

Notas de Álgebra

Mariano Suárez-Álvarez

Índice

1	Conjuntos	1
1.1	Conjuntos	1
1.2	Subconjuntos	5
1.3	Operaciones entre conjuntos	6
1.4	Tablas de verdad	18
1.5	Ejercicios	24
2	Relaciones	27
2.1	El producto cartesiano	27
2.2	Relaciones	29
2.3	Relaciones en un conjunto	36
2.4	Relaciones de equivalencia	41
2.5	Relaciones de orden	51
2.6	Ejercicios	54
3	Funciones	59
3.1	Funciones	59
3.2	Inyectividad, sobreyectividad, biyectividad	61
3.3	Funciones inversibles y funciones inversas	63
3.4	Ejercicios	66
4	Inducción	71
4.1	El principio de inducción	71
4.2	Algunos ejemplos de pruebas por inducción	75
4.3	Dos variaciones del Principio de Inducción	84
4.4	Tres pruebas por «inducción fuerte»	89
4.5	Ejercicios	93
5	Recursión	95
5.1	Sucesiones	95

5.2	Definiciones por recursión	96
5.3	Variaciones sobre la recursión	102
5.4	Manipulación de sucesiones definidas recursivamente	107
5.5	Ejercicios	120
6	Divisibilidad	127
6.1	La relación de divisibilidad	127
6.2	El algoritmo de la división	129
6.3	La notación posicional	131
6.4	Máximo común divisor	134
6.5	Algunas aplicaciones de la identidad de Bézout	144
6.6	Ejercicios	148
7	Congruencias	156
7.1	La relación de congruencia	156
7.2	Algunos criterios de divisibilidad	161
7.3	Los enteros módulo m	164
7.4	Ejercicios	167
8	Ecuaciones diofánticas	169
8.1	Ecuaciones diofánticas	169
8.2	Ecuaciones lineales	172
9	Números primos	175
9.1	Números primos	175
9.2	El Teorema Fundamental de la Aritmética	180
9.3	Valuaciones	185
9.4	Sumas de divisores	191
10	Potencias	202
10.1	El pequeño teorema de Fermat	202
10.2	La función de Euler	204
10.3	El Teorema de Euler	209
10.4	Dos aplicaciones	214
10.5	Órdenes	217
10.6	Raíces primitivas	221
10.7	El Teorema de Carmichael	235
	Bibliografía	241

Capítulo 1

Conjuntos

§1.1. Conjuntos

1.1.1. Un *conjunto* es una colección de objetos, a los que nos referimos como sus *elementos*. Si un objeto x es un elemento de un conjunto A , decimos que el objeto x *pertenece* a A y escribimos

$$x \in A.$$

Si por el contrario x no es un elemento de A , decimos que x no pertenece a A y escribimos

$$x \notin A.$$

Un conjunto queda completamente determinado por sus elementos. Como consecuencia de esto, si A y B son dos conjuntos, entonces es claro que A y B son iguales si y solamente si tienen exactamente los mismos elementos.

1.1.2. Si un conjunto tiene un número finito de elementos y éstos no son muchos, podemos describir el conjunto simplemente listando sus elementos y en ese caso lo hacemos entre llaves $\{\dots\}$. Por ejemplo, si escribimos

$$\{1, 3, 101, 7\} \tag{1}$$

estamos mencionando el conjunto que tiene por elementos a los números 1, 3, 101 y 7, y a ninguna otra cosa más — observemos que de esta forma el conjunto queda completamente determinado. Cuando usamos este tipo de descripción de un conjunto

—listar sus elementos— decimos que lo damos por *enumeración*. Si llamamos A al conjunto de (1), entonces claramente tenemos que

$$1 \in A, \quad 99 \notin A, \quad 101 \in A, \quad 0 \notin A.$$

Es importante tener en cuenta que el orden en que listamos los elementos de un conjunto cuando lo damos por enumeración es irrelevante y, por lo tanto, que podríamos haber escrito

$$\{7, 101, 1, 3\}$$

para describir exactamente el mismo conjunto que el de (1). De manera similar, la cantidad de veces que aparece un objeto en la lista de elementos de un conjunto en una descripción como (1) es irrelevante: lo único importante es si un objeto aparece o no en la lista. Esto significa que el conjunto

$$\{1, 1, 101, 3, 3, 3, 7, 101, 7, 7\}$$

es exactamente el mismo que el conjunto de (1). Por supuesto, casi siempre es preferible evitar repeticiones inútiles, pero esto puede no ser fácil o posible.

1.1.3. Los elementos de un conjunto pueden ser de cualquier tipo. Por ejemplo, el conjunto

$$\{1, \color{red}{\bullet}, \clubsuit, (2, 3)\}$$

tiene cuatro elementos: el número 1, el disco rojo $\color{red}{\bullet}$, el palo de trébol \clubsuit de la baraja francesa y el par ordenado $(2, 3)$. Los elementos de un conjunto pueden ser ellos mismos conjuntos: así, los elementos del conjunto

$$\{1, \{2, 3\}, 4, \{5, 6\}\}$$

son cuatro: los números 1 y 4 y los conjuntos $\{2, 3\}$ y $\{5, 6\}$. Es importante observar que, por ejemplo, el número 2 no es un elemento de este conjunto. De manera similar, el conjunto

$$\{\{1, 2\}\}$$

tiene exactamente *un* elemento, el conjunto $\{1, 2\}$, y

$$\{\{1\}, 1\}$$

tiene *dos*: el número 1 y el conjunto $\{1\}$. Finalmente,

$$\{1, \{1\}, \{1, \{1\}\}, \{\{1, \{1\}\}\}$$

denota el conjunto que tiene cuatro elementos: el número 1 y los conjuntos $\{1\}$, $\{1, \{1\}\}$ y $\{\{1, \{1\}\}\}$, que tienen 1, 2 y 1 elementos, respectivamente.

1.1.4. Un conjunto puede no tener elementos: decimos en ese caso que es *vacío*. Si A y B son dos conjuntos que son vacíos, entonces tienen exactamente los mismos elementos: a saber, ninguno — esto implica, como observamos arriba, que A y B son de hecho el mismo conjunto. Vemos así que hay exactamente un conjunto que es vacío y no hay ninguna ambigüedad si nos referimos a él como *el* conjunto vacío.

Podemos dar el conjunto vacío por enumeración: de acuerdo a las convenciones que describimos arriba, el símbolo

$$\{\}$$

denota al conjunto vacío. Casi siempre, sin embargo, usamos el símbolo especial

$$\emptyset$$

para representar al conjunto vacío. Este símbolo fue propuesto por *André Weil* (1906–998, Francia), inspirado en la letra \emptyset del idioma noruego, y fue usado por primera vez en 1939 en el libro sobre la teoría de conjuntos de Nicolás Bourbaki¹. El concepto de conjunto vacío, sin embargo, es muy anterior: el primero en usar explícitamente el conjunto vacío fue *Georges Boole* (1815–854, Inglaterra) en 1847.

Observemos que el conjunto $\{\emptyset\}$ tiene un elemento —el conjunto vacío— así que no es vacío. De manera similar, $\{\emptyset, \{\emptyset\}\}$ tiene dos, ya que \emptyset y $\{\emptyset\}$ son dos cosas distintas.

1.1.5. Si un conjunto es finito pero tiene muchos elementos o, peor, si tiene infinitos elementos, entonces no es práctico o posible darlo por enumeración. En ese caso, podemos describirlo dando alguna condición que permita decidir si un objeto pertenece o no al conjunto. Por ejemplo, escribimos

$$A = \{x : x \text{ es un entero positivo y par}\} \tag{2}$$

para decir que A es el conjunto de todos los objetos x que satisfacen la condición « x es un entero positivo y par». Así, los números 2 y 1928 pertenecen a este conjunto A mientras que el número 7, el número -4 o el conjunto $\{4, 9\}$ no: el número 7 es un

¹En su autobiografía, Weil cuenta: «Wisely, we had decided to publish an installment establishing the system of notation for set theory, rather than wait for the detailed treatment that was to follow: it was high time to fix these notations once and for all, and indeed the ones we proposed, which introduced a number of modifications to the notations previously in use, met with general approval. Much later, my own part in these discussions earned me the respect of my daughter Nicolette, when she learned the symbol \emptyset for the empty set at school and I told her that I had been personally responsible for its adoption. The symbol came from the Norwegian alphabet, with which I alone among the Bourbaki group was familiar.»

entero positivo pero no es par, el número -4 es un entero y es par, pero no es positivo, y el conjunto $\{4, 9\}$ no es ni siquiera un entero. De manera similar, al conjunto

$$\{x : x \text{ es un número real y } 0 < x \leq 3\} \quad (3)$$

pertenecen los números 1 , $\sqrt{2}$ y 3 , pero no el número -9 , el número 12 o el par ordenado $(1, 2)$.

Los conjuntos de (2) y (3) son infinitos, así que no sería posible darlos por enumeración de sus elementos. Por otro lado, el conjunto

$$\{x : x \text{ es un entero positivo menor que } 1\,000\,000\}$$

es finito pero tiene $999\,999$ elementos, así que aunque es en principio posible describirlo por enumeración hacerlo no es muy práctico.

1.1.6. Cuando describimos un conjunto dando una condición que permite decidir si cada objeto pertenece o no a él, decimos que lo damos *por comprensión*. El símbolo «:» que usamos en (2) y en (3) se lee «tal que» y entonces leemos en voz alta lo que aparece a la derecha del símbolo igual de (2) «el conjunto de los objetos x tales que x es un entero positivo y par». A veces usamos una barra vertical «|» en lugar de «:» y escribimos entonces

$$\{x \mid x \text{ es un entero positivo y par}\}.$$

En estas notas usaremos exclusivamente el símbolo «:», ya que reservaremos la barra vertical para denotar la divisibilidad.

1.1.7. Casi siempre que damos un conjunto por comprensión, parte de la condición que lo determina es que los objetos tienen que pertenecer a algún conjunto ya conocido. Así, la condición que aparece en el conjunto (2) incluye la de que x pertenezca al conjunto \mathbb{Z} de los números enteros, mientras que la de (3) que x pertenezca al conjunto \mathbb{R} de los números reales. Cuando es ése el caso y queremos enfatizarlo, preferimos escribir

$$\{x \in \mathbb{Z} : x \text{ es positivo y par}\}$$

y

$$\{x \in \mathbb{R} : 0 < x \leq 3\}$$

en lugar de las fórmulas de (2) y (3). Cuando leemos en voz alta la primera de estas fórmulas, por ejemplo, decimos «el conjunto de los x que pertenecen a \mathbb{Z} tales que x es positivo y par».

§1.2. Subconjuntos

1.2.1. Decimos que un conjunto A es un *subconjunto* de un conjunto B o que A está *contenido* en B , y en ese caso escribimos $A \subseteq B$, si todo elemento de A es un elemento de B , esto es, si

$$x \in A \implies x \in B.$$

Si además es $A \neq B$, decimos que A es un subconjunto *propio* de B y escribimos, si queremos enfatizar esto, $A \subsetneq B$.

1.2.2. Proposición. Sean A, B y C conjuntos.

- (i) Se tiene que $A \subseteq A$.
- (ii) Si $A \subseteq B$ y $B \subseteq A$, entonces $A = B$.
- (iii) Si $A \subseteq B$ y $B \subseteq C$, entonces $A \subseteq C$.

Demostración. (i) Si x es un elemento de A , entonces claramente x es un elemento de A : esto significa, precisamente, que A está contenido en A , es decir, que $A \subseteq A$.

(ii) Supongamos que $A \subseteq B$ y que $B \subseteq A$ y mostremos que $A = B$. Si x es un elemento de A , entonces, como $A \subseteq B$, tenemos que $x \in B$; se manera similar, si x es un elemento de B , entonces como $B \subseteq A$ podemos deducir que $x \in A$. Vemos así que A y B tienen exactamente los mismos elementos y, por lo tanto, que $A = B$.

(iii) Supongamos que $A \subseteq B$ y que $B \subseteq C$ y sea x un elemento de A . Como $A \subseteq B$, de que x pertenezca a A se deduce que x pertenece a B . De esto y de que $B \subseteq C$ se deduce, a su vez, que x pertenece a C . Vemos así que todo elemento de A es un elemento de C y, por lo tanto, que $A \subseteq C$, como afirma el enunciado. \square

1.2.3. Proposición. Sea A un conjunto.

- (i) Se tiene que $\emptyset \subseteq A$.
- (ii) Si $A \subseteq \emptyset$, entonces $A = \emptyset$.

Demostración. (i) Todo elemento de \emptyset pertenece a A , simplemente porque no hay ningún elemento en \emptyset : esto nos dice que $\emptyset \subseteq A$.

(ii) Supongamos que $A \subseteq \emptyset$ y que A no es vacío, de manera que A posee al menos un elemento x . Como $x \in A$ y $A \subseteq \emptyset$, vemos así que $x \in \emptyset$. Esto es absurdo y esta contradicción provino de haber supuesto que A no es vacío: podemos concluir entonces que A tiene que ser necesariamente vacío. \square

1.2.4. Si A es un conjunto, el *conjunto de partes* de A es el conjunto $\mathcal{P}(A)$ cuyos elementos son los subconjuntos de A . Así, se tiene que

$$B \in \mathcal{P}(A) \iff B \subseteq A.$$

1.2.5. Proposición. Sean A y B conjuntos.

- (i) El conjunto vacío \emptyset y el conjunto A son elementos de $\mathcal{P}(A)$ y, en particular, el conjunto $\mathcal{P}(A)$ no es vacío.
- (ii) Si $A \subseteq B$, entonces $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.

Demostración. (i) Sabemos de la Proposición 1.2.3(i) y de la Proposición 1.2.2(i) que $\emptyset \subseteq A$ y que $A \subseteq A$, así que $\emptyset \in \mathcal{P}(A)$ y $A \in \mathcal{P}(A)$.

(ii) Supongamos que $A \subseteq B$ y sea $C \in \mathcal{P}(A)$, de manera que $C \subseteq A$. Usando la Proposición 1.2.2(iii) y el hecho de que $C \subseteq A$ y $A \subseteq B$, vemos que $C \subseteq B$, esto es, que $C \in \mathcal{P}(B)$. Así, todo elemento de $\mathcal{P}(A)$ está en $\mathcal{P}(B)$ y, por lo tanto, $\mathcal{P}(A) \subseteq \mathcal{P}(B)$, como afirma el enunciado. \square

1.2.6. El único subconjunto del conjunto vacío es el conjunto vacío —esto es precisamente lo que nos dice la Proposición 1.2.3(ii)— así que $\mathcal{P}(\emptyset)$ tiene exactamente un elemento. Los subconjuntos del conjunto $\{1\}$ son

$$\emptyset \text{ y } \{1\}$$

así que $\mathcal{P}(\{1\})$ tiene 2 elementos. De manera similar, los subconjuntos de $\{1,2\}$ y de $\{1,2,3\}$ son, respectivamente,

$$\emptyset, \{1\}, \{2\}, \{1,2\},$$

y

$$\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\},$$

así que los conjuntos de partes $\mathcal{P}(\{1,2\})$ y $\mathcal{P}(\{1,2,3\})$ tienen $4 = 2^2$ y $8 = 2^3$ elementos. Veremos un poco más adelante que este patrón se cumple con toda generalidad, de manera que tenemos el siguiente resultado:

Proposición. Si A es un conjunto finito y $n \in \mathbb{N}_0$ es el número de elementos de sus elementos, entonces el conjunto de partes $\mathcal{P}(A)$ es finito y tiene exactamente 2^n elementos.

Daremos la prueba de esta proposición cuando tengamos a nuestra disposición el principio de inducción.

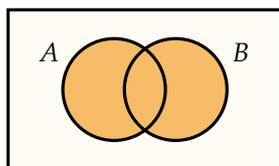
§1.3. Operaciones entre conjuntos

Unión

1.3.1. Si A y B son conjuntos, la **unión** de A y B es el conjunto $A \cup B$ tal que un elemento pertenece a $A \cup B$ si y solamente si pertenece a A o a B , esto es, tal que

$$x \in A \cup B \iff x \in A \text{ o } x \in B.$$

En términos de diagramas de Venn, la unión de A y B es



1.3.2. Proposición. Sean A , B y C tres conjuntos.

- (i) $A \subseteq A \cup B$ y $B \subseteq A \cup B$.
- (ii) Si $A \subseteq C$ y $B \subseteq C$, entonces $A \cup B \subseteq C$.
- (iii) Se tiene que $A \subseteq B$ si y solamente si $A \cup B = B$.

Demostración. (i) Si $x \in A$, entonces claramente se tiene que $x \in A$ o $x \in B$, y esto significa que $x \in A \cup B$: vemos así que $A \subseteq A \cup B$. Para ver la segunda parte del enunciado procedemos de exactamente la misma manera.

(ii) Supongamos que $A \subseteq C$ y que $B \subseteq C$ y mostremos que $A \cup B \subseteq C$. Sea $x \in A \cup B$, de manera que $x \in A$ o $x \in B$. En el primer caso, de que $x \in A$ y que $A \subseteq C$ podemos deducir que $x \in C$; en el segundo, de que $x \in B$ y que $B \subseteq C$, que también $x \in C$. Así, en cualquier caso se tiene que $x \in C$ y esto prueba que todo elemento de $A \cup B$ es un elemento de C , esto es, que $A \cup B \subseteq C$, como queremos.

(iii) Supongamos primero que $A \subseteq B$. Como además es $B \subseteq B$, usando la parte (ii) que acabamos de probar podemos deducir que $A \cup B \subseteq B$. Por otro lado, la parte (i) nos dice que $B \subseteq A \cup B$. Juntando estas dos cosas, la Proposición 1.2.2(ii) nos permite concluir que $A \cup B = B$. Vemos así que si $A \subseteq B$, entonces $A \cup B = B$.

Probemos ahora la implicación recíproca: que si $A \cup B = B$, entonces $A \subseteq B$. Supongamos entonces que $A \cup B = B$. De la parte (i) de la proposición sabemos que $A \subseteq A \cup B$ y, por hipótesis, este último conjunto es igual a B , así que $A \subseteq B$, que es lo que queremos. \square

1.3.3. Proposición. Sean A , B y C tres conjuntos.

- (i) $A \cup A = A$.
- (ii) $A \cup \emptyset = A$.
- (iii) $A \cup B = B \cup A$.

$$(iv) (A \cup B) \cup C = A \cup (B \cup C).$$

Demostración. (i) De la Proposición 1.3.2(i) sabemos que $A \subseteq A \cup A$, y de la Proposición 1.3.2(ii), como $A \subseteq A$, que $A \cup A \subseteq A$. Estas dos inclusiones nos dicen que $A \cup A = A$.

(ii) Como $A \subseteq A$ y $\emptyset \subseteq A$, de la Proposición 1.3.2(ii) tenemos que $A \cup \emptyset \subseteq A$. Por otro lado, de la Proposición 1.3.2(i) sabemos que $A \subseteq A \cup \emptyset$. Vemos así que $A \cup \emptyset = A$.

(iii) De la Proposición 1.3.2(i) sabemos que $A \subseteq B \cup A$ y que $B \subseteq B \cup A$ y entonces, gracias a la Proposición 1.3.2(ii), podemos concluir que $A \cup B \subseteq B \cup A$. Exactamente el mismo argumento pero intercambiando los roles de A y de B muestra que $B \cup A \subseteq A \cup B$ y, juntando todo, que $A \cup B = B \cup A$.

(iv) Sea x un elemento de $(A \cup B) \cup C$, de manera que o $x \in A \cup B$ o $x \in C$.

- En el segundo caso, tenemos que $x \in B \cup C$ y, por lo tanto que $x \in A \cup (B \cup C)$.
- En el primer caso, tenemos que o $x \in A$ o $x \in B$. Si $x \in A$, entonces claramente $x \in A \cup (B \cup C)$. Si en cambio $x \in B$, entonces $x \in B \cup C$ y, por lo tanto, $x \in A \cup (B \cup C)$.

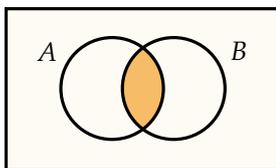
Vemos así que en cualquier caso se tiene que x pertenece a $A \cup (B \cup C)$, y esto prueba que $(A \cup B) \cup C \subseteq A \cup (B \cup C)$. Un razonamiento completamente similar muestra que $A \cup (B \cup C) \subseteq (A \cup B) \cup C$ y podemos concluir entonces que $(A \cup B) \cup C = A \cup (B \cup C)$, como afirma el enunciado. \square

Intersección

1.3.4. Si A y B son conjuntos, la *intersección* de A y B es el conjunto $A \cap B$ de los elementos que pertenecen simultáneamente a A y a B , esto es, el conjunto tal que

$$x \in A \cap B \iff x \in A \text{ y } x \in B.$$

En términos de diagramas de Venn, la intersección de A y B es



Decimos que A y B son *disjuntos* si la intersección $A \cap B$ es vacía.

1.3.5. Proposición. Sean A , B y C tres conjuntos.

(i) $A \cap B \subseteq A$ y $A \cap B \subseteq B$.

- (ii) Si $C \subseteq A$ y $C \subseteq B$, entonces $C \subseteq A \cap B$.
- (iii) Se tiene que $A \subseteq B$ si y solamente si $A \cap B = A$.

Demostración. (i) Si $x \in A \cap B$, entonces $x \in A$ y $x \in B$: en particular, x es un elemento de A . Esto nos dice que todo elemento de $A \cap B$ es elemento de A , es decir, que se tiene que $A \cap B \subseteq A$. Que $A \cap B \subseteq B$ se prueba de la misma forma.

(ii) Supongamos que $C \subseteq A$ y que $C \subseteq B$ y mostremos que $C \subseteq A \cap B$. Sea $x \in C$. Como $C \subseteq A$, de que x pertenezca a C podemos deducir que $x \in A$; de manera similar, de que $C \subseteq B$ obtenemos que $x \in B$. Como x pertenece tanto a A como a B , pertenece a $A \cap B$. Esto muestra que bajo nuestras hipótesis es $C \subseteq A \cap B$, como queremos.

(iii) Mostremos primero que si $A \subseteq B$ entonces $A \cap B = A$. Supongamos, para ello, que $A \subseteq B$. De la parte (i) de la proposición sabemos que $A \cap B \subseteq A$. Por otro lado, si $x \in A$, entonces $x \in B$ porque $A \subseteq B$ y, en consecuencia, $x \in A \cap B$: esto muestra que todo elemento de A es pertenece a $A \cap B$, es decir, que $A \subseteq A \cap B$. Como valen las dos inclusiones, vemos de esta forma que $A \cap B = A$.

Mostremos ahora que si $A \cap B = A$ entonces $A \subseteq B$. Supongamos para ello que $A \cap B = A$ y sea $x \in A$. Como x pertenece a A y $A = A \cap B$, tenemos por supuesto que $x \in A \cap B$ y, en particular, que x pertenece a B . Esto prueba que $A \subseteq B$. \square

1.3.6. Proposición. Sean A, B y C tres conjuntos.

- (i) $A \cap A = A$.
- (ii) $A \cap \emptyset = \emptyset$.
- (iii) $A \cap B = B \cap A$.
- (iv) $(A \cap B) \cap C = A \cap (B \cap C)$.

Demostración. (i) De la Proposición 1.3.5(i) sabemos que $A \cap A \subseteq A$. Por otro lado, como $A \subseteq A$, de la Proposición 1.3.5(ii) sabemos también que $A \subseteq A \cap A$. En definitiva, tenemos que $A = A \cap A$.

(ii) Es $A \cap \emptyset \subseteq \emptyset$ por la Proposición 1.3.5(i) y entonces, de acuerdo a la Proposición 1.2.3(ii), es $A \cap \emptyset = \emptyset$.

(iii) Sabemos que $A \cap B \subseteq B$ y que $A \cap B \subseteq A$, así que la Proposición 1.3.5(ii) implica que $A \cap B \subseteq B \cap A$. Intercambiando los roles de A y B en este razonamiento, vemos que también $B \cap A \subseteq A \cap B$ y, por lo tanto, que $A \cap B = B \cap A$.

(iv) Sea $x \in (A \cap B) \cap C$. Se tiene entonces que $x \in A \cap B$ y que $x \in C$, y que x pertenezca a $A \cap B$ implica que $x \in A$ y que $x \in B$. Ahora bien, como $x \in B$ y $x \in C$, es $x \in B \cap C$; como además $x \in A$, tenemos que $x \in A \cap (B \cap C)$. Vemos de esta forma que

$$(A \cap B) \cap C \subseteq A \cap (B \cap C). \quad (4)$$

Para probar la inclusión recíproca, observemos que

$$\begin{aligned}
 A \cap (B \cap C) &= A \cap (C \cap B) && \text{porque } B \cap C = C \cap B, \text{ en vista de la parte (iii)} \\
 &= (C \cap B) \cap A && \text{otra vez por la parte (iii)} \\
 &\subseteq C \cap (B \cap A) && \text{porque ya sabemos que (4) vale} \\
 &= (B \cap A) \cap C && \text{por (iii)} \\
 &= (A \cap B) \cap C && \text{por la misma razón.}
 \end{aligned}$$

En definitiva, tenemos que $(A \cap B) \cap C = A \cap (B \cap C)$, como afirma el enunciado. \square

1.3.7. Las Proposiciones **1.3.5** y **1.3.6** son completamente paralelas a las Proposiciones **1.3.2** y **1.3.3**. El siguiente resultado, por su parte, nos dice cómo se relacionan entre sí las operaciones de unión e intersección.

Proposición. Sean A , B y C tres conjuntos.

- (i) $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$.
- (ii) $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$.

Demostración. (i) Supongamos primero que $x \in (A \cap B) \cup C$. Hay dos casos:

- Si $x \in C$, entonces claramente $x \in A \cup C$ y $x \in B \cup C$, así que $x \in (A \cup C) \cap (B \cup C)$.
- Si en cambio $x \in A \cap B$, entonces sabemos que tanto $x \in A$ como $x \in B$. De lo primero deducimos que $x \in A \cup C$ y de lo segundo que $x \in B \cup C$ y, juntando estas dos cosas, que $x \in (A \cup C) \cap (B \cup C)$.

En cualquier caso, entonces, se tiene que $x \in (A \cup C) \cap (B \cup C)$ y esto prueba que

$$(A \cap B) \cup C \subseteq (A \cup C) \cap (B \cup C). \quad (5)$$

Supongamos ahora que $x \in (A \cap C) \cup (B \cap C)$. Otra vez hay dos posibilidades:

- Si $x \in A \cap C$, entonces tenemos que $x \in A$ y que $x \in C$. De lo primero se deduce que $x \in A \cup B$, y de todo que $x \in (A \cup B) \cap C$.
- Si $x \in B \cap C$, entonces tenemos que $x \in B$ y que $x \in C$. Lo primero implica que $x \in A \cup B$ y esto y lo segundo que $x \in (A \cup B) \cap C$.

Vemos así que x pertenece a $(A \cup B) \cap C$ independientemente de en qué caso estemos, y esto muestra que

$$(A \cup C) \cap (B \cup C) \subseteq (A \cup B) \cap C. \quad (6)$$

Finalmente, de (5) y de (6) vemos que $(A \cup C) \cap (B \cup C) \subseteq (A \cap B) \cup C$, como queremos.

(ii) Sea $x \in (A \cup B) \cap C$. Sabemos que $x \in C$ y que $x \in A \cup B$, de manera que $x \in A$ o $x \in B$. En el primer caso, tenemos que $x \in A \cap C$ y, por lo tanto, que $x \in (A \cap C) \cup (B \cap C)$. En el segundo, tenemos que $x \in B \cap C$ y, por lo tanto, que $x \in (A \cap C) \cup (B \cap C)$. En cualquier caso, entonces, es $x \in (A \cap C) \cup (B \cap C)$, de manera que

$$(A \cup B) \cap C \subseteq (A \cap C) \cup (B \cap C). \quad (7)$$

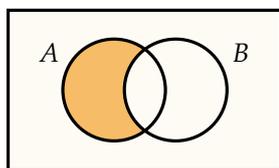
Supongamos ahora que x es un elemento de $(A \cap C) \cup (B \cap C)$. Si $x \in A \cap C$, entonces $x \in A$ y $x \in C$, así que $x \in A \cup B$ y, más aún, que $x \in (A \cup B) \cap C$. Si en cambio $x \in B \cap C$, entonces $x \in B$ y $x \in C$, así que $x \in A \cup B$ y $x \in (A \cup B) \cap C$. Vemos de esta forma que $(A \cap C) \cup (B \cap C) \subseteq (A \cup B) \cap C$ y esto, junto con (7), prueba que $(A \cap C) \cup (B \cap C) = (A \cup B) \cap C$, completando la prueba de la proposición. \square

Diferencia

1.3.8. Si A y B son conjuntos, la *diferencia* de A y B es el conjunto $A - B$ cuyos elementos son precisamente los elementos de A que no son elementos de B , esto es, el conjunto tal que

$$x \in A - B \iff x \in A \text{ y } x \notin B.$$

En términos de diagramas de Venn, la diferencia de $A - B$ es



Observemos que si $x \notin A - B$, entonces se tiene que $x \notin A$ o $x \in B$.

1.3.9. Proposición. Sean A, B y C tres conjuntos.

- (i) El conjunto $A - B$ está contenido en A y es disjunto de B .
- (ii) $A - A = \emptyset$ y $\emptyset - A = \emptyset$.
- (iii) Si $A - B = B - A$, entonces $A = B$.
- (iv) Es $(A - B) - C \subseteq A - (B - C)$.

Demostración. (i) Si $x \in A - B$, entonces de la definición misma de la diferencia de conjuntos sabemos que x pertenece a A : esto significa que $A - B \subseteq A$ y prueba la primera afirmación. Para probar la segunda, supongamos por un momento que el conjunto $(A - B) \cap B$ no es vacío, de manera que posee algún elemento x . Por supuesto

se tiene en ese caso que $x \in B$. Por otro lado, es $x \in A - B$ y, por lo tanto, $x \notin B$: esto es imposible. Esta contradicción muestra que nuestra suposición de que $(A - B) \cap B$ no es vacío no puede ser cierta y, en consecuencia, que podemos concluir de esto que $(A - B) \cap B = \emptyset$, esto es, que $A - B$ y B son disjuntos.

(ii) Supongamos que la diferencia $A - A$ no es vacía, de manera que posee algún elemento x . Como $x \in A - A$, de la definición de la diferencia tenemos que $x \in A$ y $x \notin A$: esto es imposible y esta contradicción proviene de haber supuesto que $A - A$ no es vacío. Vemos así que debe ser $A - A = \emptyset$.

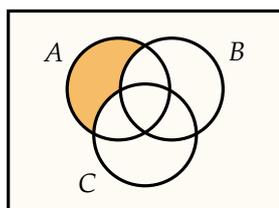
De la parte (i) sabemos que $\emptyset - A \subseteq \emptyset$, así que usando la Proposición 1.2.3(ii) podemos deducir que $\emptyset - A = \emptyset$.

(iii) Supongamos que $A \neq B$, de manera que $A \not\subseteq B$ o $B \not\subseteq A$. Si $A \not\subseteq B$, entonces existe un elemento x de A que no es un elemento de B : es claro que $x \in A - B$ y, como $B - A \subseteq B$, que $x \notin B - A$, así que $A - B \neq B - A$. Si en cambio $B \not\subseteq A$, entonces hay un elemento x de B que no pertenece a A , es $x \in B - A$ y $x \notin A - B$, ya que $A - B \subseteq A$: vemos otra vez que $A - B \neq B - A$.

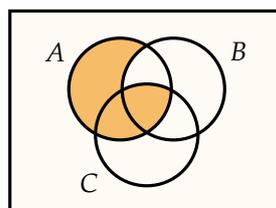
Hemos mostrado que si $A \neq B$, entonces $A - B \neq B - A$, y esta implicación es equivalente a la que aparece en el enunciado, ya que es su contrarrecíproca.

(iv) Sea x un elemento de $(A - B) - C$, de manera que $x \in A - B$ y $x \notin C$. Como $x \in A - B$, entonces $x \in A$ y $x \notin B$. En particular, de que x no pertenezca a B deducimos que $x \notin B - C$ y, juntando todo, que $x \in A - (B - C)$. \square

1.3.10. Observemos que no es cierto que valga la igualdad en la Proposición 1.3.9(iv). Por ejemplo, si tomamos $A = C = \{1\}$ y $B = \emptyset$, entonces el conjunto $(A - B) - C = \emptyset$ está contenido propiamente en $A - (B - C) = \{1\}$. En general, los conjuntos que aparecen en ese enunciado tienen los diagramas de Venn siguientes:



$(A - B) - C$



$A - (B - C)$

1.3.11. Proposición. Sean A , B y C tres conjuntos.

- (i) Es $(A - B) - C = A - B \cup C$.
- (ii) $A - (B - C) = (A - B) \cup (A \cap C)$.
- (iii) $A \cup (B - C) = (A \cup B) - (C - A)$.
- (iv) $A \cap (B - C) = (A \cap B) - (A \cap C)$.

Demostración. (i) Sea $x \in (A - B) - C$, de manera que $x \in A - B$ y $x \notin C$. Entonces $x \in A$ y $x \notin B$, así que $x \notin B \cup C$ y, por lo tanto $x \in A - B \cup C$.

Recíprocamente, sea $x \in A - B \cup C$, de forma que $x \in A$ y $x \notin B \cup C$. De esto último se deduce que $x \notin B$ y que $x \notin C$, así que tenemos que $x \in A - B$ y, finalmente que $x \in (A - B) - C$.

(ii) Sea $x \in A - (B - C)$. Se tiene entonces que $x \in A$ y $x \notin B - C$ y, por lo tanto, que $x \notin B$ o $x \in C$. En el primer caso tenemos que $x \in A - B$ y en el segundo que $x \in A \cap C$: vemos así que en cualquier caso es $x \in (A - B) \cup (A \cap C)$. Esto muestra que $A - (B - C) \subseteq (A - B) \cup (A \cap C)$.

Recíprocamente, supongamos que $x \in (A - B) \cup (A \cap C)$. Si $x \in A - B$, entonces $x \in A$ y $x \notin B$, así que $x \notin B - C$ y, en definitiva, $x \in A - (B - C)$. Si en cambio es $x \in A \cap C$, entonces $x \in A$ y $x \notin B - C$, así que $x \in A - (B - C)$. Esto prueba que $(A - B) \cup (A \cap C) \subseteq A - (B - C)$ y, junto con la inclusión que probamos antes, que vale la igualdad del enunciado.

(iii) Sea $x \in A \cup (B - C)$. Si $x \in A$, entonces $x \in A \cup B$ y $x \notin C - A$ y, por lo tanto, $x \in (A \cup B) - (C - A)$. Por otro lado, si $x \in B - C$, entonces $x \in B$, de manera que $x \in A \cup B$, y $x \notin C$, de manera que $x \notin C - A$ y, otra vez, $x \in (A \cup B) - (C - A)$. Concluimos de esta forma que

$$A \cup (B - C) \subseteq (A \cup B) - (C - A). \quad (8)$$

Sea ahora $x \in (A \cup B) - (C - A)$. Es $x \in A \cup B$ y $x \notin C - A$. Si $x \in A$, entonces claramente $x \in A \cup (B - C)$. Si $x \notin A$, entonces debe ser $x \in B$, ya que $x \in A \cup B$, y, como $x \notin C - A$, debe ser también $x \notin C$, así que $x \in B - C$ y, por lo tanto, $x \in A \cup (B - C)$. Esto nos dice que $A \cup (B - C) \subseteq (A \cup B) - (C - A)$ y, junto con (8), prueba lo que queremos.

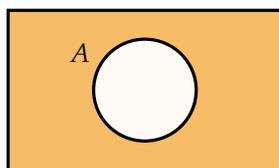
(iv) Sea $x \in A \cap (B - C)$, de manera que $x \in A$ y $x \in B - C$, es decir, $x \in B$ y $x \notin C$. Como $x \in A$ y $x \in B$, sabemos que $x \in A \cap B$; por otro lado, como $x \in A$ y $x \notin C$, es $x \notin A \cap C$. Estas dos cosas implican que $x \in A \cap B - A \cap C$ y, en definitiva, que $A \cap (B - C) \subseteq A \cap B - A \cap C$.

Sea, para verificar la inclusión recíproca, $x \in A \cap B - A \cap C$, de forma que $x \in A \cap B$ y $x \notin A \cap C$. Lo primero nos dice que $x \in A$ y $x \in B$, mientras que lo segundo nos dice, dado que x pertenece a A , que $x \notin C$. Tenemos así que $x \in B - C$ y, en consecuencia, que $x \in A \cap (B - C)$. Esto prueba que $A \cap B - A \cap C \subseteq A \cap (B - C)$ y, en vista de la inclusión que ya probamos, que vale de hecho la igualdad. \square

Complemento

1.3.12. Fijemos un conjunto U , al que llamaremos en este contexto el *conjunto de referencia*. Si A es un subconjunto de U , llamamos *complemento* de A (con respecto al

conjunto de referencia U) al conjunto $A^c = U - A$.



Es importante observar que el complemento A^c depende de la elección del conjunto de referencia U y que solamente está definido para subconjuntos de éste.

1.3.13. Proposición. Sea U un conjunto de referencia y sean A y B dos subconjuntos de U .

(i) Es $A \cup A^c = U$ y $A \cap A^c = \emptyset$.

(ii) $\emptyset^c = U$ y $U^c = \emptyset$.

(iii) $(A^c)^c = A$.

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

Observemos que si A es un subconjunto de U , entonces su complemento A^c con respecto a U también lo es, así que tiene sentido considerar su complemento $(A^c)^c$, como hicimos en la parte (iii) de esta proposición.

Demostración. (i) Es

$$\begin{aligned} A \cup A^c &= A \cup (U - A) \\ &= (A \cup U) - (A - A) && \text{por la Proposición 1.3.11(iii)} \\ &= U - \emptyset && \text{porque } A \subseteq U \\ &= U \end{aligned}$$

y

$$\begin{aligned} A \cap A^c &= A \cap (U - A) \\ &= A \cap U - A \cap A && \text{por la Proposición 1.3.11(iv)} \\ &= A - A && \text{porque } A \subseteq U \\ &= \emptyset. \end{aligned}$$

(ii) Claramente $\emptyset^c = U - \emptyset = U$ y $U^c = U - U = \emptyset$.

(iii) Es

$$\begin{aligned} (A^c)^c &= U - A^c \\ &= U - (U - A) \\ &= (U - U) \cup (U \cap A) && \text{por la Proposición 1.3.11(ii)} \\ &= \emptyset \cup A && \text{porque } A \subseteq U \end{aligned}$$

$$= A.$$

(iv) Si $x \in A - B$, entonces $x \in A$ y $x \notin B$. Como $A \subseteq U$, de que $x \in A$ obtenemos que $x \in U$ y, por lo tanto, que $x \in U - B = B^c$. Así, $x \in A \cap B^c$. Recíprocamente, si $x \in A \cap B^c$, entonces $x \in A$ y $x \in B^c = U - B$, de manera que $x \notin B$: vemos de esta forma que $x \in A - B$. \square

1.3.14. Las dos afirmaciones de la siguiente proposición son conocidas como las Leyes de Dualidad de De Morgan, por *Augustus De Morgan* (1806–1871, Inglaterra), uno de los fundadores de la lógica moderna.

Proposición. Sea U un conjunto de referencia y sean A y B dos subconjuntos de U .

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

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

Observemos que si A y B son subconjuntos de U , entonces $A \cup B$ y $A \cap B$ también lo son, así que tiene sentido considerar, como en esta proposición, los complementos $(A \cup B)^c$ y $(A \cap B)^c$ con respecto al conjunto U .

Demostración. (i) Supongamos que $x \in (A \cup B)^c$, de manera que $x \in U$ y $x \notin A \cup B$. Esto último significa que $x \notin A$ y que $x \notin B$. Vemos así que $x \in U - A = A^c$ y que $x \in U - B = B^c$ y, entonces, que $x \in A^c \cap B^c$.

Recíprocamente, sea $x \in A^c \cap B^c$. Es $x \in A^c$ y $x \in B^c$, así que $x \in U$, $x \notin A$ y $x \notin B$: de esto se deduce que $x \notin A \cup B$ y, por lo tanto, que $x \in U - A \cup B = (A \cup B)^c$.

(ii) Tenemos que

$$\begin{aligned} (A \cap B)^c &= ((A^c)^c \cap (B^c)^c)^c && \text{porque } A = (A^c)^c \text{ y } B = (B^c)^c \\ &= ((A^c \cup B^c)^c)^c && \text{por la parte (i) de la proposición} \\ &= A^c \cup B^c. \end{aligned}$$

Esta última igualdad es consecuencia de que $(X^c)^c = X$ para todo conjunto X y, en particular, cuando X es el conjunto $A^c \cup B^c$. \square

1.3.15. Proposición. Sea U un conjunto de referencia. Si A y B son dos subconjuntos de U , entonces

$$A \subseteq B \iff B^c \subseteq A^c.$$

Demostración. Sean A y B dos subconjuntos de U , supongamos que $A \subseteq B$ y sea $x \in B^c$. Como $x \in U$ y $x \notin B$, entonces $x \notin A$ y, por lo tanto, $x \in U - A = A^c$.

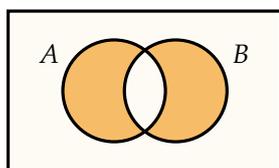
Supongamos, para probar la implicación recíproca, que $B^c \subseteq A^c$ y sea $x \in A$. Esto último implica que $x \notin A^c$ y, por lo tanto, que $x \notin B^c = U - B$. Como $x \in A \subseteq U$, de que x no pertenezca a $U - B$ podemos deducir que $x \in B$. Vemos así que $A \subseteq B$, como queremos. \square

Diferencia simétrica

1.3.16. Si A y B son dos conjuntos, la *diferencia simétrica* de A y B es el conjunto

$$A \triangle B = A \cup B - A \cap B.$$

En términos de diagramas de Venn, la diferencia simétrica de A y B es



1.3.17. Proposición. Si A y B son conjuntos, entonces

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

Muchas veces, la diferencia simétrica de dos conjuntos se define de esta forma, de hecho.

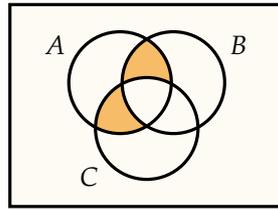
Demostración. Sea $x \in A \triangle B = A \cup B - A \cap B$, de manera que $x \in A \cup B$ y $x \notin A \cap B$. Hay dos posibilidades:

- Si $x \in A$, entonces, como $x \notin A \cap B$, necesariamente es $x \notin B$ y, por lo tanto, $x \in A - B$.
- Si en cambio $x \in B$, entonces de que $x \notin A \cap B$ deducimos ahora que $x \notin A$ y que $x \in B - A$.

En cualquiera de estos dos casos tenemos que $x \in (A - B) \cup (B - A)$ y, en definitiva, concluimos que $A \triangle B \subseteq (A - B) \cup (B - A)$.

Recíprocamente, supongamos que $x \in (A - B) \cup (B - A)$. Otra vez tenemos que considerar dos casos:

- Si $x \in A - B$, entonces $x \in A$ y $x \notin B$, así que $x \in A \cup B$ y $x \notin A \cap B$, por lo que $x \in A \cup B - A \cap B = A \triangle B$.
- Si $x \in B - A$, entonces $x \in B$ y $x \notin A$, así que $x \in B - A$ y $x \notin A \cap B$ y, como consecuencia de esto, otra vez tenemos que $x \in A \cup B - A \cap B = A \triangle B$.



$$A \cap (B \Delta C) = (A \cap B) \Delta (A \cap C)$$

Figura 1.1. El conjunto de la Proposición 1.3.18(iii).

Vemos así que $(A - B) \cup (B - A) \subseteq A \Delta B$. □

1.3.18. Proposición. Sean A , B y C tres conjuntos.

- (i) $A \Delta \emptyset = A$ y $A \Delta A = \emptyset$.
- (ii) $A \Delta B = B \Delta A$.
- (iii) $A \cap (B \Delta C) = (A \cap B) \Delta (A \cap C)$.

El conjunto que aparecen en la parte (iv) de esta proposición está ilustrado en la Figura 1.1.

Demostración. (i) Es

$$A \Delta \emptyset = A \cup \emptyset - A \cap \emptyset = A - \emptyset = A$$

y

$$A \Delta A = A \cup A - A \cap A = A - A = \emptyset.$$

(ii) Tenemos que

$$A \Delta B = A \cup B - A \cap B = B \cup A - B \cap B = B \Delta A.$$

(iii) Es

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

Esto completa la prueba de la proposición. □

1.3.19. Proposición. Sea U un conjunto de referencia. Si A y B son subconjuntos de U , entonces

$$(A \triangle B)^c = A^c \triangle B = A \triangle B^c.$$

Demostración. Sean A y B dos subconjuntos de U . Tenemos que

$$\begin{aligned} A^c \triangle B &= (U - A) \triangle B \\ &= ((U - A) - B) \cup (B - (U - A)) \\ &= (U - A \cup B) \cup ((B - U) \cup (A \cap B)) && \text{por 1.3.11(i) y 1.3.11(ii)} \\ &= (U - A \cup B) \cup (\emptyset \cup (A \cap B)) && \text{ya que } B \subseteq U \\ &= (U - A \cup B) \cup (A \cap B), \end{aligned} \tag{9}$$

que

$$\begin{aligned} A \triangle B^c &= B^c \triangle A && \text{por 1.3.18(ii)} \\ &= (U - B \cup A) \cup (B \cap A) && \text{por la igualdad (9)} \\ &= (U - A \cup B) \cup (A \cap B) && \text{por 1.3.3(iii) y 1.3.6(iii)} \end{aligned} \tag{10}$$

y que

$$\begin{aligned} (A \triangle B)^c &= U - A \triangle B \\ &= U - (A \cup B - A \cap B) \\ &= (U - A \cup B) \cup (U \cap (A \cap B)) && \text{por 1.3.11(ii)} \\ &= (U - A \cup B) \cup (A \cap B) && \text{porque } A \cap B \subseteq U. \end{aligned} \tag{11}$$

Comparando (9), (10) y (11) obtenemos las igualdades del enunciado. □

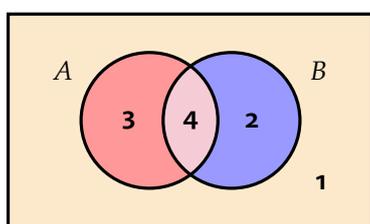
§1.4. Tablas de verdad

1.4.1. Muchas de las demostraciones que hicimos en la sección anterior requirieron la consideración de varios casos. Cada vez que hacemos eso, es importante ser sistemáticos, para asegurarnos de que no estamos dejando de lado alguna posibilidad. Hay varias estrategias para lograr eso. Veamos una de ellas.

Si estamos trabajando con dos conjuntos A y B y tenemos un elemento x , puede ser que x pertenezca o no a A y, por otro lado, que pertenezca o no a B . Tenemos entonces cuatro casos distintos posibles, que son las cuatro entradas de la siguiente tabla:

		$\text{¿}x \in B\text{?}$	
		No	Sí
$\text{¿}x \in A\text{?}$	No	1	2
	Sí	3	4

En un diagrama de Venn para A y B , cada uno de esos cuatro casos se corresponde con una de las regiones del dibujo:



Normalmente tabulamos esos casos en la siguiente forma, que es más conveniente:

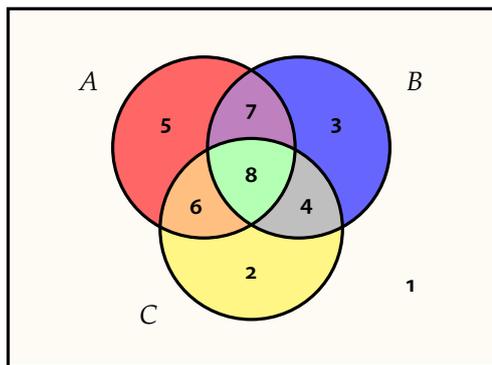
	$\text{¿}x \in A\text{?}$	$\text{¿}x \in B\text{?}$
1	No	No
2	No	Sí
3	Sí	No
4	Sí	Sí

Si en lugar de dos conjuntos tenemos tres, A , B y C , entonces un elemento x puede o no pertenecer a A , puede o no pertenecer a B y puede o no pertenecer a C : en total

esto nos da ocho casos, que son los que aparecen en la siguiente tabla:

	$\text{¿}x \in A\text{?}$	$\text{¿}x \in B\text{?}$	$\text{¿}x \in C\text{?}$
1	No	No	No
2	No	No	Sí
3	No	Sí	No
4	No	Sí	Sí
5	Sí	No	No
6	Sí	No	Sí
7	Sí	Sí	No
8	Sí	Sí	Sí

Como en el caso anterior, cada una de las filas de esta tabla se corresponde con una de las regiones del correspondiente diagrama de Venn:



1.4.2. Supongamos que queremos verificar que para cada par de conjuntos A y B se tiene que

$$A - A \triangle B = A \cap B. \quad (12)$$

Una forma de verlo es considerar un elemento x y considerar los cuatro casos que se obtienen de acuerdo a que x pertenezca o no a A y a B , y decidir en cada uno de ellos si x pertenece por un lado a $A - A \triangle B$ y por otro a $A \cap B$: si en cada uno de los cuatro casos x pertenece o bien a los dos o bien a ninguno, entonces habremos verificado la igualdad que queremos. Para organizar esta verificación, podemos usar tablas como las que describimos arriba para listar todos los casos.

Empecemos por ver en qué casos x pertenece a $A - A \triangle B$. Para ello, en primer lugar construimos la siguiente tabla y determinamos en qué casos x pertenece a $A \triangle B$:

$\text{¿}x \in A\text{?}$	$\text{¿}x \in B\text{?}$	$\text{¿}x \in A \triangle B\text{?}$
No	No	No
No	Sí	Sí
Sí	No	Sí
Sí	Sí	No

Hecho eso, extendemos la tabla con una columna en la que tabularemos, para cada uno de los casos, si x pertenece o no a la diferencia $A - A \triangle B$:

$\text{¿}x \in A\text{?}$	$\text{¿}x \in B\text{?}$	$\text{¿}x \in A \triangle B\text{?}$	$\text{¿}x \in A - A \triangle B\text{?}$
No	No	No	No
No	Sí	Sí	No
Sí	No	Sí	No
Sí	Sí	No	Sí

(13)

Por otro lado, podemos hacer una tabla que nos diga, para cada uno de los cuatro casos, si x pertenece o no a $A \cap B$:

$\text{¿}x \in A\text{?}$	$\text{¿}x \in B\text{?}$	$\text{¿}x \in A \cap B\text{?}$
No	No	No
No	Sí	No
Sí	No	No
Sí	Sí	Sí

(14)

Observemos ahora que en las tablas (13) y (14) las columnas « $\text{¿}x \in A - A \triangle B\text{?}$ » y « $\text{¿}x \in A \cap B\text{?}$ » son iguales: esto significa que en cada uno de los cuatro casos correspondientes a las filas de esas tablas el elemento x o bien pertenece a los dos conjuntos $A - A \triangle B$ y $A \cap B$, o bien no pertenece a ninguno de los dos. Claramente esto prueba que vale la igualdad (12).

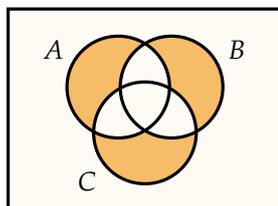
1.4.3. Veamos un ejemplo un poco más complicado:

Proposición. Si A , B y C son tres conjuntos, entonces

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

$\{x \in A?$	$\{x \in B?$	$\{x \in C?$	$\{x \in B \triangle C?$	$\{x \in A \triangle (B \triangle C)?$	$\{x \in A \triangle B?$	$\{x \in (A \triangle B) \triangle C?$
No	No	No	No	No	No	No
No	No	Sí	Sí	Sí	No	Sí
No	Sí	No	Sí	Sí	Sí	Sí
No	Sí	Sí	No	No	Sí	No
Sí	No	No	No	Sí	Sí	No
Sí	No	Sí	Sí	No	Sí	Sí
Sí	Sí	No	Sí	No	No	Sí
Sí	Sí	Sí	No	Sí	No	No

Tabla 1.1. La tabla de verdad de la prueba de la Proposición 1.4.3.



Demostración. En este caso tenemos tres conjuntos, A , B y C , así que cuando consideramos las distintas posibilidades en que un elemento x puede pertenecer o no a cada uno de ellos, tenemos ocho casos distintos. En cada uno de ellos tenemos que decidir si x pertenece o no a $A \triangle (B \triangle C)$ y a $(A \triangle B) \triangle C$, y para ello es útil decidir antes si pertenece a $B \triangle C$ y a $A \triangle B$. La Tabla 1.1 contiene todos los resultados.

Si comparamos la quinta columna de esa tabla y la séptima, notamos inmediatamente que son iguales: esto significa que un elemento x pertenece a $A \triangle (B \triangle C)$ si y solamente si pertenece a $(A \triangle B) \triangle C$ y, por lo tanto, estos dos conjuntos son iguales, como afirma la proposición. \square

1.4.4. Consideremos un último ejemplo de cómo podemos usar estas «tablas de verdad»:

$\text{¿}x \in A\text{?}$	$\text{¿}x \in B\text{?}$	$\text{¿}x \in C\text{?}$	$\text{¿}x \in A \cup B\text{?}$	$\text{¿}x \in (A \cup B) \cap C^c\text{?}$	$\text{¿}x \in B - C\text{?}$	$\text{¿}x \in A \Delta C\text{?}$	$\text{¿}x \in (B - C) \cup (A \Delta C)\text{?}$
No	No	No	No	No	No	No	No
No	No	Sí	No	No	No	Sí	Sí
No	Sí	No	Sí	Sí	Sí	No	Sí
No	Sí	Sí	Sí	No	No	Sí	Sí
Sí	No	No	Sí	Sí	No	Sí	Sí
Sí	No	Sí	Sí	No	No	No	No
Sí	Sí	No	Sí	Sí	Sí	Sí	Sí
Sí	Sí	Sí	Sí	No	No	No	No

Tabla 1.2. La tabla de verdad de la prueba de la Proposición 1.4.4.

Proposición. Sean A , B y C tres conjuntos. Si $C \subseteq A$, entonces

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

Demostración. Sean A , B y C tres conjuntos y supongamos que $C \subseteq A$. Otra vez tenemos tres conjuntos, así que hay en principio ocho posibilidades para la pertenencia de un elemento x a cada uno de ellos. La hipótesis que hicimos de que C está contenido en A hace, sin embargo, que algunos de esos casos sean imposibles: no puede ser que x pertenezca a C y no a A . Esto significa que cuando armemos la tabla que tabule todos los casos posibles hay que excluir todos aquellos en los que esa condición no se cumpla, que son dos: las marcamos en rojo.

Si comparamos la quinta columna con la octava, vemos que coinciden en todas sus entradas no marcadas en rojo. Esto prueba la proposición. \square

Es importante notar que esas dos columnas no son completamente iguales: sus entradas correspondientes a las filas rojas son efectivamente distintas, y eso significa

que la igualdad

$$(A \cup B) \cap C^c = (B - C) \cup (A \triangle C)$$

es falsa en general. La tabla nos permite encontrar un ejemplo de esto: las dos columnas difieren en las entradas correspondientes a la primera de las filas rojas, así que basta encontrar tres conjuntos A , B y C tales que haya un elemento x que corresponda a esa fila, es decir, tal que $x \notin A$, $x \notin B$ y $x \in C$. Por ejemplo, podemos elegir $A = B = \emptyset$ y $C = \{1\}$. En ese caso es $(A \cup B) \cap C^c = C^c$ mientras que $(B - C) \cup (A \triangle C) = C$, y estos dos conjuntos son efectivamente distintos.

Las columnas también difieren en sus entradas correspondientes a la segunda fila roja, en la que $x \notin A$, $x \in B$ y $x \in C$: esto nos sugiere otro ejemplo, con $A = \emptyset$ y $B = C = \{1\}$. Ahora $(A \cup B) \cap C^c = \emptyset$ mientras que $(B - C) \cup (A \triangle C) = C$.

§1.5. Ejercicios

Uniones e intersecciones de familias de conjuntos

1.5.1. Si \mathcal{F} es una familia de conjuntos, la *unión* de \mathcal{F} y la *intersección* de \mathcal{F} son los conjuntos que denotamos con los símbolos

$$\bigcup_{A \in \mathcal{F}} A \qquad \text{y} \qquad \bigcap_{A \in \mathcal{F}} A$$

tales que

$$x \in \bigcup_{A \in \mathcal{F}} A \iff \text{existe } A \in \mathcal{F} \text{ tal que } x \in A$$

y

$$x \in \bigcap_{A \in \mathcal{F}} A \iff \text{para cada } A \in \mathcal{F} \text{ se tiene que } x \in A.$$

Estas construcciones generalizan la unión y la intersección que ya vimos. En efecto, si X e Y son dos conjuntos, entonces la intersección y la unión de la familia $\mathcal{F} = \{X, Y\}$ son, respectivamente,

$$\bigcup_{A \in \mathcal{F}} A = X \cup Y, \qquad \bigcap_{A \in \mathcal{F}} A = X \cap Y.$$

1.5.2. Si \mathcal{F} es una familia de conjuntos y B es un conjunto, entonces

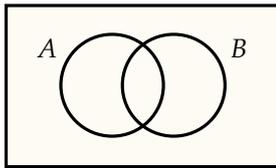
$$\bigcap_{A \in \mathcal{F}} (A \cup B) = \left(\bigcap_{A \in \mathcal{F}} A \right) \cup B, \quad \bigcup_{A \in \mathcal{F}} (A \cap B) = \left(\bigcup_{A \in \mathcal{F}} A \right) \cap B$$

y si todos los miembros de la familia \mathcal{F} están contenidos en un conjunto de referencia U , entonces además

$$\left(\bigcap_{A \in \mathcal{F}} A \right)^c = \bigcup_{A \in \mathcal{F}} A^c, \quad \left(\bigcup_{A \in \mathcal{F}} A \right)^c = \bigcap_{A \in \mathcal{F}} A^c.$$

Sistemas completos de operaciones

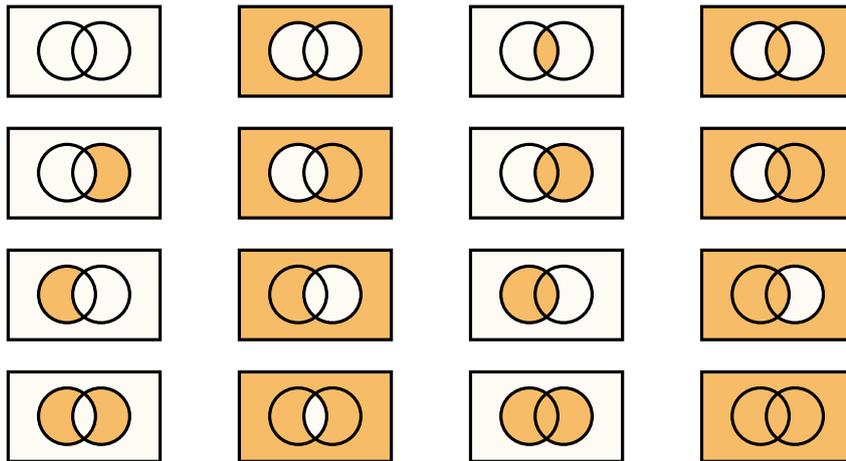
1.5.3. Sea U un conjunto de referencia y sean A y B dos subconjuntos de U . Consideremos el diagrama de Venn correspondiente a esta situación:



El conjunto U queda dividido así en 4 regiones:

$$A - B, \quad B - A, \quad A \cap B, \quad (A \cup B)^c$$

y considerando uniones de ellas podemos armar 16 conjuntos distintos.



Esto significa que podemos describir estos 16 conjuntos a partir de A y de B usando las operaciones de unión, intersección, diferencia y complemento.

1.5.4.

- (a) Muestre que para describir estos 16 conjuntos a partir de A y B es suficiente usar únicamente las operaciones de unión y complemento, o las de intersección y complemento.
- (b) Si X e Y son subconjuntos de U , definimos dos nuevas operaciones \downarrow y \uparrow poniendo

$$X \downarrow Y = (X \cup Y)^c, \quad X \uparrow Y = (X \cap Y)^c$$

Muestre que es posible describir cada uno de los 16 conjuntos del diagrama anterior a partir de A y B usando únicamente la operación \downarrow y también usando únicamente la operación \uparrow . Así, por ejemplo, se tiene que

$$A \cap B = (A \downarrow A) \downarrow (B \downarrow B)$$

y

$$A \cap B = (A \uparrow B) \uparrow (A \uparrow B).$$

Capítulo 2

Relaciones

§2.1. El producto cartesiano

2.1.1. Si A y B son dos conjuntos, el *producto cartesiano* de A y B es el conjunto $A \times B$ cuyos elementos son los pares ordenados (a, b) con $a \in A$ y $b \in B$.

Así, por ejemplo, si $A = \{1, 2\}$ y $B = \{\clubsuit, \diamond, \heartsuit, \spadesuit\}$, entonces el producto cartesiano $A \times B$ tiene por elementos a los ocho pares

$$(1, \clubsuit) \quad (1, \diamond) \quad (1, \heartsuit) \quad (1, \spadesuit) \quad (2, \clubsuit) \quad (2, \diamond) \quad (2, \heartsuit) \quad (2, \spadesuit).$$

De manera similar, el conjunto $\mathbb{N} \times \mathbb{R}$ es el de todos los pares (n, r) con n un número natural y r un número real, $\mathbb{Z} \times \mathbb{Z}$ es el de todos los pares (a, b) con a y b números enteros y $\mathbb{R} \times \mathbb{R}$ es el conjunto de pares ordenados (x, y) de números reales.

2.1.2. Es fácil decidir cuándo el producto cartesiano de dos conjuntos es vacío:

Proposición. Sean A y B dos conjuntos. El producto cartesiano $A \times B$ es vacío si y solamente si A es vacío o B es vacío.

Demostración. Supongamos primero que $A \times B$ no es vacío. Esto significa que existe algún par ordenado (a, b) con $a \in A$ y $b \in B$ y, en particular, ni A ni B son vacíos, ya que contienen, respectivamente, a a y a b .

Recíprocamente, supongamos que $A \times B$ es vacío y que A no lo es, de manera que existe un elemento a en A . Si B no fuera vacío, habría también un elemento b en B y podríamos, por lo tanto, construir el par ordenado (a, b) : este par sería en ese caso un elemento de $A \times B$ y esto es absurdo, ya que estamos suponiendo que el producto

cartesiano es vacío. Vemos así que B debe ser necesariamente vacío y esto prueba la proposición. \square

2.1.3. En el caso en que ambos factores son conjuntos finitos, el producto cartesiano es él mismo finito y podemos precisar su número de elementos:

Proposición. Sean A y B dos conjuntos. Si A y B son finitos y poseen, respectivamente, n y m elementos, entonces el producto cartesiano $A \times B$ es finito y tiene exactamente nm elementos.

Observemos que si A y B son finitos y alguno de los dos es vacío, de manera que $n = 0$ o $m = 0$, entonces esta proposición nos dice que $A \times B$ tiene $nm = 0$ elementos; recíprocamente, si $A \times B$ es vacío, es $nm = 0$ y, por lo tanto, alguno de n o m tiene que ser nulo. Esto es compatible, por supuesto, con lo que afirma la Proposición 2.1.2.

Demostración. Supongamos que A y B son finitos y que tienen n y m elementos, respectivamente. Sean

$$a_1, a_2, \dots, a_n \tag{1}$$

los elementos de A listados en algún orden y sin repeticiones, sean

$$b_1, b_2, \dots, b_m \tag{2}$$

los de B en algún orden y, otra vez, sin repeticiones y consideremos los nm pares ordenados

$$\begin{array}{cccc} (a_1, b_1), & (a_1, b_2), & \dots, & (a_1, b_m), \\ (a_2, b_1), & (a_2, b_2), & \dots, & (a_2, b_m), \\ \vdots & \vdots & \ddots & \vdots \\ (a_n, b_1), & (a_n, b_2), & \dots, & (a_n, b_m). \end{array} \tag{3}$$

Todos ellos pertenecen a $A \times B$ y, de hecho, todo elemento de $A \times B$ es uno de ellos. En efecto, si (a, b) es un elemento de $A \times B$, entonces a es un elemento de A , así que aparece en la lista (1) y hay un índice i tal que $a = a_i$, y b es un elemento de B , así que aparece en la lista (2) y hay un índice j tal que $b = b_j$: el par (a, b) es entonces el par (a_i, b_j) y es uno de los que están listados en (3).

Por otro lado, los nm pares ordenados que escribimos en (3) son distintos dos a dos. Supongamos, por ejemplo, que los pares $x = (a_i, b_j)$ y $u = (a_k, b_l)$ son iguales. Eso significa que son iguales componente a componente: esto es, que $a_i = a_k$ y que $b_j = b_l$. Ahora bien, los elementos de la lista (1) son distintos dos a dos y entonces como a_i y a_k son iguales se debe tener que los índices i y k mismos son iguales. Por la misma razón, los índices j y l son iguales, y vemos así que los pares x y u con los que empezamos son, de hecho, el mismo.

Concluimos así que la lista (3) incluye todos los elementos de $A \times B$ sin repeticiones: como hay allí nm elementos, vemos que $A \times B$ tiene nm elementos y, en particular, que es un conjunto finito. \square

§2.2. Relaciones

2.2.1. Si A y B son dos conjuntos, una *relación de A a B* es simplemente un subconjunto R del producto cartesiano $A \times B$. Llamamos a A el *dominio* de la relación R y a B su *codominio*. Si a y b son elementos de A y de B , respectivamente, entonces cuando el par ordenado (a, b) pertenece a R decimos que a *está relacionado* con b por R y escribimos

$$a R b.$$

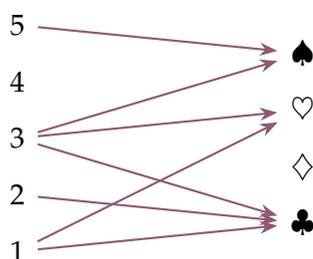
Si en cambio $(a, b) \notin R$, escribimos

$$a \not R b.$$

2.2.2. Consideremos un ejemplo sencillo. Sean $A = \{1, 2, 3, 4, 5\}$ y $B = \{\clubsuit, \spadesuit, \diamondsuit, \heartsuit\}$. El conjunto

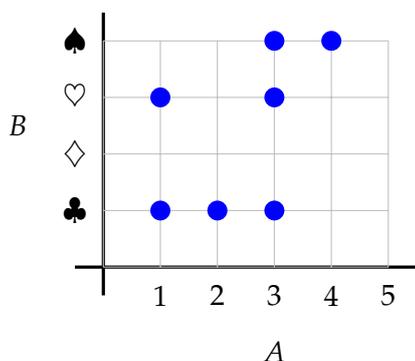
$$R = \{(1, \clubsuit), (1, \heartsuit), (2, \clubsuit), (3, \heartsuit), (3, \clubsuit), (3, \spadesuit), (4, \spadesuit)\}$$

es una relación de A a B . Una forma más eficiente de describir una relación como ésta, que va de un conjunto finito a otro, es dar un diagrama —al que llamamos el *grafo* de R — construido de la siguiente manera: ponemos a la izquierda los elementos de A encolumnados, a la derecha los de B y conectamos un elemento a de A con uno b de B con una flecha si y solamente si el par ordenado (a, b) está en R . En el ejemplo anterior, si hacemos esto obtenemos el siguiente diagrama:



Observemos que en este dibujo bien puede haber elementos de A o de B que no estén conectados con ningún elemento del otro conjunto y elementos que estén conectados con más de uno.

También podemos usar para representar gráficamente nuestra relación R un diagrama —el *gráfico* de la relación— como

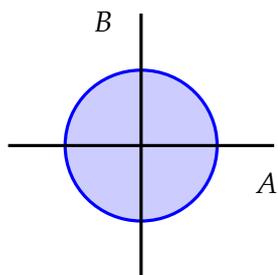


Aquí el eje horizontal y el vertical listan en algún orden y sin repeticiones los elementos de A y de B , respectivamente, y ponemos un punto por cada par ordenado de R de la manera evidente.

Esta última idea, a diferencia de la primera, puede usarse en ciertos casos para representar gráficamente relaciones entre conjuntos infinitos. Por ejemplo, si $A = B = \mathbb{R}$, entonces el conjunto

$$R = \{(x, y) \in \mathbb{R} \times \mathbb{R} : x^2 + y^2 \leq 1\}$$

es una relación de \mathbb{R} a \mathbb{R} y podemos representarla gráficamente usando el dibujo



Aquí, como siempre, vemos a los puntos a los puntos del plano como pares ordenados (x, y) con coordenadas $x \in A$ y $y \in B$, y pintamos los puntos que pertenecen a la relación.

2.2.3. Si A y B son conjuntos, siempre hay relaciones de A a B : esto es simplemente la observación de que el conjunto $\mathcal{P}(A \times B)$ de $A \times B$ no es vacío. Hay dos ejemplos extremos:

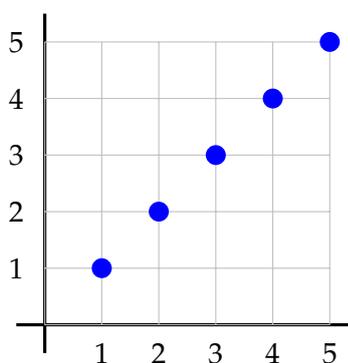
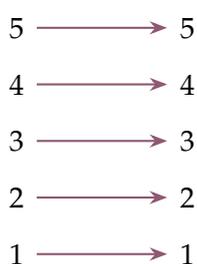
- la **relación vacía** de A a B es la relación $E = \emptyset \subseteq A \times B$, y
- la **relación total** de A a B es la relación $T = A \times B$.

Es posible que la relación vacía de A a B y la relación total sean la misma relación: esto pasa exactamente cuando alguno de los conjuntos A o B es vacío.

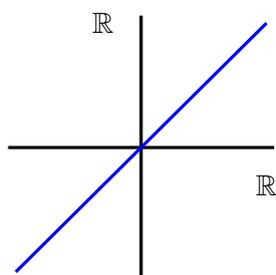
2.2.4. Si A es un conjunto, llamamos a la relación

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

de A a A la **relación identidad** de A . Si por ejemplo $A = \{1, 2, 3, 4\}$, el grafo y el gráfico de la relación I_A son, respectivamente,



En cambio, el gráfico de la relación identidad $I_{\mathbb{R}}$ del conjunto \mathbb{R} de los números reales es



Composición de relaciones

2.2.5. Si A , B y C son conjuntos, y $R \subseteq A \times B$ y $S \subseteq B \times C$ son relaciones de A a B y de B a C , respectivamente, entonces podemos construir una nueva relación de A a C , la **composición** $S \circ R$ de S y R , poniendo

$$S \circ R = \{(a, c) \in A \times C : \text{existe } b \in B \text{ tal que } a R b \text{ y } b S c\}.$$

Es importante observar que solamente consideramos esta construcción cuando el codominio de la relación R coincide con el dominio de la relación S .

2.2.6. Por ejemplo, si $A = \{\clubsuit, \diamond, \spadesuit, \heartsuit\}$, $B = \{1, 2, 3, 4, 5, 6\}$ y $C = \{\color{red}\bullet, \color{blue}\bullet, \color{yellow}\bullet, \color{teal}\bullet\}$ y tenemos las relaciones

$$R = \{(\heartsuit, 1), (\heartsuit, 4), (\heartsuit, 6), (\spadesuit, 3), (\spadesuit, 6), (\clubsuit, 1), (\clubsuit, 2), (\clubsuit, 4)\}$$

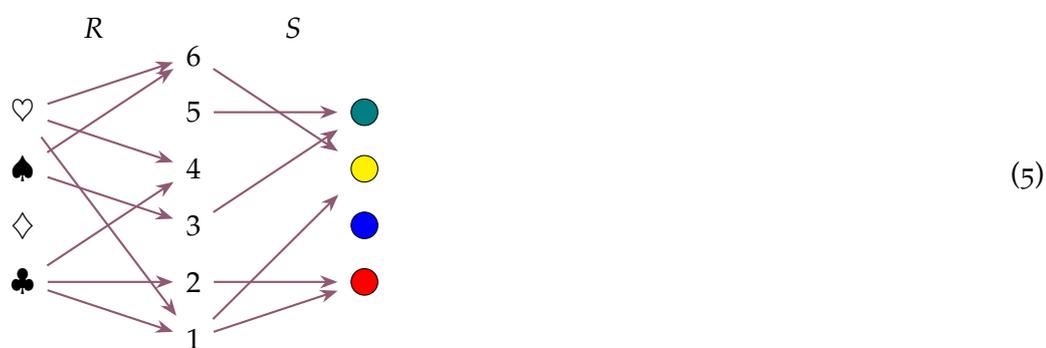
y

$$S = \{(1, \color{red}\bullet), (1, \color{yellow}\bullet), (2, \color{red}\bullet), (3, \color{teal}\bullet), (5, \color{teal}\bullet), (6, \color{yellow}\bullet)\},$$

entonces la composición de S y R es la relación de A a C

$$S \circ R = \{(\clubsuit, \color{red}\bullet), (\spadesuit, \color{teal}\bullet), (\spadesuit, \color{yellow}\bullet), (\heartsuit, \color{red}\bullet), (\heartsuit, \color{yellow}\bullet)\}. \quad (4)$$

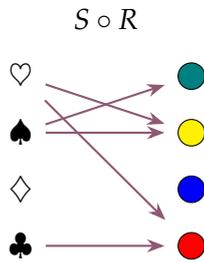
La forma más sencilla de verlo es construir el siguiente diagrama, que contiene simultáneamente el grafo de la relación R y el de la relación S :



Ahora bien, de acuerdo a la definición de la composición $S \circ R$, un elemento a de A está relacionado con uno c de C por la relación $S \circ R$ exactamente cuando hay un elemento b en B tal que $a R b$ y $b R c$. Así, por ejemplo, el par ordenado $(\heartsuit, \color{yellow}\bullet)$ pertenece a $S \circ R$ porque existe un elemento en B —a saber, el 6— tal que $(\heartsuit, 6) \in R$ y $(6, \color{yellow}\bullet) \in S$: en términos del diagrama anterior, podemos decir que \heartsuit está conectado con $\color{yellow}\bullet$ en la relación $S \circ R$ porque se puede llegar del primero al segundo pasando por 6 a lo largo de las flechas. De la misma forma, como se puede llegar de \clubsuit a $\color{red}\bullet$ pasando por 1, el par $(\clubsuit, \color{red}\bullet)$ pertenece a $S \circ R$. Notemos que también es posible llegar de \clubsuit a $\color{red}\bullet$ pasando por 2, pero esto no es importante: es suficiente con que haya *alguna* forma de llegar de uno al otro para que el correspondiente par ordenado esté en $S \circ R$. Finalmente, el par ordenado $(\spadesuit, \color{teal}\bullet)$ no es un elemento de $S \circ R$, ya que no hay forma de ir de \spadesuit a $\color{teal}\bullet$ en el diagrama.

Considerando con cuidado todos los pares, fácilmente construimos el grafo de la

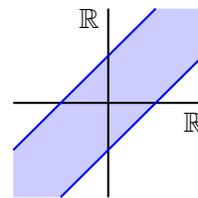
relación $S \circ R$ a partir del diagrama (5), y obtenemos



La descripción de $S \circ R$ que dimos en (4) es simplemente una transcripción de esto.

2.2.7. Veamos otro ejemplo: sean los conjuntos A , B y C todos iguales a \mathbb{R} y sea

$$R = \{(x, y) \in \mathbb{R} \times \mathbb{R} : |x - y| \leq 1\},$$



que es una relación de \mathbb{R} a \mathbb{R} . Si x e y son elementos de \mathbb{R} , entonces $x R y$ si y solamente si la distancia entre x e y es a lo sumo 1. Afirmamos que

$$R \circ R = \{(x, y) \in \mathbb{R} \times \mathbb{R} : |x - y| \leq 2\}. \quad (6)$$

Llamemos por un momento T a la relación de \mathbb{R} a \mathbb{R} que aparece en el miembro derecho de esta igualdad y probemos que $R \circ R = T$ probando las dos inclusiones entre los conjuntos $R \circ R$ y T .

Supongamos primero que $(x, y) \in R \circ R$, de manera que, de acuerdo a la definición de la composición, existe $z \in \mathbb{R}$ tal que $x R z$ y $z R y$. Esto significa que $|x - z| \leq 1$ y que $|z - y| \leq 1$ y entonces, gracias a la desigualdad triangular, tenemos que

$$|x - y| = |(x - z) - (z - y)| \leq |x - z| + |z - y| \leq 1 + 1 = 2.$$

Esto muestra que $(x, y) \in T$ y, en definitiva, que $R \circ R \subseteq T$.

Recíprocamente, supongamos que $(x, y) \in T$, de manera que $x, y \in \mathbb{R}$ y $|x - y| \leq 2$. Si ponemos $z = (x + y)/2$, tenemos que

$$|x - z| = \left| x - \frac{x + y}{2} \right| = \left| \frac{x - y}{2} \right| = \frac{|x - y|}{2} \leq \frac{2}{2} = 1$$

y, de manera similar, que

$$|z - y| \leq 1.$$

Esto nos dice que $x R z$ y que $z R y$ y, por lo tanto, que $(x, y) \in R \circ R$. Esto completa la prueba de nuestra afirmación (6).

2.2.8. La composición de relaciones es una operación asociativa:

Proposición. Sean A, B, C y D conjuntos y $R \subseteq A \times B$, $S \subseteq B \times C$ y $T \subseteq C \times D$ relaciones de A a B , de B a C y de C a D , respectivamente. Se tiene que

$$T \circ (S \circ R) = (T \circ S) \circ R.$$

Demostración. Sean $a \in A$ y $d \in D$.

Supongamos primero que $(a, d) \in T \circ (S \circ R)$. Esto significa que existe $c \in C$ tal que $(a, c) \in S \circ R$ y $(c, d) \in T$. La primera de estas dos cosas significa, a su vez, que existe $b \in B$ tal que $(a, b) \in R$ y $(b, c) \in S$. Ahora bien, de que $(b, c) \in S$ y $(c, d) \in T$ podemos deducir que $(b, d) \in T \circ S$ y de esto y de que $(a, b) \in R$, que $(a, d) \in (T \circ S) \circ R$. Concluimos de esta forma que $T \circ (S \circ R) \subseteq (T \circ S) \circ R$.

Supongamos ahora que $(a, d) \in (T \circ S) \circ R$, de manera que existe $b \in B$ tal que $(a, b) \in R$ y $(b, d) \in T \circ S$. Esto último nos dice que existe $c \in C$ tal que $(b, c) \in S$ y $(c, d) \in T$. Como $(a, b) \in R$ y $(b, c) \in S$, sabemos que $(a, c) \in S \circ R$ y de esto y de que $(c, d) \in T$, que $(a, d) \in T \circ (S \circ R)$. Esto prueba que $(T \circ S) \circ R \subseteq T \circ (S \circ R)$ y, junto con la inclusión anterior, la igualdad que aparece en el enunciado. \square

2.2.9. Las relaciones identidades se comportan como elementos neutros para la composición:

Proposición. Sean A y B dos conjuntos. Si $R \subseteq A \times B$ es una relación de A a B , entonces

$$I_B \circ R = R = R \circ I_A.$$

Demostración. Mostremos la primera de las dos igualdades — la segunda puede probarse de exactamente la misma forma. Sean $a \in A$ y $b \in B$ y supongamos primero que $(a, b) \in I_B \circ R$: esto significa que existe $b' \in B$ tal que $(b, b') \in I_B$ y $(a, b') \in R$. Pero si (b, b') está en I_B , entonces necesariamente $b' = b$ y, por lo tanto, tenemos que $(a, b) \in R$. Esto nos dice que $I_B \circ R \subseteq R$.

Recíprocamente, si $(a, b) \in R$, como además $(b, b) \in I_B$, tenemos claramente que $(a, b) \in I_B \circ R$: vemos así que $R \subseteq I_B \circ R$. \square

Inversión de relaciones

2.2.10. Si A y B son dos conjuntos y R es una relación de A a B , la *relación inversa* de R es la relación de B a A

$$R^{-1} = \{(x, y) \in B \times A : y R x\}.$$

Observemos que esto significa que si $x \in A$ e $y \in B$, entonces

$$y R^{-1} x \iff x R y.$$

El dominio y el codominio de la relación R^{-1} son, respectivamente, el codominio y el dominio de la relación de partida R .

2.2.11. Por ejemplo, si $A = \{\heartsuit, \spadesuit, \diamondsuit, \clubsuit\}$ y $B = \{1, 2, 3, 4, 5, 6\}$, la relación inversa de

$$R = \{(\heartsuit, 1), (\heartsuit, 4), (\heartsuit, 6), (\spadesuit, 3), (\spadesuit, 6), (\clubsuit, 1), (\clubsuit, 2), (\clubsuit, 4)\}$$

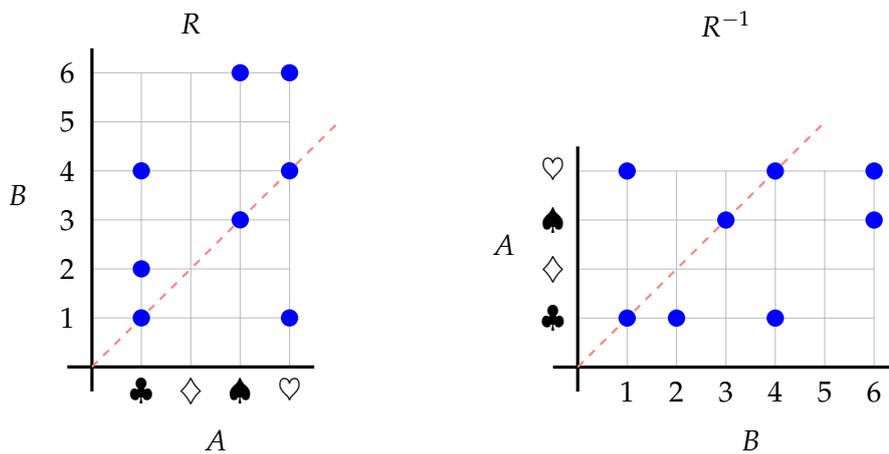
es

$$R^{-1} = \{(1, \heartsuit), (4, \heartsuit), (6, \heartsuit), (3, \spadesuit), (6, \spadesuit), (1, \clubsuit), (2, \clubsuit), (4, \clubsuit)\}.$$

Los grafos de estas relaciones son



y sus gráficos son



Es claro que el grafo de R^{-1} se obtiene del de R dando vuelta la dirección de las flechas e intercambiando de lugar las dos columnas de elementos, mientras que el gráfico

de R^{-1} se obtiene del de R reflejando el diagrama con respecto a la diagonal —la línea punteada roja.

2.2.12. Proposición. Sean A, B y C tres conjuntos. Si $R \subseteq A \times B$ es una relación de A a B y $S \subseteq B \times C$ una de B a C , entonces la relación inversa de la composición $S \circ R \subseteq A \times C$ es

$$(S \circ R)^{-1} = R^{-1} \circ S^{-1}.$$

Demostración. Sea R una relación de A a B y S una de B a C . Sean $c \in C$ y $a \in A$.

Supongamos primero que $(c, a) \in (S \circ R)^{-1}$. Esto significa que $(a, c) \in S \circ R$ y, por lo tanto, que existe $b \in B$ tal que $(a, b) \in R$ y $(b, c) \in S$. Pero entonces tenemos que $(b, a) \in R^{-1}$ y $(c, b) \in S^{-1}$, así que $(c, a) \in S^{-1} \circ R^{-1}$. Vemos así que $(S \circ R)^{-1} \subseteq S^{-1} \circ R^{-1}$.

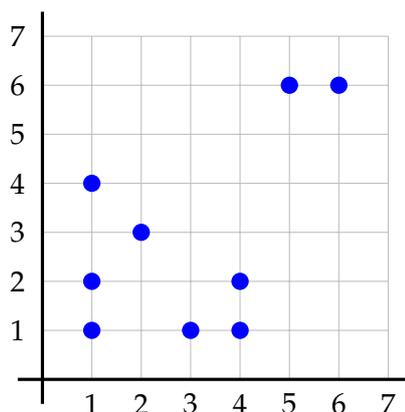
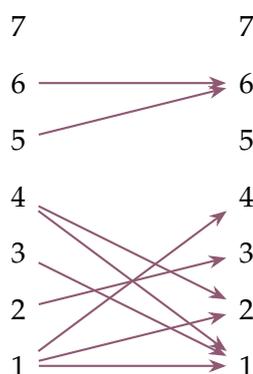
Supongamos ahora que $(c, a) \in R^{-1} \circ S^{-1}$. Esto significa que existe $b \in B$ tal que $(c, b) \in S^{-1}$ y $(b, a) \in R^{-1}$, es decir, tal que $(b, c) \in S$ y $(a, b) \in R$. Estas dos cosas implican entonces que $(a, c) \in S \circ R$, de manera que $(c, a) \in (S \circ R)^{-1}$, y esto prueba que $R^{-1} \circ S^{-1} \subseteq (S \circ R)^{-1}$. \square

§2.3. Relaciones en un conjunto

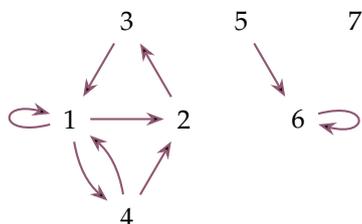
2.3.1. Si A es un conjunto y $R \subseteq A \times A$ es una relación de A a A , decimos que R es una **relación en A** . Por ejemplo, si $A = \{1, 2, 3, 4, 5, 6, 7\}$, la relación

$$R = \{(1, 1), (1, 2), (2, 3), (3, 1), (1, 4), (4, 1), (4, 2), (5, 6), (6, 6)\}$$

es una relación en A . Su grafo y su gráfico, respectivamente, son



En este caso, como el dominio y el codominio de R son ambos el mismo conjunto A , podemos dibujar el grafo poniendo una sola copia de cada elemento de A , de la siguiente manera:



No hay ya necesidad de encolumnar los elementos de A y generalmente los ubicamos de la manera que haga que el diagrama sea lo más claro posible.

Casi siempre que hacemos un diagrama para una relación *en* un conjunto lo hacemos de esta forma. Observemos que es importante marcar la dirección de cada una de las flechas: bien puede ser que una relación tenga un par (x, y) pero no el par inverso (y, x) , como en este ejemplo en el que $(1, 2)$ pertenece a R pero $(2, 1)$ no. De manera similar, la relación de nuestro ejemplo contiene el par $(1, 1)$ pero no el $(3, 3)$: marcamos en el diagrama la presencia del primero usando el bucle $1 \rightarrow$.

En el grafo de una relación R en un conjunto puede haber a lo sumo *dos* flechas entre dos elementos distintos x e y del su dominio: las que van en una y en otra dirección, correspondiendo a los pares (x, y) e (y, x) que, por supuesto, pueden o no pertenecer a la relación. Por otro lado, puede haber a lo sumo *una* flecha de un elemento x a sí mismo, correspondiendo a que el par ordenado (x, x) puede o no estar en R .

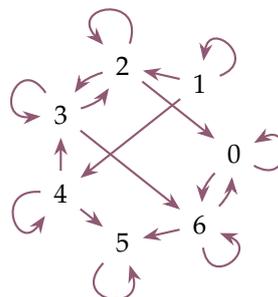
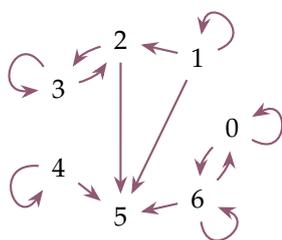
Relaciones reflexivas

2.3.2. Una relación $R \subseteq A \times A$ en un conjunto no vacío A es *reflexiva* si para todo elemento a de A se tiene que

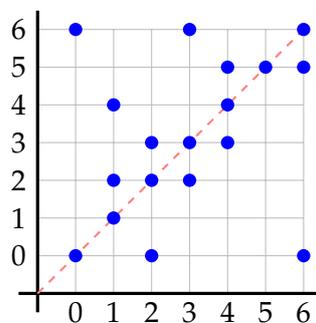
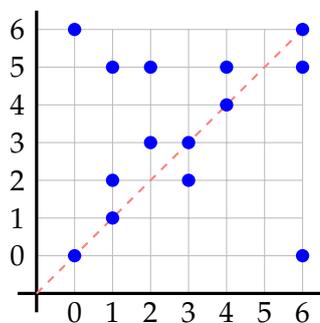
$$a R a,$$

es decir, que el par (a, a) pertenece a R . En términos del grafo de la relación R , esto significa que en cada uno de los puntos que representan a los elementos de A hay un

bucle: así, de los siguientes dos grafos de relaciones en el conjunto $\{0, 1, 2, 3, 4, 5, 6\}$



sólo el de la derecha representa una que es reflexiva. En términos de los gráficos también es inmediato reconocer la reflexividad: por ejemplo, las dos relaciones que acabamos de considerar tienen gráficos



y que el segundo corresponda a una relación que es reflexiva mientras que el primero no se refleja en que todos los puntos que están sobre la diagonal roja están marcados en él, mientras que ése no es el caso en el primero.

2.3.3. La siguiente observación es inmediata:

Proposición. Sea A un conjunto no vacío y sea $R \subseteq A \times A$ una relación en A . La relación R es reflexiva si y solamente si contiene a la relación identidad I_A .

Demostración. En efecto, esto es consecuencia directa de la definición de I_A . □

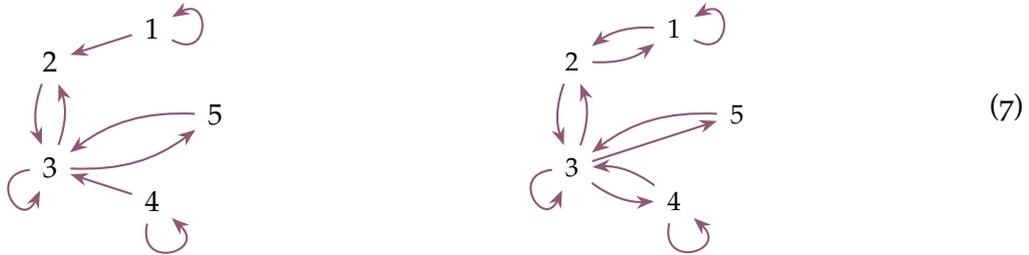
Relaciones simétricas

2.3.4. Una relación $R \subseteq A \times A$ en un conjunto no vacío A es *simétrica* si cada vez que a y b son elementos de A se tiene que

$$a R b \implies b R a.$$

En términos del grafo de la relación, esto significa que si a y b son dos elementos de A tales que hay una flecha que va de a a b en el grafo, entonces necesariamente hay también otra que va en la dirección contraria, esto es, de b a a .

Los siguientes grafos representan dos relaciones en el conjunto $A = \{1, 2, 3, 4, 5\}$



La primera no es simétrica: contiene la flecha que va de 4 a 3 pero no la que va de 3 a 4. En cambio, la segunda de estas relaciones es simétrica.

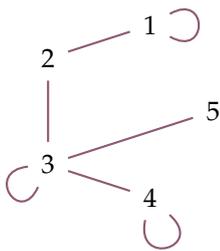
Cuando dibujamos el grafo de una relación simétrica cada flecha viene acompañada siempre de su flecha inversa. Para simplificar el dibujo podemos convenir en dibujar simplemente una línea entre dos elementos, sin dirección,



en lugar del par de flechas mutuamente inversas



Usando esta convención, podemos representar la relación del segundo diagrama de (7) con el dibujo más sencillo



Observemos que aquí también eliminamos la orientación de las flechas que forman bucles: claramente esa orientación no agrega información alguna.

2.3.5. Proposición. Sea A un conjunto no vacío. Una relación $R \subseteq A \times A$ en A es simétrica si y solamente si es igual a su relación inversa, esto es, si y solamente si

$$R = R^{-1}.$$

Demostración. Sea $R \subseteq A \times A$ una relación en A y supongamos primero que R es simétrica: tenemos que mostrar que $R = R^{-1}$. Si $(a, b) \in R$, de manera que $a R b$, entonces la simetría de R nos dice que $b R a$, esto es, que $(b, a) \in R$: de acuerdo a la definición de R^{-1} , entonces, tenemos que $(a, b) \in R^{-1}$. Vemos así que $R \subseteq R^{-1}$, y un razonamiento exactamente análogo prueba que también $R^{-1} \subseteq R$, de manera que $R = R^{-1}$, como queremos.

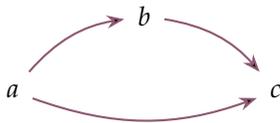
Supongamos ahora que $R = R^{-1}$ y probemos que R es necesariamente simétrica. Sean a y b dos elementos de R tales que $a R b$, esto es, tales que $(a, b) \in R$. Como $R = R^{-1}$ por nuestra hipótesis, esto nos dice que $(a, b) \in R^{-1}$ y, de acuerdo a la definición de la relación R^{-1} , que $(b, a) \in R$: la relación R es por lo tanto simétrica. \square

Relaciones transitivas

2.3.6. Una relación $R \subseteq A \times A$ en un conjunto no vacío A es *transitiva* si cada vez que a, b y c son elementos de A se tiene que

$$a R b \text{ y } b R c \implies a R c.$$

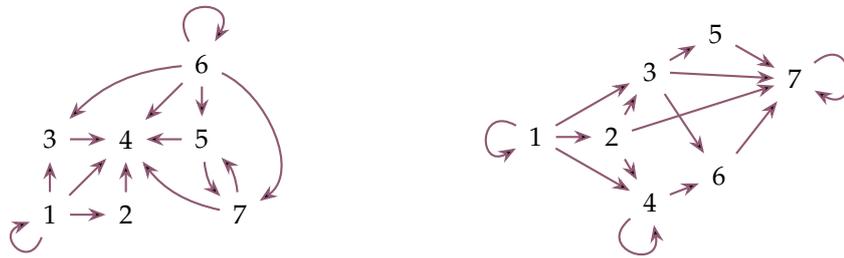
En términos del grafo de R , esto significa que si hay una flecha que va de a hasta b y otra que va de b hasta c , entonces tiene que haber también una flecha que va de a a c :



Así, la condición de transitividad es que si se puede llegar de un vértice a otro en dos pasos siguiendo las flechas, también se puede llegar en uno — en otras palabras, que siempre hay un “atajo”.

2.3.7. Veamos algunos ejemplos. Si $A = \{1, 2, 3, 4, 5, 6, 7\}$, la primera de las dos relacio-

nes siguientes es transitivas, mientras que la segunda no.



En efecto, en la segunda tenemos por ejemplo la flecha que va de 2 a 4 y la de 4 a 6, pero no la de 2 a 6.

2.3.8. Proposición. Sea A un conjunto no vacío. Una relación $R \subseteq A \times A$ en A es transitiva si y solamente si $R \circ R \subseteq R$.

Demostración. Sea $R \subseteq A \times A$ una relación en el conjunto A .

Supongamos primero que R es transitiva y sea (a, c) un elemento de $R \circ R$, de manera que existe $b \in A$ tal que $(a, b) \in R$ y $(b, c) \in R$. Como R es transitiva, de esto se deduce que $(a, c) \in R$: vemos así que $R \circ R \subseteq R$.

Recíprocamente, supongamos que $R \circ R \subseteq R$ y veamos que R es una relación transitiva. Supongamos que a, b y c son tres elementos de A tales que $a R b$ y $b R c$. Se tiene entonces que los pares ordenados (a, b) y (b, c) están en R , así que el par (a, c) está en $R \circ R$. Ahora bien, estamos suponiendo que $R \circ R \subseteq R$, así que esto último implica que $(a, c) \in R$, es decir, que $a R c$. Concluimos de esta manera que R es transitiva, como queremos. \square

§2.4. Relaciones de equivalencia

2.4.1. Una relación R en un conjunto no vacío A es una *relación de equivalencia* si es reflexiva, simétrica y transitiva.

2.4.2. Veamos algunos ejemplos de relaciones de equivalencia:

- (a) La relación identidad I_A y la relación total $A \times A$ en un conjunto no vacío A .

(b) Si $A = \{1\}$ tiene un único elemento, entonces hay dos relaciones en A —la vacía y la identidad— y la segunda de ellas es la única que es de equivalencia.



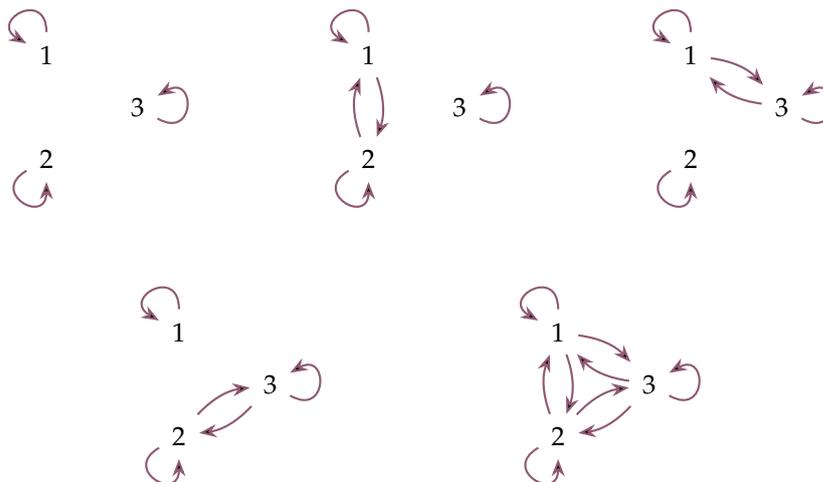
Si $A = \{1,2\}$ tiene dos elementos, entonces sabemos que $A \times A$ tiene 4 elementos y, por lo tanto, que el conjunto de partes $\mathcal{P}(A \times A)$ tiene $2^4 = 16$: esto nos dice que hay 16 relaciones sobre el conjunto A . De todas ellas, hay exactamente *dos* que son relaciones de equivalencia: la relación identidad y la relación total. En efecto, supongamos que R es una relación de equivalencia sobre A . Como es reflexiva, sabemos que los pares $(1,1)$ y $(2,2)$ están en R . Por otro lado, puede ser que $(1,2)$ esté o no en R . En el primer caso, como R es simétrica también está en ella el par $(2,1)$ y vemos que están todos los pares: la relación es, por lo tanto, la relación total



Si en cambio el par $(1,2)$ no está en R , entonces el par $(2,1)$ tampoco —ya que la relación es simétrica— y, por lo tanto, la relación es la relación identidad de A ,



Razonando de la misma forma, es fácil ver que sobre el conjunto $A = \{1,2,3\}$ hay cinco relaciones de equivalencia:



En general, si un conjunto A es finito y tiene n elementos, llamamos n -ésimo *número de Bell* a la cantidad de relaciones de equivalencia que hay en A y lo escribimos B_n . El nombre recuerda a *Eric Temple Bell* (1883–1960, Escocia), matemático y autor de ciencia ficción. Los primeros números de Bell son

n	1	2	3	4	5	6	7	8	9	10	11
B_n	1	2	5	15	52	203	877	4 140	21 147	115 975	678 570

Por supuesto, para contar las 115975 relaciones de equivalencia que hay sobre un conjunto de 10 elementos se requiere una estrategia más eficiente que la que usamos arriba!

- (c) La relación $R \subseteq \mathbb{Z} \times \mathbb{Z}$ en el conjunto \mathbb{Z} tal que para cada $x, y \in \mathbb{Z}$ se tiene que

$$x R y \iff |x| = |y|.$$

- (d) La relación $R \subseteq \mathbb{R} \times \mathbb{R}$ en el conjunto \mathbb{R} tal que cada vez que x e y son elementos de \mathbb{R} se tiene que

$$x R y \iff x^2 - 2x + 2 = y^2 - 2y + 2.$$

- (e) La relación $R \subseteq \mathbb{Z} \times \mathbb{Z}$ en el conjunto \mathbb{Z} dada por

$$R = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} : y - x \text{ es par}\}.$$

Más generalmente, si $k \in \mathbb{N}$ tenemos una relación de equivalencia $R_k \subseteq \mathbb{Z} \times \mathbb{Z}$ en el conjunto \mathbb{Z} dada por

$$R_k = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} : k \text{ divide a } y - x\}.$$

Probemos que esto es, en efecto, una relación de equivalencia.

- Si $x \in \mathbb{Z}$, entonces $x - x = 0 \cdot k$, así que k divide a $x - x$ y, por lo tanto, tenemos que $x R_k x$. Vemos así que la relación R_k es reflexiva.
- Supongamos que x e y son elementos de \mathbb{Z} tales que $x R_k y$, es decir, tales que k divide a $y - x$. Esto significa que existe $u \in \mathbb{Z}$ tal que $y - x = u \cdot k$. Por supuesto, tenemos entonces que $x - y = (-u) \cdot k$, así que k divide a la diferencia $x - y$ y, por lo tanto, $y R_k x$: vemos así que la relación R_k es simétrica.
- Finalmente, supongamos que x, y y z son elementos de \mathbb{Z} tales que $x R_k y$ e $y R_k z$, de manera que k divide a $y - x$ y a $z - y$. Esto significa que existen enteros $u, v \in \mathbb{Z}$ tales que $y - x = u \cdot k$ e $z - y = v \cdot k$: usando esto, vemos que

$$z - x = (z - y) + (y - x) = v \cdot k + u \cdot k = (v + u) \cdot k,$$

así que k también divide a la diferencia $z - x$ y, por lo tanto, es $x R_k z$. Concluimos de esta forma que R_k es una relación transitiva.

Cuando x e y son dos enteros y se tiene que $x R_k y$, decimos que x e y son **congruentes módulo k** y normalmente escribimos

$$x \equiv y \pmod{k}$$

en lugar de $x R_k y$. Esta relación de equivalencia es de extraordinaria importancia en teoría de los números enteros. Fue considerada de manera sistemática por primera vez por *Carl Friedrich Gauss* (1777–1855, Alemania) en su libro *Disquisitiones Arithmeticae* —escrito en 1798, cuando tenía 21 años, y publicado 1801— que es la fundación de la teoría moderna de números. La definición de la relación de congruencia ocupa, de hecho, la primera línea de ese texto — véase la Figura 2.1 en la página siguiente.

Clases de equivalencia

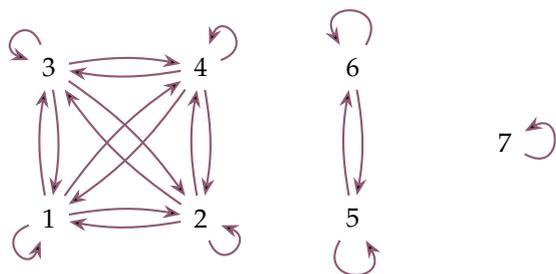
2.4.3. Sea A un conjunto no vacío y sea $R \subseteq A \times A$ una relación de equivalencia sobre A . Si x es un elemento de A , entonces la **clase de equivalencia** de x en A con respecto a la relación R es el conjunto

$$[x] = \{y \in A : x R y\}.$$

En otras palabras, la clase de equivalencia de x es el conjunto de todos los elementos de A que están relacionados por R con x . Llamamos **conjunto cociente** de A por R , y escribimos A/R , al conjunto de las clases de equivalencia de R en A :

$$A/R = \{[x] : x \in A\}.$$

Así, por ejemplo, si A es el conjunto $\{1, 2, 3, 4, 5, 6, 7\}$ y la relación R es la que tiene grafo



entonces las clases de equivalencia de los elementos de A son

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

DISQUISITIONES ARITHMETICAE.

SECTIO PRIMA

DE

NUMERORUM CONGRUENTIA IN GENERE.

Numeri congrui, moduli, residua et nonresidua.

1.

Si numerus a numerorum b, c differentiam metitur. b et c secundum a congrui dicuntur, sin minus, incongrui: ipsum a modulum appellamus. Uterque numerorum b, c priori in casu alterius residuum, in posteriori vero nonresiduum vocatur.

Hae notiones de omnibus numeris integris tam positivis quam negativis*) valent, neque vero ad fractos sunt extendendae. E. g. -9 et $+16$ secundum modulum 5 sunt congrui; -7 ipsius $+15$ secundum modulum 11 residuum, secundum modulum 3 vero nonresiduum. Ceterum quoniam cifram numerus quisque metitur, omnis numerus tamquam sibi ipsi congruus secundum modulum quemcunque est spectandus.

Figura 2.1. El primer párrafo de las *Disquisitiones Arithmeticae* de Carl Friedrich Gauss, con la definición de la relación de congruencia. «Si un número a divide la diferencia de números b y c , b y c se dicen congruentes y si no incongruentes. Llamamos a a el módulo y a cada uno de los números b y c residuos del otro en el primer caso y no residuos en el segundo. [...] Por ejemplo, -9 y 16 son congruentes módulo 5; -7 es residuo de 15 módulo 11 y no residuo módulo 3. Como 0 es divisible por todos los enteros, e sigue que podemos considerar a todo número congruente consigo mismo con respecto a un módulo cualquiera.»

$$[5] = \{5, 6\}, \quad [6] = \{5, 6\}, \quad [7] = \{7\}.$$

En este ejemplo, entonces, las clases de equivalencia de la relación R son tres, a saber:

$$\{1, 2, 3, 4\}, \quad \{5, 6\}, \quad \{7\}.$$

El conjunto cociente de A por R es, por lo tanto,

$$A/R = \{\{1, 2, 3, 4\}, \{5, 6\}, \{7\}\}.$$

2.4.4. La siguiente es la observación más importante que podemos hacer sobre las clases de equivalencia de una relación de equivalencia:

Proposición. Sea A un conjunto no vacío y sea $R \subseteq A \times A$ una relación de equivalencia en A . Si x e y son elementos de A tales que $x \in [y]$, entonces $[x] = [y]$.

Demostración. Sean x e y elementos de A tales que $x \in [y]$, es decir, tales que

$$y R x. \tag{8}$$

Queremos probar que $[x] = [y]$ y para ello probamos, como es usual, las inclusiones mutuas de los dos conjuntos $[x]$ e $[y]$. Supongamos entonces primero que $u \in [x]$, de manera que $x R u$. Como la relación R es transitiva, de esto y de la hipótesis (8) tenemos que $y R u$, esto es, que $u \in [y]$: esto muestra que $[x] \subseteq [y]$.

Recíprocamente, supongamos que $u \in [y]$, de manera que $y R u$ y, como R es simétrica, que $u R y$. De esto y de la hipótesis (8) tenemos que $u R x$ y, otra vez por la simetría, que $x R u$, es decir, que $u \in [x]$. Esto muestra que $[y] \subseteq [x]$ y completa la prueba de la proposición. \square

2.4.5. Vamos cuáles son las clases de equivalencia de las relaciones de equivalencia que listamos en **2.4.2**.

- (a) Sea A un conjunto no vacío y sea $R = I_A$ la relación identidad de A . Si $x \in A$, entonces la clase de equivalencia $[x]$ es el conjunto $\{x\}$. En efecto, si $y \in A$ es tal que $x R y$, entonces se sigue inmediatamente de la definición de la relación que necesariamente $y = x$: esto muestra que $[x] \subseteq \{x\}$. Por otro lado, como $x R x$ porque R es reflexiva, tenemos que $x \in [x]$ y, en consecuencia, que $\{x\} \subseteq [x]$. Vemos así que $[x] = \{x\}$, como dijimos. En este ejemplo, entonces, hay tantas clases de equivalencia como elementos hay en A y el conjunto cociente es

$$A/R = \{\{x\} : x \in A\}.$$

- (b) Sea A un conjunto no vacío y consideremos ahora la relación total $R = A \times A$ en A . En este caso, cualquiera sea el elemento x en A la clase de equivalencia

de x es $[x] = A$ y, por lo tanto, hay exactamente una clase de equivalencia, todos los elementos de A tienen la misma clase de equivalencia y el conjunto cociente es

$$A/R = \{A\}.$$

(c) Sea $A = \mathbb{Z}$ y sea $R \subseteq \mathbb{Z} \times \mathbb{Z}$ la relación de equivalencia tal que si x e y están en \mathbb{Z} entonces

$$x R y \iff |x| = |y|.$$

Sea $x \in \mathbb{Z}$. Un entero $y \in \mathbb{Z}$ pertenece a $[x]$ si $x R y$, es decir, si $|x| = |y|$, y esto ocurre exactamente cuando o $y = x$ o $y = -x$. Vemos así que la clase de equivalencia de x es $[x] = \{x, -x\}$. Esta clase tiene dos elementos, x y $-x$, cuando x es distinto de 0, y uno solo en caso contrario.

En este ejemplo dos elementos de \mathbb{Z} tienen la misma clase de equivalencia si y solamente si son o iguales o opuestos. La clase de equivalencia de 0 tiene un único elemento, ya que $[0] = \{0\}$, mientras que todas las otras clases de equivalencia tienen exactamente dos. El conjunto cociente es

$$A/R = \{[x] : x \in \mathbb{N}_0\}.$$

(d) Sea ahora $A = \mathbb{R}$ y $R \subseteq \mathbb{R} \times \mathbb{R}$ la relación de equivalencia en \mathbb{R} tal que si x e y son dos elementos de \mathbb{R} , entonces

$$x R y \iff x^2 - 2x + 2 = y^2 - 2x + 2.$$

Fijemos $x \in \mathbb{R}$ y encontremos la clase de equivalencia $[x]$ de x con respecto a R . Un número $y \in \mathbb{R}$ pertenece a $[x]$ si y solamente si $x R y$, es decir, si y solamente si

$$x^2 - 2x + 2 = y^2 - 2x + 2.$$

Observemos que podemos reescribir esta igualdad en la forma

$$(x - 1)^2 + 1 = (y - 1)^2 + 1,$$

y entonces es claro que esa igualdad se cumple si y solamente si $y - 1$ es igual a $x - 1$ o a $-(x - 1)$, es decir, si y es igual a x o a $2 - x$. Vemos así que

$$[x] = \{x, 2 - x\}.$$

Si $x \neq 1$, entonces $x \neq 2 - x$ y la clase de equivalencia $[x]$ tiene exactamente dos elementos; si en cambio es $x = 1$, entonces $x = 1 = 2 - x$ y $[x]$ tiene un único elemento. Afirmamos que el conjunto cociente es, en este ejemplo,

$$A/R = \{[x] : x \in \mathbb{R}, x \geq 1\}. \quad (9)$$

En efecto, sea $y \in \mathbb{R}$. Si $y \geq 1$, entonces claramente la clase $[y]$ es uno de los elementos del conjunto que aparece a la derecha en (9). Si en cambio $y < 1$, entonces $2 - y > 1$ y $[y] = \{y, 2 - y\} = [2 - y]$, así que $[y]$ también es uno de los elementos de ese conjunto.

(e) Sea $A = \mathbb{Z}$ y $R \subseteq \mathbb{Z} \times \mathbb{Z}$ la relación tal que si x e y son elementos de \mathbb{Z} entonces

$$x R y \iff y - x \text{ es par.}$$

Fijemos un entero $x \in \mathbb{Z}$. Si $y \in [x]$, entonces $y - x$ es par, es decir, existe $k \in \mathbb{Z}$ tal que $y - x = 2k$ y, por lo tanto, $y = x + 2k$. Vemos así que $[x] \subseteq \{x + 2k : k \in \mathbb{Z}\}$ y vale, de hecho, la igualdad. En efecto, si y es un entero de la forma $x + 2k$ para algún $k \in \mathbb{Z}$, entonces la diferencia $y - x = 2k$ es un número par y, en consecuencia, $x R y$, de manera que $y \in [x]$.

Concluimos de esta forma que para cada $x \in \mathbb{Z}$ la clase de equivalencia de x con respecto a R es

$$[x] = \{x + 2k : k \in \mathbb{Z}\}.$$

Afirmamos que el conjunto cociente en este caso es

$$A/R = \{[0], [1]\}$$

y que éste tiene dos elementos distintos. Para verlo, tenemos que mostrar, por un lado, que toda clase de equivalencia de la relación R es igual o a $[0]$ o a $[1]$ y, por otro, que $[0] \neq [1]$.

Sea $y \in \mathbb{Z}$ un entero. Si y es par, entonces por supuesto la diferencia $y - 0$ es par, de manera que $0 R y$ y, por lo tanto, $y \in [0]$: esto implica, como sabemos, que $[y] = [0]$. Si en cambio y es impar, entonces la diferencia $y - 1$ es par y ahora tenemos que $y \in [1]$ y que $[y] = [1]$. Esto prueba la primera de las dos cosas que queremos. Para ver la segunda basta observar que como la diferencia $1 - 0$ no es par, entonces $0 \not R 1$ y, por lo tanto $1 \notin [0]$: como $1 \in [1]$, es claro que esto muestra que las clases $[0]$ y $[1]$ son distintas.

2.4.6. Proposición. *Sea A un conjunto no vacío y sea $R \subseteq A \times A$ una relación de equivalencia en A .*

- (i) Toda clase de equivalencia de R es no vacía.
- (ii) Todo elemento de A pertenece a alguna una clase de equivalencia de R .
- (iii) Dos clases de equivalencia de R son o bien disjuntas o bien iguales.

Observemos que de (ii) y (iii) se deduce que, de hecho, todo elemento de A pertenece a *exactamente* una clase de equivalencia de R .

Demostración. (i) Si c es una clase de equivalencia de R , entonces existe $x \in A$ tal que $c = [x]$ y, por lo tanto, $x \in c$: en efecto, la relación R es reflexiva, así que $x R x$ y, en consecuencia, $x \in [x]$.

(ii) Si x es un elemento de A , entonces $[x]$ es una clase de equivalencia de R que contiene a x .

(iii) Sean c y d dos clases de equivalencia de la relación R , de manera que existen elementos x e y de A tales que $c = [x]$ y $d = [y]$, y supongamos que c y d no son conjuntos disjuntos. Existe entonces $z \in c \cap d = [x] \cap [y]$ y, en particular, $z \in [x]$ y $z \in [y]$. De acuerdo a la Proposición 2.4.4, esto implica que $[z] = [x]$ y que $[z] = [y]$, así que, por supuesto, tenemos que $[x] = [y]$. \square

Particiones

2.4.7. Si A es un conjunto, una *partición* de A es un conjunto \mathcal{F} contenido en $\mathcal{P}(A)$ —de manera que los elementos de \mathcal{F} son subconjuntos de A — que satisface las siguientes tres condiciones:

- $\emptyset \notin \mathcal{F}$;
- todo elemento de A pertenece a algún elemento de \mathcal{F} ;
- dos elementos de \mathcal{F} son o bien iguales o disjuntos.

Llamamos a los elementos de \mathcal{F} las *partes* de la partición.

Por ejemplo, el conjunto $A = \{1, 2, 3, 4, 5, 6\}$ tiene a

$$\mathcal{F}_1 = \{\{1, 2, 5\}, \{4, 6\}, \{3\}\},$$

$$\mathcal{F}_2 = \{\{1\}, \{2\}, \{3\}, \{4\}, \{5\}, \{6\}\}$$

y a

$$\mathcal{F}_3 = \{\{1, 2, 3, 4, 5, 6\}\}$$

como particiones, entre otras.

2.4.8. Podemos obtener una partición de un conjunto a partir de una relación de equivalencia:

Proposición. Sea A un conjunto no vacío y sea $R \subseteq A \times A$ una relación de equivalencia en A . El conjunto cociente A/R es una partición de A .

Demostración. En efecto, que las tres condiciones de la definición 2.4.7 se cumplen es precisamente lo que afirma la Proposición 2.4.6. \square

2.4.9. Recíprocamente, si tenemos una partición en un conjunto, podemos construir de manera natural una relación de equivalencia:

Proposición. Sea A un conjunto no vacío y sea \mathcal{F} una partición de A . La relación $R \subseteq A \times A$ tal que si x e y son elementos de A entonces

$$x R y \iff \text{existe una parte } P \in \mathcal{F} \text{ tal que } x \in P \text{ e } y \in P$$

es una relación de equivalencia en A y su conjunto cociente es $A/R = \mathcal{F}$.

Demostración. Mostremos primero que la relación R definida en el enunciado de esta proposición es una relación de equivalencia.

- Si $x \in A$, entonces como \mathcal{F} es una partición, existe una parte $P \in \mathcal{F}$ tal que $x \in P$ y, por lo tanto, $x R x$.
- Sean x e y dos elementos de A tales que $x R y$, de manera que existe una parte $P \in \mathcal{F}$ tal que $x \in P$ e $y \in P$. Por supuesto, tenemos entonces que $y \in P$ y $x \in P$, así que $y R x$.
- Finalmente, sean x, y y z elementos de A tales que $x R y$ e $y R z$. Existen entonces partes P y Q en la partición \mathcal{F} tales que $x \in P, y \in P, y \in Q$ y $z \in Q$. En particular, vemos de esto que $y \in P \cap Q$, de manera que las partes P y Q no son disjuntas: como \mathcal{F} es una partición y satisface por lo tanto la tercera de las condiciones de la definición 2.4.7, vemos que tiene que ser $P = Q$. Pero en ese caso tenemos que $x \in P$ y $z \in P$, por lo tanto, que $x R z$.

Como consecuencia de todo esto, la relación R es reflexiva, simétrica y transitiva y, por lo tanto, se trata de una relación de equivalencia.

Veamos ahora que $A/R = \mathcal{F}$. Para ello, tenemos que mostrar las dos inclusiones entre los conjuntos A/R y \mathcal{F} .

- Sea primero c un elemento de A/R , es decir, una clase de equivalencia de la relación R , de manera que existe $x \in A$ tal que $c = [x]$. Como \mathcal{F} es una partición del conjunto A , sabemos que existe una parte $P \in \mathcal{F}$ tal que $x \in P$. Afirmamos que c y P son el mismo conjunto y, en particular, que $c \in \mathcal{F}$. Cuando probemos esto tendremos, por lo tanto, que $A/R \subseteq \mathcal{F}$.

Sea $y \in c = [x]$: esto significa que $x R y$ y, de acuerdo a la definición de la relación R , que existe una parte $Q \in \mathcal{F}$ tal que $x \in Q$ e $y \in Q$. Ahora bien, como $x \in P \cap Q$, las partes P y Q no son disjuntas, así que tienen que ser iguales, esto es, debe ser $P = Q$. En particular, como $y \in Q$ tenemos que $y \in P$, y en definitiva esto muestra que $c \subseteq P$.

Por otro lado, sea $y \in P$. Como $x \in P$ e $y \in P$, la definición de R nos dice que $x R y$, así que $y \in [x]$: esto implica que $P \subseteq c$.

- Sea ahora P una parte de \mathcal{F} . Como \mathcal{F} es una partición, P no es el conjunto vacío y, por lo tanto, existe $x \in A$ tal que $x \in P$. Para ver que P pertenece a A/R es suficiente con que mostremos que $P = [x]$.

Si y es un elemento de P , entonces tenemos que $x \in P$ e $y \in P$, así que $x R y$ y, por lo tanto, $y \in [x]$. Esto muestra que $P \subseteq [x]$. Recíprocamente, si $y \in [x]$, de manera que $x R y$, entonces existe una parte Q de \mathcal{F} tal que $x \in Q$ e $y \in Q$. Como la intersección $P \cap Q$ no es vacía, ya que contiene a x , debe ser $P = Q$ y, por lo tanto, tenemos que $y \in P$. Concluimos de esta forma que $[x] \subseteq P$.

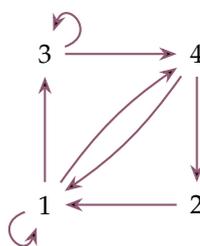
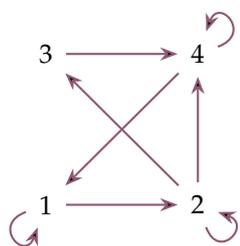
Esto completa la prueba de la proposición. □

§2.5. Relaciones de orden

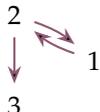
2.5.1. Si A es un conjunto no vacío y $R \subseteq A \times A$ es una relación en A , entonces decimos que R es *anti-simétrica* si cada vez que a y b son elementos de A se tiene que

$$a R b \text{ y } b R a \implies a = b.$$

En términos del grafo de la relación, esta condición nos dice que hay a lo sumo *una* flecha entre dos elementos *distintos* de A . De las siguientes dos relaciones en el conjunto $\{1, 2, 3, 4\}$ sólo la primera es anti-simétrica:



Es importante observar que la propiedad de anti-simetría de una relación es independiente de la de simetría y, en particular, que no es lo mismo que la de no ser simétrica. La siguiente tabla muestra relaciones que tienen las cuatro posibles combinaciones de estas dos propiedades.

		¿Es anti-simétrica?	
		Sí	No
¿Es simétrica?	Sí		
	No		

2.5.2. Una relación $R \subseteq A \times A$ en un conjunto no vacío A es una *relación de orden* si es reflexiva, anti-simétrica y transitiva.

2.5.3. Veamos algunos ejemplos de relaciones de orden.

- (a) La relación identidad I_A en un conjunto no vacío A .
- (b) Si $A = \mathbb{N}$, entonces la relación $R \subseteq A \times A$ tal que si $a, b \in A$ es

$$a R b \iff a \leq b$$

es una relación de orden. Podemos reemplazar al conjunto \mathbb{N} por \mathbb{Z} , por \mathbb{R} y, más generalmente, por cualquier subconjunto de \mathbb{R} . Este ejemplo es el que motiva el nombre de «relación de orden» de la propiedad que estamos estudiando.

- (c) Si B es un conjunto, podemos considerar la relación $R \subseteq \mathcal{P}(B) \times \mathcal{P}(B)$ en el conjunto de partes $\mathcal{P}(B)$ de B tal que si $X, Y \in \mathcal{P}(B)$ entonces

$$X R Y \iff X \subseteq Y.$$

Es inmediato verificar que se trata de una relación de orden en $\mathcal{P}(B)$. En efecto, ya sabemos que es reflexiva y transitiva, y la Proposición 1.2.2(ii) nos dice precisamente que es anti-simétrica.

- (d) En el conjunto \mathbb{N} consideremos la relación $R \subseteq \mathbb{N} \times \mathbb{N}$ tal que si x e y son elementos de \mathbb{N} entonces

$$x R y \iff x \text{ divide a } y.$$

Sabemos que se trata de una relación reflexiva y transitiva y es, de hecho, una relación de orden. Para verlo, bastará que mostremos que es anti-simétrica.

Supongamos que x e y son elementos de \mathbb{N} tales que $x R y$ e $y R x$, es decir, tales que $x \mid y$ e $y \mid x$. Existen entonces k y l en \mathbb{N} tales que $y = lx$ y $x = ky$, y se tiene entonces que

$$x = ky = klx,$$

de manera que $(1 - kl)x = 0$. Como x no es nulo, esta igualdad implica que $1 - kl$ sí lo es, es decir, que $kl = 1$. Como tanto k como l están en \mathbb{N} , vemos así que necesariamente $k = 1$ y, por lo tanto, que $x = ky = y$. Esto prueba que la relación es anti-simétrica, como queríamos.

Si definimos en \mathbb{Z} una relación $R \subseteq \mathbb{Z} \times \mathbb{Z}$ de manera que para cada x e $y \in \mathbb{Z}$ se tenga que vale

$$x R y \iff x \text{ divide a } y,$$

entonces *no* obtenemos una relación de orden: por ejemplo, $2 R (-2)$ y $(-2) R 2$, pero ciertamente 2 y -2 no son iguales.

(e) Sea $A = \mathbb{R} \times \mathbb{R}$ y consideremos la relación $R \subseteq A \times A$ tal que cada vez que (x_1, x_2) e (y_1, y_2) son dos elementos de A se tiene que

$$(x_1, x_2) R (y_1, y_2) \iff \begin{cases} x_1 > y_1 \\ \text{o} \\ x_1 = y_1 \text{ e } x_2 \geq y_2. \end{cases} \quad (10)$$

Veamos que se trata de una relación de orden en el conjunto A . Observemos antes que claramente se tiene que

$$(x_1, x_2) R (y_1, y_2) \implies x_1 \geq y_1 \quad (11)$$

siempre que (x_1, x_2) e (y_1, y_2) son elementos de A .

- Si (x_1, x_2) es un elemento de A , entonces es claro que $(x_1, x_2) R (x_1, x_2)$, así que la relación es reflexiva.
- Sean (x_1, x_2) e (y_1, y_2) dos elementos de A para los que se tiene que

$$(x_1, x_2) R (y_1, y_2) \quad (12)$$

y

$$(y_1, y_2) R (x_1, x_2). \quad (13)$$

De nuestra observación (11) y de esto deducimos que $x_1 \geq y_1$ y que $y_1 \geq x_1$, así que, de hecho, es $x_1 = y_1$.

Ahora bien, de (12) y de esto vemos que debe ser $x_2 \geq y_2$, ya que la primera de las alternativas de la definición (10) no puede valer. De la misma forma, de (13) y de que $x_1 = y_1$ deducimos que $y_2 \geq x_2$. Juntando las dos desigualdades, vemos que, de hecho, $x_2 = y_2$ y, por lo tanto, que $(x_1, x_2) = (y_1, y_2)$. Esto prueba que la relación R es anti-simétrica.

- Finalmente, supongamos que (x_1, x_2) , (y_1, y_2) y (z_1, z_2) son elementos de A tales que

$$(x_1, x_2) R (y_1, y_2) \tag{14}$$

y

$$(y_1, y_2) R (z_1, z_2). \tag{15}$$

En particular, de acuerdo a nuestra observación (11), tenemos que $x_1 \geq y_1$ y que $y_1 \geq z_1$. Si alguna de estas dos desigualdades es estricta, entonces tenemos que $x_1 > z_1$ y, por lo tanto, que $(x_1, x_2) R (z_1, z_2)$. Supongamos entonces que ninguna de esas dos desigualdades es estricta, de manera que $x_1 = y_1$ e $y_1 = z_1$. De la definición de la relación R y de (14) y de (15) podemos deducir entonces que $x_2 \geq y_2$ y que $y_2 \geq z_2$. Tenemos en consecuencia que $x_1 = z_1$ y que $x_2 \geq z_2$, así que otra vez $(x_1, x_2) R (z_1, z_2)$.

En cualquier caso, entonces, es $(x_1, x_2) R (z_1, z_2)$ y, por lo tanto, la relación R es transitiva.

Vemos de esta forma que la relación R es una relación de orden en el conjunto A , como queríamos.

§2.6. Ejercicios

Intersección de relaciones

2.6.1. Sea A un conjunto.

- (a) Si R y S son dos relaciones en A que son reflexivas, simétricas, transitivas o anti-simétricas, entonces la intersección $R \cap S$, que es una relación en A , tiene la misma propiedad. Si R y S son relaciones de equivalencia o de orden, entonces $R \cap S$ también lo es.
- (b) Mas generalmente, si \mathcal{F} es una familia no vacía de relaciones en A y todos los miembros de \mathcal{F} son relaciones reflexivas, simétricas, transitivas o anti-simétricas,

entonces la intersección

$$\bigcap_{R \in \mathcal{F}} R,$$

que también es una relación en A , tiene la misma propiedad. Si todos los miembros de la familia \mathcal{F} son relaciones de equivalencia o de orden, entonces la intersección de la familia también lo es.

- (c) ¿Hay resultados como los de las dos partes anteriores de este ejercicio pero con respecto a la unión de relaciones?

Clausura transitiva

2.6.2. Sea A un conjunto y sea $R \subseteq A \times A$ una relación en A .

- (a) La familia \mathcal{F} de todas las relaciones $S \subseteq A \times A$ que son transitivas y tales que $R \subseteq S$ es no vacía. Podemos entonces considerar la relación

$$\bar{R} = \bigcap_{S \in \mathcal{F}} S.$$

Esta relación \bar{R} es una relación transitiva en A que contiene a R y es la menor relación en A con esa propiedad, en el sentido de que

si $S \subseteq A \times A$ es una relación transitiva en el conjunto A y $R \subseteq S$, entonces $\bar{R} \subseteq S$.

Llamamos a la relación \bar{R} la **clausura transitiva** de R .

- (b) Sea $R \subseteq \mathbb{N} \times \mathbb{N}$ la relación en \mathbb{N} tal que si x e y son elementos de \mathbb{N} entonces

$$x R y \iff y = x + 1.$$

Describe la clausura transitiva \bar{R} de R .

2.6.3. Sea A un conjunto y sea $R \subseteq A \times A$ una relación en A . Consideremos la relación $R' \subseteq A \times A$ tal que si x e y son elementos de A , entonces se tiene que

$$x R' y$$

si y solamente si se cumple la siguiente condición:

existen $n \in \mathbb{N}$ y elementos $z_0, z_1, \dots, z_n \in A$ tales que $z_0 = x$, $z_n = y$ y para cada $i \in \{1, \dots, n\}$ es $z_{i-1} R z_i$.

Muestre que R' es una relación transitiva en A , que $R \subseteq R'$ y que, de hecho, R' es la clausura transitiva de R .

Relación de equivalencia generada por una relación

2.6.4. Sea A un conjunto y sea $R \subseteq A \times A$ una relación.

- (a) La familia \mathcal{F} de todas las relaciones $S \subseteq A \times A$ que contienen a R y que son relaciones de equivalencia no es vacía y podemos, por lo tanto, considerar la intersección

$$\bar{R} = \bigcap_{S \in \mathcal{F}} S.$$

Esta relación en A es una relación de equivalencia, contiene a R y es la menor relación de equivalencia en A que contiene a R , en el sentido de que

si $S \subseteq A \times A$ es una relación de equivalencia en el conjunto A y $R \subseteq S$, entonces $\bar{R} \subseteq S$.

Llamamos a esta relación \bar{R} la relación de equivalencia **generada** por R .

- (b) Sea $R' \subseteq A \times A$ la relación en A tal que si x e y son elementos de A , entonces se tiene que

$$x R' y$$

si y solamente si se cumple la condición de que

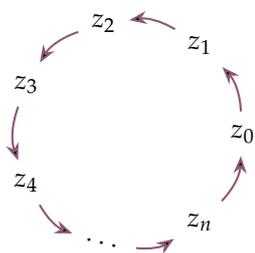
existen $n \in \mathbb{N}_0$ y elementos $z_0, z_1, \dots, z_n \in A$ tales que $z_0 = x, z_n = y$ y para cada $i \in \{1, \dots, n\}$ es $z_{i-1} R z_i$ o $z_i R z_{i-1}$.

Muestre que R' es una relación de equivalencia en A , que $R \subseteq R'$ y que R' es, de hecho, la relación de equivalencia en A generada por R .

Relación de orden generada por una relación acíclica

2.6.5. Si A es un conjunto y $R \subseteq A \times A$ es una relación en A decimos que R es **posee un ciclo** si existen $n \in \mathbb{N}$ y elementos $z_0, \dots, z_n \in A$ tales que $z_{i-1} R z_i$ para cada

$i \in \{1, \dots, n\}$ y $z_n R z_0$.



Si R no posee un ciclo, entonces decimos que R es *acíclica*.

2.6.6. Sea A un conjunto y sea $R \subseteq A \times A$ una relación en A .

- (a) Si la relación R posee un ciclo, entonces no existe ninguna relación de orden $S \subseteq A \times A$ tal que $R \subseteq S$.
- (b) Supongamos ahora que R es acíclica. Si R^+ es la clausura transitiva de la relación $R \cup I_A$, entonces R^+ es una relación de orden en A y $R \subseteq R^+$.
- (c) En particular, esto muestra que si R es acíclica, entonces la familia \mathcal{F} de todas las relaciones de orden S en A tales que $R \subseteq S$ no es vacía y que, por lo tanto, podemos considerar la intersección

$$\bigcap_{S \in \mathcal{F}} S,$$

que es una relación en A . Esta relación es precisamente la relación R^+ construida en la parte (b) y es la menor relación de orden en A que contiene a R , en el sentido de que

si $S \subseteq A \times A$ es una relación de orden en el conjunto A y $R \subseteq S$, entonces $R^+ \subseteq S$.

Llamamos a esta relación R^+ la relación de orden *generada* por R .

La relación de cubrimiento de una relación de orden

2.6.7. Sea A un conjunto y sea $R \subseteq A \times A$ una relación de orden en A . Definimos una nueva relación $R^\circ \subseteq A \times A$ en A de la siguiente manera: si x e y son elementos de A , entonces $x R^\circ y$ si y solamente se se cumplen las siguientes dos condiciones

- es $x R y$, y
- cada vez que $z \in R$ es tal que $x R z$ y $z R y$ se tiene que $z = x$ o $z = y$.

En otras palabras, si x e y son elementos de A , entonces se tiene que $x R^\circ y$ si y solamente si $x R y$ y no hay elementos z de R distintos de x y de y que sean «intermedios» entre x e y , en el sentido que se tengan las relaciones

$$x R z, \quad z R y.$$

Llamamos a la relación R° la *relación de cubrimiento* correspondiente a la relación R de partida.

2.6.8. Describa en cada uno de los siguientes ejemplos la relación de cubrimiento correspondiente.

(a) Sea $R \subseteq \mathbb{Z} \times \mathbb{Z}$ la relación de orden en \mathbb{Z} tal que si x e y son elementos de \mathbb{Z} entonces

$$x R y \iff x \leq y.$$

(b) Sea B un conjunto y sea $R \subseteq \mathcal{P}(B) \times \mathcal{P}(B)$ la relación de orden en el conjunto de partes $\mathcal{P}(B)$ tal que si X e Y son elementos de $\mathcal{P}(B)$ entonces

$$X R Y \iff X \subseteq Y.$$

(c) Sea $R \subseteq \mathbb{Q} \times \mathbb{Q}$ la relación de orden en \mathbb{Q} tal que si x e y son elementos de \mathbb{Q} entonces

$$x R y \iff x \leq y.$$

Capítulo 3

Funciones

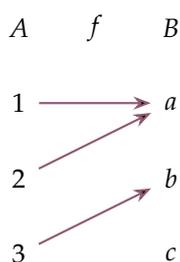
§3.1. Funciones

3.1.1. Sean A y B dos conjuntos. Decimos que una relación $f \subseteq A \times B$ de A a B es una *función* de A a B si

- para cada $a \in A$ existe $b \in B$ tal que $(a, b) \in f$, y
- si $a \in A$ y $b, b' \in B$ son tales que los pares ordenados (a, b) y (a, b') están en f , entonces necesariamente $b = b'$.

En términos del grafo de la relación f , la primera de estas condiciones dice que de cada elemento de A sale *al menos* una flecha, mientras que la segunda que sale *a lo sumo* una: juntas, entonces, nos dicen que de cada elemento del dominio de la relación f sale *exactamente* una flecha. Observemos que ambas condiciones son sobre lo que sucede con los elementos del *dominio* de f : bien puede suceder que haya elementos del *codominio*, el conjunto B , a los que no llegue ninguna flecha en el grafo de f o elementos a los que llegue más de una. Así, por ejemplo, si $A = \{1, 2, 3\}$ y $B = \{a, b, c\}$, entonces la

relación $f \subseteq A \times B$ cuyo grafo es



es una función. En efecto, en este grafo de cada elemento de A sale exactamente una flecha.

3.1.2. Cuando una relación $f \subseteq A \times B$ de un conjunto A a otro B es una función, escribimos $f : A \rightarrow B$. Esta notación nos dice cuál son el dominio y el codominio de la relación f y deja en claro que se trata de una función.

Por otro lado, si $f : A \rightarrow B$ es una función de A a B y a un elemento de A , sabemos que existe un elemento b en B y uno solo tal que $(a, b) \in f$: a ese elemento lo escribimos $f(a)$ y lo llamamos el *valor* de f en a o la *imagen* de a por f . En otras palabras, cuando escribimos que

$$b = f(a)$$

estamos diciendo, ni más ni menos, que el par ordenado (a, b) pertenece a f .

3.1.3. Proposición. Sean A, B y C tres conjuntos.

- (i) La relación identidad $I_A \subseteq A \times A$ es una función.
- (ii) Si $f : A \rightarrow B$ y $g : B \rightarrow C$ son funciones, entonces la relación $g \circ f \subseteq A \times C$ es una función de A a C .

Demostración. (i) Veamos que I_A es una función, verificando las dos condiciones de la definición **3.1.1**.

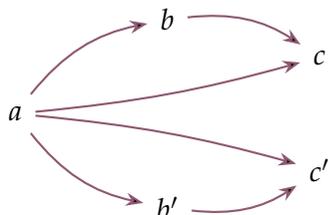
- Si a es un elemento de A , entonces el par ordenado (a, a) pertenece a I_A .
- Supongamos que $a \in A$ y $b, b' \in A$ son tales que los pares ordenados (a, b) y (a, b') están en I_A . De la definición de I_A se sigue, claro, que $a = b$ y que $a = b'$ y, en particular, que $b = b'$.

(ii) Otra vez, para mostrar que la relación compuesta $g \circ f$ de A a C es una función verificamos las dos condiciones de la definición **3.1.1**.

- Sea $a \in A$. Como f es una función, existe un elemento $b \in B$ tal que $(a, b) \in f$ y, por otro lado, como g es una función, existe un elemento $c \in C$ tal que $(b, c) \in g$.

De acuerdo a la definición de la composición de relaciones, entonces, se tiene que $(a, c) \in g \circ f$.

- Sean $a \in A$ y $c, c' \in C$ tales que los pares ordenados (a, c) y (a, c') están en $g \circ f$. Esto significa que existen elementos b y b' en B tales que (a, b) y (a, b') están en f y (b, c) y (b', c') están en g .



Ahora bien, como f es una función, de que los pares (a, b) y (a, b') estén en f se deduce que $b = b'$. Tenemos entonces que los pares (b, c) y (b, c') están en g y, como g también es una función, vemos que $c = c'$.

Esto completa la prueba de la proposición. □

§3.2. Inyectividad, sobreyectividad, biyectividad

3.2.1. Sean A y B dos conjuntos y sea $f : A \rightarrow B$ una función de A a B . Decimos que

- f es **inyectiva** si cada vez que a y a' son dos elementos de A tales que $f(a) = f(a')$ se tiene que $a = a'$, que
- f es **sobreyectiva** si para cada $b \in B$ existe $a \in A$ tal que $f(a) = b$, y que
- f es **biyectiva** si es a la vez inyectiva y sobreyectiva.

En términos del grafo de la función f , la condición de inyectividad es que a cada elemento de B llegue *lo sumo* una flecha desde un elemento de A , mientras que la de sobreyectividad que a cada elemento de B llegue *al menos* una flecha.

3.2.2. Estas tres propiedades de las funciones se preservan al componerlas:

Proposición. Sean A, B y C conjuntos y sean $f : A \rightarrow B$ y $g : B \rightarrow C$ funciones.

- (i) Si las funciones f y g son inyectivas, entonces la composición $g \circ f$ es inyectiva.
- (ii) Si las funciones f y g son sobreyectivas, entonces la composición $g \circ f$ es sobreyectiva.
- (iii) Si las funciones f y g son biyectivas, entonces la composición $g \circ f$ es biyectiva.

Demostración. (i) Supongamos que f y g son inyectivas y sean a y a' elementos de A tales que $(g \circ f)(a) = (g \circ f)(a')$, es decir, tales que $g(f(a)) = g(f(a'))$. Como g es inyectiva, esto implica que $f(a) = f(a')$ y, a su vez, como f es inyectiva, esto implica que $a = a'$: vemos así que la composición $g \circ f$ es inyectiva.

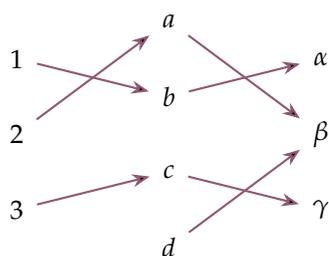
(ii) Supongamos ahora que f y g son inyectivas y sea $c \in C$. Como g es sobreyectiva, existe $b \in B$ tal que $g(b) = c$ y, por otro lado, como f es sobreyectiva, existe $a \in A$ tal que $f(a) = b$. Tenemos entonces que

$$(g \circ f)(a) = g(f(a)) = g(b) = c,$$

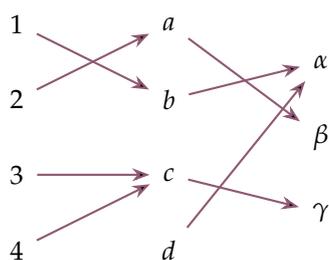
y esto nos dice que $g \circ f$ es sobreyectiva.

(iii) Supongamos finalmente que f y g son biyectivas. Como f y g son entonces inyectivas, la primera parte de esta proposición nos dice que la composición $g \circ f$ es inyectiva; por otro lado, como f y g son sobreyectivas, la segunda parte nos dice que esa composición es sobreyectiva. Vemos así que $g \circ f$ es biyectiva, como queremos. \square

3.2.3. Las implicaciones recíprocas a las de la Proposición 3.2.2 son falsas. Así, por ejemplo, la composición indicada en el gráfico



es inyectiva, pero la segunda función no lo es. De manera similar, la composición



es ciertamente sobreyectiva pero la primera de las dos funciones que estamos componiendo no lo es. Sin embargo, tenemos el siguiente resultado parcial:

3.2.4. Proposición. Sean A, B y C conjuntos y sean $f : A \rightarrow B$ y $g : B \rightarrow C$ funciones.

(i) Si la composición $g \circ f$ es inyectiva, entonces la función f es inyectiva.

(ii) Si la composición $g \circ f$ es sobreyectiva, entonces la función g es sobreyectiva.

Demostración. (i) Probaremos la implicación contrarrecíproca, esto es, que

si f no es inyectiva, entonces la composición $g \circ f$ tampoco lo es.

Supongamos entonces que f no es inyectiva, de manera que hay elementos a y a' en A tales que $a \neq a'$ y $f(a) = f(a')$. Se tiene entonces que

$$(g \circ f)(a) = g(f(a)) = g(f(a')) = (g \circ f)(a'),$$

y, como $a \neq a'$, que la composición $g \circ f$ no es inyectiva.

(ii) Supongamos que la composición $g \circ f$ es una función sobreyectiva y sea $c \in C$. La hipótesis nos dice que existe $a \in A$ tal que $c = (g \circ f)(a)$, es decir, que $c = g(f(a))$. El elemento $b = f(a)$ de B es entonces tal que $g(b) = c$: esto muestra que la función g es sobreyectiva. \square

§3.3. Funciones inversibles y funciones inversas

3.3.1. Sea $f : A \rightarrow B$ una función de un conjunto A a otro B . Decimos que f es **inversible** si existe una función $g : B \rightarrow A$ tal que $g \circ f = I_A$ y que $f \circ g = I_B$ y en ese caso decimos que g es una **función inversa** de f .

3.3.2. Una observación importante es la siguiente:

Lema. Si una función es inversible, entonces posee exactamente una función inversa.

En vista de esto, cuando tengamos una función inversible podremos hablar de *la* función inversa y no solamente de *una* función inversa, ya que ésta está bien determinada.

Demostración. Sea $f : A \rightarrow B$ una función. Supongamos que f es inversible y que las funciones $g_1, g_2 : B \rightarrow A$ son funciones inversas de f , de manera que se tiene que

$$g_1 \circ f = g_2 \circ f = I_A, \quad f \circ g_1 = f \circ g_2 = I_B.$$

Usando estas igualdades, vemos que

$$g_1 = g_1 \circ I_B = g_1 \circ (f \circ g_2) = (g_1 \circ f) \circ g_2 = I_A \circ g_2 = g_2.$$

Esto prueba el lema. □

3.3.3. Proposición. Sean A y B dos conjuntos. Una función $f : A \rightarrow B$ es inversible si y solamente si es biyectiva. Cuando ése es el caso, la relación inversa $f^{-1} \subseteq B \times A$ es una función y es, de hecho, la función inversa de f .

Demostración. Sea $f : A \rightarrow B$ una función y supongamos primero que f es inversible, de manera que existe una función $g : B \rightarrow A$ tal que $g \circ f = I_A$ y $f \circ g = I_B$. Como la composición $g \circ f$ es inyectiva, ya que es la función identidad de A , la Proposición 3.2.4(i) nos dice que f es inyectiva. De manera similar, como la composición $f \circ g$ es sobreyectiva, ya que es la función identidad de B , la Proposición 3.2.4(ii) nos dice que f es sobreyectiva. Vemos así que f es biyectiva.

Supongamos en segundo lugar que f es biyectiva y consideremos la relación inversa $f^{-1} \subseteq B \times A$. Se trata de una función: para verlo, verificamos las dos condiciones de la definición 3.1.1.

- Si $b \in B$, entonces, como f es sobreyectiva, existe $a \in A$ tal que $b = f(a)$, esto es, tal que el par ordenado (a, b) pertenece a f . Esto significa que el par ordenado (b, a) pertenece a la relación f^{-1} .
- Sean $b \in B$ y $a, a' \in A$ tales que los pares ordenados (b, a) y (b, a') están en f^{-1} . Esto significa que los pares ordenados (a, b) y (a', b) están en f , es decir, que $f(a) = b$ y que $f(a') = b$. Pero entonces $f(a) = f(a')$ y, como f es inyectiva, tenemos necesariamente que $a = a'$.

Vemos así que, como dijimos, tenemos una función $f^{-1} : B \rightarrow A$. Mostremos que f^{-1} es una función inversa de f y, por lo tanto, que la función f es inversible.

- Sea $a \in A$. Pongamos $b = f(a)$, de manera que $(a, b) \in f$ y, por lo tanto, $(b, a) \in f^{-1}$, es decir, $f^{-1}(b) = a$. Usando esto, vemos que

$$(f^{-1} \circ f)(a) = f^{-1}(f(a)) = f^{-1}(b) = a = I_A(a)$$

y concluimos que las funciones $f^{-1} \circ f$ e I_A toman el mismo valor en cada elemento de su dominio común A : esto significa, precisamente, que $f^{-1} \circ f = I_A$.

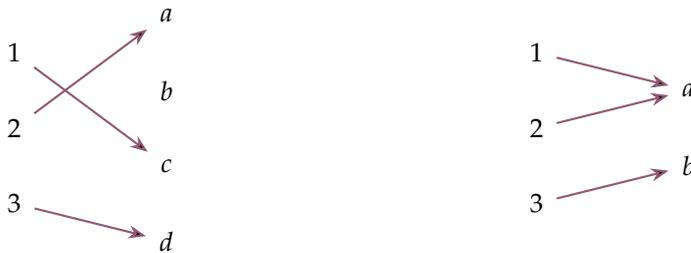
- Sea ahora $b \in B$ y pongamos $a = f^{-1}(b)$, de manera que $(b, a) \in f^{-1}$ y $(a, b) \in f$, es decir, $f(a) = b$. Tenemos que

$$(f \circ f^{-1})(b) = f(f^{-1}(b)) = f(a) = b = I_B(b)$$

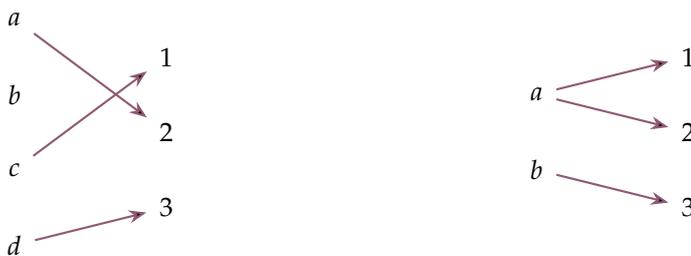
y, en consecuencia, que $f \circ f^{-1} = I_B$.

Esto completa la prueba de la proposición. \square

3.3.4. Es importante observar que si $f : A \rightarrow B$ es una función que no es biyectiva, entonces la relación inversa $f^{-1} : B \times A$ no es una función. Por ejemplo, las relaciones inversas de las funciones



son, respectivamente,



y ninguna de estas dos últimas es una función.

3.3.5. Proposición. Sean $f : A \rightarrow B$ y $g : B \rightarrow C$ dos funciones inversibles, de manera que poseen funciones inversas $f^{-1} : B \rightarrow A$ y $g^{-1} : C \rightarrow B$. La composición $g \circ f$ es inversible y su función inversa es

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}.$$

Demostración. Como f y g son inversibles, la Proposición 3.3.3 nos dice que son biyectivas y la Proposición 3.2.2(iii), a su vez, que la composición $g \circ f$ es biyectiva. La primera de esas proposiciones, por lo tanto, implica que esta composición es inversible. Esto prueba la primera de las dos afirmaciones del enunciado. Para ver la segunda, es suficiente que mostremos que $h = f^{-1} \circ g^{-1}$ es una función inversa de $k = g \circ f$ y para ello tenemos que probar que $h \circ k = I_A$ y que $k \circ h = I_C$.

Si $a \in A$, entonces

$$(h \circ k)(a) = h(k(a)) = f^{-1}(g^{-1}(g(f(a)))) = f^{-1}(f(a)) = a.$$

De manera similar, si $c \in C$, es

$$(k \circ h)(c) = k(h(c)) = g(f(f^{-1}(g^{-1}(c)))) = g(g^{-1}(c)) = c.$$

La proposición queda así probada. □

§3.4. Ejercicios

Imagen y preimagen de subconjuntos por una función

3.4.1. Sean A y B dos conjuntos y sea $f : A \rightarrow B$ una función de A a B . Si X es un subconjunto de A , llamamos *imagen* de X por f al subconjunto

$$f[X] = \{f(a) : a \in X\}$$

de B , de manera que si $b \in B$ se tiene que

$$b \in f[X] \iff \text{existe } a \in X \text{ tal que } f(a) = b.$$

De manera similar, si Y es un subconjunto de B , llamamos *preimagen* o *imagen inversa* de Y por f al subconjunto

$$f^{-1}[Y] = \{a \in A : f(a) \in Y\}$$

de A , y entonces para cada $a \in A$ se tiene que

$$a \in f^{-1}[Y] \iff f(a) \in Y.$$

3.4.2. Sea $f : A \rightarrow B$ una función.

- (a) Para cada subconjunto $X \subseteq A$ se tiene que $X \subseteq f^{-1}[f[X]]$ y, más aún, si la función f es inyectiva, entonces $X = f^{-1}[f[X]]$. Esta última igualdad no vale siempre.
- (b) Para cada subconjunto $Y \subseteq B$ se tiene que $f[f^{-1}[Y]] \subseteq Y$ y, más aún, si la función f es sobreyectiva, entonces $f[f^{-1}[Y]] = Y$. Esta igualdad no vale siempre.
- (c) Si X_1 y X_2 son subconjuntos de A tales que $X_1 \subseteq X_2$, entonces $f[X_1] \subseteq f[X_2]$.
- (d) Si Y_1 e Y_2 son subconjuntos de B tales que $Y_1 \subseteq Y_2$, entonces $f^{-1}[Y_1] \subseteq f^{-1}[Y_2]$.

3.4.3. Sean $f : A \rightarrow B$ y $g : B \rightarrow C$ dos funciones.

(a) Si X es un subconjunto de A , entonces $(g \circ f)[X] = g[f[X]]$.

(b) Si Y es un subconjunto de B , entonces $(g \circ f)^{-1}[Y] = f^{-1}[g^{-1}[Y]]$.

3.4.4. Sea $f : A \rightarrow B$ una función.

(a) Si X_1 y X_2 son subconjuntos de A , entonces

$$f[X_1 \cup X_2] = f[X_1] \cup f[X_2]$$

y

$$f[X_1 \cap X_2] \subseteq f[X_1] \cap f[X_2],$$

y, más aún, si la función f es inyectiva entonces de hecho se tiene que

$$f[X_1 \cap X_2] = f[X_1] \cap f[X_2].$$

Esta igualdad no vale siempre, sin embargo. Además, se tiene que

$$f[X_1 - X_2] \supseteq f[X_1] - f[X_2]$$

(b) Si Y_1 e Y_2 son subconjuntos de B , entonces

$$f^{-1}[Y_1 \cup Y_2] = f^{-1}[Y_1] \cup f^{-1}[Y_2],$$

$$f^{-1}[Y_1 \cap Y_2] = f^{-1}[Y_1] \cap f^{-1}[Y_2]$$

y

$$f^{-1}[Y_1 - Y_2] = f^{-1}[Y_1] - f^{-1}[Y_2].$$

3.4.5. Si $f : A \rightarrow B$ es una función y X e Y son subconjuntos de A y de B , respectivamente, entonces se tiene que

$$X \subseteq f^{-1}(Y) \iff f(X) \subseteq Y$$

y vale que

$$f[X] \cap Y = f[X \cap f^{-1}[Y]],$$

$$f[X] \cup Y \supseteq f[X \cup f^{-1}[Y]],$$

$$X \cap f^{-1}[Y] \subseteq f^{-1}[f[X] \cap Y],$$

$$X \cup f^{-1}[Y] \subseteq f^{-1}[f[X] \cup Y].$$

Ninguna de las últimas tres igualdades vale siempre: encuentre ejemplos en los que sean estrictas las inclusiones y condiciones sobre f que garanticen las igualdades.

Restricción y correstricción de funciones

3.4.6. Sea $f : A \rightarrow B$ una función y recordemos que, como f es una relación de A a B , se trata de un subconjunto del producto cartesiano $A \times B$.

- (a) Si C es un subconjunto de A , entonces el subconjunto $f \cap (C \times B)$ de $A \times B$ es una función de C a B . La llamamos la **restricción** de f a C y la escribimos $f|_C$.
- (b) Si D es un subconjunto de B tal que $D \supseteq f[A]$, entonces el subconjunto $f \cap (A \times D)$ de $A \times B$ es una función de A a D . La llamamos la **correstricción** de f a B y la escribimos $f|_D$.
- (c) Más generalmente, si C y D son subconjuntos de A y de B , respectivamente, y se tiene que $f[C] \subseteq D$, entonces la intersección $f \cap (C \times D)$ es una función de C a D .

“Pegado” de funciones

3.4.7. Sean A_1, A_2 y B tres conjuntos y sean $f : A_1 \rightarrow B$ y $g : A_2 \rightarrow B$ dos funciones. Si las restricciones $f|_{A_1 \cap A_2}$ y $g|_{A_1 \cap A_2}$ coinciden, entonces existe una y sólo una función $h : A_1 \cup A_2 \rightarrow B$ tal que $h|_{A_1} = f$ y $h|_{A_2} = g$. En esta situación, decimos que la función h se obtiene por “pegado” de las funciones f y g .

Caracterizaciones alternativas de la inyectividad y la sobreyectividad

3.4.8. Sea $f : A \rightarrow B$ una función.

- (a) La función f es inyectiva si y solamente si cada vez que $g_1 : C \rightarrow A$ y $g_2 : C \rightarrow A$ son funciones tales que $f \circ g_1 = f \circ g_2$ se tiene que $g_1 = g_2$.
- (b) La función f es sobreyectiva si y solamente si cada vez que $g_1 : B \rightarrow C$ y $g_2 : B \rightarrow C$ son funciones tales que $g_1 \circ f = g_2 \circ f$ se tiene que $g_1 = g_2$.

3.4.9. Si $f : A \rightarrow B$ es una función, entonces las siguientes tres condiciones son equivalentes:

- (a) La función f es inyectiva.
- (b) Cada vez que X e Y son subconjuntos de A se tiene que $f[X \cap Y] = f[X] \cap f[Y]$.
- (c) Cada vez que X e Y son subconjuntos de A tales que $X \subseteq Y$ se tiene que $f[Y - X] = f[Y] - f[X]$.

Funciones inversas a izquierda y a derecha

3.4.10. Sea $f : A \rightarrow B$ una función. Decimos que una función $f : B \rightarrow A$ es

- una *inversa a izquierda* de f si $g \circ f = I_A$, y
- una *inversa a derecha* de f si $f \circ g = I_B$.

3.4.11. Sea $f : A \rightarrow B$ una función.

- La función f posee una función inversa a izquierda si y solamente si f es inyectiva, pero en general no tiene una sola.
- La función f posee una inversa a derecha si y solamente si f es sobreyectiva, pero en general no tiene una sola.
- Si f posee una inversa a izquierda $g : B \rightarrow A$ y una inversa a derecha $h : B \rightarrow A$, entonces f es inversible y se tiene que $g = h = f^{-1}$.

Relaciones de equivalencia inducidas por funciones

3.4.12. Sea $f : A \rightarrow B$ una función. La relación $R_f \subseteq A \times A$ en el conjunto A tal que si x e y son elementos de A entonces

$$x R_f y \iff f(x) = f(y)$$

es una relación de equivalencia. Llamamos a R_f la relación de equivalencia *inducida* por la función f .

3.4.13. Sea A un conjunto y sea $R \subseteq A \times A$ una relación de equivalencia en A . Hay una función $f : A \rightarrow A/R$ con codominio en el conjunto cociente de A por R tal que

$$f(a) = [a]$$

para cada $a \in A$, esta función es sobreyectiva, y la relación de equivalencia $R_f \subseteq A \times A$ inducida por f es precisamente la relación R con la que empezamos. Llamamos a la función f la *proyección canónica* de A al cociente A/R .

Observemos que este resultado nos dice que *toda* relación de equivalencia es la relación de equivalencia inducida por alguna función.

Funciones definidas sobre un conjunto cociente

3.4.14. Sean A y B dos conjuntos, sea $R \subseteq A \times A$ una relación de equivalencia en A y sea $f : A \rightarrow B$ una función. Si cada vez que a y a' son elementos de A se tiene que

$$a R a' \implies f(a) = f(a'),$$

entonces existe una y una sola función $F : A/R \rightarrow B$ con dominio en el conjunto cociente A/R de A por R tal que para cada $a \in A$ es

$$F([a]) = f(a).$$

Capítulo 4

Inducción

§4.1. El principio de inducción

4.1.1. Decimos que un subconjunto S de \mathbb{N} es *inductivo* si tiene las siguientes dos propiedades:

- $1 \in S$, y
- para cada $k \in \mathbb{N}$ vale que

$$k \in S \implies k + 1 \in S.$$

Es evidente que el conjunto \mathbb{N} es inductivo y una propiedad fundamental del conjunto \mathbb{N} de los números naturales es que, de hecho, éste es el único ejemplo:

Proposición. Si S es un subconjunto inductivo de \mathbb{N} , entonces $S = \mathbb{N}$.

Llamamos a este resultado el *Principio de Inducción*. Veamos por qué es cierto. Sea S un subconjunto inductivo de \mathbb{N} y supongamos que S no es igual a \mathbb{N} , de manera que la diferencia $T = \mathbb{N} - S$ es un conjunto no vacío. Ahora bien, como T es un subconjunto no vacío de \mathbb{N} , posee un menor elemento m : es decir, existe un elemento $m \in T$ tal que para todo $n \in T$ se tiene que $m \leq n$. Como 1 pertenece a S , es $m \neq 1$ y, en consecuencia, el número $m - 1$ pertenece a \mathbb{N} . Más aún, como $m - 1$ es estrictamente menor que m , la forma en que elegimos a m implica que $m - 1 \notin T$, es decir, que $m - 1 \in S$. Usando esto y el hecho de que S es inductivo, entonces, podemos deducir que $m \in S$: esto es absurdo, ya que m pertenece a T . Esta contradicción provino de suponer que S es

un subconjunto propio de \mathbb{N} y todo esto prueba, en consecuencia, que $S = \mathbb{N}$, como queremos.

Este argumento es convincente pero adolece de un problema: depende de que sepamos que la afirmación

todo subconjunto no vacío de \mathbb{N} posee un menor elemento

es cierta y —más allá de que es intuitivamente plausible— no sabemos que esto es así. El problema es que para poder establecer formalmente el Principio de Inducción necesitamos hacer antes un tratamiento formal de qué es el conjunto \mathbb{N} y de sus propiedades básicas. En estas notas no haremos esto. Usaremos, de todas formas, con total libertad ese principio.

4.1.2. La razón por la que estamos interesados en el Principio de Inducción es que nos da un mecanismo muy efectivo para probar que un subconjunto de \mathbb{N} coincide con \mathbb{N} . Vamos un ejemplo sencillo de por qué esto es útil.

Supongamos que queremos probar la siguiente afirmación:

$$\text{para todo } n \in \mathbb{N} \text{ se tiene que } 2^n + 3^n \leq 5^n. \quad (1)$$

Esto puede hacerse de muchas formas. Una de ellas consiste en considerar el subconjunto

$$S = \{n \in \mathbb{N} : 2^n + 3^n \leq 5^n\}$$

de \mathbb{N} y probar que coincide con \mathbb{N} : claramente, esto es lo mismo que probar que la afirmación (1) vale. Para ver que S es igual a \mathbb{N} es suficiente, de acuerdo al Principio de Inducción, con mostrar que se trata de un conjunto inductivo, es decir, que tiene las dos propiedades de la definición 4.1.1. Así, tenemos que probar que

$$1 \in S$$

y que para todo $k \in \mathbb{N}$ se tiene que

$$k \in S \implies k + 1 \in S. \quad (2)$$

La primera de estas dos cosas puede verificarse por un cálculo directo: en efecto, basta observar que

$$2^1 + 3^1 = 5 \leq 5^1.$$

Veamos la segunda. Para ello, supongamos que k es un elemento de \mathbb{N} tal que $k \in S$, es decir, tal que

$$2^k + 3^k \leq 5^k. \quad (3)$$

Tenemos que

$$2^{k+1} + 3^{k+1} = 2^k \cdot 2 + 3^k \cdot 3$$

y, como $2 \leq 5$ y $3 \leq 5$, esto es

$$\leq 2^k \cdot 5 + 3^k \cdot 5 = (2^k + 3^k) \cdot 5 \quad (4)$$

Ahora bien, estamos suponiendo que k pertenece a S , así que vale la desigualdad (3), y entonces tenemos que el último miembro de la igualdad (4) es

$$\leq 5^k \cdot 5 = 5^{k+1}.$$

Esto nos dice, precisamente, que $k + 1$ pertenece a S . Hemos probado así que vale la segunda condición (2)

4.1.3. Demos otro ejemplo de este procedimiento: probemos que

$$\text{para todo } n \in \mathbb{N} \text{ se tiene que } 1 + \dots + n = \frac{n(n+1)}{2}. \quad (5)$$

A la izquierda de la igualdad que aparece en esta afirmación tenemos la suma de los primeros n números naturales, del 1 hasta n . Como hicimos antes, consideramos el subconjunto

$$S = \left\{ n \in \mathbb{N} : 1 + \dots + n = \frac{n(n+1)}{2} \right\}$$

de \mathbb{N} , mostramos que es inductivo y, entonces, gracias al Principio de Inducción, podemos concluir que $S = \mathbb{N}$, que es precisamente lo que se afirma en (5).

La verificación de la primera condición de la definición 4.1.1 es, como en el ejemplo, anterior, un simple cálculo directo: cuando $n = 1$, la suma de los primeros n números naturales es claramente igual a 1 y, por otro lado, es

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

Esto muestra que $1 \in S$.

Probemos ahora que la segunda condición de 4.1.1 también se cumple. Supongamos que k es un elemento de \mathbb{N} tal que $k \in S$, es decir, tal que

$$1 + \dots + k = \frac{k(k+1)}{2}. \quad (6)$$

La suma de los primeros $k + 1$ números naturales es

$$1 + \dots + (k+1) = \underbrace{1 + \dots + k} + (k+1)$$

Ahora bien, los primeros k sumandos de esta suma son precisamente los primeros k números naturales, y estamos suponiendo que vale (6): usando esto vemos que

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

y, observando que $k+1$ es un factor común en los dos términos del miembro derecho de esta igualdad, podemos reescribirlo:

$$= (k+1) \left(\frac{k}{2} + 1 \right) = (k+1) \frac{k+2}{2} = \frac{(k+1)(k+2)}{2}.$$

Observemos que hemos probado que, bajo la hipótesis de que vale (6), se tiene que

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

y esto significa, precisamente, que

$$k \in S \implies k+1 \in S.$$

Esto completa la prueba de que el conjunto S es inductivo y, como dijimos antes, de la afirmación (5)

4.1.4. En estos dos ejemplos el procedimiento que seguimos fue completamente similar. En efecto, en ambos casos tenemos un predicado $P(n)$ que depende de un número natural n y queremos probar que

$$\text{para todo } n \in \mathbb{N} \text{ vale } P(n). \tag{7}$$

En el primer ejemplo $P(n)$ es el predicado « $2^n + 3^n \leq 5^n$ » mientras que en el segundo es « $1 + \cdots + n = n(n+1)/2$ ». Consideramos entonces el subconjunto $S = \{n \in \mathbb{N} : P(n)\}$ de \mathbb{N} y mostramos que se trata de un subconjunto inductivo, esto es, que $1 \in S$ y que para cada $k \in \mathbb{N}$ se tiene que $k \in S \implies k+1 \in S$. En vista de la definición del conjunto S , esto es lo mismo que mostrar que

- la afirmación $P(1)$ vale, y que
- para cada $k \in \mathbb{N}$ se tiene que si la afirmación $P(k)$ vale entonces también vale la afirmación $P(k+1)$.

Hecho esto, el Principio de Inducción nos permite concluir que $S = \mathbb{N}$, esto es, que vale (7), como queremos. En la próxima sección daremos varios ejemplos más de este procedimiento.

Una demostración hecha de esta forma es llamada una *prueba por inducción*. La parte en que probamos que vale la afirmación $P(1)$ es llamada el *paso inicial* o *caso base*

de la inducción, mientras que la prueba de la implicación $P(k) \implies P(k+1)$ para cada $k \in \mathbb{N}$ es llamada el *paso inductivo*. Habitualmente, la prueba del paso inductivo procede de la siguiente forma: elegimos un número natural $k \in \mathbb{N}$ y suponemos que la afirmación $P(k)$ se cumple —esta hipótesis es la *hipótesis inductiva*— y de alguna manera, usando esa hipótesis inductiva, probamos que en ese caso también vale la afirmación $P(k+1)$.

§4.2. Algunos ejemplos de pruebas por inducción

Sumas geométricas

4.2.1. Fijemos un número $a \in \mathbb{R}$ distinto de 1 y mostremos que

$$\text{para cada } n \in \mathbb{N} \text{ se tiene que } 1 + a + \dots + a^{n-1} = \frac{a^n - 1}{a - 1}. \quad (8)$$

El miembro izquierdo de esta igualdad es la suma de las primeras n potencias de a , desde la 0-ésima, $a^0 = 1$, hasta la $(n-1)$ -ésima, a^{n-1} ; llamamos a esa suma la *suma geométrica* de razón a . Para ello, para cada n consideramos la afirmación

$$P(n) : 1 + a + \dots + a^{n-1} = \frac{a^n - 1}{a - 1}$$

y procedemos por inducción.

- Vemos que vale $P(1)$ calculando directamente: si $n = 1$, entonces por un lado es $1 + a + \dots + a^{n-1} = 1$ y, por otro, $(a^n - 1)/(a - 1) = 1$. Esto establece el caso base de la inducción.
- Veamos ahora el paso inductivo. Sea $k \in \mathbb{N}$ y supongamos que vale $P(k)$, de manera que

$$1 + a + \dots + a^{k-1} = \frac{a^k - 1}{a - 1}.$$

Usando esto, vemos que

$$\begin{aligned} 1 + a + \dots + a^k &= (1 + a + \dots + a^{k-1}) + a^k = \frac{a^k - 1}{a - 1} + a^k \\ &= \frac{a^k - 1 + a^k(a - 1)}{a - 1} = \frac{a^{k+1} - 1}{a - 1} \end{aligned}$$

y esto significa, precisamente, que vale la afirmación $P(k+1)$.

La inducción queda así completa y prueba, como queríamos, la afirmación (8).

La suma alternada de los cuadrados de los primeros números naturales

4.2.2. Probemos que si $n \in \mathbb{N}$ entonces

$$\sum_{i=1}^n (-1)^i i^2 = \frac{(-1)^n n(n+1)}{2}. \quad (9)$$

Llamemos $P(n)$ a la afirmación de que esta igualdad vale y procedamos por inducción.

- Vale $P(1)$, ya que $\sum_{i=1}^1 (-1)^i i^2 = -1$ y $(-1)^1 1(1+1)/2 = -1$.
- Supongamos que $k \in \mathbb{N}$ y que vale la afirmación $P(k)$, de manera que

$$\sum_{i=1}^k (-1)^i i^2 = \frac{(-1)^k k(k+1)}{2}.$$

Separando el último término de la suma, tenemos que

$$\sum_{i=1}^{k+1} (-1)^i i^2 = \sum_{i=1}^k (-1)^i i^2 + (-1)^{k+1} (k+1)^2$$

y entonces, usando la hipótesis inductiva, vemos que esto es

$$\begin{aligned} &= \frac{(-1)^k k(k+1)}{2} + (-1)^{k+1} (k+1)^2 \\ &= (-1)^k \left(\frac{k}{2} - (k+1) \right) (k+1) \\ &= (-1)^k \frac{k - 2(k+1)}{2} (k+1) \\ &= (-1)^k \frac{-(k+2)}{2} (k+1) = \frac{(-1)^{k+1} (k+1)(k+2)}{2}. \end{aligned}$$

Esto nos dice que, bajo la hipótesis inductiva, vale la afirmación $P(k+1)$.

De esto podemos concluir, gracias al Principio de Inducción, que vale la igualdad (9) para todo $n \in \mathbb{N}$.

Una suma de fracciones

4.2.3. Queremos probar que

$$\text{para cada } n \in \mathbb{N} \text{ se tiene que } \sum_{i=1}^n \frac{1}{i(i+1)} = \frac{n}{n+1}.$$

De manera similar a lo que hicimos antes, para cada $n \in \mathbb{N}$ llamamos $P(n)$ a la afirmación de que

$$\sum_{i=1}^n \frac{1}{i(i+1)} = \frac{n}{n+1}$$

y probamos por inducción que $P(n)$ vale para todo $n \in \mathbb{N}$.

- Calculando, vemos que cuando $n = 1$ es

$$\sum_{i=1}^n \frac{1}{i(i+1)} = \frac{1}{2} = \frac{n}{n+1}'$$

así que la afirmación $P(1)$ vale.

- Sea ahora $k \in \mathbb{N}$ y supongamos que vale la afirmación $P(k)$, es decir, que

$$\sum_{i=1}^k \frac{1}{i(i+1)} = \frac{k}{k+1}. \quad (10)$$

Se tiene entonces que

$$\sum_{i=1}^{k+1} \frac{1}{i(i+1)} = \sum_{i=1}^k \frac{1}{i(i+1)} + \frac{1}{(k+1)(k+2)}$$

y, en vista de la hipótesis inductiva (10), esto es

$$\begin{aligned} &= \frac{k}{k+1} + \frac{1}{(k+1)(k+2)} \\ &= \frac{1}{k+1} \left(k + \frac{1}{k+2} \right) = \frac{k(k+2) + 1}{(k+1)(k+2)} = \frac{k+1}{k+2} \end{aligned}$$

Vemos así que

$$\sum_{i=1}^{k+1} \frac{1}{i(i+1)} = \frac{k+1}{k+2}$$

y, por lo tanto, que vale la afirmación $P(k+1)$.

Esto prueba lo que queremos.

El producto de los primeros números impares

4.2.4. Mostremos que para todo $n \in \mathbb{N}$ se tiene que

$$\prod_{i=1}^n (2i-1) = \frac{(2n)!}{n!2^n} \quad (11)$$

haciendo inducción con respecto a n . Llamemos $P(n)$ a la afirmación de que esa igualdad vale.

- Si $n = 1$, entonces

$$\prod_{i=1}^n (2i-1) = 1 = \frac{2}{2} = \frac{(2n)!}{n!2^n},$$

así que vale la afirmación $P(1)$.

- Supongamos ahora que $k \in \mathbb{N}$ y que vale la afirmación $P(k)$, es decir, que

$$\prod_{i=1}^k (2i - 1) = \frac{(2k)!}{k!2^k}.$$

Separando el último factor del producto, vemos que

$$\prod_{i=1}^{k+1} (2i - 1) = \prod_{i=1}^k (2i - 1) \cdot (2(k + 1) - 1)$$

y, usando ahora la hipótesis inductiva, que esto es

$$= \frac{(2k)!}{k!2^k} \cdot (2(k + 1) - 1) = \frac{(2k)!}{k!2^k} (2k + 1).$$

Si multiplicamos al último miembro de esta cadena de igualdades por $1 = \frac{2k+2}{2k+2}$, vemos finalmente que

$$\prod_{i=1}^{k+1} (2i - 1) = \frac{(2k)!}{k!2^k} (2k + 1) \frac{2k + 2}{2k + 2} = \frac{(2(k + 1))!}{(k + 1)!2^{k+1}},$$

es decir, que vale la afirmación $P(k + 1)$.

Esto completa la inducción y, por lo tanto, la prueba de (11).

Una sucesión de enteros divisibles por 5

4.2.5. Probemos que

$$\text{para todo } n \in \mathbb{N} \text{ el número } 8^n - 3^n \text{ es divisible por 5.} \quad (12)$$

Para ello, para cada $n \in \mathbb{N}$ llamamos $P(n)$ a la afirmación « $8^n - 3^n$ es divisible por 5» y procedemos por inducción.

- Como $8^1 - 3^1 = 8 - 3 = 5$, y esto es evidentemente divisible por 5, es claro que la afirmación $P(1)$ vale: esto establece el caso base.
- Sea, por otro lado, $k \in \mathbb{N}$ y supongamos que la afirmación $P(k)$ vale, de manera que 5 divide a $8^k - 3^k$, esto es, que existe un número $r \in \mathbb{Z}$ tal que $8^k - 3^k = 5r$. Entonces

$$\begin{aligned} 8^{k+1} - 3^{k+1} &= 8^k \cdot 8 - 8^k \cdot 3 + 8^k \cdot 3 - 3^k \cdot 3 \\ &= 8^k \cdot (8 - 3) + (8^k - 3^k) \cdot 3 \end{aligned}$$

y, de acuerdo a la hipótesis inductiva, esto es

$$\begin{aligned} &= 8^k \cdot 5 + 5r \cdot 3 \\ &= (8^k + 3r) \cdot 5. \end{aligned}$$

Vemos así $8^{k+1} - 3^{k+1}$ es divisible por 5, esto es, que vale la afirmación $P(k + 1)$.

Esto completa la inducción y, por lo tanto, la prueba de (12).

La cardinalidad del conjunto de partes de un conjunto finito

4.2.6. Mostremos que

si $n \in \mathbb{N}$ y A es un conjunto finito de n elementos, entonces el conjunto de partes $\mathcal{P}(A)$ tiene 2^n elementos. (13)

Para cada $n \in \mathbb{N}$ sea $P(n)$ la afirmación «si A es un conjunto finito de n elementos, entonces $\mathcal{P}(A)$ tiene 2^n elementos» y procedamos por inducción con respecto a n .

- Sea A un conjunto que tiene 1 elemento y sea a ese elemento, de manera que $A = \{a\}$. Es claro que $\mathcal{P}(A) = \{\emptyset, A\}$ y, como $A \neq \emptyset$, que $\mathcal{P}(A)$ tiene exactamente dos elementos. Como $2^1 = 2$, esto nos dice que la afirmación $P(1)$ vale.
- Sea ahora $k \in \mathbb{N}$ y supongamos que vale la afirmación $P(k)$. Sea A un conjunto finito con $k + 1$ elementos y sean a_1, \dots, a_{k+1} esos $k + 1$ elementos listados en algún orden y sin repeticiones. El conjunto $B = \{a_1, \dots, a_k\}$ tiene entonces k elementos, así que —como estamos suponiendo que vale la afirmación $P(k)$ —

el conjunto de partes $\mathcal{P}(B)$ de B tiene 2^k elementos. (14)

Ahora bien, un subconjunto de A puede contener a a_{k+1} o no, y esto significa que si llamamos

$$P = \{X \in \mathcal{P}(A) : a_{k+1} \notin X\}$$

y

$$Q = \{X \in \mathcal{P}(A) : a_{k+1} \in X\}$$

entonces tenemos que $\mathcal{P}(A) = P \cup Q$ y $P \cap Q = \emptyset$. Esto implica que el número de elementos de $\mathcal{P}(A)$ es la suma del número de elementos de P y el número de elementos de Q .

Observemos que P es, de hecho, el conjunto $\mathcal{P}(B)$: un subconjunto de A que no contiene a a_{k+1} es un subconjunto de B y, recíprocamente, todo subconjunto de B es un subconjunto de A que no contiene a a_{k+1} . De acuerdo a (14), sabemos entonces que P tiene exactamente 2^k elementos.

Por otro lado, hay tantos elementos en P como en Q . En efecto, hay una función $f : P \rightarrow Q$ tal que si $X \in P$ entonces $f(X) = X \cup \{a_{k+1}\}$ y esta función es biyectiva, así que su dominio y codominio tienen el mismo número de elementos. Vemos así que Q tiene 2^k elementos.

Juntando todo, concluimos que $\mathcal{P}(A)$ tiene $2^k + 2^k = 2^{k+1}$ elementos y, por lo tanto, que vale la afirmación $P(k + 1)$.

Queda así completa la prueba de (13)

Veamos en un ejemplo como funciona este argumento. Sea $A = \{1, 2, 3, 4\}$, de manera que $k = 3$, y pongamos $a_1 = 1$, $a_2 = 2$, $a_3 = 3$ y $a_4 = 4$. Dividimos a $\mathcal{P}(A)$ en dos partes: P y Q son los subconjuntos de $\mathcal{P}(A)$ de los subconjuntos X de A que no contienen y que contienen, respectivamente, a 4. Así, los elementos de P son

$$\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\},$$

y los de Q son

$$\{4\}, \{1, 4\}, \{2, 4\}, \{3, 4\}, \{1, 2, 4\}, \{1, 3, 4\}, \{2, 3, 4\}, \{1, 2, 3, 4\}.$$

Es claro que P es precisamente $\mathcal{P}(\{1, 2, 3\})$ y, gracias a la hipótesis inductiva, tiene entonces 2^3 elementos. Por otro lado, la función $X \in P \mapsto X \cup \{4\} \in Q$ es claramente biyectiva y, por lo tanto, Q tienen la misma cantidad de elementos que P , es decir, 2^3 .

Subconjuntos de dos elementos de un conjunto finito

4.2.7. Para cada $n \in \mathbb{N}$ vale que

$$\text{un conjunto de } n \text{ elementos posee } n(n-1)/2 \text{ subconjuntos de dos elementos.} \quad (15)$$

Para verlo, llamemos $P(n)$ a esta afirmación y procedamos por inducción.

- Si un conjunto A tiene 1 elemento, entonces por supuesto A no posee ningún subconjunto de dos elementos. Como $n(n-1)/2$ es 0 si $n = 1$, esto nos dice que el caso base funciona, es decir, que vale la afirmación $P(1)$.
- Supongamos ahora que $k \in \mathbb{N}$ y que vale la afirmación $P(k)$, y sea A un conjunto con $k+1$ elementos. Digamos que los elementos de A , listados en algún orden y sin repeticiones, son a_1, \dots, a_{k+1} . Hay dos tipos de subconjuntos de A de dos elementos:
 - En primer lugar, están los subconjuntos de A de dos elementos que *no* contienen a a_{k+1} . Estos son, por supuesto, los subconjuntos de $\{a_1, \dots, a_k\}$ de dos elementos. Como el conjunto $\{a_1, \dots, a_k\}$ tiene k elementos y nuestra hipótesis inductiva es que la afirmación $P(k)$ vale, hay $k(k-1)/2$ subconjuntos de este tipo.
 - En segundo lugar, están los subconjuntos de A de dos elementos que *sí* contienen a a_{k+1} . Éstos son de la forma $\{a_i, a_{k+1}\}$ con i algún elemento de $\{1, \dots, k\}$ y, por lo tanto, hay k de ellos.

Concluimos así que, en total, hay $k(k-1)/2 + k$ subconjuntos de A de dos elementos, y este número es igual a $(k+1)k/2$. Esto muestra que vale $P(k+1)$.

Gracias al Principio de Inducción, podemos concluir con todo esto que vale (15).

La dualidad de De Morgan

4.2.8. Fijemos un conjunto de referencia U y mostremos la siguiente generalización de la Proposición 1.3.14(i):

si $n \in \mathbb{N}$ y A_1, \dots, A_n son subconjuntos de U , entonces se tiene que

$$(A_1 \cap \dots \cap A_n)^c = A_1^c \cup \dots \cup A_n^c.$$

Procedamos por inducción. En este caso, si $n \in \mathbb{N}$ la afirmación $P(n)$ que nos interesa es

si A_1, \dots, A_n son subconjuntos de U , entonces $(A_1 \cap \dots \cap A_n)^c = A_1^c \cup \dots \cup A_n^c$

Observemos que la afirmación $P(1)$ es evidente, así que el caso base se satisface automáticamente. Resta entonces probar que vale el paso inductivo. Sea k un elemento de \mathbb{N} , supongamos que vale la afirmación $P(k)$ y sean A_1, \dots, A_{k+1} subconjuntos de U . Tenemos entonces que

$$\begin{aligned}(A_1 \cap \dots \cap A_{k+1})^c &= ((A_1 \cap \dots \cap A_k) \cap A_{k+1})^c \\ &= (A_1 \cap \dots \cap A_k)^c \cup A_{k+1}^c\end{aligned}$$

porque vale la Proposición 1.3.14(i), y esto es, de acuerdo a la hipótesis inductiva,

$$\begin{aligned}&= (A_1^c \cup \dots \cup A_k^c) \cup A_{k+1}^c \\ &= A_1^c \cup \dots \cup A_k^c \cup A_{k+1}^c.\end{aligned}$$

El «principio del palomar»

4.2.9. Mostremos que si $n \in \mathbb{N}$, entonces vale que

si distribuimos m bolas en n cajas y $m > n$, alguna caja necesariamente contiene dos bolas o más. (16)

Por ejemplo, una posible distribución de 11 bolas en 6 cajas es



y claramente hay cajas que tienen al menos dos bolas.

Llamemos $P(n)$ a la afirmación (16) y procedamos por inducción.

- Consideremos primero el caso en que $n = 1$. Es evidente que si tenemos una sola caja y más que una bola, al distribuir las bolas va a haber más de una bola en esa única caja: esto nos dice que la afirmación $P(1)$, el caso base, vale.

- Supongamos ahora que $k \in \mathbb{N}$ y que sabemos que vale la afirmación $P(k)$. Supongamos que distribuimos $k + 1$ cajas y m bolas, con $m > k + 1$, y consideremos tres casos:
 - Si la caja número $k + 1$ está vacía, entonces en realidad lo que hicimos fue distribuir las m bolas en las primeras k cajas, y la hipótesis inductiva nos dice que alguna de éstas contiene al menos dos bolas.
 - Si la caja número $k + 1$ contiene al menos dos bolas, entonces por supuesto alguna de las cajas contiene al menos dos bolas: por ejemplo, la número $k + 1$.
 - Consideremos, finalmente, el caso en que la caja $k + 1$ contiene exactamente una bola. En ese caso, distribuimos las otras $m - 1$ bolas en las primeras k cajas, y como $m - 1 > k$, ya que $m > k + 1$, la hipótesis inductiva nos dice que alguna de esas primeras k cajas contiene al menos dos bolas.

Así, en cualquier caso podemos garantizar que alguna caja contiene al menos dos bolas y, por lo tanto, que vale la afirmación $P(k + 1)$. Esto completa la inducción.

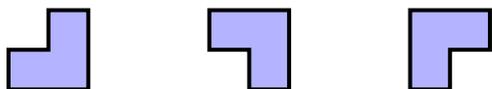
Un embalado

4.2.10. Supongamos que tenemos muchas piezas de la siguiente forma:



(17)

y que podemos rotarlas 90° , 180° y 270° , de manera que obtenemos



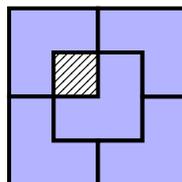
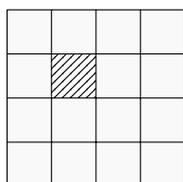
(18)

Afirmamos que para cada $n \in \mathbb{N}$ vale que

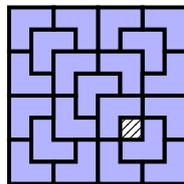
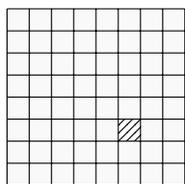
si tenemos un tablero de ajedrez de $2^n \times 2^n$ cuadrados al que le falta uno de los cuadrados, podemos taparlo con piezas como la de (17) y sus rotaciones (18) sin que falte cubrir ninguno de los cuadrados restantes ni haya uno cubierto más de una vez.

(19)

Así, por ejemplo, si $n = 2$ y tenemos un tablero de $2^2 \times 2^2$ cuadrados al que le falta un cuadrado como en el dibujo de la izquierda

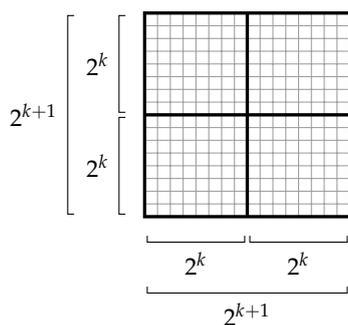


entonces podemos taparlo con fichas como está indicado en la figura derecha. De manera similar, el siguiente dibujo indica como tapar un tablero de $2^3 \times 2^3$ al que le falta el cuadrado gris siguiente:

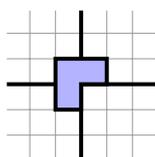


Probemos nuestra afirmación (19) haciendo inducción sobre n . El caso base, en el que $n = 1$, es inmediato: si tenemos un tablero de $2^1 \times 2^1$ al que le falta un cuadrado, el tablero tiene la forma es de una de nuestras piezas, así que ciertamente podemos taparlo de la manera correcta.

Supongamos entonces que $k \in \mathbb{N}$, que la afirmación (19) vale cuando n es k y consideremos un tablero de tamaño $2^{k+1} \times 2^{k+1}$ al que le falta uno de los casilleros. A ese tablero podemos dividirlo en cuatro tableros de tamaño $2^k \times 2^k$, y el casillero faltante está en uno de los cuatro:



Podemos poner una de nuestras piezas en la posición central, de manera que tenga un casillero en cada uno de los subtableros que no contienen el casillero que falta. Por ejemplo, si el casillero que falta en el tablero está en el subtablero que está en la esquina inferior derecha, ponemos una pieza en el centro orientada de la siguiente manera:



Hecho esto, cada uno de los cuatro subtableros es un tablero de tamaño $2^k \times 2^k$ al que le falta un casillero, y la hipótesis inductiva nos dice que podemos taparlo con nuestras

piezas de manera que no haya casilleros cubiertos más de una vez. Si hacemos esto con cada uno de estos subtableros, vemos que hemos cubierto el tablero original de la manera que queríamos. Esto significa que vale la afirmación (19) cuando n es $k + 1$ y completa la inducción.

§4.3. Dos variaciones del Principio de Inducción

Inducción «corrida»

4.3.1. Muchas veces tenemos una afirmación $P(n)$ para cada entero positivo n pero, a diferencia de los ejemplos que vimos antes, queremos mostrar no que vale para todo $n \in \mathbb{N}$ sino que vale a partir de algún entero en adelante. Así, por ejemplo, la afirmación « $n! \geq 3^n$ » vale para todo entero $n \geq 7$ (y no vale si $1 \leq n \leq 6$). Para probar cosas como esta podemos usar el Principio de Inducción bajo la siguiente forma:

Proposición. Sea n_0 un elemento de \mathbb{Z} y consideremos, para cada entero $n \geq n_0$, una afirmación $P(n)$. Si

- vale $P(n_0)$ y
- para cada entero $k \geq n_0$ se tiene que

$$P(k) \implies P(k + 1),$$

entonces la afirmación $P(n)$ vale para todo entero $n \geq n_0$.

Demostración. Para cada $n \in \mathbb{N}$ sea $Q(n)$ la afirmación $P(n + n_0 - 1)$. Las dos condiciones que aparecen en el enunciado nos dicen que vale $Q(1)$ y que para cada $k \in \mathbb{N}$ se tiene que $Q(k) \implies Q(k + 1)$, así que el Principio de Inducción nos dice que la afirmación $Q(n)$ vale para todo $n \in \mathbb{N}$: esto significa precisamente que la afirmación $P(n)$ vale para todo entero $n \geq n_0$. \square

4.3.2. Veamos, como ejemplo, que, como dijimos antes,

$$\text{para todo } n \geq 7 \text{ se tiene que } n! \geq 3^n \tag{20}$$

usando esta proposición. Llamemos $P(n)$ a la afirmación « $n! \geq 3^n$ ».

- Calculando, vemos que $7! = 5040$ mientras que $3^7 = 2187$, así que claramente vale que $3^7 \leq 7!$, es decir, vale la afirmación $P(7)$.

- Por otro lado, supongamos que $k \geq 7$ y que vale la afirmación $P(k)$, de manera que $3^k \leq k!$. Entonces se tiene que

$$3^{k+1} = 3^k \cdot 3 \leq k! \cdot (k+1)$$

usando la hipótesis inductiva y el hecho de que $3 \leq k+1$, y esto es

$$= (k+1)!$$

Vemos así que para cada entero $k \geq 7$ se tiene que

$$P(k) \implies P(k+1).$$

Estas dos observaciones y la Proposición 4.3.1 implican que vale (20).

Es de notar que la prueba del segundo punto que hicimos muestra que, de hecho, para todo entero $k \geq 2$ se tiene que $P(k) \implies P(k+1)$: esto no nos permite concluir que $P(r)$ valga para todo $n \geq 2$, ya que $P(2)$ no vale —en efecto, $2! = 2 < 9 = 3^2$.

4.3.3. La proposición anterior nos dice, informalmente, que podemos arrancar la inducción en cualquier entero. Es importante, de todas formas, arrancarla en *alguno*. Por ejemplo, si para cada $n \in \mathbb{N}$ llamamos $P(n)$ a la afirmación

$$n = n + 1,$$

entonces es cierto que si $k \in \mathbb{Z}$ vale que

$$P(k) \implies P(k+1).$$

En efecto, supongamos que k es un elemento de \mathbb{Z} y que vale $P(k)$, esto es, que $k = k + 1$. En ese caso, sumando 1 a ambos lados de esa igualdad vemos inmediatamente que $k + 1 = (k + 1) + 1$, es decir, que vale la afirmación $P(k + 1)$. Por supuesto, no existe *ningún* entero $n_0 \in \mathbb{Z}$ tal que $P(n_0)$ valga, así que no podemos usar la Proposición 4.3.1 para concluir nada.

Inducción «fuerte»

4.3.4. En todos los ejemplos de pruebas por inducción que llevamos vistos hasta ahora, para probar que una afirmación $P(n)$ vale cualquiera sea el entero positivo n mostramos que para cada $k \in \mathbb{N}$ se tiene que

$$P(k) \implies P(k+1).$$

Al hacer eso, fijamos $k \in \mathbb{N}$, supusimos que vale la afirmación $P(k)$ —ésta es la llamada «hipótesis inductiva»— y de alguna forma, a partir de eso, concluimos que vale la afirmación $P(k + 1)$. La razón por la que esto funciona, en todos los casos que vimos, es que saber que $P(k)$ vale ayuda a probar que $P(k + 1)$ vale. Hay situaciones, sin embargo, en que esto no es así.

4.3.5. Veamos un ejemplo sencillo de esto. Supongamos que tenemos monedas de 3 y de 7 centavos y tratemos de probar que

para cada $n \geq 12$ es posible juntar exactamente n centavos usando estas monedas.

Así, como $2 \cdot 3 + 4 \cdot 7 = 34$, podemos juntar 34 centavos usando 2 monedas de 3 centavos y 4 de 7. Si intentamos proceder por inducción, es natural llamar $P(n)$, para cada $n \in \mathbb{N}$, a la afirmación

es posible juntar n centavos usando monedas de 3 y de 7 centavos.

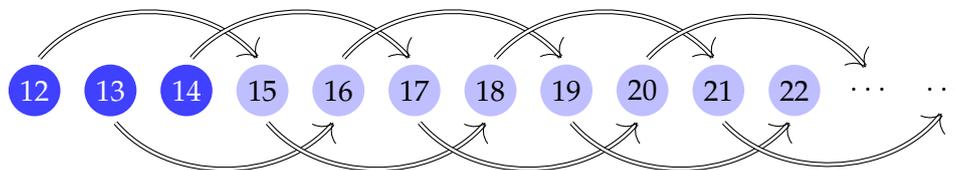
Como $12 = 4 \cdot 3$, con 4 monedas de 3 centavos juntamos 12 centavos: esto significa que vale la afirmación $P(12)$. Tenemos sin embargo un problema cuando intentamos mostrar que vale el paso inductivo: si suponemos que $k \in \mathbb{N}$ es tal que $k \geq 12$ y vale $P(k)$, entonces no hay ninguna forma de concluir que vale $P(k+1)$. En efecto, no es difícil convencerse que no es útil saber cómo juntar k centavos usando nuestras monedas si lo que queremos es juntar $k+1$.

De todas formas, podemos hacer la siguiente observación: si k es un entero positivo, entonces vale que

$$P(k-2) \implies P(k+1). \tag{21}$$

En efecto, si suponemos que la afirmación $P(k-2)$ vale, entonces existen a y b en \mathbb{N}_0 tales que $k-2 = 3a + 7b$ y, por lo tanto, $k+1 = 3(a+1) + 7b$: esto implica que vale la afirmación $P(k+1)$.

Usando que vale la implicación (21) y el hecho de que $P(12)$ vale, podemos concluir que $P(15)$, $P(18)$, $P(21)$ valen y, más generalmente, que $P(12+3c)$ vale para todo $c \in \mathbb{N}_0$, pero no que $P(16)$ vale, por ejemplo. Sin embargo, basta observar que $13 = 2 \cdot 3 + 1 \cdot 7$ y que $14 = 2 \cdot 7$ para deducir que $P(13)$ y $P(14)$ valen, y esto junto a la implicación (21) sí nos permite concluir que $P(n)$ vale para todo $n \geq 12$. El argumento puede representarse gráficamente de la siguiente manera



4.3.6. Estamos en una situación similar cuando queremos probar el siguiente resultado:

todo entero no negativo $n \in \mathbb{N}_0$ puede escribirse como suma de potencias distintas de 2.

Así, $77 = 2^0 + 2^2 + 2^3 + 2^6$, $530 = 2^1 + 2^4 + 2^9$ y 0 puede escribirse como la suma con cero sumandos y esa suma es una suma de potencias distintas de 2. Como ocurre en el ejemplo anterior, no es obvio que saber que el número $k - 1$ puede escribirse como suma de potencias distintas de 2 ayude a escribir a k de esa forma. En este caso, podemos proceder de la siguiente manera.

Sea $k \in \mathbb{N}$ y elijamos $r \in \mathbb{N}_0$ de manera que 2^r sea la potencia más grande de 2 que no supera a k , es decir, tal que $2^r \leq k$. El número $k - 2^r$ es un elemento de \mathbb{N}_0 . Supongamos por un momento que vale $P(k - 2^r)$, es decir, que $k - 2^r$ puede ser escrito como suma de potencias distintas de 2. Todas las potencias de dos que aparecen en esa suma son menores que 2^r : de no ser así, tendríamos que $k - 2^r \geq 2^r$ y, por lo tanto, que $k \geq 2^{r+1}$, lo que contradice la forma en que elegimos el número r . Como

$$k = (k - 2^r) + 2^r$$

y sabemos ahora que podemos escribir a $k - 2^r$ como suma de potencias de 2 distintas dos a dos y distintas de 2^r , es claro que k puede ser escrito como suma de potencias de dos distintas dos a dos: vale por lo tanto $P(k)$.

Lo que esto muestra es lo siguiente: para cada $k \in \mathbb{N}$ vale que

$$\text{si } r \text{ es el mayor elemento de } \mathbb{N}_0 \text{ tal que } k \geq 2^r \text{ y vale } P(k - 2^r), \text{ entonces} \quad (22) \\ \text{vale } P(k).$$

No es difícil convencerse que esto es suficiente para probar que $P(n)$ vale para todo $n \in \mathbb{N}_0$. Así, para ver que vale $P(22)$ observamos que la potencia más grande de 2 menor que 22 es 2^4 , así que basta ver que vale $P(22 - 2^4) = P(6)$. Ahora bien, la potencia de 2 más grande que es menor que 6 es 2^2 , así que es suficiente verificar que vale $P(6 - 2^2) = P(2)$: como 2 es él mismo una potencia de 2, esto es claro. Este razonamiento puede ilustrarse con el siguiente diagrama:

$$P(0) \rightsquigarrow P(2) \rightsquigarrow P(6) \rightsquigarrow P(22)$$

De manera similar, para ver que vale $P(5785)$ usando (22) hacemos las siguientes reducciones:

$$P(0) \rightsquigarrow P(1) \rightsquigarrow P(9) \rightsquigarrow P(25) \rightsquigarrow P(153) \rightsquigarrow P(665) \rightsquigarrow P(1689) \rightsquigarrow P(5785)$$

Lo que es importante es que (22) permite reducir la verificación de que la afirmación $P(k)$ vale a la verificación de que $P(l)$ vale para algún número l que es *menor* que k y entonces iterando este proceso un cierto número finito de veces concluimos que para verificar afirmación $P(k)$ es suficiente con verificar $P(0)$.

4.3.7. En general, tenemos el siguiente resultado:

Proposición. Sea $n_0 \in \mathbb{Z}$ y para cada entero $n \geq n_0$ sea $P(n)$ una afirmación. Si

- vale la afirmación $P(n_0)$ y
- para cada $k \geq n_0$ se tiene que

si valen las afirmaciones $P(n_0), P(n_0 + 1), \dots, P(k)$, entonces también vale la afirmación $P(k + 1)$,

entonces la afirmación $P(n)$ vale para todo entero $n \geq n_0$.

Demostración. Para cada entero $n \geq n_0$ sea $Q(n)$ la afirmación

las afirmaciones $P(n_0), P(n_0 + 1), \dots, P(n)$ valen.

y mostremos por inducción que $Q(n)$ vale cualquiera sea el entero $n \geq n_0$.

- En primer lugar, la afirmación $Q(n_0)$ vale, porque esta afirmación es simplemente la misma que $P(n_0)$ y que esta vale es la primera de las condiciones del enunciado.
- Supongamos ahora que $k \geq n_0$ y que vale $Q(k)$, es decir, que las afirmaciones $P(n_0), P(n_0 + 1), \dots, P(k)$ valen. De acuerdo a la segunda condición del enunciado, esto implica que $P(k + 1)$ vale: vemos así que si $Q(k)$ vale, entonces $P(n_0), \dots, P(k + 1)$ valen, es decir, que $Q(k + 1)$ vale.

Ahora bien, es claro que si $Q(n)$ vale para todo entero $n \neq 0$ en particular $P(n)$ vale para todo entero $n \geq n_0$, y esto es precisamente lo que queríamos probar. \square

4.3.8. Usando esta proposición, podemos formalizar los argumentos que hicimos en **4.3.5** y **4.3.6**.

- En el primer caso, para cada $n \geq 12$ llamamos $P(n)$ a la afirmación «es posible juntar n centavos con monedas de 3 y de 7 centavos». Que $P(12)$ vale es consecuencia de que $12 = 4 \cdot 3$, así que con 4 monedas de 3 centavos tenemos 12 centavos. Para usar la Proposición **4.3.7**, tenemos que probar ahora que para cada $k \geq 12$ se tiene que

si $P(12), P(13), \dots, P(k)$ valen, entonces vale $P(k + 1)$.

Supongamos entonces que $k \geq 12$ y que valen las afirmaciones $P(12), \dots, P(k)$. En particular, por supuesto, vale la afirmación $P(k - 2)$ y, como vimos antes, de esto se deduce que vale $P(k + 1)$: esto es lo que nos dice la implicación (21). Esto prueba el enunciado de **4.3.5**.

- Veamos ahora como usar la Proposición **4.3.7** para probar el enunciado de **4.3.6**. En este caso, para cada $n \in \mathbb{N}_0$ escribimos $P(n)$ a la afirmación

n puede escribirse como suma de potencias distintas de 2.

Es claro que $P(0)$ vale, ya que cero es suma de cero potencias de dos. Para el paso inductivo, supongamos que $k \in \mathbb{N}_0$ y que valen $P(0), \dots, P(k)$. Sea $r \in \mathbb{N}_0$ el mayor entero no negativo tal que $2^r \leq k + 1$. Si $k + 1 = 2^r$, entonces claramente $k + 1$ puede escribirse como suma de potencias distintas de 2. Si en cambio $k + 1 > 2^r$, entonces el número $l = k + 1 - 2^r$ es un de los elementos de $\{0, \dots, k\}$ y, de acuerdo a la hipótesis, vale $P(l)$, es decir, l puede escribirse como suma de potencias distintas de 2. Más aún, todas las potencias de dos que aparecen en esa suma son menores que 2^r : si no fuese ése el caso, tendríamos que $k + 1 - 2^r \geq 2^r$ y por lo tanto, $k + 1 \geq 2^{r+1}$, lo que es imposible en vista de la forma en que elegimos a r . Como

$$k + 1 = (k + 1 - 2^r) + 2^r$$

y ahora sabemos que $k + 1 - 2^r$ puede escribirse como suma de potencias distintas de 2 y todas distintas de 2^r , vemos que $k + 1$ puede escribirse como suma de potencias distintas de 2, es decir, que vale $P(k + 1)$.

Observemos que en ambos casos no estamos usando la hipótesis inductiva completa: en el primer ejemplo, la hipótesis inductiva es que valen $P(12), \dots, P(k)$, pero sólo usamos el hecho de que $P(k - 2)$ vale, mientras que en el segundo ejemplo la hipótesis inductiva es que valen $P(0), \dots, P(k)$ pero sólo necesitamos que $P(k + 1 - 2^r)$ valga.

4.3.9. Llamamos a un argumento basado en la Proposición 4.3.7 una *inducción fuerte*, porque es una forma de inducción en la que la hipótesis inductiva es mas fuerte que la usual. De todas formas, es importante notar que este principio es simplemente una aplicación del principio usual que usamos antes —esto queda claro en la prueba que dimos de la Proposición 4.3.7.

§4.4. Tres pruebas por «inducción fuerte»

Potencias de dos

4.4.1. Mostremos que para cada $n \in \mathbb{N}$ vale que

$$\text{existen } r \in \mathbb{N}_0 \text{ y un entero impar } u \text{ tales que } n = 2^r u. \tag{23}$$

Sea $P(n)$, para cada $n \in \mathbb{N}$, esta última afirmación.

- Es claro que $P(1)$ vale: como $1 = 2^0 \cdot 1$, basta tomar $r = 0$ y $u = 1$ en (23).

- Sea $k \in \mathbb{N}$ y supongamos que $P(1), \dots, P(k)$ valen. Si $k + 1$ es impar, entonces podemos tomar $r = 0$ y $u = k + 1$ en (23), y $P(k + 1)$ vale en ese caso. Si $k + 1$ es par, entonces existe $k' \in \mathbb{N}$ tal que $k + 1 = 2k'$. Como $k' = (k + 1)/2 < k + 1$, la hipótesis inductiva implica que $P(k')$ vale, es decir, que existen $r \in \mathbb{N}_0$ y un entero impar u tales que $k' = 2^r u$. Pero entonces es $k + 1 = 2k' = 2^{r+1}u$, y esto muestra que $P(k + 1)$ vale también en este caso.

Usando estas dos observaciones y la Proposición 4.3.7 podemos concluir, como queremos, que $P(n)$ vale para todo $n \in \mathbb{N}$.

Números irreducibles

4.4.2. Decimos que un número $n \in \mathbb{N}$ es *irreducible* si no puede ser escrito en la forma $n = ab$ con a y b enteros mayores que 1. Por ejemplo, es fácil ver que 2, 3, 5 y 7 son irreducibles, pero 6 o 9 no lo son: en efecto, $6 = 2 \cdot 3$ y $9 = 3 \cdot 3$.

Queremos probar que

$$\text{todo elemento de } \mathbb{N} \text{ es producto de números irreducibles} \quad (24)$$

usando la Proposición 4.3.7 y para ello llamaremos $P(n)$, para cada $n \in \mathbb{N}$, a la afirmación « n es igual a un producto de números irreducibles».

- La afirmación $P(1)$ vale: en efecto, 1 es igual a un producto con cero factores y —de manera tautológica— cada uno de esos factores es irreducible.
- Sea ahora $k \in \mathbb{N}$ y supongamos inductivamente que $P(1), \dots, P(k)$ valen. El número $k + 1$ puede ser o no irreducible. Si es irreducible, entonces ciertamente es igual a un producto de irreducibles —un producto con un único factor, él mismo— así que en ese caso $P(k + 1)$ vale. Si, por el contrario, $k + 1$ no es irreducible, entonces existen a y b en \mathbb{N} tales que $k + 1 = ab$ y $a, b \geq 2$. Observemos que

$$a = \frac{ab}{b} = \frac{k + 1}{b} \leq \frac{k + 1}{2} < k + 1$$

y, de manera similar, que $b < k + 1$. De acuerdo a la hipótesis inductiva, entonces, las afirmaciones $P(a)$ y $P(b)$ valen: esto significa que a y b son iguales a producto $p_1 \cdots p_u$ y $q_1 \cdots q_v$ de números irreducibles: se sigue de eso, claro, que

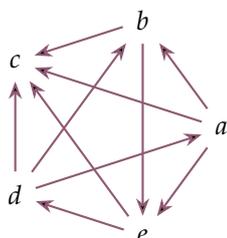
$$k + 1 = ab = p_1 \cdots p_u q_1 \cdots q_v,$$

así que también $k + 1$ es igual a un producto de números irreducibles. Vemos así que $P(k + 1)$ vale.

Estos dos puntos, junto con la Proposición 4.3.7, nos permiten concluir que la afirmación (24) vale.

Caminos

4.4.3. Supongamos que en un país hay n ciudades y que entre cada par de esas ciudades hay una ruta de una sola mano. Por ejemplo, si $n = 5$ y las ciudades se llaman a, b, c, d y e , podríamos describir las rutas usando el siguiente diagrama



Observemos que en este caso hay un camino que recorre todas las ciudades avanzando en la dirección permitida de las rutas, a saber

$$a \rightarrow b \rightarrow e \rightarrow d \rightarrow c.$$

No es el único, ya que también está el camino

$$d \rightarrow a \rightarrow b \rightarrow e \rightarrow c,$$

pero lo único que nos interesa es que hay alguno.

Queremos mostrar que para cada $n \in \mathbb{N}$ se tiene, de hecho, que

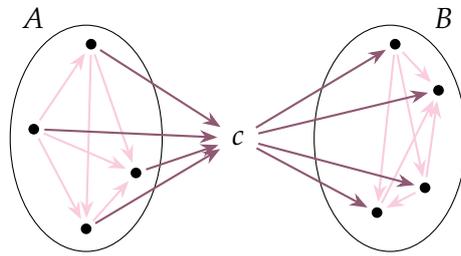
si hay n ciudades y entre cada dos de ellas hay una ruta de una sola mano, entonces hay al menos un camino que las recorre todas.

Sea $P(n)$ esta afirmación y procedamos por inducción en n .

- La afirmación $P(1)$ vale: si hay una sola ciudad, entonces hay un camino que recorre todas las ciudades, que consiste en empezar en esa ciudad y no moverse.
- Sea ahora $k \in \mathbb{N}$ y supongamos que todas las afirmaciones $P(1), \dots, P(k)$ valen. Supongamos además que tenemos $k + 1$ ciudades conectadas dos a dos con rutas de una sola mano y llamemos c a una de esas ciudades.

Sea A al conjunto de ciudades a tales que la ruta que une a y c va desde a a c , y B al conjunto de ciudades b tales que la ruta que une b y c va desde c hasta b .

Podemos representar esquemáticamente esta situación de la siguiente manera:



Como cada par de ciudades está conectado por una ruta, es claro que $A \cup B \cup \{c\}$ es el conjunto de todas las ciudades; por otro lado, los conjuntos A , B y $\{c\}$ son disjuntos dos a dos. En otras palabras, el conjunto $\{A, B, \{c\}\}$ es una partición del conjunto de nuestras $k + 1$ ciudades.

Supongamos ahora por un momento que tanto A como B son conjuntos no vacíos. Si r es el número de elementos de A , entonces claramente $1 \leq r \leq k$ y, de acuerdo a nuestra hipótesis inductiva, la afirmación $P(r)$ vale: esto significa que hay un camino —llamémoslo α — que recorre todas las ciudades de A . De manera similar, si s es el número de elementos de B , entonces $1 \leq s \leq k$ y la hipótesis inductiva nos dice que hay un camino —que podemos llamar β — que recorre todas las ciudades de B . Pero entonces hay un camino que recorre todas las ciudades: consiste en

- seguir primero el camino α ,
- tomar luego la ruta que va desde la última ciudad visitada por α hasta la ciudad c (notemos que esto es posible precisamente porque esa última ciudad visitada por α está en el conjunto A y, por lo tanto, la ruta que la une con c va en dirección de c),
- continuar por la ruta que va desde c hasta la primera ciudad visitada por el camino β (y esto es posible porque esta ciudad está en B) y,
- finalmente, recorrer el camino β .

Si alguno de los conjuntos A o B es vacío, podemos hacer algo parecido. Supongamos, por ejemplo, que A es vacío. En este caso, B tiene exactamente k elementos y la hipótesis inductiva nos dice que hay un camino β que recorre esas ciudades. Un camino que recorre todas las ciudades consiste entonces en empezar en c , tomar la ruta que va desde c hasta la primera ciudad visitada por ese camino β , y luego recorrer el camino β . Por supuesto, si B es vacío podemos proceder de manera similar.

Esto completa la inducción: gracias a la Proposición 4.3.7 podemos concluir que $P(n)$

vale cualquiera sea $n \in \mathbb{N}$.

§4.5. Ejercicios

4.5.1. Pruebe las siguientes afirmaciones por inducción con respecto a n .

- (a) $\sum_{i=1}^n i(i+1) = \frac{n(n+1)(n+2)}{2}$ para cada $n \geq 1$.
- (b) $\sum_{i=2}^n \frac{1}{i^2-1} = \frac{(n-1)(3n+2)}{4n(n+1)}$ para cada $n \geq 2$.
- (c) $\sum_{i=n}^{2n-1} (2i+1) = n^2$ para cada $n \geq 1$.
- (d) $\sum_{i=1}^n \frac{1}{i^2} \leq 2 - \frac{1}{n}$ para cada $n \geq 1$.
- (e) $\sqrt{n} \leq \sum_{i=1}^n \frac{1}{\sqrt{i}} \leq 2\sqrt{n} - 1$ para cada $n \geq 1$.

4.5.2. Muestre que

- (a) $2^n > n$ si $n \geq 1$;
- (b) $2^n \geq n^2$ si $n \geq 4$;
- (c) $n! > 2^n$ si $n \geq 4$;
- (d) $(1-x)^n \geq 1-nx$ si $n \geq 0$ y $x \in (0,1)$;
- (e) $(1+x)^n \geq 1+nx$ si $n \geq 0$ y $x > 0$.

4.5.3. Pruebe por inducción los siguientes enunciados:

- (a) El producto de n números enteros impares es impar.
- (b) Si $n \in \mathbb{N}$ x_1, \dots, x_n son números reales, entonces

$$\left| \sin \left(\sum_{i=1}^n x_i \right) \right| \leq \sum_{i=1}^n |\sin x_i|.$$

- (c) Si $n \in \mathbb{N}$ y $x \in \mathbb{R}$ es tal que $\sin \frac{1}{2}x \neq 0$, entonces

$$\sum_{i=1}^n \sin nx = \frac{\sin \frac{1}{2}(n+1)x \cdot \sin \frac{1}{2}nx}{\sin \frac{1}{2}x}$$

y

$$\frac{1}{2} + \sum_{i=1}^n \cos nx = \frac{\sin(n + \frac{1}{2})x}{2 \sin \frac{1}{2}x}.$$

(d) Si $n \in \mathbb{N}$ y $x \in \mathbb{R}$ es tal que $\sin x \neq 0$, entonces

$$\prod_{i=1}^n \cos 2^i x = \frac{\sin 2^{n+1} x}{2^n \sin x}.$$

4.5.4. Muestre que para cada entero $n \geq 0$ se tiene que $\sum_{i=1}^n i \cdot i! = (n + 1)! - 1$. Usando eso, pruebe que todo entero positivo $m \in \mathbb{N}$ puede escribirse en la forma

$$m = d_1 \cdot 1! + d_2 \cdot 2! + \cdots + d_r \cdot r!$$

para algún $r \in \mathbb{N}$ y con $d_i \in \{0, \dots, i\}$ para cada $i \in \{1, \dots, r\}$.

4.5.5.

- (a) Todo entero positivo puede escribirse en la forma $3a + 5b$ con a y b enteros.
- (b) Si $n \in \mathbb{N}$, entonces el número $3^{3n} + 5^{4n+2}$ es divisible por 13.

4.5.6. Todo número natural puede escribirse como suma de números de Fibonacci distintos y no consecutivos. Por ejemplo,

$$278 = 1 + 2 + 8 + 34 + 233 = F_1 + F_3 + F_6 + F_9 + F_{13}.$$

Este resultado —junto con la afirmación adicional de que esa escritura es única— es conocido como Teorema de Zeckendorf, por *Edouard Zeckendorf* (1901–1983, Bélgica), ya que éste publicó ese resultado en su trabajo [[Zec1972](#)], aunque había sido encontrado antes por *Cornelis Gerrit Lekkerkerker* (1922–1999, Países Bajos) en 1952..

Capítulo 5

Recursión

§5.1. Sucesiones

5.1.1. Si A es un conjunto, una *sucesión* de elementos de A es una función $f : \mathbb{N} \rightarrow A$. Casi siempre que tenemos una tal sucesión y un número $n \in \mathbb{N}$, preferimos escribir f_n en lugar de $f(n)$ y llamamos a f_n la *n-ésima componente* de la sucesión en lugar de «el valor de f en n ». Más aún, solemos escribir a una sucesión en la forma

$$(f_n)_{n \geq 1}$$

o, más explícitamente, listando las primeras de sus componentes

$$f_1, f_2, f_3, f_4, \dots$$

Por ejemplo, la función $f : \mathbb{N} \rightarrow \mathbb{R}$ tal que $f(n) = 2^n$ para todo $n \in \mathbb{N}$ es una sucesión de números reales puede ser escrita en la forma

$$(2^n)_{n \geq 1}$$

o en la forma

$$2, 4, 8, 16, 32, \dots \tag{1}$$

Es importante observar que esta última notación es solamente indicativa y no determina completamente a la sucesión. Así, la sucesión $g : \mathbb{N} \rightarrow \mathbb{R}$ tal que

$$g_n = \frac{1}{12}(x^4 - 6x^3 + 23x^2 - 18x + 24)$$

para cada $n \in \mathbb{N}$ tiene las mismas primeras cinco componentes que f y podríamos escribirla también en la forma (1). Para evitar ambigüedades, incluimos en la lista de las primeras componentes de una sucesión la expresión de tu componente general: escribimos, por ejemplo,

$$2, 4, 8, 16, 32, \dots, 2^n, \dots$$

y

$$2, 4, 8, 16, 32, \dots, \frac{1}{12}(x^4 - 6x^3 + 23x^2 - 18x + 24), \dots$$

para referirnos a f y a g , respectivamente.

5.1.2. Una pequeña variación de la definición de sucesión que acabamos de dar es la siguiente. Si $n_0 \in \mathbb{Z}$ y A es un conjunto, una *sucesión de elementos de A que empieza en n_0* es una función $f : \{n \in \mathbb{Z} : n \geq n_0\} \rightarrow A$. Escribimos a una tal sucesión en la forma

$$(f_n)_{n \geq n_0}$$

o listando sus componentes empezando por la n_0 -ésima,

$$f_{n_0}, f_{n_0+1}, f_{n_0+2}, \dots$$

Por ejemplo, la función $f : \mathbb{N}_0 \rightarrow \mathbb{Z}$ tal que $f(n) = 2^n$ es una sucesión de enteros

$$1, 2, 3, 4, \dots, 2^n, \dots$$

que empieza en la componente 0-ésima y la sucesión

$$\frac{1}{24}, \frac{1}{120}, \frac{1}{360}, \frac{1}{840}, \frac{1}{1680}, \dots, \frac{1}{n(n-1)(n-2)(n-3)}, \dots$$

empieza en su componente con índice 4.

§5.2. Definiciones por recursión

5.2.1. Muchas sucesiones se dan de manera explícita, como dimos los todos los ejemplos de sucesiones de la sección anterior, exhibiendo una *fórmula* que determine los valores de cada una de sus componentes. También es posible dar una sucesión de manera

implícita o *recursiva*. Veamos un ejemplo de qué significa esto: afirmamos que hay exactamente una sucesión $(a_n)_{n \geq 0}$ que empieza en su componente 0-ésima, que tiene

$$a_0 = 1 \tag{2}$$

y tal que para cada $n \geq 1$ vale que

$$a_n = n \cdot a_{n-1}. \tag{3}$$

Observemos que no estamos diciendo con esto *cuál* es el valor de cada componente a_n de la sucesión, sino que estamos dando un *procedimiento* o *algoritmo* que permite calcular esas componentes:

- Así, es claro que la 0-ésima componente de la sucesión es $a_0 = 1$, porque eso es precisamente uno de los dos datos que tenemos sobre ella.
- De la componente a_1 sabemos, gracias a (3), que es igual a $1 \cdot a_0$. Como sabemos ya cuál es el valor de a_0 , esto nos permite determinar de manera unívoca el valor de a_1 : en efecto, es $a_1 = 1 \cdot a_0 = 1 \cdot 1 = 1$.
- Podemos seguir de esta forma: de la componente a_2 de la sucesión sabemos que es igual a $2 \cdot a_1$ y como la componente a_1 está bien determinada por los datos que tenemos —y vale 1— tenemos que $a_2 = 2 \cdot a_1 = 2 \cdot 1 = 2$.
- Por supuesto, de manera similar vemos que $a_3 = 3 \cdot a_2 = 3 \cdot 2 = 6$, que $a_4 = 4 \cdot a_3 = 4 \cdot 6 = 24$, etc.

Vemos así que los datos que tenemos sobre la sucesión implican que las primeras componentes de la sucesión son, necesariamente,

$$1, 1, 2, 6, 24, 120, \dots$$

Más aún, debería ser intuitivamente claro que con este procedimiento podemos determinar de manera unívoca a partir de las ecuaciones (2) y (3) con las que empezamos *cualquier* componente de la sucesión: es por eso que hay exactamente una sucesión $(a_n)_{n \geq 0}$ que satisface esas dos ecuaciones.

5.2.2. Veamos otro ejemplo de una sucesión definida recursivamente. Afirmamos que hay exactamente una sucesión de números $(C_n)_{n \geq 0}$ tal que

$$C_0 = 1 \tag{4}$$

y, para cada entero $n \geq 1$,

$$C_n = \frac{2(2n-1)}{n+1} C_{n-1}. \tag{5}$$

En efecto, claramente toda sucesión que satisfaga esas dos condiciones tiene $C_0 = 1$, $C_1 = \frac{2(2 \cdot 1 - 1)}{1+1} C_0 = 1$, $C_2 = \frac{2(2 \cdot 2 - 1)}{2+1} C_1 = 2$, $C_3 = \frac{2(2 \cdot 3 - 1)}{3+1} C_2 = 5$, $C_4 = \frac{2(2 \cdot 4 - 1)}{4+1} C_3 = 14$, etc. Es fácil ver de esta manera que las primeras componentes de una sucesión que cumple (4) y (5) necesariamente son

n	0	1	2	3	4	5	6	7	8	9	10	11
C_n	1	1	2	5	14	42	132	429	1430	4862	16796	58786

Estos números se llaman *números de Catalan*, por Eugène Charles Catalan (1814–1894, Bélgica), y aparecen en los más variados contextos.

5.2.3. La forma general de las definiciones recursivas de sucesiones del tipo de los dos ejemplos que acabamos de ver es la siguiente. Empezamos con un conjunto A , un elemento $\alpha \in A$ y una función $f : \mathbb{N} \times A \rightarrow A$, y consideramos la sucesión $(a_n)_{n \geq 0}$ tal que

$$a_0 = \alpha \tag{6}$$

y

$$a_n = f(n, a_{n-1}) \tag{7}$$

para cada entero $n \geq 1$. Así,

- para obtener el ejemplo de la sucesión de **5.2.1**, podemos tomar $A = \mathbb{Z}$, $\alpha = 1$ y $f : \mathbb{N} \times \mathbb{Z} \rightarrow \mathbb{Z}$ a la función tal que $f(n, x) = n \cdot x$ para cada $n \in \mathbb{N}$ y $x \in \mathbb{Z}$, mientras que
- en el ejemplo de **5.2.2** de los números de Catalan se obtiene eligiendo $A = \mathbb{Q}$, $\alpha = 1$ y como $f : \mathbb{N} \times \mathbb{Q} \rightarrow \mathbb{Q}$ a la función que para cada $n \in \mathbb{N}$ y $x \in \mathbb{Q}$ tiene

$$f(n, x) = \frac{2(2n - 1)}{n + 1} x.$$

Aunque es intuitivamente claro, es sin embargo necesario verificar que una vez que A , α y f están fijos existe efectivamente una sucesión que satisface las condiciones (6) y (7) y que, más aún, existe una sola: esto es lo que justifica usar esas dos ecuaciones para definir la sucesión $(a_n)_{n \geq 0}$. De esto se ocupan las siguientes dos proposiciones.

5.2.4. Empecemos por la unicidad, que es la parte más sencilla:

Proposición. *Sea A un conjunto, sea α un elemento de A y sea $f : \mathbb{N} \times A \rightarrow A$ una función. Existe a lo sumo una sucesión $(a_n)_{n \geq 0}$ de elementos de A tal que*

$$a_0 = \alpha$$

y

$$a_n = f(n, a_{n-1})$$

para cada $n \in \mathbb{N}$.

Demostración. Supongamos que $(a_n)_{n \geq 0}$ y $(b_n)_{n \geq 0}$ son dos sucesiones de elementos de A tales que

$$a_0 = \alpha, \quad b_0 = \alpha \quad (8)$$

y que para cada $n \in \mathbb{N}$ se tiene que

$$a_n = f(n, a_{n-1}), \quad b_n = f(n, b_{n-1}). \quad (9)$$

Tenemos que mostrar que en estas condiciones las sucesiones $(a_n)_{n \geq 0}$ y $(b_n)_{n \geq 0}$ son iguales: es decir, que para todo $n \in \mathbb{N}_0$ se tiene que $a_n = b_n$. Llamemos para ello $P(n)$ a la afirmación « $a_n = b_n$ » y probemos que $P(n)$ vale para todo $n \in \mathbb{N}_0$ procediendo por inducción.

- Que $P(0)$ vale es consecuencia inmediata de las igualdades de (8).
- Supongamos que k es un elemento de \mathbb{N}_0 y que $P(k)$ vale, de manera que $a_k = b_k$. En ese caso, tenemos que

$$\begin{aligned} a_{k+1} &= f(k+1, a_k) && \text{porque vale la primera igualdad de (9)} \\ &= f(k+1, b_k) && \text{por la hipótesis inductiva} \\ &= b_{k+1} && \text{porque vale la segunda igualdad de (9).} \end{aligned}$$

Vemos así que vale la afirmación $P(k+1)$

Esto completa la inducción y, por lo tanto, la prueba de la proposición. \square

5.2.5. Consideremos ahora la cuestión de la existencia. Este resultado es bastante técnico, así que el lector puede saltarse sin mucha pérdida su demostración.

Proposición. Sea A un conjunto, sea α un elemento de A y sea $f : \mathbb{N} \times A \rightarrow A$ una función. Existe una sucesión $(a_n)_{n \geq 0}$ de elementos de A tal que

$$a_0 = \alpha$$

y

$$a_n = f(n, a_{n-1})$$

para cada $n \in \mathbb{N}$.

Demostración. Organizamos esta demostración en tres pasos.

Primer paso. Si $n \in \mathbb{N}$, sea $P(n)$ la afirmación

$$\begin{aligned} &\text{existe una \u00fanica funci\u00f3n } h_n : \{0, \dots, n\} \rightarrow A \text{ tal que } h_n(0) = \alpha \text{ y} \\ &h_n(i) = f(i, h_n(i-1)) \text{ para cada } i \in \{1, \dots, n\}. \end{aligned} \quad (10)$$

Nuestro primer objetivo es probar por inducci\u00f3n en n que esta afirmaci\u00f3n vale cualquiera sea $n \in \mathbb{N}$.

- Hay una funci\u00f3n $h_0 : \{0\} \rightarrow A$ tal que $h_0(0) = \alpha$. Esta funci\u00f3n satisface las condiciones y claramente es la \u00fanica funci\u00f3n $\{0\} \rightarrow A$ que las satisface: esto significa que vale la afirmaci\u00f3n $P(0)$.
- Sea $k \in \mathbb{N}_0$ y supongamos que vale la afirmaci\u00f3n $P(k)$, de manera que existe una \u00fanica funci\u00f3n $h_k : \{0, \dots, k\} \rightarrow A$ tal que

$$h_k(0) = \alpha$$

y

$$h_k(i) = f(i, h_k(i-1)) \text{ para cada } i \in \{1, \dots, k\}.$$

Definimos una nueva funci\u00f3n $g : \{0, \dots, k+1\} \rightarrow A$ de la siguiente manera: si $i \in \{0, \dots, k+1\}$, ponemos

$$g(i) = \begin{cases} h_k(i), & \text{si } 0 \leq i \leq k; \\ f(k+1, h_k(k)), & \text{si } i = k+1. \end{cases} \quad (11)$$

Afirmamos que g satisface las condiciones de que

$$g(0) = \alpha \quad (12)$$

y

$$g(i) = f(i, g(i-1)) \text{ para cada } i \in \{1, \dots, k+1\}. \quad (13)$$

Que la primera se cumple es evidente, ya que $g(0) = h_k(0) = \alpha$. Por otro lado, si i es un elemento de $\{1, \dots, k+1\}$, entonces hay dos casos: o bien $i \leq k$, y entonces

$$g(i) = h_k(i) = f(i, h_k(i-1)) = f(i, g(i-1)),$$

o bien $i = k+1$, y en ese caso

$$g(i) = g(k+1) = f(k+1, h_k(k)) = f(k+1, g(k)) = f(i, g(i-1))$$

por la forma en que definimos a g .

Veamos ahora que la función $g : \{0, \dots, k+1\} \rightarrow A$ que definimos en (11) es la única función $\{0, \dots, k+1\} \rightarrow A$ que satisface las condiciones (12) y (13). Para verlo, supongamos que $g' : \{0, \dots, k+1\} \rightarrow A$ es otra función con $g'(0) = \alpha$ y tal que $g'(i) = f(i, g'(i-1))$ para cada $i \in \{1, \dots, k+1\}$, y mostremos que, de hecho, g y g' son la misma función. Si no lo son, entonces el conjunto

$$X = \{i \in \{0, \dots, k+1\} : g(i) \neq g'(i)\}$$

es no vacío y tiene, por lo tanto, un menor elemento $j = \min X$. No puede ser que j sea igual a 0, ya que $g(0) = \alpha = g'(0)$, así que j es un elemento positivo de $\{0, \dots, k+1\}$. Se sigue de eso que $j-1$ es un elemento de $\{0, \dots, k+1\}$ que *no* pertenece al conjunto X , es decir, tal que $g(j-1) = g'(j-1)$: pero esto es absurdo, porque en ese caso tenemos que

$$g(j) = f(j, g(j-1)) = f(j, g'(j-1)) = g'(j),$$

contradiendo el hecho de que j pertenece a X .

Hemos probado que la función g que definimos en (11) satisface las condiciones (12) y (13), y que es la única que las satisface: esto significa que podemos poner $h_{k+1} = g$ para concluir que la afirmación $P(k+1)$ se cumple.

Esto completa la inducción y, por lo tanto, la prueba de que la afirmación $P(n)$ de (10) vale cualquiera sea para todo $n \in \mathbb{N}$.

Segundo paso. El segundo paso de la demostración es mostrar que

$$\begin{aligned} & \text{si } n \in \mathbb{N}_0, \text{ entonces la restricción de la función } h_{n+1} \text{ al conjunto } \{0, \dots, n\} \\ & \text{es } h_{n+1}|_{\{0, \dots, n\}} = h_n \text{ y, en particular, se tiene que } h_{n+1}(n) = h_n(n). \end{aligned} \quad (14)$$

Antes de eso, observemos que esta afirmación tiene sentido: el conjunto $\{0, \dots, n\}$ está contenido en el dominio de la función h_{n+1} y podemos entonces considerar la restricción $h_{n+1}|_{\{0, \dots, n\}}$, y esa restricción tiene el mismo dominio y codominio que h_n .

Para verificar (14), fijemos $n \in \mathbb{N}_0$ y llamemos q a la restricción $h_{n+1}|_{\{0, \dots, n\}}$, que es una función $\{0, \dots, n\} \rightarrow A$. Se tiene que

$$q(0) = h_{n+1}(0) = \alpha.$$

Por otro lado, si $k \in \{1, \dots, n\}$, entonces

$$q(k) = h_{n+1}(k) = f(k, h_{n+1}(k-1)) = f(k, q(k-1)).$$

Esto significa que q tiene las mismas propiedades que, de acuerdo a la afirmación $P(n)$, caracterizan unívocamente a la función h_n : se sigue de eso, entonces, que $q = h_n$, como queremos.

Tercer paso. Estamos por fin en condiciones de definir una sucesión $(a_n)_{n \geq 0}$ en A poniendo, para cada $n \in \mathbb{N}_0$,

$$a_n = h_n(n).$$

Esto tiene sentido precisamente porque a esta altura tenemos determinada para cada $n \in \mathbb{N}_0$ una función h_n que tiene al número n en su dominio. Para concluir la prueba de la proposición es suficiente que mostremos que la sucesión $(a_n)_{n \geq 0}$ satisface las condiciones del enunciado. Procedemos, como siempre, por inducción.

Primero, observemos que claramente $a_0 = h_0(0) = \alpha$, porque h_0 hace que valga la afirmación $P(0)$. Por otro lado, supongamos que $k \in \mathbb{N}_0$ es tal que vale que $a_k = f(k, a_{k-1})$ y observemos que entonces

$$\begin{aligned} a_{k+1} &= h_{k+1}(k+1) \\ &= f(k+1, h_{k+1}(k)) && \text{porque vale } P(k+1) \\ &= f(k+1, h_k(k)) && \text{gracias a (14)} \\ &= f(k+1, a_k) \end{aligned}$$

De acuerdo al Principio de Inducción, entonces, la sucesión a satisface las condiciones del enunciado. Esto completa la prueba de la proposición. \square

§5.3. Variaciones sobre la recursión

5.3.1. En la sección anterior vimos que es posible determinar una sucesión $(a_n)_{n \geq 0}$ de elementos de un conjunto A dando la componente inicial a_0 y describiendo cómo cada una de las demás componentes puede obtenerse a partir de la inmediatamente anterior. El punto clave que hace que esta idea funcione es que a pesar de que no damos una fórmula explícita para cada componente de la sucesión, la información que damos es de todas formas suficiente como para determinar unívocamente cada una de esas componentes.

Esta idea admite muchas variaciones. Consideraremos en esta sección algunas.

Recurrencias de orden superior

5.3.2. Existe exactamente una sucesión $(F_n)_{n \geq 0}$ de elementos de \mathbb{Z} tal que

$$F_0 = 0,$$

$$F_1 = 1$$

y

$$F_n = F_{n-1} + F_{n-2}$$

para cada entero $n \geq 2$. En efecto, F_0 y F_1 quedan completamente determinados por las dos primeras condiciones y sus valores son 0 y 1, respectivamente. La tercera condición, por su parte, nos dice que $F_2 = F_1 + F_0$, así que la componente F_2 también está completamente determinada: su valor es $F_2 = 1 + 0 = 1$. Esa misma tercera condición nos dice que $F_3 = F_2 + F_1$ y, de acuerdo a lo que ya sabemos, es entonces $F_3 = 1 + 1 = 2$. Claramente podemos continuar de esta forma: cada una de las componentes de la sucesión $(F_n)_{n \geq 0}$ empezando por la segunda está determinada por las dos anteriores: es su suma. Así, las primeras componentes de la sucesión son

$$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610, 987, 1597, \dots$$

Llamamos a esta sucesión la *sucesión de números de Fibonacci*, por *Fibonacci*, nombre por el que es conocido¹ *Leonardo de Pisa* (1175–1250, Italia). Durante su infancia, Fibonacci acompañó a su padre, que era comerciante, en sus viajes por la costa del Mediterráneo, donde aprendió los métodos de los árabes para hacer cálculos aritméticos. Años más tarde, en 1202, escribió un libro titulado *Liber Abaci* («El libro del cálculo» en latín) en el que explica el sistema de numeración que hoy llamamos arábigo: esta obra tuvo un rol fundamental en convencer a los europeos —tanto a los comerciantes como a los matemáticos— de abandonar el sistema de numeración romano, que usaban hasta ese momento, y adoptar el arábigo, que seguimos usando hasta hoy. En ese libro, Fibonacci plantea y resuelve un problema sobre el crecimiento de una población de conejos, y es en ese contexto que estudia la sucesión de números que hoy lleva su nombre.

5.3.3. Decimos que la definición de la sucesión de los números de Fibonacci es por una recurrencia *de orden dos*, porque cada una de las componentes de la sucesión —a partir de la segunda— depende del valor de las *dos* anteriores. Es fácil dar muchos ejemplos de sucesiones de esa forma.

Un ejemplo importante y estrechamente relacionado con el de los números de Fibonacci es la sucesión $(L_n)_{n \geq 0}$ de enteros que está determinada por las condiciones de que

$$L_0 = 2,$$

¹El apellido de su padre era Bonacci: Fibonacci es una contracción de la frase latina *filius Bonacci*, que significa «hijo de Bonacci». Es de notar que este sobrenombre le fue puesto recién en 1838 por el historiador francés Guillaume Libri.

$$L_1 = 1$$

y

$$L_n = L_{n-1} + L_{n-2}$$

para cada entero $n \geq 2$. Las primeras componentes de esta sucesión son

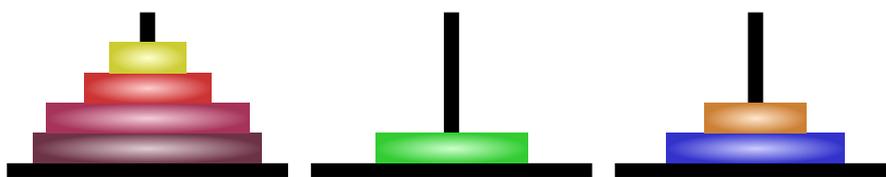
2, 1, 3, 4, 7, 11, 18, 29, 47, 76, 123, 199, 322, 521, 843, 1364, 2207, ...

Notemos que la relación de recurrencia que define a esta sucesión es exactamente la misma que la que usamos para construir la sucesión de los números de Fibonacci: cada componente, desde la segunda en adelante, es suma de las dos que la preceden. La única diferencia entre las dos definiciones radica en los valores iniciales de la recursión.

Esta sucesión $(L_n)_{n \geq 0}$ es la de los *números de Lucas*. El nombre recuerda a *François Édouard Anatole Lucas* (1842–1891, Francia), que estudió con gran detalle a los números de Fibonacci. Uno de sus intereses era el desarrollo de métodos para verificar si un número es primo o no: en 1857, a la edad de 15 años, empezó a probar un algoritmo —llamado hoy el «método de las secuencias de Lucas»— para decidir si el número

$$2^{127} - 1 = 170\,141\,183\,460\,469\,231\,731\,687\,303\,715\,884\,105\,727$$

es primo y en 1879, 19 años después, concluyó que sí lo es. Él inventó el juego conocido como *La Torre de Hanoi*, con el que el autor de estas notas se entretenía cuando era niño durante los largos viajes en auto que hacía con sus padres por la Patagonia.



5.3.4. Podemos también dar definiciones por recursión de órdenes más altos. Así, hay exactamente una sucesión $(T_n)_{n \geq 0}$ tal que

$$T_0 = T_1 = 0,$$

$$T_2 = 1$$

y

$$T_n = T_{n-1} + T_{n-2} + T_{n-3}$$

para cada $n \geq 3$. Calculando en orden, vemos que las primeras componentes de esta sucesión son

0, 0, 1, 1, 2, 4, 7, 13, 24, 44, 81, 149, 274, 504, 927, 1705, 3136, ...

La recursión que define esta sucesión —a la que llamamos, un poco en broma, *sucesión de números de tribonacci*— es de orden *tres*: cada uno de las componentes, a partir de la tercera, se calcula a partir de las tres anteriores.

5.3.5. De manera similar, hay exactamente una sucesión $(a_n)_{n \geq 0}$ tal que

$$a_0 = 0, \quad a_1 = 1, \quad a_2 = 2, \quad a_3 = 3$$

y

$$a_n = a_{n-1}a_{n-4} + (-1)^n$$

para cada $n \geq 4$, y sus primeras componentes son, empezando por la 0-ésima,

$$0, 1, 2, 3, 1, 0, 1, 2, 3, -1, 0, -1, -2, 1, 1, -2, 5, 4, 5, -11, -54, \dots$$

5.3.6. En general, para cada $k \in \mathbb{N}$ podemos considerar sucesiones dadas por relaciones de recursión de orden k : el siguiente resultado es el análogo de las Proposiciones 5.2.5 y 5.2.4 para esta situación:

Proposición. Sea A un conjunto, sea $k \in \mathbb{N}$, sean $\alpha_0, \dots, \alpha_{k-1}$ elementos de A y sea

$$f : \mathbb{N} \times \underbrace{A \times \dots \times A}_{k \text{ factores}} \rightarrow A$$

una función. Existe una y una única sucesión $(a_n)_{n \geq 0}$ de elementos de A tal que

$$a_i = \alpha_i \text{ si } 0 \leq i < k$$

y

$$a_n = f(n, a_{n-1}, a_{n-2}, \dots, a_{n-k})$$

para cada entero $n \geq k$. □

Omitimos la demostración, porque es enteramente similar a las de aquellas dos proposiciones. Esta proposición nos permite justificar la buena definición de los ejemplos que consideramos arriba:

- La sucesión $(F_n)_{n \geq 0}$ de los números de Fibonacci se obtiene tomando $A = \mathbb{N}_0$, $k = 2$, $\alpha_0 = 0$, $\alpha_1 = 1$ y como $f : \mathbb{N} \times A \times A \rightarrow A$ a la función tal que $f(n, x, y) = x + y$ para cada $(n, x, y) \in \mathbb{N} \times A \times A$.
- La sucesión $(L_n)_{n \geq 0}$ de los números de Lucas, por su parte, se obtiene con esa misma elección de A , k y f , pero con $\alpha_0 = 2$ y $\alpha_1 = 1$.

- La sucesión $(T_n)_{n \geq 0}$ de los números de tribonacci se obtiene tomando $A = \mathbb{N}$, $k = 3$, $\alpha_0 = \alpha_1 = 0$, $\alpha_2 = 1$ y como $f : \mathbb{N} \times A \times A \times A \rightarrow A$ a la función tal que $f(n, x, y, z) = x + y + z$ cada vez que $n \in \mathbb{N}$ y $x, y, z \in A$.
- Finalmente, la sucesión del ejemplo 5.3.5 se obtiene tomando $A = \mathbb{Z}$, $k = 4$, $\alpha_i = i$ para cada $i \in \{0, 1, 2, 3\}$ y $f : \mathbb{N} \times A \times A \times A \times A \rightarrow A$ a la función tal que

$$f(n, x, y, z, w) = xw + (-1)^n$$

cada vez que $n \in \mathbb{N}$ y $x, y, z, w \in A$.

5.3.7. Es posible definir sucesiones por recursiones más complicadas que las que se consideran en la Proposición 5.3.6. Veamos dos ejemplos

- (a) Hay una sucesión $(t_n)_{n \geq 1}$ que tiene $t_1 = 1$ y que es tal que, para cada entero $n \geq 2$, satisface la relación

$$t_n = \begin{cases} 1 + t_{n/2}, & \text{si } n \text{ es par;} \\ t_{n-1}, & \text{si } n \text{ es impar.} \end{cases}$$

Las primeras componentes de esta sucesión son

$$1, 2, 2, 3, 3, 3, 3, 4, 4, 4, 4, 4, 4, \dots$$

- (b) Hay una sucesión $(u_n)_{n \geq 0}$ tal que $u_1 = 0$ y

$$u_n = \sum_{m=0}^{n-1} m^2 u_m$$

para cada entero $n \geq 1$. Las primeras componentes de esta sucesión son

$$1, 5, 50, 850, 22100, 817700, 40885000, 2657525000, \dots$$

En cada uno de estos dos ejemplos, la relación de recursión que determina cada componente de la sucesión no depende de un número fijo de componentes anteriores: en el primer ejemplo, t_n depende, cuando n es par, de $t_{n/2}$, mientras que en el segundo ejemplo para calcular u_n usando la relación de recurrencia necesitamos conocer *todas* las componentes anteriores, u_0, \dots, u_{n-1} . De todas formas, es claro que en ambos casos las sucesiones consideradas están bien determinadas. Esto puede formalizarse en una proposición del mismo estilo que la Proposición 5.3.6, pero no lo haremos. Nos tomaremos, de todas formas, la libertad de usar éstos y otros tipos de recursiones para definir sucesiones

§5.4. Manipulación de sucesiones definidas recursivamente

5.4.1. El Principio de Inducción es una herramienta natural para probar cosas sobre sucesiones que están definidas usando relaciones de recurrencia. El objetivo de esta sección es usar las sucesiones ejemplos concretos y de Catalan para ejemplificar esto.

Números de Fibonacci

5.4.2. Sea $(F_n)_{n \geq 0}$ la sucesión de números de Fibonacci, de manera que

$$F_0 = 0,$$

$$F_1 = 1$$

y

$$F_n = F_{n-1} + F_{n-2} \tag{15}$$

para cada entero $n \geq 2$.

5.4.3. Lema. Para todo $n \in \mathbb{N}_0$ se tiene que $F_n \leq 2^n$.

Demostración. Procedemos por inducción, llamando $P(n)$ a la afirmación « $F_n \leq 2^n$ ». Es claro que $F_0 = 0 \leq 2^0$ y que $F_1 = 1 \leq 2^1$, así que $P(0)$ y $P(1)$ valen.

Supongamos, para establecer el paso inductivo, que $k \in \mathbb{N}$ es tal que $k \geq 2$ y que las afirmaciones $P(k-1)$ y $P(k-2)$ valen. Entonces

$$\begin{aligned} F_k &= F_{k-1} + F_{k-2} && \text{por (15)} \\ &\leq 2^{k-1} + 2^{k-2} && \text{por } P(k-1) \text{ y } P(k-2) \\ &\leq 2^{k-1} + 2^{k-1} && \text{ya que } 2^{k-2} \leq 2^{k-1} \\ &= 2 \cdot 2^{k-1} = 2^k. \end{aligned}$$

Esto nos dice que, bajo la hipótesis inductiva, vale la afirmación $P(k)$ y, por lo tanto, completa la inducción. □

5.4.4. La suma de los primeros números de Fibonacci difiere ella misma de un número de Fibonacci en una unidad:

Lema. Si $n \in \mathbb{N}$, entonces $F_1 + F_2 + \dots + F_n = F_{n+2} - 1$.

Demostración. Procedemos por inducción con respecto a n . Si $n = 1$, el lado izquierdo de la igualdad que queremos probar es $F_1 = 1$ y el derecho es $F_3 - 1 = 2 - 1 = 1$: vemos así que en ese caso la igualdad vale.

Supongamos ahora que $k \in \mathbb{N}$ es tal que $k \geq 2$ y que la igualdad del enunciado vale cuando n es $k - 1$, esto es, que

$$F_1 + F_2 + \cdots + F_{k-1} = F_{k+1} - 1.$$

Usando esto, vemos que

$$F_1 + F_2 + \cdots + F_{k-1} + F_k = F_{k+1} - 1 + F_k = F_{k+2} - 1,$$

así que la igualdad del enunciado también vale cuando n es k . Esto completa la inducción y prueba el lema. \square

5.4.5. La siguiente identidad es conocida como Identidad de Cassini, por *Giovanni Domenico Cassini* (1625–1712, Italia):

Lema. Para cada $n \in \mathbb{N}$ se tiene que $F_{n+1}F_{n-1} - F_n^2 = (-1)^n$.

Demostración. Cuando $n = 1$, el lado izquierdo de la igualdad que queremos probar es $F_2F_0 - F_1^2 = 0 \cdot 1 - 1 = -1$ y el derecho $(-1)^1 = -1$, así que vale.

Supongamos ahora que $k \in \mathbb{N}$ es tal que la igualdad del enunciado vale cuando n es k , es decir, tal que

$$F_{k+1}F_{k-1} - F_k^2 = (-1)^k \tag{16}$$

y calculemos, usando la relación de recurrencia que define a los números de Fibonacci:

$$\begin{aligned} F_{k+2}F_k - F_{k+1}^2 &= (F_k + F_{k+1})F_k - F_{k+1}(F_{k-1} + F_k) \\ &= F_k^2 + F_{k+1}F_k - F_{k+1}F_{k-1} - F_{k+1}F_k \\ &= F_k^2 - F_{k+1}F_{k-1} \end{aligned}$$

y esto es, de acuerdo a la hipótesis inductiva (16),

$$= (-1)^{k+1}.$$

Vemos así que bajo esa hipótesis la igualdad del enunciado también vale cuando n es $k + 1$. El lema es consecuencia de esto y del Principio de Inducción. \square

5.4.6. Las sumas de los productos de números de Fibonacci consecutivos tienen también una descripción directa en término de números de Fibonacci:

5.4.7. Lema. Para cada entero $n \geq 2$ se tiene que

$$F_1F_2 + F_2F_2 + \cdots + F_{n-1}F_n = \begin{cases} F_n^2, & \text{si } n \text{ es par;} \\ F_n^2 - 1, & \text{si } n \text{ es impar.} \end{cases}$$

Demostración. Sea $P(n)$ la afirmación de que vale la igualdad del enunciado. Cuando $n = 2$, a izquierda y a derecha en la igualdad del enunciado tenemos $F_1F_2 = 1 \cdot 1 = 1$ y $F_2^2 = 1^2 = 1$, respectivamente, así que esa igualdad vale en ese caso: en otras palabras, vale $P(2)$.

Supongamos ahora que k es un entero tal que $k \geq 2$ y que vale que

$$F_1F_2 + F_2F_2 + \cdots + F_{k-1}F_k = \begin{cases} F_k^2, & \text{si } k \text{ es par;} \\ F_k^2 - 1, & \text{si } k \text{ es impar.} \end{cases}$$

Tenemos entonces que

$$F_1F_2 + F_2F_2 + \cdots + F_kF_{k+1} = \begin{cases} F_k^2 + F_kF_{k+1}, & \text{si } k \text{ es par;} \\ F_k^2 - 1 + F_kF_{k+1}, & \text{si } k \text{ es impar.} \end{cases}$$

Ahora bien, es

$$F_k^2 + F_kF_{k+1} = F_k(F_k + F_{k+1}) = F_kF_{k+2} = F_{k+1}^2 + (-1)^{k+1}$$

de acuerdo a la identidad de Cassini 5.4.5, así que

$$F_1F_2 + F_2F_2 + \cdots + F_kF_{k+1} = \begin{cases} F_{k+1}^2 + (-1)^{k+1}, & \text{si } k \text{ es par;} \\ F_{k+1}^2 + (-1)^{k+1} - 1, & \text{si } k \text{ es impar;} \end{cases}$$

y esto es lo mismo que

$$\begin{cases} F_{k+1}^2 - 1, & \text{si } k + 1 \text{ es impar;} \\ F_{k+1}^2, & \text{si } k + 1 \text{ es par.} \end{cases}$$

Hemos mostrado así que si $k \geq 2$, entonces la afirmación $P(k)$ implica la afirmación $P(k + 1)$. El lema sigue de esto, gracias al Principio de Inducción. \square

5.4.8. Lema. Si $n \in \mathbb{N}$ y $m \in \mathbb{N}_0$, entonces

$$F_{n+m} = F_{n-1}F_m + F_nF_{m+1}.$$

Demostración. Para cada $n \in \mathbb{N}$ sea $P(n)$ la afirmación

$$\text{para todo } m \in \mathbb{N}_0 \text{ se tiene que } F_{n+m} = F_{n-1}F_m + F_nF_{m+1}.$$

Observemos que es evidente que $P(1)$ vale: es simplemente la afirmación de que para todo $m \in \mathbb{N}_0$ se tiene que $F_{m+1} = F_{m+1}$.

Supongamos entonces, para hacer inducción, que $k \in \mathbb{N}$ y que vale la afirmación $P(k)$, de manera que para todo $m \in \mathbb{N}_0$ se tiene que $F_{k+m} = F_{k-1}F_m + F_kF_{m+1}$. Ahora bien, para todo $m \in \mathbb{N}_0$ tenemos que

$$F_{(k+1)+m} = F_{k+(m+1)}$$

y, usando la hipótesis inductiva, vemos que esto es

$$\begin{aligned} &= F_{k-1}F_{m+1} + F_kF_{m+2} \\ &= F_{k-1}F_{m+1} + F_k(F_m + F_{m+1}) \\ &= F_kF_m + (F_{k-1} + F_k)F_{m+1} \\ &= F_kF_m + F_{k+1}F_{m+1}. \end{aligned}$$

Esto nos dice, precisamente, que vale la afirmación $P(k+1)$, y completa la prueba del lema, gracias al Principio de Inducción. \square

5.4.9. Este lema tiene el siguiente corolario inmediato: las fórmulas que aparecen en él se llaman *fórmulas de duplicación*, ya que permiten duplicar el índice.

Corolario. Para todo $n \in \mathbb{N}$ se tiene que

$$F_{2n} = F_{n+1}^2 - F_{n-1}^2 = F_n(2F_{n+1} - F_n)$$

y

$$F_{2n+1} = F_{n+1}^2 + F_n^2.$$

Demostración. Si en la identidad del Lema 5.4.8 ponemos $m = n$, vemos que

$$\begin{aligned} F_{2n} &= F_{n-1}F_n + F_nF_{n+1} \\ &= F_n(F_{n-1} + F_{n+1}) \\ &= (F_{n+1} - F_{n-1})(F_{n-1} + F_{n+1}) \\ &= F_{n+1}^2 - F_{n-1}^2, \end{aligned} \tag{17}$$

y esta es la primera de las igualdades del corolario. Volviendo a la igualdad (17), tenemos también que

$$F_{2n} = F_n(F_{n-1} + F_{n+1}) = F_n(2F_{n+1} - F_n),$$

ya que $F_{n-1} = F_{n+1} - F_n$, y ésta es la segunda igualdad del enunciado.

Finalmente, si ponemos $m = n + 1$ en el Lema 5.4.8, éste nos dice que

$$\begin{aligned} F_{2n+1} &= F_{n-1}F_{n+1} + F_nF_{n+2} \\ &= F_{n-1}F_{n+1} + F_n(F_n + F_{n+1}) \\ &= (F_{n-1} + F_n)F_{n+1} + F_n^2 \\ &= F_{n+1}^2 + F_n^2, \end{aligned}$$

que es la segunda de las igualdades del corolario. \square

5.4.10. La siguiente identidad, a la que llamamos *identidad de Catalan*, generaliza a la de Cassini:

Lema. Si $0 \leq r \leq n$, entonces

$$F_{n-r}F_{n+r} - F_n^2 = (-1)^{n-r+1}F_r^2.$$

En efecto, la identidad de Cassini es el caso particular de ésta en el que $r = 1$. La prueba de esta proposición es un poco más complicada que las de las anteriores: procederemos por inducción y para probar el paso inductivo haremos una inducción.

Demostración. Para cada $r \in \mathbb{N}_0$ sea $P(r)$ la afirmación

$$\text{para cada entero } n \geq r \text{ se tiene que } F_{n-r}F_{n+r} - F_n^2 = (-1)^{n-r+1}F_r^2.$$

Probaremos que para todo $r \in \mathbb{N}_0$ la afirmación $P(r)$ vale, procediendo por inducción con respecto a r : esto es demostrará la proposición. Observemos que la validez de la afirmación $P(0)$ es evidente, así que bastará que nos ocupemos del paso inductivo.

Sea entonces $s \in \mathbb{N}_0$ y mostremos que $P(s) \implies P(s+1)$. Para ello, supongamos que $P(s)$ vale, es decir, que

$$\text{si } n \geq s, \text{ entonces } F_{n-s}F_{n+s} - F_n^2 = (-1)^{n-s+1}F_s^2, \quad (18)$$

y mostremos que entonces también vale $P(s+1)$, es decir, que se tiene que

$$\text{si } n \geq s+1, \text{ entonces } F_{n-s-1}F_{n+s+1} - F_n^2 = (-1)^{n-s+2}F_{s+1}^2. \quad (19)$$

Para hacer esto, procederemos por inducción: para cada entero $n \geq s+1$, llamemos $Q_s(n)$ a la afirmación

$$F_{n-s-1}F_{n+s+1} - F_n^2 = (-1)^{n-s+2}F_{s+1}^2$$

y mostremos que $Q_s(n)$ vale para todo entero $n \geq s+1$. Esto probará (19).

La afirmación $Q_s(s+1)$ vale, ya que lo que afirma es que

$$F_0 F_{2(s+1)} - F_{s+1}^2 = (-1)^{s+1-s+2} F_{s+1}^2,$$

que es evidente. Supongamos entonces que $k \in \mathbb{N}$ es tal que $k \geq s+1$ y que $Q_s(k)$ vale. Sumando y restando $F_{k+1+s} F_{k+1-s}$, vemos que

$$\begin{aligned} F_{k+1-s-1} F_{k+1+s+1} - F_{k+1}^2 & \quad (20) \\ &= F_{k+1-s-1} F_{k+1+s+1} - F_{k+1+s} F_{k+1-s} + \underbrace{F_{k+1+s} F_{k+1-s} - F_{k+1}^2}. \end{aligned}$$

Como $k+1 \geq s$ y estamos suponiendo que $P(s)$ vale —es decir, que vale (18)— podemos reemplazar la parte marcada, y ver que esto es

$$= F_{k+1-s-1} F_{k+1+s+1} - F_{k+1+s} F_{k+1-s} + (-1)^{k+1-s+1} F_s^2$$

y esto, reescribiendo $F_{k+1+s+1}$ usando la relación de recurrencia de los números de Fibonacci y simplificando un poco, es, a su vez,

$$\begin{aligned} &= F_{k-s} (F_{k+1+s} + F_{k+s}) - F_{k+1+s} F_{k+1-s} + (-1)^{k-s} F_s^2 \\ &= (F_{k-s} - F_{k+1-s}) F_{k+1+s} + F_{k-s} F_{k+s} + (-1)^{k-s} F_s^2 \\ &= -F_{k-s-1} F_{k+1+s} + \underbrace{F_{k-s} F_{k+s} + (-1)^{k-s} F_s^2}. \end{aligned}$$

Como estamos suponiendo que $P(s)$ vale y $k \geq s$, reemplazando la parte marcada, vemos que esta última expresión es

$$= -F_{k-s-1} F_{k+1+s} + F_k^2$$

y, finalmente, como estamos suponiendo que $Q_s(k)$ vale, esto es

$$= (-1)^{k-s+1} F_{s+1}^2. \quad (21)$$

Con toda esta cadena de igualdades —que va de (20) a (21)— hemos probado que

$$F_{k+1-s-1} F_{k+1+s+1} - F_{k+1}^2 = (-1)^{(k+1)-(s+1)+1} F_{s+1}^2,$$

es decir, que vale $Q_s(k+1)$. Esto completa la prueba de la proposición. \square

5.4.11. Todo lo que hemos probado hasta ahora sobre los números de Fibonacci estuvo basado pura y exclusivamente en el hecho de que satisfacen la relación de recurrencia que los define. En particular, hasta ahora no tenemos ninguna fórmula cerrada para calcular los números de Fibonacci, sino solamente un algoritmo para calcularlos. El siguiente resultado, conocido como la *fórmula de Binet*, por *Jacques Philippe Marie Binet* (1786–1856, Francia), nos da una fórmula explícita:

Lema. Sean $\alpha = \frac{1 + \sqrt{5}}{2}$ y $\beta = \frac{1 - \sqrt{5}}{2}$ las dos raíces del polinomio $X^2 - X - 1$. Para cada $n \in \mathbb{N}_0$ se tiene que

$$F_n = \frac{\alpha^n - \beta^n}{\sqrt{5}}.$$

Demostración. Para cada $n \in \mathbb{N}_0$ sea $G_n = (\alpha^n - \beta^n)/\sqrt{5}$. Lo que tenemos que probar es que para cada $n \in \mathbb{N}_0$ es

$$F_n = G_n \tag{22}$$

y, como siempre, procedemos por inducción con respecto a n .

Como $G_0 = (1 - 1)/\sqrt{5} = 0$ y $G_1 = (\alpha - \beta)/\sqrt{5} = 1$, así que la igualdad (22) vale si n es 0 o 1. Para ver que vale el paso inductivo, supongamos que $k \in \mathbb{N}_0$ y que la igualdad (22) si n es k o $k + 1$. En ese caso, tenemos que

$$\sqrt{5} \cdot F_{k+2} = \sqrt{5} \cdot F_{k+1} + \sqrt{5} \cdot F_k = \alpha^{k+1} - \beta^{k+1} + \alpha^k - \beta^k.$$

Calculando, vemos que $\alpha^2 = \alpha + 1$ y $\beta^2 = \beta + 1$, así que $\alpha^{k+2} = \alpha^{k+1} + \alpha^k$ y $\beta^{k+2} = \beta^{k+1} + \beta^k$, y entonces lo que tenemos es que

$$\sqrt{5} \cdot F_{k+2} = \alpha^{k+2} - \beta^{k+2},$$

es decir, que $F_{k+2} = G_{k+2}$ y, por lo tanto, la igualdad (22) vale si n es $k + 2$. Esto prueba el lema. \square

Números de Catalan

5.4.12. Recordemos de 5.2.2 que la sucesión $(C_n)_{n \geq 0}$ de los números de Catalan es tal que

$$C_0 = 1$$

y

$$C_n = \frac{2(2n-1)}{n+1} C_{n-1} \tag{23}$$

para cada entero $n \geq 1$. Calculando, vemos que sus primeras componentes son

$$1, 1, 2, 5, 14, 42, 132, 429, 1430, 4862, 16796, \dots \tag{24}$$

5.4.13. Una primera observación que podemos hacer es que la sucesión de números de Catalan está, como la de Fibonacci, acotada por una sucesión de crecimiento exponencial:

Lema. Para cada $n \in \mathbb{N}_0$ se tiene que

$$C_n \leq \frac{4^n}{n+1}.$$

Demostración. Sea $P(n)$ la afirmación de que vale la desigualdad del enunciado. Como $C_0 = 1$ y $4^0/(0+1) = 1$, es claro que $P(0)$ vale. Por otro lado, si $k \in \mathbb{N}$ y suponemos que vale $P(k-1)$, entonces

$$C_n = \frac{2(2n-1)}{n+1} C_{n-1} \leq \frac{2(2n-1)}{n+1} \frac{4^{n-1}}{n} = \frac{2n-1}{2n} \frac{4^n}{n+1} \leq \frac{4^n}{n+1},$$

es decir, vale $P(k)$. El lema es consecuencia de esto y del Principio de Inducción. \square

5.4.14. A partir de la definición por recursión de los números de Catalan es fácil obtener una fórmula explícita:

Lema. Para todo $n \in \mathbb{N}_0$ es

$$C_n = \frac{1}{n+1} \frac{(2n)!}{n!n!}.$$

Demostración. Es inmediato que la igualdad del enunciado vale cuando $n = 0$. Veamos que si $k \in \mathbb{N}_0$ es tal que esa igualdad vale cuando n es k , entonces ella también vale cuando n es $k+1$: el lema seguirá entonces por inducción.

Sea entonces $k \in \mathbb{N}_0$ y supongamos que

$$C_k = \frac{1}{k+2} \frac{(2k)!}{k!k!}.$$

En ese caso, en vista de la relación de recurrencia que define a los números de Catalan, tenemos que

$$C_{k+1} = \frac{2(2(k+1)-1)}{(k+1)+1} C_k$$

y esto, gracias a nuestra hipótesis inductiva, es

$$= \frac{2(2k+1)}{k+2} \frac{1}{k+1} \frac{(2k)!}{k!k!}.$$

Multiplicando el numerador y el denominador de este cociente por $k+1$, vemos que es

$$\begin{aligned} &= \frac{2(2k+1)}{k+2} \frac{1}{k+1} \frac{(2k)!}{k!k!} \frac{k+1}{k+1} \\ &= \frac{1}{k+2} \frac{(2k+2)!}{(k+1)!(k+1)!} \end{aligned}$$

y esto completa la inducción. \square

5.4.15. Del cálculo directo de los números de Catalan, como en (24), vemos que parecen ser todos enteros: esto no es obvio ni a partir de la relación de recurrencia (23) que los define ni a partir de la fórmula explícita para ellos que nos da el Lema 5.4.14. Un primer paso para probar que se trata efectivamente de números enteros es el siguiente resultado, que es fundamental en el estudio de los números de Catalan:

Lema. Para cada $n \in \mathbb{N}_0$ se tiene que

$$C_{n+1} = \sum_{i=0}^n C_i C_{n-i}.$$

Demostración. Para cada $n \in \mathbb{N}_0$, llamemos $P(n)$ a la afirmación de que vale la igualdad del enunciado. Es claro que $P(0)$ vale: el miembro izquierdo de la igualdad es $C_1 = 1$ y el derecho $\sum_{i=0}^0 C_i C_{0-i} = C_0 C_0 = 1$.

Sea ahora $k \in \mathbb{N}_0$ y supongamos inductivamente que $P(k)$ vale. Tenemos que

$$\begin{aligned} (k+2) \sum_{i=0}^k C_i C_{k-i} &= \sum_{i=0}^k (k+2) C_i C_{k-i} = \sum_{i=0}^k (i+1+k-i+1) C_i C_{k-i} \\ &= \sum_{i=0}^k (i+1) C_i C_{k-i} + \sum_{i=0}^k (k-i+1) C_i C_{k-i} \\ &= C_0 C_k + \sum_{i=1}^k (i+1) C_i C_{k-i} + \sum_{i=0}^{k-1} (k-i+1) C_i C_{k-i} + C_k C_0 \end{aligned}$$

y, usando la relación (23), vemos que esto es

$$= C_0 C_k + \sum_{i=1}^k 2(2i-1) C_{i-1} C_{k-i} + \sum_{i=0}^{k-1} 2(2(k-i)-1) C_i C_{k-i-1} + C_k C_0.$$

Si cambiamos el índice i por $i-1$ en la primera de las dos sumas, podemos reescribir esto en la forma

$$C_0 C_k + \sum_{i=0}^{k-1} 2(2(i+1)-1) C_i C_{k-1-i} + \sum_{i=0}^{k-1} 2(2(k-i)-1) C_i C_{k-i-1} + C_k C_0$$

y, una vez hecho eso, juntar las dos sumas en una para obtener

$$2C_0 C_k + \sum_{i=0}^{k-1} 2 \left((2(i+1)-1) + (2(k-i)-1) \right) C_i C_{k-1-i}.$$

Esto es lo mismo que

$$2C_k + \sum_{i=0}^{k-1} 2 \cdot 2k \cdot C_i C_{k-1-i} = 2C_k + 2 \cdot 2k \sum_{i=0}^{k-1} C_i C_{k-1-i}$$

y, de acuerdo a la hipótesis inductiva, esto es igual a

$$2C_k + 2 \cdot 2kC_k = 2(2(k+1) - 1)C_k = (k+2)C_{k+1}.$$

Hemos probado de esta manera que

$$(k+2) \sum_{i=0}^k C_i C_{k-i} = (k+2)C_{k+1}$$

y, por lo tanto, que la afirmación $P(k+1)$ vale. El lema sigue por inducción. \square

5.4.16. Una primera consecuencia del Lema 5.4.15 es que podríamos haber definido la sucesión $(C_n)_{n \geq 0}$ de los números de Catalan diciendo que

$$C_0 = 1$$

y que

$$C_{n+1} = \sum_{i=0}^n C_i C_{n-i}$$

para cada $n \in \mathbb{N}_0$. De hecho, esta definición es la más frecuente en la literatura.

5.4.17. Una segunda consecuencia de ese lema es que podemos ahora fácilmente verificar que todos los números de Catalan son enteros:

Lema. Para todo $n \in \mathbb{N}_0$ el n -ésimo número de Catalan C_n es un entero.

Demostración. Esto sigue inductivamente del lema anterior. En efecto, C_0 es un entero y si $k \in \mathbb{N}_0$ y suponemos inductivamente que cada uno de los números C_0, \dots, C_k es un entero, entonces el Lema 5.4.15 nos dice que

$$C_{k+1} = \sum_{i=0}^k C_i C_{k-i}$$

y claramente esto implica que C_{k+1} también es un entero. \square

Un método rápido para calcular potencias

5.4.18. Fijemos un número real α no nulo y consideremos la sucesión $(a_n)_{n \geq 0}$ tal que

$$a_0 = 1$$

y

$$a_n = \alpha a_{n-1}$$

para cada $n \in \mathbb{N}$. Es inmediato que

para todo $n \in \mathbb{N}_0$ se tiene que $a_n = \alpha^n$.

En efecto, sigue inmediatamente de la definición de la sucesión que $a_0 = \alpha^0$, y si $k \in \mathbb{N}$ es tal que $a_{k-1} = \alpha^{k-1}$, entonces claramente se tiene que $a_k = \alpha a_{k-1} = \alpha \alpha^{k-1} = \alpha^k$. Esto nos da un procedimiento —el obvio— para calcular las potencias de α : para calcular α^n empezamos con 1 y lo multiplicamos n veces por α . Es evidente que cuando llevamos a cabo esto hacemos n multiplicaciones. Hay una forma mucho más eficiente para determinar α^n , basada en el siguiente resultado:

5.4.19. Lema. Hay una única sucesión $(b_n)_{n \geq 0}$ con $b_0 = 1$ y tal que para cada $n \in \mathbb{N}$ se tiene que

$$b_n = \begin{cases} (b_{n/2})^2, & \text{si } n \text{ es par;} \\ \alpha(b_{(n-1)/2})^2, & \text{si } n \text{ es impar.} \end{cases}$$

De hecho, si $(b_n)_{n \geq 0}$ es una sucesión que satisface estas dos condiciones entonces $b_n = \alpha^n$ para todo $n \in \mathbb{N}_0$.

Demostración. Veamos por inducción que si $(b_n)_{n \geq 0}$ es una sucesión que satisface las dos condiciones del enunciado entonces $b_n = \alpha^n$ para todo $n \in \mathbb{N}_0$. Es claro que $b_0 = \alpha^0$. Sea, por otro lado, $k \in \mathbb{N}$ y supongamos que $b_i = \alpha^i$ para todo entero i tal que $0 \leq i < k$. Consideramos ahora dos casos, de acuerdo a la paridad de k .

- Si k es par, entonces $k/2$ es un entero no negativo menor que k , la hipótesis inductiva nos dice que $b_{k/2} = \alpha^{k/2}$ y, por lo tanto,

$$b_k = (b_{k/2})^2 = (\alpha^{k/2})^2 = \alpha^k.$$

- Si en cambio k es impar, entonces $(k-1)/2$ es un entero no negativo menor que k y otra vez la hipótesis inductiva nos dice que $b_{(k-1)/2} = \alpha^{(k-1)/2}$. Usando esto, vemos que

$$b_k = \alpha(b_{(k-1)/2})^2 = \alpha(\alpha^{(k-1)/2})^2 = \alpha^k.$$

Así, en cualquier caso tenemos que $b_k = \alpha^k$ y esto completa la inducción.

Esto nos dice que a lo sumo hay una sucesión que satisface las dos condiciones del enunciado, a saber, la sucesión $(\alpha^n)_{n \geq 0}$ de las potencias de α . Para completar la prueba del lema, entonces, es suficiente con mostrar que esta última sucesión satisface efectivamente aquellas dos condiciones: esto es inmediato. \square

```

potencia :: Num a => a -> Integer -> a
potencia a 0 = 1
potencia a n
  | even n   = potencia a (n `div` 2) ^ 2
  | odd n    = a * potencia a ((n - 1) `div` 2) ^ 2

```

Figura 5.1. Un algoritmo rápido en HASKELL para calcular las potencias de un número. La expresión `potencia a n` se evalúa a a^n , asumiendo que n es un entero no negativo.

5.4.20. Este lema nos dice, por ejemplo, que

$$\alpha^{10} = b_{10} = b_5^2 = (\alpha b_2^2)^2 = (\alpha(b_1^2)^2)^2 = (\alpha(\alpha^2)^2)^2.$$

Esta expresión muestra que podemos calcular α^{10} haciendo cuatro productos: calculamos primero α^2 , luego lo elevamos al cuadrado, multiplicamos por α el resultado y elevamos lo que obtenemos al cuadrado. Esto es menos que la mitad de las multiplicaciones que hacemos si calculamos α^{10} de la manera evidente. De manera similar, usando el lema vemos que

$$\alpha^{154} = (a((a((a((a^2)^2)^2)^2)^2)^2)^2$$

y la expresión que aparece a la derecha en esta igualdad puede calcularse usando 10 productos: esto es considerablemente mejor que hacerlo con 154 productos!

En general, el lema nos provee una forma rápida de calcular las potencias de α — en la Figura 5.1 damos una implementación en HASKELL. Queremos ahora estimar la cantidad de trabajo que este algoritmo realiza.

Para cada $n \in \mathbb{N}$ sea M_n la cantidad de multiplicaciones que realizamos cuando usamos el Lema 5.4.19 para calcular α^n . De acuerdo a las fórmulas que aparecen en el enunciado de ese lema, tenemos que

$$M_1 = 0$$

y para cada entero $n \geq 2$ que

$$M_n = \begin{cases} 1 + M_{n/2}, & \text{si } n \text{ es par;} \\ 2 + M_{(n-1)/2}, & \text{si } n \text{ es impar.} \end{cases}$$

Las primeras componentes de la sucesión $(M_n)_{n \geq 0}$ son

$$0, 0, 1, 2, 2, 3, 3, 4, 3, 4, 4, 5, 4, 5, 5, 6, 4, 5, 5, 6, 5, 6, 6, 7, 5, 6, 6, 7, 6, 7, 7, \dots$$

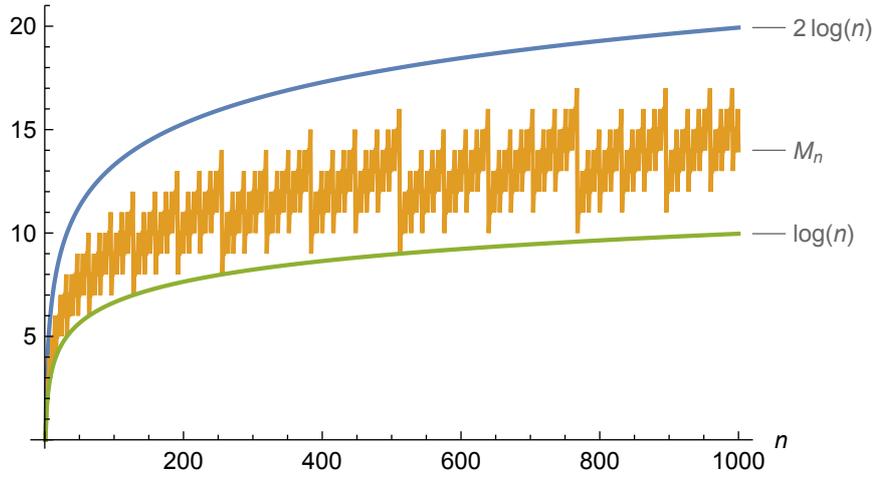


Figura 5.2. Un gráfico de la cantidad de multiplicaciones M_n que el algoritmo del Lema 5.4.19 hace al calcular α^n .

Esta sucesión es bastante irregular —como puede verse en la Figura 5.2— pero podemos acotarla sin mucha dificultad.

5.4.21. Lema. Para todo $n \in \mathbb{N}$ se tiene que $\log_2 n \leq M_n \leq 2 \log_2 n$.

De acuerdo a esto, el algoritmo que se deduce del Lema 5.4.19 calcula $\alpha^{1\,000\,000}$ usando entre 20 y 40 multiplicaciones —ya que $\log_2 1\,000\,000 = 19,931\dots$

Demostración. Cuando $n = 1$ la desigualdad es inmediata. Sea, por otro lado, $k \in \mathbb{N}$ tal que $k \geq 2$ y supongamos inductivamente que para todo entero i tal que $1 \leq i < k$ se tiene que $\log_2 i \leq M_i \leq 2 \log_2 i$. Dependiendo de la paridad de k tenemos dos casos.

Si k es par, entonces

$$M_k = 1 + M_{k/2} \leq 1 + 2 \log_2 \frac{k}{2} = 1 + 2 \log_2 k - 2 \log_2 2 \leq 2 \log_2 k,$$

ya que $1 - 2 \log_2 2 = -1 \leq 0$, y

$$M_k = 1 + M_{k/2} \geq 1 + \log_2 \frac{k}{2} = 1 + \log_2 k - \log_2 2 = \log_2 k.$$

Si en cambio k es impar, tenemos que

$$\begin{aligned} M_k &= 2 + M_{(k-1)/2} \leq 2 + 2 \log_2 \frac{k-1}{2} = 2 + 2 \log_2(k-1) - 2 \log_2 2 \\ &= 2 \log_2(k-1) \leq 2 \log_2 k \end{aligned}$$

y que

$$\begin{aligned}M_k &= 2 + M_{(k-1)/2} \geq 2 + \log_2 \frac{k-1}{2} = 2 + \log_2(k-1) - \log_2 2 \\ &= 1 + \log_2(k-1) \geq \log_2 k,\end{aligned}$$

ya que para todo número real $x \geq 2$ se tiene que $1 + \log_2(x-1) \geq \log_2 x$.

Vemos así que en cualquier caso se tiene que $\log_2 k \leq M_k \leq 2 \log_2 k$, y el lema sigue por inducción. \square

§5.5. Ejercicios

Una cota inferior exponencial para los números de Fibonacci

5.5.1. El Lema 5.4.3 nos dice que la sucesión de números de Fibonacci está acotada componente a componente superiormente por la sucesión $(2^n)_{n \geq 1}$, que crece exponencialmente. También podemos acotarla inferiormente:

Muestre que existe un número real $a > 1$ tal que para todo entero $n \geq 3$ se tiene que $F_n \geq a^n$.

Subsucesiones de la sucesión de los números de Fibonacci

5.5.2.

(a) Para cada entero $n \geq 2$ se tiene que

$$F_{2n} = 3F_{2(n-1)} - F_{2(n-2)}$$

y

$$F_{2n+1} = 3F_{2(n-1)+1} - F_{2(n-2)+1}.$$

(b) Sea $d \in \{0, 1, 2\}$. Para cada entero $n \geq 2$ se tiene que

$$F_{3n+d} = 4F_{3(n-1)+d} + F_{3(n-2)+d}.$$

5.5.3.

(a) Existe $u \in \mathbb{Z}$ tal que para cada $d \in \{0, 1, 2, 3\}$ y cada entero $n \geq 2$ se tiene que

$$F_{4n+d} = uF_{4(n-1)+d} - F_{4(n-2)+d}.$$

(b) Existen $u, v \in \mathbb{Z}$ tal que para cada $d \in \{0, 1, 2, 3, 4\}$ y cada entero $n \geq 2$ se tiene que

$$F_{5n+d} = uF_{5(n-1)+d} + vF_{5(n-2)+d}.$$

Sumas de números de Fibonacci

5.5.4. El Lema 5.4.4 nos da el valor de la suma de los primeros números de Fibonacci. También podemos considerar la suma de los de índice par o impar:

Si $n \in \mathbb{N}$, entonces

(a) $F_2 + F_4 + \cdots + F_{2n} = F_{2n+1} - 1.$

(b) $F_1 + F_3 + \cdots + F_{2n-1} = F_{2n}.$

5.5.5. Para cada $n \in \mathbb{N}_0$ sean

$$A_n = F_0 + F_3 + \cdots + F_{3n},$$

$$B_n = F_1 + F_4 + \cdots + F_{3n+1},$$

$$C_n = F_2 + F_5 + \cdots + F_{3n+2}.$$

Para cada entero $n \geq 3$ se tiene que

$$A_n = 5A_{n-1} - 3A_{n-2} - A_{n-3},$$

$$C_n = 5C_{n-1} - 3C_{n-2} - C_{n-3}$$

y para cada entero $n \geq 2$ se tiene que

$$B_n = 4B_{n-1} + B_{n-2}.$$

La sumas de los cuadrados de los números de Fibonacci

5.5.6. El Lema 5.4.7 nos dice que la suma de los productos de los primeros pares de números de Fibonacci consecutivos es esencialmente el cuadrado de un número de

Fibonacci. El siguiente resultado nos da el valor de una suma de cuadrados de números de Fibonacci:

Para cada $n \in \mathbb{N}$ se tiene que $\sum_{i=1}^n F_i^2 = F_n F_{n+1}$

Cocientes de números de Fibonacci

5.5.7. Usando la identidad de Cassini 5.4.5 muestre que para todo $n \in \mathbb{N}$ es

$$\frac{F_{n+1}}{F_n} - \frac{F_n}{F_{n-1}} = \frac{(-1)^n}{F_{n-1}F_n}.$$

Deduzca de ello que la sucesión $(F_{2n}/F_{2n-1})_{n \geq 1}$ es creciente, que la sucesión $(F_{2n+1}/F_{2n})_{n \geq 1}$ es decreciente, que ambas tienen el mismo límite y que ese límite es el número $(1 + \sqrt{5})/2$.

5.5.8. Muestre que

$$\frac{F_3}{F_2} = 1 + 1, \quad \frac{F_4}{F_3} = 1 + \frac{1}{1+1} \quad \frac{F_5}{F_4} = 1 + \frac{1}{1 + \frac{1}{1+1}} \quad \frac{F_6}{F_5} = 1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1+1}}}$$

y que, más generalmente, para cada entero $n \geq 2$ se tiene que

$$\frac{F_{n+1}}{F_n} = 1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \dots}}}$$

con $n - 2$ fracciones anidadas.

5.5.9. Usando ahora la identidad de Catalan 5.4.10 estudie la sucesión de cocientes $(F_{n+r}/F_n)_{n \geq 1}$ para cada $r \in \mathbb{N}$.

Números de Lucas

5.5.10. Recordemos que la sucesión $(L_n)_{n \geq 0}$ de números de Lucas es la sucesión tal que

$$L_0 = 2,$$

$$L_1 = 1$$

y

$$L_n = L_{n-1} + L_{n-2}$$

para cada entero $n \geq 2$.

5.5.11.

(a) $L_n = F_{n-1} + F_{n+1}$.

(b) $L_{2n} = L_n^2 + 2(-1)^n$.

(c) $F_{2n} = L_n F_n$.

(d) $F_{3n} = F_n(L_{2n} + (-1)^n)$.

(e) $F_{m+n} = \frac{1}{2}(F_m L_n + F_n L_m)$ y $F_{m-n} = \frac{1}{2}(-1)^n(F_m L_n - F_n L_m)$.

(f) $L_n^2 - 5F_n^2 = 4(-1)^n$.

(g) $\sum_{j=1}^n 2^{j-1} L_j = 2^n F_{n+1} - 1$.

5.5.12. Si $n, m \in \mathbb{N}_0$ son tales que $m \leq n$, entonces

$$F_{n+m} = L_m F_n - (-1)^m F_{n-m}.$$

Observe que esto da una relación de recurrencia de orden dos para la sucesión

$$F_d, F_{m+d}, F_{2m+d}, F_{3m+d}, F_{4m+d}, \dots$$

cada vez que $0 \leq d < m$. Esto generaliza los resultados de los ejercicios [5.5.4](#) y [5.5.5](#).

La razón áurea

5.5.13. Sea $\alpha = (1 + \sqrt{5})/2$.

(a) Para todo $n \in \mathbb{N}$ es $\alpha^n = \alpha F_n + F_{n-1}$ y $\alpha^n = \frac{L_n + F_n \sqrt{5}}{2}$.

(b) Para cada $n \in \mathbb{N}_0$ se tiene que

$$F_n = \left\lfloor \frac{\alpha^n}{\sqrt{5}} + \frac{1}{2} \right\rfloor.$$

Esto significa que F_n es el entero más cercano a $\alpha^n / \sqrt{5}$.

Cálculo rápido de los números de Fibonacci

5.5.14. La razón por la que las fórmulas de duplicación del Corolario 5.4.9 son importantes es que nos permiten calcular números de Fibonacci muy rápidamente. Así, por ejemplo, nos dice que

$$F_{100} = F_{50}(2F_{51} - F_{50})$$

y entonces para calcular F_{100} es suficiente que determinemos primero F_{50} y F_{51} . También tenemos que

$$F_{51} = F_{26}^2 - F_{25}^2, \quad F_{50} = F_{25}(2F_{26} - F_{25}),$$

así que basta que encontremos F_{25} y F_{26} . Por supuesto, podemos iterar este proceso y usando el corolario encontrar las siguientes igualdades:

$$\begin{aligned} F_{26} &= F_{13}(2F_{14} - F_{13}), & F_{25} &= F_{13}^2 - F_{12}^2, & F_{14} &= F_7(2F_8 - F_7), \\ F_{13} &= F_7^2 - F_6^2, & F_{12} &= F_6(2F_7 - F_6), & F_8 &= F_4(2F_5 - F_4), \\ F_7 &= F_4^2 - F_3^2, & F_6 &= F_3(2F_4 - F_3), & F_5 &= F_3^2 - F_2^2, \\ F_4 &= F_2(2F_3 - F_2), & F_3 &= F_2^2 - F_1^2, & F_2 &= F_1(2F_2 - F_1), \\ F_1 &= F_1^2 - F_0^2. \end{aligned}$$

Esto significa que para calcular F_{100} podemos ir calculando en orden cada uno de los números

$$F_1, F_2, F_3, F_4, F_5, F_6, F_7, F_8, F_{12}, F_{13}, F_{14}, F_{25}, F_{26}, F_{50}, F_{51}, F_{100}.$$

usando las igualdades que obtuvimos. De esta forma, vemos que podemos calcular F_{100} determinando solamente 15 otros números de Fibonacci y realizando unas 40 operaciones aritméticas. Esta idea puede extenderse a un algoritmo general. Veamos cómo.

Para cada $n \in \mathbb{N}_0$ sea P_n el par ordenado (F_n, F_{n+1}) . La sucesiones de pares ordenados

$$P_0, P_1, P_2, \dots$$

está determinada por una relación de recurrencia que permite calcular cada P_n en términos de $P_{\lfloor n/2 \rfloor}$:

Muestre que $P_0 = (0, 1)$ y que si $n \geq 1$, el par $P_{\lfloor n/2 \rfloor}$ es (a, b) y ponemos $c = a(2b - a)$

y $d = a^2 + b^2$, entonces

$$P_n = \begin{cases} (c, d), & \text{si } n \text{ es par;} \\ (d, c + d), & \text{si } n \text{ es impar.} \end{cases}$$

5.5.15. Para cada $n \in \mathbb{N}_0$ llamemos $T(n)$ al número de sumas, diferencias y multiplicaciones que hacemos usando esta relación de recurrencia para calcular el par ordenado P_n usando esta relación de recurrencia. Mirando las fórmulas, claramente tenemos que

$$T(0) = 0$$

y

$$T(n) = \begin{cases} 6 + T(\frac{1}{2}n), & \text{si } n \text{ es par;} \\ 7 + T(\frac{1}{2}(n-1)), & \text{si } n \text{ es impar.} \end{cases}$$

Muestre que $T(n) \leq 10 \log_2 n$ para todo $n \geq 3$.

Esto implica, por ejemplo, que si calculamos $F_{1\,000\,000}$ determinando primero el par ordenado $P_{1\,000\,000}$ y nos quedamos luego con su primera componente, hacemos como mucho 200 operaciones aritméticas. Observemos que $F_{1\,000\,000}$ es un número de 208 988 cifras decimales.

$$F_{1\,000\,000} = \underbrace{19532821287077577316 \dots \dots \dots 68996526838242546875}_{208\,988 \text{ dígitos}}$$

Si lo calculamos usando la recurrencia de orden dos que usamos para definir originalmente a los números de Fibonacci realizaremos un millón de sumas.

Hay que notar que muchas de esas 200 operaciones aritméticas son multiplicaciones y, más aún, multiplicaciones de números de muchos dígitos, así que hay que tener cuidado al comparar con el millón de sumas: multiplicar lleva bastante más tiempo que sumar. Hay, de todas formas, algoritmos muy rápidos para multiplicar números enteros —mucho más rápidos que el algoritmo que aprendemos de niños— y que entonces la determinación de un número como $F_{1\,000\,000}$ es factible. Usando la implementación dada en la Figura 5.3 en la página siguiente, que es una transcripción directa a HASKELL de la recurrencia del Ejercicio 5.5.14, podemos calcular $F_{1\,000\,000}$ en todo su esplendor en 43 milisegundos.

```

fibonacci :: Integer -> Integer
fibonacci n | n >= 0 = fst (fib n)

fib :: Integer -> (Integer, Integer)
fib 0      = (0, 1)
fib n
  | even n  = (c, d)
  | otherwise = (d, c + f)
  where (a, b) = fib (n `div` 2)
        c = a * (2 * b - a)
        d = a * a + b * b

```

Figura 5.3. Un algoritmo rápido en HASKELL para calcular números de Fibonacci, basado en la recurrencia del Ejercicio 5.5.14. La expresión `fib n` calcula el par ordenado P_n mientras que `fibonacci n` es la primera componente de ese par.

Una cota inferior exponencial para los números de Catalan

5.5.16. Para todo $n \in \mathbb{N}$ se tiene que $C_n \geq \frac{4^{n-1}}{n^2}$.

Capítulo 6

Divisibilidad

§6.1. La relación de divisibilidad

6.1.1. Si a y b son enteros, decimos que b *divide* a a , que b es un *divisor* de a y que a es un *múltiplo* de b , si existe un tercer entero c tal que $a = bc$ y en ese caso escribimos $b \mid a$. Obtenemos de esta forma una relación \mid en el conjunto \mathbb{Z} de los números enteros.

6.1.2. Proposición. (i) Para todo $a \in \mathbb{Z}$ se tiene que $1 \mid a$ y que $a \mid 0$.
(ii) Si a y $b \in \mathbb{Z}$ son tales que $b \mid a$, entonces también $(-b) \mid a$, $b \mid (-a)$ y $(-b) \mid (-a)$.

Demostración. (i) Si $a \in \mathbb{Z}$, entonces $a = 1 \cdot a$ y $0 = a \cdot 0$ y, por lo tanto, $1 \mid a$ y $a \mid 0$.

(ii) Sean a y b elementos de \mathbb{Z} tales que $b \mid a$, de manera que existe $c \in \mathbb{Z}$ tal que $a = bc$. Se sigue inmediatamente de eso que $a = (-b)c$, $(-a) = b(-c)$ y $(-a) = (-b)c$ y, por lo tanto, que $(-b) \mid a$, que $b \mid (-a)$ y que $(-b) \mid (-a)$. \square

6.1.3. Proposición. (i) La relación \mid de divisibilidad en \mathbb{Z} es reflexiva, transitiva y para cada $a, b \in \mathbb{Z}$ se tiene que

$$a \mid b, b \mid a \implies a = b \text{ o } a = -b. \quad (1)$$

(ii) La restricción de la relación \mid de divisibilidad a \mathbb{N} es una relación de orden, es decir, es reflexiva, transitiva y anti-simétrica.

Demostración. (i) Si $a \in \mathbb{Z}$, entonces $a = a \cdot 1$ y, por lo tanto, $a \mid a$: esto nos dice que la relación de divisibilidad es reflexiva. Por otro lado, si a, b y c son enteros y se tiene que

$a \mid b$ y $b \mid c$, de manera que existen enteros x e y tales que $b = ax$ y $c = by$, entonces claramente $c = axy$ y esto nos dice que $a \mid c$: vemos así que la relación \mid es transitiva.

Sean ahora a y b dos elementos de \mathbb{Z} y supongamos que $a \mid b$ y que $b \mid a$, de manera que existen enteros c y d tales que $b = ac$ y $a = bd$. Tenemos entonces que $a = acd$, es decir, que

$$a(1 - cd) = 0. \tag{2}$$

Si $a = 0$, entonces $b = ac = 0c = 0$ y a y b son iguales. Si en cambio $a \neq 0$, entonces de la igualdad (2) se deduce que $1 - cd = 0$, esto es, que $cd = 1$ y, por lo tanto, que $c = 1$ o $c = -1$. Correspondiendo a esas dos posibilidades tenemos que $b = a1 = a$ o que $b = a(-1) = -a$. Esto prueba la implicación (1).

(ii) La restricción de la relación \mid a \mathbb{N} es reflexiva y transitiva porque la relación original en \mathbb{Z} lo es, como acabamos de mostrar. Nos queda entonces probar que es anti-simétrica. Sean a y b dos elementos de \mathbb{N} tales que $a \mid b$ y $b \mid a$. Como en \mathbb{Z} vale la implicación (1), tenemos que $a = b$ o $a = -b$. Ahora bien, no puede ser que a sea $-b$, ya que a es positivo y $-b$ no: tiene que ser entonces $a = b$, que es lo que queríamos. \square

6.1.4. Usaremos muchas veces la siguiente observación, que establece una relación entre la relación de divisibilidad y la del orden usual de los números enteros:

Proposición. Sean a y b dos enteros. Si $b \mid a$ y $a \neq 0$, entonces $|b| \leq |a|$.

Notemos que la hipótesis de que el entero a no es nulo es necesaria para alcanzar la conclusión de la proposición: por ejemplo, es $1 \mid 0$ pero ciertamente no vale que $1 \leq 0$.

Demostración. Supongamos que b divide a a , de manera que existe $c \in \mathbb{Z}$ tal que $a = bc$. De esto se sigue que $|a| = |b||c|$. Si $a \neq 0$, entonces tiene que ser $c \neq 0$ y, por lo tanto, como c es un entero, $|c| \geq 1$. Tenemos entonces que $|a| = |b||c| \geq |b|$, como afirma la proposición. \square

6.1.5. Otra propiedad básica de la divisibilidad es su compatibilidad con las operaciones aritméticas:

Proposición. Sean a, b y c tres enteros. Si c divide a a y a b , entonces también divide a $a + b$ y a $a - b$.

Demostración. Supongamos que c divide a a y a b , de manera que existen enteros x e y tales que $a = cx$ y $b = cy$. En ese caso tenemos que $a + b = cx + cy = c(x + y)$ y $a - b = cx - cy = c(x - y)$: como claramente $x + y$ y $x - y$ son enteros, esto nos dice que c divide a $a + b$ y a $a - b$. La proposición queda así probada. \square

6.1.6. Muchas veces usaremos la Proposición 6.1.5 vía el siguiente corolario:

Corolario. Sean a, b y c tres enteros. Si c divide a a y a $a + b$, entonces también divide a b .

Demostración. En efecto, bajo esas condiciones de la proposición se sigue que c divide a $(a + b) - a = b$. \square

§6.2. El algoritmo de la división

6.2.1. Si a y b son enteros y b divide a a , entonces existe $c \in \mathbb{Z}$ tal que $a = bc$. Cuando b no divide a a , esto no es cierto, por supuesto. La Proposición 6.2.3 que probaremos más abajo nos permite describir exactamente qué sucede en el caso general.

6.2.2. Antes de eso, hagamos una observación que nos será útil varias veces:

Lema. Sea $b \in \mathbb{N}$ y sean $i, j \in \mathbb{Z}$. Si $0 \leq i, j < b$ y $b \mid i - j$, entonces $i = j$.

Demostración. Supongamos que i y j son dos enteros tales que $0 \leq i, j < b$ y $b \mid i - j$. Tenemos entonces que $-b < i - j < b$, así que $|i - j| < b$. Por otro lado, como b divide a $i - j$, de la Proposición 6.1.4 sabemos que o bien $i - j = 0$ o bien $|b| \leq |i - j|$. La segunda de estas dos posibilidades no ocurre, así que debe ocurrir la primera: esto nos dice que $i = j$, como afirma el lema. \square

6.2.3. La siguiente proposición establece una propiedad fundamental de los números enteros:

Proposición. Sean $a \in \mathbb{Z}$ y $b \in \mathbb{N}$. Existen enteros q y r tales que $a = qb + r$ y $0 \leq r < b$, y q y r están unívocamente determinados por a y b .

Llamamos a q y a r el *cociente* y el *resto* de la división de a por b , respectivamente.

Demostración. Consideremos el conjunto

$$S = \{a - kb : k \in \mathbb{Z}, a - kb \geq 0\}.$$

Este conjunto no es vacío: si $a \geq 0$, entonces $a - 0 \cdot b = a \geq 0$, así que $a \in S$, y si en cambio $a < 0$, entonces $a - (2a)b = (1 - 2a)a \geq 0$, así que $a - (2a)b \in S$. Como además es evidente que S está contenido en \mathbb{N}_0 , podemos considerar su mínimo $r = \min S$.

Como r pertenece a S , es $r \geq 0$ y existe $q \in \mathbb{Z}$ tal que $r = a - qb$, es decir, tal que $a = qb + r$. Para ver que $r < b$, supongamos por un momento que esto no es así, de

manera que $r \geq b$ y, por lo tanto,

$$a - (q + 1)b = r - b \geq 0.$$

Como consecuencia de esto, tenemos que $r - b \in S$: Esto es absurdo, ya que $r - b$ es estrictamente menor que r , porque b es positivo, y r es el menor elemento de S . Vemos así que $a = qb + r$ y que $0 \leq r < b$, y esto prueba la afirmación de existencia del enunciado. Veamos la de unicidad.

Supongamos que q, r, q' y r' son enteros tales que

$$a = qb + r, \quad 0 \leq r < b, \quad (3)$$

y

$$a = q'b + r', \quad 0 \leq r' < b. \quad (4)$$

Observemos que

$$qb + r = q'b + r' \quad (5)$$

y, por lo tanto, que $r - r' = (q' - q)b$. En particular, b divide a $r - r'$: como $0 \leq r, r' < b$, de acuerdo al Lema 6.2.2 tenemos entonces que $r = r'$. Usando esto en (5), concluimos que $qb = q'b$ y, en consecuencia, que $(q - q')b = 0$. Como $b \neq 0$, esto nos dice que $q - q' = 0$, esto es, que $q = q'$.

Así, si se cumplen las condiciones (3) y (4) se tiene necesariamente que $q = q'$ y que $r = r'$: esto prueba la afirmación de unicidad de la proposición. \square

6.2.4. El siguiente corolario de la proposición es casi inmediato y muestra que podemos ver al resto de la división de un número por otro, en cierta forma, como la única "obstrucción" a la divisibilidad.

Corolario. Sean $a \in \mathbb{Z}$ y $b \in \mathbb{N}$. El resto de la división de a por b es 0 si y solamente si b divide a a .

Demostración. Sean q y r el cociente y el resto, respectivamente, de la división de a por b , de manera que $a = qb + r$ y $0 \leq r < b$. Observemos que es $|r| < b$.

Si $r = 0$, entonces tenemos que $a = qb$ y, por lo tanto, que b divide a a . Supongamos, para probar la implicación recíproca, que b divide a a . Existe entonces $c \in \mathbb{Z}$ tal que $a = bc$ y, por lo tanto, $bc = qb + r$. De esta igualdad vemos que $r = (c - q)b$, así que, en particular, b divide a r y, de acuerdo a la Proposición 6.1.4, o bien $r = 0$ o bien $|b| \leq |r|$. Esta segunda posibilidad no ocurre —en efecto, sabemos que $|r| < b = |b|$ — así necesariamente $r = 0$. Esto completa la prueba del corolario. \square

6.2.5. Una observación importante que debemos hacer es que dados $a \in \mathbb{Z}$ y $b \in \mathbb{N}$, siempre podemos encontrar de manera efectiva al cociente q y al resto r de la división de a por b . En la base de esto esta la siguiente descripción alternativa de ese cociente:

Lema. Sea a un entero no negativo. El conjunto $T = \{k \in \mathbb{N}_0 : a - kb \geq 0\}$ es no vacío y finito, y su elemento máximo es el cociente de la división de a por b .

Demostración. El conjunto T no es vacío, ya que contiene a 0. Por otro lado, si $k \in T$, entonces $a - kb \geq 0$ y, por lo tanto, $k \leq a/b$: esto nos dice que el conjunto T está contenido en $\{0, \dots, \lfloor a/b \rfloor\}$ y, en particular, que es finito. Tiene entonces sentido considerar su elemento máximo q . Pongamos además $r = a - qb$.

Como $q \in T$, es $r \geq 0$. Tiene que ser $r < b$: si no fuese ese el caso, tendríamos que

$$a - (q + 1)b = a - qb - b = r - b \geq 0$$

y, por lo tanto, que $q + 1 \in T$: esto es absurdo, ya que elegimos a q como el mayor elemento de T . Concluimos de esta manera que $a = qb + r$ y que $0 \leq r < b$. De acuerdo a la Proposición 6.2.3, se sigue de esto que q y r son el cociente y el resto de la división de a por b y esto prueba el lema. \square

6.2.6. Si $a \in \mathbb{N}_0$ y $b \in \mathbb{N}$, este lema nos dice que para buscar el cociente y el resto de la división de a por b podemos proceder de la siguiente manera: para cada número $i \in \mathbb{N}_0$ desde 0 en adelante, en orden, calculamos $a - (i + 1)b$ y paramos la primera vez que esa diferencia sea negativa: tenemos entonces que el cociente es $q = i$ y que el resto es $r = a - ib$.

Si en cambio $a < 0$, podemos usar este procedimiento para encontrar el cociente q' y el resto r' de la división de $-a$ por b , de manera que $-a = q'b + r'$ y $0 \leq r' < b$. Si $r' = 0$, entonces tenemos que $a = (-q')b$, así que $q = -q'$ y $r = 0$ son el resto y el cociente de dividir a a por b ; si en cambio $r' \neq 0$, entonces es $a = (-q' - 1)b + (b - r')$ y $0 \leq b - r' < b$, así que $q = -q' - 1$ y $r = b - r'$ son el resto y el cociente de esa división.

En la Figura 6.1 en la página siguiente damos una implementación de este algoritmo en HASKELL. Es de notar que todos los lenguajes de programación proveen herramientas para calcular el cociente y el resto de la división entre dos enteros, usando algoritmos mucho más eficientes que éste. Así, en HASKELL, por ejemplo, tenemos las funciones `quot` y `rem` que hacen precisamente eso: las expresiones `quot a b` y `rem a b` denotan, respectivamente, el cociente y el resto de dividir a a por b .

```

division :: Integer -> Integer -> (Integer, Integer)
division a b
  | a >= 0          = (q, a - q * b)
  where q = head [i | i <- [0..], a - (i+1) * q < 0]
division a b
  | a < 0 && r /= 0 = (-q - 1, b - r)
  | otherwise       = (-q, 0)
  where (q, r) = division (-a) b

```

Figura 6.1. Un implementación del algoritmo de la división en HASKELL. La expresión `fib a b` se evalúa a un par ordenado `(q,r)` en el que `q` y `r` son, respectivamente, el cociente y el resto de la división de `a` por `b`.

§6.3. La notación posicional

6.3.1. Una aplicación simple pero importante de la Proposición 6.2.3 de la sección anterior es el siguiente resultado:

Proposición. Sea $b \in \mathbb{N}$ tal que $b \geq 2$. Si $a \in \mathbb{N}$, entonces hay una forma de elegir $k \in \mathbb{N}_0$ y $d_0, \dots, d_k \in \{0, \dots, b-1\}$ de manera que

$$a = d_0 + d_1b + d_2b^2 + \dots + d_kb^k$$

y $d_k \neq 0$.

Demostración. Si $a \in \mathbb{N}$, sea $P(a)$ la afirmación

existe una forma de elegir $k \in \mathbb{N}_0$ y $d_0, \dots, d_k \in \{0, \dots, b-1\}$ de manera que $a = \sum_{i=0}^k d_i b^i$ y $d_k \neq 0$.

Probaremos haciendo inducción con respecto a a que $P(a)$ vale cualquiera sea $a \in \mathbb{N}$.

Si $a = 1$, podemos elegir $k = 0$ y $d_0 = 1$ para tener $a = \sum_{i=0}^k d_i b^i$. Esto prueba que vale la afirmación $P(1)$.

Sea ahora $a \in \mathbb{N}$ y supongamos que cada una de las afirmaciones $P(1), P(2), \dots, P(a-1)$ vale. De acuerdo a la Proposición 6.2.3, existen enteros q y r tales que $a = qb + r$ y $0 \leq r < b$. Como $q = (a-r)/b \leq a/b$ y $b \geq 2$, tenemos que $q < a$.

Si $q = 0$, entonces $a = r$ y podemos elegir $k = 0$ y $d_0 = r$ para ver que $P(a)$ vale. Supongamos entonces que $q > 0$. En ese caso, nuestra hipótesis inductiva nos dice que $P(q)$ vale, es decir, que existen $l \in \mathbb{N}_0$ y $e_0, \dots, e_l \in \{0, \dots, b-1\}$ tales que $q = \sum_{i=0}^l e_i b^i$

y $e_l \neq 0$. Como consecuencia de esto tenemos que

$$a = r + qb = r + \left(\sum_{i=0}^l e_i b^i \right) b = r + \sum_{i=0}^l e_i b^{i+1} = r + \sum_{i=1}^{l+1} e_{i-1} b^i.$$

Podemos entonces elegir $k = l + 1$, $d_0 = r$ y $d_i = e_{i-1}$ para cada $i \in \{1, \dots, k\}$ para tener $a = \sum_{i=0}^k d_i b^i$ y $d_k \neq 0$, y esto muestra que vale la afirmación $P(a)$ también en este caso. La inducción queda así completa y eso prueba la proposición. \square

6.3.2. Los números k y d_0, \dots, d_k de la Proposición 6.3.1 están bien determinados por los números b y a con los que empezamos.

Proposición. Sea $b \in \mathbb{N}$ tal que $b \geq 2$. Si $a \in \mathbb{N}$, entonces hay exactamente una forma de elegir $k \in \mathbb{N}$ y $d_0, \dots, d_k \in \{0, \dots, b-1\}$ de manera que se cumplan las dos condiciones de la Proposición 6.3.1.

Demostración. Supongamos que $k, l \in \mathbb{N}_0$ y que $d_0, \dots, d_k, e_0, \dots, e_l \in \{0, \dots, b-1\}$ son tales que

$$d_0 + d_1 b + \dots + d_k b^k = e_0 + e_1 b + \dots + e_l b^l, \quad (6)$$

$d_k \neq 0$ y $e_k \neq 0$. Probaremos que en esta situación necesariamente se tiene que $k = l$ y que $d_i = e_i$ para todo $i \in \{0, \dots, k\}$: la proposición es consecuencia inmediata de esto. Observemos que sin pérdida de generalidad podemos suponer que $k \leq l$.

De la igualdad (6) se deduce que

$$d_0 - e_0 = \sum_{i=1}^l e_i b^i - \sum_{i=1}^k d_i b^i = \left(\sum_{i=1}^l e_i b^{i-1} - \sum_{i=1}^k d_i b^{i-1} \right) b,$$

así que $b \mid d_0 - e_0$. Como $0 \leq d_0, e_0 < b$, el Lema 6.2.2 nos permite concluir que $d_0 = e_0$.

Esto nos dice que el conjunto

$$S = \{i \in \{0, \dots, k\} : d_j = e_j \text{ para cada } j \in \{0, \dots, i\}\}$$

no es vacío y podemos, por lo tanto, considerar su máximo m . Tenemos entonces que $m \in S$, de manera que

$$d_j = e_j \text{ para cada } j \in \{0, \dots, m\},$$

y o bien $m = k$ o bien $m < k$ y $d_{m+1} \neq e_{m+1}$.

Supongamos que estamos en el segundo de estos dos casos. De la igualdad (6), tenemos que

$$0 = \sum_{i=0}^l e_i b^i - \sum_{i=0}^k d_i b^i = \sum_{i=m+1}^l e_i b^i - \sum_{i=m+1}^k d_i b^i$$

$$= e_{m+1} - d_{m+1} + b \left(\sum_{i=m+1}^l e_i b^{i-1} - \sum_{i=m+1}^k d_i b^{i-1} \right).$$

Como la expresión entre paréntesis es un entero, vemos que b divide a $d_{m+1} - e_{m+1}$. Como además $0 \leq d_{m+1}, e_{m+1} < b$, el Lema 6.2.2 nos dice que $d_{m+1} = e_{m+1}$: esto es absurdo, ya que contradice nuestra hipótesis.

Esto implica que necesariamente tenemos $m = k$. Así, todos los sumandos que aparecen a la izquierda de la igualdad (6) también aparecen a la derecha y, por lo tanto, esa igualdad implica que

$$0 = \sum_{i=k+1}^l e_i b^i.$$

Como cada uno de los términos de esta última suma es positivo, la única forma en que esto es posible es que no haya, de hecho, ninguno: en otras palabras, que se tenga, $k = l$. Ahora bien, que los tres números m , l y k sean iguales significa precisamente que vale lo que queremos, y esto completa la prueba de la proposición. \square

6.3.3. Si fijamos $b \in \mathbb{N}$ con $n \geq 2$ y $a \in \mathbb{N}$, las Proposiciones 6.3.1 y 6.3.2 nos dicen que hay exactamente una forma de elegir $k \in \mathbb{N}_0$ y $d_0, \dots, d_k \in \{0, \dots, b-1\}$ de manera que $a = \sum_{i=0}^k d_i b^i$ y $d_k \neq 0$. Para representar esto escribimos

$$a = (d_k, d_{k-1}, \dots, d_1, d_0)_b.$$

Llamamos a esto la **representación en base b** del número a y a los números d_k, \dots, d_0 los **dígitos** de a en base b . Cuando b es 10, 2, 8 o 16, decimos **representación decimal**, **binaria**, **octal** o **hexadecimal** en lugar de representación en base b .

Así, por ejemplo, es fácil verificar que

$$1234 = (5, 4, 1, 4)_6 = (1, 6, 2, 1)_9 = (1, 18, 19)_{27} = (1, 0)_{1234} = (1234)_{10000}.$$

§6.4. Máximo común divisor

6.4.1. Sean a y b dos enteros y supongamos que no son los dos nulos. Un **divisor común** de a y b es simplemente un entero d que es tanto un divisor de a como de b . Escribimos $D(a, b)$ al conjunto de todos los divisores comunes positivos de a y b .

Este conjunto $D(a, b)$ no es vacío: en efecto, el número 1 pertenece a $D(a, b)$. Por otro lado, si $d \in D(a, b)$, entonces de la Proposición 6.1.4 tenemos que o bien $a = 0$ o bien

$d \leq |a|$, y que o bien $b = 0$ o bien $d \leq |b|$. Como a y b no son los dos nulos, se sigue de esto que $d \leq \max\{|a|, |b|\}$. En otras palabras, si ponemos $N = \max\{|a|, |b|\}$, entonces $D(a, b) \subseteq \{1, \dots, N\}$. Vemos así que el conjunto $D(a, b)$ es finito y, en particular, que podemos considerar su elemento máximo: lo llamamos *máximo común divisor* de a y b y lo escribimos $\text{mcd}(a, b)$.

Esto define el máximo común divisor de dos números que no son simultáneamente nulos. Observemos que si $a = b = 0$, entonces todo elemento de \mathbb{N} es un divisor común positivo de a y b y que, por lo tanto, no tiene sentido hablar en este caso del elemento máximo de $D(a, b)$. En este caso especial definimos $\text{mcd}(0, 0) = 0$.

6.4.2. Decimos que dos enteros a y b son *coprimos* cuando $\text{mcd}(a, b) = 1$. Esta condición significa, precisamente, que no son ambos nulos y que el único divisor común positivo que tienen es 1.

6.4.3. El máximo común divisor de dos enteros es un elemento de \mathbb{N}_0 y es nulo si y solamente si esos dos enteros son nulos: esto es consecuencia inmediata de la definición. Otras observaciones sencillas que podemos hacer son las siguientes:

Proposición. Sean a y b dos enteros.

- (i) Es $\text{mcd}(a, b) = \text{mcd}(b, a)$.
- (ii) Se tiene que $\text{mcd}(a, b) = |a|$ si y solamente si a divide a b .
- (iii) En particular, se tiene que $\text{mcd}(a, 0) = |a|$.
- (iv) Se tiene que $\text{mcd}(a, b) = \text{mcd}(-a, b) = \text{mcd}(a, -b) = \text{mcd}(-a, -b)$.

Demostración. (i) Si $a = b = 0$, entonces es evidente que $\text{mcd}(a, b) = \text{mcd}(b, a)$. Si en cambio alguno de a o b es no nulo, entonces los conjuntos $D(a, b)$ y $D(b, a)$ coinciden, así que tienen el mismo elemento máximo: esto significa, precisamente, que $\text{mcd}(a, b) = \text{mcd}(b, a)$ también en este caso.

(ii) Supongamos primero que a divide a b . Si $a = 0$, entonces también $b = 0$ y la igualdad $\text{mcd}(a, b) = |a|$ es evidente. Supongamos entonces que $a \neq 0$. Si $d \in D(a, b)$, entonces d divide a a y, de acuerdo a la Proposición 6.1.4, se tiene que $d \leq |a|$. Como además $|a| \in D(a, b)$, vemos que $|a|$ es el elemento máximo del conjunto $D(a, b)$, es decir, que $|a| = \text{mcd}(a, b)$. Esto muestra que la condición del enunciado es suficiente.

Veamos que es necesaria. Supongamos que $\text{mcd}(a, b) = |a|$. Si $b = 0$, entonces a divide a b independientemente de nuestra hipótesis, así que supongamos que $b \neq 0$. En ese caso, $\text{mcd}(a, b)$ es el elemento máximo del conjunto $D(a, b)$, y esto significa que, que particular, $|a|$ divide a b . Por supuesto, esto implica que a divide a b .

(iii) Como $a \mid 0$, esto es consecuencia de (ii).

(iv) Si $a = b = 0$, lo que afirma el enunciado es evidente. Si en cambio alguno de a o b es no nulo, entonces $D(a, b) = D(-a, b) = D(a, -b) = D(-a, -b)$ y, por lo tanto,

estos cuatro conjuntos tienen el mismo elemento máximo. \square

6.4.4. La siguiente propiedad es fundamental:

Proposición. Si a , b y c son tres enteros, entonces

$$\text{mcd}(a - cb, b) = \text{mcd}(a, b)$$

y

$$\text{mcd}(a, b - ca) = \text{mcd}(a, b).$$

Demostración. En vista de la Proposición 6.4.3(i) es suficiente que mostremos la primera de las igualdades del enunciado. Sean a , b y c tres enteros. Si b es cero, entonces esa igualdad evidente. Supongamos entonces que $b \neq 0$. Afirmamos que

$$D(a, b) = D(a - cb, b). \quad (7)$$

En efecto, si $d \in D(a, b)$, entonces d es un entero positivo que divide a a y a b y, por lo tanto, divide a $a - bc$ y a b : esto significa que $d \in D(a - cb, b)$. Recíprocamente, si $d \in D(a - cb, b)$, entonces d es un entero positivo que divide a $a - cb$ y a b , y por lo tanto divide a $a = (a - cb) + cb$ y a b , así que pertenece a $D(a, b)$.

De la igualdad (7) se deduce que

$$\text{mcd}(a, b) = \max D(a, b) = \max D(a - cb, b) = \text{mcd}(a - cb, b)$$

y esto prueba la proposición. \square

6.4.5. Una de las razones por las que la Proposición 6.4.4 es importante es que está en la base de un algoritmo para calcular el máximo común divisor de dos enteros.

En vista de la Proposición 6.4.3(iv), es suficiente que veamos cómo hacer esto cuando los dos enteros son no negativos. Supongamos entonces que a y b son dos enteros no negativos y que, por ejemplo, $a \geq b$. Si $b = 0$, entonces sabemos que $\text{mcd}(a, b) = a$ y no es necesario hacer más nada. Si en cambio $b > 0$, entonces podemos dividir a a por b . Sean q y r el cociente y el resto, respectivamente. Como $a = qb + r$, la Proposición 6.4.4 nos dice que

$$\text{mcd}(a, b) = \text{mcd}(a - qb, b) = \text{mcd}(r, b).$$

Notemos que r y b son dos enteros no negativos y que $a + b > r + b$, ya que $a \geq b > r$. De esta forma reducimos el cálculo del máximo común divisor de dos números no negativos al del máximo común divisor de otros dos cuya suma es menor que la de los originales. Podemos repetir este procedimiento y como en cada paso la suma de los dos números decrece el proceso tiene que terminar.

Veamos un ejemplo. Para calcular $\text{mcd}(385, 150)$, observamos que el cociente y el resto de la división de 385 por 150 son 2 y 85, respectivamente, de manera que $385 = 2 \cdot 150 + 85$ y entonces

$$\text{mcd}(385, 150) = \text{mcd}(385 - 2 \cdot 150, 150) = \text{mcd}(85, 150).$$

Tenemos que calcular ahora $\text{mcd}(85, 150)$. Dividiendo ahora a 150 por 85 vemos que $150 = 1 \cdot 85 + 65$, así que

$$\text{mcd}(85, 150) = \text{mcd}(85, 150 - 1 \cdot 85) = \text{mcd}(85, 65).$$

Otra vez, dividiendo vemos que $85 = 1 \cdot 65 + 20$ y, por lo tanto, que

$$\text{mcd}(85, 65) = \text{mcd}(85 - 1 \cdot 65, 65) = \text{mcd}(20, 65).$$

Finalmente, como $65 = 3 \cdot 20 + 5$,

$$\text{mcd}(20, 65) = \text{mcd}(20, 65 - 3 \cdot 20) = \text{mcd}(20, 5)$$

y, como 5 divide a 20, este último máximo común divisor es 5. Concluimos así que

$$\text{mcd}(385, 150) = 5.$$

Este algoritmo funciona en todos los casos, como veremos más abajo. Se lo conoce como el *algoritmo de Euclides*, porque Euclides lo describe en el Libro 7 de sus *Elementos*, publicados aproximadamente 300 años a.C. —aunque es probable que el algoritmo haya sido conocido desde mucho tiempo antes. En la Figura 6.2 reproducimos el pasaje relevante.

6.4.6. Describamos precisamente el algoritmo de Euclides en una forma conveniente para probar que funciona. Empezamos como arriba con dos números enteros no negativos a y b , suponemos que $a \geq b$ y definimos una sucesión

$$r_0, r_1, r_2, r_3, \dots$$

de enteros no negativos de la siguiente manera. Ponemos $r_0 = a$, $r_1 = b$, y para cada $i \geq 2$ ponemos

$$r_i = \begin{cases} \text{el resto de dividir } r_{i-2} \text{ por } r_{i-1}, & \text{si } r_{i-1} \neq 0; \\ 0, & \text{en caso contrario.} \end{cases} \quad (8)$$

El algoritmo de Euclides para determinar el máximo común divisor de a y de b consiste en calcular las componentes de esta sucesión y quedarse con la última no nula. Por ejemplo, si $a = 385$ y $b = 150$, entonces la sucesión $(r_i)_{i \geq 0}$ es

$$385, 150, 85, 65, 20, 5, 0, 0, 0, 0, 0, 0, \dots$$

y, por lo tanto, $\text{mcd}(385, 150) = 5$.

Δύο ἀριθμῶν δοθέντων μὴ πρώτων πρὸς ἀλλήλους τὸ μέγιστον αὐτῶν κοινὸν μέτρον εὑρεῖν. Ἐστῶσαν οἱ δοθέντες δύο ἀριθμοὶ μὴ πρώτοι πρὸς ἀλλήλους οἱ $AB, ΓΔ$. δεῖ δὴ τῶν $AB, ΓΔ$ τὸ μέγιστον κοινὸν μέτρον εὑρεῖν. Εἰ μὲν οὖν ὁ $ΓΔ$ τὸν AB μετρεῖ, μετρεῖ δὲ καὶ ἑαυτὸν, ὁ $ΓΔ$ ἄρα τῶν $ΓΔ, AB$ κοινὸν μέτρον ἐστίν. καὶ φανερόν, ὅτι καὶ μέγιστον: οὐδεὶς γὰρ μείζων τοῦ $ΓΔ$ τὸν $ΓΔ$ μετρήσει. Εἰ δὲ οὐ μετρεῖ ὁ $ΓΔ$ τὸν AB , τῶν $AB, ΓΔ$ ἀνθυφαρουμενοῦ ἀεὶ τοῦ ἐλάσσονος ἀπὸ τοῦ μείζονος λειψθήσεται τις ἀριθμὸς, ὃς μετρήσει τὸν πρὸ ἑαυτοῦ. μονὰς μὲν γὰρ οὐ λειψθήσεται: εἰ δὲ μὴ, ἔσσονται οἱ $AB, ΓΔ$ πρώτοι πρὸς ἀλλήλους: ὅπερ οὐχ ὑπόκειται. λειψθήσεται τις ἄρα ἀριθμὸς, ὃς μετρήσει τὸν πρὸ ἑαυτοῦ. καὶ ὁ μὲν $ΓΔ$ τὸν BE μετρῶν λειπέτω ἑαυτοῦ ἐλάσσονα τὸν EA , ὁ δὲ EA τὸν $ΔZ$ μετρῶν λειπέτω ἑαυτοῦ ἐλάσσονα τὸν $ZΓ$, ὁ δὲ $ΓZ$ τὸν AE μετρεῖτω. ἐπεὶ οὖν ὁ $ΓZ$ τὸν AE μετρεῖ, ὁ δὲ AE τὸν $ΔZ$ μετρεῖ, καὶ ὁ $ΓZ$ ἄρα τὸν $ΔZ$ μετρήσει: μετρεῖ δὲ καὶ ἑαυτὸν: καὶ ὅλον ἄρα τὸν $ΓΔ$ μετρήσει. ὁ δὲ $ΓΔ$ τὸν BE μετρεῖ: καὶ ὁ $ΓZ$ ἄρα τὸν BE μετρεῖ: μετρεῖ δὲ καὶ τὸν EA : καὶ ὅλον ἄρα τὸν BA μετρήσει: μετρεῖ δὲ καὶ τὸν $ΓΔ$: ὁ $ΓZ$ ἄρα τοὺς $AB, ΓΔ$ μετρεῖ. ὁ $ΓZ$ ἄρα τῶν $AB, ΓΔ$ κοινὸν μέτρον ἐστίν. λέγω δὴ, ὅτι καὶ μέγιστον. εἰ γὰρ μὴ ἐστὶν ὁ $ΓZ$ τῶν $AB, ΓΔ$ μέγιστον κοινὸν μέτρον, μετρήσει τις τοὺς $AB, ΓΔ$ ἀριθμοὺς ἀριθμὸς μείζων ὢν τοῦ $ΓZ$. μετρεῖτω, καὶ ἔστω ὁ H . καὶ ἐπεὶ ὁ H τὸν $ΓΔ$ μετρεῖ, ὁ δὲ $ΓΔ$ τὸν BE μετρεῖ, καὶ ὁ H ἄρα τὸν BE μετρεῖ: μετρεῖ δὲ καὶ ὅλον τὸν BA : καὶ λοιπὸν ἄρα τὸν AE μετρήσει. ὁ δὲ AE τὸν $ΔZ$ μετρεῖ: καὶ ὁ H ἄρα τὸν $ΔZ$ μετρήσει: μετρεῖ δὲ καὶ ὅλον τὸν $ΔΓ$: καὶ λοιπὸν ἄρα τὸν $ΓZ$ μετρήσει ὁ μείζων τὸν ἐλάσσονα: ὅπερ ἐστὶν ἀδύνατον: οὐκ ἄρα τοὺς $AB, ΓΔ$ ἀριθμοὺς ἀριθμὸς τις μετρήσει μείζων ὢν τοῦ $ΓZ$: ὁ $ΓZ$ ἄρα τῶν $AB, ΓΔ$ μέγιστόν ἐστι κοινὸν μέτρον: [ὅπερ ἔδει δεῖξαι].

Figura 6.2. La proposición 2 del Libro 7 de los Elementos de Euclides, en el que enuncia el problema de encontrar el máximo común divisor de dos números y lo resuelve, presentando el algoritmo que lleva su nombre. Empieza con «Dados dos números no primos uno al otro, encontrar su medida más grande. Sean AB y CD los dos números dados no primos uno al otro. Si CD mide a AB , y también se mide a sí mismo, entonces CD es una medida común de AB, CD . Y es manifiesto que es la más grande. Pero si CD no mide a AB , entonces, el menos de los números AB, CD se puede restar varias veces del más grande, y algún número sera el resto, que medirá al que está antes de él. Etc».

6.4.7. Proposición. Sean a y b dos enteros no negativos tales que $a \geq b$ y sea $(r_i)_{i \geq 0}$ la sucesión que acabamos de describir.

- (i) Existe $N \in \mathbb{N}_0$ tal que $r_i \neq 0$ para todo $i \leq N$ y $r_i = 0$ para todo $i > N$.
- (ii) Para todo $i \in \mathbb{N}$ tal que $i \leq N + 1$ se tiene que $\text{mcd}(a, b) = \text{mcd}(r_{i-1}, r_i)$.
- (iii) Es $\text{mcd}(a, b) = r_N$.

Este resultado nos dice que el algoritmo de Euclides, cuando empezamos con dos enteros no negativos a y b , se detiene después de un número finito de pasos —el número N — y el último número que produce es precisamente el máximo común divisor de a y b . En otras palabras, nos dice que el algoritmo funciona, como queríamos.

Demostración. Observemos que

$$r_i \geq 0 \text{ para todo } i \in \mathbb{N}. \quad (9)$$

En efecto, se tiene que $r_1 = b \geq 0$ y para todo $i \geq 2$ se tiene que $r_i \geq 0$ ya que r_i es, de acuerdo a la definición (8), o bien el resto de una división, que es siempre un número no negativo, o bien 0.

Por otro lado, se tiene que

$$\text{para todo } i \in \mathbb{N} \text{ o bien } r_i = 0 \text{ o bien } r_i > r_{i+1}. \quad (10)$$

Para verlo, basta notar que si $i \in \mathbb{N}$ y $r_i \neq 0$, entonces r_{i+1} es el resto de dividir a un número por r_i , que es necesariamente menor que r_i .

Supongamos por un momento que $r_i \neq 0$ para todo $i \in \mathbb{N}$. De acuerdo a (9), el conjunto $R = \{r_i : i \in \mathbb{N}\}$ está contenido en \mathbb{N}_0 , así que tiene un menor elemento: esto es, existe $i \in \mathbb{N}$ tal que $r_i \leq r_j$ para todo $j \in \mathbb{N}$. Esto es absurdo, ya que como $r_i \neq 0$ por nuestra hipótesis, de (10) sabemos que $r_i > r_{i+1}$.

Esta contradicción implica que tiene que existir $i \in \mathbb{N}$ tal que $r_i = 0$ y, por lo tanto, que el conjunto $S = \{i \in \mathbb{N} : r_{i+1} = 0\}$ no es vacío. Como está contenido en \mathbb{N} , sabemos que él también tiene un menor elemento. Llamémoslo N . Se tiene, claro, que $r_i \neq 0$ si $i \leq N$ y $r_{N+1} = 0$. Más aún, en vista de la forma en que está definida la sucesión $(r_i)_{i \geq 0}$, es claro que como $r_{N+1} = 0$ se tiene que $r_i = 0$ para todo entero $i > N$. Esto prueba que vale la parte (i) de la proposición.

Para cada $i \in \mathbb{N}$ sea $P(i)$ la afirmación

$$i > N + 1 \text{ o } \text{mcd}(a, b) = \text{mcd}(r_{i-1}, r_i)$$

y mostremos que $P(i)$ vale para todo $i \in \mathbb{N}$: esto probará la parte (ii) de la proposición.

Que $P(1)$ vale es evidente, ya que $r_0 = a$ y $r_1 = b$. Supongamos que $j \in \mathbb{N}$ y que la afirmación $P(j)$ vale, es decir, que $j > N + 1$ o

$$\text{mcd}(a, b) = \text{mcd}(r_{j-1}, r_j). \quad (11)$$

```

mcd :: Integer -> Integer -> Integer
mcd 0 0          = 0
mcd a b
  | a < 0 || b < 0 = mcd (abs a) (abs b)
  | a < b          = mcd b a
  | otherwise      = paso a b

paso :: Integer -> Integer -> Integer
paso x y
  | y == 0        = x
  | otherwise      = paso y (rem x y)

```

Figura 6.3. Una implementación en HASKELL del algoritmo de la Euclides, tal cual como lo presentamos en 6.4.6.

Si $j > N + 1$, entonces por supuesto es $j + 1 > N + 1$ y, por lo tanto, la afirmación $P(j + 1)$ vale. Consideremos el caso en que $j \leq N$, de manera que vale la igualdad (11). La forma en que elegimos el número N implica que $r_j \neq 0$, así que la definición de la sucesión $(r_i)_{i \geq 0}$ nos dice que r_{j+1} es el resto de dividir a r_{j-1} por r_j . Si q es el cociente de esa división, tenemos entonces que $r_{j+1} = r_{j-1} - qr_j$ y, por lo tanto,

$$\text{mcd}(r_{j-1}, r_j) = \text{mcd}(r_{j-1} - qr_j, r_j) = \text{mcd}(r_{j+1}, r_j) = \text{mcd}(r_j, r_{j+1}).$$

Junto con (11) esto nos dice que $\text{mcd}(a, b) = \text{mcd}(r_j, r_{j+1})$ y, en definitiva, que $P(j + 1)$ también vale en este caso. La inducción queda así completa.

Finalmente, tomando $i = N + 1$ en la igualdad de la parte (ii), vemos que

$$\text{mcd}(a, b) = \text{mcd}(r_N, r_{N+1}) = \text{mcd}(r_N, 0) = r_N,$$

como se afirma en la parte (iii). □

6.4.8. Proposición. Sean a y b dos enteros no simultáneamente nulos. El conjunto

$$S(a, b) = \{xa + yb : x, y \in \mathbb{Z}, xa + yb > 0\}$$

es un subconjunto no vacío de \mathbb{N} y su elemento mínimo es $\text{mcd}(a, b)$.

Demostración. Alguno de los cuatro números $a, -a, b$ o $-b$ es positivo y, por lo tanto, pertenece a $S(a, b)$: esto muestra que este conjunto no es vacío. Como está contenido en \mathbb{N} , podemos considerar su elemento mínimo $d = \min S$. Como $d \in S(a, b)$, es claro que $d \geq 1$ y que existen $u, v \in \mathbb{Z}$ tales que $d = ua + vb$.

Sean q y r el cociente y el resto de la división de a por d , de manera que $a = qd + r$ y $0 \leq r < d$. Si $r > 0$, entonces como

$$(1 - qu)a - qvb = r$$

y $1 - qu$ y $-qv$ son enteros, se tiene que $r \in S(a, b)$: esto es imposible ya que $r < d$. Vemos así que tiene que ser $r = 0$ y, por lo tanto, d divide a a . Un argumento similar muestra que d divide a b y, por lo tanto, d es un divisor común de a y b .

Sea ahora e un elemento de $D(a, b)$, de manera que e divide a a y a b . Como $d = ua + vb$, es claro que e divide también a d y, como $d \neq 0$, la Proposición 6.1.4 nos dice que $e \leq d$. Esto muestra que d es el mayor elemento de $D(a, b)$ y, por lo tanto, que $d = \text{mcd}(a, b)$, como afirma la proposición. \square

6.4.9. Una consecuencia inmediata e importante de esta proposición es el siguiente corolario:

Corolario. Si a y b son dos enteros y $d = \text{mcd}(a, b)$, entonces existen enteros $x, y \in \mathbb{Z}$ tales que $d = xa + yb$.

Llamamos a esta igualdad la *identidad de Bézout*, por Étienne Bézout (1730–783, Francia), que probó un análogo de este resultado para polinomios.

Demostración. Si $a = b = 0$, entonces $d = 0$ y eligiendo $x = y = 0$ es evidente que vale la igualdad del enunciado. Si en cambio a y b no son simultáneamente nulos, la Proposición 6.4.8 nos dice que el número d pertenece al conjunto $S(a, b)$ allí descrito y, por lo tanto, existen enteros x e y tales que $d = xa + yb$. \square

6.4.10. Para muchas aplicaciones, necesitamos no solamente poder calcular el máximo común divisor de dos enteros sino que también queremos encontrar números x e y para los que valga la identidad de Bézout. Veamos cómo podemos hacer esto.

Supongamos como en 6.4.6 que tenemos dos enteros no negativos a y b tales que $a \geq b$, sea $d = \text{mcd}(a, b)$ y definamos la sucesión $(r_i)_{i \geq 0}$ como allí, esto es, poniendo $r_0 = a, r_1 = b$ y para cada $i \geq 2$

$$r_i = \begin{cases} \text{el resto de dividir } r_{i-2} \text{ por } r_{i-1}, & \text{si } r_{i-1} \neq 0; \\ 0, & \text{en caso contrario.} \end{cases}$$

Sea N el número que nos provee la Proposición 6.4.7, de manera que $r_i \neq 0$ si $i \leq N$, $r_i = 0$ si $i > N$ y $r_N = d$. Estamos buscando enteros x e y tales que $xa + yb = r_N$. Busquemos, más generalmente, pares de enteros $x_0, y_0, x_1, y_1, \dots, x_N, y_N$ tales que para cada $i \in \{0, \dots, N\}$ se tenga $x_i a + y_i b = r_i$.

Observemos que cuando $i = 0$ o $i = 1$ esto es fácil: basta poner $x_0 = 1, y_0 = 0, x_1 = 0, y_1 = 1$, ya que $r_0 = a$ y $r_1 = b$. Ahora bien, supongamos que $2 \leq i \leq N$ y

que ya encontramos enteros $x_{i-1}, y_{i-1}, x_i, y_i$ de manera tal que $x_{i-1}a + y_{i-1}b = r_{i-1}$ y $x_i a + y_i b = r_i$. Si llamamos q_{i+1} al cociente de la división de r_{i-1} por r_i , de manera que $r_{i-1} = q_{i+1}r_i + r_{i+1}$, tenemos entonces que

$$\begin{aligned} r_{i+1} &= r_{i-1} - q_{i+1}r_i = (x_{i-1}a + y_{i-1}b) - q_{i+1}(x_i a + y_i b) \\ &= (x_{i-1} - q_{i+1}x_i)a + (y_{i-1} - q_{i+1}y_i)b \end{aligned}$$

y, por lo tanto, basta que pongamos

$$x_{i+1} = x_{i-1} - q_{i+1}x_i \tag{12}$$

e

$$y_{i+1} = y_{i-1} - q_{i+1}y_i \tag{13}$$

para que se tenga que $x_{i+1}a + y_{i+1}b = r_{i+1}$.

De esta manera vamos determinando enteros x_i e y_i para cada i de 0 hasta N , hasta finalmente encontrar x_N e y_N : estos satisfacen la condición de que $x_N a + y_N b = r_N = d$, que es la identidad de Bézout.

Veamos un ejemplo. Determinemos los coeficientes de la identidad de Bézout para $a = 385$ y $b = 150$. Como en 6.4.6, calculamos las componentes de la sucesión $(r_i)_{i \geq 0}$ pero en cada paso, correspondiente a un índice $i \geq 2$, no solamente calculamos el resto r_i de dividir r_{i-2} por r_{i-1} sino también el cociente q_i . La primera componente nula de la sucesión de restos es r_6 , así que sabemos que $r_5 = \text{mcd}(a, b)$.

i	0	1	2	3	4	5	6
r_i	385	150	85	65	20	5	0
q_i			2	1	1	3	
x_i	1	0	1	-1	2	-7	
y_i	0	1	-2	3	-5	18	

Ahora calculamos en orden los números x_i e y_i : empezamos poniendo $x_0 = 1, y_0 = 0, x_1 = 0$ e $y_1 = 1$, y a todos los otros los determinamos usando las fórmulas (12) y (13). Encontramos de esta forma que

$$(-7) \cdot 385 + 18 \cdot 150 = 5,$$

que es la identidad de Bézout para 385 y 150, como queríamos.

Este procedimiento es conocido como el *algoritmo de Euclides extendido* y es la forma en que se determinan los coeficientes de la identidad de Bézout en la práctica. Todos los programas de álgebra computacional tienen implementaciones de este algoritmo. En la Figura 6.4 en la página siguiente damos una posible implementación en HASKELL.

```

emcd :: Integer -> Integer -> (Integer, Integer, Integer)
emcd 0 0      = (0, 0, 0)
emcd a b
  | a < 0     = let (d, x, y) = emcd (-a) b in (d, -x, y)
  | b < 0     = let (d, x, y) = emcd a (-b) in (d, x, -y)
  | a < b     = let (d, x, y) = emcd b a    in (d, y, x)
  | otherwise = paso a b 1 0 0 1

paso :: Integer -> Integer -> Integer -> Integer ->
       Integer -> Integer -> (Integer, Integer, Integer)
paso a b x0 y0 x1 y1
  | b == 0     = (a, x0, y0)
  | otherwise  = paso b r x1 y1 (x0 - q * x1) (y0 - q * y1)
  where r = rem a b
        q = quot a b

```

Figura 6.4. Un implementación en HASKELL del algoritmo de Euclides extendido.

6.4.11. Probemos que este algoritmo funciona en todos los casos:

Proposición. Sean a y b dos enteros no negativos y supongamos que $a \geq b$. Sea $(r_i)_{i \geq 0}$ la sucesión construida en 6.4.6 a partir de a y b , y sea $N \in \mathbb{N}_0$ como en la Proposición 6.4.7, de manera que $r_i \neq 0$ si $i \leq N$, $r_i = 0$ para todo $i > N$ y $r_N = \text{mcd}(a, b)$. Sean x_0, x_1, \dots, x_N y y_0, y_1, \dots, y_N las secuencias de enteros tales que

$$x_0 = 1, \quad y_0 = 0, \quad (14)$$

$$x_1 = 0, \quad y_1 = 1, \quad (15)$$

y, para cada $i \in \{2, \dots, N\}$,

$$x_i = x_{i-2} - q_i x_{i-1}, \quad y_i = y_{i-2} - q_i y_{i-1} \quad (16)$$

con q_i el resto de dividir a r_{i-2} por r_{i-1} . Se tiene entonces que

$$r_i = x_i a + y_i b \quad (17)$$

para cada $i \in \{0, \dots, N\}$ y, en particular,

$$\text{mcd}(a, b) = x_N a + y_N b.$$

Demostración. Es suficiente que mostremos que para cada $i \in \{0, \dots, N\}$ vale la igualdad (17), ya que cuando i es N ésta nos dice que $x_N a + y_N b = r_N = \text{mcd}(a, b)$.

Sea $P(i)$, para cada $i \in \mathbb{N}_0$, la afirmación «o bien $i > N$ o bien $r_i = x_i a + y_i b$ » y mostremos que $P(i)$ vale para todo $i \in \mathbb{N}_0$ haciendo inducción. Las afirmaciones $P(0)$ y $P(1)$ valen: esto es consecuencia inmediata de las igualdades (14) y (15). En efecto, $x_0 a + y_0 b = a = r_0$ y $x_1 a + y_1 b = b = r_1$.

Veamos ahora el paso inductivo. Sea j un entero tal que $j \geq 2$ y supongamos que las afirmaciones $P(j-1)$ y $P(j-2)$ valen. Si $j > N$, entonces claramente la afirmación $P(j)$ vale. Consideremos el caso en que $j \leq N$. Que $P(j-1)$ y $P(j-2)$ valgan, entonces, nos dice que $r_{j-1} = x_{j-1} a + y_{j-1} b$ y que $r_{j-2} = x_{j-2} a + y_{j-2} b$. Si q_j es el resto de dividir a r_{j-2} por r_{j-1} , tenemos que

$$\begin{aligned} r_j &= r_{j-2} - q_j r_{j-1} \\ &= (x_{j-2} a + y_{j-2} b) - q_j (x_{j-1} a + y_{j-1} b) \\ &= (x_{j-2} - q_j x_{j-1}) a + (y_{j-2} - q_j y_{j-1}) b \end{aligned}$$

y, de acuerdo a las ecuaciones (16), esto es

$$= x_j a + y_j b.$$

Vemos así que $P(j)$ vale también en este caso y esto completa la inducción. □

§6.5. Algunas aplicaciones de la identidad de Bézout

6.5.1. Vamos a usar la identidad de Bézout para varias cosas en todo lo que sigue. Una primera aplicación es la siguiente caracterización del máximo común divisor de dos enteros que es extremadamente útil:

Proposición. Sean a y b dos enteros. El máximo común divisor de a y b es el único elemento d de \mathbb{N}_0 que tiene las siguientes dos propiedades:

- d es un divisor común de a y b , y
- todo elemento de \mathbb{N}_0 que es un divisor común de a y b también divide a d .

Demostración. Sea $d = \text{mcd}(a, b)$ y sean x e y enteros tales que $d = xa + yb$. Si $e \in \mathbb{N}$ es un divisor común de a y b , entonces e también divide a $d = xa + yb$. Como d es un divisor común de a y b , vemos así que d tiene las dos propiedades del enunciado.

Supongamos ahora que tenemos otro entero no negativo positivo d' que tiene esas dos propiedades. Como d' es un divisor común de a y b y d tienen la segunda propiedad del enunciado, tenemos que $d \mid d'$. Por otro lado, como d es un divisor común de a y de b y d' tiene la segunda propiedad del enunciado, tenemos que $d' \mid d$. Podemos concluir entonces que $d = d'$, ya que tanto d como d' son enteros no negativos. Esto prueba la proposición. \square

6.5.2. Corolario. Si a, a', b y b' son enteros tales que $a \mid a'$ y $b \mid b'$, entonces

$$\gcd(a, b) \mid \gcd(a', b').$$

Demostración. Sean a, a', b y b' enteros y supongamos que $a \mid a'$ y que $b \mid b'$. Sea además $d = \gcd(a, b)$. Como d divide a a y a divide a a' , vemos que d divide a a' . De manera similar, d divide a b' : como d es entonces un divisor común de a' y b' , la Proposición 6.5.1 nos dice que d divide a $\gcd(a', b')$. \square

6.5.3. Proposición. Si a, b y c son enteros, entonces

$$\gcd(ac, bc) = \gcd(a, b) \cdot c.$$

Demostración. Sean $d = \gcd(a, b)$ y $e = \gcd(ac, bc)$. De acuerdo a la identidad de Bézout 6.4.9, existen enteros x e y tales que $d = xa + yb$. Como $dc = xac + ybc$ y e divide a ac y a bc , vemos entonces que e divide a dc .

Por otro lado, como d divide a a y a b , es claro que dc divide a bc y a bd , así que la Proposición 6.5.1 nos dice que dc divide a e . Como d y e son enteros no negativos, podemos concluir de todo esto que $d = e$, que es lo que afirma la proposición. \square

6.5.4. Usando la Proposición 6.5.3 podemos dar una nueva caracterización del máximo común divisor de dos números que es muchas veces útil:

Corolario. Sean a y b dos enteros y sea $d = \gcd(a, b)$.

- (i) Los enteros a' y b' tales que $a = da'$ y $b = db'$ son coprimos.
- (ii) Si e es un entero no negativo tal que existen dos enteros coprimos u y v para los que se tiene que $a = eu$ y $a = ev$, entonces $e = d$.

Demostración. (i) En la situación del enunciado, tenemos que

$$d = \gcd(a, b) = \gcd(da', db') = d \cdot \gcd(a', b'),$$

así que necesariamente $\gcd(a', b') = 1$.

(ii) Si $e \in \mathbb{N}_0$ y $u, v \in \mathbb{Z}$ son tales que $a = eu, b = ev$ y $\text{mcd}(u, v) = 1$, entonces

$$\text{mcd}(a, b) = \text{mcd}(eu, ev) = e \cdot \text{mcd}(u, v) = e$$

y esto es lo que queremos. □

6.5.5. Proposición. Sean a, b y c tres enteros y supongamos que a y b son coprimos.

- (i) Si $a \mid bc$, entonces $a \mid c$.
- (ii) Si $a \mid c$ y $b \mid c$, entonces $ab \mid c$.
- (iii) Se tiene que $\text{mcd}(a, bc) = \text{mcd}(a, c)$.
- (iv) Se tiene que $\text{mcd}(ab, c) = \text{mcd}(a, c) \cdot \text{mcd}(b, c)$.

Demostración. Como a y b son coprimos, existen enteros x e y tales que $xa + yb = 1$.

(i) Supongamos primero que a divide a bc . Como $xac + ybc = c$ y a divide a los dos sumandos del lado izquierdo, también divide al lado derecho.

(ii) Supongamos ahora que $a \mid c$ y que $b \mid c$. De eso se sigue que ab divide a bc y a ac , así que como $xac + ybc = c$, vemos que ab divide a c .

(iii) Sean $d = \text{mcd}(a, c)$ y $e = \text{mcd}(a, bc)$. Como d divide a a y a c , divide a a y a bc : de acuerdo a la Proposición 6.5.1, tenemos entonces que d divide a e . Por otro lado, como e divide a a y a bc , vemos que e divide a $c = (xa + yb)c = xac + ybc$. Esto nos dice que e es un divisor común positivo de a y c , así que e divide a d . Como d y e se dividen mutuamente y son no negativos, concluimos de esta forma que $d = e$. Esto prueba la primera de las dos igualdades del enunciado.

(iv) Pongamos $d = \text{mcd}(a, c)$, $e = \text{mcd}(b, c)$ y $f = \text{mcd}(ab, c)$. Como $d \mid a$ y $e \mid b$, se tiene que $de \mid ab$. Por otro lado, como $d \mid a$ y $e \mid c$, tenemos que $de \mid ac$, y como $d \mid c$ y $e \mid b$ que $de \mid bc$: usando esto y la igualdad $c = xac + ybc$, podemos concluir que $de \mid c$. Vemos así que de es un divisor común de ab y de c , así que $de \mid f$.

Por otro lado, existen enteros u, v, r y s tales que $d = ua + vc$ y $e = rb + sc$, así que

$$de = (ua + vc)(rb + sc) = urab + (usa + vrb + vsc)c.$$

Como f divide a ab y a c , vemos entonces que también divide a de . Como f y de son enteros no negativos que se dividen mutuamente, tenemos en definitiva que $de = f$, que es lo que queríamos probar. □

6.5.6. Corolario. Sea $r \in \mathbb{N}$. Si a_1, \dots, a_r son enteros coprimos dos a dos y $b \in \mathbb{Z}$, entonces

$$\text{mcd}(a_1 \cdots a_r, b) = \text{mcd}(a_1, b) \cdots \text{mcd}(a_r, b).$$

Demostración. Procedamos por inducción con respecto a r , notando que cuando r es 1 la afirmación es evidente. Sea entonces $s \in \mathbb{N}$, supongamos que la afirmación del enunciado vale cuando r es s y mostremos que entonces vale también cuando r es $s + 1$.

Sean entonces a_1, \dots, a_{s+1} enteros coprimos dos a dos y sea b otro entero. Como los s enteros a_1, \dots, a_s son coprimos dos a dos, la hipótesis inductiva nos dice que

$$\text{mcd}(a_1 \cdots a_s, a_{s+1}) = \text{mcd}(a_1, a_{s+1}) \cdots \text{mcd}(a_s, a_{s+1}) = 1,$$

así que los números $a_1 \cdots a_s$ y a_{s+1} son coprimos. La Proposición 6.5.5(iv) nos dice entonces que

$$\text{mcd}(a_1 \cdots a_{s+1}, b) = \text{mcd}(a_1 \cdots a_s \cdot a_{s+1}, b) = \text{mcd}(a_1 \cdots a_s, b) \cdot \text{mcd}(a_{s+1}, b)$$

y usando otra vez la hipótesis inductiva vemos que esto es igual a

$$\text{mcd}(a_1, b) \cdots \text{mcd}(a_s, b) \cdot \text{mcd}(a_{s+1}, b).$$

Esto completa la inducción. □

6.5.7. Podemos generalizar la parte (ii) de la Proposición 6.5.5 al caso en que tenemos varios divisores:

Corolario. Sea $r \in \mathbb{N}$. Si a_1, \dots, a_r son enteros coprimos dos a dos y cada uno de ellos divide a un entero b , entonces el producto $a_1 \cdots a_r$ también divide a b .

Demostración. De acuerdo al Corolario 6.5.6, tenemos que

$$\text{mcd}(a_1 \cdots a_r, b) = \text{mcd}(a_1, b) \cdots \text{mcd}(a_r, b)$$

y, de acuerdo a la Proposición 6.4.3(ii) y la hipótesis de que cada uno de los enteros a_1, \dots, a_r divide a b , tenemos que $\text{mcd}(a_i, b) = |a_i|$ para cada $i \in \{1, \dots, r\}$ y, por lo tanto, tenemos que

$$\text{mcd}(a_1 \cdots a_r, b) = |a_1 \cdots a_r|.$$

Esa misma Proposición 6.4.3(ii) nos dice entonces que $a_1 \cdots a_r$ divide a b . □

6.5.8. Proposición. Sean a y b dos enteros y sea $k, l \in \mathbb{N}$. Si $\text{mcd}(a, b) = 1$, entonces también $\text{mcd}(a^k, b^l) = 1$.

Demostración. Supongamos que $\text{mcd}(a, b) = 1$, de manera que existen enteros x e y tales que $1 = xa + yb$. Se sigue de esto que

$$1 = 1^{k+l} = (xa + yb)^{k+l} = \sum_{i=0}^{k+l} \binom{k+l}{i} x^{k+l-i} y^i a^{k+l-i} b^i$$

$$= \left(\sum_{i=0}^l \binom{k+l}{i} x^{k+l-i} y^i a^{l-i} b^i \right) a^k + \left(\sum_{i=l+1}^{k+l} \binom{k+l}{i} x^{k+l-i} y^i a^{k+l-i} b^{i-l} \right) b^l$$

y las dos expresiones encerradas entre paréntesis son enteros. Sea $d = \text{mcd}(a^k, b^l)$. Como d divide a a^k y a b^l , esa igualdad implica que d divide a 1. Por supuesto, esto nos dice que $d = 1$, como queremos. \square

6.5.9. Corolario. Si a y b son enteros y $k \in \mathbb{N}$, entonces

$$\text{mcd}(a^k, b^k) = \text{mcd}(a, b)^k.$$

Demostración. Sea $d = \text{mcd}(a, b)$. Como d divide a a y a b , existen enteros u y v tales que $a = du$ y $b = dv$. De acuerdo a la Proposición 6.5.3, tenemos que

$$d \cdot \text{mcd}(u, v) = \text{mcd}(du, dv) = \text{mcd}(a, b) = d,$$

de manera que $\text{mcd}(u, v) = 1$. La Proposición 6.5.8 nos dice entonces que también $\text{mcd}(u^k, v^k) = 1$ y usando esto podemos concluir que

$$\text{mcd}(a^k, b^k) = \text{mcd}(d^k u^k, d^k v^k) = d^k \cdot \text{mcd}(u^k, v^k) = d^k,$$

que es lo que afirma el corolario. \square

§6.6. Ejercicios

El máximo común divisor de un conjunto finito de números

6.6.1. Sean $k \in \mathbb{N}$ y $a_1, \dots, a_k \in \mathbb{Z}$.

(a) Si los enteros a_1, \dots, a_k no todos simultáneamente nulos, el conjunto $D(a_1, \dots, a_k)$ de los enteros positivos que dividen a cada uno de ellos es finito y no vacío. Tiene sentido entonces considerar su elemento máximo, al que llamamos el **máximo común divisor** de los enteros a_1, \dots, a_k y escribimos $\text{mcd}(a_1, \dots, a_k)$. Si en cambio todos los enteros a_1, \dots, a_k son nulos, definimos $\text{mcd}(0, \dots, 0) = 0$.

(b) Si $k \geq 3$, entonces se tiene que

$$\text{mcd}(a_1, \dots, a_k) = \text{mcd}(\text{mcd}(a_1, a_2), a_3, \dots, a_k). \quad (18)$$

(c) Existen enteros x_1, \dots, x_k tales que

$$x_1 a_1 + \dots + x_k a_k = \text{mcd}(a_1, \dots, a_k). \quad (19)$$

(d) El entero $\text{mcd}(a_1, \dots, a_k)$ es el único que tiene las siguientes dos propiedades:

- es un divisor común positivo de los números a_1, \dots, a_k , y
- divide a cada divisor común de los números a_1, \dots, a_k .

(e) Describa un algoritmo basado en la igualdad (18) y el algoritmo de Euclides para encontrar tanto a $\text{mcd}(a_1, \dots, a_k)$ como a enteros x_1, \dots, x_k para los que vale la igualdad (19).

El mínimo común múltiplo de dos enteros

6.6.2. Sean a y b dos enteros.

(a) Sea $M(a, b)$ el conjunto de los múltiplos positivos comunes de a y de b , es decir, de los números enteros positivos m tales que $a \mid m$ y $b \mid m$. Si a y b no son simultáneamente nulos, entonces el conjunto $M(a, b)$ no es vacío y podemos entonces considerar su mínimo elemento: lo llamamos el **mínimo común múltiplo** de a y b , y lo escribimos $\text{mcm}(a, b)$. Si en cambio alguno de a o b es nulo definimos $\text{mcm}(a, b) = 0$.

(b) El entero no negativo $\text{mcm}(a, b)$ es el único que tiene las siguientes dos propiedades:

- es un múltiplo común de a y de b , y
- divide a todo múltiplo común de a y de b .

(c) Si a y b son no negativos, se tiene que $ab = \text{mcd}(a, b) \cdot \text{mcm}(a, b)$. En particular, es $\text{mcm}(a, b) = ab$ si y solamente si $\text{mcd}(a, b) = 1$.

(d) Si a, b y c son enteros, entonces

$$\text{mcm}(ac, bc) = \text{mcm}(a, b) \cdot c.$$

Si además a y b son coprimos, entonces

$$\text{mcm}(ab, c) \cdot c = \text{mcd}(a, c) \cdot \text{mcd}(b, c).$$

(e) Dé una definición del mínimo común múltiplo de un conjunto finito de enteros, en el espíritu del Ejercicio 6.6.1, y pruebe sus propiedades básicas. En particular, muestre que si $n \in \mathbb{N}$ es al menos 3 y a_1, \dots, a_n son enteros, entonces

$$\text{mcm}(\text{mcm}(a_1, a_2), a_3, \dots, a_n) = \text{mcm}(a_1, a_2, a_3, \dots, a_n).$$

Algunas propiedades del máximo común divisor y del mínimo común múltiplo

6.6.3.

(a) Si a, b y c son enteros, entonces

$$\text{mcd}(\text{mcd}(a, b), c) = \text{mcd}(a, \text{mcd}(b, c))$$

y

$$\text{mcm}(\text{mcm}(a, b), c) = \text{mcm}(a, \text{mcm}(b, c)).$$

En otras palabras, las operaciones $\text{mcd}(\cdot, \cdot)$ y $\text{mcm}(\cdot, \cdot)$ son asociativas.

(b) Si a, b, c son enteros, entonces

$$\text{mcd}(a, \text{mcm}(b, c)) = \text{mcm}(\text{mcd}(a, b), \text{mcd}(a, c))$$

y

$$\text{mcm}(a, \text{mcd}(b, c)) = \text{mcd}(\text{mcm}(a, b), \text{mcm}(a, c))$$

(c) Si $k \in \mathbb{N}$ y $\text{mcd}(a, b) = d$, entonces $\text{mcd}(a^k, b^k) = d^k$.

(d) Si a y b no son simultáneamente nulos, se tiene que

$$\text{mcd}\left(\frac{a}{\text{mcd}(a, b)}, \frac{b}{\text{mcd}(a, b)}\right) = 1.$$

(e) Si a, b y c son enteros, entonces

$$\text{mcm}(a, b, c) \cdot \text{mcd}(a, b) \cdot \text{mcd}(b, c) \cdot \text{mcd}(c, a) = bac \cdot \text{mcd}(b, a, c).$$

Este ejercicio fue uno de los tomados en la primera Olimpiada de Matemáticas de Moscú en 1935.

La sucesión $(a^n - 1)_{n \geq 0}$

6.6.4. Sea a un entero distinto de 0 y de 1.

(a) Si x e y son enteros y $n \in \mathbb{N}$, entonces

$$x^n - y^n = (x - y)(x^{n-1} + x^{n-2}y + x^{n-3}y^2 + \cdots + xy^{n-2} + y^{n-1})$$

y, en particular, $x - y$ divide a $x^n - y^n$.

(b) Si $n, m \in \mathbb{N}$ y n divide a m , entonces $a^n - 1$ divide a $a^m - 1$.

(c) Si $n, m \in \mathbb{N}$ y r es el resto de la división de n por m , entonces

$$\text{mcd}(a^n - 1, a^m - 1) = \text{mcd}(a^r - 1, a^m - 1).$$

(d) Si $n, m \in \mathbb{N}$, entonces $\text{mcd}(a^n - 1, a^m - 1) = a^{\text{mcd}(n, m)} - 1$.

Los números de Fibonacci

6.6.5. Sea $(F_n)_{n \geq 0}$ la sucesión de los números de Fibonacci.

(a) Muestre que para todo $n \in \mathbb{N}$ se tiene que $\text{mcd}(F_n, F_{n+1}) = 1$ y encuentre enteros x e y tales que $xF_n + yF_{n+1} = 1$.

(b) Si $n, m \in \mathbb{N}$ y n divide a m , entonces F_n divide a F_m .

(c) Si $n, m \in \mathbb{N}$ y r es el resto de la división de n por m , entonces

$$\text{mcd}(F_n, F_m) = \text{mcd}(F_r, F_m).$$

(d) Si $n, m \in \mathbb{N}_0$, entonces

$$\text{mcd}(F_n, F_m) = F_{\text{mcd}(n,m)}.$$

Sugerencia: Para probar la parte (b) es útil recordar el Lema 5.4.8 del Capítulo 5.

6.6.6. Sea $n \in \mathbb{N}$.

- (a) El algoritmo de Euclides necesita $n + 1$ pasos para calcular $\text{mcd}(F_{n+3}, F_{n+2})$.
(b) Si a y b son dos enteros positivos tales $a > b$ y para los cuales el algoritmo de Euclides necesita $n + 1$ pasos para calcular $\text{mcd}(a, b)$, entonces $a \geq F_{n+3}$ y $b \geq F_{n+2}$.

Observemos que la conjunción de estas dos afirmaciones nos dice que el peor caso —en el sentido que tarda la máxima cantidad de pasos— para el algoritmo de Euclides es aquél en el que sus datos de partida so dos números de Fibonacci consecutivos.

- (c) Si a y b son enteros tales que $1 < b, a < N$, entonces el número de pasos que algoritmo de Euclides requiere para calcular $\text{mcd}(a, b)$ no excede a $\lceil \log_\varphi(\sqrt{5}N) \rceil - 2$. Aquí $\varphi = (1 + \sqrt{5})/2$, \log_φ denota el logaritmo en base φ y para cada número real u escribimos $\lceil u \rceil$ el menor entero mayor que u .

Este resultado es conocido como *Teorema de Lamé*, por *Gabriel Lamé* (1795–1870, Francia), quien lo obtuvo en 1844. Puede encontrarse una discusión detallada del algoritmo de Euclides desde el punto de vista de la complejidad en el libro [Knu1969].

El desarrollo en fracción continua finita de un número racional

6.6.7. Sea a/b un número racional positivo escrito de manera irreducible, de manera que a y b son enteros positivos y $\text{mcd}(a, b) = 1$. Sea $(r_i)_{i \geq 0}$ la sucesión construida por el algoritmo de Euclides para calcular el máximo común divisor de a y b , como en 6.4.6, y sea N el número que nos da la Proposición 6.4.7, de manera que $r_i \neq 0$ si $i \leq N$, $r_N = \text{mcd}(a, b) = 1$ y $r_i = 0$ si $i > N$. Sean, finalmente, q_2, \dots, q_{N+1} la sucesión de los cocientes que encontramos al llevar a cabo el algoritmo: esto es, tales que $r_{i-2} = q_i r_{i-1} + r_i$ para cada $i \in \{2, \dots, N+1\}$.

Muestre que

$$\frac{a}{b} = q_2 + \frac{r_2}{r_1} = q_2 + \frac{1}{q_3 + \frac{r_3}{r_2}} = q_2 + \frac{1}{q_3 + \frac{1}{q_4 + \frac{r_4}{r_3}}} = q_2 + \frac{1}{q_3 + \frac{1}{q_4 + \frac{1}{q_5 + \frac{r_5}{r_4}}}} = \dots$$

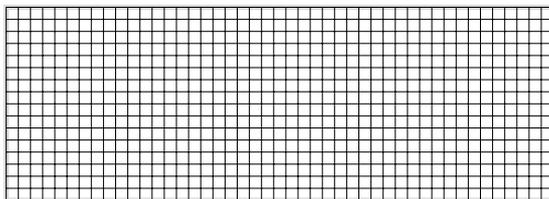
y que se puede continuar así hasta obtener la expresión

$$\frac{a}{b} = q_2 + \frac{1}{q_3 + \frac{1}{q_4 + \frac{1}{\ddots + \frac{1}{q_{N+1}}}}}$$

Esta escritura para el número a/b se llama su expresión como *fracción continua finita*. Así, por ejemplo, tenemos que

$$\frac{77}{30} = 2 + \frac{1}{1 + \frac{1}{1 + \frac{1}{3 + \frac{1}{4}}}}, \quad \frac{81\,201}{56\,660} = 1 + \frac{1}{2 + \frac{1}{3 + \frac{1}{4 + \frac{1}{5 + \frac{1}{6 + \frac{1}{7 + \frac{1}{8}}}}}}}$$

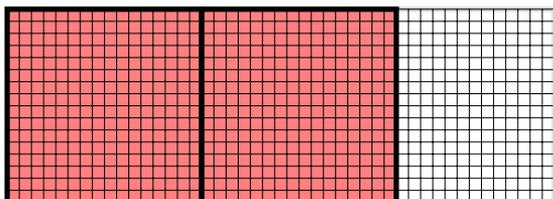
6.6.8. Sean a y b dos enteros positivo tales que $a \geq b$ y supongamos que tenemos una cuadrícula de a por b . Por ejemplo, si $a = 45$ y $b = 16$, tenemos el siguiente diagrama



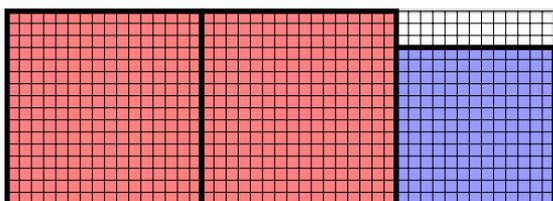
Nuestro objetivo es cubrir esta cuadrilla con cuadrados de tamaños enteros. Es claro

que esto es posible: basta usar $45 \cdot 16 = 720$ cuadrados de 1 por 1. Lo que queremos, sin embargo, es usar la menor cantidad posible de cuadrados. Una estrategia posible que podemos probar es la de usar la mayor cantidad posible de cuadrados lo más grandes que podamos.

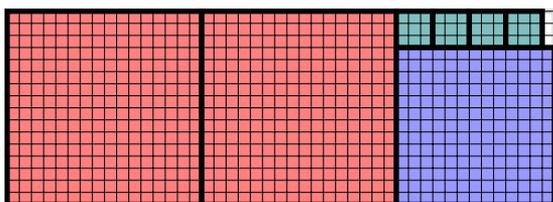
En este ejemplo concreto, es claro que el tamaño máximo de un cuadrado de lados enteros que entra en el diagrama es 16. Además, como el cociente de dividir 45 por 16 es 2, el número máximo de cuadrados de lado 16 que podemos poner es 2.



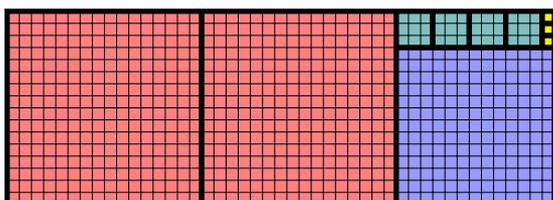
Después de poner esos dos rectángulos, nos queda sin cubrir una región de 13 por 16. El lado del cuadrado más grande que entra en ella es 13 y claramente entra uno solo: si lo ponemos, queda



Quedó libre una región de 13 por 3: el cuadrado más grande que entra ahí es de 3 por 3 y entran 4 de ellos.



Finalmente, es claro que la región que nos queda sólo la podemos cubrir con 3 cuadrados de 1 por 1. Al terminar, entonces, tenemos la siguiente situación:

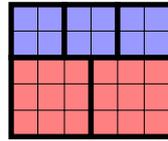
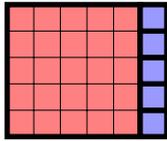


6.6.9. Sean a y b dos enteros positivos tales que $a \geq b$ y sean $(r_i)_{i \geq 0}$, N y q_2, \dots, q_{N+1} como en el Ejercicio 6.6.7. Se tiene que

$$ab = q_2 r_1^2 + q_3 r_2^2 + \dots + q_{N+1} r_N^2$$

y es posible cubrir un rectángulo de a por b con $q_2 + q_3 + \dots + q_{N+1}$ cuadrados de lados de longitud entera.

Observemos que no es claro que la estrategia que describimos arriba para hacer cubrir el rectángulo sea una que minimice el número de cuadrados y, de hecho, esto no es cierto. El menor ejemplo de esto aparece cuando consideramos un rectángulo de 6 por 5: de los siguientes dos diagramas el de la izquierda fue construido usando la estrategia anterior y usa en total 6 cuadrados, mientras que el de la derecha usa solamente 5.



Si a y b son enteros positivos tales que $a \geq b$ y $\text{mcd}(a, b)$, escribamos $\sigma(a, b)$ al menor número de cuadrados de lados enteros con los que es posible cubrir un rectángulo de a por b . Richard Kenyon mostró en su trabajo [Ken1996] que hay una constante positiva C tal que

$$\max \left\{ \frac{a}{b}, \log_2 a \right\} \leq \sigma(a, b) \leq \frac{a}{b} + C \log_2 b$$

cada vez que a y b son enteros coprimos y $a \geq b > 0$.

En el contexto de este problema, es interesante recordar el siguiente teorema clásico de Max Dehn [Deh1903] y Roland Sprague [Spr1940], que tiene una demostración sorprendentemente difícil: un rectángulo puede ser cubierto con finitos cuadrados sin que estos se superpongan si y solamente si el cociente de las longitudes de sus lados es un número racional. Una demostración muy simplificada y más conceptual de este resultado —en el que el problema se reduce a un problema sobre el flujo de electricidad en un circuito eléctrico que es luego resuelto usando la Ley de Kirchoff— puede encontrarse en [BSST1940].

Capítulo 7

Congruencias

§7.1. La relación de congruencia

7.1.1. Sea $m \in \mathbb{N}$. Decimos que dos enteros a y b son *congruentes módulo m* si $m \mid a - b$ y en ese caso escribimos

$$a \equiv b \pmod{m}.$$

Esto define una relación en el conjunto \mathbb{Z} , la relación de *congruencia módulo m* .

Proposición. Sea $m \in \mathbb{N}$. La relación de congruencia módulo m en \mathbb{Z} es una relación de equivalencia.

Demostración. Verifiquemos que esa relación tiene las tres propiedades necesarias.

- Si $a \in \mathbb{Z}$, entonces sabemos que $m \mid 0 = a - a$, así que $a \equiv a \pmod{m}$.
- Sean $a, b \in \mathbb{Z}$ tales que $a \equiv b \pmod{m}$, de manera que $m \mid a - b$. De acuerdo a la Proposición 6.1.2(ii), entonces, tenemos que $m \mid -(a - b) = b - a$ y, por lo tanto, que $b \equiv a \pmod{m}$.
- Sean $a, b, c \in \mathbb{Z}$ tales que $a \equiv b \pmod{m}$ y $b \equiv c \pmod{m}$, de manera que $m \mid a - b$ y $m \mid b - c$. La Proposición 6.1.5 nos dice que entonces

$$m \mid (a - b) + (b - c) = a - c$$

y, en consecuencia, que $a \equiv c \pmod{m}$.

Así, la congruencia módulo m es reflexiva, simétrica y transitiva: esto prueba que es una relación de equivalencia. \square

7.1.2. La relación de congruencia está estrechamente conectada con el algoritmo de la división:

Proposición. Sea $m \in \mathbb{N}$. Dos enteros son congruentes módulo m si y solamente si tienen el mismo resto en la división por m .

Demostración. Sean a y b dos enteros y sean q y r , por un lado, y q' y r' , por otro, el cociente y el resto de la división de a y de b por m , de manera que $a = qm + r$, $0 \leq r < m$, $b = q'm + r'$ y $0 \leq r' < m$.

Supongamos primero que $a \equiv b \pmod{m}$, es decir, que $m \mid a - b$. Como m divide a $(q - q')m$ y

$$a - b = (qm + r) - (q'm + r') = (q - q')m + r' - r,$$

vemos que m divide a $r - r'$. Usando el Lema 6.2.2 podemos concluir que $r = r'$.

Supongamos ahora, para probar la implicación recíproca, que $r = r'$. En ese caso tenemos que

$$a - b = (qm + r) - (q'm + r') = (q - q')m + (r - r') = (q - q')m$$

y, en particular, m divide a $a - b$, es decir, $a \equiv b \pmod{m}$. La proposición queda así probada. \square

7.1.3. Usando congruencias, es fácil caracterizar al resto de la división de un número por otro:

Proposición. Sea $m \in \mathbb{N}$ y sea $a \in \mathbb{Z}$.

- (i) Si r es el resto de dividir a a por m , entonces $a \equiv r \pmod{m}$.
- (ii) Recíprocamente, si s es un elemento de $\{0, \dots, m - 1\}$ tal que $a \equiv s \pmod{m}$, entonces s es el resto de dividir a a por m .

Estas dos afirmaciones muestran que el resto de dividir a a por m es el único elemento de $\{0, \dots, m - 1\}$ que es congruente con a módulo m .

Demostración. Sea a un entero y sean q y r , respectivamente, el cociente y el resto de dividir a a por m , de manera que, en particular, $a = qm + r$. Se sigue de esta igualdad que $a - r = qm$, así que claramente $m \mid a - r$, esto es, $a \equiv r \pmod{m}$. Esto prueba la primera parte de la proposición.

Para ver la segunda, supongamos que $s \in \{0, \dots, m - 1\}$ es tal que $a \equiv s \pmod{m}$. Como además $a \equiv r \pmod{m}$, como acabamos de probar, vemos que $r \equiv s \pmod{m}$, es

decir, que m divide a $r - s$: de acuerdo al Lema 6.2.2, esto implica que $r = s$, esto es, que s es el resto de dividir a a por m . \square

7.1.4. La relación de congruencia es compatible con las operaciones aritméticas, en el siguiente sentido:

Proposición. Sea $m \in \mathbb{N}$. Si a, a', b y b' son números enteros tales que $a \equiv a' \pmod{m}$ y $b \equiv b' \pmod{m}$, entonces

$$-a \equiv -a' \pmod{m},$$

$$a + b \equiv a' + b' \pmod{m}$$

y

$$ab \equiv a'b' \pmod{m}.$$

Demostración. Sean $a, a', b, b' \in \mathbb{Z}$ tales que $a \equiv a' \pmod{m}$ y $b \equiv b' \pmod{m}$, de manera que m divide a $a - a'$ y a $b - b'$. Existen entonces enteros c y d tales que $a - a' = cm$ y $b - b' = dm$. Por un lado, tenemos que

$$(-a) - (-a') = -(a - a') = (-c)m$$

así que m divide a $(-a) - (-a')$ y, en consecuencia, $-a \equiv -a' \pmod{m}$. Por otro,

$$(a + b) - (a' + b') = (a - a') + (b - b') = cm + dm = (c + d)m$$

y

$$\begin{aligned} ab - a'b' &= ab - a'b + a'b - a'b' = (a - a')b + a'(b - b') \\ &= cmb + a'dm = (cb + a'd)m. \end{aligned}$$

Esto nos dice que m divide a $(a + b) - (a' + b')$ y a $ab - a'b'$, es decir que $a + b \equiv a' + b' \pmod{m}$ y que $ab \equiv a'b' \pmod{m}$, como afirma la proposición. \square

7.1.5. La Proposición 7.1.4 nos dice que la relación de congruencia es compatible con la suma y el producto de pares de enteros, pero una inducción más o menos evidente muestra que esto se extiende a sumas y productos de cualquier número finito de enteros:

Corolario. Sea $m \in \mathbb{N}$. Si $n \in \mathbb{N}$ y $a_1, \dots, a_n, b_1, \dots, b_n \in \mathbb{Z}$ son tales que $a_i \equiv b_i \pmod{m}$ para cada $i \in \{1, \dots, n\}$, entonces

$$a_1 + \dots + a_n \equiv b_1 + \dots + b_n \pmod{m}$$

y

$$a_1 \cdots a_n \equiv b_1 \cdots b_n \pmod{m}.$$

Demostración. Para cada $n \in \mathbb{N}$ sea $P(n)$ la afirmación

si $a_1, \dots, a_n, b_1, \dots, b_n$ son enteros tales que $a_i \equiv b_i \pmod{m}$ para cada $i \in \{1, \dots, n\}$, entonces $a_1 + \cdots + a_n \equiv b_1 + \cdots + b_n \pmod{m}$ y $a_1 \cdots a_n \equiv b_1 \cdots b_n \pmod{m}$.

Mostraremos que $P(n)$ vale para todo $n \in \mathbb{N}$ y esto claramente probará el corolario. Observemos que la afirmación $P(1)$ vale trivialmente, así que bastará que establezcamos el paso inductivo.

Sea entonces $n \in \mathbb{N}$ tal que $n \geq 2$, supongamos que la afirmación $P(n-1)$ vale y sean $a_1, \dots, a_n, b_1, \dots, b_n$ enteros tales que $a_i \equiv b_i \pmod{m}$ para cada $i \in \{1, \dots, n\}$. En particular, tenemos que $a_i \equiv b_i \pmod{m}$ para cada $i \in \{1, \dots, n-1\}$ y, por lo tanto, la hipótesis inductiva nos dice que

$$a_1 + \cdots + a_{n-1} \equiv b_1 + \cdots + b_{n-1} \pmod{m}$$

y

$$a_1 \cdots a_{n-1} \equiv b_1 \cdots b_{n-1} \pmod{m}.$$

Como además $a_n \equiv b_n \pmod{m}$, usando la Proposición 7.1.4, tenemos que

$$\begin{aligned} a_1 + \cdots + a_n &= (a_1 + \cdots + a_{n-1}) + a_n \\ &\equiv (b_1 + \cdots + b_{n-1}) + b_n \pmod{m} \\ &= b_1 + \cdots + b_n \end{aligned}$$

y, de manera similar,

$$\begin{aligned} a_1 \cdots a_n &= (a_1 \cdots a_{n-1})a_n \\ &\equiv (b_1 \cdots b_{n-1})b_n \pmod{m} \\ &= b_1 \cdots b_n. \end{aligned}$$

Esto significa que la afirmación $P(n)$ vale y completa la inducción. \square

7.1.6. Un caso particular útil del corolario que acabamos de probar es aquél en que consideramos productos en que todos los factores son iguales:

Corolario. Sea $m \in \mathbb{N}$. Si a y b son dos enteros tales que $a \equiv b \pmod{m}$ y $k \in \mathbb{N}$, entonces $a^k \equiv b^k \pmod{m}$.

Demostración. Este resultado es un caso particular de la segunda afirmación del Corolario 7.1.5 en el que $a_1 = \cdots = a_k = a$ y $b_1 = \cdots = b_k = b$. \square

7.1.7. Como consecuencia de la Proposición 7.1.4 y sus corolarios, cuando tenemos una expresión aritmética construida a partir de enteros usando sumas, productos y potencias y estamos trabajando módulo algún número $m \in \mathbb{N}$ podemos reemplazar esos enteros por otros congruentes. Así, por ejemplo, trabajando módulo 7 es

$$222 + 210^{23} - 297 \cdot 91 \equiv 5 + 0^{23} - 3 \cdot 0 = 5,$$

ya que $222 \equiv 5$, $210 \equiv 91 \equiv 0$ y $297 \equiv 3$. De manera similar, podemos ver que para todo $n \in \mathbb{N}$ el número $10^{3n} + 1$ es divisible por 7 si y solamente si n es impar. En efecto, trabajando módulo 7 tenemos que $10^3 \equiv -1$, así que

$$10^{3n} + 1 = (10^3)^n + 1 \equiv (-1)^n + 1,$$

y esto es 0 si y solamente si n es impar. Observemos que esto nos dice además que cuando n es par el resto de dividir a $10^{3n} + 1$ por 7 es 2.

Veremos muchas aplicaciones de esto en todo lo que sigue, pero mostremos cómo podemos usar los resultados de esta sección para resolver una parte del Ejercicio 6.6.4:

Proposición. Si a es un entero distinto de 1 y $n \in \mathbb{N}$, entonces $a - 1$ divide a $a^n - 1$.

Demostración. Sea $a \in \mathbb{Z}$ distinto de 1 y sea $n \in \mathbb{N}$. Como $|a - 1|$ divide a $a - 1$, trabajando módulo $|a - 1|$ es claro que $a \equiv 1$. De acuerdo al Corolario 7.1.6, entonces, tenemos que $a^n \equiv 1^1 = 1$ y esto significa, precisamente, que $|a - 1|$ divide a $a^n - 1$. Por supuesto, la proposición siguen inmediatamente de esto. \square

Es importante notar cuál es la diferencia entre esta forma de proceder y la sugerida por el ejercicio 6.6.4. Allí, para ver que $a - 1$ divide a $a^n - 1$ mostramos explícitamente cuál es el cociente (a saber, la suma geométrica $1 + a + \dots + a^{n-1}$) mientras que aquí llegamos a la misma conclusión sin necesidad de hacer eso. Es más: el argumento que acabamos de usar no nos da ninguna idea sobre cuál es ese cociente.

En la sección siguiente haremos uso de esta misma idea para obtener varios criterios de divisibilidad.

7.1.8. Una última propiedad importante que tenemos que hacer y que nos será extremadamente útil es la siguiente:

Proposición. Sea $m \in \mathbb{N}$ y sea $a \in \mathbb{Z}$. Existe un entero $b \in \mathbb{Z}$ tal que $ab \equiv 1 \pmod{m}$ si y solamente si a es coprimo con m .

Demostración. Supongamos primero que a y m son coprimos, de manera que existen enteros b y c tales que $ab + mc = 1$. Tenemos entonces que $ab = 1 - mc \equiv 1 \pmod{m}$ y esto muestra que la condición del enunciado es suficiente.

Por otro lado, supongamos que existe un entero b tal que $ab \equiv 1 \pmod{m}$, de manera que m divide a $ab - 1$, esto es, existe $x \in \mathbb{Z}$ tal que $ab - 1 = mx$. Si d un divisor común positivo de a y m , entonces d divide también a $ab - mx = 1$: esto sólo es posible si $d = 1$ y muestra que $\text{mcd}(a, m) = 1$. \square

§7.2. Algunos criterios de divisibilidad

7.2.1. Como $10 \equiv 1 \pmod{9}$, el Corolario 7.1.6 nos dice que $10^n \equiv 1^n = 1 \pmod{9}$ para todo $n \in \mathbb{N}$. De esto obtenemos fácilmente el siguiente criterio de divisibilidad por 9:

Proposición. Sea $a \in \mathbb{N}$. Si $a = (d_k, \dots, d_0)_{10}$ es la escritura de a en base 10, entonces a es divisible por 9 si y solamente si la suma $d_0 + \dots + d_k$ de sus dígitos decimales lo es y, de hecho, ambos números tienen el mismo en la división por 9.

Así, por ejemplo, la suma de los dígitos decimales de 45 261 189 es 36, y la suma de los dígitos decimales de este último número es 9: vemos así que 9 divide a 45 261 189. Esta proposición es el primer ejemplo que da Gauss en su *Disquisitiones Arithmeticae* de una aplicación de la relación de congruencia, y la prueba de damos es exactamente la misma que él da —que reproducimos en la Figura 7.1 en la página siguiente.

Demostración. Sea $(d_k, \dots, d_0)_{10}$ la escritura decimal de a , de manera que

$$a = d_0 + d_1 \cdot 10 + \dots + d_k \cdot 10^k.$$

Como observamos arriba, es $10^n \equiv 1 \pmod{9}$ para todo $n \in \mathbb{N}$, así que gracias a la Proposición 7.1.4 tenemos que $d_i \cdot 10^i \equiv d_i \cdot 1 = d_i \pmod{9}$ para cada $i \in \{0, \dots, k\}$ y entonces, usando el Corolario 7.1.5, que

$$a = d_0 + d_1 \cdot 10 + \dots + d_k \cdot 10^k \equiv d_0 + d_1 + \dots + d_k \pmod{9}.$$

Sabemos que a es divisible por 9 si y solamente si $a \equiv 0 \pmod{9}$ y, de acuerdo a lo que acabamos de probar, esto sucede si y solamente si $d_0 + \dots + d_k \equiv 0 \pmod{9}$, es decir, si la suma $d_0 + \dots + d_k$ es divisible por 9. Esto prueba la proposición. \square

7.2.2. De manera similar podemos obtener un criterio de divisibilidad por 11:

Proposición. Sea $a \in \mathbb{N}$ y sea $(d_k, \dots, d_0)_{10}$ la escritura decimal de a . El número a es divisible

Theorematibus in hoc capite traditis complura quae in arithmetiis doceri solent innotuntur, e. g. regulae ad explorandam divisibilitatem numeri propositi per 9, 11 aut alios numeros. *Secundum modulum 9* omnes numeri 10 potestates unitati sunt congruae: quare si numerus propositus habet formam $a + 10b + 100c + \text{etc.}$, idem residuum minimum secundum modulum 9 dabit, quod $a + b + c + \text{etc.}$ Hinc manifestum est, si figurae singulae numeri decadice expressi sine respectu loci quem occupant addantur, summam hanc numerumque propositum eadem residua minima praeberere, adeoque hunc per 9 dividi posse, si illa per 9 sit divisibilis, et contra. Idem etiam de divisore 3 tenendum. Quoniam *secundum modulum 11*, $100 \equiv 1$ crit generaliter $10^{2k} \equiv 1$, $10^{2k+1} \equiv 10 \equiv -1$, et numerus formae $a + 10b + 100c + \text{etc.}$ secundum modulum 11 idem residuum minimum dabit quod $a - b + c \text{ etc.}$; unde regula nota protinus derivatur. Ex eodem principio omnia similia praecepta facile deducuntur.

Figura 7.1. El párrafo 12 de las *Disquisitiones Arithmeticae* de Carl Friedrich Gauss, en el que enuncia y prueba nuestra Proposición 7.2.1.

por 11 si y solamente si 11 divide a la suma alternada de sus dígitos decimales,

$$d_0 - d_1 + d_2 - d_3 + \cdots + (-1)^k d_k.$$

Por ejemplo, el número 64320883 es divisible por 11: en efecto, la suma alternada de sus dígitos decimales es $3 - 8 + 8 - 0 + 2 - 3 + 4 - 6 = 0$, que es divisible por 11.

Demostración. Como $10 \equiv -1 \pmod{11}$, para todo $n \in \mathbb{N}_0$ es $10^n \equiv (-1)^n \pmod{11}$, así que, como en la prueba de la proposición anterior, tenemos que

$$a = \sum_{i=0}^k d_i \cdot 10^n \equiv \sum_{i=0}^k d_i \cdot (-1)^n \pmod{11}.$$

De esto se deduce que 11 divide a a si y solamente si divide a $\sum_{i=0}^k d_i \cdot (-1)^n$, que es lo que afirma la proposición. \square

7.2.3. El siguiente resultado es similar al de la Proposición 7.2.1, pero ahora tomando los dígitos en bloques de a tres:

Proposición. Sea $a \in \mathbb{N}$ y sean $(d_k \dots, d_0)_{10}$ la escritura decimal de a . El número a es divisible por 27 si y solamente si la suma de los números que se obtienen agrupando sus dígitos de a tres

desde la derecha,

$$(d_2, d_1, d_0)_{10} + (d_5, d_4, d_3)_{10} + (d_8, d_7, d_6)_{10} + \cdots,$$

es divisible por 27.

Así, el número 12 492 342 315 es divisible por 27 porque $315 + 342 + 492 + 12 = 1161$ lo es, y esto es así porque $161 + 1 = 162 = 27 \cdot 6$ lo es.

Demostración. Sea $l = \lfloor k/3 \rfloor$ y, para cada $i \in \{0, \dots, l\}$, sea $e_i = (d_{3i+2}, d_{3i+1}, d_{3i})_{10}$. Sabemos que $a = (e_l, \dots, e_0)_{1000}$ y la proposición es consecuencia de que

$$a = \sum_{i=0}^l e_i \cdot 1000^i \equiv \sum_{i=0}^l e_i \pmod{27},$$

ya que $1000 \equiv 1 \pmod{27}$. □

7.2.4. Hay muchos criterios de divisibilidad que miran solamente los últimos dígitos del número. Algunos de ellos son los siguientes:

Proposición. Sea $a \in \mathbb{N}$ y sea $(d_k, \dots, d_0)_{10}$ la escritura decimal de a .

- (i) El número a es divisible por 2 si y solamente si d_0 es par, y es divisible por 5 si y solamente si $d_0 \in \{0, 5\}$.
- (ii) El número a es divisible por 4 o por 25 si y solamente si el número $(d_1, d_0)_{10}$ lo es.

Usando esta proposición vemos inmediatamente que 12 326 es divisible por 2, que 101 436 no es divisible por 5, que 874 917 no es divisible por 4 y que 1 927 225 es divisible por 25.

Demostración. Como $10 \equiv 0 \pmod{2}$ y $10 \equiv 0 \pmod{5}$, para todo $n \in \mathbb{N}$ se tiene que $10^n \equiv 0 \pmod{2}$ y $10^n \equiv 0 \pmod{5}$. Esto implica que

$$a = \sum_{i=0}^k d_i \cdot 10^i \equiv d_0$$

tanto módulo 2 como módulo 5. La primera afirmación de la proposición es consecuencia de esto. Por otro lado, como $10^2 \equiv 0$ módulo 4 y módulo 25, tenemos que para cada entero $n \geq 2$ es $10^n = 10^2 \cdot 10^{n-2} \equiv 0 \cdot 10^{n-2} = 0$ tanto módulo 4 como módulo 25 y, por lo tanto,

$$a = \sum_{i=0}^k d_i \cdot 10^i \equiv d_0 + d_1 \cdot 10 = (d_1, d_0)_{10}$$

módulo 4 o módulo 25. De esta congruencia se deduce la segunda afirmación de la proposición. □

7.2.5. Un tercer tipo de criterio de divisibilidad puede deducirse usando las mismas ideas.

Proposición. Sea $a \in \mathbb{N}$ y sea $(d_k, \dots, d_0)_{10}$ la escritura decimal de a . El número a es divisible por 7 si $2(d_k, \dots, d_2)_{10} + (d_1, d_0)_{10}$ lo es.

El interés de esto es que el número $2(d_k, \dots, d_2)_{10} + (d_1, d_0)_{10}$ es más chico que a y, por lo tanto, que podemos usar el criterio recursivamente. Por ejemplo, para ver que 96502 es divisible por 7 basta observar que $2 \cdot 965 + 2 = 1932$ lo es, y para esto que $2 \cdot 19 + 32 = 70$ lo es.

Demostración. Si $b = (d_k, \dots, d_2)_{10}$ y $c = (d_1, d_0)_{10}$, entonces

$$a = 100b + c \equiv 2b + c \pmod{7},$$

ya que $100 \equiv 2 \pmod{7}$. La proposición es consecuencia de esta congruencia. \square

§7.3. Los enteros módulo m

7.3.1. Si $m \in \mathbb{N}$, escribimos \mathbb{Z}_m al conjunto cociente de \mathbb{Z} por la relación de congruencia módulo m y lo llamamos el conjunto de los *enteros módulo m* . Es importante recordar que a pesar de este nombre, los elementos de \mathbb{Z}_m no son enteros sino clases de equivalencia, es decir, *conjuntos* de enteros.

7.3.2. Una consecuencia importante de la Proposición 7.1.2 es la determinación de la cantidad de elementos de \mathbb{Z}_m :

Proposición. Sea $m \in \mathbb{N}$. La relación de congruencia módulo m parte a \mathbb{Z} en m clases de equivalencia, que son

$$[0], [1], \dots, [m-1].$$

Demostración. Sea $a \in \mathbb{Z}$ y sean $q \in \mathbb{Z}$ y $r \in \{0, \dots, m-1\}$ el cociente y el resto de la división de a por m . Como $a - r = qm$, tenemos que $a \equiv r \pmod{m}$ y, por lo tanto, que $[a] = [r]$. Esto nos dice que todas las clases de congruencia módulo m aparecen en la lista del enunciado. Para terminar, entonces, bastará que probemos que las m clases allí listadas son distintas dos a dos.

Sean $i, j \in \{0, \dots, m-1\}$ y supongamos que $[i] = [j]$, de manera que $i \equiv j \pmod{m}$. La Proposición 7.1.2 nos dice entonces que i y j dan el mismo resto al ser divididos por m : como $0 \leq i, j < m$, esto implica que $i = j$ y prueba lo que queríamos. \square

7.3.3. La compatibilidad entre la relación de congruencia y las operaciones aritmética que afirma la Proposición 7.1.4 se ve reflejada en el siguiente resultado:

Proposición. Sea $m \in \mathbb{N}$. Hay funciones $S, P : \mathbb{Z}_m \times \mathbb{Z}_m \rightarrow \mathbb{Z}_m$ tales que cada vez que a y b está en \mathbb{Z} se tiene que

$$S([a], [b]) = [a + b]$$

y

$$P([a], [b]) = [ab].$$

Demostración. Consideremos el subconjunto

$$S = \{(([a], [b]), [a + b]) \in (\mathbb{Z}_m \times \mathbb{Z}_m) \times \mathbb{Z}_m : a, b \in \mathbb{Z}\}$$

del conjunto $(\mathbb{Z}_m \times \mathbb{Z}_m) \times \mathbb{Z}_m$. Se trata, por supuesto, de una relación de $\mathbb{Z}_m \times \mathbb{Z}_m$ a \mathbb{Z}_m . Mostremos que se trata, de hecho, de una función.

- Sea $x \in \mathbb{Z}_m \times \mathbb{Z}_m$, de manera que existen α y $\beta \in \mathbb{Z}_m$ tales que $x = (\alpha, \beta)$. Como \mathbb{Z}_m es el cociente de \mathbb{Z} por la relación de congruencia módulo m , existen enteros a y b tales que $\alpha = [a]$ y $\beta = [b]$ y, de acuerdo a la definición del conjunto S , el par ordenado $(x, [a + b]) = (([a], [b]), [a + b])$ pertenece a S .
- Supongamos, por otro lado, que $x \in \mathbb{Z}_m \times \mathbb{Z}_m$ e $y, y' \in \mathbb{Z}_m$ son tales que los pares ordenados (x, y) y (x, y') están en S . Como recién, existen enteros a, b, c y c' tales que $x = ([a], [b])$, $y = [c]$ e $y' = [c']$.

Ahora bien, como $(x, y) = (([a], [b]), [c])$ está en S , existen $a_1, b_1 \in \mathbb{Z}$ tales que $[a] = [a_1]$, $[b] = [b_1]$ y $[c] = [a_1 + b_1]$. Esto nos dice que modulo m se tiene que $a \equiv a_1$, $b \equiv b_1$ y $c \equiv a_1 + b_1$ y, por lo tanto, $c \equiv a + b$.

De manera similar, como $(x, y') = (([a], [b]), [c'])$ está en S , existen $a_2, b_2 \in \mathbb{Z}$ tales que $[a] = [a_2]$, $[b] = [b_2]$ y $[c'] = [a_2 + b_2]$, de manera que $a \equiv a_2$, $b \equiv b_2$ y $c' \equiv a_2 + b_2$: esto implica que $c \equiv a + b$.

Juntando estas dos cosas, concluimos que $c \equiv c'$ y, como consecuencia de ello, que $y = [c] = [c'] = y'$.

Si a y b son enteros, entonces es claro que $(([a], [b]), [a + b])$ está en S y esto significa, precisamente, que $S([a], [b]) = [a + b]$. Esto muestra que la función S satisface la condición que aparece en el enunciado.

Para ver el resto de la proposición, basta considerar el subconjunto

$$P = \{([a], [b]), [ab] \in (\mathbb{Z}_m \times \mathbb{Z}_m) \times \mathbb{Z}_m : a, b \in \mathbb{Z}\}$$

de $(\mathbb{Z}_m \times \mathbb{Z}_m) \times \mathbb{Z}_m$ y mostrar que es también una función $\mathbb{Z}_m \times \mathbb{Z}_m \rightarrow \mathbb{Z}_m$ y que satisface la condición del enunciado. Esto puede hacerse de exactamente la misma forma a lo que acabamos de hacer: dejamos los detalles al lector. \square

7.3.4. Normalmente escribimos a las funciones S y P que nos da la proposición que acabamos de probar usando los símbolos $+$ y \cdot de suma y producto: si α y β son dos elementos de \mathbb{Z}_m , escribimos $\alpha + \beta$ y $\alpha \cdot \beta$ en lugar de $S(\alpha, \beta)$ y $P(\alpha, \beta)$.

Así, si a y b son dos enteros, usando esta notación tenemos que

$$[a] + [b] = [a + b] \tag{1}$$

y

$$[a] \cdot [b] = [a \cdot b].$$

Es importante observar que los símbolos $+$ y \cdot en estas igualdades denotan cosas distintas a la izquierda y a la derecha del signo de igualdad: a la derecha $+$ y \cdot denotan las operaciones usuales entre enteros, mientras que a la izquierda denotan las operaciones que acabamos de definir entre elementos de \mathbb{Z}_m . Esto introduce, por supuesto, una ambigüedad en lo que escribimos, pero el contexto es siempre suficiente para resolverla.

7.3.5. Las operaciones de suma y producto que hemos definido en el conjunto \mathbb{Z}_m tienen las mismas propiedades formales que las usuales de \mathbb{Z} :

Proposición. Sea $m \in \mathbb{N}$. En \mathbb{Z}_m se tiene que:

- La suma es asociativa: si $\alpha, \beta, \gamma \in \mathbb{Z}_m$, entonces $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$.
- Hay un elemento neutro para la suma, la clase $z = [0]$: para todo $\alpha \in \mathbb{Z}_m$ se tiene que $\alpha + z = \alpha = z + \alpha$.
- Todo elemento de \mathbb{Z}_m tiene un elemento opuesto: si $\alpha \in \mathbb{Z}_m$, existe $\beta \in \mathbb{Z}_m$ tal que $\alpha + \beta = \beta + \alpha = z$. De hecho, si $a \in \mathbb{Z}$ es tal que $\alpha = [a]$, entonces $\beta = [-a]$.
- La suma es conmutativa: para cada $\alpha, \beta \in \mathbb{Z}_m$ se tiene que $\alpha + \beta = \beta + \alpha$.
- El producto es asociativo: si α, β, γ son elementos de \mathbb{Z}_m , entonces $(\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$.
- Hay un elemento neutro para el producto, la clase $u = [1]$: para todo $\alpha \in \mathbb{Z}_m$ se tiene que $\alpha \cdot u = \alpha = u \cdot \alpha$.
- El producto es conmutativo: para cada $\alpha, \beta \in \mathbb{Z}_m$ se tiene que $\alpha \cdot \beta = \beta \cdot \alpha$.

- El producto se distribuye sobre la suma: si α , β y γ son elementos de \mathbb{Z}_m , entonces $(\alpha + \beta) \cdot \gamma = \alpha \cdot \gamma + \beta \cdot \gamma$

Demostración. Cada una de estas afirmaciones es consecuencia de la correspondiente afirmación sobre las operaciones entre enteros y de la observación de que todo elemento de \mathbb{Z}_m es de la forma $[a]$ para algún $a \in \mathbb{Z}$.

Por ejemplo, si α y β son dos elementos de \mathbb{Z}_m , entonces existen enteros a y b tales que $\alpha = [a]$ y $\beta = [b]$ y, por lo tanto,

$$\alpha + \beta = [a] + [b] = [a + b] = [b + a] = [b] + [a] = \beta + \alpha,$$

de manera que la suma en \mathbb{Z}_m es conmutativa. La segunda y la cuarta de estas igualdades son consecuencia directa de la relación (1) y la tercera de la conmutatividad de la suma de enteros. Dejamos al lector la verificación de las demás afirmaciones de la proposición. \square

7.3.6. A pesar de esta proposición, que nos dice que las operaciones de suma y producto en \mathbb{Z}_m funcionan en muchos aspectos como las de \mathbb{Z} , hay diferencias importantes. Mencionemos las dos que son probablemente las principales:

- En \mathbb{Z} el producto de dos enteros no nulo es siempre no nulo. En \mathbb{Z}_m , por otro lado, esto no es siempre cierto. Por ejemplo, si $m = 6$ sabemos que las clase $[2]$ y $[3]$ no son la clase nula $[0]$, pero su producto es $[2] \cdot [3] = [2 \cdot 3] = [6] = [0]$.
- En \mathbb{Z} los dos únicos elementos inversibles son 1 y -1 . En \mathbb{Z}_m esto puede no ser cierto. Si $m = 11$, por ejemplo, la clase $[4]$ es inversible, ya que el producto $[4] \cdot [3] = [12] = [1]$ es la clase unidad $[1]$: esto nos dice que $[4]$ es inversible en \mathbb{Z}_{11} y, sin embargo, $[4]$ no es ni $[1]$ ni $[-1]$.

§7.4. Ejercicios

Algunos criterios de divisibilidad

7.4.1. Sea $a \in \mathbb{N}$ y sean $(d_k \dots, d_0)_{10}$ la escritura decimal de a . El número a es divisible por 7 si y solamente si la suma alternada de los números que se obtienen agrupando sus dígitos de a tres desde la derecha,

$$(d_2, d_1, d_0)_{10} - (d_5, d_4, d_3)_{10} + (d_8, d_7, d_6)_{10} + \dots,$$

es divisible por 7. Así, por ejemplo, para ver que 13 476 066 723 es divisible por 7 observamos que $723 - 66 + 476 - 13 = 1\,120$ y que $120 - 1 = 119 = 7 \cdot 17$.

Capítulo 8

Ecuaciones diofánticas

§8.1. Ecuaciones diofánticas

8.1.1. En el sentido más general, una *ecuación diofántica* es una ecuación en la que buscamos soluciones con valores enteros. Así, tenemos una ecuación en r variables está determinada por

- una función $F : \Omega \rightarrow A$ con dominio un subconjunto Ω del producto cartesiano de r copias de \mathbb{Z} y codominio algún conjunto A , y
- un elemento $a_i \in A$,

y consiste en el problema de determinar si existen elementos (x_1, \dots, x_r) del conjunto Ω tales que

$$F(x_1, \dots, x_r) = a_0$$

Con frecuencia consideramos sólo ecuaciones en las que la función F es tal que $F(x_1, \dots, x_r)$ tiene una expresión en términos de los enteros x_1, \dots, x_r y las operaciones usuales —la suma, el producto, el cociente, la exponenciación, etc.— pero esto no es ciertamente necesario.

El nombre de estas ecuaciones recuerda a *Diofanto de Alejandría* (c. 201–c. 285, Egipto), conocido como “el padre del álgebra” y autor de una serie de libros, la *Arithmetica*, sobre la solución de ecuaciones algebraicas.

8.1.2. Vamos algunos ejemplos.

- (a) *Ecuaciones diofánticas lineales.* Si $r \in \mathbb{N}$ y $a_1, \dots, a_r, b \in \mathbb{Z}$, podemos poner $\Omega = \mathbb{Z}^r$ y $A = \mathbb{Z}$, definir una función $F : \mathbb{Z}^r \rightarrow \mathbb{Z}$ poniendo $F(x_1, \dots, x_r) = a_1x_1 + \dots + a_rx_r$

para cada $(x_1, \dots, x_r) \in \mathbb{Z}^r$, y considerar la ecuación diofántica

$$F(x_1, \dots, x_r) = b.$$

Explícitamente, esta ecuación consiste en decidir si existen r -uplas (x_1, \dots, x_r) de enteros tales que

$$a_1x_1 + \dots + a_rx_r = b.$$

- (b) *La ecuación de Pitágoras.* Pongamos $r = 3$, $\Omega = \mathbb{Z}^3$ y $A = \mathbb{Z}$, y sean $F : \mathbb{Z}^3 \rightarrow \mathbb{Z}$ la función tal que $F(x_1, x_2, x_3) = x_1^2 + x_2^2 - x_3^2$ y $a_0 = 0$. La ecuación diofántica correspondiente, llamada *ecuación de Pitágoras*, es, por lo tanto, el problema de encontrar, si es que existen, enteros x , y y z tales que

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

- (c) *La ecuación de Pell.* Fijamos $n \in \mathbb{N}$. El problema de encontrar enteros x e y tales que

$$x^2 - ny^2 = 1$$

es una ecuación diofántica, la *ecuación de Pell*, por *John Pell* (1611–1685, Inglaterra), aunque esta ecuación fue estudiada mucho tiempo antes —de hecho, la ecuación se conoce con el nombre de Pell porque Euler equivocadamente atribuyó a éste un método para su solución, que fue en realidad fue desarrollado por *William Brouncker* (1620–1684, Inglaterra) Para verla como un caso particular de la definición general que dimos arriba, podemos elegir $r = 2$, $\Omega = \mathbb{Z}^2$, $A = \mathbb{Z}$, $F : (x_1, x_2) \in \mathbb{Z}^2 \mapsto x_1^2 - nx_2^2 \in \mathbb{Z}$ y $a_0 = 1$.

- (d) *La ecuación de Fermat.* Fijemos n . La ecuación de Fermat de exponente n es el problema de encontrar enteros x , y y z tales que

$$x^n + y^n = z^n. \tag{1}$$

Famosamente Fermat hizo la siguiente anotación en un margen de su copia del libro de Diofanto, al lado de donde está enunciado el Problema VIII, que es precisamente el de la ecuación de Pitágoras, que mencionamos recién:

Es imposible separar un cubo en dos cubos, o una potencia cuarta en dos potencias cuartas, o en general cualquier potencia más alta que la segunda en dos potencias similares. He descubierto una demostración verdaderamente maravillosa de esto, pero este margen es demasiado angosto para contenerla.»

Lo que ahí afirma Fermat es que la ecuación (1) no tiene soluciones (salvo las triviales). Hoy hay acuerdo en que Fermat no tenía ninguna prueba de esto y fue recién en 1993 que *Andrew Wiles* (1953–, Inglaterra) pudo probar que la afirmación de Fermat es cierta —aunque hubo muchos resultados parciales antes.

(e) *La ecuación Ramanujan–Nagell*. Así es conocido el problema de encontrar enteros x y n tales que

$$2^n - 7 = x^2.$$

Notemos que en esta ecuación, a diferencia de todas las anteriores, hay una incógnita que aparece como un exponente. El problema fue planteado originalmente por Srinivasa Ramanujan en 1913, quien además conjeturó que hay exactamente cinco soluciones con x positivo, y esta conjetura fue probada por *Trygve Nagell* (1895–1988, Noruega) en 1948. Las cinco soluciones (x, n) de la ecuación son los pares

$$(1, 3), \quad (3, 4), \quad (5, 5), \quad (11, 7), \quad (181, 15).$$

La ecuación de Ramanujan–Nagell parece a primera vista bastante exótica y antojadiza, pero aparece en realidad en varios contextos. Por ejemplo, es equivalente al problema de encontrar los números de Mersenne, es decir, de la forma $2^a - 1$ con $a \in \mathbb{N}_0$, que son triangulares, esto es, de la forma $b(b + 1)/2$ con $b \in \mathbb{N}_0$. En efecto,

$$\begin{aligned} 2^a - 1 = \frac{b(b + 1)}{2} &\iff 8(2^a - 1) = 4b(b + 1) \\ &\iff 2^{a+3} - 8 = 4b^2 + 4b \\ &\iff 2^{a+3} - 7 = 4b^2 + 4b + 1 \\ &\iff 2^{a+3} - 7 = (2b + 1)^2. \end{aligned}$$

Esto nos dice que el número de Mersenne $2^a - 1$ es igual al número triangular $b(b + 1)/2$ si y solamente si el par $(x, n) = (2b + 1, a + 3)$ es una solución de la ecuación de Ramanujan–Nagell. Por supuesto, el problema de encontrar números de Mersenne que son triangulares no parece mucho menos antojadizo que la ecuación de Ramanujan–Nagell! En el trabajo [BS1956] de Georges Browkin y André Schinzel hay un estudio de este problema.

De todas formas, la ecuación de Ramanujan–Nagell aparece de forma natural en el estudio de los códigos con corrección de errores [SS1959], en teoría de álgebra diferencial [Mea1973] y en computación cuántica [PR2013].

§8.2. Ecuaciones lineales

8.2.1. Como dijimos antes, una *ecuación diofántica lineal* es un problema de la siguiente forma: dados $r \in \mathbb{N}$ y $a_1, \dots, a_r, b \in \mathbb{Z}$, decidir si hay r -uplas de enteros (x_1, \dots, x_r) tales que

$$a_1x_1 + \dots + a_rx_r = b$$

y, si ése es el caso, encontrarlas. Nuestro objetivo en esta sección es resolver este problema completamente.

8.2.2. Empecemos por el caso más sencillo: aquél en que $r = 1$ y hay, por lo tanto, una sola incógnita. Así, tenemos dos enteros a y b y queremos determinar si existen enteros x tales que $ax = b$ y, cuando los hay, encontrarlos. Reconocemos inmediatamente aquí el problema de la división entera, que ya sabemos resolver:

Proposición. Sean a y b dos enteros y consideremos el problema de encontrar enteros x tales que

$$ax = b.$$

Hay soluciones si y solamente si a divide a b . Si ése es el caso, entonces

- (i) si $a \neq 0$, entonces hay exactamente una solución, que es $x = b/a$, y
- (ii) si $a = 0$, entonces necesariamente $b = 0$ y todo entero es solución.

Demostración. Si hay una solución al problema, esto es, si existe un entero x tal que $ax = b$, entonces a divide a b simplemente por definición: esto muestra que la condición del enunciado es necesaria para que exista una solución. Recíprocamente, si suponemos que esa condición se cumple, de manera que a divide a b y existe un entero c tal que $ac = b$, entonces claramente ese entero c , que es b/a , es una solución a la ecuación. Esto muestra que la condición es suficiente.

Supongamos ahora que $a \neq 0$ y que x y x' son dos soluciones a la ecuación. En ese caso, tenemos que $ax = b = ax'$ y, por lo tanto, $a(x - x') = 0$. Como a no es nulo, esto es sólo posible si $x - x' = 0$, esto es, si $x = x'$. Vemos así que cuando $a \neq 0$ y hay soluciones, hay de hecho una única solución.

Supongamos en segundo lugar que $a = 0$ y que hay soluciones. Como ya vimos, el entero b tiene que ser divisible por a , así que $b = 0$, y claramente, entonces, todo número entero x es tal que $ax = b$. La proposición queda así completamente probada. \square

8.2.3. Consideremos ahora el caso en que hay dos variables, es decir, en que $r = 2$ en la situación de **8.2.1**. Así, tenemos tres enteros a , b y c y buscamos pares ordenados (x, y)

de enteros tales que

$$ax + by = c.$$

8.2.4. Empezamos considerando el *caso homogéneo*, es decir, aquél en el que $c = 0$.

Proposición. Sean a y b dos enteros y consideremos el problema de encontrar pares de enteros $(x, y) \in \mathbb{Z}^2$ tales que

$$ax + by = 0. \tag{2}$$

Sea $d = \text{mcd}(a, b)$.

(i) Supongamos que $d \neq 0$ y sean a' y b' los enteros tales que $a = da'$ y $b = db'$. Para cada $t \in \mathbb{Z}$ el par ordenado (x, y) con

$$x = b't, \qquad y = -a't$$

es una solución del problema y, más aún, toda solución del problema es de esta forma para un único entero t .

(ii) Si en cambio $d = 0$, entonces todo par $(x, y) \in \mathbb{Z}^2$ es solución del problema.

En particular, en cualquier caso hay infinitas soluciones.

Demostración. (i) Supongamos que $d \neq 0$ y sean a' y b' como en el enunciado.

Sea $(x, y) \in \mathbb{Z}^2$ una solución del problema (2), de manera que $ax + by = 0$. Tenemos que

$$0 = ax + by = da'x + db'y = d(a'x + b'y)$$

y, como d no es nulo, que $a'x + b'y = 0$ o, equivalentemente, que

$$a'x = -b'y. \tag{3}$$

Ahora bien, como d no es nulo, alguno de a o b es no nulo.

- Supongamos primero que $a \neq 0$ y que, por lo tanto, $a' \neq 0$. De la igualdad (3) se deduce que a' divide a $-b'y$ y, como $\text{mcd}(a', b') = 1$, que a' divide a $-y$. Existe entonces un entero t y sólo uno tal que $y = -a't$. Usando esto en (3) vemos que $a'x = b'a't$, así que $a'(x - b't) = 0$ y, como $a' \neq 0$, que finalmente $x = b't$. Concluimos de esta forma que $(x, y) = (b't, -a't)$ para un entero t completamente determinado por el par (x, y) .
- Supongamos ahora que $a = 0$. En este caso es necesariamente $b \neq 0$, $d = |b|$, $a' = 0$ y b' es 1 o -1 , según que b sea positivo o negativo, y la igualdad (3) es

$$0x = -b'y.$$

Como $b \neq 0$, esto nos dice que $y = 0$. Por otro lado, es claro que $x = b't$ para exactamente un entero t , a saber, para $t = b'x$. Vemos así que ahora (x, y) es el par $(b't, -a't)$, con t otra vez completamente determinado.

Concluimos así que en cualquier caso toda solución (x, y) de la ecuación (2) es de la forma $(b't, -a't)$ para exactamente un valor de $t \in \mathbb{Z}$. Por otro lado, si $t \in \mathbb{Z}$ y ponemos $x = b't$ e $y = -a't$, entonces

$$ax + by = da'b't - db'a't = 0,$$

así que el par (x, y) es una solución de la ecuación (2). Esto prueba la primera parte de la proposición.

Veamos ahora la segunda: supongamos que $d = 0$. Esto implica, como sabemos, que $a = b = 0$, y es evidente que todo par (x, y) de \mathbb{Z}^2 es solución de la ecuación (2). \square

Capítulo 9

Números primos

§9.1. Números primos

9.1.1. Si a es un entero, llamamos a todo número $b \in \mathbb{Z}$ tal que $b \mid a$ un *divisor* de a . De acuerdo a la Proposición 6.1.4, si a es distinto de 0 y b es un divisor de a , entonces $|b| \leq |a|$. Esto implica que si queremos buscar los divisores de un número a no nulo basta buscarlos entre los elementos del conjunto $\{i \in \mathbb{Z} : -a \leq i \leq a\}$. Esto es importante, ya que este conjunto es *finito*: para encontrar todos los divisores de a hay que hacer un número finito de cálculos.

Si a es positivo, entonces a tiene por lo menos a 1 y a a como divisores positivos. Una consecuencia inmediata de esto es que el único entero positivo que tiene exactamente *un* divisor positivo es 1: todos los otros enteros positivos tienen al menos dos.

Decimos que un número entero positivo p es *primo* cuando tiene exactamente *dos* divisores positivos. Un entero positivo mayor que 1 que no es primo es *compuesto*. Observemos que el entero 1 no es ni primo ni compuesto.

9.1.2. Para determinar si un entero $a > 1$ es primo, hay que verificar en principio que ningún entero b tal que $1 < b < a$ divide a a . El siguiente resultado implica que basta verificar que ningún *primo* p tal que $1 < p < a$ divide a a .

Proposición. *Un entero positivo mayor que 1 es o primo o divisible por un número primo menor que él.*

Una forma equivalente de decir esto es que todo un número mayor que 1 que tiene por lo menos tres divisores tiene uno que es primo.

Demostración. Para cada entero n sea $P(n)$ la afirmación « n es primo o divisible por un número primo menor que él» y mostremos por inducción que $P(n)$ vale para todo entero $n \geq 2$.

El número 2 es primo, ya que ningún entero b tal que $1 < b < 2$ lo divide: de hecho, no hay ningún entero que satisfaga ni siquiera la primera de esas condiciones. Vemos así que la afirmación $P(2)$ vale y esto nos da el paso inicial de la inducción.

Supongamos ahora que k es un entero tal que $k \geq 2$ y que las afirmaciones $P(2), P(3), \dots, P(k-1)$ valen. Si k es primo, entonces $P(k)$ vale. Si en cambio k no es primo, como es mayor que 1 tiene más que dos divisores positivos: esto implica que tiene un divisor positivo l distinto de 1 y de k . Por supuesto, esto implica que $1 < l < k$ y entonces nuestra hipótesis inductiva nos dice que la afirmación $P(l)$ vale.

Si l es primo, entonces como l es un primo menor que k , vemos que $P(k)$ vale. Si en cambio l no es primo, la validez de $P(l)$ implica que existe un primo p menor que l tal que $p \mid l$. Como $l \mid k$, gracias a transitividad de la divisibilidad tenemos que $p \mid k$: vemos así que p es un primo que divide a k y, como es menor que l , es menor que k .

En cualquier caso, se tiene que $P(k)$ vale. Esto completa la inducción. \square

9.1.3. Un corolario inmediato pero útil de la proposición que acabamos de probar es:

Corolario. *Todo entero mayor que 1 es divisible por un número primo.*

Demostración. En efecto, de acuerdo a la proposición un número entero mayor que 1 es primo o tiene un divisor primo menor que él: en cualquiera de los dos casos tiene un divisor primo. \square

9.1.4. Apoyándonos en la Proposición **9.1.2**, podemos describir un algoritmo para obtener la lista de los números primos menores que un número entero positivo dado N . Empezamos escribiendo la lista en orden de los números enteros desde el 2 hasta N . A medida que vayamos avanzando, vamos a ir tachando alguno de estos números y marcando otros con un círculo. Llevaremos a cabo el siguiente paso repetidas veces, mientras podamos:

encerramos con un círculo el primer número de la lista que no esté ni tachado ni encerrado con un círculo y a continuación tacharemos todos los números más grandes que él y que son sus múltiplos.

El procedimiento se detiene cuando no podamos realizar esto: cuando no quede ningún número que no esté ni tachado ni encerrado en un círculo.

Veamos cómo funciona esto cuando N es 59. Empezamos con la lista de los números

de 2 al 59:

2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19
20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39
40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59

El primer paso es localizar el primer número de la lista que no está ni tachado ni encerrado en un círculo: como no hay ninguno tachado ni marcado con un círculo, es claro que se trata del 2. Ahora encerramos al 2 con un círculo y tachamos todos sus múltiplos: nos queda

$\textcircled{2}$ 3 ~~4~~ 5 ~~6~~ 7 ~~8~~ 9 ~~10~~ 11 ~~12~~ 13 ~~14~~ 15 ~~16~~ 17 ~~18~~ 19
~~20~~ ~~21~~ ~~22~~ 23 ~~24~~ 25 ~~26~~ 27 ~~28~~ 29 ~~30~~ 31 ~~32~~ 33 ~~34~~ 35 ~~36~~ 37 ~~38~~ 39
~~40~~ 41 ~~42~~ 43 ~~44~~ 45 ~~46~~ 47 ~~48~~ 49 ~~50~~ 51 ~~52~~ 53 ~~54~~ 55 ~~56~~ 57 ~~58~~ 59

En este momento, el primer número que no está ni tachado ni encerrado en un círculo es el 3, así que lo encerramos en un círculo y tachamos sus múltiplos:

$\textcircled{2}$ $\textcircled{3}$ ~~4~~ 5 ~~6~~ 7 ~~8~~ ~~9~~ ~~10~~ 11 ~~12~~ 13 ~~14~~ ~~15~~ ~~16~~ 17 ~~18~~ 19
~~20~~ ~~21~~ ~~22~~ 23 ~~24~~ 25 ~~26~~ ~~27~~ ~~28~~ 29 ~~30~~ 31 ~~32~~ ~~33~~ ~~34~~ 35 ~~36~~ 37 ~~38~~ ~~39~~
~~40~~ 41 ~~42~~ 43 ~~44~~ ~~45~~ ~~46~~ 47 ~~48~~ 49 ~~50~~ ~~51~~ ~~52~~ 53 ~~54~~ 55 ~~56~~ ~~57~~ ~~58~~ 59

Observemos que al tachar los múltiplos de 3 volvimos a tachar algunos números que ya estaban tachados, como el 6 o el 12. Para el tercer paso, el primer entero libre es el 5 y lo que nos queda después de encerrarlo en un círculo y tachar sus múltiplos es

$\textcircled{2}$ $\textcircled{3}$ ~~4~~ $\textcircled{5}$ ~~6~~ 7 ~~8~~ ~~9~~ ~~10~~ 11 ~~12~~ 13 ~~14~~ ~~15~~ ~~16~~ 17 ~~18~~ 19
~~20~~ ~~21~~ ~~22~~ 23 ~~24~~ ~~25~~ ~~26~~ ~~27~~ ~~28~~ 29 ~~30~~ 31 ~~32~~ ~~33~~ ~~34~~ ~~35~~ ~~36~~ 37 ~~38~~ ~~39~~
~~40~~ 41 ~~42~~ 43 ~~44~~ ~~45~~ ~~46~~ 47 ~~48~~ 49 ~~50~~ ~~51~~ ~~52~~ 53 ~~54~~ ~~55~~ ~~56~~ ~~57~~ ~~58~~ 59

Continuamos de esta forma: en sucesivos pasos encerramos en círculos al 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, y al 59, tachando en cada paso los múltiplos de estos números. Al terminar de hacer eso, lo que tenemos es:

$\textcircled{2}$ $\textcircled{3}$ ~~4~~ $\textcircled{5}$ ~~6~~ $\textcircled{7}$ ~~8~~ ~~9~~ ~~10~~ $\textcircled{11}$ ~~12~~ $\textcircled{13}$ ~~14~~ ~~15~~ ~~16~~ $\textcircled{17}$ ~~18~~ $\textcircled{19}$
~~20~~ ~~21~~ ~~22~~ $\textcircled{23}$ ~~24~~ ~~25~~ ~~26~~ ~~27~~ ~~28~~ $\textcircled{29}$ ~~30~~ $\textcircled{31}$ ~~32~~ ~~33~~ ~~34~~ ~~35~~ ~~36~~ $\textcircled{37}$ ~~38~~ ~~39~~
~~40~~ $\textcircled{41}$ ~~42~~ $\textcircled{43}$ ~~44~~ ~~45~~ ~~46~~ $\textcircled{47}$ ~~48~~ ~~49~~ ~~50~~ ~~51~~ ~~52~~ $\textcircled{53}$ ~~54~~ ~~55~~ ~~56~~ ~~57~~ ~~58~~ $\textcircled{59}$

```

primos :: Integer -> [Integer]
primos n = cribar [2..n]

cribar :: [Integer] -> [Integer]
cribar [] = []
cribar (x : xs) = x : cribar [i | i <- xs, i `mod` x /= 0]

```

Figura 9.1. Un implementación de la criba de Eratóstenes en HASKELL. La expresión `primos n` se evalúa a la lista creciente de los primos menores o iguales que `n`. Es interesante observar que con estas definiciones, la expresión `cribar [2..]` se evalúa a la lista de *todos* los primos y entonces, por ejemplo, podemos calcular `takeWhile (<1000) (cribar [2..])` para determinar la lista de los primos menores que 1000 y `cribar [2..] !! 100` para determinar el centésimo primo.

Como ya no quedan números que no estén ni tachados ni encerrados en un círculo, el algoritmo termina. Los números que quedaron encerrados en círculos son

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59

y éstos son precisamente los números primos menores o iguales a 59.

Este procedimiento se llama la *criba*¹ de Eratóstenes, por Eratóstenes de Cirena (276 a.C.–195 a.C., Grecia), a quien se le atribuye desde principios de la era cristiana su invención. Eratóstenes llegó a ser el bibliotecario de la Biblioteca de Alejandría, en Egipto. Su más célebre logro es la determinación de la circunferencia de la Tierra “sin haber salido de su biblioteca”.

En la Figura 9.1 damos una posible implementación de este algoritmo en HASKELL.

9.1.5. Imaginemos que empezamos con la lista infinita de *todos* los enteros mayores que 1 y realizamos el proceso de cribado tal cual como lo describimos arriba: al comenzar cada paso, identificamos el primer entero de la lista que no está ni tachado ni encerrado en un círculo, lo encerramos en un círculo y tachamos todos sus (¡infinitos!) múltiplos. Una cosa que podría ocurrir, *a priori*, es que lleguemos a un punto —después de realizar un cierto número de pasos— en el que no podamos continuar porque ya no quedan números que no estén ni tachados ni encerrados en círculos y, entonces, no podamos realizar el paso siguiente.

¹La palabra *criba* designa el utensilio que se usa para cribar, es decir, para filtrar y seleccionar semillas o minerales.

Si esto ocurriera, en ese momento tendríamos un número finito de números encerrados en círculos (ya que en cada uno de los pasos que sí pudimos hacer en encerramos exactamente un número en un círculo) y todos los otros números estarían tachados. Claramente, esto nos diría que hay un número finito de números primos.

Una observación fundamental —debida a Euclides— es que esto no ocurre:

Proposición. *Existen infinitos números primos.*

Así, el proceso de cribado de la lista de todos los enteros mayores que 1 nunca se detiene. La demostración que daremos es, de hecho, debida a Euclides mismo.

Demostración. Supongamos que, por el contrario, hay un número finito de números primos, sea

$$p_1, p_2, \dots, p_m \tag{1}$$

la lista de todos ellos y consideremos el número $N = p_1 \cdots p_m + 1$. Como los números primos son todos positivos, es claro que $N > 1$ y la Proposición 9.1.2 nos dice entonces que N tiene un divisor primo. Ese divisor primo tiene que ser uno de los números de la lista (1), así que existe $i \in \{1, \dots, m\}$ tal que $p_i \mid p_1 \cdots p_m + 1$. Como claramente p_i también divide al producto $p_1 \cdots p_m$, el Corolario 6.1.6 nos dice que p_i divide a 1: esto es, por supuesto, absurdo. Esta contradicción muestra que nuestra hipótesis es insostenible y, por lo tanto, que el conjunto de los números primos es infinito, como afirma la proposición. \square

9.1.6. Otra consecuencia importante de la Proposición 9.1.2 es:

Proposición. *Todo entero positivo es igual a un producto de números primos.*

Demostración. Para cada $n \in \mathbb{N}$ sea $P(n)$ la afirmación «el número n es igual a un producto de números primos». Mostremos que $P(n)$ vale para todo $n \in \mathbb{N}$ por inducción. Que $P(1)$ vale es claro, ya que 1 es igual al producto de cero factores primos, y esto establece el paso base.

Supongamos ahora que $k \in \mathbb{N}$ y que las afirmaciones $P(1), \dots, P(k-1)$ valen, y mostremos que entonces también vale $P(k)$. Ahora bien, si k es primo, entonces es claro que $P(k)$ vale, ya que k es igual a un producto de números primos con un sólo factor. Si en cambio k no es primo, entonces la Proposición 9.1.2 nos dice que hay un número primo p menor k tal que $p \mid k$. Hay entonces un entero positivo l tal que $k = pl$ y claramente $1 \leq l < k$, ya que

$$l = \frac{k}{p} \leq \frac{k}{2} < k$$

porque $p \geq 2$. Ahora bien, como $1 \leq l < k$, nuestra hipótesis inductiva nos dice que la afirmación $P(l)$ vale, es decir, que l es igual a un producto de números primos, esto es, que existe $r \in \mathbb{N}_0$ y números primos p_1, \dots, p_r tales que $l = p_1 \cdots p_r$. Como entonces tenemos que $k = pl = pp_1 \cdots p_r$, vemos que k es igual a un producto de números primos, es decir, que $P(k)$ vale. Esto completa la inducción. \square

§9.2. El Teorema Fundamental de la Aritmética

9.2.1. En la sección anterior probamos la Proposición 9.1.6, que nos dice que todo entero positivo es igual a un producto de números primos. Nuestro objetivo en ésta es mostrar que, de hecho, ese producto de primos es esencialmente único.

9.2.2. El primer paso es establecer la siguiente caracterización de los números primos, usualmente conocida como el Lema de Euclides —es, de hecho, la Proposición 30 del libro VII de sus *Elementos*.

Proposición. *Un número p mayor que 1 es primo si cada vez que divide al producto de dos enteros divide a alguno de los dos factores.*

Demostración. Veamos primero que la condición del enunciado es necesaria. Sea p un entero mayor que 1 que es primo, sean a y b dos enteros tales que p divide a ab , supongamos que p no divide a a y mostremos que entonces p necesariamente divide a b . El máximo común divisor de p y a es 1: en efecto, si d es un divisor común positivo de p y a , entonces en particular divide a p y, como p es primo, es o bien 1 o bien p , pero como estamos suponiendo que p no divide a a , esta segunda posibilidad no ocurre.

De acuerdo a la identidad de Bézout 6.4.9, existen entonces enteros x e y tales que $xp + ya = 1$. Si multiplicamos esta igualdad por b , vemos que $xpb + yab = b$. Como p divide tanto a xpb como a yab , deducimos de esto que p divide a b , como queríamos.

En segundo lugar, probemos que la condición del enunciado es suficiente para que p sea primo. Esto es, supongamos que p es un entero mayor que 1 tal que cada vez que divide a un producto de dos enteros divide a uno de los factores y mostremos que p debe ser entonces primo.

Supongamos para ello que, por el contrario, p no es primo. En ese caso, como es mayor que 1, posee un divisor d tal que $1 < d < p$. Si e es el cociente de la división de p por d , tenemos entonces que $p = de$. En particular, vemos que p divide al producto de y, de acuerdo a la hipótesis, divide entonces a alguno de los factores: esto es absurdo,

ya que $1 < d < p$ y $1 < e < p$. Esta contradicción provino de haber supuesto que p no es primo, así que debe serlo. Esto completa la prueba de la proposición. \square

9.2.3. La siguiente generalización de la proposición anterior nos será útil:

Corolario. Sea p un número primo, sea $r \in \mathbb{N}$ y sean $a_1, \dots, a_r \in \mathbb{Z}$. Si p divide al producto $a_1 \cdots a_r$, entonces existe $i \in \{1, \dots, r\}$ tal que p divide a a_i .

Demostración. Para cada $r \in \mathbb{N}$ sea $P(r)$ la afirmación

si p divide a un producto $a_1 \cdots a_r$ de r enteros a_1, \dots, a_r , entonces existe $i \in \{1, \dots, r\}$ tal que p divide a a_i .

Que $P(1)$ vale es evidente. Supongamos, para hacer inducción, que $k \in \mathbb{N}$ y que $P(k)$ vale, y mostremos que entonces $P(k+1)$ también vale: esto probará el corolario.

Sean entonces a_1, \dots, a_{k+1} enteros, supongamos que p divide al producto $a_1 \cdots a_{k+1}$ y mostremos que p divide a alguno de los $k+1$ factores. Ahora bien, si llamamos b al producto $a_1 \cdots a_k$, entonces tenemos que p divide a ba_{k+1} : de acuerdo a la Proposición 9.2.2, se sigue de esto que p divide a b o a a_{k+1} . Si la segunda de estas posibilidades ocurre, entonces claramente p divide a uno de los factores del producto $a_1 \cdots a_{k+1}$. Si en cambio p divide a $b = a_1 \cdots a_k$, entonces la hipótesis inductiva nos dice que p divide a alguno de los factores a_1, \dots, a_k de b . En cualquier caso, vemos que la afirmación $P(k+1)$ vale, como queríamos. \square

9.2.4. De acuerdo a la Proposición 9.1.6, un entero positivo n es igual a un producto de números primos, esto es, existen $r \in \mathbb{N}_0$ y números primos p_1, p_2, \dots, p_r tales que

$$n = p_1 \cdots p_r. \tag{2}$$

Los números primos que aparecen en esta factorización no son necesariamente distintos. De todas formas, como la multiplicación de enteros es conmutativa, reindexándolos apropiadamente podemos suponer que tenemos que $p_1 \leq p_2 \leq \dots \leq p_r$. Mostraremos ahora que, bajo esta condición extra, hay exactamente una factorización como (2) de n .

9.2.5. Proposición. Si $r, s \in \mathbb{N}_0$ y p_1, \dots, p_r y q_1, \dots, q_s son números primos tales que $p_1 \leq \dots \leq p_r, q_1 \leq \dots \leq q_s$ y

$$p_1 \cdots p_r = q_1 \cdots q_s,$$

entonces $r = s$ y $p_i = q_i$ para cada $i \in \{1, \dots, r\}$.

Demostración. Para cada $n \in \mathbb{N}$ sea $P(n)$ la afirmación

Si $r, s \in \mathbb{N}_0$ y p_1, \dots, p_r y q_1, \dots, q_s son números primos tales que $p_1 \leq \dots \leq p_r, q_1 \leq \dots \leq q_s$ y $n = p_1 \cdots p_r = q_1 \cdots q_s$, entonces $r = s$ y $p_i = q_i$ para cada $i \in \{1, \dots, r\}$

Vamos a mostrar que $P(n)$ vale cualquiera sea $n \in \mathbb{N}$ haciendo inducción.

Empecemos por $P(1)$. Supongamos que $r, s \in \mathbb{N}_0$ y p_1, \dots, p_r y que q_1, \dots, q_s son números primos tales que $p_1 \leq \dots \leq p_r, q_1 \leq \dots \leq q_s$ y $1 = p_1 \cdots p_r = q_1 \cdots q_s$. Si $r > 1$, entonces p_1 evidentemente divide al producto $p_1 \cdots p_r$, que es igual a 1: esto es absurdo y esta contradicción nos dice que debe ser $r = 0$. De manera similar podemos ver que $s = 0$ y, por lo tanto, tenemos que $r = s$ y, de manera tautológica, que $p_i = q_i$ para todo $i \in \{1, \dots, r\}$. Concluimos de esta forma que la afirmación $P(1)$ vale.

Sera ahora $k \in \mathbb{N}$, supongamos que para cada entero i tal que $1 \leq i < k$ la afirmación $P(i)$ vale y mostremos que entonces la afirmación $P(k)$ también vale. Para ello, supongamos que $r, s \in \mathbb{N}_0$ y que p_1, \dots, p_r y q_1, \dots, q_s son números primos tales que $p_1 \leq \dots \leq p_r, q_1 \leq \dots \leq q_s$ y

$$k = p_1 \cdots p_r = q_1 \cdots q_s. \quad (3)$$

No puede ser que se tenga que $p_r < q_s$. En efecto, como claramente q_s divide a k y $k = p_1 \cdots p_r$, el Corolario 9.2.3 nos dice que existe $i \in \{1, \dots, r\}$ tal que q_s divide a p_i : esto es imposible, ya que de acuerdo a la Proposición 6.1.4 se tiene entonces que $q_s \leq p_i \leq p_r < q_s$.

De manera similar podemos ver que no puede ser que se tenga que $p_r > q_s$, y concluir, en definitiva, que $p_r = q_s$. Si ponemos $l = k/p_r$, de la igualdad (3) deducimos, dividiendo en cada miembro por p_r , que

$$l = p_1 \cdots p_{r-1} = q_1 \cdots q_{s-1}. \quad (4)$$

Ahora bien, l es un entero positivo estrictamente menor que k (porque $p_r \geq 2$), así que nuestra hipótesis inductiva nos dice que la afirmación $P(l)$ vale. Usándola en (4), vemos que $r - 1 = s - 1$, es decir, que $r = s$, y que $p_i = q_i$ para cada $i \in \{1, \dots, r - 1\}$. Junto con el hecho que ya establecimos antes de que $p_r = q_r$, esto muestra que vale la afirmación $P(k)$, como queríamos. \square

9.2.6. Podemos ahora enunciar y probar el llamado Teorema Fundamental de la Aritmética:

Proposición. Si $n \in \mathbb{N}$, entonces existe $r \in \mathbb{N}_0$, números primos p_1, \dots, p_r y enteros positivos a_1, \dots, a_r tales que $p_1 < \dots < p_r$ y $n = p_1^{a_1} \cdots p_r^{a_r}$ y, más aún, r , los primos p_1, \dots, p_r y los exponentes a_1, \dots, a_r están unívocamente determinados por n .

Demostración. Sea $n \in \mathbb{N}$. De la Proposición 9.1.6 sabemos que existen $s \in \mathbb{N}_0$ y números primos q_1, \dots, q_s tales que $n = p_1 \cdots p_s$. Más aún, como observamos en 9.2.4, podemos suponer sin pérdida de generalidad que $q_1 \leq \dots \leq q_s$, ya que si no es ése el caso basta reindexar apropiadamente los primos q_1, \dots, q_s .

Los primos q_1, \dots, q_s no son necesariamente distintos dos a dos. Sea r la cantidad de elementos del conjunto $\{q_1, \dots, q_s\}$, sean p_1, \dots, p_r los elementos de este conjunto listados en orden estrictamente creciente y para cada $i \in \{1, \dots, r\}$ sea a_i la cantidad de veces que el primo p_i aparece en la lista q_1, \dots, q_s , es decir, el cardinal del conjunto $\{j \in \{1, \dots, s\} : q_j = p_i\}$. Es claro, entonces, que

$$n = q_1 \cdots q_s = \underbrace{p_1 \cdots p_1}_{a_1 \text{ factores}} \underbrace{p_2 \cdots p_2}_{a_2 \text{ factores}} \cdots \underbrace{p_r \cdots p_r}_{a_r \text{ factores}} = p_1^{a_1} \cdots p_r^{a_r}.$$

Esto prueba la afirmación de existencia de la proposición.

Para ver la de unicidad, supongamos que $r, s \in \mathbb{N}_0$, que p_1, \dots, p_r y q_1, \dots, q_s son dos secuencias estrictamente crecientes de números primos, y que $a_1, \dots, a_r, b_1, \dots, b_s \in \mathbb{N}$ son tales que

$$n = p_1^{a_1} \cdots p_r^{a_r} = q_1^{b_1} \cdots q_s^{b_s}.$$

Podemos reescribir esta última igualdad en la forma

$$\underbrace{p_1 \cdots p_1}_{a_1 \text{ factores}} \cdots \underbrace{p_r \cdots p_r}_{a_r \text{ factores}} = \underbrace{q_1 \cdots q_1}_{b_1 \text{ factores}} \cdots \underbrace{q_s \cdots q_s}_{b_s \text{ factores}}.$$

A la izquierda tenemos un producto de $a_1 + \dots + a_r$ números primos y los factores están en orden no decreciente, mientras que a la derecha tenemos un producto de $b_1 + \dots + b_s$ números primos también listados en orden no decreciente. De acuerdo a la Proposición 9.1.6, entonces, a ambos lados de la igualdad tenemos la misma cantidad de factores, así que $a_1 + \dots + a_r = b_1 + \dots + b_s$, y los factores son los mismos en el mismo orden. Es inmediato entonces que $r = s$ y que $p_i = q_i$ y $a_i = b_i$ para cada $i \in \{1, \dots, r\}$. La proposición queda así probada. \square

9.2.7. A pesar de que este Teorema Fundamental de la Aritmética es en efecto fundamental, fue recién Gauss en 1801, en sus *Disquisitiones Arithmeticae*, el primero en enunciarlo precisamente y probarlo. El teorema no aparece en los *Elementos* de Euclides: aunque ciertamente aparecen ahí nuestro Corolario 9.1.3, que us para probar la existencia de una factorización en factores primos, y nuestra Proposición 9.2.2, que está en la base de nuestro argumento para probar la unicidad, ninguna de estas dos partes de la Proposición 9.2.6 puede leerse en los *Elementos*.

Luego de Euclides, el siguiente en ocuparse de la cuestión fue Kamāl al-Dīn al-Fārisī, un gran matemático, físico y astrónomo persa que murió hacia 1320. al-Fārisī escribió

THEOREMA. *Numerus compositus quicumque unico tantum modo in factores primos resolvi potest.*

Dem. Quemvis numerum compositum in factores primos resolvi posse, ex elementis constat, sed pluribus modis diversis fieri hoc non posse perperam plerumque supponitur tacite. Fingamus numerum compositum A , qui sit $= a^\alpha b^\beta c^\gamma$ etc., designantibus a, b, c etc. numeros primos inaequales, alio adhuc modo in factores primos esse resolubilem. Primo manifestum est. in secundum hoc factorum systema alios primos quam a, b, c etc. ingredi non posse, quum quicumque alius primus numerum A ex his compositum metiri nequeat. Similiter etiam in secundo hoc factorum systemate nullus primorum a, b, c etc. deesse potest, quippe qui alias ipsum A non metiretur (art. praec.). Quare hae binae in factores resolutiones in eo tantummodo differre possunt, quod in altera aliquis primus pluries quam in altera habeatur. Sit talis primus p , qui in altera resolutione m , in altera vero n vicibus occurrat, sitque $m > n$: Iam deleatur ex utroque systemate factor p , n vicibus, quo fiet ut in altero adhuc $m - n$ vicibus remaneat, ex altero vero omnino abierit. I. e. numeri $\frac{A}{p^n}$ duae in factores resolutiones habentur, quarum altera a factore p prorsus libera, altera vero $m - n$ vicibus eum continet, contra ea quae modo demonstravimus.

Figura 9.2. El párrafo 16 de las *Disquisitiones Arithmeticae* de Gauss, en el que enuncia y prueba el Teorema Fundamental de la Aritmética. El enunciado dice: «Todo número compuesto puede resolverse en factores primos de una única manera».

un libro sobre los “números amigos” en el que aparece el primer enunciado y la primera prueba de la afirmación de existencia de factorizaciones con factores primos de la que se tiene registro. Después de él, Jean Prestet en 1689, Leonard Euler en 1770 y Adrien-Marie Legendre en 1798 hicieron ciertos avances en el estudio de estas factorizaciones pero no llegaron a enunciar ni probar la afirmación de unicidad, aunque la usaron implícitamente. Como dijimos, el teorema aparece en toda su gloria recién en 1801 en las *Disquisitiones Arithmeticae*, donde Gauss lo enuncia esencialmente igual que nosotros y lo prueba de una manera muy parecida a la nuestra, aunque con menos detalles. En la Figura 9.2 reproducimos el pasaje relevante.

En el trabajo [AÖ2001] puede encontrarse una descripción detallada de la historia de la Proposición 9.2.6 y en [AÖ1997] una revista de las muchas pruebas que han sido dadas de ella.

9.2.8. Si uno tiene acceso a la lista de los números primos menores que un entero

positivo n , es fácil —aunque laborioso— encontrar la factorización de n como producto de números primos. Basta ir recorriendo la lista de los primos desde en 2 e adelante y para cada uno de ellos determinar cuántas veces lo divide. Una simplificación de este proceso consiste en observar que cada vez que encontramos un primo que lo divide, es suficiente continuar buscando una factorización del correspondiente cociente.

Por ejemplo, supongamos que queremos factorizar el entero 29 822 375. Los primos primos son

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, ...

Probamos dividir nuestro número por 2 y por 3, sin éxito. Es divisible por 5, y el cociente es 5 964 475; éste es otra vez divisible por 5, con cociente 1 192 895, y éste también, con cociente 238 579. Ya 5 no divide a este número: probamos entonces con 7, que no lo divide, y con 11, que sí funciona. El cociente es 21 689. Este número no es divisible por 11, así que continuamos probando con 13, 17 y 19, que no lo dividen, y con 23, que sí lo hace. El cociente es 943, que es otra vez divisible por 23, con cociente 41. Como 41 es primo, aquí termina el proceso. Concluimos así que la factorización que buscábamos es $29\,822\,375 = 5^3 \cdot 11 \cdot 23^2 \cdot 41$.

29 822 375	5
5 964 475	5
1 192 895	5
238 579	11
21 689	23
943	23
41	41
1	

En la Figura 9.3 en la página siguiente damos una implementación en HASKELL de este algoritmo. Con esas definiciones, podemos evaluar en un intérprete

```
*Main> factorizar 29822375
[5,5,5,11,23,23,41]
*Main> pares 29822375
[(5,3),(11,1),(23,2),(41,1)]
```

El primer resultado nos da la lista de primos con repeticiones que aparecen en la factorización de 29 822 375 mientras que el segundo nos da los pares (p, a) de primos y exponentes que aparecen en esa factorización.

```

factorizar :: Integer -> [Integer]
factorizar n = reducir n (primos n)

reducir :: Integer -> [Integer] -> [Integer]
reducir 1 (p : ps) = []
reducir x (p : ps)
  | x `mod` p == 0 = p : reducir (x `div` p) (p : ps)
  | otherwise     = reducir x ps

pares :: Integer -> [(Integer, Integer)]
pares n = [(p, count p factores) | p <- nub factores]
  where factores = factorizar n
        count x ys = length [y | y <- ys, y == x]

sigma :: Integer -> Integer -> Integer
sigma 0 n = product [a + 1 | (p,a) <- pares n]
sigma k n = product [f (p, a) | (p, a) <- pares n]
  where f (p, a) = (p ^ (k * (a+1)) - 1) `div` (p ^ k - 1)

```

Figura 9.3. Una implementación en HASKELL de la factorización de un entero positivo como producto de números primos y de las funciones σ_k de la sección 9.4, usando las definiciones de la Figura 9.1 en la página 178.

§9.3. Valuaciones

9.3.1. Fijemos un número primo p y sea n un entero no nulo. Si $k \in \mathbb{N}_0$ es tal que p^k divide a n , entonces $p^k \leq |n|$ y, por lo tanto, $k \leq \log_p |n|$. Esto implica que el conjunto

$$V_p(n) = \{k \in \mathbb{N}_0 : p^k \mid n\}$$

está contenido en $\{0, \dots, \lfloor \log_p |n| \rfloor\}$ y es, en consecuencia, finito. Como además no es vacío, tiene sentido entonces considerar su máximo elemento, al que escribimos $v_p(n)$ y llamamos la **valuación p -ádica** de n . Así, por ejemplo, $v_2(168) = 3$ y $v_5(50) = 2$.

9.3.2. Una observación inmediata que podemos hacer es:

Lema. Sea p un número primo. Si n es un entero no nulo, entonces

$$V_p(n) = \{k \in \mathbb{N}_0 : 0 \leq k \leq v_p(n)\}.$$

En otras palabras, una potencia entera p^k de p divide a n si y solamente si $0 \leq k \leq v_p(n)$. En particular, p divide a n si y solamente si $v_p(n) > 0$.

Demostración. En efecto, si k es un entero tal que $0 \leq k \leq v_p(n)$, entonces $p^k \mid p^{v_p(n)}$ y, como $p^{v_p(n)} \mid n$, tenemos que $p^k \mid n$, es decir, que $k \in V_p(n)$. Esto muestra que $\{k \in \mathbb{N}_0 : 0 \leq k \leq v_p(n)\} \subseteq V_p(n)$. Por otro lado, como $v_p(n)$ es el máximo elemento de $V_p(n)$, es claro que $V_p(n)$ está contenido en $\{k \in \mathbb{N}_0 : 0 \leq k \leq v_p(n)\}$. Vale, en definitiva, la igualdad del enunciado. \square

9.3.3. Podemos dar una caracterización alternativa sencilla de la valuación p -ádica:

Proposición. Sea p un número primo y sea n un entero no nulo.

- (i) Existe un entero n' no divisible por p tal que $n = p^{v_p(n)} n'$.
- (ii) Recíprocamente, si $k \in \mathbb{N}_0$ y $m \in \mathbb{Z}$ son tales que $n = p^k m$ y $p \nmid m$, entonces $k = v_p(n)$.

Demostración. (i) Como $v_p(n)$ es un elemento del conjunto $V_p(n)$, tenemos que $p^{v_p(n)} \mid n$ y, por lo tanto, que existe $n' \in \mathbb{Z}$ tal que $n = p^{v_p(n)} n'$.

Supongamos por un momento que p divide a n' , de manera que existe $n'' \in \mathbb{Z}$ tal que $n' = pn''$. En ese caso tenemos que $n = p^{v_p(n)+1} n''$ y, por lo tanto, que $p^{v_p(n)+1}$ divide a n , es decir, que $v_p(n) + 1 \in V_p(n)$: esto es imposible, ya que $v_p(n)$ es el mayor elemento del conjunto $V_p(n)$. Vemos así que necesariamente se tiene que $p \nmid n'$.

(ii) Sean $k \in \mathbb{N}_0$ y $m \in \mathbb{Z}$ tales que $n = p^k m$ y $p \nmid m$. Esto nos dice, en particular, que p^k divide a n , así que $k \in V_p(n)$ y, por lo tanto,

$$k \leq v_p(n), \tag{5}$$

ya que $v_p(n)$ es el mayor elemento de $V_p(n)$.

Supongamos que la desigualdad (5) es estricta, de manera que $k + 1 \leq v_p(n)$. Tenemos entonces que $p^{k+1} \mid p^{v_p(n)} \mid n = p^k m$, así que existe $u \in \mathbb{Z}$ tal que $p^k m = p^{k+1} u$. Esto implica que $p^k(m - pu) = 0$ y, como $p \neq 0$, que $m = pu$, es decir, que p divide a m : esto contradice a nuestra hipótesis.

Esta contradicción provino de suponer que la desigualdad (5) era estricta y podemos concluir entonces que $k = v_p(n)$, como afirma el enunciado. \square

9.3.4. Proposición. Sea p un número primo.

- (i) Si n es un entero no nulo, entonces $v_p(n) \in \mathbb{N}_0$ y

$$v_p(-n) = v_p(n).$$

- (ii) Si n y m son dos enteros no nulos, entonces nm no es nulo y

$$v_p(nm) = v_p(n) + v_p(m).$$

- (iii) Si n y m son dos enteros no nulos tales que $n + m \neq 0$, entonces

$$v_p(n + m) \geq \min\{v_p(n), v_p(m)\}.$$

Demostración. (i) Sea n un entero no nulo. Como $v_p(n)$ es el máximo elemento del conjunto finito $V_p(n)$ y éste está contenido en \mathbb{N}_0 , es evidente que $v_p(n) \geq 0$. Por otro lado, es evidente que $V_p(-n) = V_p(n)$, así que claramente $v_p(-n) = v_p(n)$.

(ii) Sean n y m dos enteros no nulos, de manera que en particular, $nm \neq 0$. La Proposición 9.3.3 nos dice que existen enteros n' y m' tales que $n = p^{v_p(n)}n'$, $m = p^{v_p(m)}m'$, $p \nmid n'$ y $p \nmid m'$. Se sigue de esto que

$$nm = p^{v_p(n)+v_p(m)}n'm'$$

y, gracias a la Proposición 9.2.2, que $p \nmid n'm'$. La segunda parte de la Proposición 9.3.3 nos permite entonces concluir que $v_p(nm) = v_p(n) + v_p(m)$.

(iii) Sean n y m dos enteros no nulos tales que $n + m \neq 0$ y consideremos el entero no negativo $k = \min\{v_p(n), v_p(m)\}$. Como $k \leq v_p(n)$ y $k \leq v_p(m)$, se tiene que p^k divide a n y a m : se sigue de eso que p^k divide a $n + m$ y, por lo tanto, que $k \in V_p(n + m)$. Como $v_p(n + m)$ es el máximo elemento de $V_p(n + m)$, vemos así que $k \leq v_p(n + m)$: esto es precisamente lo que afirma el enunciado. \square

9.3.5. Proposición. Sea n un número entero positivo. Si p_1, \dots, p_r son todos los números primos que dividen a n listados sin repeticiones, entonces

$$n = p_1^{v_{p_1}(n)} \cdots p_r^{v_{p_r}(n)}.$$

Demostración. Sea m el número que aparece a la derecha en la igualdad que queremos probar. Como los primos p_1, \dots, p_r son distintos dos a dos, son coprimos dos a dos y se sigue de la Proposición 6.5.8 que los números $p_1^{v_{p_1}(n)}, \dots, p_r^{v_{p_r}(n)}$ también son coprimos dos a dos. Cada uno de ellos divide a n , así que el Corolario 6.5.7 implica que su producto, el número m , también divide a n .

Sea q el cociente de la división de n por m , de manera que $n = qm$. Para probar la proposición será suficiente que mostremos que $q = 1$ y para esto, a su vez y en vista del Corolario 9.1.3, que ningún primo divide a q .

Sea p un número primo. Tenemos que

$$\begin{aligned} v_p(n) &= v_p(qm) \\ &= v_p(q) + v_p(m) \\ &= v_p(q) + v_p\left(p_1^{v_{p_1}(n)}\right) + \cdots + v_p\left(p_r^{v_{p_r}(n)}\right) \\ &= v_p(q) + v_{p_1}(n) \cdot v_p(p_1) + \cdots + v_{p_r}(n) \cdot v_p(p_r) \end{aligned}$$

Si p es distinto de todos los primos p_1, \dots, p_r , entonces por un lado tenemos que $v_p(n) = 0$ y, por otro, $v_p(p_i) = 0$ para todo $i \in \{1, \dots, r\}$, y esta igualdad nos dice que

$$0 = v_p(n) = v_p(q).$$

Si en cambio existe $j \in \{1, \dots, r\}$ tal que $p = p_j$, entonces $v_p(n) = v_{p_j}(n)$, $v_p(p_j) = 1$ y $v_p(p_i) = 0$ para todo $i \in \{1, \dots, r\} - \{j\}$, así que la igualdad a la que llegamos nos dice que

$$v_{p_j}(n) = v_p(q) + v_{p_j}(n).$$

En cualquier caso, entonces, vemos que $v_p(q) = 0$, es decir, que p no divide a q . Esto completa la prueba. \square

9.3.6. Proposición. Sean n y m dos enteros. Una condición necesaria y suficiente para que n divida a m es que para todo número primo se tenga que $v_p(n) \leq v_p(m)$.

Demostración. Sean p_1, \dots, p_r los primos que dividen al producto n . De acuerdo a la Proposición 9.3.5 tenemos que

$$n = p_1^{v_{p_1}(n)} \cdots p_r^{v_{p_r}(n)}.$$

Supongamos primero que se cumple la condición del enunciado. Si $i \in \{1, \dots, r\}$, entonces $v_{p_i}(n) \leq v_{p_i}(m)$, así que $p_i^{v_{p_i}(n)} \mid m$. Como los números $p_1^{v_{p_1}(n)}, \dots, p_r^{v_{p_r}(n)}$ son coprimos dos a dos, el Corolario 6.5.7 nos permite deducir de eso que $n = p_1^{v_{p_1}(n)} \cdots p_r^{v_{p_r}(n)}$ también divide a m . La condición es por lo tanto suficiente para que n divida a m .

Para probar la necesidad, supongamos que n divide a m y sea p un número primo. Como $p^{v_p(n)}$ divide a n , la transitividad de la divisibilidad implica que también divide a m y, por lo tanto, que $v_p(n) \leq v_p(m)$: vemos así que la condición se satisface. \square

9.3.7. Proposición. Si n y m son dos enteros positivos y p_1, \dots, p_r son los primos que dividen a nm listados sin repeticiones, entonces

$$\text{mcd}(n, m) = p_1^{a_1} \cdots p_r^{a_r}$$

y

$$\text{mcm}(n, m) = p_1^{b_1} \cdots p_r^{b_r}$$

con $a_i = \min\{v_{p_i}(n), v_{p_i}(m)\}$ y $b_i = \max\{v_{p_i}(n), v_{p_i}(m)\}$ para cada $i \in \{1, \dots, r\}$.

Demostración. Sea $d = p_1^{a_1} \cdots p_r^{a_r}$ y para cada $i \in \{1, \dots, r\}$ pongamos

$$s_i = v_{p_i}(n) - a_i,$$

$$t_i = v_{p_i}(m) - a_i.$$

Observemos que s_i y t_i son enteros no negativos y que alguno de los dos es nulo. Consideremos, finalmente, los números $x = p_1^{s_1} \cdots p_r^{s_r}$ e $y = p_1^{t_1} \cdots p_r^{t_r}$. Se tiene que

$$xd = p_1^{s_1} \cdots p_r^{s_r} \cdot p_1^{a_1} \cdots p_r^{a_r} = p_1^{v_{p_1}(n)} \cdots p_r^{v_{p_r}(n)} = n,$$

ya que $a_i + s_i = v_{p_i}(n)$ para todo $i \in \{1, \dots, r\}$. De manera similar, es $yd = m$.

Por otro lado, es $\text{mcd}(x, y) = 1$. En efecto, sea f ese máximo común divisor. Si p es un primo y p divide a f , entonces p divide tanto a x como a y , por lo tanto, existe $i \in \{1, \dots, r\}$ tal que $p = p_i$, $s_i > 0$ y $t_i > 0$: esto es imposible, ya que alguno de los dos números s_i o t_i es nulo. Vemos así que ningún primo divide a f y, como f es un entero positivo, que $f = 1$.

Juntando todo, vemos que tenemos dos enteros coprimos x e y tales que $n = xd$ y $m = yd$. De acuerdo al Corolario 6.5.4(ii), podemos concluir que $d = \text{mcd}(n, m)$. Esto prueba la primera de las igualdades de la proposición.

Sea ahora $e = p_1^{b_1} \cdots p_r^{b_r}$. Tenemos que

$$\begin{aligned} d \cdot e &= p_1^{a_1} \cdots p_r^{a_r} \cdot p_1^{b_1} \cdots p_r^{b_r} \\ &= p_1^{a_1+b_1} \cdots p_r^{a_r+b_r} \\ &= p_1^{v_{p_1}(n)+v_{p_1}(m)} \cdots p_r^{v_{p_r}(n)+v_{p_r}(m)}, \end{aligned}$$

porque $a_i + b_i = v_{p_i}(n) + v_{p_i}(m)$ para todo $i \in \{1, \dots, r\}$, y esto es

$$\begin{aligned} &= p_1^{v_{p_1}(n)} \cdots p_r^{v_{p_r}(n)} \cdot p_1^{v_{p_1}(m)} \cdots p_r^{v_{p_r}(m)} \\ &= n \cdot m. \end{aligned}$$

Así, tenemos que $\text{mcd}(n, m) \cdot e = n \cdot m$ y, gracias al Ejercicio 6.6.2(c), podemos concluir que $e = \text{mcm}(n, m)$. \square

9.3.8. Proposición. Si n y m son dos enteros positivos, entonces existen enteros coprimos u y v tales que $\text{mcm}(n, m) = uv$, $u \mid n$ y $u \mid m$.

Demostración. Sean n y m dos enteros positivos y sean p_1, \dots, p_r los primos que dividen al producto nm , listados sin repeticiones. Para cada $i \in \{1, \dots, r\}$ sean

$$a_i = \begin{cases} v_{p_i}(n), & \text{si } v_{p_i}(n) \geq v_{p_i}(m); \\ 0, & \text{en caso contrario} \end{cases}$$

y

$$b_i = \begin{cases} v_{p_i}(m), & \text{si } v_{p_i}(n) < v_{p_i}(m); \\ 0, & \text{en caso contrario.} \end{cases}$$

y consideremos los enteros $u = p_1^{a_1} \cdots p_r^{a_r}$ y $v = p_1^{b_1} \cdots p_r^{b_r}$. Para todo $i \in \{1, \dots, r\}$ tenemos que

- $v_{p_i}(u) = a_i \leq v_{p_i}(m)$ y $v_{p_i}(v) = b_i \leq v_{p_i}(m)$,
- $v_{p_i}(u) + v_{p_i}(v) = a_i + b_i = \max(v_{p_i}(n), v_{p_i}(m))$, y
- $\min\{v_{p_i}(u), v_{p_i}(v)\} = \min(a_i, b_i) = 0$.

De la primera de estas observaciones y la Proposición 9.3.6 vemos que $u \mid n$ y que $v \mid n$. De la segunda y de la tercera, usando la Proposición 9.3.7, que $\text{mcd}(u, v) = 1$ y que $uv = \text{mcm}(n, m)$. La proposición queda así probada. \square

§9.4. Sumas de divisores

9.4.1. Si n es un entero positivo, escribimos $\sigma_0(n)$ al número de los divisores positivos de n . Por ejemplo, los divisores positivos de 300 son

1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 25, 30, 50, 60, 75, 100, 150, 300

y, por lo tanto, $\sigma_0(300) = 18$.

Para calcular $\sigma_0(n)$, en principio, hay que determinar todos los divisores positivos de n , pero mostraremos más abajo en la Proposición 9.4.2 que es suficiente encontrar la factorización de n como producto de primos. Veamos antes un ejemplo.

La factorización de $n = 172772$ como producto de primos es $2^3 \cdot 3^2 \cdot 7^4$. Si d es un divisor positivo de n , entonces los primos que dividen a d necesariamente están entre 2, 3 y 7: esto significa que $d = 2^{a_1} \cdot 3^{a_2} \cdot 7^{a_3}$ para ciertos enteros no negativos a_1 , a_2 y a_3 . Más aún, como d divide a n , la Proposición 9.3.6 nos dice que

$$0 \leq a_1 \leq 3, \quad 0 \leq a_2 \leq 2, \quad 0 \leq a_3 \leq 4. \quad (6)$$

Por supuesto, el divisor d queda completamente determinado por estos tres exponentes y un momento de reflexión es suficiente para convencernos de que cualquier elección de tres enteros a_1 , a_2 y a_3 que satisfagan las condiciones (6) produce un divisor de n . Como hay 4 formas de elegir a a_1 , 3 de elegir a_2 y 5 de elegir a_3 , y dos elecciones distintas de estos exponentes producen divisores de n distintos —esto es consecuencia del Teorema Fundamental de la Aritmética— podemos concluir que n tiene $4 \cdot 3 \cdot 5 = 60$ divisores. Probaremos el resultado general siguiendo exactamente esta misma idea.

9.4.2. Proposición. Sea n un entero positivo, sean p_1, \dots, p_r los primos que dividen a n , de manera que se tiene $n = p_1^{v_{p_1}(n)} \cdots p_r^{v_{p_r}(n)}$. La cantidad de divisores positivos de n es

$$\sigma_0(n) = (v_{p_1}(n) + 1) \cdots (v_{p_r}(n) + 1).$$

Así, por ejemplo, como $300 = 2^2 \cdot 3 \cdot 5^2$, esta proposición nos dice que

$$\sigma_0(300) = (2 + 1)(1 + 1)(2 + 1) = 3 \cdot 2 \cdot 3 = 18.$$

Por supuesto, esto coincide con nuestro cálculo anterior.

Demostración. Consideremos para cada $i \in \{1, \dots, r\}$ el conjunto

$$I_i = \{t \in \mathbb{N}_0 : 0 \leq t \leq v_{p_i}(n)\}.$$

Si d es un divisor de n , entonces los primos que dividen a d son algunos de los primos p_1, \dots, p_r y, por lo tanto,

$$d = p_1^{v_{p_1}(d)} \cdots p_r^{v_{p_r}(d)}$$

Más aún, como d divide a n la Proposición 9.3.6 nos dice que $0 \leq v_{p_i}(d) \leq v_{p_i}(n)$ para todo $i \in \{1, \dots, r\}$. Esto significa que la r -upla $(v_{p_1}(d), \dots, v_{p_r}(d))$ es un elemento del producto cartesiano $I_1 \times \cdots \times I_r$.

Si escribimos $D(n)$ al conjunto de todos los divisores positivos de n , podemos definir entonces una función

$$\varphi : D(n) \rightarrow I_1 \times \cdots \times I_r$$

poniendo, para cada $d \in D$, $\varphi(d) = (v_{p_1}(d), \dots, v_{p_r}(d))$. Esta función es una biyección:

- Si (a_1, \dots, a_r) es un elemento de $I_1 \times \cdots \times I_r$, entonces podemos considerar el entero $e = p_1^{a_1} \cdots p_r^{a_r}$. Como los primos que dividen a e están entre p_1, \dots, p_r y para cada $i \in \{1, \dots, r\}$ se tiene evidentemente que $v_{p_i}(e) = a_i \leq v_{p_i}(n)$, la Proposición 9.3.6 nos dice que $e \in D(n)$. Como $\varphi(d)$ es precisamente la r -upla (a_1, \dots, a_r) con la que empezamos, esto muestra que la función φ es sobreyectiva.
- Supongamos, por otro lado, que d y e son dos elementos de $D(n)$ tales que $\varphi(d) = \varphi(e)$. Esto significa precisamente que

$$\text{para cada } i \in \{1, \dots, r\} \text{ se tiene que } v_{p_i}(d) = v_{p_i}(e). \quad (7)$$

Ahora bien, como d y e son divisores de n , los primos que los dividen están entre p_1, \dots, p_r , así que la Proposición 9.3.5 nos dice que $d = p_1^{v_{p_1}(d)} \cdots p_r^{v_{p_r}(d)}$ y $e = p_1^{v_{p_1}(e)} \cdots p_r^{v_{p_r}(e)}$. En vista de (7) es claro que los miembros derechos de estas dos igualdades coinciden, así que $d = e$. Vemos así que la función φ es inyectiva.

Como φ es biyectiva, tenemos que

$$|D(n)| = |I_1 \times \cdots \times I_r| = |I_1| \cdots |I_r| = (v_{p_1}(n) + 1) \cdots (v_{p_r}(n) + 1)$$

y esto es lo que afirma la proposición. \square

9.4.3. Decimos que un número $n \in \mathbb{N}$ es *altamente compuesto* si tiene más divisores que cualquier otro entero positivo menor que él. Usando la Proposición 9.4.2, es fácil ver (¡usando una computadora!) que los primeros números altamente compuestos son

$$1, 2, 4, 6, 12, 24, 36, 48, 60, 120, 180, 240, 360, 720, 840, 1260, 1680, 2520, 5040, \dots$$

Esta definición fue dada por Srinivasa Ramanujan en 1915 pero es probable que ya los griegos hayan considerado estos números. Platón, por ejemplo, explica en *Las Leyes* —el último y el más largo de sus diálogos, en el que expone sus ideas sobre como deben organizarse las sociedades— que el número ideal de ciudadanos² de una ciudad es 5040, precisamente porque este número tiene muchos divisores.

9.4.4. Además de la función σ_0 que definimos arriba, se estudian otras funciones de tipo similar. Si $k \in \mathbb{R}$, para cada $n \in \mathbb{N}$ escribimos $\sigma_k(n)$ a la suma de las potencias k -ésimas de n . Por ejemplo,

$$\sigma_3(24) = 1^3 + 2^3 + 3^3 + 4^3 + 6^3 + 8^3 + 12^3 + 24^3 = 16\,380.$$

Observemos que $d^0 = 1$ para todo entero positivo d , y entonces $\sigma_0(n)$ es simplemente la suma de muchos unos, uno por cada divisor de n y esto es lo mismo que el número de divisores que n tiene: vemos así que esta definición para σ_0 coincide con la que dimos en 9.4.1. Nos proponemos obtener un resultado similar al de la Proposición 9.4.2 para σ_k . Como el argumento que usamos para probar esa proposición es bastante flexible, haremos antes algunas consideraciones generales que nos servirán también más adelante.

9.4.5. Decimos que una función $f : \mathbb{N} \rightarrow A$ con valores en un subconjunto A de \mathbb{R} es *multiplicativa* si cada vez que n y m son enteros positivos coprimos se tiene que $f(nm) = f(n)f(m)$. Un ejemplo sencillo de esto es el siguiente: la función identidad $I_{\mathbb{N}} : \mathbb{N} \rightarrow \mathbb{N}$ es multiplicativa. Obtenemos otro ejemplo, un poco más interesante, fijando un entero a y considerando la función $f_a : n \in \mathbb{N} \mapsto \text{mcd}(n, a) \in \mathbb{N}_0$: que esta función es multiplicativa es precisamente lo que afirma la Proposición 6.5.5(iv).

9.4.6. Que una función sea multiplicativa nos da una forma de evaluarla en un producto de dos números coprimos. El siguiente resultado extiende esa propiedad a productos de un número arbitrario de factores.

²Para Platón no todos los habitantes de una ciudad son ciudadanos.

Lema. Sea $f : \mathbb{N} \rightarrow \mathbb{R}$ una función multiplicativa. Si $r \in \mathbb{N}$ y n_1, \dots, n_r son enteros positivos coprimos dos a dos, entonces $f(n_1 \cdots n_r) = f(n_1) \cdots f(n_r)$.

Demostración. Procedemos por inducción con respecto a r . Si r es 1, entonces no hay nada que probar, y si es 2, lo que se afirma es cierto precisamente por la definición de multiplicatividad.

Supongamos entonces que $r \geq 3$ y sean n_1, \dots, n_r enteros positivos coprimos dos a dos. De acuerdo al Corolario 6.5.6, tenemos que

$$\text{mcd}(n_1 \cdots n_{r-1}, n_r) = \text{mcd}(n_1, n_r) \cdots \text{mcd}(n_{r-1}, n_r) = 1,$$

porque n_r es coprimo con cada uno de los números n_1, \dots, n_{r-1} . Como la función f es multiplicativa, tenemos entonces que

$$f(n_1 \cdots n_r) = f(n_1 \cdots n_{r-1})f(n_r).$$

Ahora bien, la hipótesis inductiva nos dice que $f(n_1 \cdots n_{r-1}) = f(n_1) \cdots f(n_{r-1})$ y si usamos esto en la igualdad que acabamos de obtener vemos que

$$f(n_1 \cdots n_r) = f(n_1) \cdots f(n_r),$$

y esto completa la inducción. □

9.4.7. El interés de que una función $f : \mathbb{N} \rightarrow \mathbb{R}$ sea multiplicativa reduce en que podemos calcular su valor $f(n)$ en un número $n \in \mathbb{N}$ usando la factorización de n como producto de números primos:

Proposición. Sea $f : \mathbb{N} \rightarrow \mathbb{R}$ una función multiplicativa. Si $n \in \mathbb{N}$ y p_1, \dots, p_r son los primos que dividen a n , de manera que $n = p_1^{v_{p_1}(n)} \cdots p_r^{v_{p_r}(n)}$, entonces

$$f(n) = f(p_1^{v_{p_1}(n)}) \cdots f(p_r^{v_{p_r}(n)}).$$

Demostración. Sea $n \in \mathbb{N}$ y sean p_1, \dots, p_r los primos que dividen a n . Como los números p_1, \dots, p_r son coprimos dos a dos, la Proposición 6.5.8 nos dice que también los números $p_1^{v_{p_1}(n)}, \dots, p_r^{v_{p_r}(n)}$ son coprimos dos a dos y, por lo tanto, gracias al Lema 9.4.6 tenemos que

$$f(n) = f(p_1^{v_{p_1}(n)} \cdots p_r^{v_{p_r}(n)}) = f(p_1^{v_{p_1}(n)}) \cdots f(p_r^{v_{p_r}(n)}),$$

como afirma el enunciado. □

9.4.8. Vamos a necesitar un par de veces un resultado sencillo sobre divisores, que probamos ahora. Para cada $n \in \mathbb{N}$ escribamos, como antes, $D(n)$ al conjunto de todos los divisores positivos de n .

Supongamos que n y m son dos enteros y que $\text{mcd}(n, m) = 1$. Si d y e son un divisor positivo de n y uno de m , respectivamente, entonces es claro que de es un divisor positivo de nm . Esto nos dice que hay una función $P : D(n) \times D(m) \rightarrow D(nm)$ tal que $P(d, e) = de$ cada vez que $(d, e) \in D(n) \times D(m)$.

Lema. Si n y m son dos enteros coprimos, entonces la función

$$P : (d, e) \in D(n) \times D(m) \mapsto de \in D(nm)$$

es una biyección y su función inversa es

$$Q : u \in D(nm) \mapsto (\text{mcd}(u, n), \text{mcd}(u, m)) \in D(n) \times D(m).$$

Demostración. Si $u \in D(nm)$, entonces $\text{mcd}(u, n) \in D(n)$ y $\text{mcd}(u, m) \in D(m)$, así que hay una función $Q : D(nm) \rightarrow D(n) \times D(m)$ tal que cada vez que $u \in D(nm)$ se tiene que

$$Q(u) = (\text{mcd}(n, u), \text{mcd}(m, u)).$$

Mostremos que esta función Q es inversa de P .

- Si $u \in D(nm)$, entonces

$$P(Q(u)) = P(\text{mcd}(n, u), \text{mcd}(m, u)) = \text{mcd}(n, u) \text{mcd}(m, u)$$

y, de acuerdo a la Proposición 6.5.5(iv) y gracias a que n y m son coprimos, esto es

$$= \text{mcd}(nm, u) = u,$$

ya que u es un divisor positivo de nm . Esto significa que $P \circ Q$ es la función identidad de $D(nm)$.

- Por otro lado, si $(d, e) \in D(n) \times D(m)$, entonces

$$Q(P(d, e)) = Q(de) = (\text{mcd}(n, de), \text{mcd}(m, de)). \quad (8)$$

Como e divide a m , el Corolario 6.5.2 nos dice que $\text{mcd}(n, e) \mid \text{mcd}(n, m) = 1$, así que n y e son coprimos: usando ahora la Proposición 6.5.5(iii), vemos que

$$\text{mcd}(n, de) = \text{mcd}(n, d) = d,$$

ya que d divide a n . De manera similar, vemos que $\text{mcd}(m, de) = e$ y, volviendo a (8), que

$$Q(P(d, e)) = (d, e).$$

Esto significa que $Q \circ P$ es la función identidad de $D(n) \times D(m)$.

Como P y Q son funciones inversas, P es biyectiva. □

9.4.9. Volvamos ahora a nuestro problema de calcular las funciones σ_k .

Proposición. Sea $k \in \mathbb{R}$. La función $\sigma_k : \mathbb{N} \rightarrow \mathbb{R}$ es multiplicativa. Si k no es nulo, $n \in \mathbb{N}$ y p_1, \dots, p_r son los primos que dividen a n , entonces

$$\sigma_k(n) = \frac{p_1^{k(v_{p_1}(n)+1)} - 1}{p_1^k - 1} \cdots \frac{p_r^{k(v_{p_r}(n)+1)} - 1}{p_r^k - 1}.$$

Observemos que es necesario excluir el caso en que $k = 0$ en la segunda afirmación de esta proposición: en ese caso los denominadores que aparecen en la fórmula se anulan, así que la fórmula no tiene sentido.

Demostración. Probemos primero que la función σ_k es multiplicativa. Sea n y m dos enteros positivos coprimos y recordemos las funciones P y Q del Lema 9.4.8. Tenemos que

$$\sigma_k(n) \cdot \sigma_k(m) = \sum_{d \in D(n)} d^k \cdot \sum_{e \in D(m)} e^k = \sum_{(d,e) \in D(n) \times D(m)} d^k e^k = \sum_{(d,e) \in D(n) \times D(m)} P(d, e)^k$$

y, usando el hecho de que P y Q son funciones inversas, podemos ver que esto es

$$= \sum_{u \in D(nm)} P(Q(u))^k = \sum_{u \in D(nm)} u^k = \sigma_k(nm).$$

Concluimos así que σ_k es una función multiplicativa, como queríamos.

Ocupemos ahora de la segunda afirmación de la proposición. Supongamos que $k \neq 0$, sea $n \in \mathbb{N}$ y sean p_1, \dots, p_r los primos que dividen a n . En vista de la Proposición 9.4.7, tenemos que

$$\sigma_k(n) = \sigma_k\left(p_1^{v_{p_1}(n)}\right) \cdots \sigma_k\left(p_r^{v_{p_r}(n)}\right). \quad (9)$$

Ahora bien, si p es un número primo y $a \in \mathbb{N}_0$, entonces de acuerdo a la Proposición 9.3.6 los divisores positivos de p^a son los $a + 1$ enteros

$$1, p, p^2, \dots, p^a,$$

así que la suma de las potencias k -ésimas de estos divisores es

$$\sigma_k(p^a) = 1^k + p^{2k} + \dots + p^{ak}.$$

Esta suma es una suma geométrica de razón p^k , así que, como vimos en 4.2.1 en el Capítulo 4, es igual a

$$\frac{p^{k(a+1)} - 1}{p^k - 1}.$$

Si usamos esta observación con cada uno de los factores que aparecen a la derecha de la igualdad (9), vemos que

$$\sigma_k(n) = \frac{p_1^{k(v_{p_1}(n)+1)}}{p_1^k - 1} \dots \frac{p_r^{k(v_{p_r}(n)+1)}}{p_r^k - 1}.$$

Esto completa la prueba de la proposición. \square

9.4.10. Usando la Proposición 9.4.9 podemos calcular fácilmente las funciones σ_k . Por ejemplo, como $317765539 = 7^2 \cdot 13 \cdot 23^3 \cdot 41$, tenemos que

$$\begin{aligned} \sigma_3(317765539) &= \frac{7^{3(2+1)} - 1}{7^3 - 1} \cdot \frac{13^{3(1+1)} - 1}{13^3 - 1} \cdot \frac{23^{3(3+1)} - 1}{23^3 - 1} \cdot \frac{41^{3(1+1)} - 1}{41^3 - 1} \\ &= 117993 \cdot 2198 \cdot 1801300709520 \cdot 68922 \\ &= 32197935268666697933108160. \end{aligned}$$

9.4.11. Un número n es *perfecto* si $\sigma_1(n) = 2n$. Por ejemplo, 6 y 28 son números perfectos, ya que

$$\sigma_1(6) = 1 + 2 + 3 + 6 = 2 \cdot 6$$

y

$$\sigma_1(28) = 1 + 2 + 4 + 7 + 14 + 28 = 2 \cdot 28.$$

Como n siempre es un divisor de n , la condición de que n sea perfecto es equivalente a que la suma de los divisores *propios* de n sea igual a n .

Esta definición aparece en el Libro VII de los *Elementos* de Euclides. Desde la época de Euclides hubo siempre una peculiar fascinación por estos números y un gran empeño en encontrarlos en los contextos más diversos: por ejemplo, Philo de Alejandría explicaba, hacia el año 100 d.C., que el mundo había sido creado en 6 días y que la luna tarda 28 días en dar una revolución alrededor de la tierra precisamente porque 6 y 28 son números perfectos.

Los primeros diez números perfectos son

6, 28, 496, 8 128, 33 550 336, 8 589 869 056, 137 438 691 328,
2 305 843 008 139 952 128, 2 658 455 991 569 831 744 654 692 615 953 842 176,
191 561 942 608 236 107 294 793 378 084 303 638 130 997 321 548 169 216

Sólo los primeros cuatro eran conocidos por los griegos clásicos: recién en el año 100 d.C. el matemático Nicómaco de Gerasa, que escribió un célebre tratado de aritmética, se dió cuenta que 8 128 es perfecto. Los siguientes tres fueron encontrados más de mil años después por el matemático *Ismail ibn Fallūs* (1194–1252, Egipto), quien también listó varios más, que ahora sabemos que no son perfectos.

El 10 de enero de 2018 se conocían 50 números perfectos. El más grande de ellos es el número

$$2^{77\,232\,916} \cdot (2^{77\,232\,917} - 1),$$

que tiene 46 498 850 dígitos. No sabemos si hay infinitos números perfectos o no, aunque se cree que sí los hay: esta afirmación es conocida como la conjetura de Lenstra, Pomerance y Wagstaff. Por otro lado, todos los números perfectos que conocemos son pares y no sabemos si existe alguno impar. Decidir si existen o no números perfectos impares es uno de los problemas más viejos de la aritmética — Euler afirmó que se trata de «un problema de la mayor dificultad» y viniendo de él esto es muy significativo!

9.4.12. La siguiente observación, que nos provee de una forma de construir números perfectos, aparece ya en el libro de Euclides:

Proposición. Si $n \in \mathbb{N}$ es tal que $2^n - 1$ es primo, entonces el número $2^{n-1}(2^n - 1)$ es perfecto.

La demostración que da Euclides de esto es bastante laboriosa. Nosotros podemos hacer otra mucho más sencilla usando los resultados que obtuvimos en esta sección.

Demostración. Si $2^n - 1$ es primo y ponemos

$$N = 2^{n-1}(2^n - 1),$$

entonces lo que aparece a la derecha de esta igualdad es la factorización de N como producto de primos. La Proposición 9.4.9 nos dice, en consecuencia, que

$$\sigma_1(N) = \frac{2^n - 1}{2 - 1} \cdot \frac{(2^n - 1)^2 - 1}{(2^n - 1) - 1} = (2^n - 1)2^n = 2N$$

Vemos así que N es perfecto, como queríamos. □

9.4.13. Observando que $3 = 2^2 - 1$, $7 = 2^3 - 1$, $31 = 2^5 - 1$ y $127 = 2^7 - 1$ son primos, concluimos gracias a esta proposición que los números

$$2^1(2^2 - 1) = 6, \quad 2^2(2^3 - 1) = 28, \quad 2^4(2^5 - 1) = 496, \quad 2^6(2^7 - 1) = 8128$$

son perfectos. Estos son los primeros cuatro números perfectos y los únicos que los antiguos griegos conocían. Los siguientes números perfectos provistos por esa proposición son

$$2^{12}(2^{13} - 1) = 33\,509\,381, \quad 2^{16}(2^{17} - 1) = 8\,589\,869\,056$$

y

$$2^{18}(2^{19} - 1) = 137\,438\,691\,328,$$

ya que $8191 = 2^{13} - 1$, $131\,071 = 2^{17} - 1$ y $524\,287 = 2^{19} - 1$ son primos. Estos son los tres números perfectos encontrados por ibn Fallūs aproximadamente en el año 1200. El octavo es

$$2^{30}(2^{31} - 1) = 2\,305\,843\,008\,139\,952\,128,$$

pero éste no fue encontrado hasta el año 1772, cuando Euler pudo determinar que $2\,147\,483\,647 = 2^{31} - 1$ es primo.

9.4.14. La Proposición **9.4.12** nos da una manera de construir números perfectos, pero para usarla necesitamos números primos de la forma $2^n - 1$. Estos primos se llaman *primos de Mersenne*, por *Marin Mersenne* (1588–1648, Francia).

Una observación sencilla que podemos hacer es que si un número de la forma $2^n - 1$ es primo, entonces n mismo tiene que ser primo. Esto es consecuencia de la afirmación del Ejercicio **6.6.4(b)**: si n no es primo y m es un divisor de n tal que $1 < m < n$, entonces $2^m - 1$ es un divisor propio de $2^n - 1$ distinto de 1.

Gracias a esto, para encontrar primos de Mersenne tenemos que decidir, para cada primo p , si $2^p - 1$ es o no primo. El problema con esto es que cuando p crece el valor de $2^p - 1$ crece mucho más rápido y decidir si es primo es muy laborioso. Por lo pronto, no es cierto que sea siempre primo: el ejemplo más chico de esto es

$$2^{11} - 1 = 2047 = 23 \cdot 89.$$

De los números de la forma $2^n - 1$ el más grande que es compuesto y que sabemos factorizar es $2^{1193} - 1$ (que tiene 360 dígitos). Por otro lado, sabemos que el número $2^{1277} - 1$ (que tiene 385 dígitos) es compuesto pero no conocemos ninguno de sus divisores propios — esto es un poco sorprendente: se debe a que conocemos algoritmos que nos permiten decidir si uno de estos números es compuesto o no pero que no nos dan ninguno de sus factores en caso de que lo sea.



Figura 9.4. En el episodio *The Duh-Vinci Code*, el quinto de la sexta temporada de *Futurama*, el equipo de Planet Express viaja a Roma y encuentra la inscripción « $II^{XI} - (XXIII * LXXXIX)$ » grabada en una tumba.

Desde 1996, un esfuerzo colaborativo y distribuido llamado *Great Internet Mersenne Prime Search* (GIMPS) busca primos de Mersenne y desde su fundación hasta enero de 2018 encontró 17 primos, el más grandes de los cuales es

$$2^{77\,232\,917} - 1,$$

que es, de hecho, el número primo más grande que conocemos — tiene 23 249 425 dígitos decimales

9.4.15. Los números perfectos que nos permite construir la Proposición 9.4.12 son todos pares. Euler probó en 1899 que de esa forma obtenemos, de hecho, *todos* los números perfectos pares.

Proposición. Si n es un número perfecto par, entonces existe un número primo p tal que $n = 2^{p-1}(2^p - 1)$.

Demostración. Sea n un numero perfecto par y sea $k = v_2(n)$, que es un número positivo. Claramente, existe un entero impar m tal que $n = 2^k m$. Como n es perfecto y la función σ_1 es multiplicativa, tenemos que

$$2^{k+1}m = 2n = \sigma_1(n) = \sigma_1(2^k m) = \sigma_1(2^k)\sigma_1(m) = (2^{k+1} - 1)\sigma_1(m).$$

Como $\text{mcd}(2^{k+1}, 2^{k+1} - 1) = 1$, de esto se deduce que $2^{k+1} - 1$ divide a m y que, por lo tanto, el número $r = m / (2^{k+1} - 1)$ es entero y divide a m ; observemos que como $k \geq 1$, se tiene que $r < m$.

Si dividimos a ambos lados de la igualdad $2^{k+1}m = (2^{k+1} - 1)\sigma_1(m)$ por $2^{k+1} - 1$, vemos que

$$2^{k+1}r = \sigma_1(m) = m + r + S$$

con S la suma de todos los divisores positivos de m distintos de m y de r , y esto es

$$= (2^{k+1} - 1)r + r + S = 2^{k+1}r + S.$$

Así, es $2^{k+1}r = 2^{k+1}r + S$: la única forma en que esto puede ocurrir es que sea $S = 0$. En otras palabras, los únicos divisores positivos de m son m mismo y r . Como $m \neq r$, m tiene exactamente dos divisores positivos, es primo y el menor de esos divisores es 1: esto nos dice que $1 = m/2^{k+1} - 1$ y, por lo tanto, que $m = 2^{k+1} - 1$. Como observamos arriba, que $2^{k+1} - 1$ sea primo implica que $p = k + 1$ es primo. Como nuestro número perfecto de partida es entonces $n = 2^k m = 2^{p-1}(2^p - 1)$, esto prueba la proposición. \square

Capítulo 10

Potencias

§10.1. El pequeño teorema de Fermat

10.1.1. Proposición. Sea p un número primo. Si i es un entero tal que $0 < i < p$, entonces p divide a $\binom{p}{i}$.

Demostración. Sea i un entero tal que $0 < i < p$. Claramente p no divide a $i!$ ni a $(p-i)!$, ya que no divide a ninguno de los factores de esos dos factoriales y es primo. Por otro lado, es evidente que divide a $p!$. De esto se sigue, por supuesto, que divide al cociente

$$\frac{p!}{i!(p-i)!} = \binom{p}{i},$$

y esto es lo que afirma la proposición. \square

10.1.2. Corolario. Sea p un número primo. Si a y b son dos enteros, entonces

$$(a+b)^p \equiv a^p + b^p \pmod{p}.$$

Demostración. Sean a y b dos enteros. El teorema del binomio de Newton nos dice que

$$(a+b)^p = \sum_{i=0}^p \binom{p}{i} a^{p-i} b^i.$$

Ahora bien, la Proposición 10.1.1 nos dice que p divide a los sumandos de esta suma que corresponden a valores del índice i tales que $0 < i < p$ y entonces la suma completa es congruente módulo p a la suma de los dos términos restantes:

$$(a + b)^p \equiv a^p + b^p \pmod{p}.$$

Esto es precisamente lo que afirma el corolario. □

10.1.3. Proposición. *Sea p un número primo. Para todo entero a se tiene que $a^p \equiv a \pmod{p}$.*

Demostración. Para cada $a \in \mathbb{Z}$ sea $P(a)$ la afirmación « $a^p \equiv a \pmod{p}$ ». Mostremos primero que $P(a)$ vale para todo $a \in \mathbb{N}_0$ haciendo inducción con respecto a a . Notemos que $P(0)$ vale por razones triviales. Supongamos entonces que $a \in \mathbb{N}_0$ y que la afirmación $P(a)$ vale. De acuerdo al Corolario 10.1.2, tenemos que

$$(a + 1)^p \equiv a^p + 1 \pmod{p}$$

y la hipótesis inductiva nos dice que $a^p \equiv a \pmod{p}$ así que, juntando todo, vemos que

$$(a + 1)^p \equiv a + 1 \pmod{p},$$

es decir, que $P(a + 1)$ vale. Esto completa la inducción.

Nos queda mostrar que $P(a)$ vale también cuando a es negativo. Ahora bien, si a es negativo, entonces $a - ap$ es positivo y congruente con a módulo p , así que

$$a^p \equiv (a - ap)^p \equiv a - ap \equiv a \pmod{p},$$

usando, en la segunda congruencia, que ya sabemos que $P(a - ap)$ vale. Esto termina la prueba de la proposición. □

10.1.4. La siguiente proposición es generalmente conocida como el *Pequeño Teorema de Fermat*, por *Pierre de Fermat* (1607–1665, Francia), quien lo enunció por primera vez (en una carta a un amigo). El primero en publicar una prueba, sin embargo, fue Euler en 1736. Gauss lo describe en sus *Disquisitiones* —donde lo demuestra de varias maneras— como un resultado «remarcable tanto por su elegancia como por su utilidad».

Proposición. *Sea p un número primo. Si a es un entero coprimo con p , entonces*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Demostración. De acuerdo a la Proposición 10.1.3 tenemos que $a^p \equiv a \pmod{p}$, es decir, que p divide a $a^p - a = a(a^{p-1} - a)$. Como p no divide a a y si a este producto, tiene que dividir a $a^{p-1} - 1$: esto significa, precisamente, que $a^{p-1} \equiv 1 \pmod{p}$. □

10.1.5. Una aplicación muy sencilla del Teorema de Fermat **10.1.4** es al cálculo de potencias módulo un número primo: tenemos un número primo p , un entero a coprimo con p y un entero no negativo n y queremos determinar a^n módulo p . Si llamamos q y r al cociente y al resto de la división de n por $p - 1$, de manera que $n = q(p - 1) + r$, tenemos que

$$a^n = (a^{p-1})^q a^r \equiv a^r \pmod{p},$$

ya que, de acuerdo al Teorema de Fermat **10.1.4**, es $a^{p-1} \equiv 1 \pmod{p}$. Por ejemplo, si $p = 11$ y queremos determinar 2^{104} módulo p , observamos que $100 = 9(p - 1) + 4$, así que

$$2^{104} = (2^{p-1})^9 2^4 \equiv 2^4 = 16 \equiv 5 \pmod{11},$$

porque $2^{p-1} \equiv 1 \pmod{11}$.

En todo el resto de este capítulo veremos un gran número de otras aplicaciones del teorema.

§10.2. La función de Euler

10.2.1. Si $n \in \mathbb{N}$, escribimos $\varphi(n)$ a la cantidad de elementos del conjunto $\{1, \dots, n\}$ que son coprimos con n , es decir, el cardinal del conjunto

$$C(n) = \{i \in \mathbb{N} : 1 \leq i \leq n, \text{mcd}(i, n) = 1\}.$$

Esa cantidad es positiva, ya que $1 \in C(n)$. De esta manera obtenemos una función $\varphi : \mathbb{N} \rightarrow \mathbb{N}$, a la que llamamos *función de Euler*. Por ejemplo, los enteros positivos que no superan a 20 son

$$\boxed{1} \quad 2 \quad \boxed{3} \quad 4 \quad 5 \quad 6 \quad \boxed{7} \quad 8 \quad \boxed{9} \quad 10 \quad \boxed{11} \quad 12 \quad \boxed{13} \quad 14 \quad 15 \quad 16 \quad \boxed{17} \quad 18 \quad \boxed{19} \quad 20$$

y los que son coprimos con 20 están marcados con un cuadrado: vemos que $\varphi(20) = 8$. Por otro lado, si p es un número primo entonces todo elemento de $\{1, \dots, p\}$, salvo p mismo, es coprimo con p y, por lo tanto, $\varphi(p) = p - 1$.

Veremos más abajo, en la Proposición **10.2.3**, cómo calcular $\varphi(n)$ a partir de la factorización de n como producto de primos. Para llegar a eso necesitamos el siguiente resultado preliminar:

10.2.2. Proposición. La función de Euler $\varphi : \mathbb{N} \rightarrow \mathbb{N}$ es multiplicativa: si n y m son dos enteros coprimos, entonces $\varphi(nm) = \varphi(n)\varphi(m)$.

Sin imponer la condición de coprimalidad entre n y m no podemos en general llegar a la conclusión de la proposición: por ejemplo, $\varphi(2 \cdot 10) = \varphi(20) = 8$, como vimos arriba, pero $\varphi(2)\varphi(10) = 1 \cdot 4 = 4$.

Demostración. Sean n y m dos enteros coprimos. Sabemos que existen dos enteros x e y tales que $xn + ym = 1$.

Primer paso. Empezamos construyendo dos funciones $f : C(n) \times C(m) \rightarrow C(nm)$ y $g : C(nm) \rightarrow C(n) \times C(m)$.

- Sean $a \in C(n)$ y $b \in C(m)$, de manera que $1 \leq a < n$, $1 \leq b < m$, $\text{mcd}(a, n) = 1$ y $\text{mcd}(b, m) = 1$, y consideremos el entero $c = xnb + yma$. Se tiene que

$$\text{mcd}(c, n) = \text{mcd}(xnb + yma, n) = \text{mcd}(yma, n) = 1,$$

ya que cada uno de los enteros y , m y a es coprimo con n . De manera similar, tenemos que $\text{mcd}(c, m) = 1$ y, por lo tanto,

$$\text{mcd}(c, nm) = \text{mcd}(c, n) \text{mcd}(c, m) = 1.$$

Si escribimos $r_{nm}(c)$ al resto de dividir a c por nm , tenemos entonces que también $r_{nm}(c)$ es coprimo con nm y que, además, $0 \leq r_{nm}(c) < nm$: esto nos dice que $r_{nm}(c)$ es un elemento de $C(nm)$. Hay por lo tanto una función $f : C(n) \times C(m) \rightarrow C(nm)$ tal que

$$f(a, b) = r_{nm}(xnb + yma)$$

para cada $(a, b) \in C(n) \times C(m)$.

- Sea $c \in C(nm)$ y sea $a = r_n(c)$ el resto de dividir a c por n . Si q es el correspondiente cociente, de manera que $r_n(c) = c - qn$, se tiene que

$$\text{mcd}(r_n(c), n) = \text{mcd}(r_n(c) + qn, n) = \text{mcd}(c, n) \mid \text{mcd}(c, nm) = 1,$$

así que $r_n(c) \in C(n)$. De manera similar podemos ver que $r_m(c) \in C(m)$ y, por lo tanto, que hay una función $g : C(nm) \rightarrow C(n) \times C(m)$ tal que para cada $c \in C(nm)$ se tiene que

$$g(c) = (r_n(c), r_m(c)).$$

Segundo paso. En segundo lugar, probaremos que las funciones f y g que construimos son mutuamente inversas.

- Sea $(a, b) \in C(n) \times C(m)$ y sea $c = xnb + yma$, de manera que $f(a, b) = r_{nm}(c)$. Sea q el cociente de dividir a c por nm . Como $xnb + yma = c = qnm + r_{nm}(c)$, tenemos que

$$r_{nm}(c) = (xb - qm)n + yma = (xb - qm)n - xna + a$$

así que, como $0 \leq a < n$, es $r_n(r_{nm}(c)) = a$. De manera similar podemos ver que $r_m(r_{nm}(c)) = b$ y entonces que

$$g(f(a, b)) = g(r_{nm}(c)) = (r_n(r_{nm}(c)), r_m(r_{nm}(c))) = (a, b).$$

Esto nos dice que $g \circ f$ es la función identidad de $C(n) \times C(m)$.

- Sea ahora $c \in C(nm)$, de manera que $g(c) = (r_n(c), r_m(c))$, y pongamos

$$d = xnr_m(c) + ymr_n(c).$$

Sean q_n y q_m los cocientes de la división de c por n y por m , respectivamente. Tenemos que

$$\begin{aligned} c &= xnc + ymc \\ &= xn(q_m m + r_m(c)) + ym(q_n n + r_n(c)) \\ &= (xq_m + yq_n)nm + xnr_m(c) + ymr_n(c) \\ &= (xq_m + yq_n)nm + d \end{aligned}$$

así que $c = r_{nm}(c) = r_{nm}(d) = f(g(c))$. Vemos de esta forma que $f \circ g$ es la función identidad de $C(nm)$.

Tercer paso. Ahora que sabemos que f y g son funciones mutuamente inversas, sabemos en particular que f es biyectiva y, por lo tanto, que su dominio y su codominio tienen el mismo cardinal, esto es, que $|C(n) \times C(m)| = |C(nm)|$. Usando esto, vemos que

$$\varphi(n)\varphi(m) = |C(n)| \cdot |C(m)| = |C(n) \times C(m)| = |C(nm)| = \varphi(nm),$$

que es lo que queremos probar. □

10.2.3. Usando la multiplicatividad de la función de φ podemos, como con toda función multiplicativa, calcularla a partir de la factorización de su argumento como producto de primos:

Proposición. Sea $n \in \mathbb{N}$, sean p_1, \dots, p_r los primos que dividen a n , listados sin repeticiones, y sean $a_1, \dots, a_r \in \mathbb{N}$ tales que $n = p_1^{a_1} \cdots p_r^{a_r}$. Se tiene que

$$\varphi(n) = (p_1^{a_1} - p_1^{a_1-1}) \cdots (p_r^{a_r} - p_r^{a_r-1})$$

y

$$\varphi(n) = n \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right).$$

La segunda expresión que nos da esta proposición para $\varphi(n)$ se llama el **producto de Euler** para φ .

Demostración. Sea p un número primo y sea $a \in \mathbb{N}$. Un número $k \in \{1, \dots, p^a - 1\}$ tiene $\text{mcd}(k, p^a) \neq 1$ si y solamente si es divisible por p , y esto ocurre si y solamente es de la forma pm con $m \in \{1, \dots, p^{a-1}\}$. Esto nos dice que en $\{1, \dots, p^a - 1\}$ hay p^{a-1} números que no son coprimos con p^a y, por lo tanto, que hay $p^a - p^{a-1}$ números que sí lo son. En otras palabras, tenemos que

$$\varphi(p^a) = p^a - p^{a-1}.$$

Sea ahora $n = p_1^{a_1} \cdots p_r^{a_r}$ como en el enunciado de la proposición. Como la función φ es multiplicativa, la Proposición 9.4.7 nos dice, en vista de lo que ya hicimos, que

$$\varphi(n) = \varphi(p_1^{a_1}) \cdots \varphi(p_r^{a_r}) = (p_1^{a_1} - p_1^{a_1-1}) \cdots (p_r^{a_r} - p_r^{a_r-1}).$$

Esta es la primera igualdad que aparece en el enunciado. Para ver la segunda observamos simplemente que esta última expresión es igual a

$$p_1^{a_1} \left(1 - \frac{1}{p_1}\right) \cdots p_r^{a_r} \left(1 - \frac{1}{p_r}\right)$$

y reordenamos los factores, recordando que el producto $p_1^{a_1} \cdots p_r^{a_r}$ es igual a n . \square

10.2.4. Si n es un entero positivo y p_1, \dots, p_r son los primos que dividen a n listados sin repeticiones, la proposición que acabamos de probar nos dice que

$$\frac{\varphi(n)}{n} = \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right). \quad (1)$$

La fracción que aparece a la izquierda en esta igualdad es el cociente entre el número de enteros coprimos con n de $\{1, \dots, n\}$ sobre el número total de elementos de este conjunto: en otras palabras, es la proporción de números coprimos con n que hay en el conjunto $\{1, \dots, n\}$. Podemos hacer algunas observaciones sencillas sobre esta proporción:

- Para cada $i \in \{1, \dots, r\}$ el factor $1 - 1/p_i$ que aparece en (1) es menor que 1 pero mientras más grande es p_i más cerca de 1 está. Esto nos dice que la proporción de números coprimos disminuye si aumenta el número de divisores primos de n y aumenta si esos divisores primos son más grandes.
- La proporción $\varphi(n)/n$ depende solamente de qué primos dividen a n y no de con qué potencias aparecen en la factorización de n . Así, por ejemplo, en proporción hay tantos números coprimos con $2 \cdot 5 \cdot 7$ como con $2^{23} \cdot 5^{12} \cdot 7^{201}$.
- Para n como en (1) se tiene que

$$\frac{\varphi(n)}{n} = \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right) \leq \left(1 - \frac{1}{2}\right)^r = \frac{1}{2^r},$$

ya que todo primo es mayor o igual que 2. De esto se deduce que los números de la forma 2^a son los que más números coprimos tienen, en proporción: la mitad de los enteros positivos que no superan a 2^a son coprimos con él.

- Si ε es un número real positivo, sabemos, por un lado, que existe $r \in \mathbb{N}$ tal que $\varepsilon < 2^{-r}$ y, por otro, que hay r primos p_1, \dots, p_r distintos dos a dos —esto último porque sabemos que hay, de hecho, infinitos números primos. Se sigue de esto que si $n = p_1 \cdots p_r$ es el producto de esos r primos, entonces $\varphi(n)/n \leq 2^{-r} < \varepsilon$.

Vemos así que hay números n para los que la proporción $\varphi(n)/n$ de números coprimos con n es tan baja como queramos. De hecho, se puede probar bastante fácilmente que cuando $n \rightarrow \infty$ es

$$\frac{\varphi(n)}{n} \approx \frac{1}{e^\gamma \log \log n}, \quad (2)$$

con $\gamma \approx 0,577216$ la llamada constante de Euler–Mascheroni, de manera que $e^\gamma \approx 1,781072$. Por ejemplo, si $n \approx 10^{100}$ el lado derecho de (2) es aproximadamente 0,103. Puede encontrarse una prueba de (2), junto con mucha más información sobre la función φ , en [HW2008, §18.4].

10.2.5. La siguiente observación es debida a Gauss:

Proposición. Si $n \in \mathbb{N}$, entonces

$$\sum_{d|n} \varphi(d) = n.$$

Los términos de la suma que aparece en el enunciado están indexados por los divisores positivos de n . Por ejemplo, los divisores de 30 son 1, 2, 3, 5, 6, 10, 15 y 30, y la proposición nos dice que $\varphi(1) + \varphi(2) + \varphi(3) + \varphi(5) + \varphi(6) + \varphi(10) + \varphi(15) + \varphi(30) = 30$.

Demostración. Para cada $n \in \mathbb{N}$ escribamos

$$\psi(n) = \sum_{d|n} \varphi(d).$$

Obtenemos de esta forma una función $\psi : \mathbb{N} \rightarrow \mathbb{N}$. Mostremos que es multiplicativa.

Sean n y m dos enteros positivos coprimos y recordemos las funciones P y Q del Lema 9.4.8. Es

$$\psi(n)\psi(m) = \sum_{d \in D(n)} \varphi(d) \cdot \sum_{e \in D(m)} \varphi(e) = \sum_{(d,e) \in D(n) \times D(m)} \varphi(d)\varphi(e).$$

Ahora bien, si $(d, e) \in D(n) \times D(m)$, entonces $\text{mcd}(d, e) \mid \text{mcd}(n, m) = 1$, así que como la función φ es multiplicativa tenemos que $\varphi(d)\varphi(e) = \varphi(de)$. Usando esto en cada uno de los términos de la última suma que obtuvimos vemos que

$$\begin{aligned} \psi(n)\psi(m) &= \sum_{(d,e) \in D(n) \times D(m)} \varphi(de) = \sum_{(d,e) \in D(n) \times D(m)} \varphi(P(d, e)) \\ &= \sum_{u \in D(nm)} \varphi(P(Q(e))) = \sum_{u \in D(nm)} \varphi(u) = \psi(nm). \end{aligned}$$

Esto muestra que ψ es multiplicativa, como queríamos.

Sea ahora p un número primo y sea $a \in \mathbb{N}$. Los divisores positivos de p^a son los números $1, p, p^2, \dots, p^{a-1}, p^a$ así que

$$\begin{aligned} \psi(p^a) &= \varphi(1) + \varphi(p) + \varphi(p^2) + \dots + \varphi(p^{a-1}) + \varphi(p^a) \\ &= 1 + (p-1) + (p^2-p) + \dots + (p^{a-1} - p^{a-2}) + (p^a - p^{a-1}) \\ &= p^a \end{aligned}$$

Finalmente sea n un entero positivo cualquiera, sean p_1, \dots, p_r los primos que dividen a n listados sin repeticiones, y sean $a_1, \dots, a_r \in \mathbb{N}$ tales que $n = p_1^{a_1} \dots p_r^{a_r}$. Usando la multiplicatividad de la función ψ podemos calcular ahora que

$$\psi(n) = \psi(p_1^{a_1} \dots p_r^{a_r}) = \psi(p_1^{a_1}) \dots \psi(p_r^{a_r}) = p_1^{a_1} \dots p_r^{a_r} = n.$$

Esto prueba la proposición. □

§10.3. El Teorema de Euler

10.3.1. El Teorema de Fermat 10.1.4 nos dice que si p es un número primo y a un entero coprimo con p entonces $a^{p-1} \equiv 1 \pmod{p}$. Esto no es cierto si p no es primo: por

ejemplo, 3 es coprimo con 4 pero $3^{4-1} \equiv 3 \not\equiv 1 \pmod{4}$. El siguiente teorema de Euler generaliza al de Fermat a módulos compuestos:

Proposición. Sea $m \in \mathbb{N}$. Si a es un entero coprimo con m , entonces $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Observemos que como $\varphi(p) = p - 1$ para todo primo p , este resultado tiene como caso particular al Teorema de Fermat **10.1.4**.

Demostración. Sea a un entero coprimo con m y sean x e y enteros tales que $xa + ym = 1$. Para cada $k \in \mathbb{Z}$ escribamos $q_m(k)$ y $r_m(k)$ al cociente y al resto de la división de k por m y consideremos el conjunto

$$C(m) = \{k \in \mathbb{N} : 1 \leq k \leq m, \text{mcd}(k, m) = 1\}.$$

Si $k \in C(m)$, entonces $k = kxa + kym$ y, por lo tanto,

$$\text{mcd}(ka, m) \mid \text{mcd}(kxa, m) = \text{mcd}(k - kym, m) = \text{mcd}(k, m) = 1,$$

de manera que ka es coprimo con m : se sigue de esto que $r_m(ka)$ es un elemento de $C(m)$. Como consecuencia de esto, vemos que hay una función $\pi : C(m) \rightarrow C(m)$ tal que para todo $k \in C(m)$ es $\pi(k) = r_m(ka)$. Afirmamos que se trata de una biyección. Como I es finito, para verificar esto suficiente con que mostremos que es sobreyectiva.

Sea entonces $k \in C(m)$. Como $k = kxa + kym$, tenemos que

$$\text{mcd}(kx, m) \mid \text{mcd}(kxa, m) = \text{mcd}(k - kym, m) = \text{mcd}(k, m) = 1,$$

así que el número $l = r_m(kx)$ pertenece a $C(m)$. Es $kx = q_m(kx)m + l$, así que

$$k - kym = kxa = aq_m(kx)m + al.$$

Tomando restos a ambos lados de esta igualdad vemos que

$$k = r_m(k) = r_m(al) = \pi(l).$$

Esto muestra que k está en la imagen de π y, por lo tanto, que esta función π es sobreyectiva, como queríamos.

Supongamos que

$$u_1, u_2, \dots, u_{\varphi(m)} \tag{3}$$

son los $\varphi(m)$ elementos de $C(m)$ listados sin repeticiones. Como la función π es biyectiva, tenemos entonces que

$$r_m(au_1), r_m(au_2), \dots, r_m(au_{\varphi(m)})$$

son esos mismos elementos, otra vez sin repeticiones, salvo que listados en otro orden, y cada uno de ellos es congruente módulo m con el correspondiente entero de la lista

$$au_1, au_2, \dots, au_{\varphi(m)}. \quad (4)$$

Se deduce de esto que el producto de los enteros listados en (3) es congruente módulo m con el producto de los enteros listados en (4), es decir, que

$$u_1 u_2 \cdots u_{\varphi(m)} \equiv au_1 au_2 \cdots au_{\varphi(m)} \pmod{m}.$$

Si llamamos w al producto $u_1 \cdots u_{\varphi(m)}$, esto nos dice que

$$w \equiv wa^{\varphi(m)} \pmod{m}. \quad (5)$$

El número w es coprimo con m . Existen entonces enteros α y β tales que $\alpha w + \beta m = 1$ y, en particular, $\alpha w \equiv 1 \pmod{m}$. Multiplicando ahora a cada lado de la congruencia (5) por α vemos que

$$1 \equiv \alpha w \equiv \alpha w a^{\varphi(m)} \equiv a^{\varphi(m)} \pmod{m}$$

y esto prueba la proposición. □

Números racionales periódicos

10.3.2. Mostremos una aplicación sencilla del Teorema de Euler **10.3.1**. Supongamos que a/b es un número racional entre 0 y 1 tal que sus cifras decimales son periódicas, esto es, tal que si escribimos

$$\frac{a}{b} = 0.d_1 d_2 d_3 d_4 \cdots d_n d_{n+1} \cdots$$

al desarrollo decimal de a/b , entonces existe $N \in \mathbb{N}$ tal que $d_{i+N} = d_i$ para todo $i \in \mathbb{N}$, de manera que lo que está después de la coma se obtiene repitiendo indefinidamente el bloque de dígitos $d_1 d_2 \cdots d_N$, al que llamamos un *periodo* del número a/b . Por ejemplo, con

$$\frac{9}{37} = 0.\underline{234} \underline{234} \underline{234} \underline{234} \dots$$

podemos tomar $N = 3$, de manera que el periodo es 234, y con

$$\frac{1}{2439} = 0.\underline{00041} \underline{00041} \underline{00041} \underline{00041} \dots$$

elegir $N = 5$, con periodo 00041. Notemos que el número N no está determinado —en el primer ejemplo podríamos haber elegido $N = 6$, con periodo 234234— aunque es

fácil ver que siempre hay un periodo más corto que todos los otros y que la longitud de éste divide a la de todos los otros. Por supuesto, no es cierto que todo número racional sea periódico en este sentido: así, no lo es

$$\frac{1}{2} = 0.5000\dots$$

Ahora bien, si multiplicamos a a/b por 10^N , obtenemos

$$10^N \cdot \frac{a}{b} = d_1 \cdots d_N \cdot \underline{d_1 \cdots d_N} \underline{d_1 \cdots d_N} \underline{d_1 \cdots d_N} \dots$$

así que si llamamos c al número $(d_1, \dots, d_N)_{10}$, tenemos que

$$10^N \cdot \frac{a}{b} - c = \frac{a}{b}$$

o, equivalentemente, que

$$\frac{a}{b} = \frac{c}{10^N - 1}.$$

Como $0 < a/b < 1$, es claro que $0 < c < 10^N - 1$.

10.3.3. Tenemos, de hecho, el siguiente resultado:

Proposición. *Un número racional entre 0 y 1 es periódico si y solamente si es de la forma*

$$\frac{c}{10^N - 1}$$

para algún $N \in \mathbb{N}$ y algún entero c tal que $0 < c < 10^N - 1$, y en ese caso tiene un periodo de longitud N .

Demostración. Vimos arriba que un número racional entre 0 y 1 que es periódico es de esa forma, así que la condición es necesaria. Veamos que también es suficiente.

Sea $N \in \mathbb{N}$, sea c un entero tal que $0 < c < 10^N - 1$ y sea $q = c/(10^N - 1)$. Es evidente que q es un número racional y que $0 < q < 1$, así que tenemos que mostrar solamente que es periódico. De la forma en que definimos a q es claro que

$$10^N \cdot q = c + q. \tag{6}$$

Si la expansión decimal de q es

$$0.d_1d_2d_3\dots, \tag{7}$$

entonces la de $10^N \cdot q$ es

$$d_1 \cdots d_N \cdot \underline{d_{N+1}d_{N+2}\dots}$$

Esto es, de acuerdo a (6), igual a $c + q$: como c es un entero y $0 < q < 1$, es claro que debe ser $c = (d_1, \dots, d_N)_{10}$ y

$$q = 0.d_{N+1}d_{N+2}d_{N+3}\dots$$

Comparando esto con (7) vemos que $d_{N+i} = d_i$ para todo $i \in \mathbb{N}$, así que q es periódico de periodo $d_1 \cdots d_N$ de longitud N . \square

10.3.4. Aunque la Proposición 10.3.3 describe todos los números racionales periódicos entre 0 y 1 no es muy útil para reconocerlos. Por ejemplo, como vimos arriba el número $9/37$ es periódico: así como lo escribimos no está escrito como una fracción con denominador de la forma $10^N - 1$, pero de todas formas

$$\frac{9}{37} = \frac{234}{10^3 - 1}.$$

Lo que aquí sucede es que el denominador de la fracción de la derecha es un múltiplo de 37, ya que $10^3 - 1 = 37 \cdot 27$: si multiplicamos el numerador y denominador de $9/37$ por 27 obtenemos esa fracción y esto hace evidente que el número $9/37$ es periódico.

Así, el problema de decidir si un número racional a/b entre 0 y 1 es periódico se reduce inmediatamente al de decidir si b divide a un número de la forma $10^n - 1$. Es con este último que el Teorema de Euler nos ayuda:

Proposición. *Un número racional a/b entre 0 y 1 escrito en forma reducida es periódico si y solamente si su denominador es coprimo con 10, y en ese caso la longitud de su periodo más corto es menor o igual a $\varphi(b)$.*

Es importante aquí que la fracción a/b sea reducida: el número $2/18 = 0,111\ 111\dots$ es periódico pero su denominador 18 no es coprimo con 10 —lo que sucede en este ejemplo es que $2/18$ puede simplificarse a $1/9$ y 9 sí es coprimo con 10.

Demostración. Sea a/b un número racional entre 0 y 1 escrito en forma reducida. Si b es coprimo con 10, entonces $10^{\varphi(b)} \equiv 1 \pmod{b}$ por el Teorema de Euler 10.3.1, así que b divide a $10^{\varphi(b)} - 1$. Si q es el correspondiente cociente, entonces

$$\frac{a}{b} = \frac{qa}{10^{\varphi(b)} - 1}$$

y, de acuerdo a la proposición anterior, tenemos que a/b es periódico y que tiene un periodo de longitud $\varphi(b)$.

Recíprocamente, si el número a/b es periódico con un periodo de periodo de longitud N , entonces hay un entero c tal que $0 < c < 10^N - 1$ y

$$\frac{a}{b} = \frac{c}{10^N - 1},$$

así que $bc = (10^N - 1)a$. Como a y b son coprimos, esto implica que b divide a $10^N - 1$. Si $d = \text{mcd}(b, 10)$, entonces d divide a 10 y a $10^N - 1$, así que divide a 1: por supuesto, esto nos dice que $d = 1$, es decir, que b es coprimo con 10. \square

§10.4. Dos aplicaciones

Los algoritmos de decisión de primalidad de Fermat y de Miller-Rabin

10.4.1. El Teorema de Fermat [10.1.4](#) nos dice que si p es un número primo y a es un entero tal que $0 < a < p$, entonces se tiene que $a^{p-1} \equiv 1 \pmod{p}$. Esto nos da una condición necesaria para que un número sea primo. Por ejemplo, consideremos el número $n = 2\,534\,968\,907$. Usando el algoritmo que describimos en el Lema [5.4.19](#) para calcular potencias, podemos ver fácilmente (haciendo unas $2 \log_2 n \approx 62.47$ multiplicaciones) que

$$2^{1\,475\,261\,599-1} \equiv 1\,475\,261\,599 \not\equiv 1 \pmod{n}.$$

Como consecuencia de esto podemos concluir que n no es primo — notemos que, a pesar esto, seguimos sin conocer siquiera un divisor propio de n . Factorizarlo es mucho más difícil: en este caso, resulta que n es el producto de los primos 40283 y 62929, pero esto no se deduce para nada de la cuenta que hicimos¹.

Esta idea es conocida como el *algoritmo de Fermat* para el problema de decidir si un número positivo n es primo o no: si encontramos un entero a tal que $0 < a < n$ y $a^{n-1} \not\equiv 1 \pmod{n}$, entonces podemos concluir con toda certeza que la respuesta a la pregunta es *no*. Llamamos a todo número a con esa propiedad un *certificado* de que n es compuesto. Así, vimos arriba que 2 es un certificado de que 1 475 261 599 es compuesto

¿Cómo buscamos un certificado? Lamentablemente, no hay ninguna forma efectiva de hacerlo. En la práctica, lo que hacemos es elegir al azar un entero a tal que $1 < a < n - 1$ y calcular su potencia $(n - 1)$ -ésima módulo n : si ésta es distinta de 1, entonces sabremos que n no es primo. Si en cambio sí es 1, entonces no sabremos nada nuevo... pero podemos repetir esta prueba con varios enteros distintos: si con todos

¹De hecho, armamos el ejemplo eligiendo primero estos dos primos y multiplicándolos para construir el número n .

encontramos un 1, podemos pensar que tenemos evidencia de que n es probablemente primo: decimos que es un *primo probable*.

En la Figura 10.1.4 en la página 203 damos una implementación sencilla de esa idea en HASKELL. Con esas definiciones, podemos evaluar

```
*Main> esPrimo fermat 3 1475261599
False
```

Esto nos dice que usando el algoritmo de Fermat y haciendo 3 intentos, alguno de los tres certifica que el número 1 475 261 599 que consideramos antes es compuesto. De manera similar, evaluando

```
*Main> esPrimo fermat 3 1020928802728505074582154940524117
False
```

vemos que ese número, que tiene 34 dígitos, es compuesto. Por otro lado, podemos calcular:

```
*Main> esPrimo fermat 10000 2038074743
True
```

Esto eligió al azar 10 000 números entre 1 y 2 038 074 743 y ninguno de ellos certificó que este último es compuesto: podemos sospechar entonces que 2 038 074 743 es primo. En este caso, esa sospecha es buena: el número es efectivamente primo. Sin embargo, también podemos calcular

```
*Main> esPrimo fermat 10000 2038074743
True
```

```

import System.Random

potencia :: Integer -> Integer -> Integer -> Integer
potencia n a 0 = 1
potencia n a k
  | even k  = (potencia n a (k `div` 2) ^ 2) `mod` n
  | odd k   = (a * potencia n a ((k - 1) `div` 2) ^ 2) `mod` n

type Test = Integer -> Integer -> Bool

trivial :: Test
trivial n a = gcd n a == 1

fermat :: Test
fermat n a = gcd n a == 1 && potencia n a (n - 1) == 1

esPrimo :: Test -> Int -> Integer -> IO Bool
esPrimo test m n = fmap (all (test n) . take m . randomRs (2, n-2)) newStdGen

```

Figura 10.1. El algoritmo de Fermat para decidir si un número es primo.

La justificación de esto es que es posible probar que para casi todos los números compuestos existen certificados y, más aún, que hay muchos. Por ejemplo, si $n = 2\,430\,101$, que es producto de los primos 1 223 y 1 987, entonces sólo 2 enteros que están estrictamente entre 1 y $n - 1$ *no* son certificados: 820 632, 1 609 469, y ciertamente hay que tener mucha mala suerte para elegir a alguno de éstos. De manera similar, entre 1 y $n = 50\,670\,601$, que se factoriza como $229 \cdot 409 \cdot 541$, hay 17 280 números que no certifican que es compuesto: son muchos, pero inmensamente menos que n : son menos que el 0,000 3% del total y es de esperar, por lo tanto, que si elegimos un número al azar no sea uno de ellos.

Es importante que si encontramos un entero a entre 0 y n tal que a^{n-1} sí sea congruente a 1 módulo n no podemos concluir nada sobre n . Así, calculando vemos que

$$2^{561-1} \equiv 1 \pmod{561}$$

y esto no nos dice nada sobre 561. Si probamos con 3, en cambio, vemos que

$$3^{561-1} \equiv 375 \not\equiv 1 \pmod{561},$$

y ahora sí podemos concluir que 561 no es primo.

Hay dos preguntas que tenemos que hacernos:

- ¿Cómo buscar certificados de que n es compuesto?
- Si no encontramos ninguno, ¿podemos concluir que n es primo?

En cuanto a la primera pregunta, la respuesta es sencilla: no hay ninguna forma efectiva de encontrar certificados.

§10.5. Órdenes

10.5.1. Sea $m \in \mathbb{N}$. Si a es un entero coprimo con m , el Teorema de Euler **10.3.1** nos dice que $a^{\varphi(m)} \equiv 1 \pmod{m}$, así que, en particular, el conjunto

$$S_a = \{k \in \mathbb{N} : a^k \equiv 1 \pmod{m}\} \tag{8}$$

no es vacío. Podemos entonces considerar su menor elemento, al que llamamos el **orden** de a módulo m y escribimos $\text{ord}_m(a)$ o, cuando esto no introduzca confusiones, simplemente $o(m)$. Notemos que definimos el orden módulo m de un entero a sólo cuando éste último es coprimo con m : si no es ése el caso, el conjunto S_a que definimos arriba es vacío.

10.5.2. Una de las razones por las que nos interesa el orden de a es que nos permite describir el conjunto S_a de (8) completo:

Proposición. Sea $m \in \mathbb{N}$ y sea a un entero coprimo con m . Tenemos que $a^{\text{ord}_m(a)} \equiv 1 \pmod{m}$ y, más aún, un entero positivo t es tal que $a^t \equiv 1 \pmod{m}$ si y solamente si es divisible por $\text{ord}_m(a)$.

Demostración. La primera afirmación es inmediata, ya que $\text{ord}_m(a)$ pertenece al conjunto S_a de (8). Veamos la segunda.

Sea t un entero positivo. Supongamos primero que $a^t \equiv 1 \pmod{m}$ y sean q y r el cociente y el resto de la división de t por $\text{ord}_m(a)$, de manera que $t = q \text{ord}_m(a) + r$ y $0 \leq r < \text{ord}_m(a)$. Tenemos entonces que

$$1 \equiv a^t \equiv a^{q \text{ord}_m(a) + r} \equiv (a^{\text{ord}_m(a)})^q a^r \equiv a^r \pmod{m},$$

así que o bien $r = 0$ o bien $r \in S_a$. Como la segunda opción no puede ocurrir, ya que $r < \text{ord}_m(a)$ y $\text{ord}_m(a)$ es el menor elemento de S_a , vemos que $r = 0$, esto es, que r es divisible por $\text{ord}_m(a)$. Esto muestra que la condición del enunciado es necesaria.

Su suficiencia, por otro lado, es casi evidente: si t es un múltiplo de $\text{ord}_m(a)$, de manera que existe $s \in \mathbb{N}$ tal que $t = s \text{ord}_m(a)$, entonces $a^t = (a^{\text{ord}_m(a)})^s \equiv 1^s \equiv 1 \pmod{m}$. \square

10.5.3. Corolario. Si $m \in \mathbb{N}$ y a es un entero coprimo con m , entonces $\text{ord}_m(a)$ divide a $\varphi(m)$. En particular, si m es primo, entonces $\text{ord}_p(a)$ divide a $m - 1$.

Demostración. De acuerdo al Teorema de Euler 10.3.1, es $a^{\varphi(m)} \equiv 1 \pmod{m}$, así que la Proposición 10.5.2 nos dice que $\text{ord}_m(a)$ divide a $\varphi(m)$. Esto prueba la primera afirmación del corolario. La segunda es consecuencia inmediata de ella, ya que cuando m es primo se tiene que $\varphi(m) = m - 1$. \square

10.5.4. Si conocemos el orden de un entero coprimo módulo un número m , todas sus potencias quedan determinadas módulo m por un número finito de ellas:

Proposición. Sea $m \in \mathbb{N}$ y sea a un entero coprimo con m . Si n es el orden de a módulo m , entonces los n enteros

$$1, a, a^2, \dots, a^{n-1} \tag{9}$$

son no congruentes módulo m dos a dos. Más aún, todas las potencias de a son congruentes a uno y a uno sólo de estos números: más precisamente, si $k \in \mathbb{N}$ y r es el resto de la división de k por n , entonces $a^k \equiv a^r \pmod{m}$.

Demostración. Sea n el orden de a módulo m y supongamos, para probar la primera afirmación por el absurdo, que i y j son enteros tales que $0 \leq i < j < n$ y $a^i \equiv a^j \pmod{m}$. Tenemos entonces que m divide a $a^j - a^i = a^i(a^{j-i} - 1)$ y, como es coprimo con a , que divide a $a^{j-i} - 1$. En otras palabras, tenemos que $a^{j-i} \equiv 1 \pmod{m}$: esto es imposible, ya que la diferencia $j - i$ es positiva y estrictamente menor que el orden de a .

Sea ahora $k \in \mathbb{N}$ y sean q y r el cociente y el resto de la división de k por n , de manera que $k = qn + r$ y $0 \leq r < n$. Es $a^k = (a^n)^q a^r \equiv a^r \pmod{m}$, así que a^k es congruente a uno de los enteros listados en (9). Sólo puede ser congruente a uno de ellos, ya que sabemos que no hay ahí dos que sean congruentes entre sí. \square

10.5.5. La siguiente observación es importante: nos dice como calcular el orden de una potencia de un entero cuando conocemos el de éste.

Proposición. Sea $m \in \mathbb{N}$ y sea a un entero coprimo con m . Si $k \in \mathbb{N}_0$, entonces el orden de a^k módulo m es

$$\text{ord}_m(a^k) = \frac{\text{ord}_m(a)}{\text{mcd}(\text{ord}_m(a), k)}.$$

Demostración. Escribamos $n = \text{ord}_m(a)$ y $t = \text{ord}_m(a^k)$. Como $a^{kt} = (a^k)^t = 1$, tenemos que n divide a kt y que, por lo tanto, existe un entero positivo m tal que $kt = nm$. Sea $d = \text{mcd}(n, k)$ y sean n_1 y k_1 enteros tales que $n = n_1 d$ y $k = k_1 d$; sabemos que es entonces $\text{mcd}(n_1, k_1) = 1$. Como

$$k_1 d t = kt = nm = n_1 d m$$

y, por supuesto, $d \neq 0$, tenemos que $k_1 t = n_1 m$. En particular, esto nos dice que n_1 divide a $k_1 t$ y, como es coprimo con k_1 , que de hecho divide a t . Esto implica que $n_1 \leq t$.

Por otro lado, tenemos que

$$(a^k)^{n_1} = a^{kn_1} = a^{k_1 d n_1} = a^{k_1 n} = (a^n)^{k_1} \equiv 1 \pmod{m},$$

así que $t = \text{ord}_m(a^k) \mid n_1$ y, por lo tanto, $t \leq n_1$. Concluimos de esta forma que

$$t = n_1 = \frac{n}{d} = \frac{\text{ord}_m(a)}{\text{mcd}(\text{ord}_m(a), k)},$$

que es lo que afirma la proposición. \square

10.5.6. La proposición que acabamos de probar tiene dos casos particulares útiles:

Corolario. Sea $m \in \mathbb{N}$, sea a un entero coprimo con m y sea $k \in \mathbb{N}$.

- (i) Si k divide a $\text{ord}_m(a)$, entonces el orden de a^k es $\text{ord}_m(a)/k$.
- (ii) Si k es coprimo con $\text{ord}_m(a)$, entonces $\text{ord}_m(a^k) = \text{ord}_m(a)$.

Demostración. Ambas afirmaciones son consecuencia inmediata de la proposición: en el primer caso $\text{mcd}(\text{ord}_m(a), k)$ es k y en el segundo es 1. \square

10.5.7. Proposición. Sea $m \in \mathbb{N}$ y sean a y b dos enteros coprimos con m .

- (i) El orden de ab es un divisor $\text{mcm}(\text{ord}_m(a), \text{ord}_m(b))$.
- (ii) Si los órdenes $\text{ord}_m(a)$ y $\text{ord}_m(b)$ son coprimos, entonces $\text{ord}_m(ab) = \text{ord}_m(a) \text{ord}_m(b)$.

Demostración. Escribamos $x = \text{ord}_m(a)$, $y = \text{ord}_m(b)$ y $z = \text{ord}_m(ab)$.

(i) Sea $s = \text{mcm}(x, y)$. Es un múltiplo común de x y de y , así que hay enteros positivos x_1 e y_1 tales que $s = xx_1$ y $s = yy_1$. Usando esto, vemos que

$$(ab)^s = a^s b^s = (a^x)^{x_1} (b^y)^{y_1} \equiv 1 \pmod{m}$$

y, en particular, $\text{ord}_m(ab)$ divide a s .

(ii) Supongamos que $\text{mcd}(x, y) = 1$. Como

$$(ab)^{xy} = (a^x)^y (b^y)^x \equiv 1^y 1^x \equiv 1 \pmod{m},$$

se tiene que $z \mid xy$. Por otro lado, tenemos que

$$a^z b^z = (ab)^z \equiv 1 \pmod{m},$$

así que

$$(a^z b^z)^y = a^{yz} (b^y)^z \equiv a^{yz} \pmod{m}$$

y, por lo tanto, $x \mid yz$: como x es coprimo con y , esto implica que x divide a z . Podemos ver, de manera similar, que y divide a z y, como x e y son coprimos, deducir de estas dos cosas que $xy \mid z$. Se tiene entonces que $xy = z$, que es lo que afirma el enunciado. \square

10.5.8. En la situación de la Proposición 10.5.7(i) no se tiene en general que el orden de ab sea igual a $\text{mcm}(\text{ord}_m(a), \text{ord}_m(b))$. Por ejemplo los órdenes de 2 y de 5 módulo 13 son 12 y 6, respectivamente, y el orden de $10 = 2 \cdot 5$ es 6, que es distinto de $\text{mcm}(12, 6) = 12$.

El siguiente resultado nos dice, de todas formas, que podemos construir en la situación de la Proposición 10.5.7(i) a partir de a y b un número de orden igual a $\text{mcm}(\text{ord}_m(a), \text{ord}_m(b))$, aunque de una forma apenas un poco más complicada que simplemente multiplicándolos:

Proposición. Sea $m \in \mathbb{N}$ y sean a y b dos enteros coprimos con m . Existen enteros positivos r y s tales que el orden de $a^r b^s$ es $\text{mcm}(\text{ord}_m(a), \text{ord}_m(b))$.

Demostración. Sean $x = \text{ord}_m(a)$ e $y = \text{ord}_m(b)$. De acuerdo a la Proposición 9.3.8, existen enteros positivos u y v tales que $\text{mcd}(u, v) = 1$, $\text{mcd}(x, y) = uv$, $u \mid x$ y $v \mid y$. Como x/u divide a x , el Corolario 10.5.6(i) nos dice que $\text{ord}_m(a^{x/u}) = \text{ord}_m(a)/(x/u) = u$ y,

de manera similar y como y/v divide a y , que $\text{ord}_m(b^{y/v}) = v$. Ahora bien, como u y v son coprimos, la Proposición 10.5.7(ii) nos dice que el orden de $a^{x/u}b^{y/v}$ es uv , que es igual a $\text{mcm}(x, y)$. Esto prueba la proposición: basta elegir $r = x/u$ y $s = y/v$. \square

10.5.9. Como es habitual, podemos extender la afirmación de la Proposición 10.5.8 al caso en que tenemos un número arbitrario de enteros:

Corolario. Sea $m \in \mathbb{N}$. Si $n \in \mathbb{N}$ y a_1, \dots, a_n son enteros coprimos con m , entonces existen enteros positivos r_1, \dots, r_n tales que $a_1^{r_1} \cdots a_n^{r_n}$ tiene orden

$$\text{mcm}(\text{ord}_m(a_1), \dots, \text{ord}_m(a_n))$$

modulo m .

Demostración. Procedemos por inducción con respecto a n , notando que si $n = 1$ no hay nada que probar y que si $n = 2$ lo que afirma el corolario es precisamente lo que dice la Proposición 10.5.8.

Supongamos entonces que $n \geq 3$ y sean a_1, \dots, a_n enteros coprimos con m . De acuerdo a la Proposición 10.5.8 existen enteros positivos r y s tales que el orden de $a_1^r a_2^s$ es $\text{mcm}(\text{ord}_m(a_1), \text{ord}_m(a_2))$. Por otro lado, la hipótesis inductiva obvia nos dice que existen enteros positivos b_1, \dots, b_{n-1} tales que el orden módulo m del entero

$$(a_1^r a_2^s)^{b_1} a_3^{b_2} \cdots a_n^{b_{n-1}} = a_1^{rb_1} a_2^{sb_1} a_3^{b_2} \cdots a_n^{b_{n-1}}$$

es

$$\text{mcm}(\text{mcm}(\text{ord}_m(a_1), \text{ord}_m(a_2)), \text{ord}_m(a_3), \dots, \text{ord}_m(a_n)),$$

que, de acuerdo al Ejercicio 6.6.2(e), es igual a

$$\text{mcm}(\text{ord}_m(a_1), \text{ord}_m(a_2), \text{ord}_m(a_3), \dots, \text{ord}_m(a_n)).$$

Esto completa la inducción y, por lo tanto, la prueba del corolario. \square

§10.6. Raíces primitivas

10.6.1. Podemos probar ahora un resultado fundamental, que tiene una demostración bastante delicada:

Proposición. Sea p un número primo y sea $n \in \mathbb{N}$. El número de enteros a tales que $1 \leq a < p$ y $a^n \equiv 1 \pmod{p}$ no supera a n .

La hipótesis de que p sea primo es en general necesaria: por ejemplo, los cuatro números 1, 4, 11 y 14 tienen todos cuadrado congruente con 1 módulo 15.

Demostración. Todas las congruencias que consideraremos en esta demostración serán módulo p y siempre que calculemos un resto será de una división por p , así que no aclararemos esto nunca. Para cada $n \in \mathbb{N}$ consideremos el conjunto

$$R(n) = \{a \in \mathbb{Z} : 1 \leq a < p, a^n \equiv 1\}$$

y, para llegar a un absurdo, supongamos que el conjunto $S = \{k \in \mathbb{N} : |R(k)| > k\}$ no es vacío. Sea n su menor elemento. Organizaremos lo que sigue, que es bastante largo, en varios pasos.

Primer paso. Sean a_1, \dots, a_t todos los elementos de $R(n)$, listados sin repeticiones, de manera que $t > n$, y sea $n' = \text{mcm}(\text{ord}_p(a_1), \dots, \text{ord}_p(a_t))$. Afirmamos que n' es igual a n .

En efecto, si $i \in \{1, \dots, t\}$, entonces $a_i^{n'} \equiv 1$, así que $\text{ord}_p(a_i)$ divide a n' : como n' es el mínimo común múltiplo de los órdenes $\text{ord}_p(a_1), \dots, \text{ord}_p(a_t)$, esto nos dice que n' divide a n . Por otro lado, si $i \in \{1, \dots, t\}$ entonces $\text{ord}_p(a_i)$ divide a n' , así que $a_i^n \equiv 1$. Vemos así que todos los elementos a_1, \dots, a_t pertenecen a $R(n')$: si fuese $n' < n$, la forma en que elegimos a n implicaría entonces que $R(n')$ tiene a lo sumo n' elementos y esto es absurdo, ya que $n' < t$. Vemos así que $n' \geq n$. Como además n' divide a n , concluimos que, de hecho, es $n' = n$, como habíamos dicho.

Usando el Corolario 10.5.9, vemos que hay enteros positivos $\alpha_1, \dots, \alpha_t$ tales que el orden del producto $a_1^{\alpha_1} \cdots a_t^{\alpha_t}$ es n . Si llamamos x al resto de la división de ese producto por p , entonces $1 \leq x < p$ y $\text{ord}_p(x) = n$. En particular, la Proposición 10.5.4 nos dice que los n enteros

$$1, x, x^2, \dots, x^{n-1} \tag{10}$$

son no congruentes dos a dos. Si $i \in \{0, \dots, n-1\}$, entonces $(x^i)^n = (x^n)^i \equiv 1$ y por lo tanto los restos de los n números de la lista (10) son n elementos distintos de $R(n)$. Más aún, tenemos que

$$\text{si } d \text{ es un divisor propio de } n, \text{ entonces } R(d) \text{ tiene exactamente } d \text{ elementos,} \\ \text{que son los restos de los enteros } 1, x^{n/d}, x^{2n/d}, \dots, x^{(d-1)n/d}. \tag{11}$$

Para verlo, basta observar que si d es un divisor propio de n , entonces los restos de los d enteros $1, x^{n/d}, x^{2n/d}, \dots, x^{(d-1)n/d}$ son distintos dos a dos y están en $R(d)$: como

$d < n$, la forma en que elegimos n implica que $R(d)$ tiene a lo sumo d elementos y , por lo tanto, tienen que ser precisamente esos.

Segundo paso. Afirmamos que

todo elemento de $R(n)$ que no es congruente con ninguno de los enteros listados en (10) tiene orden n .

Para verlo, supongamos que y es un elemento de $R(n)$ que no es congruente con ninguno de los números de (10) y sea m el orden de y . Como $y^m \equiv 1$, m divide a n . Supongamos por un momento que $m < n$, de manera que m es un divisor propio de n . De acuerdo a nuestra observación (11), los elementos de $R(m)$ son entonces los restos de $1, x^{n/m}, x^{2n/m}, \dots, x^{(m-1)n/m}$: como y pertenece a $R(m)$, vemos que y es congruente con alguno de ellos y esto es absurdo, dada la forma en que elegimos y . Esta contradicción nos dice que debe ser $m \geq n$. Como además m divide a n , tenemos en definitiva que $m = n$: el entero y tienen orden n , como queríamos ver.

Tercer paso. Sea y un elemento de $R(n)$ que no es congruente con ninguno de los enteros de la lista (10); que tal elemento existe es consecuencia de la forma en que elegimos al número n , por supuesto. Queremos probar ahora que

el número n es primo e impar.

Para ver esto, supongamos que por el contrario n es compuesto y sea q uno de sus divisores primos. Como $(y^q)^{n/q} = y^n \equiv 1$, el entero y^q es congruente a un elemento de $R(n/q)$. Como n/q es menor que n , nuestra observación (11) nos dice que los elementos de $R(n/q)$ son los restos de los enteros $1, x^q, x^{2q}, \dots, x^{(n/q-1)q}$ y esto implica que y^q es congruente con uno de ellos. En otras palabras, existe $i \in \{0, \dots, n/q - 1\}$ tal que $y^q \equiv x^{iq}$.

Como x^i es coprimo con p , sabemos que hay un entero z coprimo con p y tal que $zx^i \equiv 1$. Tenemos entonces que

$$(zy)^q \equiv z^p y^q \equiv z^q (x^i)^q \equiv (zx^i)^q \equiv 1,$$

así que el resto de zy pertenece a $R(q)$. Como los elementos de $R(q)$ son los restos de $1, x^{n/q}, \dots, x^{(q-1)n/q}$ vemos que $zy \equiv x^j$ para algún entero no negativo j . Se sigue de esto que $x^{i+j} \equiv x^i x^j \equiv x^i zy \equiv y$ y esto es absurdo en vista de la forma en que elegimos a y . Esta contradicción muestra que n tiene que ser primo.

Si z es un elemento de $R(2)$, tenemos que $z^2 \equiv 1$ y, por lo tanto, que p divide a $z^2 - 1 = (z + 1)(z - 1)$. Esto significa que z es congruente o a 1 o a -1 y, como $1 \leq z < p$, que de hecho z es o bien 1 o bien $p - 1$. Vemos así que $R(2)$ tiene a lo sumo dos elementos y entonces la forma en que elegimos n nos dice que $n > 2$. Así, n es necesariamente un primo impar.

Cuarto paso. Para cada entero u consideramos el producto

$$f(u) = (1 - u)(x - u)(x^2 - u) \cdots (x^{n-1} - u). \quad (12)$$

En particular, tenemos que

$$f(xu) = (1 - xu)(x - xu)(x^2 - xu) \cdots (x^{n-1} - xu) \quad (13)$$

Ahora bien, para cada $j \in \{1, \dots, n-1\}$ tenemos que

$$x^j - xu \equiv \begin{cases} x(x^{n-1} - u), & \text{si } j = 1; \\ x(x^{j-1} - u), & \text{si } 1 \leq j < n. \end{cases}$$

Usando esto con cada uno de los factores del producto de (13), vemos que

$$f(xu) \equiv x^n(x^{n-1} - u)(1 - u)(x - u) \cdots (x^{n-2} - u)$$

y, como $x^n \equiv 1$ y los n factores finales que aparecen en este producto son los mismos que aparecen en (12) salvo que en otro orden, que

$$f(xu) \equiv f(u).$$

Esta igualdad es cierta cualquiera sea el entero u : haciendo tomar a u los valores $u, xu, x^2u, \dots, x^{n-2}u$, en orden, vemos inmediatamente que para todo entero u se tiene que

$$f(u) \equiv f(xu) \equiv f(x^2u) \equiv \cdots \equiv f(x^{n-1}u). \quad (14)$$

Quinto paso. Volvamos ahora a considerar el producto $f(u)$ de (12): si distribuimos todos los productos que allí aparecen, obteniendo de esa forma 2^n sumandos, y los asociamos luego de acuerdo a la potencia de u que tienen como factor, encontramos que

$$f(u) = c_0 + c_1u + c_2u^2 + \cdots + c_nu^n \quad (15)$$

para ciertos enteros c_0, \dots, c_n , cada uno de los cuales es una suma con signos de productos de las potencias $1, x, \dots, x^{n-1}$. Nos interesan en particular dos de ellos:

- El entero c_0 es igual a $1 \cdot x \cdot x^2 \cdots x^{n-1} = x^{n(n-1)/2}$. Como n es impar, el cociente $(n-1)/2$ es un entero, y entonces $c_0 = (x^n)^{(n-1)/2} \equiv 1$.
- Por otro lado, es claro que $c_n = (-1)^n = -1$, ya que n es impar.

Gracias las congruencias (14), tenemos que

$$nf(u) = \underbrace{f(u) + f(u) + f(u) + \cdots + f(u) + \cdots + f(u)}_{n \text{ sumandos}}$$

$$\equiv f(u) + f(xu) + f(x^2u) + \cdots + f(x^i) + \cdots + f(x^{n-1}u)$$

Si usamos ahora la expresión (15) para cada sumando y luego cambiamos el orden de sumación, vemos que

$$nf(u) \equiv \sum_{i=0}^{n-1} \sum_{j=0}^n c_j x^{ij} u^j = \sum_{j=0}^n \left(\sum_{i=0}^{n-1} x^{ij} \right) c_j u^j$$

Cuando $j = 0$, la suma entre paréntesis es $\sum_{i=0}^{n-1} x^0 = n$. Cuando $j = n$, esa suma es $\sum_{i=0}^{n-1} (x^n)^i \equiv n$, ya que $x^n \equiv 1$. Finalmente, si $0 < j < n$, esa suma es igual a

$$\sum_{i=0}^{n-1} (x^j)^i = 0,$$

ya que el orden de x^j es n . Usando esto, vemos que $nf(u) \equiv nc_0 + nc_n u^n$ y, como n es coprimo con p , que de hecho

$$f(u) = c_0 + c_n u^n \equiv 1 - u^n.$$

Esto vale para todo entero u . En particular, como $y \in R(n)$, tenemos que

$$(1 - y)(1 - y^2) \cdots (x^{n-1} - y) = f(y) \equiv 1 - y^n \equiv 0$$

y, por lo tanto, que p divide al producto $(1 - y)(1 - y^2) \cdots (x^{n-1} - y)$. Como p es primo, esto implica que existe $i \in \{0, \dots, n-1\}$ tal que p divide a $x^i - y$, esto es, tal que $y \equiv x^i$. Esto es absurdo, ya que elegimos a y de manera que no sea congruente con ninguno de los enteros listados en (10). Esta contradicción nos dice que nuestra hipótesis de partida es insostenible y, en consecuencia, que la proposición es cierta. \square

10.6.2. La Proposición 10.6.1 nos permite probar fácilmente el siguiente resultado bastante sorprendente y notado por primera vez por Gauss —de hecho, la demostración que damos es exactamente la que él da en sus *Disquisitiones*.

Proposición. Sea p un número primo y sea n un divisor positivo de $p - 1$. El número de enteros a tales que $1 \leq a < p$ que tienen orden n es $\varphi(n)$.

Demostración. Para cada divisor d positivo de $p - 1$ consideremos el conjunto

$$\Psi(d) = \{a \in \mathbb{Z} : 1 \leq a < p, \text{ord}_p(a) = d\}$$

y sea $\psi(d) = |\Psi(d)|$ su cardinal. Como cada entero entre 1 y $p - 1$ tiene un orden módulo p que es un divisor de $p - 1$, tenemos que

$$\{a \in \mathbb{Z} : 1 \leq a < p\} = \bigcup_{d|p-1} \Psi(d),$$

con el índice d de la unión recorriendo los divisores positivos de $p - 1$, y claramente esta unión es disjunta. Tomando cardinales a ambos lados de esta igualdad, vemos que

$$p - 1 = \sum_{d|p-1} \psi(d). \quad (16)$$

Por otro lado, supongamos que d es un divisor positivo de $p - 1$ y que $\psi(d) > 0$, de manera que existe un entero y tal que $1 \leq y < p$ y $\text{ord}_p(y) = d$. En ese caso, sabemos que los restos módulo p de los enteros $1, y, y^2, \dots, y^{d-1}$ son distintos dos a dos y, por lo tanto, de acuerdo a la Proposición 10.6.1, todo número cuya potencia d -ésima es congruente con 1 módulo p es congruente a uno de ellos. En particular, todos los enteros que tienen orden d son congruentes a una de estas d potencias de y . Si $i \in \{0, \dots, d - 1\}$, sabemos que el orden de y^i es $d / \text{mcd}(d, i)$: esto nos dice que y^i tiene orden d si y solamente si i es coprimo con d . Concluimos de esta forma que el número $\psi(d)$ es o bien 0 o bien $\varphi(d)$.

Esto nos dice que para todo divisor positivo d de $p - 1$ se tiene que

$$\psi(d) \leq \varphi(d) \quad (17)$$

y, por lo tanto, que

$$\sum_{d|p-1} \psi(d) \leq \sum_{d|p-1} \varphi(d), \quad (18)$$

ya que cada sumando de la primera suma es menor o igual que el correspondiente sumando de la segunda.

Ahora bien, si para algún divisor positivo d_0 de $p - 1$ fuera $\psi(d_0) < \varphi(d_0)$, teniendo en cuenta (16), (17), (18) y la Proposición 10.2.5 tendríamos que

$$p - 1 = \sum_{d|p-1} \psi(d) < \sum_{d|p-1} \varphi(d) = p - 1.$$

Como esto es imposible, vemos que lo que afirma la proposición es cierto. \square

10.6.3. La consecuencia más importante de las dos proposiciones que acabamos de probar es:

Corolario. Sea p un número primo. Existen enteros a tales que $1 \leq a < p$ y que tienen orden módulo p igual a $p - 1$ y hay, de hecho, $\varphi(p - 1)$ de ellos.

Demostración. En efecto, esto es precisamente lo que nos dice la Proposición 10.6.2 cuando $n = p - 1$. \square

10.6.4. Si m es un entero positivo y a es un entero coprimo con m tal que $1 \leq a < m$ y $\text{ord}_m(a) = \varphi(m)$, entonces decimos que a es una **raíz primitiva** módulo m . Gauss define esta noción en el Párrafo 57 de sus *Disquisitiones*.

El Corolario **10.6.3** que acabamos de probar afirma que si p es un número primo entonces existen raíces primitivas módulo p , ya que $\varphi(p) = p - 1$. Si a es una raíz primitiva módulo p , sabemos de la Proposición **10.5.4** que las $p - 1$ potencias

$$1, a, a^2, \dots, a^{p-2}$$

son coprimas con p y no congruentes módulo p dos a dos, así que sus restos módulo p son precisamente los elementos de $\{1, \dots, p - 1\}$, listados en algún orden.

Por ejemplo, 3 es una raíz primitiva módulo 7, ya que sus primeras potencias son

$$3^0 \equiv 1, \quad 3^1 \equiv 3, \quad 3^2 \equiv 2, \quad 3^3 \equiv 6, \quad 3^4 \equiv 4, \quad 3^5 \equiv 5, \quad 3^6 \equiv 1 \pmod{7}.$$

El Corolario **10.6.3** nos dice que módulo 7 hay $\varphi(7 - 1) = 2$ raíces primitivas: la otra es 5 y la correspondiente lista de potencias es

$$5^0 \equiv 1, \quad 5^1 \equiv 5, \quad 5^2 \equiv 4, \quad 5^3 \equiv 6, \quad 5^4 \equiv 2, \quad 5^5 \equiv 3, \quad 5^6 \equiv 1 \pmod{7}.$$

En la Tabla **10.1 en la página siguiente** damos las listas de las raíces primitivas para los primeros primos.

10.6.5. Decidir si un entero a es una raíz primitiva módulo un número primo p no es fácil. Si podemos factorizar a $p - 1$, entonces la siguiente proposición nos da un criterio razonable:

Proposición. Sea p un número primo, sean q_1, \dots, q_r los divisores primos de $p - 1$ y sea a un entero tal que $1 \leq a < p - 1$. Si $a^{(p-1)/q_i} \not\equiv 1 \pmod{p}$ para cada $i \in \{1, \dots, r\}$, entonces a es una raíz primitiva módulo p .

Así, por ejemplo, el número $p = 503$ es primo y $2 \cdot 251$ es la factorización en factores primos de $p - 1$: como $2^2 \equiv 4$ y $2^{251} \equiv 2$ módulo 503, vemos que 2 es una raíz primitiva módulo 503.

Demostración. Sea n el orden de a módulo p y supongamos que a no es una raíz primitiva. Sabemos que n divide a $p - 1$. Como la hipótesis implica que $n \neq p - 1$, existe un primo q que divide a n tal que $v_q(n) < v_q(p - 1)$ y, en particular, n divide a $(p - 1)/q$. Si k es el cociente de esa división, tenemos entonces que $a^{(p-1)/q} = (a^n)^k \equiv 1 \pmod{p}$. Esto prueba la implicación contrarrecíproca a la del enunciado. \square

p	
2	1
3	2
5	2, 3
7	3, 5
11	2, 6, 7, 8
13	2, 6, 7, 11
17	3, 5, 6, 7, 10, 11, 12, 14
19	2, 3, 10, 13, 14, 15
23	5, 7, 10, 11, 14, 15, 17, 19, 20, 21
29	2, 3, 8, 10, 11, 14, 15, 18, 19, 21, 26, 27
31	3, 11, 12, 13, 17, 21, 22, 24
37	2, 5, 13, 15, 17, 18, 19, 20, 22, 24, 32, 35
41	6, 7, 11, 12, 13, 15, 17, 19, 22, 24, 26, 28, 29, 30, 34, 35
43	3, 5, 12, 18, 19, 20, 26, 28, 29, 30, 33, 34
47	5, 10, 11, 13, 15, 19, 20, 22, 23, 26, 29, 30, 31, 33, 35, 38, 39, 40, 41, 43, 44, 45
53	2, 3, 5, 8, 12, 14, 18, 19, 20, 21, 22, 26, 27, 31, 32, 33, 34, 35, 39, 41, 45, 48, 50, 51
59	2, 6, 8, 10, 11, 13, 14, 18, 23, 24, 30, 31, 32, 33, 34, 37, 38, 39, 40, 42, 43, 44, 47, 50, 52, 54, 55, 56
61	2, 6, 7, 10, 17, 18, 26, 30, 31, 35, 43, 44, 51, 54, 55, 59
67	2, 7, 11, 12, 13, 18, 20, 28, 31, 32, 34, 41, 44, 46, 48, 50, 51, 57, 61, 63
71	7, 11, 13, 21, 22, 28, 31, 33, 35, 42, 44, 47, 52, 53, 55, 56, 59, 61, 62, 63, 65, 67, 68, 69
73	5, 11, 13, 14, 15, 20, 26, 28, 29, 31, 33, 34, 39, 40, 42, 44, 45, 47, 53, 58, 59, 60, 62, 68
79	3, 6, 7, 28, 29, 30, 34, 35, 37, 39, 43, 47, 48, 53, 54, 59, 60, 63, 66, 68, 70, 74, 75, 77
83	2, 5, 6, 8, 13, 14, 15, 18, 19, 20, 22, 24, 32, 34, 35, 39, 42, 43, 45, 46, 47, 50, 52, 53, 54, 55, 56, 57, 58, 60, 62, 66, 67, 71, 72, 73, 74, 76, 79, 80
89	3, 6, 7, 13, 14, 15, 19, 23, 24, 26, 27, 28, 29, 30, 31, 33, 35, 38, 41, 43, 46, 48, 51, 54, 56, 58, 59, 60, 61, 62, 63, 65, 66, 70, 74, 75, 76, 82, 83, 86
97	5, 7, 10, 13, 14, 15, 17, 21, 23, 26, 29, 37, 38, 39, 40, 41, 56, 57, 58, 59, 60, 68, 71, 74, 76, 80, 82, 83, 84, 87, 90, 92

Tabla 10.1. Raíces primitivas para primos menores que 100.

10.6.6. Un segundo problema que aparece cuando queremos encontrar una raíz primitiva módulo un primo p es el de decidir cómo elegir qué enteros a probar. Para esto no se conoce ninguna estrategia efectiva y normalmente lo que hacemos es elegir candidatos al azar entre 1 y $p - 1$. Esto tiene sentido, porque la proporción de números en ese rango que son raíces primitivas es, de acuerdo a la Proposición 10.2.3, es

$$\frac{\varphi(p-1)}{p-1} = \left(1 - \frac{1}{q_1}\right) \cdots \left(1 - \frac{1}{q_r}\right)$$

con q_1, \dots, q_r los primos que dividen a $p - 1$, y este número no es muy cercano a 0. Los factores que aparecen a la derecha son todos menores que 1 y están más cerca de 1 mientras mayores son los divisores primos de $p - 1$: esto nos dice que si p es tal que $p - 1$ tiene pocos divisores primos y estos son grandes, entonces la proporción de raíces primitivas entre los elementos de $\{1, \dots, p - 1\}$ es relativamente alta.

Por ejemplo, el número $p = 900^{16} + 1$ es primo (probaremos esto en 10.6.14, más adelante) y $p - 1 = 2^{32} \cdot 3^{32} \cdot 5^{32}$, así que la proporción de raíces primitivas módulo p es en este caso

$$\frac{\varphi(p-1)}{p-1} = \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) \left(1 - \frac{1}{5}\right) = \frac{4}{15} \approx 0,266\ 666\dots,$$

así que cada cuatro números elegidos al azar entre 1 y $p - 1$ es razonable esperar que uno sea una raíz primitiva módulo p .

Una primera aplicación: el Teorema de Wilson

10.6.7. Como primera aplicación de la existencia de raíces primitivas módulo un número primo, podemos dar una nueva demostración del Teorema de Wilson:

Proposición. *Un entero $p > 1$ es primo si y solamente si $(p - 1)! \equiv -1 \pmod{p}$.*

Demostración. Sea p un entero mayor que 1. Veamos primero que la condición del enunciado es necesaria para que p sea primo. Si $p = 2$, entonces es inmediato que esa condición se cumple, así que bastará que consideremos el caso en que p es un número primo impar.

Sea a una raíz primitiva módulo p . Sabemos que los restos de dividir por p a los enteros

$$1, a, a^2, \dots, a^{p-2} \tag{19}$$

son los números

$$1, 2, 3, \dots, p - 1 \tag{20}$$

listados en algún orden. En particular, el producto de los $p - 1$ enteros de (19) es congruente módulo p con el producto de los de (20), esto es,

$$(p - 1)! \equiv a^0 \cdot a^1 \cdot a^2 \cdots a^{p-2} = a^{(p-1)p(p-2)/2} \pmod{p}. \quad (21)$$

Sabemos que en $\{1, \dots, p - 1\}$ hay a lo sumo dos enteros con cuadrado congruente con 1 módulo p . Como $1^1 \equiv (p - 1)^2 \equiv 1$, vemos que hay exactamente dos tales enteros y que son 1 y $p - 1$. Por otro lado, el Teorema de Fermat 10.1.4 nos dice que

$$(a^{(p-1)/2})^2 = a^{p-1} \equiv 1 \pmod{p},$$

es congruente con 1 módulo p , así que $a^{(p-1)/2}$ es congruente o con 1 o con -1 . Como el orden de a es $p - 1$, no puede ser que $a^{(p-1)/2} \equiv 1$, así que debe ser necesariamente $a^{(p-1)/2} \equiv -1$. Finalmente, como p es impar, tenemos que

$$a^{(p-1)(p-2)/2} = (a^{(p-1)/2})^{p-2} \equiv (-1)^{p-2} \equiv -1 \pmod{p}.$$

Esto junto con (21) nos dice que $(p - 1)! \equiv -1 \pmod{p}$, como queremos.

Veamos ahora la suficiencia de la condición. Si el entero p no es primo, entonces tiene un divisor d distinto de 1: como $1 < d < p$, es claro que d divide a $(p - 1)!$ y, por lo tanto, que no divide a $(p - 1)! + 1$. Esto implica que esta suma tampoco es divisible por p y, en consecuencia, que $(p - 1)! \not\equiv -1 \pmod{p}$. \square

Una segunda aplicación: el Criterio de Euler

10.6.8. Veamos ahora como usar la existencia de raíces primitivas para obtener un criterio de Euler para decidir si que un número es congruente a un cuadrado módulo un primo.

Proposición. Sea p un número primo. Un entero a coprimo con p es congruente a un cuadrado módulo p si y solamente si $a^{(p-1)/2} \equiv 1 \pmod{p}$.

Observemos que el Teorema de Fermat 10.1.4 nos dice que $a^{(p-1)/2}$ tiene cuadrado congruente con 1 módulo p , así que es congruente o bien a 1 o bien a -1 .

Demostración. Si hay un entero b tal que $a \equiv b^2 \pmod{p}$, entonces el Teorema de Fermat 10.1.4 nos dice que

$$a^{(p-1)/2} \equiv (b^2)^{(p-1)/2} = b^{p-1} \equiv 1 \pmod{p}.$$

Esto muestra que la condición de la proposición es necesaria. Veamos que es también suficiente.

Sea r una raíz primitiva módulo p , de manera que, en particular, existe un entero no negativo i tal que $a \equiv r^i \pmod{p}$. Si suponemos que la condición del enunciado vale, entonces tenemos que

$$1 \equiv a^{(p-1)/2} \equiv r^{i(p-1)/2} \pmod{p}.$$

Como r tiene orden módulo p igual a $p-1$, esto implica que $p-1$ divide a $i(p-1)/2$, lo que es posible sólo si i es par, digamos $i = 2j$ para algún entero j . Pero entonces es $a \equiv r^i \equiv (r^j)^2 \pmod{p}$ y a es congruente a un cuadrado módulo p . \square

10.6.9. Usando el Criterio de Euler **10.6.8** podemos describir muy concretamente con respecto a qué primos -1 es congruente a un cuadrado. Este resultado es conocido habitualmente como el *Primer Suplemento a la Ley de Reciprocidad Cuadrática*.

Corolario. Sea p un número primo impar. Existe un entero x tal que $x^2 \equiv -1 \pmod{p}$ si y solamente si $p \equiv 1 \pmod{4}$.

Demostración. De acuerdo al Criterio de Euler **10.6.8**, el entero -1 es congruente a un cuadrado módulo p si y solamente si $(-1)^{(p-1)/2} \equiv 1 \pmod{p}$. Ahora bien, como p es impar, es o bien de la forma $4k+1$ o bien de la forma $4k+3$, para algún entero no negativo k . En el primer caso se tiene que $(-1)^{(p-1)/2} = (-1)^{2k} = 1$ y en el segundo que $(-1)^{(p-1)/2} = (-1)^{2k+1} = -1$. Como p no es 2, $-1 \not\equiv 1 \pmod{p}$. Esto prueba el corolario. \square

10.6.10. El Criterio de Euler **10.6.8** nos permite probar también el llamado *Segundo Suplemento a la Ley de Reciprocidad Cuadrática*:

Corolario. Sea p un número primo impar. Existe un entero x tal que $x^2 \equiv 2 \pmod{p}$ si y solamente si 16 divide a $p^2 - 1$.

Como p es impar, es congruente a 1 o a 3 módulo 4, y usando esto es fácil ver que $(p^2 - 1)/8$ es un entero. La condición del corolario es entonces que este entero sea par.

Demostración. Sea $s = (p-1)/2$. Es

$$s! = \prod_{1 \leq k \leq s} k = \prod_{1 \leq k \leq s} \left((-1)^k k \cdot (-1)^k \right) = \prod_{1 \leq k \leq s} \left((-1)^k k \right) \cdot \prod_{1 \leq k \leq s} (-1)^k. \quad (22)$$

Sabemos que

$$\prod_{1 \leq k \leq s} (-1)^k = (-1)^{1+2+\dots+s} = (-1)^{s(s+1)/2}. \quad (23)$$

Por otro lado,

$$\prod_{1 \leq k \leq s} ((-1)^k k) = \prod_{\substack{1 \leq k \leq s \\ k \text{ par}}} ((-1)^k k) \cdot \prod_{\substack{1 \leq k \leq s \\ k \text{ impar}}} ((-1)^k k) = \prod_{\frac{1}{2} \leq l \leq \frac{s}{2}} (2l) \cdot \prod_{0 \leq l \leq \frac{s-1}{2}} (-(2l+1)).$$

Como $-(2l+1) \equiv 2(s-l) \pmod{p}$ para todo entero l , este último producto es congruente módulo p con

$$\prod_{\frac{1}{2} \leq l \leq \frac{s}{2}} (2l) \cdot \prod_{0 \leq l \leq \frac{s-1}{2}} (2(s-l)).$$

Cambiando el índice del segundo producto, podemos reescribir esto en la forma

$$\prod_{\frac{1}{2} \leq l \leq \frac{s}{2}} (2l) \cdot \prod_{\frac{s+1}{2} \leq l \leq s} (2l)$$

y si consideramos ahora con cuidado qué factores aparecen aquí vemos que este producto es igual a $2^s s!$. Usando esto y (23) en la igualdad (22) vemos que

$$s! \equiv (-1)^{s(s+1)/2} 2^s s! \pmod{p}.$$

Como $s!$ es coprimo con p , esto implica inmediatamente que

$$2^s \equiv (-1)^{s(s+1)/2} = (-1)^{(p^2-1)/8} \pmod{p}.$$

De acuerdo al Criterio de Euler 10.6.8, vemos que 2 es congruente con un cuadrado módulo p si y solamente si el entero $(p^2-1)/8$ es par, es decir, si y solamente si 16 divide a p^2-1 . \square

Una tercera aplicación: raíces primitivas para primos seguros

10.6.11. No hay muchos resultados que nos den raíces primitivas. Uno muy conocido es:

Proposición. Sea p un número primo tal que $2p+1$ es también primo. Si además $p \equiv 1 \pmod{4}$, entonces 2 es una raíz primitiva módulo $2p+1$.

Así, 2 es una raíz primitiva módulo $83 = 2 \cdot 41 + 1$.

Demostración. Sea p un número primo tal que $p \equiv 1 \pmod{4}$ y $q = 2p+1$ es primo. El orden de 2 módulo q , cualquiera que sea, es un divisor de $q-1 = 2p$, así que es 1, o 2, o p , o $2p$. Como $q > 4$, es claro que ni 2^1 ni 2^2 son congruentes a 1 módulo q : esto nos dice que $\text{ord}_q(2)$ no es ni 1 ni 2. Por otro lado, la Proposición 10.6.8 nos dice que $2^p = 2^{(q-1)/2}$ es congruente módulo q a 1 si y solamente si 2 es congruente a un

cuadrado módulo q , y según el Corolario 10.6.10 esto ocurre si y solamente si 16 divide a $q^2 - 1$. Como $p \equiv 1 \pmod{4}$, existe $k \in \mathbb{N}$ tal que $p = 4k + 1$: usando esto, vemos que

$$q^2 - 1 = (2p + 1)^2 - 1 = 4p^2 + 4p = 4(4k + 1)^2 + 4(4k + 1) = 64k^2 + 48k + 8.$$

Como este número no es divisible por 16, vemos que $2^p \not\equiv 1 \pmod{q}$ y, por lo tanto, $\text{ord}_q(2) \neq p$. La única posibilidad que queda, entonces, es que el orden de 2 módulo q sea $2p = q - 1$ y esto significa que 2 es una raíz primitiva módulo q . \square

10.6.12. Un número primo p tal que $2p + 1$ también es primo, como en la proposición que acabamos de probar, se llama un *primo de Sophie Germain*, por, precisamente, *Sophie Germain* (1776–1831, Francia), quien los consideró en medio de su trabajo sobre el Último Teorema de Fermat. Si p es un primo de Sophie Germain, decimos que el primo $2p + 1$ es un *primo seguro*.

Los primeros primos de Sophie Germain son

2, 3, 5, 11, 23, 29, 41, 53, 83, 89, 113, 131, 173, 179, 191, 233, 239, 251,
281, 293, 359, 419, 431, 443, 491, 509, 593, 641, 653, 659, 683, 719, 743,
761, 809, 911, 953, 1 013, 1 019, 1 031, 1 049, 1 103, 1 223, 1 229, 1 289,
1 409, 1 439, 1 451, 1 481, 1 499, 1 511, 1 559, ...

y se conjetura que hay infinitos. El más grande de ellos que conocemos (en 2016) es

$$2\,618\,163\,402\,417 \cdot 2^{1\,290\,000} - 1,$$

que tiene 388 342 dígitos decimales.

Germain aprendió matemáticas en su infancia, leyendo los libros que su padre tenía en la biblioteca —hasta aprendió por sí misma latín poder leer a Newton y a Euler— aunque sus padres no veían esto con buenos ojos: la matemática no era considerada algo muy apropiado para las mujeres. Cuando en 1794 se fundó, como parte de la Revolución Francesa, la Escuela Politécnica en París, Germain no podía asistir a las clases porque que la entrada estaba prohibida a las mujeres, pero pudo empezar sus estudios de manera no presencial —adoptando el nombre de Monsieur Antoine-August Le Blanc, para ocultar su identidad— con Joseph Louis Lagrange como tutor. Después de un tiempo, Lagrange, que estaba impresionado con las habilidades de su ‘alumno’, pidió conocerlo. Ella accedió y él no tuvo mayor problema con la novedad.

A lo largo de su vida interactuó por carta y siempre con su seudónimo masculino con varios de los más grandes matemáticos de su época —sobre todo con Adrien-Marie Legendre y Carl Gauss. Gauss fue uno de los pocos a quienes reveló su verdadera identidad. Por carta, Gauss le respondió:

Pero cómo describirte mi admiración y asombro al ver que mi estimado correspondal Sr. Le Blanc se metamorfosea en este personaje ilustre que me ofrece un

ejemplo tan brillante de lo que sería difícil de creer. La afinidad por las ciencias abstractas en general y sobre todo por los misterios de los números es demasiado rara: lo que no me asombra ya que los encantos de esta ciencia sublime solo se revelan a aquellos que tienen el valor de profundizar en ella. Pero cuando una persona del sexo que, según nuestras costumbres y prejuicios, debe encontrar muchísimas más dificultades que los hombres para familiarizarse con estos espinosos estudios, y sin embargo tiene éxito al sortear los obstáculos y penetrar en las zonas más oscuras de ellos, entonces sin duda esa persona debe tener el valor más noble, el talento más extraordinario y un genio superior. De verdad que nada podría probarme de forma tan meridiana y tan poco equívoca que los atractivos de esta ciencia que ha enriquecido mi vida con tantas alegrías no son quimeras que las predilección con la que tú has hecho honor a ella.

Un criterio de primalidad

10.6.13. Es interesante que el Corolario 10.6.3 que nos dice que para todo primo hay una raíz primitiva tiene un recíproco parcial:

Proposición. Sea $m \in \mathbb{N}$. Si existe un entero coprimo con m y de orden $m - 1$, entonces m es primo.

Demostración. En efecto, supongamos que a es un entero coprimo con m y cuyo orden módulo m es $m - 1$. En ese caso, sabemos que los enteros $1, a, a^2, \dots, a^{m-2}$ son no congruentes módulo m dos a dos. En particular, los restos módulo m de esos $m - 1$ números son todos números coprimos con m distintos y que pertenecen al conjunto $S = \{1, \dots, m - 1\}$: esto significa que esos restos son todos los elementos de S y, por lo tanto, que todos los elementos de S son coprimos con m . Por supuesto, esto implica inmediatamente que m no posee divisores propios, así que es un número primo. \square

10.6.14. Consideremos el número $m = 2^{16} + 1 = 65\,537$. Calculando las potencias elevando al cuadrado repetidas veces, vemos inmediatamente que $3^{2^{15}} \equiv 65\,536$ mientras que $3^{2^{16}} \equiv 1$, todo módulo m . Esto nos dice que 3 tiene orden $m - 1$ módulo m y, por lo tanto, que m es primo. Notemos que pudimos concluir esto hacer esto calculando solamente 16 cuadrados y 16 restos módulo m .

Sea, por otro lado, $m = 900^{16} + 1$, que es el número

185 302 018 885 184 100 000 000 000 000 000 000 000 000 000 001

de 48 dígitos. En este caso $m - 1 = 2^{32} \cdot 3^{32} \cdot 5^{32}$. Podemos calcular que $2^{m-1} \equiv 1 \pmod{m}$

haciendo 217 multiplicaciones. Otras 220 multiplicaciones nos permiten concluir que

$$2^{(m-1)/3} \equiv 23\,872\,712\,020\,769\,780\,231\,829\,076\,893\,206\,244\,805\,098\,674\,046 \\ \not\equiv 1 \pmod{m}.$$

Así, 2 tiene orden $m - 1$ módulo m y, en consecuencia, m es primo. Pudimos probar esto calculando unos 500 productos y unos 500 restos. Si hubiéramos intentado verificar que es primo probando con la división por todos los enteros menores que \sqrt{m} y a cada una de esas divisiones la hubiéramos hecho en una milésima de segundo, el proceso completo nos hubiera llevado unos trece millones de millones de años —esto es unas mil veces más que la edad del universo, según los cálculos más recientes [Plank2016].

§10.7. El Teorema de Carmichael

10.7.1. En la sección anterior probamos el Corolario 10.6.3, que afirma que módulo un primo existen raíces primitivas. Sin la condición de que el módulo sea primo en general esa conclusión no vale. Si tomamos, por ejemplo, a 8 como módulo, los elementos de $\{1, \dots, 8 - 1\}$ que son coprimos con 8 son 1, 3, 5 y 7, así que $\varphi(8) = 4$, y sus órdenes módulo 8 son a 1, 2, 2 y 2, respectivamente: se sigue de esto que ninguno de ellos es una raíz primitiva módulo 8.

Uno de nuestros objetivos en esta sección es describir exactamente para qué módulos existen raíces primitivas. Empezaremos considerando los módulos que son potencias de primos o el doble de potencias de primos y luego, usando esto, el caso general.

Raíces primitivas para módulos de la forma p^n o $2p^n$ con p primo

10.7.2. Proposición. *Sea p un número primo impar. Si a es una raíz primitiva módulo p , entonces alguno de a o $a + p$ es una raíz primitiva módulo p^2 . En particular, existen raíces primitivas módulo p^2 .*

Demostración. Sea a una raíz primitiva módulo p y sean $m = \text{ord}_{p^2}(a)$ y $n = \text{ord}_{p^2}(a + p)$ los órdenes de a y de $a + p$ módulo p^2 . El Teorema de Euler 10.3.1 implica que m y n dividen a $\varphi(p^2) = p(p - 1)$. Por otro lado, como $a^m \equiv (a + p)^n \equiv 1 \pmod{p^2}$ también tenemos que $a^m \equiv (a + p)^n \equiv 1 \pmod{p}$ y, por lo tanto, que $p - 1$ divide a m y a n , ya que los órdenes de a y de $a + p$ módulo p son ambos $p - 1$.

Supongamos ahora que ni a ni $a + p$ son raíces primitivas módulo p^2 : en vista de lo anterior, esto implica que necesariamente tenemos que $m = n = p - 1$. En particular, tenemos entonces que módulo p^2 es

$$\begin{aligned} a^{p-1} &\equiv (a + p)^{p-1} = \sum_{i=0}^{p-1} \binom{p-1}{i} a^{p-1-i} p^i \\ &= a^{p-1} + (p-1)a^{p-2}p + p^2 \sum_{i=2}^{p-1} \binom{p-1}{i} a^{p-1-i} p^{i-2} \\ &\equiv a^{p-1} + (p-1)a^{p-2}p \pmod{p^2}, \end{aligned}$$

así que $(p-1)a^{p-2}p$ es divisible por p^2 . Esto es absurdo, ya que tanto $p-1$ como a son coprimos con p . \square

10.7.3. Proposición. Sea p un número primo impar y sea $n \in \mathbb{N}$. Existe una raíz primitiva módulo p^n .

Demostración. Probemos esto haciendo inducción con respecto a n . Cuando n es 1 o 2, sabemos que hay raíces primitivas módulo p^n por el Corolario 10.6.3 y la Proposición 10.7.2, respectivamente.

Supongamos entonces que k es un entero tal que $k \geq 2$ y que existe una raíz primitiva a módulo p^k . Sea $m = \text{ord}_{p^{k+1}}(a)$. De acuerdo al Teorema de Euler 10.3.1, tenemos que m divide a $\varphi(p^{k+1}) = p^k(p-1)$. Por otro lado, como $a^m \equiv 1 \pmod{p^{k+1}}$, es $a^m \equiv 1 \pmod{p^k}$ y, por lo tanto, $\varphi(p^k) = p^{k-1}(p-1)$ divide a m . Esto significa que m es o bien $p^{k-1}(p-1)$ o bien $p^k(p-1)$, y para ver que a es una raíz primitiva módulo p^{k+1} es suficiente con mostrar que $a^{p^{k-1}(p-1)} \not\equiv 1 \pmod{p^{k+1}}$.

Ahora bien, de acuerdo al Teorema de Euler tenemos que $a^{p^{k-2}(p-1)} \equiv 1 \pmod{p^{k-1}}$, así que hay un entero x tal que

$$a^{p^{k-2}(p-1)} = 1 + p^{k-1}x \tag{24}$$

y entonces

$$a^{p^{k-1}(p-1)} = (1 + p^{k-1}x)^p = \sum_{i=0}^p \binom{p}{i} p^{i(k-1)} x^i = 1 + p^k x + \sum_{i=2}^p \binom{p}{i} p^{i(k-1)} x^i \tag{25}$$

Si $2 \leq i < p$, entonces $i(k-1) \geq k$: como p divide a $\binom{p}{i}$, vemos así que p^{k+1} divide a $\binom{p}{i} p^{i(k-1)}$. Por otro lado, como $p \geq 3$ y $k \geq 2$, es $p(k-1) \geq k+1$, así que p^{k+1} divide a $\binom{p}{i} p^{i(k-1)}$. Esto nos dice que todos los términos de la suma que aparece en (25) son divisibles por p^{k+1} y, por lo tanto, que

$$a^{p^{k-1}(p-1)} \equiv 1 + p^k x \pmod{p^{k+1}}.$$

Si tuviéramos que $a^{p^{k-1}(p-1)} \equiv 1 \pmod{p^{k+1}}$, tendríamos que $p^k x \equiv 0 \pmod{p^{k+1}}$ y, por lo tanto, que p divide a x . Esto y la igualdad (24) implican inmediatamente que $a^{p^{k-2}(p-1)} \equiv 1 \pmod{p^k}$: esto es absurdo, ya que a es una raíz primitiva módulo p^k . \square

10.7.4. Proposición. *Sea p un número primo impar y sea $n \in \mathbb{N}$. Existe una raíz primitiva módulo $2p^n$.*

Demostración. Sea a una raíz primitiva módulo p^n . Sin pérdida de generalidad, podemos suponer que a es impar: si ése no es el caso, podemos reemplazarla por $a + p^n$, que también es una raíz primitiva módulo p^n y es impar.

Como a es impar y coprimo con p^n , es coprimo con $2p^n$ y podemos considerar su orden $m = \text{ord}_{2p^n}(a)$ módulo $2p^n$. De acuerdo al Teorema de Euler 10.3.1, tenemos que m divide a $\varphi(2p^n)$. Por otro lado, como $a^m \equiv 1 \pmod{2p^n}$, es $a^m \equiv 1 \pmod{p^n}$ y, por lo tanto $\varphi(2p^n) = \varphi(p^n) = \text{ord}_{p^n}(a) \mid m$. Vemos así que $m = \varphi(2p^n)$ y, en definitiva, que a es una raíz primitiva módulo $2p^n$. \square

10.7.5. Juntando todo lo que hicimos obtenemos el siguiente resultado:

Corolario. *Hay raíces primitivas módulo 2, 4, p^n y $2p^n$ para cada primo impar p y cada $n \in \mathbb{N}$.*

Demostración. En efecto, esto sigue de las tres proposiciones que acabamos de probar y de que -1 es una raíz primitiva módulo 1 y módulo 4, como uno puede verificar inmediatamente. \square

10.7.6. En este corolario, las potencias de 2 faltan desde el cubo en adelante y esto es por buena razón:

Proposición. *Sea $n \geq 3$. No hay raíces primitivas módulo 2^n y el orden de todo entero coprimo con 2^n divide a 2^{n-2} . El orden de 5 módulo 2^n es 2^{n-2} y todo entero coprimo con 2^n es congruente a uno y sólo uno de la forma $(-1)^i 5^j$ con $0 \leq i < 2$ y $0 \leq j < 2^{n-2}$.*

Demostración. Si $k \in \mathbb{N}_0$, entonces $5^k + 1$ es par y $5^k + 1 \equiv 1^k + 1 \equiv 2 \pmod{4}$, así que

$$\text{para todo } k \in \mathbb{N}_0 \text{ es } v_2(5^k + 1) = 1. \quad (26)$$

Afirmamos que, por otro lado, se tiene que

$$\text{para todo } m \geq 2 \text{ se tiene que } v_2(5^{2^{m-2}} - 1) = m. \quad (27)$$

Podemos verlo por inducción: cuando $m = 2$ esta afirmación es evidente y si k un entero tal que $k \geq 2$ y $v_2(5^{2^{k-2}} - 1) = k$, tenemos que

$$v_2(5^{2^{k-1}} - 1) = v_2\left((5^{2^{k-2}} - 1)(5^{2^{k-2}} + 1)\right) = v_2(5^{2^{k-2}} - 1) + v_2(5^{2^{k-2}} + 1) = k + 1,$$

lo que completa la inducción.

Supongamos ahora que $n \geq 3$, como en el enunciado. La afirmación (27) nos dice que 2^n divide a $5^{2^{n-2}} - 1$, así que $5^{2^{n-2}} \equiv 1 \pmod{2^n}$ y, por lo tanto, $\text{ord}_{2^n}(5)$ divide a 2^{n-2} . Si dividiese además a 2^{n-3} , tendríamos que $2^{n-2} \mid 5^{2^{n-3}} - 1$, y esto contradice a (27). Vemos así que $\text{ord}_{2^n}(5) = 2^{n-2}$.

En particular, los 2^{n-2} enteros

$$1, 5, 5^2, \dots, 5^{2^{n-2}-1} \quad (28)$$

son no congruentes dos a dos módulo 2^n . Se sigue inmediatamente de eso que los 2^{n-2} enteros

$$-1, -5, -5^2, \dots, -5^{2^{n-2}-1} \quad (29)$$

también son no congruentes dos a dos módulo 2^n . Más aún, ningún entero de la lista (28) es congruente con ninguno de la lista (29): supongamos que, por el contrario, hay enteros $i, j \in \{0, \dots, 2^{n-2} - 1\}$ tales que $5^i \equiv -5^j \pmod{2^n}$. Si $i \geq j$, esto implica que $2^n \mid 5^j(5^{i-j} + 1)$ y, como 2 y 5 son coprimos, que $2^n \mid 5^{i-j} + 1$, de manera que $v_2(5^{i-j} + 1) \geq n \geq 3$, contra lo que afirma (26). Si en cambio $i \leq j$ podemos proceder de manera similar para llegar a otra contradicción.

Vemos así que los restos módulo 2^n de los 2^{n-1} números de la forma $(-1)^i 5^j$ con $0 \leq i < 2$ y $0 \leq j < 2^{n-2}$ son distintos dos a dos. Como todos esos restos son impares, vemos que se trata de todos los 2^{n-1} elementos impares del conjunto $\{0, \dots, 2^n - 1\}$. En otras palabras, todo entero impar a es congruente módulo 2^n a un número de la forma $(-1)^i 5^j$ con $0 \leq i < 2$ y $0 \leq j < 2^{n-2}$ y, en particular, su potencia (2^{n-2}) -ésima es congruente a

$$((-1)^i 5^j)^{2^{n-2}}$$

que es, a su vez, congruente a 1. Con esto quedan todas las afirmaciones del enunciado probadas. \square

La función de Carmichael

10.7.7. Si p es un número primo y $a \in \mathbb{N}$, escribimos

$$t(p, n) = \begin{cases} \frac{1}{2}\varphi(p^n), & \text{si } p = 2 \text{ y } n \geq 3; \\ \varphi(p^n), & \text{en caso contrario.} \end{cases}$$

y definimos una función $\lambda : \mathbb{N} \rightarrow \mathbb{N}$ de la siguiente manera: si $n \in \mathbb{N}$ y $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ es la factorización de n como producto de potencias de números primos distintos dos a dos, ponemos

$$\lambda(n) = \text{mcm}(t(p_1, \alpha_1), \dots, t(p_r, \alpha_r)).$$

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
$\lambda(n)$	1	1	2	2	4	2	6	2	6	4	10	2	12	6	4	4	16	6	18	4
$\varphi(n)$	1	1	2	2	4	2	6	4	6	4	10	4	12	6	8	8	16	6	18	8

n	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
$\lambda(n)$	6	10	22	2	20	12	18	6	28	4	30	8	10	16	12	6	36	18	12	4
$\varphi(n)$	12	10	22	8	20	12	18	12	28	8	30	16	20	16	24	12	36	18	24	16

n	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60
$\lambda(n)$	40	6	42	10	12	22	46	4	42	20	16	12	52	18	20	6	18	28	58	4
$\varphi(n)$	40	12	42	20	24	22	46	16	42	20	32	24	52	18	40	24	36	28	58	16

n	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80
$\lambda(n)$	60	30	6	16	12	10	66	16	22	12	70	6	72	36	20	18	30	12	78	4
$\varphi(n)$	60	30	36	32	48	20	66	32	44	24	70	24	72	36	40	36	60	24	78	32

n	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100
$\lambda(n)$	54	40	82	6	16	42	28	10	88	12	12	22	30	46	36	8	96	42	30	20
$\varphi(n)$	54	40	82	24	64	42	56	40	88	24	72	44	60	46	72	32	96	42	60	40

Tabla 10.2. Los primeros valores de la función λ de Carmichael, junto con los de la función φ de Euler. Marcamos en negrita los lugares donde las dos funciones difieren.

Esta es la *función de Carmichael*, por *Robert Carmichael* (1879–1967, Estados Unidos). En la Tabla 10.2 están tabulados los primeros 100 valores de esta función junto con los de la función φ de Euler, con la que coincide muchas veces.

10.7.8. Proposición. Sea $m \in \mathbb{N}$. Un entero positivo N tiene la propiedad de que para todo

entero a coprimo con n se tiene que

$$a^N \equiv 1 \pmod{m}$$

si y solamente si N es divisible por $\lambda(m)$.

Bibliografía

- [AÖ1997] A. Göksel Ağargün and E. Mehmet Özkan, *The fundamental theorem of arithmetic dissected*, *Mathematica Gazette* **81** (1997), no. 490, 53–57.
- [AÖ2001] A. Göksel Ağargün and E. Mehmet Özkan, *A historical survey of the fundamental theorem of arithmetic*, *Historia Math.* **28** (2001), no. 3, 207–214, DOI 10.1006/hmat.2001.2318. MR1849798
- [BSST1940] R. L. Brooks, Cedric A. B. Smith, Arthur Harold Stone, and William Thomas Tutte, *The dissection of rectangles into squares*, *Duke Math. J.* **7** (1940), 312–340. MR0003040
- [BS1956] Georges Browkin and André Schinzel, *Sur les nombres de Mersenne qui sont triangulaires*, *C. R. Acad. Sci. Paris* **242** (1956), 1780–1781 (French). MR0077546
- [Deh1903] Max Dehn, *Über Zerlegung von Rechtecken in Rechtecke*, *Math. Ann.* **57** (1903), no. 3, 314–332, DOI 10.1007/BF01444289 (German). MR1511212
- [HW2008] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, 6th ed., Oxford University Press, Oxford, 2008. Revised by D. R. Heath-Brown and J. H. Silverman; With a foreword by Andrew Wiles. MR2445243
- [Ken1996] Richard Kenyon, *Tiling a rectangle with the fewest squares*, *J. Combin. Theory Ser. A* **76** (1996), no. 2, 272–291, DOI 10.1006/jcta.1996.0104. MR1416017
- [Knu1969] Donald E. Knuth, *The art of computer programming. Vol. 2: Seminumerical algorithms*, Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont, 1969. MR0286318

- [Mea1973] D. G. Mead, *The equation of Ramanujan-Nagell and $[y^2]$* , Proc. Amer. Math. Soc. **41** (1973), 333–341, DOI 10.2307/2039090. MR0327725
- [PR2013] Yaroslav Pavlyukh and A. R. P. Rau, *1-, 2-, and 6-qubits, and the Ramanujan-Nagell theorem*, Int. J. Quantum Inf. **11** (2013), no. 6, 1350056, 8, DOI 10.1142/S0219749913500561. MR3149432
- [Plank2016] Planck Collaboration, P. A. R. Ade, N. Aghanim, M. Arnaud, M. Ashdown, J. Aumont, C. Baccigalupi, A. J. Banday, R. B. Barreiro, J. G. Bartlett, N. Bartolo, E. Battaner, R. Battye, K. Benabed, A. Benoît, A. Benoit-Lévy, J.-P. Bernard, M. Bersanelli, P. Bielewicz, J. J. Bock, A. Bonaldi, L. Bonavera, J. R. Bond, J. Borrill, F. R. Bouchet, F. Boulanger, M. Bucher, C. Burigana, R. C. Butler, E. Calabrese, J.-F. Cardoso, A. Catalano, A. Challinor, A. Chamballu, R.-R. Chary, H. C. Chiang, J. Chluba, P. R. Christensen, S. Church, D. L. Clements, S. Colombi, L. P. L. Colombo, C. Combet, A. Coulais, B. P. Crill, A. Curto, F. Cuttaia, L. Danese, R. D. Davies, R. J. Davis, P. de Bernardis, A. de Rosa, G. de Zotti, J. Delabrouille, F.-X. Désert, E. Di Valentino, C. Dickinson, J. M. Diego, K. Dolag, H. Dole, S. Donzelli, O. Doré, M. Douspis, A. Ducout, J. Dunkley, X. Dupac, G. Efstathiou, F. Elsner, T. A. Enßlin, H. K. Eriksen, M. Farhang, J. Fergusson, F. Finelli, O. Forni, M. Frailis, A. A. Fraisse, E. Franceschi, A. Frejsel, S. Galeotta, S. Galli, K. Ganga, C. Gauthier, M. Gerbino, T. Ghosh, M. Giard, Y. Giraud-Héraud, E. Giusarma, E. Gjerløw, J. González-Nuevo, K. M. Górski, S. Gratton, A. Gregorio, A. Gruppuso, J. E. Gudmundsson, J. Hamann, F. K. Hansen, D. Hanson, D. L. Harrison, G. Helou, S. Henrot-Versillé, C. Hernández-Monteagudo, D. Herranz, S. R. Hildebrandt, E. Hivon, M. Hobson, W. A. Holmes, A. Hornstrup, W. Hovest, Z. Huang, K. M. Huffenberger, G. Hurier, A. H. Jaffe, T. R. Jaffe, W. C. Jones, M. Juvela, E. Keihänen, R. Kesitalo, T. S. Kisner, R. Kneissl, J. Knoche, L. Knox, M. Kunz, H. Kurki-Suonio, G. Lagache, A. Lähteenmäki, J.-M. Lamarre, A. Lasenby, M. Lattanzi, C. R. Lawrence, J. P. Leahy, R. Leonardi, J. Lesgourgues, F. Levrier, A. Lewis, M. Liguori, P. B. Lilje, M. Linden-Vørnle, M. López-Caniiego, P. M. Lubin, J. F. Macías-Pérez, G. Maggio, D. Maino, N. Mandolesi, A. Mangilli, A. Marchini, M. Maris, P. G. Martin, M. Martinelli, E. Martínez-González, S. Masi, S. Matarrese, P. McGehee, P. R. Meinhold, A. Melchiorri, J.-B. Melin, L. Mendes, A. Mennella, M. Migliaccio, M. Millea, S. Mitra, M.-A. Miville-Deschênes, A. Moneti, L. Montier, G. Morgante, D. Mortlock, A. Moss, D. Munshi, J. A. Murphy, P. Naselsky, F. Nati, P. Natoli, C. B. Netterfield, H. U. Nørgaard-Nielsen, F. Noviello, D. Novikov, I. Novikov, C. A. Oxborrow, F. Paci, L. Pagano, F. Pajot, R. Paladini, D. Paoletti, B.

Partridge, F. Pasian, G. Patanchon, T. J. Pearson, O. Perdereau, L. Perotto, F. Perrotta, V. Pettorino, F. Piacentini, M. Piat, E. Pierpaoli, D. Pietrobon, S. Plaszczynski, E. Pointecouteau, G. Polenta, L. Popa, G. W. Pratt, G. Prézeau, S. Prunet, J.-L. Puget, J. P. Rachen, W. T. Reach, R. Rebolo, M. Reinecke, M. Remazeilles, C. Renault, A. Renzi, I. Ristorcelli, G. Rocha, C. Rosset, M. Rossetti, G. Roudier, B. Rouillé d'Orfeuil, M. Rowan-Robinson, J. A. Rubiño-Martín, B. Rusholme, N. Said, V. Salvatelli, L. Salvati, M. Sandri, D. Santos, M. Savelainen, G. Savini, D. Scott, M. D. Seiffert, P. Serra, E. P. S. Shellard, L. D. Spencer, M. Spinelli, V. Stolyarov, R. Stompor, R. Sudiwala, R. Sunyaev, D. Sutton, A.-S. Suur-Uski, J.-F. Sygnet, J. A. Tauber, L. Terenzi, L. Toffolatti, M. Tomasi, M. Tristram, T. Trombetti, M. Tucci, J. Tuovinen, M. Türlér, G. Umama, L. Valenziano, J. Valiviita, F. Van Tent, P. Vielva, F. Villa, L. A. Wade, B. D. Wandelt, I. K. Wehus, M. White, S. D. M. White, A. Wilkinson, D. Yvon, A. Zacchei, and A. Zonca, *Planck 2015 results - XIII. Cosmological parameters*, *A&A* **594** (2016), A13, DOI 10.1051/0004-6361/201525830.

- [SS1959] H. S. Shapiro and D. L. Slotnick, *On the mathematical theory of error-correcting codes*, *IBM J. Res. Develop.* **3** (1959), 25–34, DOI 10.1147/rd.31.0025. MR0098636
- [Spr1940] Roland Sprague, *Zur Abschätzung der Mindestzahl inkongruenter Quadrate, die ein gegebenes Rechteck ausfüllen*, *Math. Z.* **46** (1940), 460–471, DOI 10.1007/BF01181451 (German). MR0002188
- [Sta2015] Richard P. Stanley, *Catalan numbers*, Cambridge University Press, New York, 2015. MR3467982
- [Rom2015] Steven Roman, *An introduction to Catalan numbers*, Compact Textbooks in Mathematics, Birkhäuser/Springer, Cham, 2015. With a foreword by Richard Stanley. MR3380815
- [Gri2012] Ralph P. Grimaldi, *Fibonacci and Catalan numbers*, John Wiley & Sons, Inc., Hoboken, NJ, 2012. An introduction. MR2963306
- [Kos2009] Thomas Koshy, *Catalan numbers with applications*, Oxford University Press, Oxford, 2009. MR2526440
- [Zec1972] Édouard Zeckendorf, *Représentation des nombres naturels par une somme de nombres de Fibonacci ou de nombres de Lucas*, *Bull. Soc. R. Sci. Liège* **41** (1972), 179–182.