LOS NÚMEROS
DE LOS NATURALES A LOS COMPLEJOS

Dr. Matías Graña
Dra. Gabriela Jeronimo
Dr. Ariel Pacetti
Dra. Alejandra P. Jancsa
Dr. Alejandro Petrovich

Colección: LAS CIENCIAS NATURALES Y LA MATEMÁTICA

Colección: LAS CIENCIAS NATURALES Y LA MATEMÁTICA

LOS NÚMEROS
DE LOS NATURALES A LOS COMPLEJOS

Dr. Matías Graña, Dra. Gabriela Jeronimo y Dr. Ariel Pacetti
Dra. Alejandra P. Jancsa y Dr. Alejandro Petrovich

autoridades

Presidente de la Nación
Dra. Cristina Fernández de Kirchner

Ministro de Educación
Dr. Alberto E. Sileoni

Secretaria de Educación
Prof. María Inés Abrile de Vollmer

Directora Ejecutiva del Instituto Nacional de Educación Tecnológica
Lic. María Rosa Almandoz

Director Nacional del Centro Nacional de Educación Tecnológica
Lic. Juan Manuel Kirschenbaum

Director Nacional de Educación Técnico Profesional y Ocupacional
Ing. Roberto Díaz

Ministerio de Educación.
Instituto Nacional de Educación Tecnológica.
Saavedra 789. C1229ACE.
Ciudad Autónoma de Buenos Aires.
República Argentina.
2010

LOS NÚMEROS
DE LOS NATURALES A LOS COMPLEJOS

Dr. Matías Graña
Dra. Gabriela Jeronimo
Dr. Ariel Pacetti
Dra. Alejandra P. Jancsa
Dr. Alejandro Petrovich

Colección: LAS CIENCIAS NATURALES Y LA MATEMÁTICA

Colección “Las Ciencias Naturales y la Matemática”.
Director de la Colección: Juan Manuel Kirschenbaum
Coordinadora general de la Colección: Haydeé Noceti.

Industria Argentina

ISBN 978-950-00-0748-1

Director de la Colección:
Lic. Juan Manuel Kirschenbaum
Coordinadora general y académica de la Colección:
Prof. Ing. Haydeé Noceti
Diseño didáctico y corrección de estilo:
Lic. María Inés Narvaja
Ing. Alejandra Santos
Coordinación y producción gráfica:
Tomás Ahumada
Diseño gráfico:
Martin Alejandro Gonzalez
Ilustraciones:
Diego Gonzalo Ferreyro
Federico Timerman
Retoques fotográficos:
Roberto Sobrado
Diseño de tapa:
Tomás Ahumada
Administración:
Cristina Caratozzolo
Néstor Hergenrether
Colaboración:
Téc. Op. en Psic. Soc. Cecilia L. Vazquez
Dra. Stella Maris Quiroga

Nuestro agradecimiento al personal del Centro Nacional de Educación Tecnológica por su colaboración.

Graña, Matías
Los números: de los naturales a los complejos / Matías Graña; Gabriela Jerónimo; Ariel Pacetti; dirigido por Juan Manuel Kirschenbaum.
- 1a ed. - Buenos Aires: Ministerio de Educación de la Nación. Instituto Nacional de Educación Tecnológica, 2009.
200 p.: il.; 24x19 cm. (Las ciencias naturales y la matemática / Juan Manuel Kirschenbaum.)

ISBN 978-950-00-0748-1

1. Enseñanza Secundaria.
I. Jerónimo, Gabriela
II. Pacetti, Ariel
III. Kirschenbaum, Juan Manuel, dir.
IV. Título

CDD 510.712

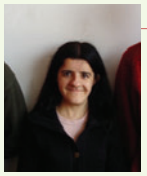
Fecha de catalogación: 16/12/2009

Impreso en Anselmo L. Morvillo S. A., Av. Francisco Pienovi 317 (B1868DRG), Avellaneda, Pcia. de Buenos Aires, Argentina.

Tirada de esta edición: 100.000 ejemplares

Los Autores

Matías Graña
Doctor en Matemática de la Universidad de Buenos Aires; es profesor del Departamento de Matemática de esa universidad e investigador del CONICET. Trabaja en Álgebra no conmutativa.



Gabriela Jeronimo
Doctora en Matemática de la Universidad de Buenos Aires; es profesora del Departamento de Matemática de esa universidad e investigadora del CONICET. Trabaja en Geometría Algebraica.

Ariel Pacetti
Doctor en Matemática de la Universidad de Texas en Austin; es profesor del Departamento de Matemática de la Universidad de Buenos Aires e investigador del CONICET. Trabaja en Teoría de Números.

Con la colaboración de:

Alejandra Patricia Jancsa
Doctora en Matemática de la Universidad Nacional de Córdoba; es investigadora y docente en la Facultad de Ciencias Exactas y Naturales de la UBA. Participa de proyectos de intercambio académico con Francia y España. Ha dictado numerosas conferencias sobre su área de investigación en reuniones científicas nacionales e internacionales. Paralelamente a la matemática, desarrolla actividades musicales como pianista y clavecinista.

Alejandro Petrovich
Doctor en Ciencias Matemáticas. Profesor adjunto del Departamento de Matemática de la Facultad de Ciencias Exactas y Naturales de la Universidad de Buenos Aires. El área principal de investigación es la Lógica Algebraica.

ÍNDICE

Prólogo

Este libro está pensado principalmente para estudiantes de la escuela secundaria y docentes. A lo largo del libro se ve el producto de siglos de avances en la matemática. Algunos de estos avances son pequeños, mientras que otros son importantes y revolucionarios. Es imposible entender el contenido del libro sin dedicarle tiempo. La comprensión en matemática es usualmente producto de la ejercitación y del trabajo, trabajo que se hace con la cabeza, con el lápiz y el papel.

Presentamos conjuntos de números, destinándole un capítulo a cada uno de ellos. El libro está organizado de la siguiente manera: primero, un capítulo donde se presentan algunas de las herramientas básicas que se utilizarán a medida que avanza el texto. A continuación, seis capítulos sobre los conjuntos de números naturales, enteros, enteros modulares, racionales, reales y complejos, respectivamente. Las construcciones se hacen formalmente, pero incluimos numerosos ejemplos, aplicaciones y ejercicios para facilitar la comprensión del material (las resoluciones están en el capítulo 7 y recomendamos al lector que no consulte la resolución de un ejercicio sin tratar de resolverlo previamente). El orden seguido no es el histórico, sino el que permite "avanzar sin sobresaltos". Usualmente, hay una concepción errónea sobre la matemática, que dice que los conceptos matemáticos son inmutables e independientes de acontecimientos culturales o históricos. Nada más lejos de la realidad. Los distintos conjuntos de números se fueron introduciendo en la medida en que hicieron falta para avanzar. Y muchas veces estos conceptos, forjados por alguien "adelantado a su época", o incorporados de otras culturas, necesitaron de varias generaciones de matemáticos para ser aceptados.

Por último, incluimos un apéndice con algunos de los algoritmos presentados en el libro, desarrollados en lenguaje Python, para mostrar la interacción de la matemática con la computación.

En cada capítulo, las proposiciones, teoremas, propiedades, corolarios y lemas están numerados de manera correlativa: tienen un primer número que indica el capítulo, y un segundo número correlativo que sirve para todos a la vez. Por ejemplo, en el capítulo 2, presentamos el teorema 2.1, luego el teorema 2.2, y luego la proposición 2.3 y la proposición 2.4. Los ejercicios tienen una numeración similar, también con dos números, donde el primero es el número del capítulo, mientras que el segundo indica el número de ejercicio dentro de ese capítulo.

Introducción

En el transcurso de la historia, los números surgieron naturalmente para contar (números cardinales: uno, dos, tres, etcétera) y, a la vez, para ordenar (números ordinales: primero, segundo, tercero, etcétera). Por este motivo, el primer conjunto de números que aparece es el de los números *naturales*. Es razonable comenzar cualquier estudio de los números con ellos, porque los números naturales están en la base de todos los otros conjuntos. Sin embargo, con el tiempo aparecieron nuevos usos para los números y, con los usos, nuevos números.

Los números naturales se pueden sumar y multiplicar. Y, a veces, se pueden restar. Sin embargo, no se puede restar a un número natural otro mayor, porque el resultado ya no es un número natural. Es así como, para poder restar, se necesitan el cero y los números negativos. A la humanidad le tomó siglos aceptar estos nuevos números, pese a que pasan a tener un sentido muy concreto cuando se los usa, por ejemplo, para expresar deudas. Hoy en día, los números negativos son de uso cotidiano. Los naturales dan lugar así a los *enteros.* Con los enteros se puede multiplicar, sumar y restar.

Con los enteros también se pueden hacer divisiones, siempre que se acepte que las divisiones pueden tener resto. Dado un número natural fijo n, si se divide un entero cualquiera por él, el resto será un número entero entre 0 y n-1. En el conjunto de todos los restos posibles se pueden hacer operaciones, dando lugar a los *enteros modulares.* Hoy en día, muchas de las propiedades de los números enteros se expresan, de manera muy satisfactoria, usando enteros modulares. Si bien estos conjuntos aparecieron definidos de manera clara hace poco tiempo (desde una perspectiva histórica), su uso permite entender más cabalmente a los números enteros, y por ello les dedicamos un capítulo.

Sin embargo, los números enteros no permiten divisiones si no se está dispuesto a tener resto. Si trabajamos en geometría, incluso si se adoptan unidades de medida tales que las cantidades a medir sean enteras, poco se podrá hacer si no se utilizan fracciones, es decir sin introducir los números *racionales.* Por ejemplo, el Teorema de Tales habla de longitudes proporcionales, que inmediatamente dan lugar a las fracciones.

Pero pronto se ve que si se quiere medir distancias, tampoco alcanza con números racionales. Por el Teorema de Pitágoras, la diagonal de un cuadrado cuyo lado mide 1 metro, mide $\sqrt{2}$ metros. Y este número, no es racional. Hacen falta entonces los números *reales.*

Y, a veces, tampoco alcanza con los enteros, los racionales o los reales. Por ejemplo, la ecuación $x^2 + 1 = 0$ no tiene solución en los números reales. Los números *complejos* se introdujeron, precisamente, para resolver este tipo de ecuaciones, aunque fueron mirados con mucha desconfianza durante tres siglos. Hizo falta que matemáticos de la talla de Leonhard Euler y Carl Friedrich Gauss los usaran para que la comunidad científica dejara de lado los prejuicios. Hoy en día, no sólo se usan para resolver este tipo de ecuaciones. Las ecuaciones de James Clerk Maxwell, por ejemplo, que explican los campos electromagnéticos, precisan de los números complejos.

Si bien las nociones de números naturales, enteros, racionales o reales eran saber popular en el siglo XVII, cuando Isaac Newton y Gottfried Leibniz introdujeron el cálculo infinitesimal, las fuertes críticas que recibió esta teoría, por el obispo George Berkeley en el siglo XVIII, entre otros, obligaron a sentar bases precisas para todos estos conjuntos numéricos. Ésta fue una empresa de grandes dimensiones: los reales se definieron a partir de los racionales, y estos a partir de los enteros, que a su vez salen de los naturales. ¿Y los naturales? La noción de número natural es tan . . . ¡natural! . . . que es sumamente difícil definirlos de manera formal y sin utilizar otros conjuntos anteriores. Fue finalmente Giuseppe Peano quien en 1889 los introdujo axiomáticamente en su libro *Arithmetices principia, nova methodo exposita.*

Una vez definidos los naturales, la definición de los enteros y los racionales es sencilla. Los reales, en cambio, son materia mucho más delicada. Hay distintas definiciones posibles de los números reales, con distintos grados de formalidad. Desde "los puntos de una recta" hasta las *cortaduras de Dedekind* (propuestas por Julius Dedekind a comienzos del siglo XX), pasando por definiciones axiomáticas, o más implícitas como "números con desarrollos decimales infinitos". Los introducimos como clases de equivalencias de sucesiones crecientes y acotadas de números racionales. Esta forma de hacerlo, aunque es técnica y requiere una gran capacidad de abstracción, permite definir las operaciones fácilmente. Para "suavizar" su introducción, primero se los presenta de manera algo más informal, utilizando la noción de límite. También se mencionan otras definiciones posibles, entre ellas la de los desarrollos decimales infinitos.

Si se cuenta con los reales, los números complejos se pueden presentar algebraicamente, como sumas $a + bi$, donde a y b son números reales e i es una solución de la ecuación $x^2 + 1 = 0$. Ésta es la forma en que los presentó William Rowan Hamilton en la primera mitad del siglo XIX, trescientos años después de que Gerolamo Cardano y Lodovico Ferrari los utilizaran por primera vez. Y ésta es la forma en que los conocemos hoy.

Los conjuntos de números que se usan hoy en día no se reducen a los que presentamos aquí: naturales, enteros, enteros modulares, racionales, reales y complejos. Dependiendo del problema que se intente resolver, se utilizan muchos otros. Como ejemplo, basta mencionar a los *cuaterniones* (introducidos por Hamilton en 1843, que se utilizan para describir de manera algebraica movimientos del espacio, como rotaciones, traslaciones u homotecias) y a los *surreales* (introducidos por John Conway y Donald Knuth en 1974, que se utilizan en teoría de juegos). No obstante, estos conjuntos se usan en medida mucho menor, y los que presentamos bastan para la gran mayoría de las aplicaciones.

0. Conjuntos y relaciones

En este capítulo presentamos las nociones elementales que utilizaremos a lo largo del libro.

□ 1. Conjuntos

La noción básica con la que vamos a trabajar es la de *conjunto*. A nuestros fines, un *conjunto* es una colección de objetos sin orden ni repeticiones. Por ejemplo:

- $\mathcal{A}_1 = \{1, 2, 3\}$.
- $\mathcal{A}_2 = \{\pi, e\}$.
- $\mathcal{A}_3 = \{\diamondsuit, \heartsuit, \spadesuit, \clubsuit\}$.
- $\mathcal{A}_4 = \{1, \heartsuit, \pi\}$.

También hay conjuntos infinitos, como el conjunto de los *números naturales*, con el que trabajaremos en el capítulo 1. Este conjunto se suele llamar $\mathbb{N}$, y es el conjunto $\{1, 2, 3, 4, 5, \ldots\}$.

Al conjunto que no tiene ningún elemento lo llamamos *conjunto vacío* y lo representamos con el símbolo $\emptyset$.

Una propiedad importante que tienen los conjuntos es que dado un elemento cualquiera se puede saber si está en el conjunto o no. Si a está en el conjunto $\mathcal{A}$ decimos que a *pertenece* a $\mathcal{A}$ y escribimos $a \in \mathcal{A}$. En caso contrario decimos que a *no pertenece* a $\mathcal{A}$ y escribimos $a \notin \mathcal{A}$. Por ejemplo, $2 \in \mathcal{A}_1$ pero $2 \notin \mathcal{A}_2$; $17 \in \mathbb{N}$ y $\heartsuit \notin \emptyset$.

Si $\mathcal{A}$ y $\mathcal{B}$ son dos conjuntos, decimos que $\mathcal{A}$ está *incluido* en $\mathcal{B}$, y escribimos $\mathcal{A} \subset \mathcal{B}$, si todos los elementos del conjunto $\mathcal{A}$ pertenecen al conjunto $\mathcal{B}$. Por ejemplo, $\mathcal{A}_1 \subset \mathbb{N}$, pero $\mathcal{A}_2 \not\subset \mathcal{A}_4$ porque $e \notin \mathcal{A}_4$.

En los ejemplos anteriores, los conjuntos fueron definidos listando sus elementos. Esta manera de dar un conjunto se llama *definición por extensión*. Hay otra forma de hacerlo: por *comprensión*, que consiste en dar una propiedad que satisfacen sus elementos y sólo ellos. Por ejemplo: el conjunto $\{1, 2\}$ se puede también definir por $\{x \in \mathcal{A}_1 : x < 3\}$, que se lee "los x que pertenecen a $\mathcal{A}_1$ tales que $x < 3$", y define el conjunto de todos los elementos de $\mathcal{A}_1$ que son menores que 3; es decir, $\{1, 2\}$. Por supuesto, este conjunto se podría haber definido de otras maneras, como $\{x \in \mathcal{A}_1 : x \neq 3\}$, $\{x \in \mathbb{N} : x^2+2 = 3x\}$, etc. El conjunto $\{y \in \mathcal{A}_3 : y \text{ es negro}\}$ es el conjunto $\{\spadesuit, \clubsuit\}$.

Operaciones entre conjuntos. Los profesores de gimnasia de la Escuela 314 quieren armar, para una competencia, un equipo de fútbol de jugadores entre 14 y 16 años, y uno de básquet de jugadores entre 15 y 17. Para armar los equipos, la dirección del colegio les entregó una lista con los alumnos entre 14 y 16 años, y otra con los alumnos entre 15 y 17.

Para citar a los alumnos a que se prueben, los profesores quieren armar cuatro listas, formadas por los alumnos que pueden: (1) integrar ambos equipos, (2) integrar alguno de los equipos, (3) integrar sólo el equipo de fútbol, (4) integrar sólo el equipo de básquet.

Para resolver problemas como éste, se utilizan ciertas operaciones entre conjuntos.

Dados dos conjuntos A y B, se definen:

- la *unión* de A y B, que es el conjunto formado por los elementos que pertenecen a uno de ellos o a ambos, y se escribe $A \cup B$;
- la *intersección* de A y B, que es el conjunto formado por los elementos que pertenecen simultáneamente a A y a B, y se escribe $A \cap B$;
- la *diferencia* entre A y B, que es el conjunto formado por los elementos que pertenecen a A pero no a B, y se escribe $A \setminus B$ o $A - B$.

Dos conjuntos se dicen *disjuntos* si su intersección es el conjunto vacío. Se dice que un conjunto A es la *unión disjunta* de dos conjuntos B y C si es la unión de ellos ($A = B \cup C$) y además B y C son disjuntos. Un conjunto es la unión disjunta de varios si es la unión de ellos y los conjuntos son disjuntos dos a dos. Por ejemplo: {1,2,3,4,5,6} es la unión disjunta de {1,4}, {2,3,6} y {5}, pero no es la unión disjunta de {1,4}, {1,2,3,6} y {3,5}, pues por ejemplo {1,4} ∩ {1,2,3,6} = {1} y por lo tanto no son disjuntos.

Ejercicio 1. Siguiendo con el ejemplo anterior, si llamamos $\mathcal{A}$ al conjunto de alumnos entre 14 y 16 años y $\mathcal{B}$ al conjunto de alumnos entre 15 y 17, describir las listas (1), (2), (3) y (4) en términos de operaciones entre $\mathcal{A}$ y $\mathcal{B}$.

Producto cartesiano. Lorena irá al cine con un amigo. Quiere elegir qué ropa ponerse entre tres pantalones (un jean azul, un jean gris y un pantalón blanco), cuatro remeras (dos musculosas, una blanca y una negra, y dos remeras de manga corta, una rosa y la otra celeste) y dos pares de calzado (unas sandalias y unos zapatos). Para esto, invita a sus amigas y les muestra cómo le quedan todas las combinaciones posibles. La noción que necesitamos introducir en este caso es la de producto cartesiano.

Si A y B son conjuntos, definimos el *producto cartesiano* de A y B como el conjunto formado por los pares ordenados (a, b) donde a pertenece a A y b pertenece a B. Escribimos este conjunto como $A \times B$.

Por ejemplo:

$\mathcal{A}_1 \times \mathcal{A}_2 = \{(1, \pi), (1, e), (2, \pi), (2, e), (3, \pi), (3, e)\}$.
$\mathcal{A}_2 \times \mathcal{A}_2 = \{(\pi, \pi), (\pi, e), (e, \pi), (e, e)\}$.
{♢, ♡, ♠, ♣} × {A, 2, 3, 4, 5, 6, 7, 8, 9, 10, J,Q,K} representa la baraja francesa.

De manera similar se define el producto cartesiano de varios conjuntos. Por ejemplo, $\{a, b, c\} \times \{1, 2\} \times \{\alpha, \beta\} = \{(a, 1, \alpha), (b, 1, \alpha), (c, 1, \alpha), (a, 2, \alpha), (b, 2, \alpha), (c, 2, \alpha), (a, 1, \beta), (b, 1, \beta), (c, 1, \beta), (a, 2, \beta), (b, 2, \beta), (c, 2, \beta)\}$.

Si definimos los conjuntos $H = \{0, 1, 2, \ldots, 22, 23\}$, $M = \{0, 1, 2, \ldots, 58, 59\}$ y $S = M$, la hora del día se puede representar por un elemento del conjunto $H \times M \times S$.

Ejercicio 2. Escribir el conjunto de combinaciones de ropa para Lorena como producto cartesiano de conjuntos y dar este conjunto por extensión.

2. Relaciones

Los profesores de gimnasia de la Escuela 314 van a probar a los alumnos para el equipo de fútbol. Los alumnos se pueden anotar para probarse como arquero, defensor, mediocampista o delantero (se pueden anotar en más de un puesto). Los profesores comenzaron a usar la palabra *versátil* para referirse a los alumnos: dicen que un alumno es más versátil que otro si el primero se anotó en todos los puestos en los que se anotó el segundo y por lo menos uno más. Por ejemplo, si Pablo se anotó como arquero y delantero, y Andrés se anotó como arquero, mediocampista y delantero, Andrés es más versátil que Pablo. La manera de formalizar esta situación, en matemática, es utilizando el concepto de *relación en un conjunto*.

Si A y B son conjuntos, una *relación* de A en B es un subconjunto del conjunto $A \times B$.

Si $\mathcal{R}$ es una relación de $\mathcal{A}$ en $\mathcal{B}$, dados $a \in \mathcal{A}$ y $b \in \mathcal{B}$ decimos que *a está relacionado con b* y escribimos $a\mathcal{R}b$ si el par $(a, b) \in \mathcal{R}$. Si el par $(a, b) \notin \mathcal{R}$ decimos que *a no está relacionado con b* y escribimos $a \not\mathcal{R} b$. Por ejemplo, $\mathcal{R} = \{(1, \pi), (1, e), (2, e)\} \subset \mathcal{A}_1 \times \mathcal{A}_2$ es una relación de $\mathcal{A}_1$ en $\mathcal{A}_2$. En este caso, 1 está relacionado con π y con e, pero 3 no está relacionado con ningún elemento de $\mathcal{A}_2$.

Relaciones en un conjunto. Si $\mathcal{R} \subset \mathcal{A} \times \mathcal{A}$ decimos que $\mathcal{R}$ es una relación en $\mathcal{A}$. Por ejemplo, $\mathcal{R} = \{(1, 2), (1, 3), (2, 3)\}$ es una relación en $\mathcal{A}_1$. Observemos que esta relación puede definirse también como $\mathcal{R} = \{(a_1, a_2) \in \mathcal{A}_1 \times \mathcal{A}_1 : a_1 < a_2\}$.
Dado un conjunto $\mathcal{A}$ y una relación $\mathcal{R}$ en $\mathcal{A}$ decimos que:

- $\mathcal{R}$ es *reflexiva* si el par $(a, a) \in \mathcal{R}$ para todo $a \in \mathcal{A}$.
- $\mathcal{R}$ es *simétrica* si para todo par $(a, b) \in \mathcal{R}$ vale que el par $(b, a) \in \mathcal{R}$.
- $\mathcal{R}$ es *transitiva* si para todos los pares $(a, b) \in \mathcal{R}$, $(b, c) \in \mathcal{R}$ vale que $(a, c) \in \mathcal{R}$.
- $\mathcal{R}$ es *antisimétrica* si para todo par de elementos $(a, b) \in \mathcal{A}$ con $a \neq b$, si $(a, b) \in \mathcal{R}$ entonces $(b, a) \notin \mathcal{R}$.

Por ejemplo:

1. $\mathcal{R} = \{(\diamondsuit,\diamondsuit), (\diamondsuit,\heartsuit), (\heartsuit,\diamondsuit), (\heartsuit,\spadesuit), (\spadesuit,\heartsuit), (\heartsuit,\clubsuit), (\clubsuit,\heartsuit), (\spadesuit,\clubsuit), (\clubsuit,\spadesuit)\}$ en $\mathcal{A}_3$. Aunque $\diamondsuit \mathcal{R} \diamondsuit$, $\mathcal{R}$ no es reflexiva porque por ejemplo $\heartsuit \not\mathcal{R} \heartsuit$. Esta relación es simétrica porque para cada par de elementos que pertenece a $\mathcal{R}$, el par con los elementos en orden inverso también pertenece a $\mathcal{R}$ (convencerse). Esta relación no es transitiva porque $\diamondsuit \mathcal{R} \heartsuit$, $\heartsuit \mathcal{R} \spadesuit$ pero $\diamondsuit \not\mathcal{R} \spadesuit$.

Observemos que para afirmar que una relación es transitiva es necesario considerar todas las posibilidades (en este ejemplo, si bien $\heartsuit \mathcal{R} \spadesuit$, $\spadesuit \mathcal{R} \clubsuit$ y $\heartsuit \mathcal{R} \clubsuit$, la relación no es transitiva). Esta relación no es antisimétrica porque $(\diamondsuit, \heartsuit) \in \mathcal{R}$ y $(\heartsuit, \diamondsuit) \in \mathcal{R}$.

2. La relación "ser más versátil que", ideada por los profesores de gimnasia de la Escuela 314, no es reflexiva ni simétrica, pero sí es transitiva y antisimétrica.

3. $\mathcal{R} = \{(\heartsuit,\heartsuit), (\heartsuit,\diamondsuit), (\diamondsuit,\heartsuit), (\diamondsuit,\diamondsuit), (\spadesuit,\spadesuit), (\spadesuit,\clubsuit), (\clubsuit,\spadesuit), (\clubsuit,\clubsuit)\}$ en $\mathcal{A}_3$. Esta relación es reflexiva, simétrica y transitiva pero no es antisimétrica. Observemos que $\mathcal{R}$ se puede definir por comprensión diciendo que dos elementos de $\mathcal{A}_3$ están relacionados si son del mismo color. Usando esta definición alternativa es más fácil verificar que valen las propiedades.

4. $\mathcal{R} = \{(1, 1), (1, 2), (1, 3), (2, 2), (2, 3), (3, 3)\}$ en $\mathcal{A}_1$ es reflexiva, antisimétrica y transitiva.

Las relaciones que son reflexivas, simétricas y transitivas son importantes y tienen un nombre especial: se llaman relaciones de *equivalencia*. Otro tipo de relaciones importante es el de las relaciones de *orden*, que son las reflexivas, antisimétricas y transitivas.

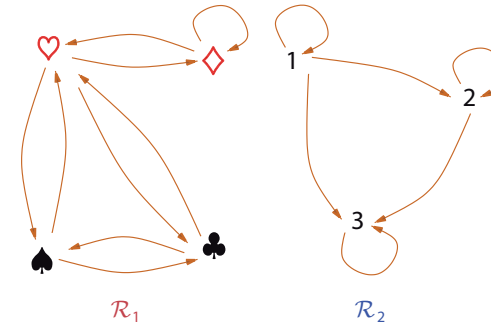


Figura 1. *Gráficos de relaciones.*

Ejemplos

1. Los profesores de gimnasia dicen que un alumno es "tan versátil como" otro si ambos se anotaron para probarse en los mismos puestos. Ésta es una relación de equivalencia.
2. Dos números naturales están relacionados si tienen la misma paridad (es decir, si son ambos pares o ambos impares). Esta es otra relación de equivalencia.
3. La relación $\mathcal{R}$ del ejemplo 4 de la lista anterior es una relación de orden.
4. La relación $a \leq b$ en los números naturales es una relación de orden.

Representación gráfica. A veces resulta cómodo representar una relación $\mathcal{R}$ en un conjunto $\mathcal{A}$ de manera gráfica. Para esto se ubican los elementos del conjunto $\mathcal{A}$ y se dibuja una flecha que sale de un elemento $a \in \mathcal{A}$ y llega a otro elemento $b \in \mathcal{A}$ para cada par de elementos tales que $a\mathcal{R}b$ (si $a\mathcal{R}a$ queda un "rulito" que sale de a y termina en a).

Por ejemplo, las relaciones
$\mathcal{R}_1 = \{(\diamondsuit,\diamondsuit), (\diamondsuit,\heartsuit), (\heartsuit,\diamondsuit), (\heartsuit,\spadesuit), (\spadesuit,\heartsuit), (\heartsuit,\clubsuit), (\clubsuit,\heartsuit), (\spadesuit,\clubsuit), (\clubsuit,\spadesuit)\}$ en $\mathcal{A}_3$ y
$\mathcal{R}_2 = \{(1, 1), (1, 2), (1, 3), (2, 2), (2, 3), (3, 3)\}$ en $\mathcal{A}_1$ pueden representarse por los gráficos de la Figura 1.

3. Particiones

En un ejemplo anterior, consideramos la relación $\mathcal{R}$ en el conjunto $\mathbb{N}$ definida por $a\mathcal{R}b$ si a y b tienen la misma paridad. Esta relación define dos clases de números naturales: los números pares y los números impares. A los números pares los podemos caracterizar por la propiedad de estar relacionados con el número 2, mientras que a los impares los podemos caracterizar por la propiedad de estar relacionados con el número 1. Así tenemos:

$$\mathbb{N} = \{n \in \mathbb{N} : n\mathcal{R}1\} \cup \{n \in \mathbb{N} : n\mathcal{R}2\}$$

También podemos definir los números pares como los números naturales relacionados con el número 4 o, más generalmente, con cualquier número natural par 2, 4, 6, ... Lo importante es que la relación de equivalencia partió al conjunto de números naturales como unión disjunta de dos subconjuntos. Además, todos los elementos de cada subconjunto están relacionados entre sí.

Veamos otro ejemplo de cómo una relación de equivalencia nos da una partición de un conjunto. Los docentes de la Escuela 314 deciden programar ciertas actividades extracurriculares. Para poder asignar a sus alumnos a cada una de estas actividades precisan saber cuán ocupado está cada alumno. Para ello, les entregan un formulario a los alumnos donde deben decir cuántas actividades extras ya realizan por cuenta propia (por actividad extra consideran deportes, idiomas, música y cualquier otra actividad que demande al menos 2 horas semanales). Definen en el conjunto de alumnos una relación diciendo que el alumno A está relacionado con el alumno B si ambos realizan el mismo número de actividades.
Verificar que ésta es una relación de equivalencia.

Se consideran los subconjuntos A_n = {alumnos que realizan n actividades}, para n = 0, 1, 2, ..., 12 (ninguno de los alumnos realiza más de 12 actividades). Es claro que estos conjuntos son disjuntos dos a dos (cada alumno desarrolla un único número de actividades y éste determina en qué conjunto está) y la unión de ellos da todo el conjunto de alumnos. Luego, el conjunto de alumnos se parte como una unión disjunta de los subconjuntos A_n.

Si $\mathcal{A}$ es un conjunto y $\mathcal{R}$ una relación de equivalencia en el conjunto $\mathcal{A}$, para cada elemento $a \in \mathcal{A}$ definimos su clase de equivalencia como $[a] = \{b \in \mathcal{A} : a\mathcal{R}b\}$.

Éste es un subconjunto del conjunto $\mathcal{A}$.

Por ejemplo, si $\mathcal{A} = \mathbb{N}$ y la relación es tener la misma paridad, [1] es el conjunto de los números naturales impares, es decir, [1] = {1, 3, 5, ...}. Las clases de equivalencia [3], [5], [7], etcétera, también son el conjunto de los números naturales impares. Por otro lado, [2] es el conjunto de los números naturales pares, y lo mismo ocurre con [4], [6], [8], etcétera. Así, $\mathbb{N}$ queda partido en dos clases de equivalencia con esta relación: [1] y [2].

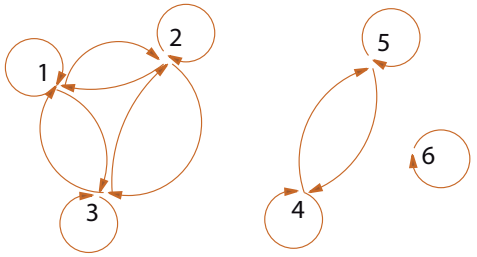


Figura 2. *Relación $\mathcal{R}$ en $\mathcal{A}$.*

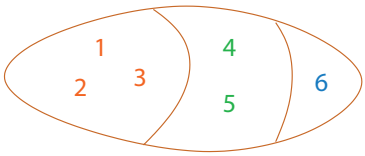


Figura 3. *Partición de {1, 2, 3, 4, 5, 6}.*

Veamos el siguiente ejemplo: consideremos en el conjunto $\mathcal{A} = \{1, 2, 3, 4, 5, 6\}$ la relación de equivalencia $\mathcal{R} = \{(1, 1), (2, 2), (3, 3), (4, 4), (5, 5), (6, 6), (1, 2), (2, 1), (1, 3), (3, 1), (2, 3), (3, 2), (4, 5), (5, 4)\}$. En la figura 2 se da la relación gráficamente.

Las clases de equivalencia para esta relación son:

$$[1] = [2] = [3] = \{1, 2, 3\}$$
$$[4] = [5] = \{4, 5\}$$
$$[6] = \{6\}$$

Así, el conjunto $\mathcal{A}$ se parte en los subconjuntos:

$$\mathcal{A} = \{1, 2, 3\} \cup \{4, 5\} \cup \{6\}.$$

donde para cada elemento de $\mathcal{A}$ consideramos todos los que están relacionados con él (ver figura 3).

En general, si $\mathcal{R}$ es una relación de equivalencia en el conjunto $\mathcal{A}$, si a y b son elementos de $\mathcal{A}$, sus clases de equivalencia son o bien iguales, o bien disjuntas. Es decir que: $[a] = [b]$ o $[a] \cap [b] = \emptyset$. El conjunto $\mathcal{A}$ se parte en las clases de equivalencia dadas por la relación $\mathcal{R}$.

□ 4. Funciones

Los profesores de gimnasia de la Escuela 314 definieron un equipo de fútbol titular. A los convocados les dieron las camisetas del 1 al 11. En términos matemáticos, a cada elemento del conjunto {1, 2, 3, ... , 10, 11} le asignaron un elemento del conjunto de alumnos.

Si $\mathcal{A}$ y $\mathcal{B}$ son dos conjuntos, una *función* de $\mathcal{A}$ en $\mathcal{B}$ es una relación $f \subset \mathcal{A} \times \mathcal{B}$ que satisface que para cada $a \in \mathcal{A}$ hay un único $b \in \mathcal{B}$, tal que $(a, b) \in f$. En este caso, usualmente se escribe $f(a) = b$. Si $f \subset \mathcal{A} \times \mathcal{B}$ es una función, también se escribe $f: \mathcal{A} \to \mathcal{B}$.

Ejemplos. Como antes, $\mathcal{A}_1 = \{1, 2, 3\}$ y $\mathcal{A}_2 = \{\pi, e\}$.

1. La relación $f = \{(1, \pi), (2, e), (3, e)\}$ es una función de $\mathcal{A}_1$ en $\mathcal{A}_2$. En este caso, $f(1) = \pi$, $f(2) = e$ y $f(3) = e$.
2. La relación $\{(1, \pi), (1, e), (2, e), (3, \pi)\} \subset \mathcal{A}_1 \times \mathcal{A}_2$ no es una función, porque $1 \in \mathcal{A}_1$ está relacionado con dos elementos de $\mathcal{A}_2$.
3. La relación $\{(1, \pi), (2, e)\} \subset \mathcal{A}_1 \times \mathcal{A}_2$ no es una función, porque $3 \in \mathcal{A}_1$ no está relacionado con ningún elemento de $\mathcal{A}_2$.
4. La asignación de las camisetas de fútbol a los alumnos de la Escuela 314 es una función.

En general, una función no se describe listando todos sus pares, sino dando una regla que permite obtener $f(a)$ en términos de a.

Ejemplos

1. La función $f: \mathcal{A}_1 \to \mathcal{A}_1$, $f = \{(1, 3), (2, 2), (3, 1)\}$ se puede describir por $f(a) = 4 - a$.
2. La función $g: \mathbb{N} \to \mathbb{N}$, $g(a) = 3a + 1$, está formada por los pares (1, 4), (2, 7), (3, 10), (4, 13), ...

□ 5. Operaciones

El equipo de fútbol de la Escuela 314 participa de un campeonato intercolegial. Una vez que todos los equipos jugaron dos partidos, los organizadores del torneo quieren armar las estadísticas. Para calcular la cantidad de goles a favor de cada equipo, deben sumar la cantidad de goles convertidos por el equipo en el primer partido con la de goles convertidos en el segundo. En este caso, la noción matemática involucrada es la de *operación*.

Una *operación en un conjunto* $\mathcal{A}$ es una función de $\mathcal{A} \times \mathcal{A} \to \mathcal{A}$. Si $*: \mathcal{A} \times \mathcal{A} \to \mathcal{A}$ es una operación, usualmente se escribe $a * b$ para el valor de $*$ en el par (a, b).

Ejemplos

1. La suma de números naturales es una operación. De hecho, cuando uno escribe por ejemplo 3 + 5 = 8, está diciendo que la función + le asigna el 8 al par (3, 5).
2. El producto de números naturales es otra operación.
3. La *potencia de números naturales*, que al par (a, b) le asigna a^b, es otra operación.

A veces es cómodo dar una operación mediante una tabla de doble entrada. A la izquierda se pone el primer elemento de cada par y arriba, el segundo. Por ejemplo, si $\mathcal{C} = \{0, 1, 2, 3, 4\}$, podemos definir las operaciones $\circ : \mathcal{C} \times \mathcal{C} \to \mathcal{C}$ y $- : \mathcal{C} \times \mathcal{C} \to \mathcal{C}$ por

$\circ$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

$-$	0	1	2	3	4
0	0	4	3	2	1
1	1	0	4	3	2
2	2	1	0	4	3
3	3	2	1	0	4
4	4	3	2	1	0

Esto quiere decir, por ejemplo, que $0 \circ 1 = 0$, que $2 \circ 3 = 1$, que $2 - 1 = 1$ y que $1 - 2 = 4$.

Si $* : \mathcal{A} \times \mathcal{A} \to \mathcal{A}$ es una operación, decimos que:

1. $*$ es *asociativa* si $a * (b * c) = (a * b) * c$ para todos los a, b, c en $\mathcal{A}$;
2. $*$ es *conmutativa* si $a * b = b * a$ para todos los a, b en $\mathcal{A}$;
3. un elemento $e \in \mathcal{A}$ es *un elemento neutro de* $*$ si $a * e = a$ y $e * a = a$ para todo a en $\mathcal{A}$.

La suma y el producto de números naturales son operaciones conmutativas y asociativas. El producto tiene un elemento neutro, que es el número uno. La suma, en cambio, no lo tiene, si se considera que el cero no pertenece al conjunto de los naturales. En cambio si agregamos el cero a los números naturales, éste resulta ser el elemento neutro de la suma.

La potencia de números naturales no es conmutativa porque, por ejemplo: $2^3 \neq 3^2$.

$$2^{(3^2)} \neq (2^3)^2$$

Tampoco es asociativa porque, por ejemplo:

Ejercicio 3. Explicitar el conjunto $\mathcal{A}$ y la operación utilizada para el cálculo de goles a favor planteado al comienzo de esta sección,

Ejercicio 4. Determinar si la operación $\circ$ en $\mathcal{C}$ definida en la tabla anterior es conmutativa, asociativa o tiene elemento neutro. Hacer lo mismo para $-$.

Cuando una operación $* : \mathcal{A} \times \mathcal{A} \to \mathcal{A}$ tiene un elemento neutro e, decimos que un elemento $a \in \mathcal{A}$ es un *inverso* de $b \in \mathcal{A}$ si $a * b = e$ y $b * a = e$. Por ejemplo, 1 es el elemento neutro de la operación $\circ$ en $\mathcal{C}$, y el inverso de 2 es 3 para esta operación. En este caso, 0 no tiene inverso.

□ 6. Sucesiones

Todos los días, Lorena y sus amigas Magalí y Natalia se reúnen en la casa de una de ellas: un día en lo de Lorena, al día siguiente en lo de Magalí, el tercero en lo de Natalia, y al cuarto día vuelven a empezar reuniéndose en lo de Lorena. Lorena quiere saber en qué casa se van a reunir el día del amigo (el 20 de julio), sabiendo que el día 1 de julio se

1 Lorena	6 Natalia	11 Magalí	16 Lorena
2 Magalí	7 Lorena	12 Natalia	17 Magalí
3 Natalia	8 Magalí	13 Lorena	18 Natalia
4 Lorena	9 Natalia	14 Magalí	19 Lorena
5 Magalí	10 Lorena	15 Natalia	20 Magalí

reunieron en su casa. Para esto, Lorena escribe:
Es decir, el día del amigo se reunirán en la casa de Magalí. Matemáticamente, lo que hizo Lorena es asignarle a cada número natural un elemento del conjunto {Lorena, Magalí, Natalia} (en realidad lo hace sólo para los primeros 20 números naturales, aunque podría extender la definición a todos ellos).

Si X es un conjunto, una *sucesión de elementos* de X es una función $f : \mathbb{N} \to X$.

En el ejemplo anterior X es el conjunto de Lorena y sus amigas. En el resto del libro las sucesiones con las que trabajaremos serán principalmente *sucesiones de números*, es decir,

el conjunto X será un conjunto de números.

Si $f: \mathbb{N} \to X$ es una sucesión y $n \in \mathbb{N}$, escribiremos a_n en lugar de $f(n)$. El elemento a_n se denomina el *enésimo término de la sucesión*. A partir de ahora, escribiremos $(a_n)_{n\geq 1}$ en lugar de f. Por lo tanto, los valores $f(1), f(2), \ldots, f(n), \ldots$ que toma la sucesión f serán expresados como $a_1, a_2, \ldots, a_n, \ldots$

Ejemplos

1. $a_n = n$.
2. $a_n = 1/n$.
3. $a_n = 2^n$.
4. $a_n = n^2$.
5. $a_n = (-1)^n$.

Es importante notar que en una sucesión dada los términos se pueden repetir. Esto sucede, por ejemplo, en la sucesión de Lorena. Las sucesiones de los ejemplos tienen la peculiaridad de que existe una *fórmula cerrada*; es decir, hay una *ley* o *fórmula q*ue dice cómo calcular a_n solamente en función de n.

Ejercicio 5. Encontrar una fórmula cerrada para la sucesión cuyos términos son 1, 2, 1, 2, 1, 2, 1, 2, . . .

1. Números naturales

□ 1. Nociones básicas

Los números naturales son, tal como los conocemos, 1, 2, 3, 4, 5, . . . Si bien todos tenemos esta idea intuitiva, más adelante, en la sección 4, daremos una definición precisa.

Llamamos $\mathbb{N}$ al conjunto de los números naturales, es decir:

$$\mathbb{N} = \{1, 2, 3, 4, 5, \ldots\}$$

Estos números se usan a diario para contar. Matemáticamente, contar significa decir cuántos elementos tiene un conjunto. Por ejemplo, el conjunto {♢, ♡, ♠, ♣} tiene 4 elementos. ¿Cuántos elementos tiene el conjunto vacío?

Como el conjunto vacío no posee ningún elemento, necesitamos un símbolo nuevo que represente la cantidad de elementos de este conjunto. Este símbolo es el 0. Llamamos $\mathbb{N}_0$ al conjunto de los números naturales con el cero, o sea:

$$\begin{aligned} \mathbb{N}_0 &= \mathbb{N} \cup \{0\} \\ &= \{0, 1, 2, 3, 4, 5, \ldots\}. \end{aligned}$$

El conjunto de los números naturales tiene dos operaciones importantes: *suma y producto*. Como mencionamos en el capítulo anterior, la suma y el producto de números naturales son operaciones asociativas y conmutativas. El 1 es el neutro para el producto, y la suma no tiene elemento neutro en $\mathbb{N}$, pero sí en $\mathbb{N}_0$: el 0.

Además, estas dos operaciones están relacionadas por la siguiente propiedad: para toda terna de números naturales *a, b, c,* vale que:

$$\begin{aligned} a \cdot (b + c) &= a \cdot b + a \cdot c \\ (a + b) \cdot c &= a \cdot c + b \cdot c \end{aligned}$$

Esta propiedad se llama *distributiva* del producto sobre la suma.

Veamos cómo se pueden usar estas propiedades para calcular el cuadrado de la suma de dos números naturales:

$$\begin{aligned} (a + b)^2 &= (a + b) \cdot (a + b) \\ &= (a + b) \cdot a + (a + b) \cdot b \\ &= a \cdot a + b \cdot a + a \cdot b + b \cdot b \\ &= a^2 + a \cdot b + a \cdot b + b^2 \\ &= a^2 + 2 \cdot a \cdot b + b^2 \end{aligned}$$

Esto también puede verse geométricamente como muestra el dibujo de la figura 1.

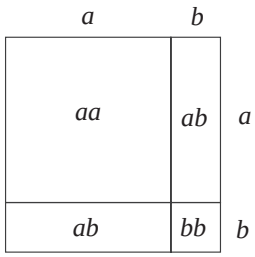


Figura 1. *El cuadrado de una suma.*

Ejercicio 1.1. Encontrar una fórmula para $(a + b)^3$.

□ 2. Inducción

Lorena y sus amigas se saludan en la puerta de la escuela con un beso. Un día, Lorena llega primera y quiere contar cuántos besos se dan en total todas las amigas (ella incluida). Cuando llega su primera amiga, Lorena la saluda y cuenta un beso. Cuando llega la segunda amiga, saluda a ambas, y Lorena cuenta dos besos más; en total, 3 besos. Cuando llega la tercera amiga, saluda a las tres y Lorena cuenta 3 besos más. En total, 6 besos. A medida que van llegando, Lorena descubre que si llegaron n amigas, la cantidad de besos es $1 + 2 + 3 + \ldots + n$. Esto nos lleva al siguiente problema: ¿cuánto da la suma de los primeros n números naturales?

A partir de la figura 2 podemos ver que:

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}$$

Más adelante, daremos una demostración distinta de esta igualdad, que nos servirá para ilustrar el principio de inducción.

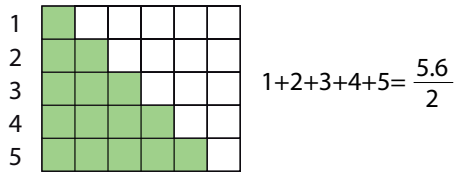


Figura 2. *La suma de los primeros números naturales.*

Consideremos ahora el siguiente problema: ¿cuánto es $1 + 2 + 2^2 + \ldots + 2^n$? Calculemos los primeros valores:

$$\begin{aligned} 1 &= 1 && n=0 \\ 1+2 &= 3 && n=1 \\ 1+2+4 &= 7 && n=2 \\ 1+2+4+8 &= 15 && n=3 \\ 1+2+4+8+16 &= 31 && n=4 \end{aligned}$$

Aunque a simple vista estos números no parecen conocidos, ¿qué pasa si a los resultados obtenidos les sumamos 1? Obtenemos que las primeras sumas, más 1, dan 2, 4, 8, 16, 32, que son potencias de 2. Parece ser que la suma $1+2+\ldots+2^n = 2^{n+1}-1$. ¿Cómo podemos convencernos de que esta fórmula vale?

Veamos qué pasa para $n = 5$:

$$\begin{aligned} \underbrace{1+2+4+8+16}_{2^5-1}+32 &= 2\cdot 2^5 - 1 \\ &= 2^6 - 1 \end{aligned}$$

Podemos repetir este razonamiento para $n = 6$, $n = 7$, ... O sea, si sabemos que vale:

$$1 + 2 + \cdots + 2^n = 2^{n+1} - 1,$$

entonces:

$$\underbrace{1 + 2 + \cdots + 2^n}_{2^{n+1}-1} + 2^{n+1} = 2 \cdot 2^{n+1} - 1$$
$$= 2^{n+2} - 1 \qquad (1)$$

Vemos así que si la fórmula es válida para un número natural n, también lo es para el siguiente número natural $n + 1$. ¿Alcanza esto para concluir que la fórmula vale para todos los números naturales?

La respuesta es sí. En la próxima sección vamos a formalizar este tipo de argumentos para poder aplicarlos en la demostración de propiedades sobre los números naturales.

□ 3. Principio de inducción

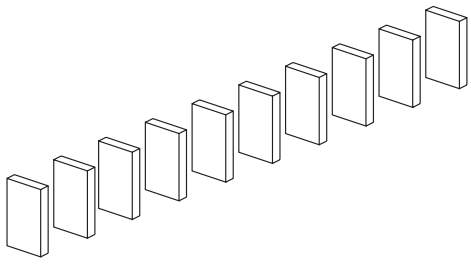


Figura 3. *Las fichas dispuestas para ser tiradas.*

Una herramienta muy usada para demostrar afirmaciones sobre los números naturales es el *principio de inducción*. Imaginemos una hilera de fichas de dominó paradas como en el dibujo de la figura 3.

Las fichas están dispuestas de manera que si cae una, tira a la siguiente. Entonces, podemos hacer que todas se caigan empujando solo la primera, como en la figura 4. Esta idea de las fichas cayendo es la base del principio de inducción.

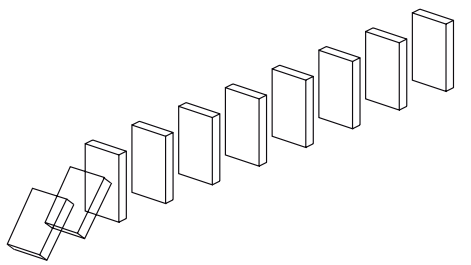


Figura 4. *Las fichas comienzan a caer.*

Principio de inducción. Supongamos que tenemos para cada número natural una afirmación $P(n)$ y queremos ver que todas estas afirmaciones son válidas. Si se puede demostrar que:

1. $P(1)$ es cierta,
2. si $P(n)$ es cierta,

entonces $P(n+1)$ también lo es, entonces $P(n)$ vale para todo $n \in \mathbb{N}$.

La parte 2. corresponde a que si una ficha de dominó cae, entonces tira la siguiente. La parte 1. corresponde a tirar la primera ficha. El hecho de que todas las fichas caigan es lo que explica que todas las afirmaciones $P(n)$ sean ciertas.

Veamos cómo funciona el principio de inducción en un ejemplo. De hecho, lo que hicimos al calcular la suma de las primeras potencias de 2 en la sección anterior fue aplicar, sin mencionarlo, el principio de inducción. Más precisamente, para cada $n \in \mathbb{N}$ afirmamos que $1 + 2 + ... + 2^n = 2^{n+1} - 1$. Esta afirmación es $P(n)$.

El principio nos dice que basta con verificar:

- $P(1) : 1 + 2 = 2^2 - 1$, lo cual es cierto.
- Supongamos que es cierto $P(n)$, es decir que $1 + 2 + \ldots + 2^n = 2^{n+1} - 1$. A partir de aquí debemos demostrar que $P(n + 1)$ es cierto, es decir que $1 + 2 + \ldots + 2^n + 2^{n+1} = 2^{n+2} - 1$. Esto es exactamente lo que hicimos en (1).

Apliquemos el principio de inducción al primer ejemplo de la sección anterior. En este caso $P(n)$ es la afirmación de que la suma de los primeros n números naturales es $\frac{n(n+1)}{2}$.

- $P(1) : 1 = \frac{1\cdot(1+1)}{2}$, lo cual es cierto.
- Supongamos que es cierto $P(n)$, es decir que $1 + 2 + \ldots + n = \frac{n(n+1)}{2}$. A partir de aquí, debemos demostrar que $P(n + 1)$ es cierto, es decir que $1 + 2 + \ldots + n + (n + 1) = \frac{(n+1)(n+2)}{2}$. Ahora:

$$\begin{aligned} \underbrace{1+2+\cdots+n}_{\frac{n(n+1)}{2}}+(n+1) &= \frac{n}{2}(n+1)+(n+1) \\ &= (n+1)\left(\frac{n}{2}+1\right) \\ &= (n+1)\left(\frac{n+2}{2}\right) \\ &= \frac{(n+1)(n+2)}{2} \end{aligned}$$

Ejercicio 1.2. Probar que para todo número natural n vale que:

$$1 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$$

Muchas veces se quiere probar la validez de afirmaciones $P(n)$ para los números naturales a partir de uno dado. Es decir, imaginemos que queremos probar que $P(n)$ es cierta para $n \geq M$, donde M es un número natural. El principio de inducción se aplica casi igual. La única diferencia es que en lugar de demostrar que $P(1)$ es cierta, demostramos que $P(M)$ es cierta.

Ejemplo. Probemos que la suma de los ángulos interiores de un n-ágono es $180^o(n - 2)$. Esta afirmación sólo tiene sentido si $n \geq 3$. En este caso, $M = 3$. Para probar la fórmula, debemos comenzar por ver que $P(3)$ es cierta. Es decir, que la suma de los ángulos interiores de un triángulo es $180^o(3 - 2) = 180^o$. Esta propiedad de los triángulos es bien conocida y no la demostraremos aquí. Debemos entonces demostrar que si la suma de los ángulos interiores de un n-ágono es $180^o(n - 2)$, entonces la de un $(n + 1)$-ágono es $180^o(n + 1 - 2) = 180^o(n - 1)$. Para ver esto, apelamos a la construcción de la Figura 5. Trazando la diagonal del dibujo, el $(n + 1)$-ágono se separa en un triángulo

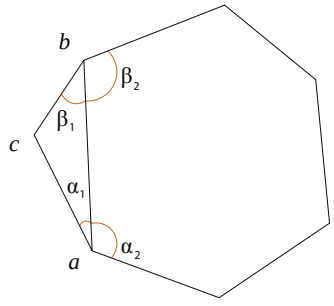


Figura 5. *Separación de un (n + 1)-ágono en un triángulo y un n-ágono.*

y un n-ágono. Observemos que la suma de los ángulos interiores del $(n + 1)$-ágono es la suma de los ángulos interiores del n-ágono más la del triángulo. El ángulo en el vértice a del $(n + 1)$-ágono se separa en α_1 (que es uno de los ángulos del triángulo) y α_2 (que es uno de los ángulos del n-ágono). Lo mismo ocurre con el ángulo en b, que se separa en β_1 y β_2. Como estamos suponiendo que $P(n)$ es cierta, la suma de los ángulos interiores del n-ágono es $180^o(n - 2)$. Por otra parte, la suma de los ángulos interiores del triángulo es 180^o. Entonces, la suma de los ángulos interiores del $(n + 1)$-ágono es $180^o(n - 2) + 180^o = 180^o(n - 2 + 1) = 180^o(n - 1)$.

Veamos otro ejemplo. Queremos probar que para todo $n \geq 8$ vale la desigualdad $2^n \geq 3n^2 + 3n + 1$. Para esto, probamos primero que vale para $n = 8$:

$$2^8 = 256, \quad 3 \cdot 8^2 + 3 \cdot 8 + 1 = 217, \text{ entonces } 2^8 \geq 3 \cdot 8^2 + 3 \cdot 8 + 1$$

Ahora, suponiendo que la desigualdad es válida para n, la probamos para $n+1$. Es decir, probamos que $2^{n+1} \geq 3(n + 1)^2 + 3(n + 1) + 1$. Por un lado:

$$\begin{aligned} 2^{n+1} &= 2 \cdot 2^n \\ &= 2^n + 2^n \end{aligned}$$

Por otro lado:

$$3(n + 1)^2 + 3(n + 1) + 1 = 3n^2 + 6n + 3 + 3n + 3 + 1 = 3n^2 + 3n + 1 + 6n + 6$$

Como estamos asumiendo que $2^n \geq 3n^2+3n+1$, si probamos que $2^n \geq 6n+6$, para todo $n \geq 8$, tendremos que:

$$2^{n+1} = 2^n + 2^n \geq 3n^2 + 3n + 1 + 6n + 6 = 3(n + 1)^2 + 3(n + 1) + 1$$

Veamos, entonces, que $2^n \geq 6n + 6$ para todo $n \geq 8$. Nuevamente, esta propiedad la probamos por inducción. Si $n = 8$, nos queda $2^8 = 256$ y $6 \cdot 8 + 6 = 54$, por lo que la propiedad vale. Si asumimos ahora que vale para n, es decir, que $2^n \geq 6n + 6$, debemos probar que $2^{n+1} \geq 6(n + 1) + 6$. Como suponemos que $n \geq 8$, $2^n \geq 2^8 = 256 \geq 6$, y entonces $2^{n+1} = 2^n + 2^n \geq 6n + 6 + 6 = 6(n + 1) + 6$.

Ejercicio 1.3. Probar que $2^n \geq n^3$ para todo $n \geq 10$.

Ejercicio 1.4. Probar que $3^n \geq 2^{n+1} + n$ para todo $n \geq 3$.

□ 4. Axiomas de Peano

A fines del siglo XIX, Giuseppe Peano[1] dio una definición axiomática de los números naturales. La clave de la definición de Peano es la noción de *sucesor*: todo número natural tiene un sucesor, que se obtiene sumándole 1. Para entender los axiomas de Peano, observemos que el conjunto $\mathbb{N}$ cumple las siguientes propiedades:

[1] Matemático italiano que vivió entre 1858 y 1932. Enseñó en la Universidad de Turín y se dedicó a la investigación de, entre otras cosas, lógica, teoría de conjuntos y ecuaciones diferenciales.

1. El 1 es el único número natural que no es sucesor de ningún número natural.
2. Si a y b son dos números naturales distintos, el sucesor de a es distinto del sucesor de b.
3. Si K es un subconjunto de $\mathbb{N}$ tal que $1 \in K$ y vale que el sucesor de cualquier elemento de K también está en K, entonces $K = \mathbb{N}$.

Peano descubrió que estas propiedades alcanzan para definir a los números naturales, en el sentido de que cualquier conjunto con una función sucesor que satisfaga las 3 propiedades anteriores es "equivalente" al conjunto de números naturales. Formalmente, se puede dar la siguiente definición:

El conjunto de números naturales es un conjunto $\mathbf{P}$ con una función sucesor $S : \mathbf{P} \to \mathbf{P}$ que satisface los siguientes 3 axiomas:

1. $\mathbf{P}$ tiene un único elemento que no es sucesor de otro elemento de $\mathbf{P}$. Llamamos 1 a este elemento.
2. La función S es inyectiva. O sea, si a y b son elementos distintos de $\mathbf{P}$ entonces $S(a)$ es distinto de $S(b)$.
3. Si K es un subconjunto de $\mathbf{P}$ tal que $1 \in K$ y vale que el sucesor de cualquier elemento de K también está en K, entonces $K = \mathbf{P}$

El axioma 3 es equivalente al principio de inducción. Para verlo, supongamos que tenemos un subconjunto K de los números naturales que tiene al 1 y que cumple que si $n \in K$, su sucesor $n+1 \in K$. Llamemos $P(n)$ a la afirmación $n \in K$.

Sabemos que $P(1)$ es cierta y que si $P(n)$ es cierta, $P(n + 1)$ también lo es. Luego por el principio de inducción, $P(n)$ es cierta para todo $n \in \mathbb{N}$, o sea $n \in K$ para todo $n \in \mathbb{N}$. Luego $K = \mathbb{N}$.

Recíprocamente, supongamos que tenemos una afirmación $P(n)$ para cada número natural n que cumple que:

- $P(1)$ es cierta y,
- si $P(n)$ es cierta, $P(n + 1)$ también lo es.

Llamemos K al subconjunto de números naturales n para los que $P(n)$ es cierta.

Luego $1 \in K$. Por otra parte, si $n \in K$, su sucesor $n + 1 \in K$. Con todo esto, por el axioma 3, $K = \mathbb{N}$. Es decir, $P(n)$ es cierta para todo número natural n.

□ 5. Definiciones recursivas

Muchas veces uno necesita definir una sucesión de *manera recursiva*. Esto es, definir un elemento de la sucesión en términos de otros anteriores. Por ejemplo, consideremos la sucesión:

$$a_1 = 2, \quad a_{n+1} = a_n^2 + 1.$$

¿Cómo calculamos a_4? Por definición:

$$a_4 = a_3^2 + 1$$

Luego, conociendo el valor de a_3 podemos calcular a_4. De la misma manera, usando la definición para a_3, tenemos que:

$$a_3 = a_2^2 + 1$$

Repitiendo el proceso para a_2:

$$a_2 = a_1^2 + 1$$

Pero el valor de a_1 lo conocemos, lo que nos permite calcular:

$$\begin{array}{rcccc} a_2 & = & 2^2 + 1 & = & 5 \\ a_3 & = & 5^2 + 1 & = & 26 \\ a_4 & = & 26^2 + 1 & = & 677 \end{array}$$

Este tipo de definiciones, en la que el valor de cada término depende del valor de términos anteriores, se denomina *definición recursiva*. Usualmente, para que la definición esté bien, es necesario precisar el valor de los primeros términos de la sucesión. La cantidad de términos necesarios depende de la definición recursiva. Si cada término de la sucesión depende exclusivamente del término anterior, como en el ejemplo, entonces es necesario definir explícitamente un término (en el ejemplo, definimos $a_1 = 2$ de manera explícita). Si cada término depende de los dos anteriores, serán necesarios dos términos, etcétera. Consideremos otro ejemplo:

$$L_1 = 2, \quad L_2 = 1, \quad L_{n+2} = L_{n+1} + L_n$$

Los primeros términos de esta sucesión son:

$$L_1 = 2,\ L_2 = 1,\ L_3 = 3,\ L_4 = 4,\ L_5 = 7,\ L_6 = 11,\ L_7 = 18,\ L_8 = 29$$

Como se ve, con la información dada se pueden calcular todos los términos de la sucesión. Esta sucesión se conoce como "números de Lucas" (ya que fueron introducidos por Edouard Lucas), y está íntimamente relacionada con la sucesión de Fibonacci, que veremos en la sección siguiente. Como la fórmula recursiva $L_{n+2} = L_{n+1} + L_n$ da un término en función de los dos anteriores, son necesarios dos valores explícitos de la sucesión (L_1 y L_2). De hecho, si cambiásemos el valor de L_1 y L_2 dejando la fórmula recursiva intacta, los valores de la sucesión cambiarían. Si por ejemplo pusiésemos:

$$L'_1 = 1, \quad L'_2 = 5, \quad L'_{n+2} = L'_{n+1} + L'_n$$

Tendríamos:

$$L'_1 = 1,\ L'_2 = 5,\ L'_3 = 6,\ L'_4 = 11,\ L'_5 = 17,\ L'_6 = 28,\ L'_7 = 45,\ L'_8 = 73$$

Una sucesión muy usada en matemática es el factorial. El factorial de un número natural n se escribe $n!$ e, informalmente, se define como:

$$n! = 1 \cdot 2 \cdot 3 \ldots (n-1) \cdot n$$

Por ejemplo, 3! = 1 · 2 · 3 = 6, y 7! = 1 · 2 · 3 · 4 · 5 · 6 · 7 = 5.040.

La definición formal de factorial es:

$$1! = 1, \quad (n+1)! = (n+1) \cdot n!$$

Entonces, por ejemplo:

$$\begin{aligned} 4! &= 4 \cdot 3! \\ &= 4 \cdot 3 \cdot 2! \\ &= 4 \cdot 3 \cdot 2 \cdot 1! \\ &= 4 \cdot 3 \cdot 2 \cdot 1 \\ &= 24 \end{aligned}$$

Puede generar dudas que una definición recursiva esté bien hecha. El hecho de definir algo en términos de sí mismo no parece muy correcto. Sin embargo, las definiciones recursivas no sólo están bien, sino que muchas veces son necesarias. Y, además, son lo suficientemente formales como para hacerlas con una computadora. Como ejemplo, veamos dos definiciones posibles para el cálculo del factorial en lenguaje Python (elegimos el Python porque es muy sencillo, incluso para quien no lo conoce. De todas maneras, se puede reemplazar por una gran colección de lenguajes que permiten definiciones recursivas).

Una primera posible definición de factorial es:

```
def factorial(n):
    f = 1
    for i in range(1,n+1):
        f = f * i
    return f
```

La línea `f=1` pone en la variable *f* el valor 1. Luego, la instrucción: `for i in range(1,n+1):` ejecuta la línea que sigue para todos los valores de *i* entre 1 y *n*. Y la línea que sigue es poner en la variable *f* el valor que tenía *f* multiplicado por el valor de *i*.

Esta definición se parece a la primera que dimos. Dice que el factorial de un número *n* se calcula recorriendo todos los números de 1 a *n* y multiplicándolos entre sí. Vamos a ver otra definición, que se parece a la definición recursiva:

```
def factorial(n):
    if n == 1:
        return 1
    else:
        return n * factorial(n-1)
```

Aquí se dice que para calcular el factorial, hay dos posibilidades: si el número es 1, el factorial vale 1. Si no, el factorial vale *n* multiplicado por el factorial de *n* - 1.

Ejercicio 1.5. (Para el lector que sabe programar). Dar una definición de los números de Lucas L_n y de la variante L'_n en un lenguaje que permita definiciones recursivas.

□ 6. Principio de inducción global

Lorena decide participar en un concurso de juegos de ingenio. Llegado su turno, le dan el siguiente problema: dada la sucesión a_n definida por:

$$a_1 = 2, \quad a_2 = 8, \quad a_{n+2} = 4(a_{n+1} - a_n)$$

calcular el término 2.009 de la sucesión. Lorena calcula los primeros términos:

$$\begin{aligned} a_1 &= 2 \\ a_2 &= 8 \\ a_3 &= 24 \\ a_4 &= 64 \\ a_5 &= 160 \\ a_6 &= 384 \end{aligned}$$

Observa que a_n es divisible por n para cada uno de los valores de la lista. Además, al dividir a_n por n, obtiene:

$$\begin{aligned} a_1 &= 1 \cdot 2 \\ a_2 &= 2 \cdot 4 \\ a_3 &= 3 \cdot 8 \\ a_4 &= 4 \cdot 16 \\ a_5 &= 5 \cdot 32 \\ a_6 &= 6 \cdot 64 \end{aligned}$$

Después de observar detenidamente la columna de la derecha, Lorena conjetura que $a_n = n \cdot 2^n$ para todo $n \in \mathbb{N}$, pero antes de contestar quiere estar segura de que su respuesta es correcta. Para probarlo, Lorena intenta recurrir al principio de inducción, pero se topa con una dificultad. Si llama $P(n)$ a la afirmación $a_n = n \cdot 2^n$, entonces vale $P(1)$ pero no puede demostrar que si $P(n)$ es cierta, entonces $P(n+1)$ es cierta.

Lo que sucede es que la fórmula $a_{n+2} = 4(a_{n+1} - a_n)$ involucra tres términos consecutivos. Por esto, el conocer un término no permite conocer el siguiente. Es para casos como éste que hace falta el *principio de inducción global*.

Principio de Inducción Global. Supongamos que tenemos para cada $n \in \mathbb{N}$ una afirmación $P(n)$ y queremos ver que todas estas afirmaciones son válidas. Si se puede demostrar que:

- $P(1)$ es cierta,
- si $P(k)$ es cierta para todo $k < n$, entonces $P(n)$ también lo es,

entonces $P(n)$ vale para todo $n \in \mathbb{N}$.

Veamos cómo puede utilizar Lorena el principio de inducción global. Probemos que $a_n = n \cdot 2^n$ para todo $n \in \mathbb{N}$. Primero, verificamos que $P(1)$ es cierta: $a_1 = 2 = 1 \cdot 2^1$. Ahora, suponemos que $P(k)$ es cierta para todo $k < n$. Por la definición de la sucesión, $a_n = 4(a_{n-1} - a_{n-2})$, pero esto vale solo para $n > 2$, ya que a_0 no está definido. Tenemos entonces dos casos: $n = 2$ y $n > 2$. Si $n = 2$, la afirmación $P(2)$ se verifica simplemente

observando que $a_2 = 8 = 2 \cdot 2^2$. Y si $n > 2$, como $n - 1 < n$ y $n - 2 < n$, nuestra hipótesis inductiva dice que valen las fórmulas para a_{n-1} y a_{n-2}, es decir:

$$a_{n-1} = (n-1) \cdot 2^{n-1}$$
$$a_{n-2} = (n-2) \cdot 2^{n-2}$$

Entonces:

$$\begin{aligned} a_n &= 4(a_{n-1} - a_{n-2}) \\ &= 4((n-1) \cdot 2^{n-1} - (n-2) \cdot 2^{n-2}) \\ &= 4 \cdot 2^{n-2}((n-1) \cdot 2 - (n-2)) \\ &= 2^2 \cdot 2^{n-2}(2n - 2 - n + 2) \\ &= 2^n \cdot n. \end{aligned}$$

Ahora sí Lorena contesta $a_{2.009} = 2^{2.009} \times 2.009$.

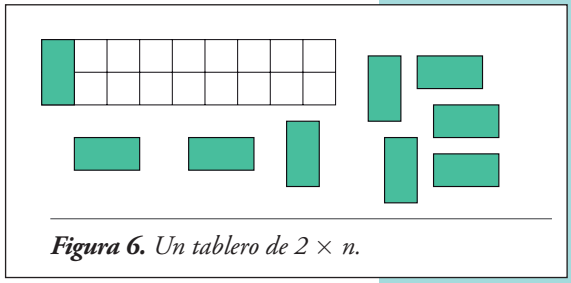


Figura 6. *Un tablero de 2 × n.*

Vamos a considerar un nuevo ejemplo, planteado por Fibonacci [2]. Tenemos un tablero de $2 \times n$, como en el dibujo de la Figura 6.

Queremos llenarlo con fichas de 2×1 con una regla: la ficha de la izquierda debe ir de manera vertical, como se muestra en la Figura 6.

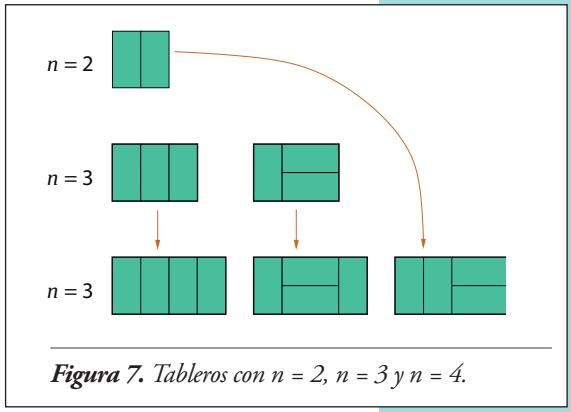


Figura 7. *Tableros con n = 2, n = 3 y n = 4.*

Llamamos F_n a la cantidad de formas de llenar el tablero de tamaño n con esta regla. Si queremos llenar un tablero, a la derecha hay dos posibilidades: o bien la última ficha la ponemos de manera vertical, o bien ponemos dos fichas de manera horizontal. En el caso vertical, al agregar esta ficha nos queda por llenar un tablero de tamaño $2 \times (n-1)$ que debe cumplir la regla. En el caso horizontal, al poner estas dos fichas, nos queda por llenar un tablero de tamaño $2 \times (n-2)$ que debe cumplir la regla. En la Figura 7, se ve cómo los tableros de tamaño 2×4 se forman a partir de los tableros de tamaño 2×3 y 2×2.

Esto dice que $F_n = F_{n-1} + F_{n-2}$ para todo $n \geq 3$. Por otra parte, $F_1 = 1$ y $F_2 = 1$. Veamos los primeros números de esta sucesión:

$$\begin{aligned} F_1 &= 1 \\ F_2 &= 1 \\ F_3 &= 2 \\ F_4 &= F_3 + F_2 = 2 + 1 = 3 \\ F_5 &= F_4 + F_3 = 3 + 2 = 5 \\ F_6 &= F_5 + F_4 = 5 + 3 = 8 \end{aligned}$$

y luego sigue con 13, 21, 34, 55, 89, etc. Es prácticamente imposible encontrar, a simple vista, una fórmula no recursiva para F_n. Sin embargo, se puede dar una:

[2] Fibonacci planteó este problema con conejos. Su libro "Liber Abaci" de 1202 dice textualmente: "Cierto hombre tenía una pareja de conejos juntos en un lugar cerrado y uno desea saber cuántos son creados a partir de este par en un año; cuando es su naturaleza parir otro par en un simple mes, y en el segundo mes, los nacidos parir también".

$$F_n = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n$$

Vamos a probar esta fórmula por inducción global. Para $n = 1$, tenemos que:

$$\begin{aligned}\frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^1 - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^1 &= \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}-1+\sqrt{5}}{2}\right)\\ &= \frac{1}{\sqrt{5}}\sqrt{5}\\ &= 1\\ &= F_1\end{aligned}$$

Para $n = 2$, tenemos:

$$\begin{aligned}\frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^2 - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^2 &= \frac{1}{\sqrt{5}}\left(\frac{(1+\sqrt{5})^2-(1-\sqrt{5})^2}{4}\right)\\ &= \frac{1}{\sqrt{5}}\frac{(1+2\sqrt{5}+5)-(1-2\sqrt{5}+5)}{4}\\ &= \frac{1}{\sqrt{5}}\frac{4\sqrt{5}}{4}\\ &= 1\\ &= F_2\end{aligned}$$

Ahora, si $n \geq 3$, suponemos que vale la fórmula para todos los $k < n$. Entonces:

$$\begin{aligned}F_n = F_{n-1} + F_{n-2} &= \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^{n-1} - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^{n-1} + \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^{n-2} - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^{n-2}\\ &= \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^{n-2}\left(\frac{1+\sqrt{5}}{2}+1\right) - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^{n-2}\left(\frac{1-\sqrt{5}}{2}+1\right)\\ &= \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^{n-2}\left(\frac{1+\sqrt{5}+2}{2}\right) - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^{n-2}\left(\frac{1-\sqrt{5}+2}{2}\right)\\ &= \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^{n-2}\left(\frac{6+2\sqrt{5}}{4}\right) - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^{n-2}\left(\frac{6-2\sqrt{5}}{4}\right)\\ &= \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^{n-2}\left(\frac{1+\sqrt{5}}{2}\right)^2 - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^{n-2}\left(\frac{1-\sqrt{5}}{2}\right)^2\\ &= \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^{n} - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^{n}\end{aligned}$$

Veamos un nuevo ejemplo de inducción global. Martín y Pablo, alumnos de la Escuela 314, compraron un chocolate que viene dividido en cuadraditos, y lo comen jugando un juego. El que pierde, va a pagar el próximo chocolate. El juego es así:

1. por turnos, Martín y Pablo cortan el chocolate en dos pedazos por una línea horizontal o vertical, como en la figura 8;
2. el que hizo el corte, elige el pedazo que quiere y deja el resto;

3. se van alternando en los cortes, hasta que queda un solo cuadradito, que ya no se puede cortar;
4. quien se queda con este último cuadradito, pierde el juego (y paga el chocolate que sigue).

La pregunta entonces es: ¿cuál es la mejor estrategia para no quedarse con el último cuadradito? Pensando en la estrategia ganadora, Martín observa que si le deja a Pablo un cuadrado de chocolate de 2×2, entonces Pablo va a perder seguro. Esto es porque con cualquier corte que haga Pablo deja un rectángulo de 2×1, y en la jugada siguiente Martín lo deja con el último cuadradito. Luego, observa que si le deja a Pablo un cuadrado de 3×3 también sabe cómo ganarle: en este caso Pablo puede dejar o bien un rectángulo de 3×2 o bien uno de 3×1. Si deja uno de 3×1, Martín le deja el último cuadradito y Pablo pierde. Si Pablo deja uno de 3×2, Martín le deja uno de 2×2 y como en el caso anterior Pablo pierde. Estudiando estos casos, Martín se da cuenta de cómo ganar si en algún momento a Pablo le queda para jugar un chocolate cuadrado de cualquier tamaño: cada vez que Pablo juega, Martín, en su turno, le deja nuevamente un chocolate cuadrado.

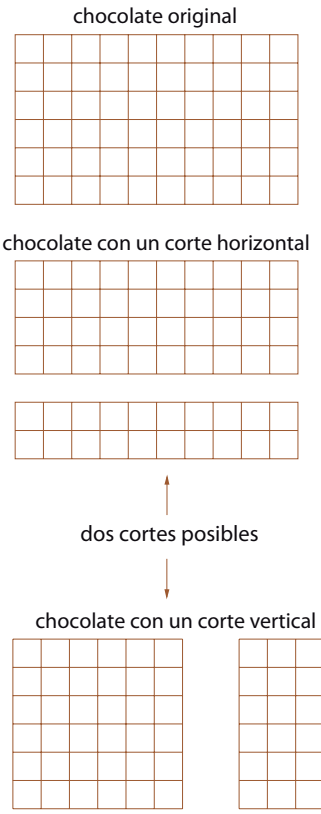


Figura 8. *El chocolate y dos cortes posibles.*

Probemos que Martín está en lo cierto. Para cada $n \in \mathbb{N}$ llamemos $P(n)$ a la afirmación siguiente: *si a Pablo le toca cortar un cuadrado de $n \times n$, Martín tiene una estrategia para ganar.*

Para $n = 1$, Martín no hace nada y gana. Supongamos que Martín tiene una estrategia para ganar si a Pablo le toca cortar un chocolate cuadrado de $k \times k$ para cualquier k menor que n (éstas son las afirmaciones $P(k)$ para $k < n$). Supongamos ahora que a Pablo le toca un chocolate cuadrado de $n \times n$. Pablo hace un corte, y le deja a Martín un chocolate rectangular de $k \times n$ para algún k menor que n. En su turno Martín corta el chocolate de manera de dejar a Pablo un cuadrado de $k \times k$ (ver Figura 9). Por hipótesis inductiva, a partir de aquí Martín tiene una estrategia para ganar.

Como conclusión, si el chocolate es cuadrado, siguiendo la estrategia de Martín el que comienza siempre pierde. Si el chocolate no es cuadrado, el que comienza siempre gana.

Ejercicio 1.6. Dada la siguiente sucesión definida recursivamente, conjeturar una fórmula para el término general y probarla:

$$a_1 = 1, \qquad a_2 = 4, \qquad a_{n+2} = 4\sqrt{a_{n+1}} + a_n \text{ para } n \in \mathbb{N}.$$

Ejercicio 1.7. Consideremos la sucesión definida recursivamente por:

$$a_1 = 2, \qquad a_2 = 3, \qquad a_{n+2} = 2a_{n+1} + a_n \text{ para } n \in \mathbb{N}.$$

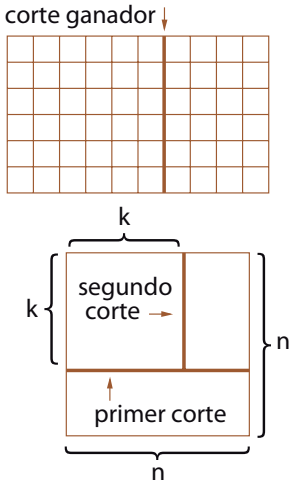


Figura 9. *Chocolate con cortes estratégicos.*

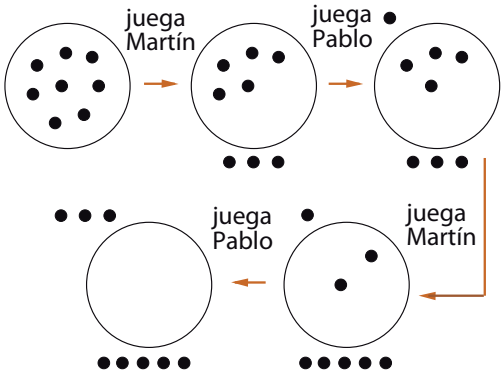


Figura 10. *Juegan Martín y Pablo.*

Probar que $a_n \leq 3^n$ para todo $n \in \mathbb{N}$.

Ejercicio 1.8. Martín y Pablo ahora juegan al siguiente juego: tienen un plato con piedritas. Por turnos, van sacando 1, 2, ó 3 piedritas. Quien vacía el plato gana. Por ejemplo, si hay 8 piedritas, Martín saca en su turno 3 y Pablo saca 1, y quedan 4. Ahora Martín saca 2 y Pablo saca las 2 que quedan. Gana Pablo. (ver figura 10)

¿Es cierto que si Martín empieza jugando con 8 piedritas, sin importar lo que haga, Pablo siempre tiene una manera de ganar? ¿Qué pasa si empieza con 9 piedritas? Para cada $n \in \mathbb{N}$, decidir quién tiene una estrategia ganadora si Martín empieza con n piedritas, y probarlo por inducción.

□ 7. Principio de buena ordenación

Con el orden usual, los naturales gozan de una propiedad importante: son bien ordenados.

Un conjunto A con una relación de orden $\leq$ se dice **bien ordenado** si todo subconjunto $B \subseteq A$ no vacío tiene un primer elemento (aquí "primer" elemento significa que es menor que todos los otros elementos de B).

Si consideramos A como el conjunto de los números enteros y B el de los enteros pares, entonces B no tiene primer elemento, porque para cualquier entero par m hay un entero par menor (por ejemplo m-2). Esto dice que el conjunto de los números enteros no es bien ordenado. Sin embargo, si ahora A es el conjunto de los números naturales y B es el de los naturales pares, entonces B sí tiene primer elemento: el 2, porque es el menor de los números naturales pares.

Gracias al principio de inducción global podemos probar el siguiente Teorema.

Teorema 1.1. *El conjunto de los números naturales es bien ordenado.*

Demostración. Vamos a demostrar que si $B \subseteq \mathbb{N}$ y B no tiene primer elemento, entonces B es vacío. Para esto, consideramos $P(n)$ como la afirmación "$n \notin B$", y vamos a probar por inducción global que $P(n)$ es verdadera para todo n. La afirmación $P(1)$ es verdadera porque si no lo fuera, 1 pertenecería a B y sería su primer elemento. Por otra parte, supongamos que $P(k)$ es cierta para todo $k < n$. Entonces, debemos probar que $P(n)$ también lo es. Como $P(k)$ es cierta para todo $k < n$, ninguno de los números $1, 2, \ldots, n-1$ pertenecen a B. Si $P(n)$ fuese

falsa, entonces n pertenecería a B y sería su primer elemento. Luego, n no puede pertenecer a B y $P(n)$ es verdadera.

En realidad, el principio de buena ordenación es *equivalente* al principio de inducción. Es decir, también podemos ver que el principio de inducción se deduce del principio de buena ordenación. De hecho, supongamos que para cada $n \in \mathbb{N}$, $P(n)$ es una afirmación tal que $P(1)$ es cierta y si $P(n)$ es cierta, entonces $P(n+1)$ también lo es. Podemos probar, gracias al principio de buena ordenación, que $P(n)$ es cierta para todos los números naturales. Para ello, consideramos B el conjunto de los n tales que $P(n)$ es falsa. Si B fuese no vacío, tendría un primer elemento, llamémoslo k. No puede ser $k = 1$ porque $P(1)$ es cierta. Entonces $k > 1$, y si $n = k - 1$, tenemos que $P(n)$ es cierta porque $k - 1 \notin B$. Pero esto dice que $P(n + 1)$ es cierta, es decir, $P(k)$ es cierta, y esto es un absurdo.

□ 8. Ejemplos surtidos

8.1. Torres de Hanoi o Torres de Brahma

El problema de las Torres de Hanoi fue inventado por el matemático francés Edouard Lucas en 1883. Tenemos tres grandes baldosas en el suelo, y un cierto número de discos de distinto tamaño apilados uno encima del otro en la primera baldosa ordenados por tamaño. El más pequeño está encima de la pila. El objetivo del juego es lograr mover toda la pila de discos a la tercera baldosa, con la condición de que:

- no se puede mover más de un disco a la vez;
- sólo se puede sacar el disco de la parte superior de cada pila de discos;
- en todo momento, en cada baldosa los discos deben estar ordenados por tamaño.

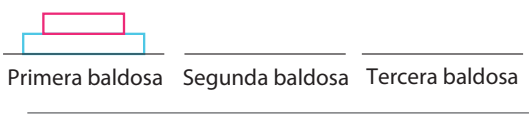


Figura 11. *Torre con 2 discos.*

Veamos cómo resolvemos este problema si tenemos simplemente dos discos:

- comenzamos con dos discos en la primera baldosa, como en la figura 11;
- en el primer paso solamente podemos quitar el disco pequeño y colocarlo en otra baldosa. Lo colocamos en la segunda baldosa;
- en el segundo paso, podemos mover el disco más grande para ubicarlo en la tercera baldosa;
- en el tercer paso, movemos el disco pequeño colocándolo encima del disco grande y conseguimos que quede la torre original en el tercer lugar.

Figura 12. *Resolución con 2 discos.*

Todo este proceso se ve en la figura 12.

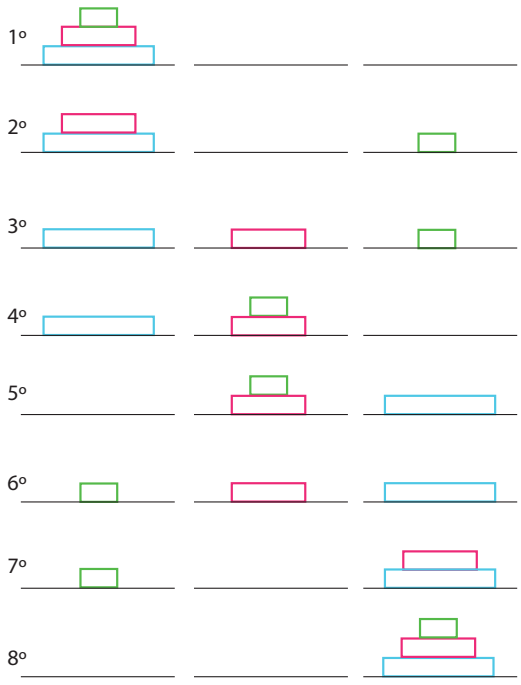


Figura 13. *Torre con 3 discos.*

Es bastante claro que no se puede hacer esto en menos de 3 pasos, dado que el primer paso es único (mover el disco pequeño). En el segundo paso tenemos dos opciones, pero si queremos lograr mover toda la torre, en algún momento deberá estar el disco grande en la tercera baldosa. Entonces, lo mejor es hacerlo en el segundo movimiento, y luego debemos colocar el disco pequeño sobre el grande.

La pregunta que hizo Lucas es si comenzamos con n discos: ¿cuál es el mínimo número de movimientos necesarios para pasar todos los discos de la primera baldosa a la tercera?

Invitamos a jugar un rato el juego, antes de continuar leyendo la respuesta. Existen versiones de plástico de este juego, que tienen tres postes tipo ábaco, y los discos están perforados para poder apilarlos de manera sencilla, aunque se puede jugar con monedas de distintos tamaños.

Llamemos H_n al número mínimo de movimientos para una torre de n discos. Sabemos que $H_1 = 1$ y $H_2 = 3$. Calculemos H_3. Como vemos en la Figura 13, alcanzan 7 movimientos. O sea: $H_3 \leq 7$.

Supongamos ahora que tenemos n discos. Para mover toda la torre a la tercera baldosa, en algún momento debemos colocar el disco más grande en la tercera baldosa. Dado que es el más grande de todos, si pensamos que este disco no existe y movemos los otros n - 1 discos de manera ordenada, los discos estarán ordenados en todo momento. Supongamos que sabemos cómo mover la torre de los n - 1 discos más pequeños a otra baldosa en H_{n-1} pasos de forma óptima. Entonces, podemos mover de esta forma los n - 1 discos más chicos a la segunda baldosa, luego mover el disco mayor hasta la tercera baldosa, y una vez hecho esto, mover los n - 1 discos menores para colocarlos de manera ordenada encima de él, nuevamente de forma óptima en H_{n-1} pasos (notar que esto fue lo hecho con 3 discos). En conclusión, probamos que

$$H_n = 2 \cdot H_{n-1} + 1.$$

Ejercicio 1.9. Probar por inducción que la sucesión dada por:

$$H_1 = 1, \qquad H_n = 2 \cdot H_{n-1} + 1 \text{ si } n \geq 1,$$

satisface $H_n = 2^n - 1$.

8.2. Algoritmo de ordenamiento (Sort)

Supongamos que tenemos una lista $[a_1, \ldots, a_n]$ de objetos que queremos ordenar con determinado criterio, por ejemplo números naturales para ordenar en forma creciente, o palabras para ordenar alfabéticamente.

Existe una gran variedad de algoritmos que permiten realizar esta tarea; vamos a analizar uno de ellos. La idea es la siguiente:

1. si la lista tiene uno o ningún elemento, no hay nada que hacer;
2. si la lista tiene dos o más elementos, se la subdivide en dos listas con la misma cantidad de elementos (o una con un elemento más que la otra si n es impar);
3. se ordena cada una de las dos listas nuevas y, a continuación, se las vuelve a unir, pero ordenando los elementos entre sí.

Para unir las dos listas ordenadas L_1 y L_2 y armar una única lista L, también ordenada, con los elementos de ambas, se utiliza el siguiente procedimiento:

- si alguna de las listas no tiene elementos, se agregan los elementos de la otra lista a L y se terminó el procedimiento;
- si ambas listas tienen elementos, se toma el primer elemento α de L_1 y se lo compara con el primer elemento β de L_2. Si $\alpha \leq \beta$, se agrega α a la lista L y se lo suprime de L_1 (L_2 no se modifica). Si $\alpha > \beta$, se agrega β a L y se lo suprime de L_2 (L_1 no se modifica). Luego, se repite el proceso con las nuevas listas.

Supongamos que queremos ordenar en forma creciente la lista $L = [4, 1, 2, 5, 7, 3, 6, 8]$. Consideramos las sublistas $L_1 = [4, 1, 2, 5]$ y $L_2 = [7, 3, 6, 8]$. Para ordenar L_1, la subdividimos nuevamente en dos listas $L_{11} = [4, 1]$ y $L_{12} = [2, 5]$.

Ordenamos L_{11} obteniendo $L'_{11} = [1, 4]$, y L_{12} obteniendo $L'_{12} = [2, 5]$. Ahora las volvemos a unir, ordenando los elementos: el primer elemento de L'_{11} es menor que el primero de L'_{12}, entonces ubicamos en primer lugar a 1. El segundo elemento de L'_{11} es mayor que el primero de L'_{12}; agregamos entonces el 2. Comparamos el segundo elemento de L'_{11} con el segundo de L'_{12}, y resulta menor, con lo que lo agregamos. Nos queda entonces la lista L_1 ordenada como $L'_1 = [1, 2, 4, 5]$.

Procediendo análogamente, se ordena la lista L'_2, obteniéndose $L'_2 = [3, 6, 7, 8]$. Para terminar, se unen las listas L'_1 y L'_2, comparando como antes uno a uno sus elementos:

L'	L'_1	L'_2	
$[\,]$	$[\underline{1}, 2, 4, 5]$	$[\underline{3}, 6, 7, 8]$	$1 < 3$
$[1]$	$[\underline{2}, 4, 5]$	$[\underline{3}, 6, 7, 8]$	$2 < 3$
$[1, 2]$	$[\underline{4}, 5]$	$[\underline{3}, 6, 7, 8]$	$4 > 3$
$[1, 2, 3]$	$[\underline{4}, 5]$	$[\underline{6}, 7, 8]$	$4 < 6$
$[1, 2, 3, 4]$	$[\underline{5}]$	$[\underline{6}, 7, 8]$	$5 < 6$
$[1, 2, 3, 4, 5]$	$[\,]$	$[6, 7, 8]$	$L'_1 = [\,]$
$[1, 2, 3, 4, 5, 6, 7, 8]$	$[\,]$	$[\,]$	

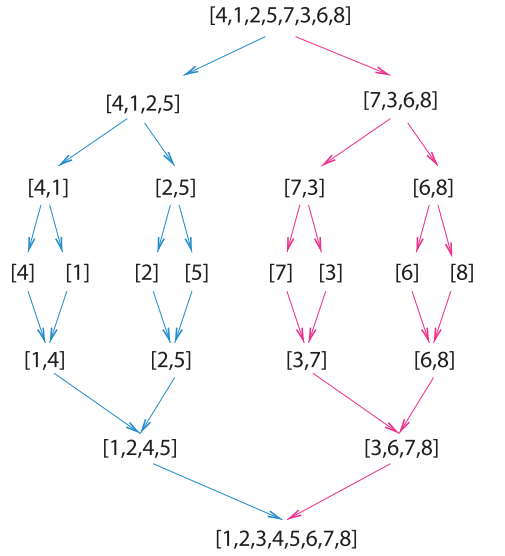


Figura 14. *El algoritmo de ordenamiento en la lista [4, 1, 2, 5, 7, 3, 6, 8].*

Se puede observar el procedimiento completo en la figura 14.

Queremos estimar la cantidad de comparaciones que realiza este algoritmo para ordenar una lista de longitud n. Supondremos que n es una potencia de 2, así al subdividir la lista sucesivamente siempre resultan dos sublistas de tamaño igual a la mitad de la anterior. Llamemos c_k a la cantidad máxima de comparaciones que realiza el algoritmo para ordenar una lista de $n = 2^k$ elementos.

Si $n = 2$, o sea $k = 1$, haciendo una sola comparación podemos ordenar la lista. Entonces $c_1 = 1$.

Si $n = 2^k$, con $k \geq 2$, en el primer paso del algoritmo vamos a partir la lista en dos sublistas de tamaño 2^{k-1}. La cantidad de comparaciones que haremos para ordenar cada una de las dos sublistas es como máximo c_{k-1}. Finalmente, debemos unir las dos listas ordenadas. En cada paso de esta unión se realiza una comparación y se ubica un elemento de alguna de las dos listas en la lista final, con lo que el algoritmo realiza menos de $n = 2^k$ comparaciones. Deducimos entonces, que $c_k < 2c_{k-1} + 2^k$.

Veamos que $c_k < k \cdot 2^k$ para todo $k \in \mathbb{N}$. Podemos probar esta propiedad por inducción:

- Si $k = 1$, vale $c_1 = 1 < 2 = 1 \cdot 2^1$.
- Supongamos que $c_k < k \cdot 2^k$ y acotemos c_{k+1}. Usando la desigualdad que probamos más arriba, junto con esta hipótesis, resulta que:

$$c_{k+1} < 2c_k + 2^{k+1} < 2 \cdot k \cdot 2^k + 2^{k+1} = k \cdot 2^{k+1} + 2^{k+1}$$
$$= (k+1) \cdot 2^{k+1}$$

Deducimos entonces que para ordenar una lista de $n = 2^k$ elementos, el algoritmo realiza menos de $k \cdot 2^k = \log_2(n) \cdot n$ comparaciones.

2. Números enteros

Patricia JANCSA

□ 1. Introducción

Estudiamos los números naturales y vimos que sirven para contar. Sin embargo, hay situaciones que para ser descriptas correctamente requieren de otro tipo de números. Los números enteros negativos se usan en diversos contextos, por ejemplo, para expresar o calcular:

- En geografía, profundidades o diferencias de altura:
  - *la capa más superficial de la estructura de la Tierra, llamada corteza terrestre, llega hasta los -30 km en el fondo oceánico;*
  - *la diferencia de altura que hay desde la cima del Aconcagua, que se halla a 6.959 metros sobre el nivel del mar, hasta el fondo de la laguna del Carbón, en la provincia de Santa Cruz, donde el altímetro marca 105 metros bajo el nivel del mar.* (Figura 1)

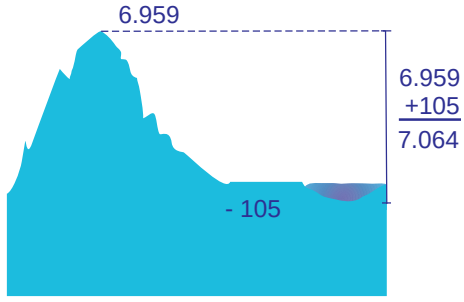


Figura 1.

- Temperaturas bajo cero: *el día más frío del año 2008 en Ushuaia fue el 16 de agosto, con una temperatura mínima de -5°C y una temperatura máxima de 7°C.*
- En contabilidad, los números negativos significan *deudas* y los positivos haberes o activos poseídos.
- Fechas en la antigüedad, años antes de Cristo: *Platón, el más importante filósofo de la antigüedad, fue alumno de Sócrates y maestro de Aristóteles; nació en Grecia en el año 427 a.C. y murió en el año 347 a.C.; por lo tanto, vivió 80 años.*

□ 2. Construcción de los números enteros

Para continuar el estudio de los números, consideremos $\mathbb{N}_0$ el conjunto de los números naturales y el cero, y pensemos en la siguiente situación. En el capítulo anterior, estudiamos operaciones de números naturales y vimos que dos números naturales se pueden sumar y se obtiene como resultado otro número natural; también se pueden multiplicar y el resultado es un número natural. Por ejemplo, $3+5 = 8 \in \mathbb{N}$ y $3 \cdot 5 = 15 \in \mathbb{N}$. Además, si quisiéramos restar uno de otro, por ejemplo, hacer 5 - 3 también se puede dentro del conjunto $\mathbb{N}$, es decir $5 - 3 = 2 \in \mathbb{N}$. Una situación cotidiana que refleja esta situación matemática es la siguiente: si Paula tiene 5 remeras, Lorena le puede pedir prestadas 3 remeras y a Paula todavía le quedan 2. En cambio, si Paula tuviera sólo 3 remeras, Lorena no debería esperar que le preste 5 porque no tiene más de 3.

Es decir, ¿qué ocurre si queremos efectuar la operación de resta en el otro sentido, o sea, 3-5? ¿A 3 se le puede restar 5? Veremos enseguida que, en realidad, sí se puede efectuar esta operación, pero el resultado ya no es un número natural.

Recordemos que la operación suma dentro de $\mathbb{N}_0$ tiene al cero como elemento neutro porque $a + 0 = a$ y $0 + a = a$ para todo número natural a. Pero ningún número natural tiene un **inverso** dentro de $\mathbb{N}_0$, respecto de la suma. La pregunta es qué tipo de números deberíamos agregarle a $\mathbb{N}_0$ para que todo elemento tenga inverso respecto de la operación suma. Es decir, si Paula tuviera 3 remeras, Lorena podría pedirle las 3 remeras (¡por lo menos para probárselas!) y en este caso, Paula no se quedaría con ninguna. Es decir, 3 - 3 = 0, o, mejor dicho, 3 + (-3) = 0 que no es un natural pero sí pertenece a $\mathbb{N}_0$.

En otras palabras, agreguémosle a $\mathbb{N}_0$ todos los "opuestos" de sus elementos, es decir, el -1, el -2, etcétera. Llamaremos al nuevo conjunto que construimos de esta forma *conjunto de los números enteros* y lo denotamos con la letra $\mathbb{Z}$. A partir de la construcción anterior:

$$\mathbb{Z} = \mathbb{N} \cup \{0\} \cup -\mathbb{N}$$

que, en particular, contiene a $\mathbb{N}$ y a $\mathbb{N}_0$. Así, dentro de $\mathbb{Z}$, cualquier $n \in \mathbb{N}$ tiene un inverso, respecto de la suma, que es su opuesto.

Veamos que la pregunta anterior también tiene respuesta dentro de $\mathbb{Z}$. Ahora, podemos realizar la operación "resta" o "diferencia" de cualquier par de enteros, por ejemplo, a 3 - 5 lo calculamos como 3 + (-5) = -2. Es decir, si Paula tuviera tres remeras, le faltarían dos para poder prestarle 5 remeras a su amiga.

Ejemplos

- *¿Qué diferencia de altura hay desde la cima del Aconcagua, que se halla a 6.959 metros sobre el nivel del mar, hasta el fondo de la laguna del Carbón, en la provincia de Santa Cruz, donde el altímetro marca 105 metros bajo el nivel del mar?*

  Para averiguarlo, necesitamos calcular 6.959 - (-105) = 6.959+105 = 7.064 metros.

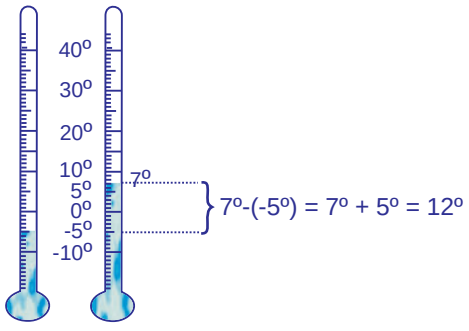


Figura 2. *En grados Celsius.*

- *¿Qué amplitud térmica hubo el 16 de agosto de 2.008 en Ushuaia?* (Figura 2)

  Dado que la temperatura mínima fue de -5°C y la máxima de 7°C, la amplitud térmica fue de 7°C -(-5°C)=12°C.

- *Si tenemos* $1.500 *en el banco, no podemos emitir un cheque por* $1.750*, salvo que el banco nos preste la diferencia, en cuyo caso generaríamos una deuda. Para informarnos de esta situación, el banco nos mandaría una carta donde explicaría que, en este caso, el saldo de nuestra cuenta sería de* $1.500 - $1.750 = -$250*, es decir que le deberíamos* $250 *al banco.*

- *Pitágoras, filósofo y matemático griego, nació aproximadamente en el año 582 a.C. y vivió 75 años; ¿en qué año murió?*

  Si Pitágoras nació en el año 582 a.C., es decir, 582 años antes del año cero, y vivió 75 años, entonces murió 75 años más tarde de su año de nacimiento, es decir que murió en el año:

$$-582 + 75 = -507$$

  La respuesta es que murió aproximadamente en el año 507 a.C.

2.1. Construcción formal de $\mathbb{Z}$

Notemos que un número entero negativo puede ser definido como la diferencia de dos números naturales. Por ejemplo -2 = 3 - 5, de donde puede asociarse el número -2 con el par ordenado (3 , 5). El problema es que (4 , 6), (11 , 13) y otros infinitos pares ordenados también dan como resultado -2 al restar sus componentes. ¿De qué forma podemos definir sin ambigüedad el número -2? Perfeccionemos la idea anterior, teniendo en cuenta a la vez *todos los pares ordenados de números naturales cuya diferencia es* -2. Es decir, dos pares ordenados (m , n) y (m', n') pueden asignarse al mismo número entero si:

$$m - n = m' - n' \quad (*)$$

El inconveniente es que las restas $(*)$ no pueden efectuarse en $\mathbb{N}$ si $m \leq n$. Pero este problema se puede solucionar si nos damos cuenta de que:

$$m - n = m' - n' \text{ es equivalente a } \quad m + n' = m' + n \quad (**)$$

y esta operación es correcta en $\mathbb{N}$, ya que la suma de cualquier par de naturales es un número natural. Entonces, estamos en condiciones de definir en $\mathbb{N} \times \mathbb{N}$ la relación ~ dada por:

$$(m\ ,\ n) \sim (m'\ ,\ n') \quad \text{si y sólo si } m + n' = m' + n$$

No es difícil ver que esta relación es de equivalencia; por lo tanto, produce en $\mathbb{N} \times \mathbb{N}$ una partición en clases de equivalencia, cada una de las cuales puede ser asociada a un único número entero y viceversa. Si denotamos por $[(m\ ,\ n)]$ la clase de equivalencia del par (m , n), para cada par de naturales m y n, resulta, por ejemplo:

$$\begin{aligned}[(3\ ,\ 5)] &\sim [(11\ ,\ 13)] \\ &\sim [(19\ ,\ 21)] \\ &\sim [(1\ ,\ 3)]\end{aligned}$$

Se define entonces m - $n \in \mathbb{Z}$ como cualquier representante de la clase $[(m\ ,\ n)]$. Explícitamente, se define el opuesto de cada número natural n como:

$$-n = [(1\ ,\ n + 1)]$$

Además, el cero puede obtenerse como:

$$0 = [(n\ ,\ n)] \text{ para cualquier } n \in \mathbb{N}.$$

2.2. La suma y la resta de números enteros

Formalmente, podemos definir la suma de dos números enteros a partir de sus clases de equivalencia $[(m\ ,\ n)]$ y $[(m',\ n')]$, con $m, m', n, n' \in \mathbb{N}$:

$$[(m\ ,\ n)] + [(m'\ ,\ n')] = [(m + m'\ ,\ n + n')]$$

Esto se interpreta como:

$$(m - n) + (m' - n') = (m + m') - (n + n')$$

Debemos ver que esta operación está bien definida en clases de equivalencias, esto es, que si $(m_1, n_1) \sim (m_2, n_2)$ y $(m'_1, n'_1) \sim (m'_2, n'_2)$, entonces $(m_1 + m'_1, n_1 + n'_1) \sim (m_2 + m'_2, n_2 + n'_2)$. Ahora, al ser $(m_1, n_1) \sim (m_2, n_2)$ vale que:

$$m_1 + n_2 = m_2 + n_1$$

y análogamente, al ser $(m'_1, n'_1) \sim (m'_2, n'_2)$ vale que:

$$m'_1 + n'_2 = m'_2 + n'_1.$$

lo que claramente implica que:

$$m_1 + m'_1 + n_2 + n'_2 = m_2 + m'_2 + n_1 + n'_1$$

como queríamos ver.

Se define la resta como:

$$[(m\ ,\ n)] - [(m'\ ,\ n')] := [(m + n'\ ,\ n + m')]$$

que interpretamos:

$$\begin{aligned}(m - n) - (m' - n') &= m - n - m' + n' \\ &= m + n' - n - m' \\ &= (m + n') - (n + m').\end{aligned}$$

Esta operación también está bien definida en clases de equivalencia: si $(m_1, n_1) \sim (m_2, n_2)$ y $(m'_1, n'_1) \sim (m'_2, n'_2)$ entonces $(m_1 + n'_1, n_1 + m'_1) \sim (m_2 + n'_2, n_2 + m'_2)$, pues:

$$\begin{aligned}m_1 + n'_1 + n_2 + m'_2 &= (m_1 + n_2) + (n'_1 + m'_2) \\ &= (m_2 + n_1) + (n'_2 + m'_1) \\ &= n_1 + m'_1 + m_2 + n'_2\end{aligned}$$

Veamos cómo resultan estas operaciones en la práctica: ya sabíamos cómo sumar dos números naturales y, en la sección anterior estudiamos que la resta de un natural de otro es un número entero. Por ejemplo, 5 - 3 = 2 y 3 - 5 = -2; podemos pensar esta operación como la suma de dos enteros, cada uno con su signo:

$$\begin{aligned} 3-5 &= 3+(-5) \\ &= -2 \end{aligned}$$

La manera más fácil de efectuar esta operación es la siguiente:

$$\begin{aligned} 3-5 &= -(5-3) \\ &= -2 \end{aligned}$$

En general, para m y $n \in \mathbb{N}$, si $m \geq n$ entonces m - n es la resta usual, y el resultado es un número natural o cero. Si $m < n$, el resultado de la resta m - n es un número entero negativo, y puede calcularse como:

$$m-n = -(n-m)$$

En cualquier caso, podemos pensar la resta de dos números naturales como una suma de dos enteros, cada uno con su signo:

$$m+(-n) = m-n$$

Luego, podemos sumar y restar dos números enteros de la siguiente manera:

- si m y $n \in \mathbb{Z}$ son positivos, entonces $m + n$ es la suma usual de números naturales, y m - n está definida arriba;
- si uno es positivo y otro negativo, digamos $m > 0$ y $-n < 0$, con $n \in \mathbb{N}$, entonces su suma es

$$m+(-n) = m-n \in \mathbb{Z}$$

y su resta o diferencia es:

$$m-(-n) = m+n \in \mathbb{N} \subset \mathbb{Z}, \qquad (-n)-m = -(n+m) \in \mathbb{Z}$$

- si ambos son negativos, digamos $-m$ y $-n$ con m y $n \in \mathbb{N}$, su suma es:

$$(-m)+(-n) = -m-n = -(m+n) \in \mathbb{Z}$$

y su diferencia es:

$$(-m)-(-n) = -m+n = n-m \in \mathbb{Z}$$

- si alguno de los dos es cero y $m \in \mathbb{Z}$, entonces:

$$m+0 = m, \quad m-0 = m \quad \text{y} \quad 0-m = -m$$

Por lo tanto, en el conjunto de los enteros se puede sumar y restar sin salir de él.

Es decir que, si $a, b \in \mathbb{Z}$ entonces $a + b$ y $a - b \in \mathbb{Z}$.

Ejemplo. ¿Qué número hay que sumarle a 16 para obtener 5?

Solución. Buscamos $n \in \mathbb{Z}$ tal que $16 + n = 5$

Si sumamos -16 a cada miembro obtenemos:

$$(*)\ 16 + n + (-16) = 5 + (-16) \iff n = -11$$

Por lo tanto, el número buscado es -11. En efecto, si reemplazamos a *n* por -11 en la igualdad inicial, obtenemos:

$$\begin{aligned} 16 + (-11) &= 16 - 11 \\ &= 5 \end{aligned}$$

como queríamos.

Notación. En $(*)$ usamos el símbolo "$\iff$" para indicar que la igualdad que está a la izquierda es equivalente a la de la derecha; es decir, que la validez de la igualdad de la izquierda implica la validez de la igualdad de la derecha y, recíprocamente, la validez de la igualdad de la derecha implica la validez de la igualdad de la izquierda.

2.3. Valor absoluto

¿Qué tienen en común los enteros 5 y -5? Sabemos que uno es el opuesto del otro; esto significa que 5 y -5 **están a la misma distancia del cero**, exactamente a una distancia igual a 5 unidades. La distancia de un número cualquiera al cero se llama el *valor absoluto* del número.

En consecuencia, el hecho anterior se expresa diciendo que el *valor absoluto* de 5 y el de -5 son ambos iguales a 5. En otras palabras, enteros opuestos tienen el mismo *valor absoluto*. En símbolos, el valor absoluto de un número *n* cualquiera se expresa de manera abreviada usando barras verticales en la forma $|n|$. La manera correcta de definirlo en general es:

$$|n| = \begin{cases} n & \text{si } n \geq 0 \\ -n & \text{si } n < 0 \end{cases}$$

Por ejemplo, |5| = 5 y, de acuerdo a la definición, también | - 5| = -(-5) = 5.

2.4. La multiplicación

El ingrediente nuevo que aparece al multiplicar números enteros es el signo: ¿cómo calculamos 3 · (-2)?

Así como para los números naturales el producto 3 · 2 significa *sumar dos veces* 3, que es 3 + 3 = 6, el producto 3 · (-2) significa *restar dos veces* 3, o sea:

$$\begin{aligned} 3 \cdot (-2) &= -3 - 3 \\ &= -6 \end{aligned}$$

De aquí surge la regla para multiplicar un número positivo por otro negativo: el resultado es un número negativo.

¿Cómo calculamos (-3) · (-2)? En este caso, debemos *restar dos veces* -3, o sea:

$$\begin{aligned}(-3)\cdot(-2) &= -(-3)-(-3)\\ &= +6\end{aligned}$$

De esta manera se deduce que el producto de dos números negativos es un número positivo.

Regla de los signos. Para multiplicar "números con signo" hay que respetar las siguientes reglas:

- (+) · (+) = +
- (+) · (-) = -
- (-) · (-) = +

Ejemplos

- (-2) · 3 = -(2 · 3) = -6.
- (-2) · (-3) = +(2 · 3) = 6.
- -[(-1) · (-2)] = -[1 · 2] = -2.

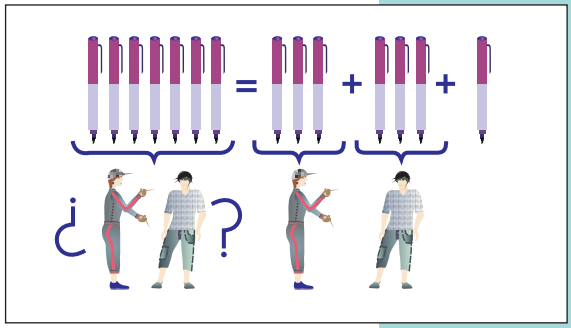
Observación. Sean b y $c \in \mathbb{Z}$ tales que $b \cdot c = 1$. Entonces $b = c = 1$ o $b = c = -1$.

En efecto, si $b \cdot c = 1$, entonces b y c son ambos positivos o ambos negativos. Si b y c son ambos positivos y ocurriera, por ejemplo, $b > 1$ entonces $b \cdot c$, que es igual a "b veces c", sería más grande que c, es decir que $b \cdot c > c \geq 1$; por lo tanto, tanto b como c deben ser 1.

Si b y c son ambos negativos, entonces $-b$ y $-c$ son positivos, y podemos usarlos para escribir el producto en la forma $b \cdot c = (-b) \cdot (-c)$ que sabemos que es igual a 1; por lo tanto, de nuevo $-b$ y $-c$ deben ser 1, o sea que b y c son iguales a -1.

□ 3. Divisibilidad y algoritmo de división

Imaginemos que tenemos una tableta de chocolate de **seis cuadraditos** que dos amigos quieren compartir por igual. Esta operación puede realizarse convenientemente, y a cada uno le tocan tres de las seis partes que tiene la tableta.



Ahora, imaginemos que tenemos 7 lapiceras que queremos repartir entre los dos amigos. Es claro que, para que a cada amigo le toque la misma cantidad, podemos darle tres lapiceras a cada uno pero *sobra una lapicera*, es decir, *la lapicera sobrante no puede partirse*.

La división es la operación que permite averiguar cuántas veces un número, el divisor, está contenido en otro número, el dividendo. Por ejemplo, el 2 está 3 veces en el 6, porque $3 \cdot 2 = 6$, entonces 6 *dividido* 2 *es igual a* 3. En este sentido, la división es la operación inversa de la multiplicación.

Se denomina *cociente* al resultado entero de la división. Si la división no es exacta, es decir, el divisor no está contenido un número exacto de veces en el dividendo, la operación tendrá un *resto*. En el caso de las lapiceras, se divide 7 por 2 y se obtiene un cociente de 3 unidades y un resto de 1 unidad, que también puede expresarse como:

Dividendo	=	**Cociente**	·	**Divisor**	+	**Resto**
7	=	3	·	2	+	1

Para obtener el cociente y el resto de efectuar la división de un número entero por otro, se efectúa el procedimiento conocido como **algoritmo de división**, que explicaremos más adelante.

3.1. Divisibilidad

Si $a, b \in \mathbb{Z}$ decimos que *a divide* a *b* si existe $q \in \mathbb{Z}$ tal que $b = q \cdot a$, donde q es el cociente de la división de b por a.

Para expresar simbólicamente este hecho, se escribe $a \mid b$. También se dice que *b es divisible por a,* o que *a es un divisor de b*.

Por ejemplo, 2 divide a 2 (en efecto, $2 = 1 \cdot 2$); 2 también divide a 4, a 6, a 8, a 20, y a todos los números pares. Justamente, un número es **par** si es divisible por 2.

Ejercicio 2.1. ¿Cómo podríamos describir a todos los números impares?

Observación. Propiedades de la noción de **divisibilidad**:

1. Para cada $n \in \mathbb{Z}$, $1 \mid n$, $n \mid n$, $-1 \mid n$ y $-n \mid n$.

   En efecto, $1 \mid n$ porque $n = 1 \cdot n$, es decir, en la división de n por 1, el cociente es n y la división es exacta. Por otra parte, en la división de n por el mismo n, el cociente es 1 y la división es exacta. Notemos, además, que $-1 \mid n$ y $-n \mid n$ porque $n = (-n) \cdot (-1)$.

2. Si $a, b \in \mathbb{Z}$, $a \mid b$ y $b \neq 0$ entonces $|a| \leq |b|$.
3. Si $a \mid b$ y $b \mid a$ entonces $|a| = |b|$.
4. Si $a \mid b$ y $b \mid c$ entonces $a \mid c$.

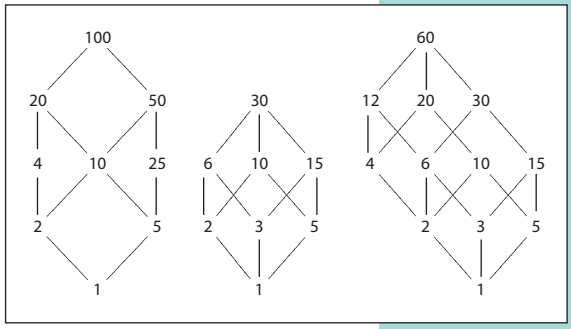
   En efecto, si $a \mid b$ existe $q \in \mathbb{Z}$ tal que $b = q \cdot a$. Si además $b \mid c$, existe $q' \in \mathbb{Z}$ tal que $c = q' \cdot b$. Entonces $c = q' \cdot (q \cdot a) = (q' \cdot q) \cdot a$.

5. Si $a \mid b$ y $a \mid c$ entonces $a \mid (h \cdot b + k \cdot c)$ para cualesquiera $h, k \in \mathbb{Z}$.

En efecto, si $a \mid b$ y $a \mid c$ existen enteros q_1 y q_2 tales que $b = q_1 \cdot a$ y $c = q_2 \cdot a$; entonces $h \cdot b + k \cdot c = h \cdot q_1 \cdot a + k \cdot q_2 \cdot a = (h \cdot q_1 + k \cdot q_2) \cdot a$.

El 1 tiene exactamente dos divisores, que son 1 y -1. Los demás enteros n distintos de 0, de 1 y de -1 tienen **por lo menos cuatro divisores**, que son el 1, el -1, el mismo n, y su opuesto $-n$, pueden tener más divisores. Un entero se dice *primo* si tiene exactamente cuatro divisores distintos. Los divisores de 6 son 1, 2, 3, 6 y sus opuestos, -1, -2, -3 y -6; es decir que 6 tiene ocho divisores en total (6 no tiene más divisores porque si $a \mid 6$ entonces $|a| \leq |6| = 6$). En particular, 6 no es primo. En cambio, los únicos divisores de 7 son 1, 7 y sus opuestos, -1 y -7; por lo tanto, 7 es primo.

Los divisores positivos de 100 son todos los números que aparecen en el primero de los diagramas siguientes. Para cada natural que aparece en el diagrama, sus divisores positivos son todos los que aparecen debajo de él, unidos a éste por un camino formado por una o más líneas. Los otros dos diagramas tienen, de la misma manera, los divisores de 30 y 60.



Notación. El símbolo "$\Rightarrow$" que utilizaremos en lo sucesivo indica que toda vez que vale el enunciado de la izquierda, como consecuencia vale el de la derecha. Es decir, que el enunciado de la izquierda implica el enunciado de la derecha.

Ejemplo. Determinar todos los $n \in \mathbb{Z}$ tales que $2 \cdot n - 1$ divide a $n^2 + 7$.

Solución: Supongamos que $n \in \mathbb{Z}$ es tal que $2 \cdot n - 1$ divide a $n^2 + 7$, en símbolos escribimos $(2 \cdot n - 1) \mid (n^2 + 7)$, entonces divide también a cualquier múltiplo de él, por ejemplo:

$$(2 \cdot n - 1) \mid 2 \cdot (n^2 + 7) = 2 \cdot n^2 + 14$$

Por otra parte, es claro que:

$$(2 \cdot n - 1) \mid n \cdot (2 \cdot n - 1) = 2 \cdot n^2 - n$$

Ahora usamos la propiedad 5, que implica que $a \mid b$ y $a \mid c \Rightarrow a \mid (b - c)$, entonces:

$$(2 \cdot n - 1) \mid [2 \cdot n^2 + 14 - (2 \cdot n^2 - n)] \Longrightarrow (2 \cdot n - 1) \mid (14 + n)$$

Por lo tanto, si $n \in \mathbb{Z}$ es tal que $2 \cdot n - 1$ divide a $n^2 + 7$ entonces $2 \cdot n - 1$ divide a $14 + n$. Nuevamente, en particular:

$$(2 \cdot n - 1) \mid 2 \cdot (14 + n) = 28 + 2 \cdot n$$

$$(2 \cdot n - 1) \mid (2 \cdot n - 1)$$

y entonces $2 \cdot n - 1$ divide a la diferencia de los dos, es decir, divide a $28 + 2 \cdot n - (2 \cdot n - 1) = 29$. Por lo tanto, si $n \in \mathbb{Z}$ es tal que $2 \cdot n - 1$ divide a $n^2 + 7$, entonces $2 \cdot n - 1$ divide a 29.

Si pensamos un momento en el número 29, nos damos cuenta de que el conjunto de todos sus divisores es:

$$\mathcal{D}_{29} = \{1,\ -1,\ 29,\ -29\}$$

(En general, si n es un entero no nulo, llamamos $\mathcal{D}_n$ al conjunto de divisores de n, que sabemos que es finito por la segunda propiedad.)

En consecuencia, $2 \cdot n - 1$ no puede ser otro número más que alguno de los elementos del conjunto anterior. Analicemos caso por caso todas las posibilidades:

- Si $2 \cdot n - 1 = 1$, entonces $n = 1 \Rightarrow n^2 + 7 = 8$ y es cierto que $1 \mid 8$.
- Si $2 \cdot n - 1 = -1$, entonces $n = 0 \Rightarrow n^2 + 7 = 7$ y es cierto que $-1 \mid 7$.
- Si $2 \cdot n - 1 = 29$, entonces $n = 15 \Rightarrow n^2 + 7 = 232$ y es cierto que $29 \mid 232$ porque $232 = 29 \cdot 8$.
- Si $2 \cdot n - 1 = -29$, entonces $n = -14 \Rightarrow n^2 + 7 = 203$ y es cierto que $-29 \mid 203$ porque $203 = -29 \cdot (-7)$.

Por lo tanto, las soluciones al problema son los elementos del conjunto:

$$\{1,\ 0,\ 15,\ -14\}$$

3.2. Algoritmo de división

Si el divisor no está contenido un número exacto de veces en el dividendo, la operación tiene un **resto**, como en el ejemplo al comienzo de esta sección, en el que se reparten siete lapiceras entre dos personas. Este **resto debe ser menor que el divisor.** Para efectuar la división de un número natural por otro y obtener la expresión

$$\textbf{Dividendo} = \textbf{Cociente} \cdot \textbf{Divisor} + \textbf{Resto}$$

el procedimiento es el que aprendimos en la escuela primaria. Recordemos que se escribe el dividendo a la izquierda y el divisor a la derecha, contenido en dos caras adyacentes de un rectángulo abierto a la derecha: si, por ejemplo, consideramos la división de 4.712, el dividendo, por 23, el divisor, el proceso empieza así:

$$4.712 \quad \big|23$$

y continúa como hacíamos en la escuela.

El resultado es el siguiente: 4.712 dividido 23 da un cociente de 204 y un resto de 20, que verificamos así:

$$204 \cdot 23 + 20 = 4.712$$

Algoritmo de división para números enteros: consideraciones de signo. ¿Qué pasa si queremos dividir por un número negativo? Por ejemplo, si nos interesa calcular 4.712 dividido -23, utilicemos el cálculo anterior en el cual **dividendo y divisor eran ambos positivos** y obtengamos la expresión para este caso. En efecto, **multipliquemos dos veces por -1 el primer término** de la igualdad (notar que esta operación no altera el resultado); luego usemos convenientemente la conmutatividad y la asociatividad del producto:

$$\begin{aligned} 4.712 &= 204 \cdot 23 + 20 \\ &= [(-1) \cdot (-1) \cdot (204 \cdot 23)] + 20 \\ &= [(-1) \cdot 204 \cdot (-1) \cdot 23] + 20 \\ &= (-204) \cdot (-23) + 20. \end{aligned}$$

Por lo tanto, en la división de 4.712 por -23 el cociente es -204 y el resto es 20.

El algoritmo de división exige que el resto sea siempre no negativo, es decir, positivo o cero.

Por ejemplo, si nos interesa calcular -4.712 dividido 23 **multiplicamos toda la expresión anterior por** -1**:**

$$\begin{aligned} -4.712 &= -(204 \cdot 23 + 20) \\ &= -204 \cdot 23 - 20 \end{aligned}$$

que es correcto, pero no cumple con la condición de que el resto sea positivo o cero. Para solucionar este problema, lo que hacemos es **sumar y restar 23, y luego conmutar y asociar convenientemente** para obtener:

$$\begin{aligned} -4.712 = -204 \cdot 23 - 20 + 23 - 23 &= (-204 \cdot 23 - 23) + (-20 + 23) \\ &= (-205) \cdot 23 + 3 \end{aligned}$$

que dice que en la división de -4.712 por 23 el cociente es -205 y el resto es 3.

Finalmente, el caso que falta considerar es el de dividir un número negativo por otro negativo, por ejemplo, -4.712 dividido -23; para ello, empezamos como antes **multiplicando toda la expresión inicial por** -1:

$$\begin{aligned} -4.712 &= -(204 \cdot 23 + 20) \\ &= 204 \cdot (-23) - 20 \end{aligned}$$

y de nuevo necesitamos **sumar y restar** 23 para obtener un resto no negativo:

$$\begin{aligned} -4.712 = 204 \cdot (-23) - 20 &= 204 \cdot (-23) - 23 + 23 - 20 \\ &= 205 \cdot (-23) + 3 \end{aligned}$$

que dice que en la división de -4.712 por -23 el cociente es 205 y el resto es 3.

Dados los enteros n y d, con $d \neq 0$, el algoritmo de división es el procedimiento que permite escribir de manera única

$$n = q \cdot d + r$$

donde $0 \leq r < |d|$. Los números q y r se dicen el cociente y el resto, respectivamente, de la división de n por d.

Notar que si $n = 0$, el algoritmo de división vale con $q = 0 = r$; en efecto, $0 = 0 \cdot d + 0$ cualquiera sea d no nulo.

Este enunciado se demuestra a continuación:

Teorema 2.1. *Sean $n, d \in \mathbb{Z}$ y $d \neq 0$, entonces existen $q, r \in \mathbb{Z}$ tales que $n = q \cdot d + r$ y $0 \leq r < |d|$; además, q y r son únicos con esta propiedad.*

Demostración. ***Caso d > 0.*** Para cada par $n, d \in \mathbb{Z}$ con $d > 0$, definamos el conjunto de los *candidatos a resto en la división de n por d*:

$$R = \{r \in \mathbb{N}_0 : \ r = n - q \cdot d, \ \text{para algún } q \in \mathbb{Z}\}$$

Entonces $R \neq \emptyset$; en efecto, mostremos un elemento en el conjunto: sea $r_1 = n - (-d \cdot |n|) \cdot d$, y veamos que $r_1 \in R$. Si $n = 0$ entonces $r_1 = 0 \in R$. Si $n > 0$, tenemos que r_1 se puede escribir como producto de dos factores positivos:

$$\begin{aligned} r_1 &= n - (-d \cdot |n|) \cdot d \\ &= n + d^2 \cdot n \\ &= n \cdot (1 + d^2) > 0 \end{aligned}$$

y si $n < 0$ entonces $|n| = -n$ y obtenemos que r_1 es el producto de dos factores negativos o cero:

$$\begin{aligned} r_1 &= n - (-d \cdot |n|) \cdot d \\ &= n - (-d \cdot (-\ n)) \cdot d \\ &= n - (d \cdot \ n\ ) \cdot d \\ &= n - \ d^2 \cdot \ n \\ &= n \cdot (\ 1 - d^2\ ) \geq 0 \end{aligned}$$

donde n es negativo y el segundo factor es negativo o cero, dado que:

$$d \geq 1 \Longrightarrow d^2 \geq d \geq 1 \Longrightarrow d^2 - 1 \geq 0$$

Por lo tanto, cualesquiera sean $n, d \in \mathbb{Z}$, $d > 0$, R es un subconjunto no vacío de $\mathbb{N}_0$; entonces R tiene primer elemento. Denotemos por r_0 al primer elemento de R, que, como todos los elementos de R, es de la forma $r_0 = n - q_0 \cdot d$ para algún $q_0 \in \mathbb{Z}$; es decir, *existe un q_0 en $\mathbb{Z}$ tal que el primer elemento de R se escribe como $r_0 = n - q_0 \cdot d$*; además, $r_0 \geq 0$ por pertenecer a R.

Afirmamos que $r_0 < d$; en efecto, si ocurriera que $r_0 \geq d$ entonces $r_0 - d \geq 0$; por otra parte:

$$r_0 - d = (n - q_0 \cdot d) - d = n - (q_0 + 1) \cdot d$$

que implicaría que $r_0 - d \in R$, pero $r_0 - d < r_0$ y esto contradice el hecho de que r_0 sea el primer elemento de R. Por lo tanto, necesariamente $0 \leq r_0 < d$.

Así, hemos probado que existen q_0 y r_0 en $\mathbb{Z}$ tales que $n = q_0 \cdot d + r_0$ satisfaciendo la condición $0 \leq r_0 < d$. Esto concluye la prueba de la existencia de enteros q y r con las propiedades del enunciado.

Ahora, comprobemos que q y r son únicos satisfaciendo estas propiedades. Supongamos, por el contrario, que existen q y r y también q' y r' tales que:

$$\begin{aligned} n &= q \cdot d + r \quad 0 \leq r < d \\ n &= q' \cdot d + r' \quad 0 \leq r' < d \end{aligned}$$

Sin pérdida de generalidad, podemos suponer que alguno de los dos restos es el más grande, por ejemplo, $r' \leq r$; entonces,

$$0 \leq r - r' < d$$

Luego, restando miembro a miembro una igualdad de la otra, obtenemos:

$$0 = (q - q') \cdot d + (r - r')$$

que es equivalente a:

$$\begin{aligned} r - r' &= -(q - q') \cdot d \\ &= (q' - q) \cdot d \end{aligned}$$

Dado que $0 \leq r - r'$ y $d > 0$ obtenemos que $q' - q \geq 0$. Si $q' - q = 0$, entonces también $r - r' = 0$ y, necesariamente, $q' = q$ y $r' = r$. Si $q' - q > 0$, entonces $q' - q \geq 1$ porque es un entero; esto implica que $(q' - q) \cdot d \geq d$, pero el lado izquierdo de esta desigualdad es igual a $r - r'$ que sabíamos que era menor que d. Llegamos a una contradicción por haber supuesto que $q' \neq q$. Por lo tanto, debe ser $q' = q$ y $r' = r$.

Caso d < 0. Le aplicamos el caso anterior a $n \in \mathbb{Z}$ cualquiera y $-d > 0$; luego existen $q, r \in \mathbb{Z}$ tales que:

$$n = q \cdot (-d) + r, \quad 0 \leq r < (-d)$$

Notar que $|d| = -d$ pues $d < 0$, entonces la desigualdad anterior dice que $0 \leq r < |d|$. A la vez, podemos reescribir la igualdad anterior como:

$$\begin{aligned} n &= q \cdot (-d) + r \\ &= (-q) \cdot d + r, \quad 0 \leq r < |d| \end{aligned}$$

Por lo tanto, el cociente de la división de n por d es $-q \in \mathbb{Z}$ y el resto es r, que satisface $0 \leq r < |d|$ como acabamos de ver. La unicidad de q y r con estas propiedades se demuestra de manera análoga al caso $d > 0$ reemplazando d por $|d|$.

Algoritmo de división para calcular (q, r) donde q es el cociente y r es el resto de la división de n por $d \neq 0$.

- Si n ≥ 0 y d > 0:
  - tomar q = 0, r = n;
  - mientras que r ≥ d, reemplazar
    q ← q + 1,
    r ← r - d
  - dar como respuesta (q, r).

- Si n ≥ 0 y d < 0 aplicar el algoritmo a n y -d y dar como respuesta (-q, r).

- Si n < 0 y d > 0:
  - aplicar el algoritmo a -n y d;
  - si r = 0, dar como respuesta (-q, 0);
  - si no, dar como respuesta (-q - 1, d - r).

- Si n < 0 y d < 0:
  - aplicar el algoritmo a -n y -d;
  - si r = 0, dar como respuesta (q, 0);
  - si no, dar como respuesta (q + 1,-r - d).

□ 4. Desarrollos en base *b*

Para escribir los números, normalmente, usamos el *desarrollo decimal o desarrollo en base* 10, que se obtiene a partir del conjunto de los diez símbolos:

$$\{0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9\}$$

Pero, a veces es útil conocer desarrollos en distintas bases de un número natural. Por ejemplo, las computadoras utilizan el *sistema binario* en el cual cualquier natural se expresa como una secuencia de unos y ceros.

En base 10, los números naturales se escriben como 1, 2, 3, 4, 5, 6, 7, 8, 9; para escribir el siguiente natural, el diez, se vuelve a empezar con el cero, pero anteponiendo un 1, o sea que el diez se expresa como 10, que es como lo conocemos.

De este modo, agotados los 10 símbolos empiezan los números de dos cifras. A partir del 9, los 10 siguientes naturales empiezan todos con un 1, es decir que hay 10 números que tienen al 1 en la cifra de las decenas; las unidades van siempre de 0 a 9; el veinte, que es el siguiente al 19, se obtiene sumando una unidad a la cifra 1 de las decenas, que entonces se convierte en un 2, y reemplazando el 9 de las unidades por un cero, es decir, 20; y así sucesivamente.

Notar que, como consecuencia, todo natural se expresa como una suma de múltiplos de potencias de 10. Por ejemplo, el número 5.607 es:

$$\begin{aligned} 5.607 &= 7 + 0 \cdot 10 + 6 \cdot 100 + 5 \cdot 1.000 \\ &= 7 + 0 \cdot 10 + 6 \cdot 10^2 + 5 \cdot 10^3 \end{aligned}$$

Si en lugar de usar diez símbolos, usamos solamente siete, 0, 1, 2, 3, 4, 5 y 6, obtenemos el *desarrollo en base* 7 de los naturales y el cero como secuencias de estos símbolos. En particular, el número siete se escribe en base 7 como un 10 porque es el siguiente al número seis que es el último de los siete símbolos a disposición:

$$(7)_{10} = (10)_7$$

El subíndice a la derecha indica la base en la cual está escrito el número entre paréntesis. Así, $(8)_{10} = (11)_7$; $(9)_{10} = (12)_7$; $(10)_{10} = (13)_7$; $(11)_{10} = (14)_7$; etcétera.

Entonces, el cero y los primeros naturales se escriben en base 7 así:

$$\{(0)_7, (1)_7, (2)_7, (3)_7, (4)_7, (5)_7, (6)_7, (10)_7, (11)_7, (12)_7, (13)_7, (14)_7, (15)_7,$$
$$(16)_7, (20)_7, (21)_7, (22)_7, (23)_7, (24)_7, (25)_7, (26)_7, (30)_7, (31)_7, (32)_7,$$
$$(33)_7, (34)_7, (35)_7, (36)_7, (40)_7, (41)_7, \ldots\}$$

Para obtener el desarrollo en base *b* de un número *n* expresado en el sistema decimal, aplicamos el algoritmo de división. El procedimiento consiste en dividir *n* sucesivamente por *b*.

Por ejemplo, para calcular el desarrollo en base 7 de 639, dividimos 639 por 7 y escribimos:

$$639 = 91 \cdot 7 + 2, \quad q_0 = 91, \ r_0 = 2$$

A continuación, dividimos a 91, el cociente de la división anterior, por 7; entonces:

$$91 = 13 \cdot 7 + 0, \quad q_1 = 13, \ r_1 = 0$$

Así siguiendo, dividimos por 7 los sucesivos cocientes; cuando se obtiene un cociente igual a cero, el proceso termina:

$$\begin{aligned} 13 &= 1 \cdot 7 + 6, \quad q_2 = 1, \ r_2 = 6 \\ 1 &= 0 \cdot 7 + 1, \quad q_3 = 0, \ r_3 = 1 \end{aligned}$$

Luego,

$$\begin{aligned} 639 &= 91 \cdot 7 + 2 \\ &= (13 \cdot 7 + 0) \cdot 7 + 2 \\ &= 13 \cdot 7^2 + 0 \cdot 7 + 2 \\ &= (1 \cdot 7 + 6) \cdot 7^2 + 0 \cdot 7 + 2 \\ &= 1 \cdot 7^3 + 6 \cdot 7^2 + 0 \cdot 7 + 2 \end{aligned}$$

Los coeficientes del desarrollo en base 7 son los sucesivos restos:

$$\begin{aligned} 639 &= (r_3 r_2 r_1 r_0)_7 \\ &= (1.602)_7 \end{aligned}$$

Recíprocamente, si queremos recuperar el 639 de su escritura en base 7, desarrollamos la suma de las potencias de 7 de acuerdo a la expresión del número:

$$(r_3 r_2 r_1 r_0)_7 = r_3 \cdot 7^3 + r_2 \cdot 7^2 + r_1 \cdot 7 + r_0$$

En el ejemplo anterior:

$$\begin{aligned} (1.602)_7 &= 1 \cdot 7^3 + 6 \cdot 7^2 + 0 \cdot 7 + 2 \cdot 7^0 \\ &= 343 + 6 \cdot 49 + 2 \\ &= 343 + 294 + 2 \\ &= 639 \end{aligned}$$

Para estudiar el *desarrollo binario o en base* 2, procedemos igual tomando el 2 como base. Por ejemplo: ¿cómo se expresa el 27 en base 2? Como antes, si aplicamos el algoritmo de división de 27 por 2, obtenemos 27 = 13 · 2 + 1. A continuación, dividimos el cociente, 13, por 2, y así se sigue:

$$\begin{aligned} 27 &= 13 \cdot 2 + 1, \quad q_0 = 13, \quad r_0 = 1 \\ 13 &= 6 \cdot 2 + 1, \quad q_1 = 6, \quad r_1 = 1 \\ 6 &= 3 \cdot 2 + 0, \quad q_2 = 3, \quad r_2 = 0 \\ 3 &= 1 \cdot 2 + 1, \quad q_3 = 1, \quad r_3 = 1 \\ 1 &= 0 \cdot 2 + 1, \quad q_4 = 0, \quad r_4 = 1 \end{aligned}$$

Luego 27 = $(11011)_2$. Recíprocamente, si queremos recuperar el 27 de su escritura en base 2, desarrollamos la suma de las potencias de 2 de acuerdo a la expresión del número:

$$(11011)_2 = 1 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1$$

$$(11011)_2 = 16 + 8 + 2 + 1$$
$$= 27$$

Algoritmo para calcular el desarrollo en base b de un número natural n.

- Comenzar con m = n, s = $(\ )_b$.
- Mientras que m ≠ 0:
  - hallar el cociente q y el resto r de la division de m por b;
  - agregar r como la cifra de más a la izquierda en s;
  - reemplazar m ← q.
- Dar como respuesta s.

Además de bases b donde b es un número de 2 a 10, en distintas situaciones de la ciencia y de la vida cotidiana se utilizan otras bases. ¡Veamos qué interesantes son los siguientes ejemplos!

Ejemplo. En ciencias de la computación se utiliza, además del sistema binario, el *sistema hexadecimal o en base* 16, que permite expresar cualquier número natural a partir de los siguientes símbolos:

$$\{0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ A,\ B,\ C,\ D,\ E,\ F\}$$

En esta base, el símbolo A significa el número 10 en base diez, o sea:

$$(A)_{16} = (10)_{10}$$

Análogamente:

$$(B)_{16} = (11)_{10},\ (C)_{16} = (12)_{10},\ (D)_{16} = (13)_{10},\ (E)_{16} = (14)_{10},\ (F)_{16} = (15)_{10}$$

Para escribir el 16 en base 16, necesitamos dos símbolos, es decir:

$$(16)_{10} = (10)_{16}$$

A partir de este número, se tienen en total 16^2 números de dos dígitos o símbolos, lo que es muy económico en términos computacionales; esto justifica que el sistema hexadecimal sea muy utilizado en informática. En efecto, en computación se utiliza frecuentemente el byte como unidad de memoria; un byte representa 2^8 valores posibles, y este número se escribe en base 16 como $(100)_{16}$ pues:

$$2^8 = 2^4 \cdot 2^4 = 16 \cdot 16 = 1 \cdot 16^2 + 0 \cdot 16^1 + 0 \cdot 16^0 = (100)_{16}$$

Una unidad menos es $2^8 - 1 = (FF)_{16}$ que es el mayor número que puede representarse con solamente dos símbolos en base 16; por lo tanto dos dígitos hexadecimales corresponden exactamente a un byte.

Ejercicio 2.2. Comprobar que $(59792018174)_{10} = (\text{DEBE1CAFE})_{16}$

Ejemplo. La hora se expresa en horas, minutos y segundos, que en realidad sigue el esquema de numeración en base 60, conocida como *base sexagesimal*. En efecto, una hora tiene 60 minutos y un minuto tiene 60 segundos.

Para una duración desde 0 hasta 59 segundos, se utilizan los números naturales habituales. Pero ¿cómo se expresan duraciones de tiempo más largas? Por ejemplo, en lugar de decir

que un nadador olímpico completó la trayectoria de la prueba en 97 segundos, se dice que la recorrió en 1 minuto y 37 segundos, y se escribe 00:01:37.

Si observamos alguna vez un cronómetro o un reloj digital que expresa la hora en horas, minutos y segundos, veremos que pasa de 00:00:59 a 00:01:00, que significa una unidad de 60 segundos, o sea, 1 minuto. Si un reloj así marca 10:38:09, entendemos que son las diez de la mañana, treinta y ocho minutos y nueve segundos.

Si quisiéramos convertir esta expresión a un número en base diez, cuyo significado es el tiempo transcurrido desde las cero horas, medido en segundos, calculamos:

$$10:38:09 = 10 \cdot 60^2 + 38 \cdot 60 + 9 = 38.289 \text{ segundos}$$

Ejemplo. Veamos otro ejemplo en base sexagesimal. Conocemos en geometría el uso del número sesenta como base para la medición de ángulos. Cada ángulo puede describirse en grados, minutos y segundos. Un grado equivale a 60 minutos y un minuto a 60 segundos.

□ 5. Máximo común divisor

Además de poder averiguar todos los divisores de un número, a veces es importante conocer los divisores comunes de dos enteros para contestar la pregunta, ¿cuánto vale el divisor más grande de ambos?

Por ejemplo, los divisores *positivos* de 54 forman el conjunto:

$$\mathcal{D}_{54} = \{1,\ 2,\ 3,\ 6,\ 9,\ 18,\ 27,\ 54\ \}$$

Por otra parte, los divisores *positivos* de 60 son:

$$\mathcal{D}_{60} = \{1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 10,\ 12,\ 15,\ 20,\ 30,\ 60\ \}$$

Notemos que los naturales 1, 2, 3 y 6 están en ambos conjuntos, es decir, que son *divisores comunes de* 54 *y* 60, de los cuales el máximo es el 6. En otras palabras, 6 es el *máximo común divisor de* 54 *y* 60; lo denotamos así:

$$mcd\,(54\ ,\ 60) = 6 \text{ ó también } (54 : 60) = 6.$$

Precisemos la definición usando el concepto de divisibilidad:

Dados a y b en $\mathbb{Z}$, ambos distintos de cero, *el máximo común divisor* de a y b es un número natural d que verifica:

1) $d \mid a$ y $d \mid b$.
2) Si $c \in \mathbb{Z}$ es cualquier otro entero tal que $c \mid a$ y $c \mid b$, entonces $c \mid d$.

La primera condición de la definición exige que *d* sea divisor de *a* y de *b*; la segunda, que sea el máximo entre todos los divisores comunes de *a* y *b*, ya que cualquier otro divisor común *c* divide a *d*.

Además, por definición, el máximo común divisor es positivo, aún si *a* y *b* no lo son. Por ejemplo, el máximo común divisor entre -54 y 60 es *d* = 6; más aún:

$$\begin{aligned} 6 &= mcd\,(54\ ,\ 60) \\ &= mcd\,(-54\ ,\ 60) \\ &= mcd\,(54\ ,\ -60) \\ &= mcd\,(-54\ ,\ -60) \end{aligned}$$

Una forma de calcular el máximo común divisor entre dos números es, como acabamos de ver, determinar todos los divisores de cada uno de los números y entre los divisores de ambos, tomar el máximo. Pero hay un procedimiento, llamado **algoritmo de Euclides**[3], debido al matemático griego homónimo, que es mucho más corto, se aplica a los valores absolutos de los enteros dados y se realiza del siguiente modo:

1) dividir el mayor de los dos números dados por el otro; en nuestro ejemplo, efectuamos *60 dividido 54* y obtenemos, por el algoritmo de división:

$$60 = 1 \cdot 54 + 6$$

2) dividir al segundo número por el resto anterior, o sea, *dividimos 54 por 6 y* obtenemos:

$$54 = 9 \cdot 6 + 0$$

3) el paso siguiente sería tomar el resto de la división anterior y dividirlo por el resto de ésta, y así sucesivamente hasta obtener resto 0. El **máximo común divisor es el último resto no nulo**.

En el ejemplo, el resto que obtuvimos en el paso anterior es cero y entonces el proceso termina acá, es decir, 6 = *mcd* (54, 60).

Notar que, si un entero *d* es un divisor tanto de 60 como de 54, entonces necesariamente *d* divide a 6. Más aún, para cada par de enteros *a* y *b*, **los divisores comunes de *a* y *b* son exactamente los mismos que los divisores comunes de *b* y *a* + *k.b* para cualquier entero *k*** por la propiedad 5 de divisibilidad. En particular, coinciden con los divisores comunes de *b* y el resto de la división de *a p*or *b*. Es por este motivo que el último resto no nulo en el algoritmo de Euclides resulta ser el máximo común divisor entre *a* y *b*. La comprobación precisa, en el caso general, está dada en la demostración del teorema.

Desarrollemos dos ejemplos más antes de plantear el teorema.

[3] Euclides fue un matemático griego que vivió alrededor del año 300 a.C. Estudió en Atenas y fundó una escuela de matemática en Alejandría (Egipto). Su obra Los Elementos es una de las obras científicas más conocidas del mundo. Este tratado de geometría ha sido utilizado como libro de texto durante 2.000 años y es, con algunas modificaciones, la base de los libros de texto de geometría plana de hoy, por lo cual se conoce a Euclides como al Padre de la Geometría. Euclides presentó el algoritmo que describiremos para resolver un problema geométrico: encontrar la medida más grande que puede utilizarse para medir, sin resto, dos segmentos de recta.

Ejemplos

a) Calcular el *mcd* (210, 99) usando el algoritmo de Euclides:

$$\begin{array}{rcll} 210 & = & 2 \cdot 99 + 12; & r_1 = 12 \\ 99 & = & 8 \cdot 12 + 3; & r_2 = 3 \\ 12 & = & 4 \cdot 3 + 0; & r_3 = 0 \end{array}$$

Entonces, el *mcd* (210, 99) = 3. En efecto, 210 = 3 · 70 y 99 = 33 · 3, ó sea que 3 es un divisor común. Más aún, como 70 y 33 no tienen divisores comunes salvo el 1, deducimos que 3 es el **máximo** de los divisores comunes.

b) Calcular el mcd (630, 50) usando el algoritmo de Euclides:

$$\begin{array}{rcll} 630 & = & 12 \cdot 50 + 30; & r_1 = 30 \\ 50 & = & 1 \cdot 30 + 20; & r_2 = 20 \\ 30 & = & 1 \cdot 20 + 10; & r_3 = 10 \\ 20 & = & 2 \cdot 10 + 0; & r_4 = 0 \end{array}$$

Entonces, el *mcd* (630, 50) = 10. En efecto, 630 = 63 · 10 y 50 = 5 · 10, entonces 10 es un divisor común. Como 5 y 63 no tienen divisores comunes salvo el 1, deducimos que 10 es el **máximo** de los divisores comunes.

Observación. ¿Cuánto vale el *mcd* (0, *a*) para $a \neq 0$? La respuesta es que:

$$mcd\,(0\ ,\ a) = a \quad \text{para todo } a > 0$$

dado que $a \mid a$, también $a \mid 0$ y $a \geq 1 > 0$. Si $a < 0$,

$$mcd\,(0\ ,\ a) = |a| = -a \in \mathbb{N}$$

El máximo común divisor de *a* y *b* no está definido si *a* = 0 y *b* = 0.

5.1. Algoritmo de Euclides

A continuación enunciamos y demostramos el teorema que justifica la existencia del máximo común divisor y provee el algoritmo que permite calcularlo.

Teorema 2.2 (Existencia y unicidad del máximo común divisor). *Dados* $a, b \in \mathbb{Z}$, *no simultáneamente nulos, existe un único* $d \in \mathbb{N}$ *que satisface las condiciones:*

1) $d \mid a$ *y* $d \mid b$.
2) Si $c \in \mathbb{Z}$ *es cualquier otro entero tal que* $c \mid a$ *y* $c \mid b$, *entonces* $c \mid d$.

El número d se llama el máximo común divisor *de a y b.*

Demostración. Teniendo en cuenta la observación anterior, basta considerar el caso

$a \neq 0$ y $b \neq 0$. Además, como ya hemos observado en el ejemplo posterior a la definición de máximo común divisor es:

$$mcd\,(a\ ,\ b) = mcd\,(|a|\ ,\ |b|)$$

En consecuencia, basta probar el resultado para $a > 0$ y $b > 0$.

Existencia del máximo común divisor. Como ya hemos visto en los ejemplos, el algoritmo de Euclides se basa en el algoritmo de división. Supongamos que $a > b > 0$ y apliquémosle el algoritmo de división a a y b; entonces existen enteros q_1 y r_1 tales que:

$$a = q_1 \cdot b + r_1 \text{ y } 0 \leq r_1 < b$$

Si $r_1 = 0$, entonces $b \mid a$ y el $mcd\ (a, b) = b$. Si $r_1 \neq 0$, dado que $0 < r_1 < b$, podemos efectuar la división de b por r_1, entonces existen enteros q_2 y r_2 tales que:

$$b = q_2 \cdot r_1 + r_2 \text{ y } 0 \leq r_2 < r_1$$

Si $r_2 = 0$, el proceso termina. Si no, tenemos que $0 < r_2 < r_1$ y dividimos r_1 por r_2; existen q_3 y r_3 del algoritmo de división. Si $r_3 \neq 0$, dividimos r_2 por r_3, y así sucesivamente:

$$\begin{array}{rcll} a & = & q_1 \cdot b + r_1 & 0 \leq r_1 < b \\ b & = & q_2 \cdot r_1 + r_2 & 0 \leq r_2 < r_1 \\ r_1 & = & q_3 \cdot r_2 + r_3 & 0 \leq r_3 < r_2 \\ r_2 & = & q_4 \cdot r_3 + r_4 & 0 \leq r_4 < r_3 \\ & & \vdots & \end{array}$$

Pero estos restos se van haciendo cada vez más chicos y no pueden ser menores que cero; por lo tanto, en algún paso, el resto se hace cero y el algoritmo termina. Explícitamente, para algún n, obtenemos $r_n = 0$, es decir que en el paso n-ésimo ocurre lo siguiente:

$$\begin{array}{rcll} r_{n-3} & = & q_{n-1} \cdot r_{n-2} + r_{n-1} & 0 \leq r_{n-1} < r_{n-2} \\ r_{n-2} & = & q_n \cdot r_{n-1} & \end{array}$$

En particular, la última igualdad dice que $r_{n-1} \mid r_{n-2}$; pero entonces, la anterior implica que también $r_{n-1} \mid r_{n-3}$ por la propiedad 5 de divisibilidad. Así siguiendo, $r_{n-1} \mid r_{n-4}$, etcétera; obtenemos que $r_{n-1} \mid r_1$, $r_{n-1} \mid b$, y finalmente, $r_{n-1} \mid a$. Por lo tanto, r_{n-1} divide a ***a*** y a ***b***, es decir, es un **divisor común de *a* y *b*.**

Afirmamos que r_{n-1}, que es el último resto distinto de cero, es el máximo común divisor. Para probarlo, falta ver que si c es un divisor cualquiera de a y b, entonces $c \mid r_{n-1}$.

Sea c un divisor cualquiera de a y b; si recorremos de manera inversa el camino anterior, de la primera igualdad se desprende que $c \mid r_1$, ya que:

$$a = q_1 \cdot b + r_1,\ c \mid a,\ c \mid b \Longrightarrow c \mid r_1$$

Análogamente, usando la segunda igualdad, tenemos que como $c \mid b$ y $c \mid r_1$, entonces $c \mid r_2$.

Así siguiendo, obtenemos que c divide a todos los restos que van apareciendo. En particular, $c \mid r_{n-1}$. Por lo tanto, $r_{n-1} = mcd\,(a\,,\,b)$.

Unicidad del máximo común divisor. Supongamos que tenemos dos máximos comunes divisores, d_1 y d_2, es decir que d_1 y $d_2 \in \mathbb{N}$ verifican ambos las condiciones 1) y 2) del enunciado; entonces, dado que $d_1 \mid a$, $d_1 \mid b$ y d_2 cumple la condición 2), obtenemos que $d_1 \mid d_2$. Por el mismo razonamiento, $d_2 \mid d_1$. Luego, la propiedad 3 de divisibilidad dice que $|d_1| = |d_2|$ y al ser ambos positivos, $d_1 = d_2$.

Algoritmo de Euclides para calcular el máximo común divisor entre dos naturales no nulos a y b.

- Comenzar con $r_1 = a$, $r_2 = b$.
- Mientras que $r_2 \neq 0$:
  - hallar el resto r de la division de r_1 por r_2;
  - reemplazar
    $r_1 \leftarrow r_2$,
    $r_2 \leftarrow r$.
- Dar como respuesta r_1.

5.2. El máximo común divisor como combinación lineal entera de a y b

Una propiedad importante del máximo común divisor de a y b es que se lo puede escribir como **combinación lineal entera** de a y de b; más aún, el máximo común divisor es el natural más chico con esta propiedad.

Si $d \in \mathbb{Z}$, decimos que d es combinación lineal entera de a y b, si existen $m,\ n \in \mathbb{Z}$ tales que:

$$d = a \cdot m + b \cdot n$$

Veamos cómo calcular esta escritura para el máximo común divisor en un ejemplo. El $mcd\,(630,\ 50) = 10$. En efecto, por el algoritmo de Euclides:

$$\begin{array}{rcl@{\quad}rcl} 630 &=& 12 \cdot 50 + 30; & r_1 &=& 30 \\ 50 &=& 1 \cdot 30 + 20; & r_2 &=& 20 \\ 30 &=& 1 \cdot 20 + 10; & r_3 &=& 10 \\ 20 &=& 2 \cdot 10 + 0; & r_4 &=& 0 \end{array}$$

Para escribir a 10 como una combinación lineal entera de 630 y 50, recorremos en sentido inverso los pasos que efectuamos en el algoritmo y despejamos en cada nivel el resto, empezando por $d = 10$:

$$\begin{array}{rcl@{\quad}rcl} 30 &=& 1 \cdot 20 + 10 & \Longrightarrow & 10 &=& 30 - 20 \\ 50 &=& 1 \cdot 30 + 20 & \Longrightarrow & 20 &=& 50 - 30 \\ 630 &=& 12 \cdot 50 + 30 & \Longrightarrow & 30 &=& 630 - 12 \cdot 50 \end{array}$$

Luego, reemplazamos a cada resto por la expresión obtenida en cada uno de los pasos anteriores:

$$\begin{array}{rcl} 10 &=& 30 - 20 \\ &=& 30 - (50 - 30) \;=\; -50 + 2 \cdot 30 \\ &=& -50 + 2 \cdot (630 - 12 \cdot 50) \;=\; 50 \cdot (-25) + 630 \cdot 2 \end{array}$$

Obteniendo así la combinación lineal entera:

$$10 = 50 \cdot (-25) + 630 \cdot 2$$

Ejemplo. Probar que si $a, b \in \mathbb{Z}$ son tales que $mcd\,(a, b) = 5$, entonces $mcd\,(a + 2 \cdot b, 3 \cdot a + 4 \cdot b) = 5$ ó 10.

Solución. Llamemos $d = mcd\,(a + 2 \cdot b, 3 \cdot a + 4 \cdot b)$; entonces d divide a ambos números, en particular, divide a sus múltiplos y a la suma y a la diferencia de múltiplos de ellos, por ejemplo:

$$\begin{aligned} d \mid (a + 2 \cdot b) \quad &\Rightarrow d \mid 3 \cdot (a + 2 \cdot b) \\ d \mid 3 \cdot (a + 2 \cdot b) \text{ y } d \mid (3 \cdot a + 4 \cdot b) \quad &\Rightarrow d \mid [3 \cdot (a + 2 \cdot b) - (3 \cdot a + 4 \cdot b)] \end{aligned}$$

Entonces, d divide a $3 \cdot (a + 2 \cdot b) - (3 \cdot a + 4 \cdot b) = 6 \cdot b - 4 \cdot b = 2 \cdot b$

Análogamente:

$$\begin{aligned} d \mid (a + 2 \cdot b) \quad &\Rightarrow d \mid 2 \cdot (a + 2 \cdot b) = 2 \cdot a + 4 \cdot b \\ d \mid (2 \cdot a + 4 \cdot b) \text{ y } d \mid (3 \cdot a + 4 \cdot b) \quad &\Rightarrow d \mid [(3 \cdot a + 4 \cdot b) - (2 \cdot a + 4 \cdot b)] \end{aligned}$$

Entonces, d divide a $(3 \cdot a + 4 \cdot b) - (2 \cdot a + 4 \cdot b) = 3 \cdot a - 2 \cdot a = a$

En consecuencia:

$$\boxed{d \text{ divide a } a \text{ y } d \text{ divide a } 2 \cdot b}$$

Por otra parte, dado que $mcd\,(a, b) = 5$, existen $m, n \in \mathbb{Z}$ tales que:

$$5 = m.a + n.b$$

Si multiplicamos a ambos miembros por 2, obtenemos:

$$10 = (2 \cdot m) \cdot a + n \cdot (2 \cdot b)$$

Pero entonces, como consecuencia de este hecho y de la afirmación recuadrada, necesariamente d divide a 10. Por lo tanto:

$$\boxed{d \text{ es igual a } 1,\ 2,\ 5 \text{ ó } 10}$$

Sólo falta descartar que d sea 1 ó 2. Notar que $mcd\,(a, b) = 5$ implica que $5 \mid a$ y $5 \mid b$, entonces 5 divide a $a + 2 \cdot b$ y a $3 \cdot a + 4 \cdot b$. Entonces, por definición de d, obtenemos también que 5 divide a d. Por lo tanto, d no puede ser ni 1 ni 2.

Más aún, notar que si a es par, entonces $a+2 \cdot b$ y $3 \cdot a+4 \cdot b$ son ambos números pares, por lo tanto, $d = 10$, mientras que si a es impar, $a + 2 \cdot b$ también es impar y en este caso, $d = 5$.

Ejercicio 2.3. Probar que $mcd\,(2^n + 7^n, 2^n - 7^n) = 1$ para todo $n \in \mathbb{N}$.

Dos enteros a y b se dicen *coprimos,* si su máximo común divisor es igual a 1.

Notar que, en este caso, el número 1 se escribe como combinación lineal entera de a y b. En efecto, el $mcd\,(a\,,\,b)$ verifica siempre esta propiedad.

Recíprocamente, si existen $m,\ n \in \mathbb{Z}$ tales que:

$$1 = a \cdot m + b \cdot n$$

entonces, $mcd\,(a,\ b) = 1$. En efecto, si $d = mcd\,(a,\ b) \in \mathbb{N}$, dado que d divide a a y b, por la propiedad 5 de divisibilidad, d divide a $a \cdot m + b \cdot n = 1$. Pero el único divisor *positivo* de 1 es el mismo 1; por lo tanto, $d = 1$.

En resumen, el razonamiento anterior es la comprobación del siguiente enunciado:

Proposición 2.3. *Dos enteros a y b son coprimos si y sólo si existen* $m,\ n \in \mathbb{Z}$ *tales que* $1 = a \cdot m + b \cdot n$

Una propiedad importante que se deduce de ésta es la siguiente:

Proposición 2.4. *Dados enteros a, b, c tales que* $a \mid b \cdot c$, *si a y b son coprimos entonces* $a \mid c$.

Demostración. Como a y b son coprimos, existen m y $n \in \mathbb{Z}$ tales que $1 = a \cdot m + b \cdot n$. Multiplicando esta igualdad por c obtenemos que $c = a \cdot c \cdot m + b \cdot c \cdot n$. Claramente, a divide al primer término, y también divide al segundo porque divide a $b \cdot c$. Luego, a divide a c.

□ 6. Teorema fundamental de la aritmética

El teorema fundamental de la Aritmética, Teorema 2.6 de esta sección, afirma que todo entero, distinto de 0, 1 y -1, puede representarse como un producto de números primos. Su nombre está plenamente justificado por las consecuencias importantes que se desprenden de él y por sus innumerables aplicaciones. Antes de enunciarlo necesitamos recordar la noción de número primo y probar una propiedad que cumplen estos números.

Un número entero se dice *primo* si tiene exactamente cuatro divisores distintos; en otras palabras, $n \in \mathbb{Z}$ es primo si y sólo si sus únicos divisores son 1, -1, n y $-n$ y estos son todos distintos. Un número entero distinto de 1, -1 y 0 que no es primo se dice *compuesto*.

La razón del nombre "compuesto", como veremos enseguida, es que **si** $n \neq 1, -1, 0$ **no es primo, entonces** n **es un producto de primos.**

El 1 no es primo. Los primeros primos positivos son 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, etcétera.

Proposición 2.5. *Si un primo p divide a un producto de dos enteros, entonces p divide a alguno de los factores.*

Demostración. Sea p un primo positivo que divide a un producto de dos enteros $m \cdot n$. Si p dividiera a m valdría el enunciado. Supongamos que p no divide a m, entonces p y m son coprimos. Demostremos esta afirmación. Sea $d = mcd\,(p, m)$ entonces $d \mid p$ que es primo; luego $d = 1$ o $d = p$, pero en el último caso tendríamos que $p = d \mid m$, que contradice la hipótesis; por lo tanto, $d = 1$.

Tenemos entonces que $p \mid m \cdot n$, y p es coprimo con m, con lo cual, por la Proposición 2.4, necesariamente $p \mid n$.

Se prueba por inducción que el enunciado anterior se extiende a productos de una cantidad arbitraria de factores.

Observación. Para el teorema utilizaremos la siguiente notación: para indicar un producto de r factores, digamos $p_1 \cdot p_2 \ldots p_r$ se utiliza la escritura abreviada

$$p_1 \cdot p_2 \cdots p_r = \prod_{i=1}^{r} p_i$$

El símbolo de la derecha indica el producto de los factores p_i, donde el subíndice i toma los valores 1 a r, esto es, el producto de los números p_1, p_2, ... hasta p_r. Por ejemplo: si $r = 4$ y los cuatro factores son $p_1 = 2$, $p_2 = 5$, $p_3 = 7$ y $p_4 = 11$, entonces:

$$\begin{aligned}\prod_{i=1}^{4} p_i &= p_1 \cdot p_2 \cdot p_3 \cdot p_4 \\ &= 2 \cdot 5 \cdot 7 \cdot 11\end{aligned}$$

Teorema 2.6 (Teorema Fundamental de la Aritmética). *Todo $n \in \mathbb{Z}$, $n \neq 0$, 1,-1, se factoriza como producto de primos. Explícitamente, todo $n \in \mathbb{N}$, $n \neq 1$, se escribe como producto de primos positivos,*

$$\begin{aligned}n &= \prod_{i=1}^{r} p_i \\ &= p_1 \cdot p_2 \cdots p_r\end{aligned}$$

y esta factorización es única, salvo por el orden de los factores.

Todo $n \in \mathbb{Z}$, $n < -1$, se escribe como -1 por un producto de primos positivos,

$$\begin{aligned}n &= (-1) \cdot \prod_{i=1}^{r} p_i \\ &= (-1) \cdot p_1 \cdot p_2 \cdots p_r\end{aligned}$$

y esta factorización es única, salvo por el orden de los factores.

Demostración. Probemos primero el enunciado para $n \in \mathbb{N}$, $n \neq 1$. Consideremos el conjunto:

$$\mathcal{P} = \{n \in \mathbb{N} : n \neq 1 \text{ y } n \text{ no admite factorización en primos positivos}\}$$

Dado que $\mathcal{P} \subset \mathbb{N}$, si fuera no vacío, $\mathcal{P}$ tendría un primer elemento, digamos n_0. En particular, n_0 no sería primo (pues si lo fuera, n_0 sería igual a una factorización en primos de un único factor, el mismo n_0), entonces existirían $d, q \in \mathbb{N}$, distintos de 1 y de n_0, tales que $n_0 = d \cdot q$; más aún, d y q deberían ser menores que n_0 por ser divisores de n_0. Por lo tanto, ni d ni q pertenecerían a $\mathcal{P}$, y entonces serían factorizables en primos, en cuyo caso el mismo n_0 se factorizaría también, lo cual sería una contradicción. Por lo tanto, $\mathcal{P}$ es vacío, es decir, *todo natural salvo el* 1 *se factoriza como un producto de primos positivos*.

Si $n \in \mathbb{Z}$, $n < -1$, entonces $-n$ es positivo, distinto de 1 y se factoriza como un producto de primos positivos, digamos:

$$\begin{aligned} -n &= \prod_{i=1}^{r} p_i \\ &= p_1 \cdot p_2 \cdots p_r \end{aligned}$$

que implica:

$$\begin{aligned} n &= -\prod_{i=1}^{r} p_i \\ &= (-1) \cdot \prod_{i=1}^{r} p_i \\ &= (-1) \cdot p_1 \cdot p_2 \cdots p_r \end{aligned}$$

Por lo tanto, *todo entero negativo distinto de* -1 *se escribe como* -1 *por un producto de primos positivos*.

Veamos que la factorización es única, salvo por el orden de los factores. Para esto basta considerar el caso de números naturales. La prueba procede por inducción en r, la cantidad de factores primos en una descomposición.

Definamos la proposición $P(r)$: *Si un número natural admite una factorización como producto de r factores primos positivos, esta factorización es única, salvo por el orden de los factores.*

Si $r = 1$, el número en cuestión es producto de un único factor, es decir, es un primo p y, por lo tanto, no tiene divisores distintos de 1 y p. Entonces, si p admite una factorización $p = p_1 \cdots p_s$ como producto de primos positivos, debe ser $s = 1$ y $p_1 = p$ (de lo contrario, p_1 sería un divisor de p y $p_1 \neq 1, p$).

Probemos el paso inductivo. Sea n un natural que admite una factorización como producto de $r + 1$ factores primos y veamos que esta factorización es única.

Supongamos que:

$$\begin{aligned} n &= \prod_{i=1}^{r+1} p_i \\ &= p_1 \cdot p_2 \cdots p_r \cdot p_{r+1} \end{aligned}$$

y también, para algún $r' \in \mathbb{N}$:

$$\begin{aligned} n &= \prod_{j=1}^{r'} p'_j \\ &= p'_1 \cdot p'_2 \cdots p'_{r'} \end{aligned}$$

Todos los primos que aparecen en la factorización de *n*, dividen a *n*. Por ejemplo: el primo p_{r+1} divide a *n*, o sea que, en particular, divide al producto de primos que forman la segunda descomposición; por lo tanto, divide a alguno de los factores; pero como ellos son todos primos positivos, necesariamente coincide con alguno de estos factores, es decir que:

$$p_{r+1} = p'_{j_0} \text{ para algún subíndice } j_0$$

Luego, si excluimos este factor, obtenemos un número natural que admite una factorización con exactamente *r* factores primos:

$$\prod_{i=1}^{r} p_i = \prod_{j=1, j \neq j_0}^{r'} p'_j \quad (*)$$

Por lo tanto, como consecuencia de la hipótesis inductiva, la descomposición de este número es única, salvo el orden de los factores; pero entonces lo mismo vale para *n*, dado que el factor que les falta a ambas descomposiciones $(*)$ es p_{r+1} que es igual a p'_{j_0}.

Corolario 2.7. *Todo número natural compuesto n es divisible por algún número primo estrictamente menor que n.*

Ejemplo. ¿Cómo obtener la descomposición en factores primos de un entero dado?

Por ejemplo, calculemos la factorización de 360; el procedimiento consiste en **dividir sucesivamente por los primos positivos, en orden, empezando por el 2, tantas veces como sea posible**, o sea:

$$\begin{aligned} 360 &= 2 \cdot 180 \\ &= 2 \cdot (2 \cdot 90) \\ &= 2 \cdot (2 \cdot (2 \cdot 45)) \\ &= 2^3 \cdot 45 \end{aligned}$$

Como 45 no es divisible por 2, dividimos este factor por 3 y finalmente por 5,

$$\begin{aligned} 360 &= 2^3 \cdot 45 \\ &= 2^3 \cdot (3 \cdot 15) \\ &= 2^3 \cdot 3^2 \cdot 5 \end{aligned}$$

Por lo tanto, la factorización prima buscada es $360 = 2^3 \cdot 3^2 \cdot 5$

Recordemos que éste era el método que usábamos en la primaria; la representación gráfica que ayuda a aplicarlo es la siguiente:

$$\begin{array}{r|l} 360 & 2 \\ 180 & 2 \\ 90 & 2 \\ 45 & 3 \\ 15 & 3 \\ 5 & 5 \\ 1 & \end{array}$$

La columna de la derecha nuevamente nos da la factorización $360 = 2^3 \cdot 3^2 \cdot 5$

Calculemos la factorización prima de -2.142: empezamos dividiendo a 2.142, su valor absoluto, por 2 y obtenemos:

$$2.142 = 2 \cdot 1.071$$

Como 1.071 no es par, continuamos dividiendo a 1.071 por 3; obtenemos:

$$\begin{aligned} 2.142 &= 2 \cdot 1.071 \\ &= 2 \cdot 3 \cdot 357 \end{aligned}$$

Dividimos a 357 por 3 y obtenemos un cociente entero, lo cual nos dice que hay otro factor 3, o sea:

$$\begin{aligned} 2.142 = 2 \cdot 1.071 &= 2 \cdot 3 \cdot 357 \\ &= 2 \cdot 3 \cdot (3 \cdot 119) \\ &= 2 \cdot 3^2 \cdot 119 \end{aligned}$$

Dado que 119 no es divisible por 3, verificamos si lo es por el primo siguiente, el 5, vemos que no. Así siguiendo, efectuamos la división por 7 y obtenemos un cociente entero, que además es primo, $119 = 7 \cdot 17$; entonces el proceso termina:

$$\begin{aligned} 2.142 &= 2 \cdot 3^2 \cdot 119 \\ &= 2 \cdot 3^2 \cdot 7 \cdot 17 \end{aligned}$$

Por lo tanto:

$$-2.142 = (-1) \cdot 2 \cdot 3^2 \cdot 7 \cdot 17$$

Es decir que **la factorización prima de un entero negativo es la de su valor absoluto multiplicada por** -1, como vimos en la demostración del teorema.

Si n es grande, puede ser difícil hallar su factorización, en particular, si el primo más chico que lo divide es un número grande. Por ejemplo, la factorización prima de 1.442.897 es:

$$1.442.897 = 113^3$$

En este ejemplo, el primo más chico que divide al número (y en realidad el único) es 113. Un ejemplo como éste requiere además la comprobación de que 113 es primo, que efectuaremos después.

Otro ejemplo que podemos considerar es n = 2.279.269, cuya factorización prima es:

$$2.279.269 = 127 \cdot 131 \cdot 137$$

Es decir, si empezamos a dividir por 2, por 3, por 5, por 7 ... etcétera, el proceso concluye en algún momento, pero es muy lento. Por otra parte, es necesario comprobar que estos tres factores son números primos.

Para comprobar que un número es primo, tenemos la siguiente herramienta:

Lema 2.8. *Un número natural n es compuesto si y sólo si existe un primo p que divide a n tal que* $1 < p \leq \sqrt{n}$.

Demostración. Sea n un número natural compuesto; dado que n no es primo, necesariamente admite algún divisor distinto de 1, -1, n y $-n$, digamos $d \in \mathbb{N}$. En particular, $1 < d < n$. Es decir que existen $d, q \in \mathbb{Z}$ que verifican:

$$n = d \cdot q \quad \text{y} \quad 1 < d, q < n$$

En efecto, si q fuera mayor o igual que n, el producto $d \cdot q$ sería mayor que n, porque $d > 1$; y si fuera $q = 1$, debería ser $d = n$, contradiciendo la elección de d.

Más aún, en realidad $d \leq \sqrt{n}$ o $q \leq \sqrt{n}$; en efecto, si ocurriera que ambos $d > \sqrt{n}$ y $q > \sqrt{n}$, obtendríamos:

$$d \cdot q > \sqrt{n} \cdot \sqrt{n} = n.$$

o sea, $d \cdot q > n$, hecho que contradice la igualdad $d \cdot q = n$ con la que empezamos.

Supongamos entonces que $d \leq \sqrt{n}$. Si d es primo, hemos terminado la demostración. Si no, se desprende del teorema fundamental que d, y por lo tanto n, admite un divisor primo, claramente menor que $\sqrt{n}$.

Recíprocamente, si existe un primo p que divide a n tal que $1 < p \leq \sqrt{n}$. entonces, como $\sqrt{n} < n$, obtenemos $p < n$, es decir que p es un primo que divide a n y no es igual a n; por lo tanto, n no es primo.

Ejemplo. Los números 109, 113, 127, 131 y 137 son primos. En efecto, dado que $13^2 = 169$, que es mayor que todos los anteriores, según el lema anterior es suficiente comprobar que no son divisibles por ningún primo positivo menor o igual que 11, es decir, que no son divisibles por 2, 3, 5, 7 ni 11.

Ejemplo. Comprobar que los siguientes números son primos: 1.009, 1.013, 1.021, 1.031, 1.033, 1.039, 1.049, 1.051. Probar que, en efecto, los anteriores no son divisibles por ningún primo menor o igual que 31, que es el máximo primo menor o igual que la raíz cuadrada de 1.051.

También 5.003 y 5.009 son primos, porque no son divisibles por ningún primo menor o igual que su raíz cuadrada. En efecto, no son divisibles por ningún primo menor que 71 y $71^2 = 5.041 > 5.009$.

Teorema 2.9. *Existen infinitos primos.*

Demostración. Vamos a comprobar que existen infinitos primos positivos. Supongamos que la afirmación no sea verdadera, sino que existan sólo una cantidad finita de primos positivos, digamos $p_1, p_2, \ldots, p_n$.

Consideremos el número entero $c = 1+p_1 \cdot p_2 \cdot \ldots \cdot p_n$, es decir, c es el *producto de todos los primos positivos más uno*. Notar que $c \neq 0, 1, -1$, porque, dado que el primo positivo más chico es 2, tenemos que $c \geq 1 + 2 = 3$. La afirmación es que c no es divisible por ningún primo positivo. En efecto, si algún primo dividiera a c, este primo debería ser alguno de los $p_1, p_2, \ldots, p_n$. Supongamos que p_1 divida a c; por otra parte es claro que p_1 divide al producto de todos los primos (pues p_1 es uno de los factores de este producto), es decir que:

$$p_1 \mid c \text{ y también } p_1 \mid p_1 \cdots p_n$$

Pero entonces p_1 dividiría a la diferencia de estos dos números, a saber, $c - p_1 \ldots p_n = 1$, ó sea que p_1 dividiría a 1; esto sería una contradicción con el hecho de que p_1 sea un número primo.

Pero entonces $c \neq 0, 1, -1$ es un entero no divisible por ningún primo, lo cual contradice el teorema fundamental; esta contradicción provino de haber negado el enunciado; por lo tanto, existen infinitos primos.

Ejemplo. Encontrar el menor número natural n tal que $2.200 \cdot n$ sea un cuadrado.

Solución. Como en numerosos ejemplos más, la herramienta esencial para este cálculo es el teorema fundamental.

Pensemos qué exponentes aparecen en la descomposición de un número natural mayor que 1 que es el cuadrado de algún otro, digamos k^2. Si escribimos en general $k = p_1 \ldots p_r$ como producto de primos y lo elevamos al cuadrado, obtenemos:

$$\begin{aligned} k^2 &= (p_1 \cdots p_r)^2 \\ &= p_1^2 \cdots p_r^2 \end{aligned}$$

Es decir que en la factorización en primos de un natural al cuadrado, los factores primos aparecen todos al cuadrado. Por ejemplo:

$$\begin{aligned} 50^2 &= (2 \cdot 5^2)^2 \\ &= (2 \cdot 5 \cdot 5)^2 \\ &= 2^2 \cdot 5^2 \cdot 5^2 \\ &= 2^2 \cdot (5^2)^2 \end{aligned}$$

El 5 ya estaba dos veces en el 50 y al elevarlo al cuadrado, aparece cuatro veces. Es decir que **en un cuadrado, todos los factores primos distintos deben estar una cantidad par de veces.**

Volviendo a nuestro problema, efectuemos la factorización de 2.200:

$$\begin{array}{r|l} 2.200 & 2 \\ 1.100 & 2 \\ 550 & 2 \\ 275 & 5 \\ 55 & 5 \\ 11 & 11 \\ 1 & \end{array}$$

Entonces:

$$2.200 = 2^3 \cdot 5^2 \cdot 11$$

Ahora pensemos en la condición de que 2.200 n sea un cuadrado, o sea, necesitamos que sea de la forma k^2 para algún $k \in \mathbb{N}$ que por el momento desconocemos.

¿Qué factores necesitamos agregarle a 2.200 para que todos los primos aparezcan elevados a un exponente par? Como el 2 está tres veces, necesitamos un 2 más; el 5 ya está una cantidad par de veces, así que no hacen falta más factores iguales a 5, el 11 está una vez, así que necesitamos al menos un 11 más. Es decir que si a 2.200 le agregamos estos dos factores cuyo producto llamamos n, o sea, $n = 2 \cdot 11$, tenemos:

$$\begin{aligned} 2.200 \cdot n &= (2^3 \cdot 5^2 \cdot 11) \cdot (2 \cdot 11) \\ &= 2^4 \cdot 5^2 \cdot 11^2 \\ &= (2^2 \cdot 5 \cdot 11)^2 \end{aligned}$$

que ya tiene la forma de un k^2, justamente, con $k = 2^2 \cdot 5 \cdot 11$. Por lo tanto, el n que buscábamos es el que construimos con los factores que agregamos, $n = 2 \cdot 11$.

6.1. El máximo común divisor a partir de la factorización prima

Una de las consecuencias del Teorema 2.6 es que podemos escribir el máximo común divisor d de dos números en términos de los primos que dividen a los números. La idea es que todo divisor primo de ambos números necesariamente también divide a d, es decir, que aparece en la factorización en primos de d y, recíprocamente, todo primo que aparece en la factorización de d debe dividir a los dos números, por propiedad del máximo común divisor.

Por ejemplo: $630 = 2 \cdot 3^2 \cdot 5 \cdot 7$ y $50 = 2 \cdot 5^2$

Observemos que 2 y 5 aparecen en la factorización tanto de 630 como de 50; por lo tanto, $10 = 2 \cdot 5$ divide a ambos números; más aún, 2 y 5 son los únicos primos que aparecen en la factorización de los dos enteros, 630 y 50. Por otro lado, recordemos que ya hemos calculado en un ejemplo anterior que:

$$\begin{aligned} mcd\,(630\ ,\ 50) &= 10 \\ &= 2 \cdot 5 \end{aligned}$$

Ejemplo. Estudiemos otro ejemplo: calcular d, el máximo común divisor de 252 y 360, a partir de sus descomposiciones primas.

Efectuemos las factorizaciones:

$$252 = 2^2 \cdot 3^2 \cdot 7 \quad \text{y} \quad 360 = 2^3 \cdot 3^2 \cdot 5$$

entonces 2 y 3 dividen a ambos números. Notar que, en realidad, 2^2 y 3^2 dividen a ambos, dado que aparecen en sus descomposiciones; no así 2^3, que está sólo en la factorización de 360 pero no en la de 252. Por lo tanto:

$$2^2 \cdot 3^2 \text{ divide a } d$$

Es decir que, dado que el 2 aparece en la descomposición prima de 252 con exponente 2, y el 2 aparece en la descomposición prima de 360 con exponente 3, el 2 aparece en la descomposición prima de d con exponente 2, que es el exponente más chico de los dos. Análogamente, 3^2 aparece en la factorización en primos de d. Más aún:

$$d = 2^2 \cdot 3^2 = 36$$

de lo contrario, debería haber algún otro primo que divida a d, pero como d divide a 252 y 360, un primo tal también dividiría a 252 y 360; pero ya vimos que los únicos primos que los dividen a ambos son 2 y 3 y vimos también cuál es la máxima potencia de cada uno de estos primos, que divide tanto a 252 como a 360.

Obtuvimos que:
el máximo común divisor es el producto de los primos comunes elevados a su menor exponente.

6.2. El mínimo común múltiplo

Para lograr un rendimiento óptimo, la fábrica X recomienda a los propietarios de sus autos cambiar el aceite cada 6.000 *km y el líquido refrigerante cada* 8.000 *km. ¿Cuál es la cantidad mínima de km al cabo de la cual hay que renovar los dos líquidos a la vez?*

La respuesta a esta pregunta es una cantidad n de km tal que coincida el cambio de aceite con el de líquido refrigerante; es decir que, en *miles de km*, n debe ser 6 ó 12 ó 18, etcétera para que toque hacer un cambio de aceite y, por otra parte, n debe ser 8 ó 16 ó 24, etcétera para que sea necesario efectuar un cambio de refrigerante. Es decir que:

n debe ser a la vez múltiplo de 6 y de 8.

¿Cuál es el natural que más fácilmente cumple esta condición? Seguramente 48, que es igual a 6 por 8, es el primer ejemplo que nos viene a la mente; claramente es un múltiplo tanto de 6 como de 8, pero no necesariamente es el más chico entre todos los múltiplos comunes.

En otras palabras, n debe ser *a la vez múltiplo de* 6 *y de* 8 y, entre todos los múltiplos de 6 y de 8, nos interesa *el mínimo.* Si pensamos cuidadosamente, nos damos cuenta de que el mínimo natural que satisface estas condiciones es $n = 24$, en unidades de miles de km. La respuesta es que cada 24.000 km corresponde renovar los dos líquidos para optimizar el rendimiento. Decimos que 24 *es el mínimo común múltiplo de* 6 *y* 8 y denotamos:

$$[6 : 8] = 24$$

Consideremos otro ejemplo. *En el campeonato interescolar, el equipo de voley femenino de la escuela tiene un partido cada* 10 *días y el de varones, cada* 12 *días. Si ambos equipos inauguran el campeonato jugando el mismo día, ¿cuántos días más tarde vuelven a coincidir?*

La respuesta es una cantidad m de días, a partir de la fecha inaugural, tal que les toque jugar a la vez a las chicas y a los varones; o sea que m debe ser a la vez múltiplo de 10 y múltiplo de 12. En otras palabras, m debe pertenecer al conjunto de los múltiplos de 10:

$$\mathcal{M}_{10} = \{10,\ 20,\ 30,\ 40,\ 50,\ \mathbf{60},\ 70,\ 80,\ 90,\ 100,\ 110\ldots\}$$

y a la vez al de los múltiplos de 12 que es

$$\mathcal{M}_{12} = \{12,\ 24,\ 36,\ 48,\ \mathbf{60},\ 72,\ 84\ldots\}$$

Si observamos los dos conjuntos, descubrimos que el número 60 está en ambos, y es el mínimo natural que es múltiplo de 10 y de 12 a la vez; es decir que *el mínimo común múltiplo de* 10 *y* 12 *es* 60 y escribimos:

$$[10 : 12] = 60$$

Dados enteros a y b, un número natural m se dice el *mínimo común múltiplo* de a y b si cumple las siguientes propiedades:

1) $a \mid m$ y $b \mid m$.
2) Si m' es otro entero tal que $a \mid m'$ y $b \mid m'$, entonces $m \mid m'$.

En otras palabras, el mínimo común múltiplo de a y b es el múltiplo positivo más chico de a y b. Lo denotamos por:

$$m = [a : b]$$

Teniendo a la vista los conjuntos de múltiplos de uno y otro número, es fácil deducir cuánto vale el mínimo común múltiplo entre ellos; pero en realidad, hay otras formas de calcularlo. Una muy eficiente se deduce del siguiente enunciado, donde debemos recordar la notación $(a : b)$ para el máximo común divisor de a y b.

Proposición 2.10. *Sean a y b números naturales, entonces el producto de a y b es igual al producto de su máximo común divisor y su mínimo común múltiplo. En símbolos, esta igualdad se expresa como:*

$$a \cdot b = (a : b) \cdot [a : b]$$

En el ejemplo previo para $a = 10$ y $b = 12$, estos números son:

$$(10 : 12) = 2 \quad \text{y} \quad [10 : 12] = 60$$

entonces la igualdad se expresa como:

$$\begin{aligned} 120 &= 10 \cdot 12 \\ &= 2 \cdot 60 \end{aligned}$$

Dados a y b, si lo que buscamos es el mínimo común múltiplo, se puede utilizar la igualdad anterior para despejarlo como el cociente entre el producto de a por b y su máximo común divisor. Es decir que, como consecuencia de la identidad anterior, tenemos que:

$$\begin{aligned} [10 : 12] &= \frac{10 \cdot 12}{(10 : 12)} \\ &= \frac{120}{2} \\ &= 60 \end{aligned}$$

Corolario 2.11. *Sean a y b números naturales, entonces el mínimo común múltiplo de a y b es igual al cociente entre el producto de a y b y su máximo común divisor. En símbolos, esta igualdad se expresa como:*

$$[a : b] = \frac{a \cdot b}{(a : b)}.$$

Si alguno de los dos números es negativo, el producto de ellos es negativo también. La relación anterior vale si corregimos el signo, es decir:

$$\text{si } a < 0 < b \quad \text{o} \quad b < 0 < a, \quad [a : b] = \frac{-a \cdot b}{(a : b)}$$

Recordemos que tanto $[a : b]$ como $(a : b)$ son naturales, cualesquiera sean los signos de a y b. Si tanto a como b son negativos, la igualdad vale sin cambiar signos.

Observación. En el caso en que a y b sean coprimos, $(a : b) = 1$, la igualdad anterior implica que $[a : b] = a \cdot b$, es decir que en este caso, el mínimo común múltiplo de a y b es igual al producto de a por b.

Por ejemplo, los múltiplos positivos de $a = 3$ son:

$$\mathcal{M}_3 = \{3,\ 6,\ 9,\ \mathbf{12},\ 15,\ 18,\ 21,\ \mathbf{24},\ 27,\ 30,\ 33,\ \mathbf{36},\ 39 \dots\}$$

y los múltiplos positivos de $b = 4$ son:

$$\mathcal{M}_4 = \{4,\ 8,\ \mathbf{12},\ 16,\ 20,\ \mathbf{24},\ 28,\ 32,\ \mathbf{36},\ 40 \dots\}$$

Entonces, el mínimo común múltiplo es:

$$\begin{aligned} [3 : 4] &= 12 \\ &= a \cdot b. \end{aligned}$$

Notar que hay infinitos múltiplos comunes de 3 y 4, que son todos múltiplos de 12, el mínimo común múltiplo.

Ejemplo. Los enteros $a = 275$ y $b = 327$ son coprimos; en efecto:

$$a = 275 \quad \text{y} \quad b = 327$$
$$= 5^2 \cdot 11 \qquad = 3 \cdot 109$$

no tienen primos comunes en sus descomposiciones; por lo tanto, su máximo común divisor es (275 : 327) = 1 y su mínimo común múltiplo es el producto de los dos números:

$$[a : b] = 275 \cdot 327$$
$$= 3 \cdot 5^2 \cdot 11 \cdot 109.$$

Como ya vimos en un ejemplo anterior, 109 es primo.

A partir de la factorización prima de los enteros *a* y *b*, es fácil obtener el mínimo común múltiplo. En efecto, si *a* = 10 y *b* = 12,

$$10 = 2 \cdot 5 \quad \text{y} \quad 12 = 2^2 \cdot 3$$

Notar que el 2 aparece en *a* = 10 y en *b* = 12, pero en el 12 el exponente es igual a 2, mientras que en el 10 el exponente es 1. Por otra parte, el 3 y el 5 no son primos comunes. Comparemos estas factorizaciones con la del mínimo común múltiplo de *a* y *b*:

$$[a : b] = 60 = 2^2 \cdot 3 \cdot 5$$

Observamos que en 60 aparecen todos los primos, tanto los de *a* como los de *b*, y el 2, que es común a *a* y a *b*, está elevado al cuadrado, que es el exponente máximo con el que aparece en *a* y en *b*. Este hecho vale en general:

El mínimo común múltiplo es el producto de los primos comunes y no comunes elevados a su mayor exponente.

Ejemplo. Hallar todos los pares de naturales *a* y *b* tales que su mínimo común múltiplo sea igual a 60 y su máximo común divisor sea igual a 15.

Solución: sabemos que si *a* y *b* son los números buscados:

$$15 \mid a, \quad 15 \mid b, \quad a \mid 60 \quad \text{y} \quad b \mid 60$$

Es decir que, en particular, *a* y *b* pertenecen al conjunto de los divisores positivos de 60 = $2^2 \cdot 3 \cdot 5$, que son:

$$\mathcal{D}_{60} = \{1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60\}$$

Además, nos interesan sólo los que a la vez son múltiplos de 15, es decir que nuestros candidatos para *a* y *b* son:

$$15, \ 30 \ \text{y} \ 60$$

Entre ellos, hay que elegir los pares *a, b* tales que (*a* : *b*) = 15 y [*a* : *b*] = 60; esto implica que uno de ellos debe ser impar, y el otro debe ser divisible por 4. Luego las soluciones son:

$$a = 15 \text{ y } b = 60 \quad \text{o} \quad a = 60 \text{ y } b = 15$$

Ejemplo. Determinar todos los naturales n tales que el mínimo común múltiplo de n y 130 sea igual a 260.

Solución: Sea n un número que cumple la condición, entonces:

$$\begin{aligned}[n : 130] &= 260 \\ &= 2^2 \cdot 5 \cdot 13\end{aligned}$$

Por definición de mínimo común múltiplo, n divide a $260 = 2^2 \cdot 5 \cdot 13$, luego en la factorización en primos de n solo pueden aparecer los primos 2, 5 y 13 y elevados a potencias que son a lo sumo las que aparecen en 260. Por lo tanto, n es de la forma:

$$n = 2^r \cdot 5^s \cdot 13^t \quad \text{con } 0 \le r \le 2,\ 0 \le s \le 1,\ 0 \le t \le 1$$

Notar que 2^2 es la máxima potencia de 2 que divide a $260 = [n : 130]$, mientras que la máxima potencia de 2 que divide a 130 es 2^1; en consecuencia, 2^2 debe aparecer en n. Por lo tanto, r, el exponente de 2 en n, debe ser 2, es decir:

$$n = 2^2 \cdot 5^s \cdot 13^t \quad \text{con } 0 \le s \le 1 \text{ y } 0 \le t \le 1$$

Analicemos caso por caso:

1. si $s = 0$ y $t = 0$, entonces $n = 2^2 = 4$, que cumple $[n : 130] = [4 : 130] = 260$;
2. si $s = 0$ y $t = 1$, entonces $n = 2^2 \cdot 13 = 52$, que cumple $[n : 130] = [52 : 130] = 260$;
3. si $s = 1$ y $t = 0$, entonces $n = 2^2 \cdot 5 = 20$, que cumple $[n : 130] = [20 : 130] = 260$;
4. si $s = 1$ y $t = 1$, entonces $n = 2^2 \cdot 5 \cdot 13 = 260$, que cumple $[n : 130] = [260 : 130] = 260$;

por lo tanto, los n que verifican $[n : 130] = 260$ son $n = 4$, $n = 20$, $n = 52$ y $n = 260$.

Ejemplo. Hallar todos los pares de naturales a y b tales que su máximo común divisor sea igual a 10 y su mínimo común múltiplo sea igual a 1.500.

Solución: Sabemos que si a y b son los números buscados, entonces:

$$a \cdot b = (a : b) \cdot [a : b] = 10 \cdot 1.500 = 15.000$$

Como además $15.000 = 3 \cdot 5 \cdot 10^3 = 3 \cdot 5 \cdot (2 \cdot 5)^3 = 2^3 \cdot 3 \cdot 5^4$ es la factorización en primos del producto de a por b, tenemos que a y b deben tener en sus descomposiciones a estos y solo a estos primos, y en el producto de a y b los exponentes de 2, 3 y 5 deben ser los de la descomposición de 15.000, o sea:

$$a = 2^r \cdot 3^s \cdot 5^t \quad \text{y} \quad b = 2^{3-r} \cdot 3^{1-s} \cdot 5^{4-t} \quad \text{con } 0 \le r \le 3,\ 0 \le s \le 1,\ 0 \le t \le 4$$

Sólo nos queda averiguar las restricciones para los exponentes de estos primos en las factorizaciones de a y de b.

El hecho de que $(a : b) = 10$ implica que los primos 2 y 5 deben aparecer como mínimo una vez en a y en b, pero no pueden estar elevados al cuadrado o a potencias mayores en ambos. Notar que si $t = 2$, tanto en a como en b, el 5 aparecería elevado al cuadrado. Por lo tanto, las posibilidades para los exponentes son:

$$1 \leq r \leq 2, \quad 0 \leq s \leq 1, \quad 1 \leq t \leq 3, \ t \neq 2$$

Analicemos caso por caso:

1. si $r = 1$ y $s = 0$, $t = 1$ entonces $a = 2 \cdot 5 = 10$ y $b = 2^2 \cdot 3 \cdot 5^3 = 1.500$;
2. si $r = 1$ y $s = 1$, $t = 1$ entonces $a = 2 \cdot 3 \cdot 5 = 30$ y $b = 2^2 \cdot 5^3 = 500$;
3. si $r = 1$ y $s = 0$, $t = 3$ entonces $a = 2 \cdot 5^3 = 250$ y $b = 2^2 \cdot 3 \cdot 5^3 = 60$;
4. si $r = 1$ y $s = 1$, $t = 3$ entonces $a = 2 \cdot 3 \cdot 5^3 = 750$ y $b = 2^2 \cdot 5^3 = 20$;

y los pares obtenidos en estos cuatro casos cumplen que $(a : b) = 10$ y $[a : b] = 1.500$.

Los casos restantes coinciden con los anteriores, intercambiando el orden de a y b. Por lo tanto, los pares (a, b), soluciones a nuestro problema, son:

$$(10, 1.500), \ (20, \ 750), \ (30, \ 500), \ (60, \ 250)$$

3. Aritmética modular

□ 1. Ecuaciones diofánticas

Los alumnos de la Escuela 314 hacen una colecta para reunir fondos para ayudar a una escuela de frontera. Para esto, ofrecen bonos contribución de dos tipos: bonos de $15 y bonos de $8.

Martín se lleva un piloncito de bonos de $15 y otro de bonos de $8. Después de vender varios bonos recaudó $100, pero no recuerda cuántos bonos vendió de cada clase (ni sabe cuántos bonos tenía cada uno de sus piloncitos al comienzo). ¿Puede Martín determinar cuántos bonos vendió de cada tipo?

Para tratar de determinar estas cantidades, Martín observa que:

- si no hubiera vendido ningún bono de $15, los $100 provendrían de vender bonos de $8; es decir, si vendió una cantidad y de bonos de $8 sería $100 = $8 · y, pero esto no puede ser porque 100 no es múltiplo de 8;
- si hubiera vendido un solo bono de $15, entonces los $100 - $15 = $85 restantes provendrían de vender bonos de $8, pero 85 tampoco es múltiplo de 8;
- si hubiera vendido 2 bonos de $15, los $100 - 2 · $15 = $70 restantes provendrían de vender bonos de $8, pero 70 no es múltiplo de 8;
- no puede ser que haya vendido 3 bonos de $15, porque $100 - 3·$15 = $55 y 55 tampoco es múltiplo de 8;
- es posible que haya vendido 4 bonos de $15, ya que $100 - 4 · $15 = $40 = 5 · $8. Esto significa que además habría vendido 5 bonos de $8;
- razonando de la misma manera deduce que no puede ser que haya vendido ni 5 ni 6 bonos de $15. Además, seguro que no vendió más de 7 de estos bonos, pues 7 · $15 = $105 y sólo recaudó $100.

Martín concluye entonces que los $100 fueron recaudados mediante la venta de 4 bonos de $15 y 5 bonos de $8.

Podemos plantear el problema de Martín mediante una igualdad de números enteros: si Martín vendió x bonos de $15 e y bonos de $8, entonces la cantidad de dinero que recaudó es:

$$15 \cdot x + 8 \cdot y = 100$$

Esto es, las cantidades de bonos de cada tipo $x, y \in \mathbb{N}_0$ que puede haber vendido Martín son las soluciones en los números enteros no negativos para esta ecuación. A continuación vamos a ver cómo es posible resolver este tipo de ecuaciones sistemáticamente.

Más precisamente, *dados a, b, c ∈ ℤ, con a y b no nulos, nos interesa hallar las soluciones en los números enteros de la ecuación:*

$$a \cdot x + b \cdot y = c \tag{2}$$

es decir, los pares $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ para los cuales se cumple la igualdad.

Estas ecuaciones son una clase particular de las que se conocen como ecuaciones diofánticas[4], que son ecuaciones con coeficientes enteros de las que se buscan soluciones en el conjunto de los números enteros.

Una ecuación de este tipo no siempre tiene solución; por ejemplo, la ecuación $12 \cdot x + 14 \cdot y = 123$ no tiene solución, porque para todo par de números $x, y \in \mathbb{Z}$, el resultado de $12 \cdot x + 14 \cdot y$ es un entero par:

$$12 \cdot x + 14 \cdot y = 2 \cdot (6 \cdot x + 7 \cdot y)$$

mientras que 123 es impar.

De la misma manera que en el ejemplo, vemos que si $d \in \mathbb{Z}$ es un divisor común de a y b, tenemos que $d \mid a \cdot x + b \cdot y$ para cualesquiera $x, y \in \mathbb{Z}$. Entonces, si $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ es una solución de la ecuación (2), resulta que $d \mid c$. Esto nos dice que para que la ecuación (2) tenga soluciones es necesario que todo divisor común de a y b sea también divisor de c.

Esta última condición es a su vez equivalente a que $(a : b)$ divida a c. En efecto, si todo divisor común de a y b divide a c, en particular lo divide su máximo común divisor $(a : b)$. Recíprocamente, si $(a : b)$ divide a c, como cualquier divisor común de a y b divide a $(a : b)$, por la transitividad de la divisibilidad, también divide a c.

Concluimos que:

> Si $(a : b) \nmid c$, la ecuación $a \cdot x + b \cdot y = c$ no tiene soluciones en $\mathbb{Z}$.

Analicemos ahora en detalle un ejemplo en el que $(a : b) \mid c$.

Ejemplo. Consideremos la ecuación $50 \cdot x + 630 \cdot y = 10$. Como vimos en la sección 5 del capítulo 2, esta ecuación tiene solución, ya que $10 = (50 : 630)$ es combinación lineal entera de 50 y 630:

$$50 \cdot (-25) + 630 \cdot 2 = 10$$

es decir $(x, y) = (-25, 2)$ es una solución.

A partir de esta solución podemos ver, por ejemplo, que la ecuación $50 \cdot x + 630 \cdot y = 20$ también tiene solución. Para obtener como resultado el doble de 10, basta duplicar los valores de x e y (o lo que es lo mismo, multiplicar por 2 la igualdad anterior):

$$50 \cdot (-25) \cdot 2 + 630 \cdot 2 \cdot 2 = 10 \cdot 2$$

[4] El nombre se debe a Diofanto de Alejandría, matemático del siglo III que las estudió en su obra Aritmética.

o sea, que $(x, y) = ((-25) \cdot 2, 2 \cdot 2) = (-50, 4)$ es solución de esta nueva ecuación. De la misma manera, para cualquier $q \in \mathbb{Z}$ resulta que la ecuación $50 \cdot x + 630 \cdot y = 10 \cdot q$ tiene como solución a $(x, y) = (-25 \cdot q, 2 \cdot q)$, ya que:

$$50 \cdot (-25) \cdot q + 630 \cdot 2 \cdot q = 10 \cdot q$$

En general, sabemos que para cualesquiera $a, b \in \mathbb{Z}$ no simultáneamente nulos, $(a : b)$ es combinación lineal entera de a y b, es decir, existen números enteros s y t tales que:

$$a \cdot s + b \cdot t = (a : b)$$

Esto nos dice que la ecuación $a \cdot x + b \cdot y = (a : b)$ siempre tiene solución. Más aún, a partir de la igualdad de arriba vemos que, si $c = (a : b) \cdot q$, la ecuación (2) tiene como una solución a $(x, y) = (s \cdot q, t \cdot q)$, ya que:

$$a \cdot \underbrace{s \cdot q}_{x} + b \cdot \underbrace{t \cdot q}_{y} = (a \cdot s + b \cdot t) \cdot q = (a : b) \cdot q$$

Tenemos entonces también que:

> Si $(a : b) \mid c$, la ecuación $a \,.\, x + b \,.\, y = c$ tiene soluciones en $\mathbb{Z}$.

Resumiendo, hemos probado la siguiente proposición:

Proposición 3.1. *Sean $a, b, c \in \mathbb{Z}$ con a y b no nulos. La ecuación diofántica $a \cdot x + b \cdot y = c$ tiene soluciones en $\mathbb{Z}$ si y solo si $(a : b)$ divide a c.*

Veamos cómo son **todas** las soluciones de (2) cuando $(a : b)$ divide a c. En primer lugar, podemos dividir ambos miembros de (2) por $(a : b)$, obteniendo la nueva ecuación:

$$\frac{a}{(a : b)} \cdot x + \frac{b}{(a : b)} \cdot y = \frac{c}{(a : b)}$$

Esta ecuación tiene las mismas soluciones en $\mathbb{Z} \times \mathbb{Z}$ que la original (se puede pasar de una ecuación a la otra simplemente multiplicando o dividiendo por $(a : b)$). Si llamamos $\alpha = \frac{a}{(a:b)}$, $\beta = \frac{b}{(a:b)}$ y $\gamma = \frac{c}{(a:b)}$, que son enteros, nos queda la ecuación:

$$\alpha \cdot x + \beta \cdot y = \gamma$$

donde ahora $(\alpha : \beta) = 1$ (observar que α y β son coprimos porque hemos suprimido todos los factores comunes de a y b). Supongamos que (x_0, y_0) es una solución de esta ecuación. Si (x, y) es otra solución, vale que $\alpha \cdot x + \beta \cdot y = \gamma = \alpha \cdot x_0 + \beta \cdot y_0$; entonces:

$$\alpha \cdot (x - x_0) = -\beta \cdot (y - y_0)$$

De esta igualdad deducimos que $\beta \mid \alpha \cdot (x - x_0)$ y, como $(\alpha : \beta) = 1$, entonces $\beta \mid x - x_0$ (ver la Proposición 2.4 del capítulo 2); luego, existe $k \in \mathbb{Z}$ tal que $x - x_0 = k \cdot \beta$. Reemplazando en la igualdad de arriba, nos queda que $\alpha \cdot k \cdot \beta = -\beta \cdot (y - y_0)$, de donde se desprende que $y - y_0 = -\alpha \cdot k$. En conclusión, toda solución (x, y) de la ecuación diofántica considerada es

de la forma $x = x_0 + k \cdot \beta$, $y = y_0 - k \cdot \alpha$, con $k \in \mathbb{Z}$.

Teorema 3.2. *Sean $a, b, c \in \mathbb{Z}$, con a y b no nulos. Si $(a : b) \mid c$, entonces las soluciones de la ecuación diofántica $a \cdot x + b \cdot y = c$ son los pares $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ tales que*

$$x = x_0 + k \cdot \frac{b}{(a : b)}, \quad y = y_0 - k \cdot \frac{a}{(a : b)}, \quad \text{con } k \in \mathbb{Z}$$

donde (x_0, y_0) es una solución particular de la ecuación.

Ejemplo. Volvamos al problema planteado al comienzo de esta sección: Martín vendió x bonos de \$15 e y bonos de \$8, y busca determinar los valores de x e y sabiendo que recaudó \$100, es decir, que:

$$15 \cdot x + 8 \cdot y = 100$$

Como $(15 : 8) = 1$, sabemos que la ecuación tiene soluciones. Comenzaremos buscando todas las soluciones en $\mathbb{Z} \times \mathbb{Z}$, y luego determinaremos las soluciones en $\mathbb{N}_0 \times \mathbb{N}_0$, que son las que le interesan a Martín.

En primer lugar, escribimos $1 = (15 : 8)$ como combinación lineal entera de 15 y 8. Para esto, utilizamos la información dada por el algoritmo de Euclides:

$$\begin{array}{rcl@{\qquad}rcl} 15 &=& 1 \cdot 8 + 7 & \longrightarrow & 7 &=& 15 - 1 \cdot 8 \\ 8 &=& 1 \cdot 7 + 1 & \longrightarrow & 1 &=& 8 - 1 \cdot 7 \\ 7 &=& 7 \cdot 1 & & &=& 8 - 1 \cdot (15 - 1 \cdot 8) \\ & & & & &=& 15 \cdot (-1) + 8 \cdot 2 \end{array}$$

Ahora tomamos la identidad obtenida:

$$15 \cdot (-1) + 8 \cdot 2 = 1$$

y la multiplicamos por 100 para conseguir una solución de la ecuación original:

$$\begin{aligned} 15 \cdot (-1) \cdot 100 + 8 \cdot 2 \cdot 100 &= 100 \\ 15 \cdot (-100) + 8 \cdot 200 &= 100 \end{aligned}$$

Tenemos así una solución particular de la ecuación: $(x_0, y_0) = (-100, 200)$.

Por el Teorema 3.2, todas las soluciones enteras de la ecuación $15 \cdot x + 8 \cdot y = 100$ son los pares $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ donde:

$$x = -100 + k \cdot 8, \quad y = 200 - k \cdot 15, \quad \text{con } k \in \mathbb{Z}$$

Finalmente, nos interesan aquellas soluciones en las cuales $x \geq 0$ e $y \geq 0$:

$$\begin{aligned} x \geq 0 &\iff -100 + k \cdot 8 \geq 0 \iff k \cdot 8 \geq 100 \iff k \geq 13 \quad (\text{porque } k \in \mathbb{Z}) \\ y \geq 0 &\iff 200 - k \cdot 15 \geq 0 \iff 200 \geq k \cdot 15 \iff 13 \geq k \quad (\text{porque } k \in \mathbb{Z}) \end{aligned}$$

De estas desigualdades deducimos que la única solución $(x, y) \in \mathbb{N}_0 \times \mathbb{N}_0$ se obtiene para $k = 13$:

$$x = -100 + 13 \cdot 8\,, \qquad y = 200 - 13 \cdot 15$$
$$= 4 \qquad\qquad = 5$$

con lo cual, si recaudó $100, Martín tiene que haber vendido 4 bonos de $15 y 5 bonos de $8.

Ejercicio 3.1. Hallar todas las soluciones enteras de la ecuación $84 \cdot x + 270 \cdot y = 66$

□ 2. Congruencias

En esta sección vamos a presentar una noción de congruencia[5] en el conjunto $\mathbb{Z}$, que resulta muy útil a la hora de trabajar con propiedades de divisibilidad sobre los números enteros.

Dado $m \in \mathbb{N}$, decimos que $a, b \in \mathbb{N}$ son *congruentes módulo m*, y escribimos $a \equiv b \pmod{m}$ o simplemente $a \equiv_{(m)} b$, si $m \mid a - b$. Si a y b no son congruentes módulo m, escribimos $a \not\equiv b \pmod{m}$.

Por ejemplo,

- $11 \equiv 5 \pmod 3$, pues $3 \mid 11 - 5 = 6$,
- $11 \not\equiv -2 \pmod 4$, pues $4 \nmid 11 - (-2) = 13$,
- $a \equiv b \pmod 1$ para cualesquiera $a, b \in \mathbb{Z}$, ya que todo número entero es múltiplo de 1.

Observemos que, cualquiera sea $m \in \mathbb{N}$, tenemos que:

$$a \equiv 0 \pmod m \iff m \mid a.$$

Antes de continuar, analicemos más en detalle el caso $m = 2$.

Tenemos que $a \equiv b \pmod 2$ si y sólo si $2 \mid a - b$. Si a es par, entonces $a = 2 \cdot \alpha$ para algún $\alpha \in \mathbb{Z}$, con lo cual $a - b = 2 \cdot \alpha - b$ es múltiplo de 2 si y sólo si b lo es, o sea, si y sólo si b es par. De la misma manera, si a es impar vemos que $2 \mid a - b$ si y sólo si b también es impar. En otras palabras:

$$a \equiv b \pmod 2 \iff a \text{ y } b \text{ son ambos pares o ambos impares.}$$

Esto nos dice que la congruencia módulo 2 *parte* al conjunto de los números enteros en dos subconjuntos: el de los enteros pares y el de los enteros impares. En cada uno de estos subconjuntos, dos elementos cualesquiera están relacionados, y un elemento de uno de estos conjuntos no está relacionado con uno del otro (es decir, un entero par es congruente a todo entero par y no es congruente a ningún impar, y un entero impar es congruente a cualquier impar, pero a ningún par). Podemos formalizar esto, mediante el concepto de relación de equivalencia.

Para $m \in \mathbb{N}$ fijo, consideremos la relación $\mathcal{R}$ en $\mathbb{Z}$ definida por

$$a \mathcal{R} b \iff a \equiv b \pmod m$$

[5] Esta noción fue introducida por Carl Friedrich Gauss en su libro Disquisitiones Arithmeticae publicado en 1801.

Esta relación satisface:

i) $\mathcal{R}$ es reflexiva: $a \equiv a$ (mód m) para todo $a \in \mathbb{Z}$, ya que $m \mid a - a = 0$.
ii) $\mathcal{R}$ es simétrica: si $a \equiv b$ (mód m), entonces $m \mid a - b = -(b - a)$, con lo que también vale que $m \mid b - a$, es decir, que $b \equiv a$ (mód m).
iii) $\mathcal{R}$ es transitiva: si $a\mathcal{R}b$ y $b\mathcal{R}c$, es porque $m \mid a - b$ y $m \mid b - c$; pero entonces $m \mid (a - b) + (b - c) = a - c$, lo que dice que $a \equiv c$ (mód m).

Por lo tanto, $\mathcal{R}$ es una relación de equivalencia. Como vimos en la sección 3 del capítulo 0, $\mathcal{R}$ nos da una partición del conjunto $\mathbb{Z}$ en subconjuntos disjuntos – las clases de equivalencia– tales que, dentro de cada uno de ellos, dos elementos cualesquiera están relacionados (en nuestro caso, son congruentes módulo m) y dos elementos de subconjuntos distintos no están relacionados.

Como vimos anteriormente, para $m = 2$ la relación de congruencia parte al conjunto $\mathbb{Z}$ en 2 subconjuntos, $\{a \in \mathbb{Z} \mid a \text{ es par}\}$ y $\{a \in \mathbb{Z} \mid a \text{ es impar}\}$. El primero de ellos es la clase de equivalencia [0] y el segundo, es la clase de equivalencia [1]. En el caso general, fijado $m \in \mathbb{N}$, la relación de congruencia módulo m parte al conjunto de los números enteros en m clases de equivalencia. La siguiente propiedad de la congruencia nos dice cómo son estas m clases.

Proposición 3.3. *Sea $m \in \mathbb{N}$. Para cada $a \in \mathbb{Z}$, si r es el resto de la división de a por m, vale $a \equiv r$ (mód m). Más aún, este resto es el único entero r tal que $0 \leq r < m$ que es congruente con a módulo m.*

Demostración. Si r es el resto de la división de a por m, existe un entero q tal que $a = m \cdot q + r$. Entonces $a - r = m \cdot q$, con lo que $m \mid a - r$ y, por lo tanto, $a \equiv r$ (mód m).

Por otro lado, si $a \equiv r$ (mód m), sabemos que $m \mid a - r$. Entonces existe $q \in \mathbb{Z}$ tal que $a - r = m \cdot q$; luego $a = m \cdot q + r$. Si vale $0 \leq r < m$, por la unicidad en el algoritmo de división, r es el resto de la división de a por m.

Como consecuencia de este resultado, fijado $m \in \mathbb{N}$, dos enteros distintos r_1 y r_2 con $0 \leq r_1, r_2 < m$ no son congruentes módulo m, es decir, las clases de equivalencia $[r_1]$ y $[r_2]$ son distintas. Además, todo entero a resulta congruente a su resto r en la división por m, y entonces $a \in [r]$. Luego, el conjunto de los enteros se parte como sigue:

$$\mathbb{Z} = [0] \cup [1] \cup \cdots \cup [m-1]$$

Volveremos sobre esta propiedad importante de la congruencia en la sección 4.

Algunas propiedades fundamentales de la congruencia son las siguientes:

Propiedades 3.4. Sea $m \in \mathbb{N}$. Entonces:

1. si $a_1 \equiv b_1$ (mód m) *y* $a_2 \equiv b_2$ (mód m), entonces $a_1 + a_2 \equiv b_1 + b_2$ (mód m);
2. si $a \equiv b$ (mód m), entonces $c \cdot a \equiv c \cdot b$ (mód m) para todo $c \in \mathbb{Z}$;

3. si $a_1 \equiv b_1 \pmod{m}$ y $a_2 \equiv b_2 \pmod{m}$, entonces $a_1 \cdot a_2 \equiv b_1 \cdot b_2 \pmod{m}$;
4. si $a \equiv b \pmod{m}$, entonces $a^k \equiv b^k \pmod{m}$ para todo $k \in \mathbb{N}$;
5. si $c \cdot a \equiv c \cdot b \pmod{m}$ y $(c : m) = 1$, entonces $a \equiv b \pmod{m}$;
6. si $d \mid m$ y $a \equiv b \pmod{m}$, entonces $a \equiv b \pmod{d}$.

Demostración. Para demostrar estas propiedades se usan básicamente las propiedades de la divisibilidad vistas en el capítulo 2.

1. Por la definición de congruencia, tenemos que $m \mid a_1 - b_1$ y $m \mid a_2 - b_2$. Entonces, $m \mid (a_1 - b_1)+(a_2 - b_2) = (a_1 + a_2) - (b_1 + b_2)$; luego, $a_1 + a_2 \equiv b_1 + b_2 \pmod{m}$.
2. Tenemos que $m \mid a - b$, entonces también $m \mid c \cdot (a - b) = c \cdot a - c \cdot b$, con lo que $c \cdot a \equiv c \cdot b \pmod{m}$.
3. Por la propiedad anterior, como $a_1 \equiv b_1 \pmod{m}$, multiplicando por a_2, resulta que $a_1 \cdot a_2 \equiv b_1 \cdot a_2 \pmod{m}$; análogamente, multiplicando por b_1 la congruencia $a_2 \equiv b_2 \pmod{m}$, obtenemos que $b_1 \cdot a_2 \equiv b_1 \cdot b_2 \pmod{m}$ y finalmente, por la transitividad, concluimos que $a_1 \cdot a_2 \equiv b_1 \cdot b_2 \pmod{m}$.
4. Se prueba por inducción aplicando la propiedad 3.
5. Por hipótesis, $m \mid c \cdot a - c \cdot b = c \cdot (a - b)$. Y como c y m son coprimos, por la Proposición 2.4 del capítulo 2, resulta que $m \mid a - b$, es decir, que $a \equiv b \pmod{m}$.
6. Como $d \mid m$ y $m \mid a - b$, la transitividad de la divisibilidad implica que $d \mid a - b$, o sea que $a \equiv b \pmod{d}$.

Ejemplo. Veamos, utilizando la noción de congruencia y sus propiedades, que si $a, b, c \in \mathbb{Z}$ son tales que $a^2 + b^2 = c^2$, entonces $3 \mid a$ o $3 \mid b$.

Si 3 no divide a a ni a b, entonces tanto a como b tienen resto 1 ó 2 en la división por 3. Ahora bien, $1^2 = 1 \equiv_{(3)} 1$ y $2^2 = 4 \equiv_{(3)} 1$. Entonces, por la propiedad 4 anterior, tenemos que $a^2 \equiv 1 \pmod{3}$ y $b^2 \equiv 1 \pmod{3}$; luego, por la propiedad 1,

$$\begin{aligned} a^2 + b^2 &\equiv 1 + 1 \pmod{3} \\ &\equiv 2 \pmod{3} \end{aligned}$$

Esto implica que $c \in \mathbb{Z}$ debería cumplir que:

$$c^2 \equiv 2 \pmod{3}$$

Pero esto no puede ocurrir, puesto que si $c \equiv 0 \pmod{3}$, entonces $c^2 \equiv 0 \pmod{3}$ y, al igual que antes, si $c \equiv 1$ ó $2 \pmod{3}$, entonces $c^2 \equiv 1 \pmod{3}$.

Ejemplo. Calcular la cifra de las unidades en el desarrollo decimal de 33^{666}.

Calculando las primeras potencias de 33:

$$\begin{aligned} 33^0 &= \underline{1} \\ 33^1 &= 3\underline{3} \\ 33^2 &= 1.08\underline{9} \\ 33^3 &= 35.93\underline{7} \\ 33^4 &= 1.185.92\underline{1} \\ 33^5 &= 39.135.39\underline{3} \\ \dots &\quad \dots \quad \dots \end{aligned}$$

vemos que las cifras de las unidades son 1, 3, 9, 7, 1, 3, ... Uno podría conjeturar que seguirá siempre así, repitiéndose la secuencia 1, 3, 9, 7 sucesivamente y, a partir de esto, tratar de determinar la cifra de las unidades pedidas.

Para formalizar esta idea utilizaremos congruencias. La observación fundamental es que si el desarrollo decimal de 33^{666} es $(n_s \ldots n_1 n_0)_{10}$, entonces:

$$\begin{aligned} 33^{666} &= n_s \cdot 10^s + \cdots + n_1 \cdot 10 + n_0 \\ &= 10 \cdot (n_s \cdot 10^{s-1} + \cdots + n_1) + n_0 \quad \text{y} \quad 0 \leq n_0 < 10 \end{aligned}$$

de donde deducimos que la cifra n_0 de las unidades es el *resto del número en la división por 10*. Para hallarlo, aplicaremos el resultado visto en la Proposición 3.3, o sea, buscaremos el único entero n_0 con $0 \leq n_0 < 10$ tal que $33^{666} \equiv n_0 \pmod{10}$.

Según los cálculos hechos al comienzo:

$$33^4 \equiv 1 \pmod{10}$$

Entonces, por la propiedad 4 de las Propiedades 3.4, para todo $k \in \mathbb{N}$, vale:

$$(33^4)^k \equiv 1^k \pmod{10}, \quad \text{o sea,} \quad 33^{4 \cdot k} \equiv 1 \pmod{10}$$

Dividamos entonces al exponente 666 por 4: como $666 = 4 \cdot 166 + 2$, deducimos que:

$$\begin{aligned} 33^{666} &= 33^{4 \cdot 166 + 2} \\ &= 33^{4 \cdot 166} \cdot 33^2 \\ &\equiv_{(10)} 1 \cdot 9 \\ &= 9 \end{aligned}$$

donde la congruencia es consecuencia de la propiedad 3 de las Propiedades 3.4. En consecuencia, la cifra de las unidades en el desarrollo decimal de 33^{666} es 9.
Observemos que, aplicando estas mismas propiedades, podemos determinar la cifra de las unidades de 33^n para $n \in \mathbb{N}$ arbitrario: dado $n \in \mathbb{N}$, por el algoritmo de división, existen enteros k y r tales que $n = 4 \cdot k + r$ y $0 \leq r < 4$, con lo cual:

$$\begin{aligned} 33^n &= 33^{4 \cdot k + r} \\ &= \underbrace{33^{4 \cdot k}}_{\equiv_{(10)} 1} \cdot 33^r \\ &\equiv_{(10)} 33^r \end{aligned}$$

Concluimos entonces que la cifra de las unidades de 33^n coincide con la de 33^r, donde r es el resto de la división de n por 4; por lo tanto, de acuerdo a los cálculos hechos al comienzo, esta cifra es 1, 3, 9, 7 si $r = 0, 1, 2, 3$ respectivamente.

Como aplicación de las propiedades de la congruencia podemos deducir los conocidos *criterios de divisibilidad*. Comencemos analizando el criterio de divisibilidad por 9 que nos dice que *"un número natural n es múltiplo de 9 si y sólo si la suma de todos sus dígitos es múltiplo de 9"*. Observamos que si el desarrollo decimal de n es $(n_s \ldots n_1 n_0)_{10}$, entonces

$$n = n_s \cdot 10^s + \cdots + n_1 \cdot 10 + n_0$$

Queremos ver cuándo n es divisible por 9 o, equivalentemente, $n \equiv 0$ (mód 9). La clave para esto es observar que $10 \equiv 1$ (mód 9). Usando la propiedad 4 de las Propiedades 3.4, deducimos que $10^k \equiv 1$ (mód 9) para todo $k \in \mathbb{N}$ y, por lo tanto, de la escritura anterior de n, aplicando las propiedades 3 y 1, concluimos que:

$$\begin{aligned} n &= n_s \cdot 10^s + \cdots + n_1 \cdot 10 + n_0 \\ &\equiv_{(9)} n_s \cdot 1 + \cdots + n_1 \cdot 1 + n_0 \\ &= n_s + \cdots + n_1 + n_0 \end{aligned}$$

En definitiva:

$$\text{si } n = (n_s \dots n_1 n_0)_{10}, \quad \text{entonces} \quad n \equiv n_s + \cdots + n_1 + n_0 \pmod 9$$

con lo cual, los enteros n y $n_s + \dots + n_1 + n_0$ tienen el mismo resto en la división por 9 (o sea, para conocer el resto de un número natural en la división por 9, basta sumar sus dígitos y calcular el resto en la división por 9 del número obtenido). En particular, n es múltiplo de 9 si y solo si $n_s + \dots + n_1 + n_0$ lo es.

Ejercicio 3.2. Enunciar y probar la validez de los criterios de divisibilidad por 3, 4, 5, 8 y 11.

Sugerencias para la divisibilidad por 4 y 8: observar que $10^2 \equiv 0$ (mód 4) y que $10^3 \equiv 0$ (mód 8).

Sugerencias para la divisibilidad por 11: tener en cuenta que $10 \equiv -1$ (mód 11) y que $(-1)^k$ es 1 si k es par o -1 si k es impar. Proceder luego en forma análoga a lo que hicimos para analizar divisibilidad por 9.

Una aplicación de la congruencia: el ISSN de las publicaciones. El ISSN (*International Standard Serial Number*) es un número de ocho dígitos que se usa para identificar publicaciones periódicas, tanto impresas como electrónicas. Cada publicación periódica (por ejemplo, las revistas) tiene asignado un ISSN único.

Los siete primeros dígitos de los ISSN son asignados secuencialmente a las publicaciones, independientemente del país de origen, el idioma, etc. (es decir, el ISSN no contiene información en sí mismo).

El octavo dígito de un ISSN es un *dígito de control* y para determinarlo se utiliza aritmética modular: Si los primeros siete dígitos del ISSN son $d_1 d_2 d_3 d_4 d_5 d_6 d_7$, el octavo dígito d_8 se determina de manera que:

$$8 \cdot d_1 + 7 \cdot d_2 + 6 \cdot d_3 + 5 \cdot d_4 + 4 \cdot d_5 + 3 \cdot d_6 + 2 \cdot d_7 + d_8$$

sea múltiplo de 11. Para esto, se calcula $8 \cdot d_1 + 7 \cdot d_2 + 6 \cdot d_3 + 5 \cdot d_4 + 4 \cdot d_5 + 3 \cdot d_6 + 2 \cdot d_7$ módulo 11 y se elige d_8 convenientemente.

Por ejemplo, la revista *Journal of Algebra* tiene ISSN: 0021-8693. Esto significa que se le asignaron los 7 dígitos 0021869 y luego el dígito de control. Teniendo en cuenta que:

$$\begin{aligned} 8\cdot 0+7\cdot 0+6\cdot 2+5\cdot 1+4\cdot 8+3\cdot 6+2\cdot 9 &= 0+0+12+5+32+18+18\\ &\equiv_{(11)} 1+5+(-1)+7+7\\ &\equiv_{(11)} 8 \end{aligned}$$

Si elegimos $d_8 = 3$, resulta que:

$$\begin{aligned} 8+d_8 &= 11\\ &\equiv 0 \pmod{11}. \end{aligned}$$

Sin embargo, el dígito de control no siempre es un número entre 0 y 9. Por ejemplo, para la revista *Trends in Microbiology* se tiene que ISSN: 0966-842X. ¿A qué se debe la "X"? Procediendo como en el ejemplo anterior, se calcula:

$$\begin{aligned} 8\cdot 0+7\cdot 9+6\cdot 6+5\cdot 6+4\cdot 8+3\cdot 4+2\cdot 2 &= 63+36+30+32+12+4\\ &\equiv_{(11)} (-3)+3+8+(-1)+1+4\\ &\equiv_{(11)} 1 \end{aligned}$$

con lo cual, d_8 debe cumplir:

$$1+d_8 \equiv 0 \pmod{11}$$

Ahora bien, el menor número natural que verifica esta igualdad es $d_8 = 10$. Cuando esto sucede, el dígito de control se escribe "X".

□ 3. Ecuaciones de congruencia

Martín compró unas cajas de chocolates para repartir entre sus 19 compañeros de división de la Escuela 314. Como eran menos de 19 cajas, para darle la misma cantidad de chocolates a cada uno, las abrió y repartió el contenido entre sus compañeros. Luego de hacer esto, le quedaron 5 chocolates. Sabiendo que cada caja tenía 12 chocolates, ¿cuántas cajas repartió Martín?

Para responder esta pregunta, observemos que si Martín repartió una cantidad x de cajas de chocolates, entonces la cantidad total de chocolates repartidos es $12 \cdot x$. Al repartir estos chocolates entre sus 19 compañeros le quedaron 5. En términos de divisibilidad, esto significa que $12 \cdot x$ tiene resto 5 en la división por 19 y, en términos de congruencias, que:

$$12 \cdot x \equiv 5 \pmod{19}$$

Como sabemos que $1 \leq x < 19$, podemos determinar la cantidad x de cajas repartidas por Martín verificando, para cada posible valor de x, si esta condición se cumple o no.

- Si $x = 1$, serían $12 \cdot 1 = 12$ chocolates, y $12 \not\equiv 5$ (mód 19). Concluimos que Martín no repartió una sola caja.
- Si $x = 2$, serían $12 \cdot 2 = 24$ chocolates, y $24 \equiv 5$ (mód 19). Entonces es posible que Martín haya repartido 2 cajas de chocolates.
- Si $x = 3$, serían $12 \cdot 3 = 36$ chocolates, y $36 \equiv 17 \not\equiv 5$ (mód 19). Entonces, Martín no repartió 3 cajas.
- ...

Haciendo esta misma verificación para $x = 4, 5, \ldots, 17, 18$, se ve que en ningún otro caso la cantidad total de chocolates resulta tener resto 5 en la división por 19. Concluimos entonces que Martín repartió 2 cajas de chocolates entre sus compañeros.

Para resolver el problema anterior, lo que hicimos fue buscar un entero x que sea solución de la ecuación $12 \cdot x \equiv 5 \pmod{19}$. Teniendo en cuenta que el valor buscado estaba comprendido entre 1 y 18, nos bastó con verificar cada uno de estos 18 casos. Pero esta verificación puede resultar ser muy larga si las cantidades involucradas son más grandes.

En lo que sigue estudiaremos *ecuaciones lineales de congruencia*. Se trata de ecuaciones del tipo:

$$a \cdot x \equiv b \pmod{m}$$

donde $m \in \mathbb{N}$ y $a, b \in \mathbb{Z}$, $a \neq 0$, están fijos y $x \in \mathbb{Z}$ es la incógnita.

Comencemos resolviendo la ecuación que apareció en el problema de las cajas de chocolates de Martín.

Ejemplo. Hallar todos los $x \in \mathbb{Z}$ tales que $12 \cdot x \equiv 5 \pmod{19}$.

La condición $12 \cdot x \equiv 5 \pmod{19}$ es equivalente a que $19 \mid 12 \cdot x - 5$, es decir, a que exista $y \in \mathbb{Z}$ tal que:

$$12 \cdot x - 5 = 19 \cdot y$$

o, lo que es lo mismo, tal que:

$$12 \cdot x - 19 \cdot y = 5$$

Ahora, ésta es una ecuación diofántica como las que estudiamos en la sección 1 de este capítulo y que ya sabemos resolver. Procediendo como vimos allí, resulta que $(40, 25)$ es una solución de esta ecuación y luego, todas sus soluciones son los pares de números enteros (x, y) de la forma $(x, y) = (40 + 19 \cdot k, 25 + 12 \cdot k)$ con $k \in \mathbb{Z}$.

En particular, lo que nos interesa para nuestro problema es que x es de la forma $x = 40 + 19 \cdot k$, que podemos reescribir usando la notación de congruencias como $x \equiv 40 \pmod{19}$, o bien (teniendo en cuenta que $40 \equiv 2 \pmod{19}$), como:

$$x \equiv 2 \pmod{19}$$

Observemos que esta ecuación tiene una única solución módulo 19, es decir, que existe un único x_0 solución de la ecuación que satisface $0 \leq x_0 < 19$ (en este caso $x_0 = 2$).

En el caso general, se puede proceder de la misma manera para llevar una ecuación de congruencias a una ecuación diofántica; para $x \in \mathbb{Z}$, vale que:

$$\begin{aligned} a \cdot x \equiv b \pmod{m} &\iff m \mid a \cdot x - b \iff \text{existe } y \in \mathbb{Z} \text{ tal que } a \cdot x - b = m \cdot y \\ &\iff \text{existe } y \in \mathbb{Z} \text{ tal que } a \cdot x - m \cdot y = b \\ &\iff \text{existe } y \in \mathbb{Z} \text{ tal que } (x, y) \text{ es solución de } a \cdot x - m \cdot y = b \end{aligned}$$

Se resuelve la ecuación diofántica así obtenida y a partir de sus soluciones se obtienen, como en el ejemplo, las soluciones de la ecuación de congruencia original.

La equivalencia anterior entre ecuación de congruencia y ecuación diofántica nos provee un criterio para determinar cuándo una ecuación de congruencia tiene solución (ver en la Proposición 3.1 la condición que dedujimos para que la ecuación diofántica tenga soluciones):

$a \,.\, x \equiv b \pmod{m}$ tiene solución $\iff (a : m) \mid b$

En particular, *si a y m son coprimos*, la ecuación $a \cdot x \equiv b \pmod{m}$ tiene solución para todo $b \in \mathbb{Z}$. En este caso, las soluciones de la ecuación diofántica $a \cdot x - m \cdot y = b$ son de la forma $(x_0 + m \cdot k,\ y_0 + a \cdot k)$, donde (x_0, y_0) es una solución particular. Entonces las soluciones a la ecuación de congruencia son todos los x de la forma $x = x_0 + m \cdot k$ con $k \in \mathbb{Z}$, lo que podemos reescribir como:

$$x \equiv x_0 \pmod{m}$$

En el caso general, si $(a : m) \mid b$, las soluciones de $a \cdot x \equiv b \pmod{m}$ son las mismas que las de:

$$\frac{a}{(a : m)} \cdot x \equiv \frac{b}{(a : m)} \quad \left(\text{mód } \frac{m}{(a : m)}\right)$$

(Observar que ya vimos que las ecuaciones diofánticas asociadas a estas dos ecuaciones de congruencia tienen las mismas soluciones).

Ejemplo. Hallar todas las soluciones de la ecuación $24 \cdot x \equiv 10 \pmod{38}$.

Como $(24 : 38) = 2$ divide a 10, esta ecuación tiene soluciones en $\mathbb{Z}$. Para hallarlas, podemos resolver la ecuación de congruencia más simple que se obtiene dividiendo la ecuación dada por $2 = (24 : 38)$, es decir:

$$\frac{24}{2} \cdot x \equiv \frac{10}{2} \quad \left(\text{mód } \frac{38}{2}\right) \iff 12 \cdot x \equiv 5 \pmod{19}$$

Pero esta ecuación es la que resolvimos en el ejemplo anterior. Concluimos entonces que las soluciones de $24 \cdot x \equiv 10 \pmod{38}$ son los $x \in \mathbb{Z}$ tales que:

$$x \equiv 2 \pmod{19}$$

La ecuación planteada en el ejemplo que acabamos de resolver es una ecuación de congruencia módulo 38, mientras que la caracterización que dimos para sus soluciones es módulo 19, que es un *divisor* de 38. Esto ocurre en general: dada la ecuación de congruencia $a \cdot x \equiv b \pmod{m}$, si $(a : m) \mid b$, existe un único entero x_0, con $0 \leq x_0 < \frac{m}{(a:m)}$, tal que las soluciones de la ecuación son los enteros x que cumplen:

$$x \equiv x_0 \quad \left(\text{mód } \frac{m}{(a : m)}\right)$$

Ejercicio 3.3. Hallar, cuando existan, todas las soluciones a las siguientes ecuaciones lineales de congruencias:

(a) $17 \cdot x \equiv 20 \pmod{45}$
(b) $84 \cdot x \equiv 66 \pmod{270}$
(c) $28 \cdot x \equiv 30 \pmod{60}$

Ejercicio 3.4. Hallar todos los enteros a tales que el resto de dividir a $45 \cdot a$ por 27 es 9.

□ 4. El anillo de enteros módulo m

Como vimos en la sección 2 de este capítulo, la relación de congruencia módulo un número natural fijo m parte al conjunto de los enteros en m clases de equivalencia:

$$\mathbb{Z} = [0] \cup [1] \cup \cdots \cup [m-1]$$

donde, para cada $0 \leq r < m$, la clase $[r]$ contiene a todos los enteros que tienen resto r en la división por m.

Escribiremos el conjunto de clases de equivalencia en la congruencia módulo m como $\mathbb{Z}_m$, es decir:

$$\mathbb{Z}_m = \{[0], [1], \ldots, [m-1]\}$$

Gracias a las propiedades 3.4, en particular a las propiedades 1 y 3, a partir de la suma y producto de números enteros se pueden definir dos operaciones en $\mathbb{Z}_m$, suma y producto, de la siguiente forma:

$$[a] +_m [b] = [a+b]$$
$$[a] \cdot_m [b] = [a \cdot b]$$

Observemos que la propiedad "$a_1 \equiv a_2 \pmod{m}$, $b_1 \equiv b_2 \pmod{m} \Rightarrow a_1 + b_1 \equiv a_2 + b_2 \pmod{m}$" nos dice que el resultado de $[a]+_m[b]$ será el mismo sin importar qué elementos de las clases de equivalencia $[a]$ y $[b]$ consideremos para hacer la cuenta (y lo mismo nos dice la propiedad sobre el producto). En general, representamos cada clase de equivalencia módulo m por su único elemento comprendido entre 0 y m - 1 (como hicimos más arriba).

Por ejemplo:

$$\mathbb{Z}_6 = \{[0], [1], [2], [3], [4], [5]\}$$

Calculemos algunas sumas y productos en $\mathbb{Z}_6$.

- $[1] +_6 [3] = [1 + 3] = [4]$.
- $[2]+_6 [4] = [2+4] = [6] = [0]$. En consecuencia, $[4]$ es el inverso de $[2]$ para la suma en $\mathbb{Z}_6$.
- $[3] \cdot_6 [5] = [3 \cdot 5] = [15] = [3]$, ya que $15 \equiv 3 \pmod{6}$.
- $[5] \cdot_6 [5] = [25] = [1]$, ya que $25 \equiv 1 \pmod{6}$. Entonces, $[5]$ es inverso de sí mismo para el producto en $\mathbb{Z}_6$.

Podemos resumir las operaciones de suma y producto en $\mathbb{Z}_6$ por medio de las siguientes tablas:

$+_6$	[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]

$\cdot_6$	[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]

Veamos algunas propiedades que cumplen las operaciones de suma y producto en $\mathbb{Z}_m$. En primer lugar, observamos que la asociatividad y conmutatividad de la suma y el producto en $\mathbb{Z}$ hacen que $+_m$ y $\cdot_m$ sean también *asociativas* y *conmutativas.* Por ejemplo:

$$\begin{aligned} ([a] +_m [b]) +_m [c] &= [a+b] +_m [c] \\ &= [(a+b)+c] \\ &= [a+(b+c)] \\ &= [a] +_m [b+c] \\ &= [a] +_m ([b] +_m [c]) \end{aligned}$$

(Análogamente se puede ver que $\cdot_m$ es asociativa y que $+_m$ y $\cdot_m$ son conmutativas).

Las clase [0] es el elemento neutro de $+_m$ y [1] es el elemento neutro de $\cdot_m$. Por otra parte, todo elemento de $\mathbb{Z}_m$ tiene un inverso para $+_m$, ya que $[a]+_m[-a] = [0]$; es decir, $[-a]$ es el inverso aditivo de $[a]$. Observemos que, sin embargo, no es cierto que todo elemento de $\mathbb{Z}_m$ tenga inverso para $\cdot_m$.Por ejemplo, mirando la tabla de $\cdot_6$, es claro que [2] no tiene inverso para $\cdot_6$, puesto que $[2] \cdot_6 [a] \neq [1]$ para todo a.

Finalmente, al igual que ocurre en $\mathbb{Z}$, las operaciones $+_m$ y $\cdot_m$ están relacionadas mediante la propiedad *distributiva* del producto sobre la suma:

$$\begin{aligned} [a] \cdot_m ([b] +_m [c]) &= [a] \cdot_m ([b+c]) \\ &= [a \cdot (b+c)] \\ &= [a \cdot b + a \cdot c] \\ &= [a \cdot b] +_m [a \cdot c] \\ &= ([a] \cdot_m [b]) +_m ([a] \cdot_m [c]) \end{aligned}$$

Tenemos entonces que $\mathbb{Z}_m$ con las operaciones $+_m$ y $\cdot_m$ definidas arriba es un a*nillo conmutativo con unidad* [6] para cada $m \geq 2$.

Observación. El producto de números enteros tiene la propiedad de que si $a, b \in \mathbb{Z}$ y $a \cdot b = 0$, entonces $a = 0$ ó $b = 0$. Esto no ocurre en general en $\mathbb{Z}_m$: mirando la tabla de $\cdot_6$ vemos que, en $\mathbb{Z}_6$, $[2] \cdot_6 [3] = [0]$, pero $[2] \neq [0]$ y $[3] \neq [0]$. Más aún, para cada $m \in \mathbb{N}$ compuesto, si $m = m_1 \cdot m_2$ con $m_1 > 1$ y $m_2 > 1$, resulta que
$[m_1] \neq [0]$, $[m_2] \neq [0]$, pero $[m_1] \cdot_m [m_2] = [m_1 \cdot m_2] = [0]$.

[6] El nombre se debe a Diofanto de Alejandría, matemático del siglo III que las estudió en su obra Aritmética.

La propiedad vale en $\mathbb{Z}_p$ si p es primo, ya que $[a] \cdot_p [b] = [a \cdot b] = [0]$ si y sólo si $p \mid a \cdot b$, y esto ocurre si y sólo si $p \mid a$ o $p \mid b$, o sea, si y sólo si $[a] = [0]$ o $[b] = [0]$ en $\mathbb{Z}_p$.

Ejercicio 3.5. Escribir las tablas de suma y producto en $\mathbb{Z}_2$, $\mathbb{Z}_4$ y $\mathbb{Z}_7$.

La "prueba del 9". Una herramienta que puede utilizarse para detectar errores cuando se efectúan operaciones con números enteros utilizando su desarrollo decimal es la llamada *prueba del* 9.

La idea básica consiste en reemplazar cada número natural involucrado en las operaciones por un único dígito, hacer luego la cuenta original con estos dígitos, y comparar el dígito así obtenido con el asociado al resultado original. El dígito que se le asigna a un número natural se obtiene por medio del siguiente procedimiento:

1. se calcula la suma de los dígitos del número sin tener en cuenta los 9;
2. si el resultado obtenido es mayor o igual que 9, se vuelve a sumar sus dígitos sin considerar los 9;
3. se sigue así reemplazando un número por la suma de sus dígitos hasta obtener un único dígito que, si es 9, se reemplaza por 0.

Este procedimiento se basa en la propiedad *"Si* $n = (n_s \ldots n_1 n_0)_{10}$, *entonces* $n \equiv n_s + \ldots + n_1 + n_0$ (mód 9)*"*. Utilizando esta propiedad, no es difícil convencerse de que el dígito asociado a cada número es simplemente su resto en la división por 9 y, por lo tanto, representa la misma clase de equivalencia en $\mathbb{Z}_9$. Al efectuar la operación indicada con los dígitos obtenidos y volver a transformar el resultado en un dígito, no estamos haciendo otra cosa que calcular el resultado de la operación en $\mathbb{Z}_9$.

Por ejemplo, si hacemos la suma 192.545+258.672 y el resultado nos da 451.217, para ver si hay un error calculamos:

- $192.545 \longrightarrow 1 + 2 + 5 + 4 + 5 = 17 \longrightarrow 1 + 7 = 8$
- $258.672 \longrightarrow 2 + 5 + 8 + 6 + 7 + 2 = 30 \longrightarrow 3$

Ahora efectuamos la suma de los dígitos obtenidos para los sumandos: 8 + 3 = 11, reemplazamos el resultado por un único dígito $11 \longrightarrow 1+1 = \boxed{2}$ y lo comparamos con el dígito asociado a la suma:

- $451.217 \longrightarrow 4 + 5 + 1 + 2 + 1 + 7 = 20 \longrightarrow 2 + 0 = \boxed{2}$

De esta manera obtenemos:

$$\begin{array}{rrcl} & 192.545 & \longrightarrow & 8 \\ + & 258.672 & \longrightarrow & + \quad 3 \\ \hline & 451.217 & \longrightarrow \boxed{2} & = \boxed{2} \end{array}$$

Como en este caso el resultado era el correcto, ambos dígitos coinciden. Sin embargo, el hecho de que la igualdad de los dígitos se cumpla no significa que la cuenta esté bien;

por ejemplo:

$$\begin{array}{rrcrcr} + & 192.545 & \to & & + & 8 \\ & 258.672 & \to & & & 3 \\ \hline & 451.\underline{12}7 & \to & \boxed{2} & = & \boxed{2} \end{array}$$

Tiene dos dígitos del resultado con errores.

Ahora, si los dígitos obtenidos en la prueba del 9 difieren, podemos asegurar que ha ocurrido un error, ya que lo que estamos haciendo es calcular de dos maneras distintas la suma en $\mathbb{Z}_9$.

$$\begin{array}{rrcrcr} + & 192.545 & \to & & + & 8 \\ & 258.672 & \to & & & 3 \\ \hline & 451.117 & \to & \boxed{1} & \neq & \boxed{2} \end{array}$$

En este caso, el haber obtenido como resultados $1 \neq 2$ nos dice que hemos cometido un error (aunque no podemos saber en cuál de los dígitos).

Análogamente, podemos aplicar el procedimiento en el caso del producto de números naturales. Si multiplicamos, por ejemplo, 192.545 x 258.672 y obtenemos por resultado 49.807.100.240, podemos darnos cuenta de que hay un error de la siguiente manera: el dígito asociado a 192.545 es 8 y el asociado a 258.672 es 3; haciendo la operación con estos dígitos obtenemos:

$$8 \cdot 3 = 24 \longrightarrow 2 + 4 = \boxed{6}$$

mientras que, para el resultado de la cuenta original, tenemos que:

$$49.807.100.240 \longrightarrow 4 + 8 + 7 + 1 + 2 + 4 = 26 \longrightarrow 2 + 6 = \boxed{8}$$

Como los dígitos calculados no coinciden, concluimos que hubo un error en la cuenta. (De hecho, el resultado correcto de esta multiplicación es 49.806.000.240.)

□ 5. Ecuaciones en $\mathbb{Z}_m$

Las ecuaciones de congruencia que estudiamos en la sección 3 pueden reinterpretarse como ecuaciones en $\mathbb{Z}_m$, simplemente observando que:

$$a \cdot x \equiv b \pmod{m} \iff [a] \cdot_m [x] = [b] \text{ en } \mathbb{Z}_m.$$

En lo que sigue, si queda claro en el contexto, escribiremos simplemente a para representar al elemento $[a] \in \mathbb{Z}_m$ y dejaremos de escribir los subíndices en la suma y el producto de $\mathbb{Z}_m$, es decir, escribiremos + en lugar de $+_m$ y $\cdot$ en lugar de $\cdot_m$

Ahora la ecuación $[a] \cdot_m [x] = [b]$ queda simplemente:

$$a \cdot x = b \text{ en } \mathbb{Z}_m$$

que tiene una forma más familiar. ¿Cómo resolvemos esta ecuación? En la sección 3 vimos cómo hacer esto en el caso general (resolvimos la ecuación de congruencia). Lo que pretendemos aquí es mostrar un camino alternativo utilizando las operaciones en $\mathbb{Z}_m$.

La idea para "despejar" x en una ecuación del tipo $a \cdot x = b$ es "pasar dividiendo" el coeficiente a. Formalmente, esto significa *multiplicar ambos miembros* de la ecuación por el *inverso multiplicativo* de a:

Si a^{-1} es un elemento tal que:

$$\begin{aligned} a \cdot a^{-1} &= a^{-1} \cdot a \\ &= 1 \end{aligned}$$

entonces:

$$a^{-1} \cdot a \cdot x = a^{-1} \cdot b$$

O, equivalentemente:

$$x = a^{-1} \cdot b$$

Reemplazando este valor de x en la ecuación vemos que, en efecto, es una solución, ya que:

$$a \cdot (a^{-1} \cdot b) = (a \cdot a^{-1}) \cdot b = 1 \cdot b = b$$

Así, si queremos resolver, por ejemplo, la ecuación $5 \cdot x = 4$ en $\mathbb{Z}_7$, como $3 \cdot 5 = 1$ en $\mathbb{Z}_7$ (o sea, 3 es el inverso multiplicativo de 5 en $\mathbb{Z}_7$), tenemos que:

$$5 \cdot x = 4 \text{ en } \mathbb{Z}_7 \implies \underbrace{3 \cdot 5}_{=1} \cdot x = 3 \cdot 4 \text{ en } \mathbb{Z}_7 \implies x = 5 \text{ en } \mathbb{Z}_7$$

y ésta es la (única) solución de la ecuación en $\mathbb{Z}_7$.

Esto nos dice que cuando $a \in \mathbb{Z}_m$ tiene inverso multiplicativo $a^{-1} \in \mathbb{Z}_m$, la ecuación $a \cdot x = b$ tiene una única solución, $x = a^{-1} \cdot b$. En cambio, si $a \in \mathbb{Z}_m$ no tiene inverso multiplicativo, la ecuación $a \cdot x = b$ puede no tener soluciones o tener más de una solución. Por ejemplo, la ecuación $2 \cdot x = 1$ en $\mathbb{Z}_4$ no tiene solución, ya que es equivalente a la ecuación de congruencias $2 \cdot x \equiv 1$ (mód 4) y $(2 : 4) = 2$, que no divide a 1. Consideremos, por otro lado, la ecuación:

$$2 \cdot x = 2 \text{ en } \mathbb{Z}_4$$

A simple vista, deducimos que $x = 1 \in \mathbb{Z}_4$ es una solución de esta ecuación. Pero no es la única: $x = 3 \in \mathbb{Z}_4$ también lo es.

Ya vimos que, para un número natural m cualquiera, no todo elemento de $\mathbb{Z}_m$ tiene inverso multiplicativo. Por ejemplo: recién vimos que $2 \in \mathbb{Z}_4$ no tiene inverso multiplicativo. Tratemos de caracterizar los elementos que sí tienen inverso.

Sea $m \in \mathbb{N}$ fijo. Dado $a \in \mathbb{Z}_m$, un inverso multiplicativo para a en $\mathbb{Z}_m$ es un elemento $x \in \mathbb{Z}_m$ tal que:

$$a \cdot x = 1 \text{ en } \mathbb{Z}_m \text{ o, equivalentemente, } a \cdot x \equiv 1 \pmod{m}$$

Sabemos que esta última ecuación tiene solución si y sólo si $(a : m)$ divide a 1; pero para que esta condición valga, necesariamente debe ser $(a : m) = 1$. En definitiva:

$a \in \mathbb{Z}_m$ tiene inverso multiplicativo si y sólo si $(a : m) = 1$.

Por ejemplo:

- en $\mathbb{Z}_6$ los únicos elementos que tienen inverso multiplicativo son $a = 1$ y $a = 5$, ya que 1 y 5 son los únicos enteros comprendidos entre 0 y 5 que son coprimos con 6 (comparar con la tabla de $\cdot_6$ en la sección 4);
- todos los elementos de $\mathbb{Z}_7$, salvo el 0, tienen inverso multiplicativo, porque $(a : 7) = 1$ para todo $1 \leq a \leq 6$;
- en $\mathbb{Z}_8$, los elementos que tienen inverso multiplicativo son las clases de los números impares, es decir, 1, 3, 5 y 7.

Es claro que $0 \in \mathbb{Z}_m$ no puede tener inverso multiplicativo para ningún $m \geq 2$, puesto que $0 \cdot x = 0 \neq 1$ para cualquier $x \in \mathbb{Z}_m$. Pero, por ejemplo, en $\mathbb{Z}_7$, todo elemento $a \neq 0$ tiene inverso multiplicativo. Nos preguntamos, ¿cómo son los $m \in \mathbb{N}$ para los cuales todo elemento $a \in \mathbb{Z}_m$, $a \neq 0$, tiene inverso multiplicativo? Por lo que vimos antes, esto es equivalente a que $(a : m) = 1$ para todo a tal que $1 \leq a \leq m - 1$. Esto ocurre si m es *primo*: en este caso, los únicos divisores positivos de m son 1 y m, con lo cual, si $1 \leq a \leq m - 1$, el único posible divisor positivo común de a y m es 1; luego, $(a : m) = 1$. Por otro lado, si m no es primo, entonces m puede escribirse como un producto de dos números naturales menores que m, es decir, $m = a \cdot a'$ con $1 < a, a' < m$. Entonces $a \in \mathbb{Z}_m$ es no nulo y no tiene inverso multiplicativo, ya que $(a : m) = a \neq 1$.

Un anillo conmutativo con unidad en el que todo elemento no nulo tiene inverso multiplicativo se llama un *cuerpo*. El razonamiento anterior prueba que:

Teorema 3.5. *$\mathbb{Z}_m$ es un cuerpo si y sólo si $m \in \mathbb{N}$ es primo.*

Ejercicio 3.6.

1. Hallar los inversos multiplicativos de todos los elementos no nulos de $\mathbb{Z}_7$.
2. Determinar todos los elementos de $\mathbb{Z}_{14}$ que tienen inverso multiplicativo y hallar dichos inversos.

Volviendo a las ecuaciones lineales, el resultado anterior nos dice que, si m es primo y $a \neq 0 \in \mathbb{Z}_m$, la ecuación $a \cdot x = b$ tiene un única solución en $\mathbb{Z}_m$. Cuando m no es primo, la ecuación $a \cdot x = b$ tiene solución en $\mathbb{Z}_m$ si y sólo si $(a : m) \mid b$. En caso que esto ocurra, existe un único entero x_0 con $0 \leq x_0 < \frac{m}{(a:m)}$ tal que las soluciones son todos los enteros x que cumplen $x \equiv x_0 \pmod{\frac{m}{(a:m)}}$, es decir, los enteros de la forma $x = x_0 + k \cdot \frac{m}{(a:m)}$ con $k \in \mathbb{Z}$. No es difícil ver que:

$$x_0,\ x_0 + \frac{m}{(a:m)},\ x_0 + 2 \cdot \frac{m}{(a:m)}, \ldots,\ x_0 + ((a:m) - 1) \cdot \frac{m}{(a:m)}$$

pertenecen a clases de equivalencia distintas en $\mathbb{Z}_m$ y que cualquier otro entero de la forma $x_0 + k \cdot \frac{m}{(a:m)}$ pertenece a la clase de alguno de ellos. Concluimos que:

Si $(a : m) \mid b$, la ecuación $a \,.\, x = b$ tiene exactamente $(a : m)$ soluciones distintas en $\mathbb{Z}_m$, que son de la forma

$$x_0 + k \cdot \frac{m}{(a : m)} \quad \text{con } 0 \leq k < (a : m)$$

para algún x_0 tal que $0 \leq x_0 < \frac{m}{(a:m)}$

Ejercicio 3.7. Para cada una de las siguientes ecuaciones, determinar si tiene soluciones y, en caso afirmativo, hallarlas:

- $5 \cdot x = 4$ en $\mathbb{Z}_{14}$
- $6 \cdot x = 10$ en $\mathbb{Z}_{21}$
- $20 \cdot x = 12$ en $\mathbb{Z}_{24}$

□ 6. Teorema chino del resto

Lorena y sus amigas juegan al *Corazones*, que es un juego de cartas que se juega con un mazo de cartas francesas, sin los comodines (son 52 cartas). No vamos a entrar en los detalles del juego, simplemente diremos que al comienzo de cada mano de *Corazones* se reparten las cartas de manera que todos los jugadores tengan la misma cantidad (eventualmente pueden sobrar algunas).

En el caso de Lorena y sus amigas, aunque ellas no lo saben, al mazo de cartas con el que están jugando le faltan algunas cartas. En la primera mano juegan 5 de las amigas; Lorena reparte todas las cartas que puede y le sobran 2. En la mano siguiente, juegan 4 y sobran 3 cartas (estaban un poco distraídas y no se dieron cuenta de que esto no puede ser). Finalmente, juegan una última mano entre 3 de las amigas y al repartir las cartas sobran 2. En este momento Lorena, que no estaba jugando porque había salido última en la mano anterior, se da cuenta de que no puede ser que sobren 2 cartas (¿cómo lo supo?).

Lorena se pregunta cuántas cartas faltan en el mazo y decide intentar calcular este número sin interrumpir el juego (o sea, ¡sin contar las cartas!). Haciendo memoria sobre lo que ocurrió en las manos anteriores, razona como sigue:

Si x es la cantidad de cartas que hay en el mazo, entonces

$$\begin{cases} x \equiv 2 \pmod 5 \\ x \equiv 3 \pmod 4 \\ x \equiv 2 \pmod 3 \end{cases}$$

Como la cantidad de cartas es $x \leq 52$, por la condición $x \equiv 2 \pmod 5$, Lorena deduce que:

$$x \in \{2, \underline{7}, 12, 17, 22, \underline{27}, 32, 37, 42, \underline{47}, 52\}$$

De entre estos posibles valores, se queda con los que además cumplen que $x \equiv 3 \pmod 4$, es decir

$$x \in \{7, 27, \underline{47}\}$$

y de estos, busca los que cumplen que $x \equiv 2 \pmod 3$. El único valor con esta propiedad resulta ser:

$$x = 47$$

Lorena concluye que están jugando con 47 cartas, es decir, que faltan 5 en el mazo.

El problema general que trataremos en esta sección es el de la resolución de s*istemas de ecuaciones de congruencias.* Más precisamente, dados $m_1, m_2, \ldots, m_n \in \mathbb{N}$ y $a_1, a_2, \ldots, a_n \in \mathbb{Z}$, se busca hallar todos los $x \in \mathbb{Z}$ tales que:

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \quad \vdots \\ x \equiv a_n \pmod{m_n} \end{cases} \tag{3}$$

Un sistema de ecuaciones de este tipo no siempre tiene solución; por ejemplo, el sistema:

$$\begin{cases} x \equiv 1 \pmod 2 \\ x \equiv 4 \pmod 6 \end{cases}$$

no tiene soluciones. En efecto, la condición $x \equiv 4 \pmod 6$ implica que $x \equiv 4 \pmod 2$ (por la propiedad 6 de la Proposición 3.4). O sea, un entero x que satisface la segunda ecuación debe ser par. Pero la primera condición, $x \equiv 1 \pmod 2$, pide que x sea impar.

Una situación en la que podemos asegurar que el sistema de ecuaciones de congruencias sí tiene soluciones es cuando los módulos $m_1, \ldots, m_n$ son coprimos de a pares, es decir, si dos cualesquiera de ellos son coprimos.

Teorema 3.6 (Teorema chino del resto[7]). *Sean $m_1, m_2 \ldots, m_n \in \mathbb{N}$ coprimos de a pares, y sean $a_1, a_2, \ldots, a_n \in \mathbb{Z}$. Entonces existe un único $x_0 \in \mathbb{Z}$ con $0 \le x_0 < m_1 \cdot m_2 \ldots m_n$ que es solución del sistema de ecuaciones:*

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \quad \vdots \\ x \equiv a_n \pmod{m_n} \end{cases}$$

y, además, un entero x es solución de las ecuaciones si y sólo si:

$$x \equiv x_0 \pmod{m_1 \cdot m_2 \cdots m_n}$$

Demostración. *Existencia.* Haremos la demostración por inducción en n, la cantidad de ecuaciones del sistema. Para $n = 1$ no hay nada que hacer, ya que el sistema es en realidad una única ecuación de congruencia.

Supongamos que el enunciado vale para sistemas de n ecuaciones y consideremos un sistema de $n + 1$ ecuaciones:

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ \quad \vdots \\ x \equiv a_n \pmod{m_n} \\ x \equiv a_{n+1} \pmod{m_{n+1}} \end{cases}$$

[7] El origen de este teorema es un problema similar al que planteamos al comienzo de esta sección que aparece en el Manual Matemático escrito por Sun Zi alrededor del año 300. Un método para resolver este problema en el caso general fue dado en el Tratado de Matemática en Nueve Secciones, escrito por Qin Jiushao en 1247.

con $(m_i; m_j) = 1$ para todo $i \neq j$. Por la hipótesis inductiva, el sistema formado por las primeras n ecuaciones es equivalente a una única ecuación de congruencia:

$$x \equiv A \pmod{m_1 \cdots m_n}$$

para un (único) entero A con $0 \leq A < m_1 \ldots m_n$. Esto dice que los enteros x que cumplen las primeras n ecuaciones son aquéllos de la forma $x = M \cdot Q + A$ con $Q \in \mathbb{Z}$, donde $M = m_1 \ldots m_n$.

Las soluciones del sistema original son los x de esta forma que además cumplen la última ecuación; o sea $x = M \cdot Q + A$ para $Q \in \mathbb{Z}$ tal que $M \cdot Q + A \equiv a_{n+1} \pmod{m_{n+1}}$. Ahora, esta última condición es equivalente a la ecuación de congruencia:

$$M \cdot Q \equiv a_{n+1} - A \pmod{m_{n+1}}$$

Como por hipótesis $(m_i; m_{n+1}) = 1$ para cada $1 \leq i \leq n$, entonces $M = m_1 \ldots m_n$ resulta también coprimo con m_{n+1} y, por lo tanto, la ecuación anterior tiene solución. Más aún, las soluciones son de la forma:

$$Q \equiv q \pmod{m_{n+1}}$$

para un único q con $0 \leq q < m_{n+1}$, es decir, de la forma $Q = m_{n+1} \cdot k + q$ con $k \in \mathbb{Z}$. En definitiva, las soluciones del sistema son los $x \in \mathbb{Z}$ tales que:

$$\begin{aligned} x &= M \cdot Q + A \\ &= M \cdot (m_{n+1} \cdot k + q) + A \\ &= M \cdot m_{n+1} \cdot k + M \cdot q + A \\ &= (m_1 \cdots m_n \cdot m_{n+1}) \cdot k + (M \cdot q + A) \end{aligned}$$

Llamando $x_0 = M \cdot q + A$, esto es equivalente a la ecuación:

$$x \equiv x_0 \pmod{m_1 \cdots m_n \cdot m_{n+1}}$$

Como $0 \leq q \leq m_{n+1} - 1$ y $0 \leq A \leq M - 1$, resulta que

$$0 \leq x_0 \leq M \cdot (m_{n+1} - 1) + M - 1 = M \cdot m_{n+1} - 1 = m_1 \ldots m_n \cdot m_{n+1} - 1.$$

Unicidad. Supongamos que $0 \leq x_0 < x'_0 < m_1 \ldots m_n$ son dos soluciones del sistema dado. Entonces $x_0 \equiv x'_0 \pmod{m_i}$ para cada $1 \leq i \leq n$ (ya que ambos son congruentes a a_i); es decir, $m_i \mid x'_0 - x_0$ para todo $1 \leq i \leq n$. En otras palabras, $x'_0 - x_0$ es un múltiplo común de $m_1, \ldots, m_n$. Pero como $m_1, \ldots, m_n$ son coprimos de a pares, su mínimo común múltiplo es $m_1 \ldots m_n$; luego, $x'_0 - x_0$ es múltiplo de $m_1 \ldots m_n$. Como $0 \leq x'_0 - x_0 < m_1 \ldots m_n$, esto implica que necesariamente $x'_0 - x_0 = 0$, es decir, $x'_0 = x_0$.

El teorema nos asegura que, si los módulos son coprimos de a pares, vamos a encontrar una solución x_0 (y sólo una) para el sistema (3) que cumple $0 \leq x_0 < m_1 \cdot m_2 \ldots m_n$, y que *todas* las soluciones del sistema son los enteros de la forma $x = m_1 \cdot m_2 \ldots m_n \cdot k + x_0$ con $k \in \mathbb{Z}$.

Algoritmo para resolver el sistema (3) si $m_1, \ldots, m_n$ son coprimos de a pares.

- Definir $M_1 = m_1$ y $A_1 = a_1$. De la primera ecuación, $x \equiv a_1$ (mód m_1), se deduce que las soluciones son de la forma $x = M_1 \cdot Q_1 + A_1$ con $Q_1 \in \mathbb{Z}$.
- Para $i = 1, \ldots, n-1$:

  resolver $M_i \cdot Q_i + A_i \equiv a_{i+1} \pmod{m_{i+1}}$

  (donde la incógnita es Q_i). Sea $q_i \in \mathbb{Z}$ con $0 \le q_i < m_{i+1}$ tal que las soluciones de esta ecuación son $Q_i \equiv q_i \pmod{m_{i+1}}$:

  definir $M_{i+1} = M_i \cdot m_{i+1}, \quad A_{i+1} = M_i \cdot q_i + A_i$

  Entonces las soluciones del sistema formado por las primeras $i+1$ ecuaciones son de la forma $x = M_{i+1} \cdot Q_{i+1} + A_{i+1}$ con $Q_{i+1} \in \mathbb{Z}$.

- Dar como respuesta $x \equiv A_n \pmod{M_n}$.

Saber que hay una solución en un rango acotado nos permite hallarla por búsqueda exhaustiva (si es que el rango no es demasiado grande). Como Lorena en el ejemplo, buscamos todos los enteros x con $0 \le x < m_1 \cdot m_2 \ldots m_n$ tales que $x \equiv a_1 \pmod{m_1}$; de estos nos quedamos con aquellos que también cumplen que $x \equiv a_2 \pmod{m_2}$, y seguimos así, agregando en cada paso una restricción, hasta llegar a tener un único elemento en la lista. Sin embargo, para valores grandes de $m_1, \ldots, m_n$ esta búsqueda puede volverse tediosa. Resulta entonces más conveniente proceder resolviendo las ecuaciones sucesivamente.

Ejemplo. Hallar todos los $x \in \mathbb{Z}$ tales que:

$$\begin{cases} x \equiv 14 \pmod{49} \\ x \equiv 17 \pmod{45} \end{cases}$$

Como $(49 : 45) = 1$, el Teorema chino del resto asegura que el sistema tiene soluciones y que tiene una única solución x_0 con $0 \le x_0 < 49 \cdot 45 = 2.205$. Buscaremos la solución resolviendo sucesivamente las ecuaciones.

Las soluciones de la primera ecuación, $x \equiv 14 \pmod{49}$, son todos los enteros x de la forma:

$$x = 49 \cdot q + 14, \quad \text{con } q \in \mathbb{Z}$$

De entre todos los posibles q, nos interesan aquéllos que hacen que se cumpla la segunda ecuación, $x \equiv 17 \pmod{45}$; en términos de q, esto es que $49 \cdot q + 14 \equiv 17 \pmod{45}$. En definitiva, nos queda una ecuación lineal de congruencia; basta determinar los $q \in \mathbb{Z}$ tales que:

$$49 \cdot q \equiv 3 \pmod{45}.$$

Acá vemos la importancia de que $(49 : 45) = 1$, que es lo que nos asegura que esta ecuación, y por lo tanto también el sistema original, tiene solución. Reduciendo módulo 45, la ecuación anterior queda $4 \cdot q \equiv 3 \pmod{45}$ y vemos que una solución es $q_0 = 12$ (en el caso general, resolvemos la ecuación de congruencia como vimos en la sección 3); luego todas sus soluciones son los $q \equiv 12 \pmod{45}$, es decir:

$$q = 45 \cdot k + 12, \quad \text{con } k \in \mathbb{Z}$$

Finalmente, concluimos que las soluciones del sistema son todos los enteros x de la forma $x = 49 \cdot q + 14 = 49 \cdot (45 \cdot k + 12) + 14 = 49 \cdot 45 \cdot k + 602 = 2.205 \cdot k + 602$, con $k \in \mathbb{Z}$.

En el caso de un sistema de ecuaciones de congruencia en el que los módulos no son coprimos, lo que puede hacerse es tratar de reducirlo a otro en el que sí lo sean. Para hacer esto, la observación fundamental es que si $m = m_1 \cdot m_2 \ldots m_r$ con $m_1, \ldots, m_r$ coprimos de a pares, entonces:

$$x \equiv a \pmod{m} \iff \begin{cases} x \equiv a & (\text{mód } m_1) \\ \vdots & \\ x \equiv a & (\text{mód } m_r) \end{cases}$$

Ejemplo. Hallar todos los $x \in \mathbb{Z}$ tales que:

$$\begin{cases} x \equiv 3 & (\text{mód } 12) \\ x \equiv 9 & (\text{mód } 14) \end{cases}$$

Tenemos que:

$$x \equiv 3 \pmod{12} \iff \begin{cases} x \equiv 3 & (\text{mód } 3) \\ x \equiv 3 & (\text{mód } 4) \end{cases} \iff \begin{cases} x \equiv 0 & (\text{mód } 3) \\ x \equiv 3 & (\text{mód } 4) \end{cases}$$

$$x \equiv 9 \pmod{14} \iff \begin{cases} x \equiv 9 & (\text{mód } 2) \\ x \equiv 9 & (\text{mód } 7) \end{cases} \iff \begin{cases} x \equiv 1 & (\text{mód } 2) \\ x \equiv 2 & (\text{mód } 7) \end{cases}$$

Aquí los módulos no son coprimos de a pares, $(4 : 2) = 2$, pero vemos que la validez de la segunda ecuación implica la de la tercera. Luego, podemos suprimir esta última y resolver el sistema que queda:

$$\begin{cases} x \equiv 0 & (\text{mód } 3) \\ x \equiv 3 & (\text{mód } 4) \\ x \equiv 2 & (\text{mód } 7) \end{cases} \iff x \equiv 51 \pmod{3 \cdot 4 \cdot 7}$$

Concluimos que las soluciones del sistema dado son los enteros de la forma $x = 84 \cdot k + 51$ con $k \in \mathbb{Z}$.

Ejercicio 3.8. Un grupo de amigos va a cenar a una pizzería. Cuando llega la cuenta, en la mesa son 10 personas; si todos ponen la misma cantidad (entera) de dinero, recolectan $6 más que lo que debían pagar. En ese momento vuelve a la mesa Martín (es decir, en realidad eran 11 amigos y no 10). Reparten entonces los gastos entre los 11, y sobran $10. Sabiendo que juntaron más de $100, ¿cuánto es lo mínimo que puede haberles costado la cena?

Ejercicio 3.9.

- Hallar todos los enteros que tienen resto 1 en la división por 3, resto 2 en la división por 5 y resto 5 en la división por 7.
- Hallar, si existen, todos los enteros que tienen resto 8 en la división por 12 y resto 6 en la división por 20.

□ 7. Pequeño teorema de Fermat

Como vimos en uno de los ejemplos de la sección 2, los restos de dividir las sucesivas potencias de un entero a por un entero m se repiten en algún momento (porque hay sólo una cantidad finita de restos posibles, mientras que consideramos infinitas potencias). Para simplificar los cálculos, es útil conocer un exponente donde ocurre esta repetición. El *pequeño teorema de Fermat*[8] es un

[8] Este teorema fue enunciado originalmente por Pierre de Fermat en una carta en 1640. Aunque se supone que Leibniz lo demostró unos pocos años después, fue recién en 1736 que Euler publicó la primera demostración. Más adelante, en 1760, Euler también probó una generalización del teorema.

resultado fundamental que nos da esa información.

Teorema 3.7 (Pequeño teorema de Fermat). *Sea $p \in \mathbb{N}$ un primo. Para cada $a \in \mathbb{Z}$ que no es múltiplo de p, vale que $a^{p-1} \equiv 1$ (mód p). Más aún, para todo $a \in \mathbb{Z}$ vale que $a^p \equiv a$ (mód p).*

Demostración. Sea $a \in \mathbb{Z}$ no divisible por p. Sea $[a] \in \mathbb{Z}_p$ la clase de equivalencia de a. Tenemos que $[a] \neq [0]$. Consideremos el conjunto $\mathbb{Z}_p^*$ de todos los elementos no nulos de $\mathbb{Z}_p$,

$$\mathbb{Z}_p^* = \{[1], [2], \ldots, [p-1]\}$$

Vamos a multiplicar cada elemento de $\mathbb{Z}_p^*$ por $[a]$ y a mirar el conjunto obtenido de esta manera. Observemos que si $[b], [c] \in \mathbb{Z}_p$ y $[a] \cdot [b] = [a] \cdot [c]$, necesariamente $[b] = [c]$ porque podemos multiplicar ambos miembros de la primera igualdad por el inverso multiplicativo de $[a]$; en particular, $[a] \cdot [b] \neq 0$ si $[b] \neq 0$. Entonces, deducimos que el conjunto:

$$[a] \cdot \mathbb{Z}_p^* = \{[a] \cdot [1], [a] \cdot [2], \ldots, [a] \cdot [p-1]\}$$

está formado por p - 1 elementos del conjunto $\mathbb{Z}_p^*$ *distintos entre sí*. Como $\mathbb{Z}_p^*$ tiene a su vez p - 1 elementos, concluimos que $[a] \cdot \mathbb{Z}_p^*$ contiene a *todos* los elementos de $\mathbb{Z}_p^*$, es decir, que $[a] \cdot \mathbb{Z}_p^* = \mathbb{Z}_p^*$.

Multiplicando los elementos de $[a] \cdot \mathbb{Z}_p^*$ obtenemos, por un lado:

$$\begin{aligned} ([a] \cdot [1]) \cdot ([a] \cdot [2]) \cdot \cdots \cdot ([a] \cdot [p-1]) &= [a]^{p-1} \cdot ([1] \cdot [2] \cdot \cdots \cdot [p-1]) \\ &= [a^{p-1}] \cdot [1 \cdot 2 \cdot \cdots \cdot (p-1)] \end{aligned}$$

Por otra parte, como $[a] \cdot \mathbb{Z}_p^* = \mathbb{Z}_p^*$, el producto de estos elementos es el producto de los elementos de $\mathbb{Z}_p^*$ (eventualmente hecho en otro orden), o sea:

$$\begin{aligned} ([a] \cdot [1]) \cdot ([a] \cdot [2]) \cdot \cdots \cdot ([a] \cdot [p-1]) &= [1] \cdot [2] \cdot \cdots \cdot [p-1] \\ &= [1 \cdot 2 \cdot \cdots \cdot (p-1)] \end{aligned}$$

Igualando ambas expresiones para el producto, resulta que:

$$[a^{p-1}] \cdot [1 \cdot 2 \cdot \cdots \cdot (p-1)] = [1 \cdot 2 \cdot \cdots \cdot (p-1)]$$

Como p no divide a $1 \cdot 2 \cdot \ldots \cdot (p-1)$, puesto que es primo y no divide a ninguno de los factores, tenemos que $[1 \cdot 2 \cdot \ldots \cdot (p-1)] \neq [0]$, con lo que tiene inverso multiplicativo en $\mathbb{Z}_p$ y, multiplicando la igualdad anterior por dicho inverso, deducimos que:

$$[a^{p-1}] = 1$$

o, en términos de congruencias:

$$a^{p-1} \equiv 1 \pmod{p}$$

Para terminar, observemos que multiplicando ambos miembros de esta congruencia por a obtenemos que:

$$a^p \equiv a \pmod{p}$$

Pero esta igualdad vale también cuando $p \mid a$, ya que en este caso $a \equiv 0 \pmod{p}$ y también $a^p \equiv 0 \pmod{p}$.

Observación. Sea $p \in \mathbb{N}$ primo y sea $a \in \mathbb{Z}$ no divisible por p. Entonces $a^n \equiv a^m \pmod{p}$ si n y m son números naturales tales que $n \equiv m \pmod{p-1}$. En particular, si r_{p-1} es el resto en la división de n por $p-1$, entonces $a^n \equiv a^{r_{p-1}} \pmod{p}$.

En efecto, suponiendo que $n \geq m$, si $n \equiv m \pmod{p-1}$, tenemos que $n = m + k \cdot (p-1)$ para algún $k \in \mathbb{N}_0$; luego:

$$\begin{aligned} a^n &= a^{m+k\cdot(p-1)} \\ &= a^m \cdot (a^{p-1})^k \\ &\equiv a^m \cdot 1^k \\ &\equiv a^m \pmod{p} \end{aligned}$$

donde la anteúltima congruencia es consecuencia del pequeño teorema de Fermat.

Ejemplo. Hallar el resto en la división de $3^{1.423}$ por 11.

Por la Proposición 3.3, sabemos que el resto buscado es el único entero r con $0 \leq r < 11$ tal que $3^{1.423} \equiv r \pmod{11}$. Ahora, por la observación anterior, como $1.423 \equiv 3 \pmod{10}$ tenemos que:

$$\begin{aligned} 3^{1.423} &\equiv 3^3 \\ &\equiv 5 \pmod{11} \end{aligned}$$

Luego, $r = 5$.

Mencionemos, para concluir esta sección, que como consecuencia del pequeño teorema de Fermat podemos obtener una expresión explícita para los inversos multiplicativos de los elementos de $\mathbb{Z}_p$, si $p \in \mathbb{N}$ es primo: *el inverso multiplicativo de un elemento* $a \in \mathbb{Z}_p$, $a \neq 0$, *es* $a^{p-2} \in \mathbb{Z}_p$. En efecto, tenemos que $a \cdot a^{p-2} = a^{p-1} = 1$ en $\mathbb{Z}_p$, con lo que $a^{-1} = a^{p-2}$ en $\mathbb{Z}_p$.

Ejercicio 3.10. Hallar el resto en la división de a por m en los siguientes casos:

- $a = 129^{111}$, $m = 7$.
- $a = 129^{111}$, $m = 35$. (Sugerencia: calcular el resto en la división por 5 y por 7 y usar el teorema chino del resto).

□ 8. Aplicación: Tests de primalidad

Un *test de primalidad* es un procedimiento para determinar si un entero dado es primo o no lo es.

Dado $n \in \mathbb{N}$ un posible test de primalidad consiste en verificar si n es divisible por algún entero m tal que $2 \leq m \leq \sqrt{n}$. Si algún $m_0 \in \mathbb{N}$ con $2 \leq m_0 \leq \sqrt{n}$ divide a n, es claro que n es compuesto (hemos encontrado un divisor propio de n). De lo contrario, podemos asegurar que n es primo por el Lema 2.8 del capítulo 2. Este procedimiento nos permite decidir con certeza si n es primo.

Sin embargo, para valores grandes de n, la cantidad de operaciones a realizar (y por consiguiente, el tiempo que lleva hacerlas) puede resultar demasiado grande a los fines prácticos.

El pequeño teorema de Fermat ha dado lugar a tests de primalidad *probabilísticos* alternativos. La idea es que el método no nos permite determinar con certeza si n es primo, sino que podemos saberlo pero con cierta probabilidad de error.

8.1. Test de primalidad de Fermat

Este procedimiento funciona como explicamos a continuación:

- dado $n \in \mathbb{N}$, se elige al azar un entero a tal que $2 \leq a \leq n - 1$ y se calcula $a^{n-1} \pmod{n}$;
- si $a^{n-1} \not\equiv 1 \pmod{n}$, la respuesta es que *n es compuesto*;
- si $a^{n-1} \equiv 1 \pmod{n}$, la respuesta es que *n probablemente sea primo*.

Observemos que en caso que $a^{n-1} \not\equiv 1 \pmod{n}$, podemos estar seguros de que a **no** es primo, porque el pequeño teorema de Fermat nos dice que de serlo, debería ocurrir que $a^{n-1} \equiv 1 \pmod{n}$ sin importar qué valor de a hayamos elegido.

Ahora bien, si n es compuesto puede ocurrir que $a^{n-1} \equiv 1 \pmod{n}$ para algún a tal que $2 \leq a \leq n - 1$. Por ejemplo, para $n = 91 = 7 \cdot 13$ (¡que no es primo!) y $a = 3$ se tiene que $3^{90} = (3^6)^{15} = 729^{15} \equiv_{(91)} 1^{15} \equiv_{(91)} 1$. Es por este motivo que no podemos estar seguros de que n sea primo si la congruencia vale.

Sin embargo, si existe algún a coprimo con n tal que $a^{n-1} \not\equiv 1 \pmod{n}$, entonces lo mismo ocurre para al menos la mitad de los posibles $2 \leq a \leq n - 1$. Esto se debe a que, si $a_1, \ldots, a_s$ son todas las bases para las cuales $a_i^{n-1} \equiv 1 \pmod{n}$, entonces $(a \cdot a_i)^{n-1} = a^{n-1} \cdot a_i^{n-1} \equiv_{(n)} a^{n-1} \cdot 1 \equiv_{(n)} a^{n-1} \not\equiv_{(n)} 1$ y, además, $a \cdot a_1, \ldots, a \cdot a_s$ son todos distintos módulo n, ya que a es coprimo con n. Así, hay una probabilidad menor que $1/2$ de que eligiendo a al azar se verifique $a^{n-1} \equiv 1 \pmod{n}$. Si el proceso se repite k veces, la probabilidad de que en todos los casos resulte $a^{n-1} \equiv 1 \pmod{n}$ es $1/2^k$ (¡muy chica si k es grande!).

El problema es que hay enteros compuestos n para los cuales $a^{n-1} \equiv 1 \pmod{n}$ para *todo* a coprimo con n. Estos enteros se conocen como *números de Carmichael* y el hecho de que sean compuestos los hace difícil de detectar para el test de Fermat (sólo nos damos cuenta de que n es compuesto si justo elegimos un a tal que $(a : n) \neq 1$).

El menor de estos números[9] es $n = 561$; veamos que tiene la propiedad mencionada, es decir que:

$$a^{560} \equiv 1 \pmod{561}$$

[9] Este número fue encontrado por Carmichael en 1910, de ahí el nombre que reciben los enteros con esta propiedad.

para todo $a \in \mathbb{Z}$ con $(a : 561) = 1$. Como $561 = 3 \cdot 11 \cdot 17$, para probar lo anterior basta ver que:

$$\begin{cases} a^{560} \equiv 1 \pmod 3 \\ a^{560} \equiv 1 \pmod{11} \\ a^{560} \equiv 1 \pmod{17} \end{cases}$$

Estas congruencias son consecuencia del pequeño teorema de Fermat: en efecto, si $(a : 561) = 1$, tenemos que a no es múltiplo de 3 ni de 11 ni de 17, y el teorema asegura entonces que:

$$a^2 \equiv 1 \pmod 3, \quad a^{10} \equiv 1 \pmod{11}, \quad a^{16} \equiv 1 \pmod{17}$$

con lo cual:

$$a^{560} = (a^2)^{280} \equiv 1 \pmod 3, \qquad a^{560} = (a^{10})^{56} \equiv 1 \pmod{11}, \qquad a^{560} = (a^{16})^{35} \equiv 1 \pmod{17}$$

8.2. Test de primalidad de Miller-Rabin

Este procedimiento alternativo para determinar si un entero dado es primo o no se basa en el pequeño teorema de Fermat más el hecho fundamental de que:

$$x^2 \equiv 1 \pmod p \iff x \equiv 1 \pmod p \quad \text{o} \quad x \equiv -1 \pmod p.$$

Esta equivalencia vale ya que, si p es primo, entonces $p \mid x^2 - 1 = (x - 1) \cdot (x + 1)$ si y sólo si $p \mid x - 1$ o $p \mid x + 1$ (recordar que un número primo divide a un producto si y sólo si divide a alguno de los factores). Más precisamente, ambos resultados se combinan en la siguiente propiedad:

Proposición 3.8. *Sea p un primo positivo impar. Factoricemos $p - 1 = t \cdot 2^r$ con $r \in \mathbb{N}$ y $t \in \mathbb{N}$ impar. Entonces, para cada $a \in \mathbb{Z}$ que no es múltiplo de p se tiene que:*

$$a^t \equiv 1 \pmod p \quad o \quad a^{t \cdot 2^k} \equiv -1 \pmod p \text{ para algún } 0 \le k < r$$

Demostración. Por el pequeño teorema de Fermat, sabemos que $a^{t \cdot 2^r} \equiv 1 \pmod p$. Como $r \ge 1$ porque $p - 1$ es par, podemos escribir $a^{t \cdot 2^r} = (a^{t \cdot 2^{r-1}})^2$ con $r - 1 \in \mathbb{N}_0$, y tenemos que:

$$(a^{t \cdot 2^{r-1}})^2 \equiv 1 \pmod p$$

Por lo que observamos más arriba, esto equivale a que:

$$a^{t \cdot 2^{r-1}} \equiv 1 \pmod p \quad \text{o} \quad a^{t \cdot 2^{r-1}} \equiv -1 \pmod p$$

Si $a^{t \cdot 2^{r-1}} \equiv -1 \pmod p$, se verifica la segunda condición del enunciado con $k = r - 1$. De lo contrario, resulta que $a^{t \cdot 2^{r-1}} \equiv 1 \pmod p$. Si $r - 1 = 0$, esto es simplemente la primera de las condiciones del enunciado. Finalmente, si $r - 1 \ge 1$, repitiendo el razonamiento anterior para $a^{t \cdot 2^{r-1}}$, deducimos que $a^{t \cdot 2^{r-2}} \equiv 1 \pmod p$ o $a^{t \cdot 2^{r-2}} \equiv -1 \pmod p$.

Siguiendo de la misma manera, o bien se llega en algún momento a un k con $0 \le k \le r - 1$ tal que $a^{t \cdot 2^k} \equiv -1 \pmod{p}$, o bien resulta que $a^t \equiv 1 \pmod{p}$.

El *test de primalidad de Miller-Rabin* funciona entonces como sigue:

- dado $n \in \mathbb{N}$ impar, se escribe $n - 1 = t \cdot 2^r$ con $r \in \mathbb{N}$ y $t \in \mathbb{N}$ impar;
- se elige a tal que $2 \le a \le n - 1$ al azar;
- se calcula $a^t \pmod{n}$. Si $a^t \equiv 1 \pmod{n}$ o $a^t \equiv -1 \pmod{n}$, decimos que *n probablemente sea primo*;
- si no, se calculan sucesivamente $a^{t \cdot 2} = (a^t)^2, a^{t \cdot 2^2} = (a^{t \cdot 2})^2, \ldots, a^{t \cdot 2^k} = (a^{t \cdot 2^{k-1}})^2, \ldots \pmod{p}$ hasta obtener como resultado -1, o bien hasta llegar a $a^{t \cdot 2^{r-1}}$. Si en algún paso el resultado es $a^{t \cdot 2^k} \equiv -1 \pmod{p}$, decimos que *n probablemente sea primo*. De lo contrario, tenemos que:

$$a^t \not\equiv 1 \pmod{n} \quad \text{y} \quad a^{t \cdot 2^k} \not\equiv -1 \text{ para todo } 0 \le k \le r - 1$$

y, por la proposición anterior, podemos asegurar que *n es compuesto.*

Se puede ver que si n es compuesto, la propiedad:

$$a^t \equiv 1 \pmod{n} \quad \text{o} \quad a^{t \cdot 2^k} \equiv -1 \pmod{n} \text{ para algún } 0 \le k < r$$

se cumple a lo sumo para la cuarta parte de los a tales que $1 \le a \le n - 1$. Es decir, que la probabilidad de que para un n compuesto el test diga que n probablemente sea primo es a lo sumo $1/4$. Esto nos dice que repitiendo el test para distintos valores de a podemos hacer que la probabilidad de obtener una respuesta incorrecta sea muy chica.

Ejemplo. Apliquemos el test de Miller-Rabin a $n = 561$.

- Escribimos $n - 1 = 560 = 35 \cdot 2^4$.
- Elegimos a tal que $2 \le a \le 560$, por ejemplo, $a = 2$.
- Calculamos $2^{35} \equiv 263 \pmod{561}$. Como $2^{35} \not\equiv 1 \pmod{561}$ y $2^{35} \not\equiv -1 \pmod{561}$, continuamos.
- Elevamos al cuadrado sucesivamente:
  - $(2^{35})^2 \equiv 263^2 \equiv 166 \not\equiv -1 \pmod{561}$
  - $(2^{35})^{2^2} \equiv 166^2 \equiv 67 \not\equiv -1 \pmod{561}$
  - $(2^{35})^{2^3} \equiv 67^2 \equiv 1 \not\equiv -1 \pmod{561}$
- Concluimos que 561 es *compuesto*.

□ 9. Aplicación: criptografía

La *criptografía* se encarga de estudiar cómo enviar mensajes de manera *secreta*. El

objetivo es que solamente el receptor a quien queremos enviarle el mensaje pueda leerlo y entenderlo, es decir, que si otra persona (en particular, alguien que nosotros no queremos que lea el mensaje) logra acceder a la información, no pueda interpretarla.

Para esto se utilizan distintos *métodos de encriptación* y, esencialmente, el proceso funciona como explicamos a continuación:

- el emisor *encripta* el mensaje, es decir, convierte la información original o *texto plano* en *texto cifrado*, que en apariencia no tiene sentido,
- se transmite el texto cifrado,
- el receptor *desencripta* el mensaje recibido, es decir, lo vuelve a su forma original.

Lo importante en este esquema es que si el texto cifrado es interceptado por quien no es el receptor, sea muy difícil o mejor aún, imposible, de descifrar.

El texto plano del mensaje m es encriptado por el emisor usando un método **e**; el resultado es el texto cifrado c que se transmite al receptor, quien lo desencripta por medio de **d** para recuperar el mensaje original m.

$$m \longrightarrow \boxed{\mathbf{e}} \longrightarrow c \longrightarrow \boxed{\mathbf{d}} \longrightarrow m$$

Emisor *Receptor*

Procedimientos de este tipo se han utilizado desde la antigüedad: por ejemplo, se cuenta que Julio César utilizaba un esquema de encriptación basado en una tabla como la siguiente:

0	A	D
1	B	E
2	C	F
3	D	G
4	E	H
5	F	I
6	G	J
7	H	K
8	I	L
9	J	M
10	K	N
11	L	O
12	M	P

13	N	Q
14	O	R
15	P	S
16	Q	T
17	R	U
18	S	V
19	T	W
20	U	X
21	V	Y
22	W	Z
23	X	A
24	Y	B
25	Z	C

La segunda columna de estas tablas contiene, ordenadas, las 26 letras del alfabeto. La tercera columna, también contiene todo el alfabeto ordenado, pero comenzando desde la letra D y volviendo a comenzar con la A una vez que se termina. Para encriptar una palabra, se reemplaza cada una de sus letras por la ubicada a su lado en la tabla anterior. Por ejemplo, la palabra

ATAQUE

se codifica como

DWDTXH.

Para desencriptar se utiliza la tabla de manera inversa: se lee en la tercera columna y se busca su interpretación en la segunda.

El mecanismo para encriptar resulta ser simplemente reemplazar cada letra por la que está tres lugares más adelante en el alfabeto, leyéndolo en forma circular (o sea, "a b c ... x

y z a b ..."), y para desencriptar, reemplazar cada letra por la que está tres lugares antes.

Podemos interpretar esto en términos matemáticos como sigue: representamos cada letra por un elemento $x \in \mathbb{Z}_{26}$ (el número ubicado en la primera columna de las tablas) y para encriptarla calculamos:

$$\mathbf{e}(x) = x + 3 \quad \text{en } \mathbb{Z}_{26}$$

y escribimos la letra representada por el elemento obtenido. Por ejemplo:

- la letra Q corresponde al elemento $16 \in \mathbb{Z}_{26}$; para encriptar, calculamos 16 + 3 = 19 en $\mathbb{Z}_{26}$ y buscamos a qué letra corresponde: la T;
- la letra Y corresponde a $24 \in \mathbb{Z}_{26}$; para encriptar, calculamos 24 + 3 = 1 en $\mathbb{Z}_{26}$ y buscamos a qué letra corresponde el resultado: la B.

Para desencriptar, reemplazamos cada letra por el elemento correspondiente $y \in \mathbb{Z}_{26}$ y calculamos:

$$\mathbf{d}(y) = y - 3 \quad \text{en } \mathbb{Z}_{26}$$

Por ejemplo, para desencriptar la letra C, que corresponde al elemento $2 \in \mathbb{Z}_{26}$, calculamos 2 - 3 = 25 en $\mathbb{Z}_{26}$ y buscamos a qué letra corresponde: la Z.

Es fácil generar nuevos métodos de encriptación que funcionen de esta manera, observando que **e** y **d** no son otra cosa que una función biyectiva $\mathbf{e} : \mathbb{Z}_{26} \to \mathbb{Z}_{26}$ y su inversa $\mathbf{d} = \mathbf{e}^{-1}$. Por ejemplo, podríamos tomar $\mathbf{e}(x) = 3 \cdot x + 4$ y $\mathbf{d}(y) = 9 \cdot y + 16$.

El inconveniente de los métodos de encriptación como éste, en los que cada letra se reemplaza siempre por el mismo símbolo, es que son fácilmente vulnerables. Dado un texto encriptado de esta manera, si se analiza la frecuencia con que aparecen los distintos caracteres es posible descubrir qué letras representan (por ejemplo, las vocales A y E aparecen con mucha frecuencia en un texto; lo mismo ocurre con consonantes como la S o la T).

Por este motivo, para aplicaciones en las que la seguridad es muy importante, se utilizan otros métodos más sofisticados. En lo que sigue, introduciremos el *algoritmo RSA*, ideado por Ron Rivest, Adi Shamir y Leonard Adleman en 1977. Este procedimiento hace uso de dos claves: una *clave pública*, que puede ser conocida por todos y se utiliza para encriptar, y una *clave privada*, que sólo debe conocer quien recibirá el mensaje, y que se usa para desencriptar. Al igual que el ejemplo básico que vimos antes, el algoritmo RSA se basa en cálculos de aritmética modular, en este caso, potenciación en lugar de suma.

Supongamos que Andrea le va a enviar un mensaje a Belén. Para armar las claves, Belén procede como sigue:

- genera dos primos grandes al azar $p \neq q$, aproximadamente del mismo tamaño;
- calcula $n = p \cdot q$ y $\varphi(n) = (p - 1) \cdot (q - 1)$;
- elige un entero e tal que:

$$1 < e < \varphi(n) \quad \text{y} \quad mcd(e, \varphi(n)) = 1$$

El par (*e, n*) es la clave pública que Belén da a conocer.

- calcula el inverso de *e* en $\mathbb{Z}_{\varphi(n)}$, es decir, obtiene el único *d* con:

$$1 < d < \varphi(n) \quad \text{y} \quad e \cdot d \equiv 1 \pmod{\varphi(n)}$$

El par (*d, n*) es la clave privada que Belén guarda en secreto.

Ahora, para mandar el mensaje, Andrea lo representa por un número *m* con $1 \leq m \leq n - 1$ y coprimo con *n* (si el mensaje es largo, lo separa en partes y lo representa por varios números), y luego lo encripta usando la clave pública de Belén:

$$\mathbf{e}(m) = m^e \quad \text{en } \mathbb{Z}_n$$

Finalmente, envía el resultado $c = \mathbf{e}(m)$ a Belén.

Belén recibe *c* y lo desencripta usando la clave privada que sólo ella conoce:

$$\mathbf{d}(c) = c^d \quad \text{en } \mathbb{Z}_n$$

Ejemplo. Supongamos que Andrea quiere mandarle el mensaje $m = 87$ a Belén. En primer lugar, Belén genera las claves:

- elige $p = 11$, $q = 17$;
- calcula $n = 11 \cdot 17 = 187$ y $\varphi(n) = 10 \cdot 16 = 160$;
- elige un entero *e* tal que $1 < e < 160$ y $mcd(e, 160) = 1$, por ejemplo $e = 7$. Hace pública la clave (7, 187);
- busca el inverso de $e = 7$ en $\mathbb{Z}_{160}$, es decir, resuelve:

$$7 \cdot d \equiv 1 \pmod{160}$$

obteniendo $d = 23$ (ya que $7 \cdot 23 = 161 \equiv 1 \pmod{160}$). Entonces (23, 187) es la clave que Belén se guarda para desencriptar el mensaje de Andrea.

Una vez que tiene la clave $(e, n) = (7, 187)$, Andrea encripta su mensaje $m = 87$ calculando:

$$m^e = 87^7 \quad \text{en } \mathbb{Z}_{187}$$

Para esto, haciendo las cuentas en $\mathbb{Z}_{187}$, calcula:

$$87^2 = 7.569 = 89$$
$$87^4 = (87^2)^2 = 89^2 = 7.921 = 67$$
$$87^7 = 87^{1+2+4} = 87^1 \cdot 87^2 \cdot 87^4 = 87 \cdot 89 \cdot 67 = 43$$

Envía entonces $\mathbf{e}(87) = 43$.

Finalmente, Belén desencripta la información recibida usando su clave privada $(d, n) = (23, 187)$, nuevamente calculando en $\mathbb{Z}_{187}$:

$$\begin{aligned}
&43^2 = 1.849 = 166\\
&43^4 = (43^2)^2 = 166^2 = 27.556 = 67\\
&43^8 = (43^4)^2 = 67^2 = 4.489 = 1\\
&43^{16} = (43^8)^2 = 1^2 = 1\\
&43^{23} = 11^{16+4+2+1} = 11^{16} \cdot 11^4 \cdot 11^2 \cdot 11 = 1 \cdot 67 \cdot 166 \cdot 43 = 87
\end{aligned}$$

Obtiene de esta manera, $\mathbf{d}(43) = 87$, que es el mensaje original que Andrea quería enviarle.

Veamos que en cualquier caso, si Belén recibe c, entonces $\mathbf{d}(c) = m$, el mensaje original. Es decir, Belén siempre descifra correctamente el mensaje. Recordando que $c = \mathbf{e}(m)$, esto es equivalente a verificar que:

$$\mathbf{d}(\mathbf{e}(m)) = m$$

Ahora bien, $\mathbf{d}(\mathbf{e}(m)) = (\mathbf{e}(m))^d = (m^e)^d = m^{e \cdot d}$ en $\mathbb{Z}_n$; con lo cual, debemos ver que:

$$m^{e \cdot d} = m \text{ en } \mathbb{Z}_n$$

o equivalentemente, que:

$$m^{e \cdot d} \equiv m \pmod{n}$$

Para esto utilizaremos el pequeño teorema de Fermat. En primer lugar, recordemos que como $n = p \cdot q$ con p y q primos distintos (y por lo tanto, enteros coprimos), vale que:

$$m^{e \cdot d} \equiv m \pmod{n} \iff \begin{cases} m^{e \cdot d} \equiv m \pmod{p} \\ m^{e \cdot d} \equiv m \pmod{q} \end{cases}$$

La elección de las claves d y e se hizo de manera que $e \cdot d \equiv 1 \pmod{\varphi(n)}$, donde $\varphi(n) = (p - 1) \cdot (q - 1)$. Entonces, existe $k \in \mathbb{Z}$ tal que $e \cdot d = 1 + (p - 1) \cdot (q - 1) \cdot k$, y, por lo tanto:

$$m^{e \cdot d} = m^{1 + (p-1) \cdot (q-1) \cdot k} = m \cdot (m^{p-1})^{(q-1) \cdot k}$$

Mirando ahora módulo p y teniendo en cuenta que, por el pequeño teorema de Fermat, vale $m^{p-1} \equiv 1 \pmod{p}$ (observar que p no divide a m, ya que $(m : n) = 1$), resulta que $m^{e \cdot d} \equiv m \pmod{p}$. De la misma manera, $m^{e \cdot d} \equiv m \pmod{q}$. En consecuencia, tenemos que:

$$m^{e \cdot d} \equiv m \pmod{n}$$

¿Por qué es difícil descifrar el mensaje para alguien que intercepta el envío de Andrea? Observemos que para hallar m a partir de $c = m^e$ es suficiente conocer d (así es como Belén descifrará el mensaje). Pero para calcular d, lo que se hizo fue buscar el inverso de e módulo $\varphi(n)$. Esto es fácil de hacer conociendo $\varphi(n)$, pero quien intercepte el mensaje, lo que conoce es la clave pública (e, n), es decir, conoce n, pero no $\varphi(n)$. Nuevamente, $\varphi(n) = (p - 1) \cdot (q - 1)$ es fácil de calcular una vez que conocemos p y q, es decir, una vez que factorizamos n. Y aquí está el problema: *factorizar números naturales grandes es difícil*. Por difícil entendemos que requiere de *mucho* tiempo: se cree que la cantidad de tiempo necesaria para factorizar un número natural crece casi exponencialmente a medida que

aumenta el tamaño de n. Por este motivo, en la actualidad se utilizan números de más de 300 dígitos en el algoritmo RSA.

No está probado que para ser capaz de desencriptar mensajes (es decir, recuperar m conociendo $c = m^e$ en $\mathbb{Z}_n$ y la clave pública (e, n)) sea necesario conocer la factorización de $n = p \cdot q$. Sin embargo, hasta el momento, no han surgido alternativas más eficientes y, más aún, existe un método probabilístico para factorizar $n = p \cdot q$ basado en poder descifrar mensajes de RSA. Por todo esto, el algoritmo RSA es uno de los métodos más utilizados en la actualidad en las aplicaciones donde realmente es necesario transmitir información de manera segura; de hecho, se usa a diario en Internet cuando se visita una página segura que requiere una clave para ingresar (como la de un banco).