una versión más general de este principio es el siguiente.

Proposición 11.17 (Principio del palomar generalizado)**.** *Sean $k, n \in \mathbb{N}$. Si al menos $kn+1$ objetos son distribuidos en n casilleros, entonces al menos uno de los casilleros debe contener al menos $k+1$ objetos.*

Demostración. Si todos los casilleros tuvieran menos de $k+1$ objetos (o sea $\leq n$), entonces en total habría a lo sumo kn, lo cual es absurdo pues hay $kn+1$. □

Ejemplo.

11.8.3. El principio de inclusión-exclusión

Cuando los conjuntos A y B no son disjuntos, el principio de adición no vale. Sin embargo podemos calcular igual el cardinal de $A \cup B$. Para 2 conjuntos cualesquiera A y B se tiene

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

Esto se llama el *principio de inclusión-exclusión* (para dos conjuntos).

Como una aplicación interesante del principio de inlcusión-exclusión, veamos una fórmula cerrada para los números de Stirling de segunda clase. (ver http://www.ams.org/bookstore/pspdf/st
65-prev.pdf pagina 196)

11.8.4. Contando funciones

Sean A y B dos conjuntos finitos. Denotemos por

$$\begin{aligned}
\mathcal{F}(A,B) &= \text{el número de funciones de } A \text{ en } B,\\
\mathcal{F}_i(A,B) &= \text{el número de funciones inyectivas de } A \text{ en } B,\\
\mathcal{F}_b(A,B) &= \text{el número de funciones biyectivas de } A \text{ en } B,\\
\mathcal{F}_s(A,B) &= \text{el número de funciones sobreyectivas de } A \text{ en } B.
\end{aligned}$$

Es claro que

$$\mathcal{F}_b(A,B) \subseteq \mathcal{F}_i(A,B) \subseteq \mathcal{F}(A,B).$$

Definimos los números

$$\begin{aligned}
\mathcal{F}(n,m) &= \#\mathcal{F}(I_n, I_m) = \#\mathcal{F}(A,B),\\
\mathcal{I}(n,m) &= \#\mathcal{F}_i(I_n, I_m) = \#\mathcal{F}_i(A,B),\\
\mathcal{B}(n,m) &= \#\mathcal{F}_b(I_n, I_m) = \#\mathcal{F}_b(A,B),\\
\mathcal{S}(n,m) &= \#\mathcal{F}_s(I_n, I_m) = \#\mathcal{F}_s(A,B),
\end{aligned}$$

donde A y B son conjuntos finitos de cardinal n y m respectivamente.

Calcularemos dichos números. Por el principio de biyeccion, basta considerar $A = I_n$ y $B = I_m$. El caso de las funciones sobreyectivas es mas delicado y lo veremos mas adelante.

Ejemplo. (1) $f : \{1, 2\} \to \{1, 2, 3\}$,
(2) $f : \{1, 2, 3\} \to \{1, 2\}$
(3) $f : \{1, 2, 3\} \to \{1, 2, 3\}$.
De estas, ¿cuántas inyectivas, sobreyectivas y biyectivas hay?

Teorema 11.18. *Para todo par de naturales n y m se cumple*

(a) $\mathcal{F}(n, m) = m^n$.

(b) $$\mathcal{I}(n, m) = \begin{cases} \frac{m!}{(m-n)!} = m(m-1)\cdots(m-n+1) & n \le m, \\ 0 & n > m. \end{cases}$$

(c) $$\mathcal{B}(n, m) = \begin{cases} n! & n = m, \\ 0 & n \neq m. \end{cases}$$

(d) $$\mathcal{S}(n, m) = \begin{cases} \sum_{k=0}^{m} (-1)^k \binom{m}{k} (m-k)^n & n \ge m, \\ 0 & n < m. \end{cases}$$

En particular,

$$\mathcal{I}(n, n) = \mathcal{B}(n, n) = \mathcal{S}(n, n) = n!$$

Demostración. La expresión para las funciones sobreyectivas sale de aplicar una version mas general del principio de inclusion-exclusion, que no veremos por ahora. □

Observación. $\mathcal{F}(n, m)$ también puede ser visto como el número de formas de distribuir n objetos distintos in m cajas de modo que no queden cajas vacías.

La fórmula para $\mathcal{S}(n, m)$ vale en realidad para cualquier n y m. Como sabemos que $\mathcal{S}(n, m) = 0$ si $n < m$, en particular tenemos la identidad

$$\sum_{k=0}^{m} (-1)^k \binom{m}{k} (m-k)^n = 0 \qquad n < m.$$

Además, de $\mathcal{S}(n, n) = \mathcal{B}(n, n) = n!$ obtenemos la identidad

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} (n-k)^n = n!$$

¡Ya nos habíamos topado antes con esta expresión! (ver (12.19) y (12.24)).

11.9. Ejercicios

> *"[...] A cada uno de los muros de cada hexágono corresponden cinco anaqueles; cada anaquel encierra treinta y dos libros de formato uniforme; cada libro es de cuatrocientas diez páginas; cada página, de cuarenta renglones; cada renglón, de unas ochenta letras de color negro. También hay letras en el dorso de cada libro; [...] todos los libros,*

por diversos que sean, constan de elementos iguales: el espacio, el punto, la coma, las veintidós letras del alfabeto. [...] No hay en la vasta Biblioteca, dos libros idénticos. De esas premisas incontrovertibles dedujo que la Biblioteca es total y que sus anaqueles registran todas las posibles combinaciones de los veintitantos símbolos ortográficos (número, aunque vastísimo, no infinito) o sea todo lo que es dable expresar: en todos los idiomas. Todo [...]", fragmento de "La Biblioteca de Babel" de Jorge Luis Borges.

Ejercicio 11.1. ¿Cuántos números de cinco cifras se pueden formar utilizando los dígitos 1, 2, 3, 5, 6, 7 y 9 con la condición de que ...

(i) ... todas las cifras son distintas?

(ii) ... todas las cifras son iguales?

(iii) ... el número obtenido sea mayor que 32992?

(iv) ... el número obtenido sea múltiplo de 4?

(v) ... el número obtenido sea capicúa?

(vi) ... el número obtenido sea par y capicúa?

Ejercicio 11.2. La cantidad de dígitos o cifras de un número se cuenta a partir del primer dígito no nulo. Por ejemplo, el número 0035010 tiene 5 dígitos. ¿Cuántos número de 6 cifras pueden formarse con los dígitos de 112300?

Ejercicio 11.3. Vamos a hacerles un regalo a Ricardo y a Paulo, y decidimos regalarles dos camisetas de fútbol a cada uno. Sabemos que Ricardo es hincha de Independiente y detesta a Racing y Boca, y que Paulo es hincha de River y detesta a Boca. En la tienda de camisetas nos ofrecieron 4 camisetas distintas de cada uno de los equipos grandes de Argentina (Independiente, River y Boca), 3 de equipos de Córdoba, otras 5 de otros equipos de Argentina y 10 de equipos extranjeros.

(i) ¿De cuántas formas podemos hacer que ambos estén contentos (esto es, regalarles camisetas de sus respectivos equipos)?

(ii) ¿De cuántas formas podemos hacer los regalos, donde una sea la de su respectivo equipo y otra sea de un equipo que no le desagrade?

(iii) ¿Y si queremos hacerles una broma y regalarles a cada uno dos camisetas, donde al menos una es de un equipo que no quieren?

(iv) ¿De cuántas formas podemos hacer que solamente Ricardo se enoje?

Ejercicio 11.4. La clave alfanumérica de un banco debe contener entre 6 y 8 caracteres. ¿Cuántas claves posibles hay si debe contener al menos una letra y al menos un dígito?

Ejercicio 11.5. (i) ¿Cuántos caminos diferentes en $\mathbb{R}^2$ hay entre $(0,0)$ y $(7,7)$ si cada camino se construye moviéndose una unidad a la derecha o una unidad hacia arriba en cada paso?

(ii) ¿Cuántos caminos hay entre $(2,7)$ y $(9,14)$?

(iii) Deduzca la fórmula general para hallar la cantidad de caminos entre $(0,0)$ y (n,m) con $n, m \in \mathbb{N}$.

Ejercicio 11.6. En el primer piso de un edificio trabajan 30 hombres y 17 mujeres. En el segundo piso trabajan 25 hombres y 33 mujeres. ¿De cuántas maneras se puede formar un equipo de 3 personas, 2 hombres y 1 mujer, si ...

(i) ... todas las personas del equipo deben pertenecer al mismo piso?

(ii) ... debe haber al menos una persona de cada piso?

(iii) ... la mujer debe pertenecer al segundo piso?

Ejercicio 11.7. El truco se juega con un mazo de 40 cartas y se reparten 3 cartas a cada jugador. Obtener el 1 de espada (el macho) es muy bueno. También lo es, por distintos motivos, obtener un 7 y un 6 del mismo palo (tener 33). ¿Qué es más probable: obtener el macho o tener 33?

Ejercicio 11.8. Mostrar que si uno arroja un dado n veces y suma todos los resultados obtenidos hay $\frac{6^n}{2}$ formas distintas de obtener un número par.

Ejercicio 11.9. (i) ¿De cuántas maneras distintas pueden sentarse 6 hombres y 6 mujeres en una mesa circular si nunca deben quedar 2 mujeres juntas?

(ii) Ídem pero con 10 hombres y 7 mujeres.

Ejercicio 11.10. ¿De cuántas formas se pueden distribuir 14 libros distintos entre 2 personas de modo tal que cada persona reciba al menos 3 libros?

Ejercicio 11.11. (i) ¿De cuántas formas distintas pueden ordenarse las letras de la palabra MATEMÁTICA?

(ii) Ídem con las palabras ÁLGEBRA y GEOMETRÍA.

(iii) ¿De cuántas maneras distintas pueden ordenarse las letras de la palabra MATEMÁTICA si se pide que las consonantes y las vocales se alternen?

Ejercicio 11.12. Con 20 socios de un club se desean formar 5 listas electorales disjuntas. Cada lista consta de un presidente, un tesorero y dos vocales. ¿De cuántas formas puede hacerse?

Ejercicio 11.13. Demostrar que:

$$\text{(i)}\ \binom{n}{k} k = n\binom{n-1}{k-1}. \quad \text{(ii)} \sum_{k=0}^{n} k\binom{n}{k} = n2^{n-1}. \quad \text{(iii)} \sum_{k=0}^{n} k^2\binom{n}{k} = n(n+1)2^{n-2}.$$

Ejercicio 11.14. A los problemas anteriores resolverlos en forma combinatoria si lo hizo de alguna otra manera y viceversa.

Ejercicio 11.15. (i) Probar que

$$\sum_{k=0}^{m} \binom{n+k}{k} = \binom{n+m+1}{m}.$$

(II) Probar la misma identidad de la parte (i) pero de modo combinatorio.

(III) Probar que

$$\sum_{k=0}^{n} \binom{n}{k}^2 = \binom{2n}{n}.$$

Ejercicio 11.16. En un grupo de 7 personas las sumas de sus edades es 332. Probar que se pueden elegir 3 de ellas tal que la suma de sus edades sea por lo menos 143.

Ejercicio 11.17. Si se distribuyen al azar los números del 1 al 10 alrededor de un círculo, probar que existen 3 números consecutivos tales que su suma es al menos 17.

Ejercicio 11.18. Se sientan 9 hombres y 7 mujeres alrededor de una mesa circular. Probar que hay dos hombres sentados en posiciones diametralmente opuestas.

Ejercicio 11.19. Se tiene un tablero de 3×3 y se coloca en cada casilla 1 ó -1 ó 0. Probar que en el conjunto formado por las sumas de: cada fila, de cada columna y de cada diagonal hay dos que coinciden.

Ejercicios complementarios

Ejercicio 11.20. (I) ¿Cuántos números de cinco cifras hay?

(II) ¿Cuántos números pares de 5 dígitos hay?

(III) ¿Cuántos números de 5 dígitos existen con sólo un 3?

(IV) ¿Cuántos números capicúas de 5 dígitos existen?

(V) ¿Cuántos números capicúas de a lo sumo 5 dígitos hay?

(VI) ¿Cuántos números múltiplos de 5 y de a lo sumo 5 dígitos hay?

Ejercicio 11.21. De una caja que contiene 122 bolillas numeradas de 1 a 122 se extraen 5 bolillas. ¿Cuántos resultados posibles hay si ...

(I) ... las bolillas se extraen una a la vez sin reposición?

(II) ... las bolillas se extraen todas juntas?

(III) ... las bolillas se extraen una a la vez con reposición?

Ejercicio 11.22. (I) Dadas dos rectas paralelas en el plano se marcan n puntos distintos sobre una y m puntos distintos sobre la otra. ¿Cuántos triángulos se pueden formar con vértices en esos puntos?

(II) ¿Cuántas diagonales tiene un polígono regular de n lados? Resolverlo de modo combinatorio.

Ejercicio 11.23. Dados $m, k, n \in \mathbb{N}$ tales que $m \leq k \leq n$, probar que

(i) $\binom{n}{k}\binom{k}{m} = \binom{n}{m}\binom{n-m}{k-m}$. (ii) $\sum_{k=0}^{n}(-1)^k k\binom{n}{k} = 0$.

(iii) $\binom{2n}{2} = 2\binom{n}{2} + n^2$. (iv) $\binom{3n}{3} = 3\binom{n}{3} + 6n\binom{n}{2} + n^3$.

Ejercicio 11.24. A los problemas anteriores resolverlos en forma combinatoria si lo hizo de alguna otra manera y viceversa.

Ejercicio 11.25. Probar la siguiente identidad y concluir que $\binom{2n}{n}$ es par

$$\sum_{j=0}^{n}\binom{2n}{j} = \frac{1}{2}\left(2^{2n} + \binom{2n}{n}\right).$$

Ejercicio 11.26. ¿De cuántas maneras pueden sentarse 129 personas en un teatro que tiene 152 asientos numerados?

Ejercicio 11.27. Un bolillero contiene n bolillas numeradas de 1 a n. Si primero se extrae una bolilla y luego se lanza una moneda tantas veces como indique la bolilla: ¿Cuántos resultados posibles hay?

Ejercicio 11.28. Si uno tiene 8 CDs distintos de rock, 7 CDs distintos de música clásica y 5 CDs distintos de cuarteto: ¿Cuántas formas hay de seleccionar ...

(I) ... 3 CDs?

(II) ... 3 CDs, uno de cada tipo?

(III) ... 3 CDs de modo que no haya más de dos tipos distintos?

Ejercicio 11.29. Se extraen 3 cartas de un mazo de 40 cartas españolas. Calcular cuántas formas hay de que ocurra que ...

(I) ... salgan más pares que impares.

(II) ... todas sean caballos.

(III) ... todas sean copas.

(IV) ... ninguna sea de copas.

Ejercicio 11.30. Se arroja una moneda 7 veces. Calcular cuántas formas hay de que ...

(I) ... salga una cantidad impar de caras.

(II) ... salgan exactamente 5 caras.

(III) ... salgan por lo menos 4 caras.

Ejercicio 11.31. ¿De cuántas formas se pueden fotografiar 7 matrimonios en una hilera de tal modo que cada hombre aparezca junto a su esposa?

Ejercicio 11.32. ¿Cuántas palabras se pueden formar permutando las letras de BIBLIOTECARIA SI ...

(I) ... todas las vocales están juntas?

(II) ... la letra T está a la derecha de la C?

(III) ... la letra T está a la derecha de la C y la C de la R?

(IV) ... las dos A están juntas?

Ejercicio 11.33. Dado un conjunto A con $3n$ elementos, $n \in \mathbb{N}$, determinar la cantidad de relaciones de equivalencia en A tales que para todo $a \in A$, la clase de equivalencia de a tiene n elementos.

Ejercicio 11.34. Dado un conjunto de n puntos, donde tres puntos cualesquiera no están alineados entre ellos, determinar de cuántas formas pueden dibujarse un triángulo y un segmento unido a uno de sus vértices.

Ejercicio 11.35. Se tienen 900 tarjetas, numeradas de 100 a 999. Se van sacando tarjetas de a una, y se anota en el pizarrón la suma de los dígitos del número de la tarjeta. ¿Cuántas tarjetas se deben sacar para garantizar que haya un número que se repita 3 veces en el pizarrón?

Ejercicio 11.36. Se eligen 10 números distintos entre 1 y 100. Probar que existen dos subconjuntos disjuntos no vacíos tales que las sumas de sus elementos coinciden.

Ejercicio 11.37. Se tiene un tablero de 3×7 y se coloca en cada casilla una ficha blanca o una negra. Probar que existen cuatro fichas del mismo color que determinan un rectángulo. Probar que si el tablero es de 3×6 no siempre existen tales 4 fichas del mismo color.

Capítulo 12

Números combinatorios

12.1. Coeficientes binomiales

En esta sección estudiamos varias propiedades de los números combinatorios y algunas identidades interesantes. En algunos casos daremos más de una prueba de las proposiciones enunciadas, una de índole combinatoria y otra algebraica.

12.1.1. Definición y fórmulas

Recordemos de (11.2) que el número de formas distintas de elegir k objetos de un total de n, o equivalentemente el número de k-subconjuntos de un n-conjunto, se denota por $\binom{n}{k}$. Denotaremos por $\mathcal{P}_k(X)$ a los k-subconjuntos de $\mathcal{P}(X)$, es decir

$$\mathcal{P}_k(X) = \{H \subseteq X : |H| = k\} \subseteq \mathcal{P}(X)$$

Luego, si $|X| = n$ tenemos

$$\mathcal{P}(X) = \bigcup_{k=0}^{n} \mathcal{P}_k(X)$$

Resumiendo, tenemos

$$\binom{n}{k} = \#\{A \subseteq X : |A| = k, |X| = n\} = \#\mathcal{P}_k(I_k)$$

y hemos visto (Proposición (11.8)) que

$$\binom{n}{k} = \frac{n!}{k!(n-k!)} = \frac{n(n-1)\cdots(n-k+1)}{k!} \tag{12.1}$$

A este número se lo llama *número combinatorio* y se lee "n en k". Extendemos la definición del número combinatorio a casos extremos:

$$\binom{0}{0} = 1 \qquad \text{y} \qquad \binom{n}{n+1} = 0 \quad n \in \mathbb{N}_0$$

Si en (12.1), en lugar de simplificar el factor $(n-k)!$, simplificamos el factor $k!$, obtenemos

$$\binom{n}{k} = \frac{n(n-1)\cdots(k+1)}{(n-k)!} = \frac{(k+1)(k+2)\cdots(k+(n-k))}{1\cdot 2\cdots(n-k)}$$

de donde se llega a la fórmula producto

$$\binom{n}{k} = (1+k)(1+\tfrac{k}{2})(1+\tfrac{k}{3})\cdots(1+\tfrac{k}{n-k}) = \prod_{j=0}^{n-k}(1+\tfrac{k}{j}) \tag{12.2}$$

Esta expresión es útil para calcular $\binom{n}{k}$ cuando n y k son muy grandes. En este caso, la expresión con factoriales, aun usando computadoras, puede dar error.

12.1.2. Propiedades básicas

De la definición de $\binom{n}{k}$ se siguen directamente las siguientes propiedades.

- $\binom{n}{0} = \binom{n}{n} = 1$.
- $\binom{n}{1} = \binom{n}{n-1} = n$.
- $\binom{n}{2} = \frac{n(n-1)}{2}$.

Si pensamos combinatóricamente, es decir, en subconjuntos de $X = \{1, 2, \ldots, n\}$, el primer inciso se refiere a que hay un único 0-conjunto, $\varnothing$, y un único n-conjunto, X; mientras que el segundo inciso se refiere a que hay una cantidad n tanto de 1-conjuntos (los singuletes $\{1\}, \{2\}, \ldots, \{n\}$), como de $(n-1)$-conjuntos (sus complementos $X \smallsetminus \{1\} = \{2, 3, \ldots, n\}$, $X \smallsetminus \{2\} = \{1, 3, \ldots, n\}, \ldots, X \smallsetminus \{n\} = \{1, 2, \ldots, n-1\}$).

Simetría

El fenómeno de mas arriba vale en general; es decir, un conjunto de n elementos tiene la misma cantidad de k-subconjuntos que de $(n-k)$-subconjuntos. Esto es así pues cada conjunto de k elementos determina uno de $n-k$ elementos, su complemento; y, recíprocamente, cada conjunto de $n-k$ es el complemento de uno único subconjunto de k elementos.

Lema 12.1 (Simetría). *Para todo n, k se tiene*

$$\binom{n}{k} = \binom{n}{n-k} \tag{12.3}$$

Demostración algebraica. Tenemos

$$\binom{n}{n-k} = \frac{n!}{(n-k)!(n-(n-k))!} = \frac{n!}{(n-k)!k!} = \binom{n}{k}$$

como se quería ver. □

De ahora en más intentaremos dar pruebas algebraicas y/o combinatorias de los hechos que mencionemos. Es difícil de explicar qué es una prueba combinatoria, pero digamos rápidamente que es aquella que se basa en "argumentos combinatorios". Estos tendrán que ver con funciones, biyecciones, conjuntos y complementos, etc. Irá quedando claro en lo sucesivo a que nos referimos por prueba combinatoria.

Demostración combinatoria. Sea X un n-conjunto. Luego, $\binom{n}{k} = \#\{H \in \mathcal{P}(X) : |H| = k\}$. Consideremos la aplicación "tomar complemento"

$$\tau : \mathcal{P}_k(X) \to \mathcal{P}_{n-k}(X), \qquad H \mapsto \tau(H) = H^c$$

que a cada k-conjunto H le asigna el $(n-k)$-conjunto H^c. En efecto, por el **PC** se tiene $|H^c| = n - |H| = n - k$. Esta aplicación resulta una biyección de $\mathcal{P}(X)$, pues $(H^c)^c = H$ (es decir $\tau^{-1} = \tau$). Luego, por el **PB**, tenemos

$$\binom{n}{n-k} = \#\mathcal{P}_{n-k}(X) = \#\mathcal{P}_k(X) = \binom{n}{k}$$

como se quería ver. □

Identidad de Pascal

Proposición 12.2 (Identidad de Pascal)**.** *Dado $n \in \mathbb{N}$, para todo $0 \leq k \leq n$ se tiene que*

$$\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k} \tag{12.4}$$

Demostración algebraica. Tenemos

$$\begin{aligned}\binom{n}{k-1} + \binom{n}{k} &= \frac{n!}{(k-1)!(n-(k-1))!} + \frac{n!}{k!(n-k)!} = \frac{n!k + n!(n-k+1)}{k!(n-k+1)!} \\ &= \frac{n!(n+1)}{k!((n-k+1)!} = \frac{(n+1)!}{k!((n+1)-k)!} = \binom{n+1}{k}\end{aligned}$$

y el resultado sigue. □

De ahora en adelante denotaremos por I_k al conjunto de los primeros n naturales, i.e.

$$I_k = \{1, 2, \ldots, n\} = [\![1, n]\!]$$

Demostración combinatoria. Un subconjunto A de I_{n+1} puede ser de dos tipos, o contiene a $n+1$ o no lo contiene. Luego, tenemos la unión disjunta

$$\mathcal{P}(I_{n+1}) = \{A \subseteq I_{n+1} : n+1 \in A\} \cup \{B \subseteq I_{n+1} : n+1 \notin B\}$$

y por lo tanto, usando que $\{B \subseteq I_{n+1} : n+1 \notin B\} = \{B \subseteq I_n\}$, vale

$$\mathcal{P}_k(I_{n+1}) = \{A \subseteq I_{n+1} : n+1 \in A, |A| = k\} \cup \{B \subseteq I_n : |B| = k\}$$

La aplicación

$$A \mapsto A \setminus \{n+1\}$$

es una biyección de $\{A \subseteq I_{n+1} : n+1 \in A, |A| = k\}$ sobre $\{B \subseteq I_n : |B| = k-1\}$, con inversa $B \mapsto B \cup \{n+1\}$. Finalmente, como $\binom{n+1}{k} = \#\mathcal{P}_k(I_{n+1})$, por el principio de adición tenemos

$$\begin{aligned}\binom{n+1}{k} &= \#\{A \subseteq I_{n+1} : n+1 \in A, |A| = k\} + \#\{B \subseteq I_n : |B| = k\} \\ &= \#\{A \subseteq I_n : |A| = k-1\} + \#\{B \subseteq I_n : |B| = k\} = \binom{n}{k-1} + \binom{n}{k}\end{aligned}$$

como se quería ver. □

Absorción

Es inmediato chequear que, para todo $k \geq 1$, valen además las siguientes identidades

$$\binom{n}{k} = \frac{n}{k}\binom{n-1}{k-1} = \frac{n-k+1}{k}\binom{n}{k-1} \tag{12.5}$$

(llamadas identidades de absorción) y lo dejamos como ejercicio. Una interpretación combinatoria de la primera igualdad fue vista en (11.8), como el número de formas de elegir un comité de k personas de un total de n con un presidente.

Número total de subconjuntos de un conjunto

Con lo visto, es posible calcular fácilmente el número total de subconjuntos de un conjunto dado.

Teorema 12.3. *El número total de subconjuntos de un n-conjunto es 2^n. En particular,*

$$\#\mathcal{P}(I_n) = \sum_{k=0}^{n} \binom{n}{k} = 2^n \tag{12.6}$$

Demostración. Sea X un n-conjunto. El número de subconjuntos de X está dado por la suma de subconjuntos de X de cardinales $0, 1, 2, \ldots, n$ respectivamente, es decir

$$\#\mathcal{P}(X) = \sum_{k=0}^{n} \#\mathcal{P}_k(X) = \sum_{k=0}^{n} \binom{n}{k}$$

Basta ver que $\sum_{k=0}^{n} \binom{n}{k} = 2^n$. Procedemos por inducción en n. Por el principio de biyección, podemos suponer que $X = I_n$.

Demostración algebraica . Si $n = 1$ tenemos $\sum_{k=0}^{1} \binom{1}{k} = \binom{1}{0} + \binom{1}{1} = 1 + 1 = 2$ (el caso $n = 0$ es trivial). Supongamos que vale $\sum_{i=0}^{k} \binom{k}{i} = 2^k$ y veamos que vale $\sum_{i=0}^{k+1} \binom{k+1}{i} = 2^{k+1}$. Luego, usando la identidad de Pascal, tenemos

$$\begin{aligned}\sum_{i=0}^{k+1} \binom{k+1}{i} &= \binom{k+1}{0} + \sum_{i=1}^{k+1} \binom{k+1}{i} = \binom{k}{0} + \sum_{i=1}^{k+1} \binom{k}{i} + \binom{k}{i-1} \\ &= \sum_{i=0}^{k} \binom{k}{i} + \sum_{i=0}^{k} \binom{k}{i} = 2\sum_{i=0}^{k} \binom{k}{i} = 2 \cdot 2^k = 2^{k+1}\end{aligned}$$

donde hicimos cambios de variables y usamos que $\binom{k}{k+1} = 0$. □

Demostración combinatoria . Si $n = 1$, $\mathcal{P}(I_1) = \{\varnothing, \{1\}\}$ (el caso $n = 0$ es trivial). Tenemos

$$\mathcal{P}(I_{k+1}) = \{A \subseteq I_{k+1} : k+1 \in A\} \cup \{B \subseteq I_{k+1} : k+1 \notin B\}$$

Luego, procediendo igual que en la prueba de la identidad de Pascal (Proposicion 12.2), por los principios de adición y biyección e hipótesis inductiva, tenemos que

$$\#\mathcal{P}(I_{k+1}) = \#\{A \subseteq I_k\} + \#\{B \subseteq I_k\} = 2\#\mathcal{P}(I_k) = 2 \cdot 2^k = 2^{k+1}$$

y la demostración está completa. □

12.2. Binomio de Newton

Ya hemos visto que $(a+b)^2 = a^2 + 2ab + b^2$ y podemos calcular, sin demasiado trabajo, algunas potencias más altas. Es fácil chequear que:

- $(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$,
- $(a+b)^4 = a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4$,
- $(a+b)^5 = a^5 + 5a^4b + 10a^3b^2 + 10a^2b^3 + 5ab^4 + b^5$.

Pregunta. ¿Podemos adivinar una expresión para $(a+b)^6$ sin hacer el producto?

Respuesta. ¡Sí! Observar la regularidad y simetría en las fórmulas de arriba. De algún modo podemos preveer que $(a+b)^6$ debería involucrar los términos de la forma

$$a^6, \quad a^5b, \quad a^4b^2, \quad a^3b^3, \quad a^2b^4, \quad ab^5, \quad b^6 \tag{12.7}$$

En efecto, tenemos que

$$(a+b)^6 = (a+b)(a+b)(a+b)(a+b)(a+b)(a+b)$$

Si expandimos estos productos distribuyendo, haciendo todas las sumas y productos productos, vemos que un término general está formado por cosas de la forma

$$a^k b^{6-k} \qquad 0 \leq k \leq 6$$

ya que de cada factor debemos elegir un término. Es decir, un a o b del primer factor, se multiplica con un a o b del segundo, etcétera.

El tema es determinar los coeficientes, los números que acompañan a estos monomios. Es decir, hay que averiguar cuántas veces aparece cada término de (12.7) en el desarrollo de $(a+b)^6$. Por ejemplo, para obtener el término a^4b^2, debemos multiplicar 4 a's y 2 b's. Hay muchas formas de hacer esto; por ejemplo, 3 formas distintas de hacerlo son eligiendo los términos que se indican con colores

$$(a+b)(a+b)(a+b)(a+b)(a+b)(a+b)$$
$$(a+b)(a+b)(a+b)(a+b)(a+b)(a+b)$$
$$(a+b)(a+b)(a+b)(a+b)(a+b)(a+b)$$

Nosotros debemos contar todas las posibles formas de hacer esto. Luego, debemos elegir 4 a's de 6 para tener el término a^4b^2, es decir hay $\binom{6}{4} = 15$. Procediendo de esta forma, llegamos a la conclusión de que

$$(a+b)^6 = a^6 + \binom{6}{5}a^5b + \binom{6}{4}a^4b^2 + \binom{6}{3}a^3b^3 + \binom{6}{2}a^2b^4 + \binom{6}{1}ab^5 + b^6$$

es decir, $(a+b)^6 = a^6 + 6a^5b + 15a^4b^2 + 20a^3b^3 + 15a^2b^4 + 6ab^5 + b^6$.

El argumento usado recién permite dar una fórmula general para $(a+b)^n$ con n arbitrario.

Teorema 12.4 (Binomio de Newton). *Para todo $a, b \in \mathbb{R}$ y para todo $n \in \mathbb{N}$, se tiene*

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} \tag{12.8}$$

Demostración combinatoria. Podemos dar un argumento general, combinatorio. Está claro que

$$(a+b)^n = \underbrace{(a+b)(a+b)\cdots(a+b)}_{n\text{-veces}} \tag{12.9}$$

Un término cualquiera al expandir el producto es de la forma $c_1c_2\cdots c_n$ con $c_i \in \{a, b\}$, $i = 1, \ldots, n$. Como hay n factores de la forma $(a+b)$ y de cada uno tenemos 2 posibles elecciones (a ó b), está claro que, por el **PM**, hay 2^n términos de esta forma. Como a y b conmutan, los términos son todos de la forma a^kb^{n-k} con $0 \le k \le n$. Lo que no sabemos es cuántos de éstos hay. Sea $c_k(n)$ el número de términos de la forma a^kb^{n-k}. Luego,

$$(a+b)^n = \sum_{k=0}^{n} c_k(n)\, a^k b^{n-k} \tag{12.10}$$

Sólo tenemos que determinar cuánto vale $c_k(n)$ para cada n y cada $0 \le k \le n$. Pero si pensamos bien, nos damos cuenta que $c_k(n)$ es igual al número de formas de elegir k factores iguales a a, y por lo tanto $n-k$ iguales a b, en (12.9). Es decir que $c_k(n) = \binom{n}{k}$, nuestro famoso número combinatorio. □

Demostración algebraica. Por inducción en n. El paso inicial es claro pues $(a+b)^1 = a+b$ y

$$\sum_{k=0}^{1} \binom{1}{k} a^k b^{n-k} = \binom{1}{0} a^0 b^1 + \binom{1}{1} a^1 b^0 = b + a$$

Supongamos que vale (12.8) para n y veamos que entonces vale

$$(a+b)^{n+1} = \sum_{k=0}^{n+1} \binom{n+1}{k} a^k b^{n+1-k}$$

Como $(a+b)^{n+1} = (a+b)^n(a+b) = (a+b)^n a + (a+b)^n b$, tenemos

$$\begin{aligned}
(a+b)^{n+1} &= \sum_{k=0}^{n} \binom{n}{k} a^{k+1} b^{n-k} + \sum_{k=0}^{n} \binom{n}{k} a^k b^{n+1-k} \\
&= \binom{n}{n} a^{n+1} + \sum_{k=0}^{n-1} \binom{n}{k} a^{k+1} b^{(n+1)-(k+1)} + \binom{n}{0} b^{n+1} + \sum_{k=1}^{n} \binom{n}{k} a^k b^{n+1-k} \\
&= \binom{n+1}{n+1} a^{n+1} + \binom{n+1}{0} b^{n+1} + \sum_{k=1}^{n} \left(\binom{n}{k-1} + \binom{n}{k} \right) a^k b^{(n+1)-k} \\
&= \sum_{k=0}^{n+1} \binom{n+1}{k} a^k b^{(n+1)-k}
\end{aligned}$$

donde hemos usado la identidad de Pascal en la última igualdad. Por el principio de inducción, la fórmula del binomio vale. □

Digresión. En nuestra hipótesis $a, b \in \mathbb{R}$, lo única propiedad que hemos usado es que a y b conmutan. Luego, el resultado vale con más generalidad, para cualquier par de elementos a, b en un anillo (conjunto con suma y producto) tal que $ab = ba$. En particular, esto es cierto por ejemplo, para $a, b \in \mathbb{Q}(\sqrt{2})$. Pero... ¿existen conjuntos en que $ab \neq ba$? ¡Sí!

Cuando aprendan a trabajar con "matrices" en álgebra lineal, verán que éstas, en general, no conmutan. Veamos el caso más simple de matrices 2×2. Una matriz real 2×2 es un bloque formado por 4 números reales

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \qquad a, b, c, d \in \mathbb{R}$$

Estas matrices se pueden sumar y multiplicar; se suman "elemento a elemento" y se multiplican de "forma cruzada" así:

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} + \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11}+b_{11} & a_{12}+b_{12} \\ a_{21}+b_{21} & a_{22}+b_{22} \end{pmatrix}$$

y

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \cdot \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11}b_{11}+a_{12}b_{21} & a_{11}b_{21}+a_{12}b_{22} \\ a_{21}b_{11}+a_{22}b_{21} & a_{21}b_{12}+a_{22}b_{22} \end{pmatrix}$$

Pueden chequear que la suma es asociativa y conmutativa y que la suma y producto distribuyen. Sin embargo, el producto en general no conmuta. Por ejemplo,

$$\begin{pmatrix}1 & 2\\ 3 & 4\end{pmatrix}\begin{pmatrix}1 & 2\\ 0 & -1\end{pmatrix} = \begin{pmatrix}1\cdot 1+2\cdot 0 & 1\cdot 2+2\cdot(-1)\\ 3\cdot 1+4\cdot 0 & 3\cdot 2+4\cdot(-1)\end{pmatrix} = \begin{pmatrix}1 & 0\\ 3 & 2\end{pmatrix}$$

mientras que

$$\begin{pmatrix}1 & 2\\ 0 & -1\end{pmatrix}\begin{pmatrix}1 & 2\\ 3 & 4\end{pmatrix} = \begin{pmatrix}1\cdot 1+2\cdot 3 & 1\cdot 2+2\cdot 4\\ 0\cdot 1+(-1)\cdot 3 & 0\cdot 2+(-1)\cdot 4\end{pmatrix} = \begin{pmatrix}7 & 10\\ -3 & -4\end{pmatrix}$$

Pero si A y B son matrices cuadradas que conmutan, por ejemplo si una de ellas es diagonal $\left(\begin{smallmatrix}a & 0\\ 0 & b\end{smallmatrix}\right)$, entonces vale

$$(A+B)^n = \sum_{k=0}^{n} \binom{n}{k} A^k B^{n-k}$$

donde por supuesto $A^2 = A\cdot A$ y A^k se define recursivamente $A^k = A^{k-1}\cdot A$.

Algunas sumas de números combinatorios

Tomando algunos valores particulares para a y b en el teorema se obtienen algunas otras identidades interesantes, como veremos a continuación.

Observación.

(1) Si tomamos $a = b = 1$, el teorema dice que $\sum_{k=0}^{n}\binom{n}{k} = (1+1)^n = 2^n$, reobteniendo así la fórmula (12.6) del Teorema 12.3.

(2) Tomando $a = 1$, $b = -1$, tenemos que la *suma alternada de los números combinatorios* se anula, es decir

$$0 = (1-1)^n = \sum_{k=0}^{n}(-1)^k\binom{n}{k} \tag{12.11}$$

Es decir,

$$\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \binom{n}{3} + \cdots + (-1)^{n-1}\binom{n-1}{n} + (-1)^n\binom{n}{n} = 0$$

Por ejemplo,

$$\binom{5}{0} - \binom{5}{1} + \binom{5}{2} - \binom{5}{3} + \binom{5}{4} - \binom{5}{5} = 1 - 5 + 10 - 10 + 5 - 1 = 0$$
$$\binom{6}{0} - \binom{6}{1} + \binom{6}{2} - \binom{6}{3} + \binom{6}{4} - \binom{6}{5} + \binom{6}{6} = 1 - 6 + 15 - 20 + 15 - 6 + 1 = 0$$

Veamos ahora que la suma de los números combinatorios $\binom{n}{k}$ sobre los k pares o sobre los k impares coinciden. En el caso en que n es impar esto es inmediato, ya que k y $n-k$ tienen distinta paridad y hay una cantidad par de términos $\binom{n}{0}, \binom{n}{1}, \ldots, \binom{n}{n-1}, \binom{n}{n}$. Por la identidad de Pascal $\binom{n}{k} = \binom{n}{n-k}$, y $\binom{n}{k}$ y $\binom{n}{n-k}$ están en sumas distintas. Por ejemplo, si $n = 7$ tenemos

$$\binom{7}{0} + \binom{7}{2} + \binom{7}{4} + \binom{7}{6} = 1 + 21 + 35 + 7 = 64 = 2^6$$
$$\binom{7}{7} + \binom{7}{5} + \binom{7}{3} + \binom{7}{1} = 1 + 21 + 35 + 7 = 64 = 2^6$$

Para n par el resultado igual vale, como veremos, aunque es menos intuitivo. Por ejemplo, si $n = 6$ tenemos

$$\binom{6}{0} + \binom{6}{2} + \binom{6}{4} + \binom{6}{6} = 1 + 15 + 15 + 1 = 32 = 2^5$$
$$\binom{6}{1} + \binom{6}{3} + \binom{6}{5} = 6 + 20 + 6 = 32 = 2^5$$

Corolario 12.5. *Para todo $n \in \mathbb{N}$ vale*

$$\sum_{\substack{k=0 \\ k \text{ par}}}^{n} \binom{n}{k} = \sum_{\substack{k=0 \\ k \text{ impar}}}^{n} \binom{n}{k} = 2^{n-1}$$

Demostración. Sea $S_p = \sum_{k \text{ par}} \binom{n}{k}$ y $S_i = \sum_{k \text{ impar}} \binom{n}{k}$. Como

$$0 = \sum_{i=0}^{n} (-1)^k \binom{n}{k} = S_p - S_i \qquad \text{y} \qquad 2^n = \sum_{i=0}^{n} \binom{n}{k} = S_p + S_i$$

tenemos que $S_p = S_i$ y $2^n = 2S_p$ de donde $S_p = S_i = 2^{n-1}$. □

Corolario 12.6. *Para todo $x \in \mathbb{R}$ y $n \in \mathbb{N}$ valen*

$$(1+x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k \qquad y \qquad (1-x)^n = \sum_{k=0}^{n} (-1)^k \binom{n}{k} x^k$$

Demostración. Salen de tomar $a = 1$ y $b = \pm x$ en el binomio de Newton (12.8). □

Uno puede "jugar" un poco con estas fórmulas y obtener potencias de un número en términos de combinaciones lineales enteras de potencias de otro número. Por ejemplo, escribamos 3^n en término de potencias de 2.

$$3^n = (2+1)^n = \sum_{k=0}^{n} \binom{n}{k} 2^k \tag{12.12}$$

En particular,

$$3^5 = 1 + 5 \cdot 2 + \binom{5}{2} 2^2 + \binom{5}{3} 2^3 + 5 \cdot 2^4 + 2^5 = 1 + 10 + 40 + 80 + 80 + 32 = 243$$

Similarmente, escribimos 2^n en término de potencias de 3,

$$2^n = (3-1)^n = \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} 3^k \tag{12.13}$$

Por ejemplo,

$$\begin{aligned} 2^6 &= \binom{6}{0}3^0 - \binom{6}{1}3^1 + \binom{6}{2}3^2 - \binom{6}{3}3^3 + \binom{6}{4}3^4 - \binom{6}{5}3^5 + \binom{6}{6}3^6 \\ &= 1 - 6 \cdot 3 + 15 \cdot 9 - 20 \cdot 27 + 15 \cdot 81 - 6 \cdot 243 + 729 = 64 \end{aligned}$$

También podemos obtener el número 1 como combinación lineal de potencias de enteros consecutivos. Para todo $n \geq 2$ tenemos

$$1 = (a-(a-1))^n = \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} a^k (a-1)^{n-k}$$

Por ejemplo, para $a = 2$,

$$1 = \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} 2^k \tag{12.14}$$

En particular,

$$1 = \sum_{k=0}^{3} (-1)^{3-k} \binom{3}{k} 2^k = -\binom{3}{0} + \binom{3}{1}2 - \binom{3}{2}2^2 + \binom{3}{3}2^3 = -1 + 6 - 12 + 8 = 1$$

Dos consecuencias: Fermat y el sueño del pibe

Necesitamos el siguiente resultado básico.

Lema 12.7. *Si p es primo se tiene $p \mid \binom{p}{i}$ para todo $1 \leq i \leq p-1$.*

Demostración. Tenemos

$$\binom{p}{k} = \frac{p(p-1)\cdots(p-k+1)}{k(k-1)\cdots 3 \cdot 2} \in \mathbb{Z}$$

Luego, cada $1 \leq m \leq k$ del denominador divide al numerador. Como $(p, m) = 1$, entonces $m \mid (p-1)\cdots(p-k+1)$, de donde

$$\binom{p}{k} = p\ell \qquad \text{con} \qquad \ell = \frac{(p-1)\cdots(p-k+1)}{k(k-1)\cdots 3 \cdot 2} \in \mathbb{Z}$$

como queríamos ver. □

Del binomio de Newton se obtienen dos propiedades interesantes si tomamos $n = p$ primo, entre ellas una prueba directa, más sencilla, del Teorema de Fermat.

Corolario 12.8 (Consecuencias de Newton). *Si $a, b \in \mathbb{Z}$ y p es un primo entonces valen*

(a) El sueño del pibe:*

$$(a+b)^p \equiv a^p + b^p \pmod{p}$$

(b) El teorema de Fermat:

$$a^p \equiv a \pmod{p}$$

Demostración.

(a) Por el binomio de Newton, $(a+b)^p = a^p + \sum_{k=1}^{p-1} \binom{p}{k} a^k b^{n-k} + b^p$ y, por el Lema 12.7, tenemos que $(a+b)^p \equiv a^p + b^p \pmod{p}$ pues $\sum_{k=1}^{p-1} \binom{p}{k} a^k b^{n-k} \equiv 0 \pmod{p}$.

(b) Si $p = 2$ entonces $a^2 - a = a(a-1)$ es par y por lo tanto $a^2 \equiv a \pmod 2$.

Supongamos que p es un primo impar. Haremos inducción en $a \in \mathbb{N}$. Para el paso inicial, si $a = 1$ tenemos $a^p = 1^p = 1 \equiv 1 \pmod p$. Para el paso inductivo, supongamos que el resultado vale para a, veamos que se cumple para $a+1$. Usando el punto (1), tenemos que

$$(a+1)^p \equiv a^p + 1 \equiv a + 1 \pmod p$$

Luego, $a^p \equiv a \pmod p$ para todo $a \in \mathbb{N}$.

Ahora, si $a = 0$ el resultado es trivial. Si $a \in \mathbb{Z}$ y $a < 0$, entonces $-a \in \mathbb{N}$ y $(-a)^p \equiv (-a) \pmod p$. Pero, por otro lado, $(-a)^p = (-1)^p a^p = -a^p$. Luego, $(-a)^p \equiv -a \pmod p$. De este modo probamos que $a^p \equiv a \pmod p$ para todo $a \in \mathbb{Z}$. □

Observación. Por (a) y (b) del Corolario 12.8 tenemos

$$(a+b)^p \equiv a + b \pmod p \qquad \text{y} \qquad (ab)^p = ab \pmod p$$

Concluimos que, en $\mathbb{Z}_p$, la suma y el producto de números que satisfacen $a^p = a$ también satisface esa propiedad.

12.3. El Triángulo de Pascal e identidades

12.3.1. El triángulo de Pascal.

Con los números combinatorios $\binom{n}{k}$ formamos un triángulo isósceles (infinito), con la fila n-ésima correspondiendo a los números $\binom{n}{0}, \binom{n}{1}, \ldots, \binom{n}{n}$. Para los primeros valores de n tenemos

$$\begin{array}{ccccccccc}
\binom{0}{0} \\
\binom{1}{0} & \binom{1}{1} \\
\binom{2}{0} & \binom{2}{1} & \binom{2}{2} \\
\binom{3}{0} & \binom{3}{1} & \binom{3}{2} & \binom{3}{3} \\
\binom{4}{0} & \binom{4}{1} & \binom{4}{2} & \binom{4}{3} & \binom{4}{4} \\
\binom{5}{0} & \binom{5}{1} & \binom{5}{2} & \binom{5}{3} & \binom{5}{4} & \binom{5}{5} \\
\binom{6}{0} & \binom{6}{1} & \binom{6}{2} & \binom{6}{3} & \binom{6}{4} & \binom{6}{5} & \binom{6}{6} \\
\binom{7}{0} & \binom{7}{1} & \binom{7}{2} & \binom{7}{3} & \binom{7}{4} & \binom{7}{5} & \binom{7}{6} & \binom{7}{7} \\
\binom{8}{0} & \binom{8}{1} & \binom{8}{2} & \binom{8}{3} & \binom{8}{4} & \binom{8}{5} & \binom{8}{6} & \binom{8}{7} & \binom{8}{8}
\end{array}$$

Notar que en las diagonales (que van de derecha a izquierda desde arriba) están los $\binom{n}{k}$ con igual k. Este triángulo, para los primeros valores de n, queda así

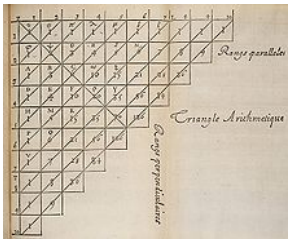
$$
\begin{array}{ccccccccccc}
 & & & & & 1 & & & & & \\
 & & & & 1 & & 1 & & & & \\
 & & & 1 & & 2 & & 1 & & & \\
 & & 1 & & 3 & & 3 & & 1 & & \\
 & 1 & & 4 & & 6 & & 4 & & 1 & \\
1 & & 5 & & 10 & & 10 & & 5 & & 1 \\
1 & & 6 & & 15 & & 20 & & 15 & & 6 & & 1 \\
1 & & 7 & & 21 & & 35 & & 35 & & 21 & & 7 & & 1 \\
1 & & 8 & & 28 & & 56 & & 70 & & 56 & & 28 & & 8 & & 1
\end{array}
$$

Para ilustrar, arriba hemos marcado con colores la simetría $\binom{n}{k} = \binom{n}{n-k}$ en violeta, y la identidad de Pascal $\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k}$ en azul y rojo, para algunos valores de $\binom{n}{k}$.

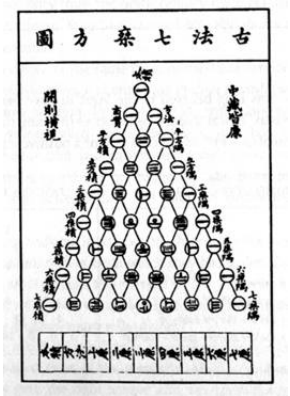
El triángulo "dice" por ejemplo que

$$(a+b)^7 = a^7 + 7a^6b + 21a^5b^2 + 35a^4b^3 + 35a^3b^4 + 21a^2b^5 + 7ab^6 + b^7$$
$$(a+b)^8 = a^8 + 8a^7b + 28a^6b^2 + 56a^5b^3 + 70a^4b^4 + 56a^3b^5 + 28a^2b^6 + 8ab^7 + b^8.$$

Nota histórica. Este es el llamado *triángulo de Pascal* en honor al francés Blaise Pascal (1623–1662) quién lo estudió en 1653. En realidad ya era conocido por el italiano Niccolo Fontana (1500–1557), alias "Tartaglia" por su tartamudez. Menos conocido es el hecho de que los chinos ya lo conocían. En China, éste se llama triángulo de Yang Hui (1238–1298) en honor a su descubridor, quien lo introdujo en 1261. Este triángulo aparece también publicado en el libro del matemático chino Chu-Shih-Chieh *"El precioso espejo de los cuatro elementos"* de 1303. Ya se ve, nada nuevo bajo el sol... Para una historia mas completa del triángulo en cuestión, ver el libro de Edwards *"Pascal's Arithmetical Triangle"* de 1987.



(a) según Pascal



(b) según Yang Hui

Figura 12.1: El triángulo de números combinatorios

La Identidad de Pascal $\binom{n}{k}+\binom{n}{k-1}=\binom{n+1}{k}$, define recursivamente a los números combinatorios. Si conocemos los números $\binom{n}{k}$ para todo k, podemos calcular los números $\binom{n+1}{k}$ para todo k. Así, la fila siguiente en el triángulo de arriba, correspondiente a $n=9$, queda

$$1 \quad 9 \quad 36 \quad 84 \quad 126 \quad 84 \quad 36 \quad 9 \quad 1.$$

Las identidades en (12.5) también permiten obtener nuevos números combinatorios a partir de números combinatorios calculados previamente. Por ejemplo, $\binom{n}{k}=\frac{n}{k}\binom{n-1}{k-1}$ permite obtener $\binom{n}{k}$ a partir de $\binom{n-1}{k-1}$ multiplicando por $\frac{n}{k}$ (gráficamente nos movemos en el triángulo en diagonal hacia abajo); mientras que $\binom{n}{k}=\frac{n-k+1}{k}\binom{n}{k-1}$ permite obtener $\binom{n}{k}$ a pertir de $\binom{n}{k-1}$ multiplicando por $\frac{n-k+1}{k}$ (gráficamente, nos movemos en el triángulo por la misma fila.

En el triángulo, se puede chequear que la suma de los combinatorios $\binom{n}{k}$ es 2^n, para valores pequeños de n.

n	$\sum\binom{n}{k}$	2^n
0	1 =1	2^0
1	1 + 1 =2	2^1
2	1 + 2 + 1 = 4	2^2
3	1 + 3 + 3 + 1 = 8	2^3
4	1 + 4 + 6 + 4 + 1 = 16	2^4
5	1 + 5 + 10 + 10 + 5 + 1 = 32	2^5
6	1+ 6 + 15 + 20 + 15 + 6 + 1 =64	2^6
7	1 + 7 + 21 + 35 + 35 + 21 + 7 + 1 =128	2^7

Observación. Este triángulo siempre ha atraído a mucha gente por su belleza y por la cantidad de propiedades que encierra.

(i) Por ejemplo, los números $\{\binom{n}{k}\}_{n\in\mathbb{N}}$ con k fijo forman diagonales. Podemos encontrar algunas sucesiones interesantes en las primeras diagonales. Para $k=1$ tenemos los números naturales. Para $k=2$ tenemos los *números triangulares* $1,3,6,10,15,21\ldots$ definidos por

$$t_n = 1+2+\cdots+n = \tfrac{1}{2}n(n+1)$$

Para $k=3$, tenemos la sucesión de *números tetraedrales* $1,4,10,20,35,56,\ldots$ definidos por

$$T_n = t_1+t_2+\cdots+t_n = \tfrac{1}{6}n(n+1)(2n+1)$$

Chequear que $T_n=\binom{n+2}{3}$.

(ii) Por otra parte, las primeras filas del triángulo son las potencias de 11,

$$1=11^0, \quad 11=11^1, \quad 121=11^2, \quad 1331=11^3, \quad 14641=11^4$$

Hemos vimos además que las sumas de las filas dan las potencias de 2.

(iii) También es posible obtener a partir del triángulo de Pascal la sucesión de números de Fibonacci f_n que empieza $1,1,2,3,5,8,13,21,\ldots$. Si escribimos el triángulo alineado a

la izquierda,

$$
\begin{array}{cccccccc}
1 & & & & & & & \\
1 & 1 & & & & & & \\
1 & 2 & 1 & & & & & \\
1 & 3 & 3 & 1 & & & & \\
1 & 4 & 6 & 4 & 1 & & & \\
1 & 5 & 10 & 10 & 5 & 1 & & \\
1 & 6 & 15 & 20 & 15 & 6 & 1 & \\
1 & 7 & 21 & 35 & 35 & 21 & 7 & 1
\end{array}
$$

entonces sumando sobre las diagonales (que comienzan en los unos de la izquierda hacia arriba) tenemos los números de Fibonacci:

$$
\begin{aligned}
1 &= 1 \\
1 &= 1 \\
1 + 1 &= 2 \\
1 + 2 &= 3 \\
1 + 3 + 1 &= 5 \\
1 + 4 + 3 &= 8 \\
1 + 5 + 6 + 1 &= 13 \\
1 + 6 + 10 + 4 &= 21 \\
1 + 7 + 15 + 10 + 1 &= 34
\end{aligned}
$$

etcétera.

12.3.2. Identidades con coeficientes binomiales

Veamos a continuación algunas identidades interesantes entre números combinatorios que se obtienen directamente del triángulo de Pascal o usando argumentos combinatorios sencillos (al estilo de los vistos en la formación de comités).

Sumas diagonales

Es claro que por simetría, la suma

$$\binom{3}{3} + \binom{4}{3} + \binom{5}{3} + \binom{6}{3} + \binom{7}{3} + \binom{8}{3}$$

es igual a esta otra suma

$$\binom{3}{0} + \binom{4}{1} + \binom{5}{2} + \binom{6}{3} + \binom{7}{4} + \binom{8}{5}$$

Gráficamente, en el triángulo:

$$\begin{array}{ccccccccccccc}
 & & & & & & \binom{0}{0} & & & & & & \\
 & & & & & \binom{1}{0} & & \binom{1}{1} & & & & & \\
 & & & & \binom{2}{0} & & \binom{2}{1} & & \binom{2}{2} & & & & \\
 & & & \binom{3}{0} & & \binom{3}{1} & & \binom{3}{2} & & \binom{3}{3} & & & \\
 & & \binom{4}{0} & & \binom{4}{1} & & \binom{4}{2} & & \binom{4}{3} & & \binom{4}{4} & & \\
 & \binom{5}{0} & & \binom{5}{1} & & \binom{5}{2} & & \binom{5}{3} & & \binom{5}{4} & & \binom{5}{5} & \\
\binom{6}{0} & & \binom{6}{1} & & \binom{6}{2} & & \binom{6}{3} & & \binom{6}{4} & & \binom{6}{5} & & \binom{6}{6}
\end{array}$$

$$\begin{array}{ccccccccc}
\binom{7}{0} & \binom{7}{1} & \binom{7}{2} & \binom{7}{3} & \binom{7}{4} & \binom{7}{5} & \binom{7}{6} & \binom{7}{7} \\
\binom{8}{0} & \binom{8}{1} & \binom{8}{2} & \binom{8}{3} & \binom{8}{4} & \binom{8}{5} & \binom{8}{6} & \binom{8}{7} & \binom{8}{7}
\end{array}$$

Ambas sumas valen $1 + 4 + 10 + 20 + 35 + 56 = 126$, que es justamente el número combinatorio $\binom{9}{4}$.

Notar que estas sumas se pueden escribir de la siguiente forma

$$\sum_{i=0}^{5} \binom{3+i}{i} = \sum_{j=0}^{5} \binom{3+j}{3}$$

Lo visto en este ejemplo es un hecho general. Las identidades de Chu-Shih-Chieh permiten calcular el valor para estas sumas.

Identidad de Chu-Shih-Chieh

Teorema 12.9 (Identidad de Chu-Shih-Chieh o suma diagonal)**.** *Para todo $n, m \in \mathbb{N}$ con $0 \leq r \leq n$ se tiene que*

$$\sum_{k=r}^{n} \binom{k}{r} = \binom{r}{r} + \binom{r+1}{r} + \cdots + \binom{n}{r} = \binom{n+1}{r+1} \tag{12.15}$$

$$\sum_{j=0}^{m} \binom{r+j}{j} = \binom{r}{0} + \binom{r+1}{1} + \cdots + \binom{r+m}{m} = \binom{r+m+1}{m} \tag{12.16}$$

Demostración. Probemos la primer identidad. Sabemos que $\binom{n+1}{r+1}$ es el número de $(r+1)$-subconjuntos de I_{n+1}. Sea $A \subseteq I_{n+1}$ con $|A| = r+1$ y sea j el mayor elemento de A. Como A tiene $r+1$ elementos, $j \geq r+1$. Luego $j+1, j+2, \ldots, n+1 \notin A$. Para completar la elección de A, debemos tomar r elementos de $\{1, 2, \ldots, j-1\}$. Luego,

$$\sum_{j=r+1}^{n+1} \binom{j-1}{r} = \sum_{k=r}^{n} \binom{k}{r} = \binom{n+1}{r+1}$$

donde hemos hecho el cambio de variable $k = j - 1$.

Notar que, por simetría, tomando $n = r + m$, la segunda identidad es equivalente a la primera. Una es la suma diagonal de derecha a izquierda empezando en $\binom{r}{r}$ y la otra es la suma diagonal de izquierda a derecha empezando en $\binom{r}{0}$. □

Ejemplo. Tenemos la suma

$$\binom{2}{2} + \binom{3}{2} + \binom{4}{2} + \binom{5}{2} + \binom{6}{2} + \binom{7}{2} = \binom{8}{3}$$

o la suma

$$\binom{1}{0} + \binom{2}{1} + \binom{3}{2} + \binom{4}{3} + \binom{5}{4} + \binom{6}{5} = \binom{7}{5}$$

En el triángulo:

$$\begin{array}{ccccccccccc}
 & & & & & \binom{0}{0} & & & & & \\
 & & & & \binom{1}{0} & & \binom{1}{1} & & & & \\
 & & & \binom{2}{0} & & \binom{2}{1} & & \binom{2}{2} & & & \\
 & & \binom{3}{0} & & \binom{3}{1} & & \binom{3}{2} & & \binom{3}{3} & & \\
 & \binom{4}{0} & & \binom{4}{1} & & \binom{4}{2} & & \binom{4}{3} & & \binom{4}{4} & \\
\binom{5}{0} & & \binom{5}{1} & & \binom{5}{2} & & \binom{5}{3} & & \binom{5}{4} & & \binom{5}{5} \\
 & \binom{6}{0} & & \binom{6}{1} & & \binom{6}{2} & & \binom{6}{3} & & \binom{6}{4} & & \binom{6}{5} & & \binom{6}{6} & \\
 & & \binom{7}{0} & & \binom{7}{1} & & \binom{7}{2} & & \binom{7}{3} & & \binom{7}{4} & & \binom{7}{5} & & \binom{7}{6} & & \binom{7}{7} & & \\
 & & & \binom{8}{0} & & \binom{8}{1} & & \binom{8}{2} & & \binom{8}{3} & & \binom{8}{4} & & \binom{8}{5} & & \binom{8}{6} & & \binom{8}{7} & & \binom{8}{7} & & & \\
\end{array}$$

Es decir, si pensamos a las sumas diagonales yendo de arriba hacia abajo y si sumamos de derecha a izquierda, el resultado es el número inmediatamente a abajo a la derecha del último sumado; por el contrario, si sumamos de izquierda a derecha, el resultado es el número inmediatamente abajo a la izquierda del último sumado. ◊

Identidad de Vandermonde

Teorema 12.10 (Identidad de Vandermonde). *Para toda terna de enteros $m, n, r \geq 0$ vale*

$$\sum_{k=0}^{r} \binom{n}{k}\binom{m}{r-k} = \binom{n+m}{r} \tag{12.17}$$

Demostración algebraica. Se tiene que

$$(1+x)^{n+m} = (1+x)^n (1+x)^m$$

El coeficiente r-ésimo de $(1+x)^{n+m}$ es $\binom{n+m}{r}$. Ahora,

$$(1+x)^m (1+x)^n = \left(\sum_{i=0}^{m} \binom{m}{i} x^i\right)\left(\sum_{j=0}^{n} \binom{n}{j} x^j\right) = \sum_{i=0}^{m}\sum_{j=0}^{n} \binom{m}{i}\binom{n}{j} x^{i+j}$$

Haciendo el cambio de variables $k = i + j$, se tiene que $i \leq k \leq i + n$ y $j = k - i$, y por lo tanto

$$(1+x)^m(1+x)^n = \sum_{i=0}^{m}\sum_{k=i}^{i+n}\binom{m}{i}\binom{n}{k-i}x^k = \sum_{k=0}^{n+m}\left(\sum_{i=0}^{k}\binom{m}{i}\binom{n}{k-i}\right)x^k$$

pues $\binom{n}{i} = 0$ para $i > n$. Luego, el coeficiente r-ésimo de $(1+x)^n(1+x)^m$ es $\sum_{i=0}^{r}\binom{m}{i}\binom{n}{r-i}$, y por lo tanto vale (12.17). □

Demostración combinatoria. Elegimos r-subconjuntos de

$$\{1, \ldots, n+m\} = \{1, \ldots, n\} \cup \{n+1, \ldots, n+m\}$$

Esto se puede hacer eligiendo un k-subconjunto de $\{1, \ldots, n\}$ y un $(r-k)$-subconjunto de $\{n+1, \ldots, n+m\}$, para cada posible $0 \leq k \leq r$. Luego, por PA y PM tenemos

$$\sum_{k=0}^{r}\binom{n}{k}\binom{m}{r-k} = \binom{n+m}{r}$$

como se quería ver. □

Demostración geométrica. Consideremos una grilla rectangular, como las vistas en §11.5.2, de $r \times (m+n-r)$ cuadrados y supongamos que $(0,0)$ es la izquierda inferior izquierda. Sabemos por (11.3) que hay $\binom{r+(m+n-r)}{r} = \binom{m+n}{r}$ caminos minimales que comienzan en $(0,0)$ y terminan en $(r, m+n-r)$.

Contemos esto de otra forma. Hay $\binom{m}{k}$ caminos minimales que comienzan en $(0,0)$ y terminan en (k,m), ya que k pasos a la derecha y $m-k$ pasos hacia arriba deben hacerse (la longitud del camino es m). Similarmente, hay $\binom{n}{r-k}$ caminos minimales de (k,m) a $(r, m+n-r)$, ya que un total de r pasos a la derecha deben hacerse y la longitud del camino debe ser $m+n$. De este modo, hay $\binom{m}{k}\binom{n}{r-k}$ caminos minimales que van del $(0,0)$ al $(r, m+n-r)$, pasando por (k,m). Este es un subconjunto del total de caminos minimales que van del $(0,0)$ al $(r, m+n-r)$. Luego, sumando desde $k=0$ hasta $k=r$ (pues el punto (k,m) está en la grilla) obtenemos el número total de caminos minimales del $(0,0)$ al $(r, m+n-r)$. Luego, vale (12.17) como se quería ver. □

Otras identidades sencillas

Existen muchísimas identidades que involucran a los números combinatorios. Hemos visto las más importantes. Veamos algunas adicionales.

Proposición 12.11 (Suma de cuadrados)**.** *Para todo $n \in \mathbb{N}$ vale*

$$\sum_{k=0}^{n}\binom{n}{k}^2 = \sum_{k=0}^{n}\binom{n}{k}\binom{n}{n-k} = \binom{2n}{n} \tag{12.18}$$

Demostración algebraica. Tomando $m = n = r$ en la identidad de Vandermonde (12.17) y usando que $\binom{n}{n-k} = \binom{n}{k}$ se tiene (12.18). □

Demostración combinatoria. Primero notamos que $\binom{n}{k}^2 = \binom{n}{k}\binom{n}{n-k}$. Pensemos que hay n hombres y n mujeres e interpretamos a $\binom{n}{k}\binom{n}{n-k}$ como el número de comités de n personas con k hombres y $n-k$ mujeres. Sumando sobre k tenemos todos los posibles comités de n personas elegidas de entre $2n$ personas (n hombres y n mujeres), y este número está claramente dado por $\binom{2n}{n}$. □

Las siguientes identidades se obtienen (aunque puede haber otras formas) usando derivadas de funciones, un concepto del análisis matemático. El lector que no conoce este concepto puede obviar las demostraciones o intentar dar otras alternativas.

Proposición 12.12. *Para todo n vale*

(a) $\sum_{k=0}^{n} k\binom{n}{k} = n2^{n-1}$,

(b) $\sum_{k=0}^{n} (-1)^k k\binom{n}{k} = 0$.

Demostración. (a) Derivando la identidad $(x+1)^n = \sum_{k=0}^{n} \binom{n}{k} x^k$ se tiene

$$n(x+1)^{n-1} = \sum_{k=1}^{n} \binom{n}{k} k x^{k-1}$$

de donde haciendo $x = 1$ se obtiene la identidad en (a).

(a') Veamos otra demostración. Usaremos que $r\binom{n}{r} = n\binom{n-1}{r-1}$. Luego,

$$\sum_{r=1}^{n} r\binom{n}{r} = \sum_{r=1}^{n} n\binom{n-1}{r-1} = n\sum_{r=1}^{n} \binom{n-1}{r-1} = n\sum_{s=0}^{n-1} \binom{n-1}{s} = n2^{n-1}$$

donde hicimos el cambio de variable $s = r-1$.

(b) Ahora, derivando la identidad $(1-x)^n = (-1)^n \sum_{k=0}^{n} (-1)^k \binom{n}{k} x^{n-k}$ se tiene que

$$-n(1-x)^{n-1} = (-1)^n \sum_{k=1}^{n} (-1)^k (n-k) \binom{n}{k} k x^{n-k-1}$$

y tomando $x = 1$ se tiene $(-1)^n \sum_{k=1}^{n} (-1)^k (n-k)\binom{n}{k} k = 0$ de donde se obtiene la identidad de (b). □

Existen muchas otras identidades entre números combinatorios. Por ejemplo,

- $\left(\sum_{k=0}^{n} \binom{n}{k}\right)^2 = \sum_{k=0}^{2n} \binom{2n}{k}$.
- $\sum_{k=0}^{m} \binom{n+k}{k} = \binom{n+m+1}{m}$.

- $\displaystyle\sum_{k=0}^{n-1}\binom{n}{k}\binom{n}{k+1}=\binom{2n}{n-1}$.

El lector puede chequear las identidades para algunos valores de n y k. No daremos las demostraciones, aunque invitamos al lector curioso a intentar alguna prueba.

Finalmente, queremos llamar la atención sobre la siguiente identidad notable

$$\sum_{k=0}^{n}(-1)^k\binom{n}{k}(x-k)^n=n! \tag{12.19}$$

válida para $n\in\mathbb{N}$ y $x\in\mathbb{R}$ (también vale para $n=0$ con $x\neq 0$). No daremos su prueba por el momento, pero el lector puede chequear que es válida para algunos valores pequeños de n. Es un caso particular de la expresión (12.24) que veremos más adelante.

Esta identidad permite probar que el Teorema de Fermat implica el Teorema de Wilson.

Ejemplo. Sea p primo. Fermat dice que $a^{p-1}\equiv 1 \pmod p$ para todo a coprimo con p y Wilson que $(p-1)!\equiv -1 \pmod p$. Como Wilson vale trivialmente para $p=2$, suponemos que p es impar.

Tomando $n=p-1$ y $x=0$ en (12.19) tenemos

$$\sum_{k=0}^{p-1}(-1)^k\binom{p-1}{k}(-k)^{p-1}=(p-1)!$$

Usando el pequeño teorema de Fermat y que p es impar tenemos

$$\sum_{k=1}^{p-1}(-1)^k\binom{p-1}{k}\equiv(p-1)! \pmod p$$

La identidad de Pascal $\binom{p}{k}=\binom{p-1}{k}+\binom{p-1}{k-1}$ implica que $\binom{p-1}{k}\equiv-\binom{p-1}{k-1} \pmod p$ para $1\leq k\leq p-1$, pues $p\mid\binom{p}{k}$ en este caso. Iterando, tenemos que

$$\binom{p-1}{k}\equiv-\binom{p-1}{k-1}\equiv(-1)^2\binom{p-1}{k-2}\equiv\cdots\equiv(-1)^k\binom{p-1}{0}\equiv(-1)^k \pmod p$$

Luego,

$$\sum_{k=1}^{p-1}(-1)^k\binom{p-1}{k}\equiv\sum_{k=1}^{p-1}(-1)^k(-1)^k=\sum_{k=1}^{p-1}1=(p-1)$$

y por lo tanto, $(p-1)!\equiv(p-1)\equiv-1 \pmod p$, como queríamos ver. ◊

12.4. El Teorema de Lucas †

Supóngase que queremos saber si un dado número combinatorio $\binom{n}{k}$ es divisible o no por cierto entero m. Para esto basta saber si es divisible por cada primo p que aparece en

la factorización de m. Parece una pregunta muy general para ser resuelta. Sin embargo, el Teorema de Lucas da cuenta de ello. Prepárese para disfrutar, porque lo que viene es una verdadera joya.

Sea p un número primo. La representación p-ádica de $n \in \mathbb{N}$ es

$$n = n_r p^r + n_{r-1} p^{r-1} + \cdots + n_2 p^2 + n_1 p + n_0$$

donde $0 \leq n_i \leq p-1$ para $i = 0, \ldots, r$ y $n_r > 0$. Ahora, dados $0 \leq k \leq n$, miramos las representaciones p-ádicas de ambos. Para poder compararlas, permitimos que los coeficientes del más pequeño puedan ser 0. De este modo, escribimos

$$\begin{aligned} n &= n_r p^r + n_{r-1} p^{r-1} + \cdots + n_2 p^2 + n_1 p + n_0 \\ k &= k_r p^r + k_{r-1} p^{r-1} + \cdots + k_2 p^2 + k_1 p + k_0 \end{aligned} \tag{12.20}$$

donde $n_r > 0$.

El siguiente teorema relaciona números combinatorios, congruencias módulo un primo p y representaciones p-ádicas. En efecto, dice que $\binom{n}{k}$ es congruente módulo p al producto de los números combinatorios $\binom{n_i}{k_i}$ formados con los coeficientes de los desarrollos p-ádicos de n y k, mirados simultáneamente.

Teorema 12.13 (Lucas, 1878). *Si $0 \leq k \leq n$ son enteros y p es un primo, entonces*

$$\binom{n}{k} \equiv \prod_{i=1}^{r} \binom{n_i}{k_i} \pmod{p} \tag{12.21}$$

donde los n_i, k_i, con $i = 0, \ldots, r$ son como en (12.20).

La prueba es muy bonita e instructiva.

Demostración. □

Ejemplo.

El caso binario

El triángulo de Sierpinski

12.5. Coeficientes multinomiales †

Cuando vimos como ordenar con repeticiones en la Sección §xxx definimos el número $\binom{n}{r_1,r_2,\ldots,r_m}$ como el número de formas distintas de ordenar n objetos en una fila, donde hay m tipos distintos de objetos y r_i objetos de cada tipo i. En la Proposición (11.11) vimos que

$$\binom{n}{r_1, r_2, \ldots, r_m} = \frac{n!}{r_1! r_2! \cdots r_m!}$$

Vimos que los números $\binom{n}{k}$ se llaman coeficientes binomiales, ya que por el teorema del binomio de Newton, estos números son casualmente los coeficientes que aparecen en el desarrollo del binomio $(a+b)^n$. ¿Qué podemos decir sobre $(a+b+c)^n$? Y más generalmente, que podemos decir sobre el desarrollo de $(x_1 + x_2 + \cdots + x_m)^n$?

Resulta que el binomio de Newton se puede generalizar a monomios de m-términos, es el llamado teorema del multinomio, formulado por Leibnitz y probado luego por Johann Bernoulli.

Teorema 12.14 (del multinomio)**.** *Para todo $n, m \in \mathbb{N}$ vale*

$$(x_1 + x_2 + \cdots + x_m)^n = \sum_{\substack{0 \le r_1, r_2, \ldots, r_m \le n \\ r_1 + r_2 + \cdots + r_m = n}} \binom{n}{r_1, r_2, \ldots, r_m} x_1^{r_1} x_2^{r_2} \cdots x_m^{r_m}.$$

No daremos la demostración, aunque mencionamos que la prueba combinatoria es muy similar a la dada para el binomio de Newton. Por este teorema es que los números $\binom{n}{r_1,r_2,\ldots,r_m}$ reciben el nombre de *coeficientes multinomiales*.

Ejemplo. Supongamos que queremos saber la potencia cuarta del trinomio $x+y+z$. Usando el teorema multinomial tenemos

$$(x+y+z)^4 = \sum_{i+j+k=4} \binom{4}{i,j,k} x^i y^j z^k.$$

O sea

$$\begin{aligned}
&\tbinom{4}{4,0,0}x^4 + \tbinom{4}{3,1,0}x^3y + \tbinom{4}{3,0,1}x^3z + \tbinom{4}{2,2,0}x^2y^2 + \tbinom{4}{2,1,1}x^2yz + \\
&\tbinom{4}{2,0,2}x^2z^2 + \tbinom{4}{1,3,0}xy^3 + \tbinom{4}{1,2,1}xy^2z + \tbinom{4}{1,1,2}xyz^2 + \tbinom{4}{1,0,3}xz^3 + \\
&\tbinom{4}{0,4,0}y^4 + \tbinom{4}{0,3,1}y^3z + \tbinom{4}{0,2,2}y^2z^2 + \tbinom{4}{0,1,3}yz^3y + \tbinom{4}{0,0,4}z^4.
\end{aligned}$$

Por ejemplo $\binom{4}{3,1,0} = \frac{4!}{3!1!} = 4$, $\binom{4}{2,2,0} = \frac{4!}{2!2!} = 6$ y $\binom{4}{2,1,1} = \frac{4!}{2!1!1!} = 12$. Luego,

$$\begin{aligned}
(x+y+z)^4 = x^4 + y^4 + z^4 + 4(x^3y + x^3z + xy^3 + xz^3 + y^3z + yz^3) + \\
6(x^2y^2 + x^2z^2 + y^2z^2) + 12(x^2yz + xy^2z + xyz^2).
\end{aligned}$$

Imagínese que flor de fastidio tener que desarrollar a mano este trinomio... ◊

Como los coeficientes multinomiales son generalizaciones de los coeficientes binomiales, para los multinomiales valen identidades similares a las que valen para los binomiales.

- *Simetría:*
$$\binom{n}{r_1,\, r_2,\, \ldots, r_m} = \binom{n}{r_{\sigma(1)},\, r_{\sigma(2)}, \ldots,\, r_{\sigma(m)}}$$
donde σ es cualquier permutación de I_n, es decir $\{\sigma(1), \sigma(2), \ldots, \sigma(n)\} = \{1, 2, \ldots, n\}$.

- *Identidad de Pascal:* La identidad de Pascal $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$ puede escribirse así
$$\binom{n}{k,\, n-k} = \binom{n-1}{k,\, n-k-1} + \binom{n-1}{k-1,\, n-k-1}$$
En general tenemos:
$$\binom{n}{r_1, r_2, \ldots, r_m} = \sum_{i=1}^{m} \binom{n}{r_1, \ldots, r_{i-1}, r_i - 1, r_{i+1}, \ldots, r_m}.$$
Es decir,
$$\tbinom{n}{r_1,r_2,\ldots,r_m} = \tbinom{n}{r_1-1,r_2,\ldots,r_m} + \tbinom{n}{r_1,r_2-1,r_3,\ldots,r_m} + \cdots + \tbinom{n}{r_1,r_2,\ldots,r_{m-1},r_m-1}.$$

- *Suma:* Tomando $x_1 = x_2 = \cdots = x_m = 1$, del teorema multinomial sale que
$$\sum_{\substack{0 \le r_1, r_2, \ldots, r_m \le n \\ r_1 + r_2 + \cdots + r_m = n}} \binom{n}{r_1, r_2, \ldots, r_m} = m^n.$$
En el ejemplo anterior, $m = 3$ y $n = 4$, y la suma de los multinomiales es
$$\sum_{i+j+k=4} \binom{4}{i, j, k} = 3 \cdot 1 + 6 \cdot 4 + 3 \cdot 6 + 3 \cdot 12 = 81 = 3^4.$$

Dejamos como ejercicio chequear con ejemplos primero estas identidades y, si se anima, tratar de probarlas luego.

12.6. Números de Stirling *

A continuación veremos dos cosas que nos quedaron pendientes: el número de formas

(1) de ordenar cíclicamente objetos distintos alrededor de círculos indistinguibles;

(2) de distribuir objetos distintos en categorías indistinguibles.

Estas cantidades están medidas por los llamados números de Stirling[*] de primer y segundo tipo, respectivamente.

[*] James Stirling (1692–1770), matemático escocés quien los estudió por primera vez.

12.6.1. Números de Stirling de primer tipo

Dados enteros r, n con $0 \leq n \leq r$, sea $s(r,n)$ el número de formas de ordenar cíclicamente r objetos distintos alrededor de n círculos indistinguibles, tal que cada círculo contenga al menos un objeto; es decir

$$s(r,n) = \#\left\{\begin{array}{c}\text{arreglos circulares de } r \text{ objetos distintos}\\ \text{alrededor de } n \text{ círculos indistinguibles,}\\ \text{al menos un objeto por círculo.}\end{array}\right\}$$

Podemos pensar al problema como en *sentar personas alrededor de mesas similares, y que no quede ninguna vacía*[**].

En el ejemplo de las 2 y 3 mesas de la página 330, vimos que $s(6,2) = 274$ y $s(6,3) = 225$. Los siguientes resultados son básicos y resultan claros:

$$\begin{aligned} s(r,0) &= 0 && \text{if } r \geq 1,\\ s(r,1) &= (r-1)! && \text{if } r \geq 0,\\ s(r,r) &= 1 && \text{if } r \geq 2,\\ s(r,r-1) &= \tbinom{r}{2} && \text{if } r \geq 2. \end{aligned}$$

Aunque es difícil obtener una fórmula para $s(r,n)$, es interesante notar que se puede obtener fórmula recursiva fácilmente.

Proposición 12.15. *Para todo $r, n \in \mathbb{N}$ con $n \geq r$ se tiene*

$$s(r,n) = s(r-1,n-1) + (r-1)s(r-1,n). \tag{12.22}$$

Demostración. Sean $a_1, a_2, \ldots, a_r$ los r objetos. Haremos inducción en r. Pueden pasar dos cosas: (i) o a_r es el único objeto en un círculo, (ii) o a_r está junto a otros objetos en un círculo.

(i) Por HI, hay $s(r-1,n-1)$ formas en que a_r puede estar solo en un círculo.

(ii) Hay $s(r-1,n)$ formas de ordenar los objetos $a_1, \ldots, a_r$ en los n círculos. Hay $r-1$ formas de ubicar a_r a la derecha de alguno de los otros objetos. Por **PM** hay en total $(r-1)s(r-1,n)$ formas de a_r no esté solo.

Por el **PA**, hya en total $s(r-1,n-1) + (r-1)s(r-1,n)$ formas de ordenar cíclicamente r objetos en n círculos iguales, con al menos un objeto por círculo, que por definición es $s(r,n)$. Luego, vale (12.22). □

Usando (12.22) y los valores iniciales se pueden obtener valores para $s(r,n)$ a partir de los $s(r',n')$ con $r' \leq r$, $n' \leq n$.

12.6.2. Números de Stirling de segundo tipo

Bolas distintas en cajas iguales

Interesa contar el número de formas de distribuir r bolas distintas en n cajas iguales tal que ninguna caja quede vacía, usualmente denotado por

$$S(r,n).$$

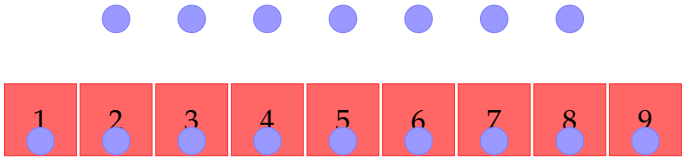
[**]Tener en cuenta para las fiestas de cumpleaños y fin de año!

Cuadro 12.1: Valores para $s(r,n)$, con $0 \leq r \leq n \leq 7$.

n	0	1	2	3	4	5	6	7
$s(0,n)$	0							
$s(1,n)$	0	1						
$s(2,n)$	0	1	1					
$s(3,n)$	0	2	3	1				
$s(4,n)$	0	6	11	6	1			
$s(5,n)$	0	24	50	35	10	1		
$s(6,n)$	0	120	274	225	85	15	1	
$s(7,n)$	0	720	1764	1624	735	175	21	1

Luego $r \geq n$ y hay al menos una bola por caja.

Por ejemplo, si $r = 16$ y $n = 9$,



Es obvio que $S(0,0) = 1$ y que

$$S(r,0) = S(0,n) = 0, \qquad S(r,1) = S(r,r) = 1$$

para $r, n \geq 1$. Además, es fácil chequear que también valen:

$$\begin{aligned} S(r,n) &= 0, \qquad n > r \geq 1, \\ S(r,n) &> 0, \qquad r \geq n \geq 1. \end{aligned}$$

Con un poco más de esfuerzo se pueden probar algunos otros casos particulares, por ejemplo

$$\begin{aligned} &S(r,2) = 2^{r-1} - 1, \\ &S(r,3) = \tfrac{1}{2}(3^{r-1} + 1) - 2^{r-1}, \\ &S(r,r-1) = \tbinom{r}{2}, \\ &S(r,r-2) = \tbinom{r}{3} + 3\tbinom{r}{4}. \end{aligned}$$

Dejamos la prueba de estas identidades como ejercicio para el lector curioso y aplicado. Es instructivo chequear aunque sea algunos casos particulares para valores pequeños de r y n.

Veamos que podemos dar una fórmula recursiva para los $S(r,n)$.

Proposición 12.16. *Para todo $r, n \in \mathbb{N}$ con $r \geq n$ se tiene*

$$S(r,n) = S(r-1,n-1) + nS(r-1,n). \tag{12.23}$$

Demostración. Sean $a_1, a_2, \ldots, a_r$ los r objetos. Cualquiera sea la forma en que los r objetos esten distribuidos en las n cajas idénticas tal que ninguna está vacía, pueden pasar 2 cosas: (i) o bien a_n es el único objeto en la caja que ocupa, (ii) o bien a_n se encuentra con otros objetos en la caja.

(i) Hay $S(r-1, n-1)$ formas de acomodar los objetos $a_1, \ldots, a_{r-1}$ en las $n-1$ cajas restantes.

(ii) Los objetos $a_1, \ldots, a_{r-1}$ se pueden colocar de $S(r-1, n)$ formas en n cajas distintas, y luego a_r puede ser colocado de n formas distintas. Luego, por **PA** hay $S(r, n) = S(r-1, n-1) + nS(r-1, n)$ formas de colocar los r objetos en n cajas idénticas, sin que haya ninguna vacía. □

Usando (12.23) y los valores iniciales se pueden obtener valores para $S(r, n)$ a partir de los $S(r', n')$ con $r' \leq r$, $n' \leq n$.

Cuadro 12.2: Valores para $S(r, n)$, con $0 \leq r \leq n \leq 7$.

n	0	1	2	3	4	5	6	7
$S(0,n)$	0							
$S(1,n)$	0	1						
$S(2,n)$	0	1	1					
$S(3,n)$	0	1	3	1				
$S(4,n)$	0	1	7	6	1			
$S(5,n)$	0	1	15	25	10	1		
$S(6,n)$	0	1	31	90	65	15	1	
$S(7,n)$	0	1	63	301	350	140	21	1

Existe una expresión cerrada para estos números:

$$S(r, n) = \frac{1}{n!} \sum_{j=0}^{n-1} (-1)^j \binom{n}{j} (n-j)^r \tag{12.24}$$

La demostración, que daremos más adelante, usa el principio de inclusión-exclusión. Notar que tomando $r = n$ se obtiene la expresión (12.19), pues $S(n, n) = 1$.

Ejemplo. Calculemos $S(8, 5)$ de dos formas. Usando (12.23) y la tabla de arriba tenemos

$$S(8, 3) = S(7, 2) + 3S(7, 3) = 63 + 3 \cdot 301 = 966.$$

Usando la fórmula (12.24) tenemos

$$\begin{aligned} S(8,3) &= \tfrac{1}{3!} \sum_{j=0}^{3} (-1)^j \tbinom{3}{j} (3-j)^8 = \tfrac{1}{6} \{ \tbinom{3}{0} 3^8 - \tbinom{3}{1} 2^8 + \tbinom{3}{2} 1^8 \} \\ &= \tfrac{1}{2} \{ 3^7 - 2^8 + 1 \} = \tfrac{1}{2} (2187 - 256 + 1) = 966. \end{aligned}$$

El hada de los números anda cerca. ◊

Nota. El caso que falta, de distribuir r bolas iguales en n cajas iguales es más difícil de tratar y está más allá de las posibilidades de este curso. Sin embargo, mencionamos que el número de formas de distribuir r bolas iguales en n cajas iguales está dado por el número de particiones de r en n partes, denotada $p_n(r)$, o menos (ver la subsección siguiente).

Resumen de cómo distribuir r en n

Resumiendo los resultados de la sección, tenemos la siguiente tabla que indica de cuántas maneras se pueden distribuir r bolas en n cajas, en todos los casos posibles.

Cuadro 12.3: Formas de distribuir r bolas en n cajas.

r bolas	n cajas	# (sin restricciones)	# (≥ 1 bola x caja)
distintas	distintas	n^r	$r!\binom{n}{r}$
iguales	distintas	$\binom{r+n-1}{r}$	$\binom{n}{r}$
distintas	iguales	??	$S(r,n)$
iguales	iguales	??	$p_1(r)+\cdots+p_n(r)$

12.6.3. Desarrollos polinomiales *

A modo de curiosidad, sólo mencionaremos que estos números aparecen (al igual que los números combinatorios) como coeficientes en desarrollos polinómicos. Veamos esto. Dado $n \in \mathbb{N}$ y x un símbolo (puede ser un número real o una indeterminada) definimos las expresiones[***]

$$\begin{aligned}(x)^n &= x(x+1)(x+2)\cdots(x+n-1),\\ (x)_n &= x(x-1)(x-2)\cdots(x-n+1).\end{aligned} \tag{12.25}$$

Por ejemplo, si $r=3$ ó $r=5$ tenemos

$$\begin{aligned}(x)^3 &= x(x+1)(x+2) = 2x+3x^2+x^3,\\ (x)^5 &= x(x+1)(x+2)(x+3)(x+4) = 24x+50x^2+35x^3+10x^4+x^5;\end{aligned}$$

que podemos escribir así

$$\begin{aligned}(x)^3 &= s(3,1)x+s(3,2)x^2+s(3,3)x^3,\\ (x)^5 &= s(5,1)x+s(5,2)x^2+s(5,3)x^3+s(5,4)x^4+s(5,5)x^5.\end{aligned}$$

[***] los nombres en inglés son "falling factorial" para $(x)_n$ y "rising factorial" para $(x)_n$, pues si $x=n$ tenemos $(n)_n = n!$

Ahora, escribamos las potencias x^r en términos de los números $(x)_n$'s. Para $r = 2, 3, 4$ es más o menos fácil hacerlo a mano y tenemos (chequear!)

$$\begin{aligned} x^2 &= x + x(x-1), \\ x^3 &= x + 3x(x-1) + x(x-1)(x-2), \\ x^4 &= x + 7x(x-1) + 6x(x-1)(x-2) + x(x-1)(x-2)(x-3). \end{aligned}$$

Notar que estas expresiones se pueden escribir así

$$\begin{aligned} x^2 &= S(2,1)(x)_1 + S(2,2)(x)_2, \\ x^3 &= S(3,1)(x)_1 + S(3,2)(x)_2 + S(3,3)(x)_3, \\ x^4 &= S(4,1)(x)_1 + S(4,2)(x)_2 + S(4,3)(x)_3 + S(4,4)(x)_4. \end{aligned}$$

Estas bonitas relaciones que hemos observado no pueden ser casualidad. En efecto, la armonía del universo se confabula una vez mas a nuestro favor y tenemos las siguientes expresiones generales.

Proposición 12.17. *Con las notaciones de arriba, valen las expresiones*

$$\begin{aligned} (x)^r &= \sum_{n=0}^{r} s(r,n)\, x^n, \\ x^r &= \sum_{n=0}^{r} S(r,n)\, (x)_n. \end{aligned} \tag{12.26}$$

para enteros n y r.

Demostración. Usaremos inducción y las relaciones de recurrencia vistas para los números $r(r,n)$ y $S(r,n)$.

Para la primera fórmula, el paso inicial de la inducción es claro pues $(x)^1 = x$ y $\sum_0^1 s(1,n)x^n = s(1,0) + s(1,1)x = x$. Para el paso inductivo, suponemos que vale para $r-1$ y hacemos

$$\begin{aligned} (x)^r &= x(x+1)\cdots(x+r-2)(x+r-1) = (x)^{r-1}(x+r-1) \\ &= \left(\sum_{n=0}^{r-1} s(r-1,n)x^n\right)(x+r-1) \\ &= \sum_{n=0}^{r-1} s(r-1,n)x^{n+1} + (r-1)\sum_{n=0}^{r-1} s(r-1,n)x^n \\ &= \sum_{n=1}^{r} \Big(s(r-1,n-1) + (r-1)s(r-1,n)\Big)x^n = \sum_{n=1}^{r} s(r,n)x^n, \end{aligned}$$

donde hemos hecho el cambio de variable $m = n+1$, la recurrencia (12.22) y el hecho de que $s(r-1,0) = s(r-1,r) = 0$.

La segunda fórmula sale similarmente, usando que $(x)_r = (x)_{n-1}(x-n+1)$ y la recurrencia (12.23), y lo dejamos como ejercicio para ese lector curioso y aplicado que todos llevamos dentro. □

12.7. Composiciones y particiones *

Definiciones

Una *partición* de $n \in \mathbb{N}$ es una representación de n como suma de números naturales. Por ejemplo, $7+1$ y $5+2+1$ son particiones de 8, pero $4+0+3+0+1$ y $3+6-1$ no lo son. Si

$$n = n_1 + n_2 + \cdots + n_k$$

$n_1, n_2, \ldots, n_k$ se llaman las *partes* de la partición y decimos que $\lambda = (n_1, n_2, \ldots, n_k)$ es una *partición de n en k-partes* o una *k-partición*.

Una *composición* de n es una partición de n en las que el orden importa. Por ejemplo, $7+1$ y $1+7$ son dos composiciones distintas de 8 (aunque la misma partición).

Definimos los siguientes números:

$$\begin{aligned} p(n) &= \#\{ \text{ particiones de } n\} \\ p_k(n) &= \#\{ \text{ particiones de } n \text{ en } k \text{ partes}\} \\ c(n) &= \#\{ \text{ composiciones de } n\} \\ c_k(n) &= \#\{ \text{ composiciones de } n \text{ en } k \text{ partes}\} \end{aligned}$$

Ejemplo. Las particiones de 4 son

$$4, \qquad 3+1, \qquad 2+2, \qquad 2+1+1, \qquad 1+1+1+1$$

y las composiciones de 4 son

4,	3+1,	2+1+1,	1+1+1+1,
	2+2,	1+2+1,	
	1+3,	1+1+2,	

Luego $p(4) = 1+2+1+1 = 5$ y $c(4) = 1+3+3+1 = 8$. ◊

Composiciones Las composiciones se pueden contar fácilmente. Si representamos gráficamente al número n con n círculos •, separando los círculos con barras verticales obtenemos una partición de n. Por ejemplo, si $n = 9$,

$$\bullet\bullet \mid \bullet\bullet\bullet \mid \bullet \mid \bullet\bullet\bullet$$

representa a la partición

$$9 = 2+3+1+2.$$

Contando todas las posibles formas de introducir estas barras estamos contando todas las composiciones de n. Si queremos una composición en k partes de n, debemos introducir $k-1$ barras en los $n-1$ posibles lugares. Luego,

$$c_k(n) = \binom{n-1}{k-1}.$$

Ahora, el número total de composiciones es

$$c(n) = \sum_{k=1}^{n} c_k(n) = \sum_{k=1}^{n} \binom{n-1}{k-1} = \sum_{j=0}^{n} \binom{n-1}{j} = 2^{n-1}.$$

Particiones Los números $p(n)$ y $p_k(n)$ son más difíciles de estudiar. Una forma de estudiarlos es asociarles un *diagrama de Ferrer*. Por ejemplo, la particion $P = (6, 4, 3, 2)$, o sea $15 = 6 + 4 + 3 + 2$...

El diagrama conjugado es intercambiar filas por columnas... que da la partición transpuesta o conjugada $P^t = (4, 4, 3, 2, 1, 1)$: $15 = 4 + 4 + 3 + 2 + 1 + 1$.

Con estas cosas se puede deducir el siguiente resultado.

Teorema 12.18 (Euler). *Si $k, n \in \mathbb{N}$ con $k \leq n$ vale*

$$p_k(n) = \#\{\textit{particiones de } n \textit{ cuya parte más grande es } k\}$$

Ejemplo. Sea $n = 8$ y $k = 3$. El número de particiones de 8 en 3 partes, $p_3(8)$, es igual al número de particiones de 8 cuya parte mayor es 3.

part. de 8 en 3	part. de 8, parte mayor $= 3$	# partes
6+1+1	3+1+1+1+1+1	(6 partes)
5+2+1	3+2+1+1+1	(5 partes)
4+3+1	3+2+2+1	(4 partes)
4+2+2	3+3+1+1	(4 partes)
3+3+2	3+3+2	(3 partes)

Notar que $(3, 3, 2)$ es autoconjugada. Luego $p_3(8) = 5$. [*] ♢

12.8. Ejercicios

"El binomio de Newton es tan bello como la Venus de Milo. Lo que hay es poca gente que se dé cuenta de ello". Fernando Pessoa

[*] dar la relacion con los numeros de Stirling $S(r, n)$

Apéndice A

Epílogo: algunas listas útiles

Colores usados

Algunos ejemplos con mas colores seleccionados.

A.1. Lista de símbolos

Símbolos generales

$\Box, \Diamond, *, \dagger, \ddagger$	pág xiii - ix

Lógica

V, F	pág 4
p, q, r	pág 4
$\neg, \vee, \wedge$; $\neg p, p \vee q, p \wedge q$	pág 5
$p \rightarrow q, p \leftrightarrow q$	pág 8
$P \equiv Q$	pág 11
$P(x), P(x, y)$	pág 13
$\forall, \exists, \exists!$; $\forall x P(x), \exists x P(x), \exists! x P(x)$	pág 14
$p \Rightarrow q, p \Leftrightarrow q$	pág 21

Conjuntos

$\in, \notin, x \in A, x \notin A$	pág 30
$A = B, A \neq B,$	pág 30
$A \subseteq B, A \nsubseteq B$	pág 30, 31

Relaciones y Funciones

Conjuntos de números

$\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$	pág 69
$\mathbb{Q}(\sqrt{2})$	pág 69
$\mathbb{Q}^c$	pág 69
$\mathbb{C}$	pág 88
$\mathbb{P}$	pág 137
$\mathbb{Z}_m$	pág 163
$\mathbb{Z}_m^*, \mathcal{U}(\mathbb{Z}_m)$	pág 163

Números

$x + y$, $x \cdot y$, $x < y$	pág 71-73
0, 1	pág 74
$-x$, x^{-1}	pág 74
$x - y$, $\frac{x}{y}$	pág 77
$\lvert a \rvert$	pág 86

Inducción y recurrencia

$s(n)$	pág 93
$P(1)$, $P(k)$, $P(k+1)$	pág 95
$x_1 + x_2 + \cdots + x_n$, $x_1 x_2 \cdots x_n$	pág 103
$\sum_{i=1}^n x_i$, $\prod_{i=1}^n x_i$	pág 104
$n!$	pág 104
a^n	pág 104
$\{a_n\}_{n\in\mathbb{N}}$	pág 105

Aritmética entera y modular

$a \mid b$, $a \nmid b$	pág 134
$\mathrm{Div}(n)$	pág 136
I_a, μ_b	pág 140
(a, b)	pág 145

Números complejos

Combinatoria

A.2. Abreviaturas y acrónimos

- ca.: del latin *circa*, significa al rededor o cerca, se usa en fechas en donde no hay precision exacta sino aproximada.
- cf.: del latín *confer*. Se usa como *comparar con* o *ver*.
- e.g.: del latín *exempli gratia*, o sea *por ejemplo*.
- i.e.: del latín *id est*, o sea *esto es*, *es decir*.
- pág.: página.
- QED: del latín *quod erat demostrandum*, o sea *que era lo que se quería demostrar*, *lo que debía ser demostrado*. Algunos creen que se trata de *queda entonces demostrado*.

- HI: Hipótesis inductiva.
- PI: Principio de inducción.
- PIC: Principio de inducción corrida.
- PIF: Principio de inducción fuerte.
- BO ó PBO: Buena ordenación o Principio de buena ordenación.

- TFA: teorema fundamental de la aritmética.
- mcd: máximo común divisor.
- mcm: mínimo común múltiplo.
- TCR: teorema chino del resto.

- **PA**: principio de adición.
- **PB**: principio de biyección.
- **PC**: principio del complemento.
- **PI**: principio de inyección.
- **PM**: principio de multiplicación.

A.3. Lista de tablas y figuras

- Tabla: suma de números combinatorios (pág. 364).
- Teorema de Lucas (falta).
- Números de Stirling de primer tipo $s(r, n)$ (falta).
- Números de Stirling de segundo tipo $S(r, n)$ (pág. 376).
- Formas de distribuir r bolas en n cajas con condiciones (Cuadro **??**, pág. 377).
- Tabla: particiones de 8 en 3 partes. (Cuadro 12.7, pág. 379).

A.4. Lista de teoremas y resultados importantes

Por orden de aparición, aparecen recuadrados en el texto.

- Leyes de De Morgan (Proposición 2.1, pág. 49).
- Axiomas de los números reales (Sección §**??**, pág. **??**).
- Axiomas de los números naturales o axiomas de Peano (Sección §5.1, pág. 131).
- Principio de inducción (Teorema 5.4, pág. 134).
- Principio de inducción corrida (Teorema **??**, pág. **??**).
- Sumas de potencias consecutivas (Proposición 5.11, pág. 171).
- Suma geométrica (Proposición 5.12, pág. 173).
- Principio de buena ordenación (Teorema 5.18, pág. 180).
- Principio de inducción fuerte (Teorema 5.6, pág. 141).
- Algoritmo de la división entera (Teorema 6.12, pág. 203).
- Combinaciones lineales enteras (Sección §6.4.1, pág. 212).
- Algoritmo de Euclides (pág. 215).
- Propiedad fundamental de los números primos (xxx).
- Teorema fundamental de la aritmética (Teorema 6.24, pág. 215).
- Relación entre m.c.d. y m.c.m. (xxx).
- Reglas de divisibilidad (xxx).
- Solución de la ecuación lineal de congruencia (Teorema **??**, pág. **??**).
- Teorema chino del resto (Teorema **??**, pág. **??**).
- Teorema de Euler (Teorema **??**, pág. **??**).
- Teorema de Euler-Fermat (Teorema 8.24, pág. 275).
- Teorema de Wilson (Teorema 8.25, pág. 277).
- El teorema de Lucas (xxx).
- Raíces de la unidad (xxx).
- Principio de adición (Teorema 11.1, pág. 306).
- Principio de multiplicación (Teorema 11.2, pág. 308).
- Principio del complemento (Teorema 11.3, pág. 311).

- Principio de inyección (Proposición 11.4, pág. 311).
- Principio de biyección (Proposición 11.5, pág. 311).
- Número de formas de ordenar n objetos en fila (xxx).
- Número de formas de ordenar n objetos en círculos (xxx).
- Número de formas de elegir k objetos de n (xxx).
- Número de formas de distribuir objetos iguales (xxx).
- Número de formas de distribuir objetos distintos (xxx).
- Identidad de Pascal (Proposición 12.2, pág. 354).
- Binomio de Newton (Teorema 12.4, pág. 357).
- Identidad de Chu-Shih-Chieh (Teorema 12.9, pág. 366).
- Identidad de van der Monde (Teorema **??**, pág. **??**).
- Principio del Palomar (pág. 344).
- Principio del Palomar generalizado (Proposición 11.17, pág. 345).
- Principio de Inclusión-Exclusión (xxx).
- Número de funciones de I_n en I_m (Teorema 11.18, pág. 346)

A.5. Lista de notas históricas

- Sobre los diagramas de Venn (pág. 59?)
- Sobre los pares ordenados (pág. 73?)
- Anécdota de Gauss a los 10 años (pág. 164?)
- Sobre la leyenda del ajedrezs (pág. 175?)
- Sobre la definición de congruencia de Gauss (pág. 232?)
- Anécdota de Hardy y Ramanujan sobre la patente de taxi (pág. ???)
- Sobre el pequeño Teorema de Fermat (pág. 273)
- Sobre el Teorema de Wilson (pág. 279)

A.6. Lista de grandes matemáticos

Damos a continuación una lista de personajes que más contribuyeron a la lógica matemática, al álgebra, la aritmética, la teoría de números y la combinatoria. La mayoría son matemáticos, pero tambien hay físicos, astrónomos y filósofos. Los ordenamos por grupos, y dentro de éstos cronológicamente. Hasta el siglo XVII damos una pequeña reseña biográfica de cada uno, para el siglo XVIII y XIX sólo los años de nacimiento y muerte. No damos la lista para el siglo XX. [*]

- Griegos
  - *Pitágoras* (Samos, ca. 570 a.C. – ca. 495 a.C.). Filósofo y matemático, considerado el primer matemático puro. Desarrolló la geometría y la aritmética.
  - *Aristóteles* (Estagira, 384 a.C. – 322 a.C.). Filósofo, lógico y científico.
  - *Euclides* de Alejandría (ca. 325 a.C. – ca. 265 a.C.). Conocido como el "padre de la geometría". Sus *Elementos* es uno de los trabajos mas influyentes de la historia de la matemática.
  - *Arquímedes* (Siracusa, 287 a.C. – 212 a.C.). El gran matemático de su época. Sus contribuciones en geometría revolucionaron el área y sus métodos anticiparon en 2000 años el cálculo de Leibnitz y Newton.
  - *Diofanto* de Alejandría (entre 200/214 – entre 284/298). Conocido como el "padre del algebra". Estudió las ecuaciones que hoy llevan su nombre (coeficientes enteros y soluciones racionales).


- Medievales de oriente
  - *Brahmagupta* (598–670). Fue el matemático indio mas sobresaliente de su tiempo. Realizó aportes en sistemas de numeración, incluyendo algoritmos para calcular raíces cuadradas y la solución de las ecuaciones cuadráticas.
  - *Bhaskara I* (Saurastra, ca. 600 – ca. 680). Matemático indio, aparentemente el primero en escribir los números en el sistema indo-arábigo posicional de base 10.
  - *al-Khwarizmi* (ca. 790 – ca. 850). Matemático islámico que escribió los números en sistema indo-arábigo y uno de los primeros en usar el 0 en el sistema posicional. La palabra "algoritmo" proviene de su nombre. De su tratado *Hisab al-jabr wál-muqabala* se deriva la palabra "algebra" y puede ser el primer libro sobre álgebra.
  - *Alhacén* (ca. 950 – ca. 1040). FALTA.
- Italianos del siglo XVI

[*] fuentes: wikipedia, MacTutor

  - *Leonardo de Pisa* (1170–1250). O Leonardo Pisano, conocido como Fibonacci. En su libro *Liber Abacci* (el libro del ábaco) de 1202, introdujo en Europa los números arábigos y el sistema posicional indo-arábigo de base decimal que usamos actualmente.
  - *Luca Pacioli* (Sansepolcro, 1445–1517). Publicó el libro *Suma* en 1494, sumariando toda la matemática conocida en esa época.
  - *Scipione del Ferro* (Bologna, 1465–1526). Conocido por ser el primero en dar la solución de una ecuación cúbica general.
  - *Niccolo Fontana* (Brescia, 1499 ó 1500 – 1557). Conocido como Tartaglia "el tartamudo". Dio la solución algebraica de las ecuaciones cúbicas, publicadas contra su voluntad en el libro Ars MAgna de Cardano.
  - *Girolamo Cardano* (Pavia, 1501–1576).doctor and mathematician who is famed for his work Ars Magna which was the first Latin treatise devoted solely to algebra. In it he gave the methods of solution of the cubic and quartic equations which he had learnt from Tartaglia.
  - *Ludovico Ferrari* (Bologna, 1522–1565). Encontró la solución de la ecuación cuártica general.

- del siglo XVII
  - *Marin Mersenne* (Oizé, 1588–1648). Matemático francés.
  - *René Descartes* (La Haye, 1596–1650). Matemático francés.
  - *Pierre de Fermat* (Beaumont-de-Lomange, 1601–1665). Matemático francés. abogado y oficial del gobierno. Matemático aficionado sobresaliente, recordado por sus trabajos en teoría de números. En particular por el Último Teorema de Fermat, que fuera conjeturado por el y probado por Andrew Wiles recien en 1995.
  - *John Pell* (Southwick, 1611–1685). Matemático inglés.
  - *Blaise Pascal* (Clermont, 1623–1662). Matemático francés.
  - *Sir Isaac Newton* (Woolsthorpe, 1643–1727). El mayor matemático y físico inglés de su generación. Sentó las bases para el cálculo diferencial. Sus trabajos en óptica y gravitación lo transformaron en uno de los mas grandes científicos del mundo.
  - *Gottfried Leibniz* (Leipzig, 1646–1716). Matemático alemán que desarrolló el cálculo diferencial e integral con las notaciones actuales. También fue filósofo e inventó una máquina calculadora.
  - *Bernoulli, Jacob* (Basel, 1654–1705). Matemático suizo. Fué el primero en usar el término integral. Estudió la catenaria, la curva de una cuerda suspendida. Fue uno de los primeros en usar coordenadas polares.
  - *Abraham de Moivre* (Vitry-le-François, 1667–1754). Matemático francés, pionero en el desarrollo de la geometría analítica y la teoría de las probabilidades.
  - *Johan Bernoulli* (Basel, 1667–1748). Matemático suizo, estudió la reflexión y refracción de la luz, las trayectorias ortogonales de familias de curvas, cuadraturas de areas por series y la braquistocrona.

  - *Nicolaus (I) Bernoulli*, (Basel, 1687–1759). Conocido por sus correspondencias con otros matemáticos, inluídos Euler y Leibniz.
  - *Christian Goldbach* (Königsberg, 1690–1764). Matemático prusiano, famoso su conjetura en una carta a Euler de que todo entero mayor que 2 es suma de dos primos.
  - *James Stirling* (1692–1770). Matemático escocés. Su trabajo más importante *Methodus Differentialis* en 1730 es un tratado sobre series infinitas, sumación, interpolación y cuadratura.
  - *Nicolaus (II) Bernoulli* (Basel, 1695–1726).

- Siglo XVIII
  - (1700-1782) Bernoulli, Daniel
  - (1707-1783) Euler
  - (1710-1790) Bernoulli, Johann(II)
  - (1734-1798) Waring
  - (1736-1813) Lagrange
  - (1741-1793) Wilson, John
  - (1744-1807) Bernoulli, Joh(III)
  - (1749-1827) Laplace
  - (1752-1833) Legendre
  - (1759-1789) Bernoulli, Jac(II)
  - 1765-1822) Ruffini
  - (1776-1831) Germain
  - (1777-1855) Gauss
  - (1790-1868) Möbius

- Siglo XIX
  - Abel (1802–1829)
  - Jacobi (1804–1851)
  - Dirichlet (1805–1859)
  - Hamilton, W R (1805-1865)
  - De Morgan (1806-1871)
  - Liouville (1809-1882)
  - Peirce, B (1809-1880)
  - Kummer (1810-1893)
  - Le Verrier (1811-1877)
  - Hesse (1811-1874)
  - Galois (1811-1832)

- Laurent, Pierre (1813-1854)
- Catalan (1814-1894)
- Sylvester (1814-1897)
- Boole (1815-1864)
- Weierstrass (1815-1897)
- Lovelace (1815-1852)
- Chebyshev (1821-1894)
- Cayley (1821-1895)
- Hermite (1822-1901)
- Eisenstein (1823-1852)
- Betti (1823-1892)
- Kronecker (1823-1891)
- Riemann (1826-1866)
- Dedekind (1831-1916)
- Lipschitz (1832-1903)
- Sylow (1832-1918)
- Laguerre (1834-1886)
- Venn (1834-1923)
- Jordan (1838-1922)
- Lucas (1842-1891)
- Frege (1848-1925)
- Gegenbauer (1849-1903)
- Frobenius (1849-1917)
- Poincaré (1854-1912)
- Stieltjes (1856-1894)
- Pell, Alexander (1857-1921)
- Peano (1858-1932)
- Hurwitz (1859-1919)
- Hilbert (1862-1943)
- Russell (1872-1970)

La lista correspondiente al siglo XX sería inmensa y la dejamos para que el lector curioso investigue por su cuenta.

Índice alfabético

Bibliografía

[1] Tom M. Apostol. *Introduction to Analityc Number Theory*, Undergraduate Texts in Mathematics, Springer, 1976.

[2] Leandro Cagliero, Daniel Penazzi, Juan Pablo Rosetti, Ana Sustar, Paulo Tirao. *Aventuras Matemáticas*, Colección: Las Ciencias Naturales y la Matemática, Ministerio de Educación, Argentina, 2010.

[3] Chen Chuan-Chong, Koh Khee-Meng. *Principles and Techniques in Combinatorics*, World Scientific, 1992.

[4] John H. Conway, Richard K. Guy. *The book of numbers*. Copernicus, New York, 1996.

[5] Enzo R. Gentile. *Notas de Algebra I*, Editorial Eudeba, 1988.

[6] Paul Halmos. *Naive set theory*, Undergraduate Texts in Mathematics, Springer, 1974.

[7] David L. Johnson. *Elements of Logic via Numbers and Sets*, Springer Undergraduate Mathematics Series, 1998.

[8] N. Patricia Kisbye, Roberto J. Miatello. *Notas de Algebra I - Matemática Discreta I*, Trabajos de Matemática, Serie C, FaMAF, UNC, 2004.

[9] Kenneth H. Rosen (editor-in-chief). *Handbook of discrete and combinatorial mathematics*, CRC Press, 2000.

[10] Alan Tucker. *Applied Combinatorics*, John Wiley & Sons, 2007.