

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 $b | a$ 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. Una observación inmediata sobre los primos es la siguiente:

Proposición. *Sea p un número primo y sea a un entero cualquiera. El máximo común divisor $\text{mcd}(p, a)$ es o 1 o p , y el segundo caso ocurre si y solamente si p divide a a .*

Demostración. En efecto, el número $\text{mcd}(p, a)$ es un divisor de p , así que es o 1 o p , y es p exactamente cuando p divide a a . \square

9.1.3. 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 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 $P(2)$, $P(3)$, ..., $P(k-1)$ 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.

Ahora bien, este número l puede ser primo o no. Si es primo, entonces es un divisor primo de k menor que k y 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 $p | l$. Como $l | k$, gracias a transitividad de la divisibilidad tenemos que $p | k$: vemos así que p es un primo que divide a k y, como es menor que l , que es menor que k . Esto muestra que en cualquiera de los dos casos la afirmación $P(k)$ vale y completa la inducción. \square

9.1.4. 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.*

Muchas veces usamos esto para probar que un número positivo es igual a 1: mostramos que no es divisible por ningún número primo.

Demostración. 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

9.1.5. Apoyándonos en la Proposición 9.1.3, 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

(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:

(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

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

(2)	(3)	(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

```

module Primos where

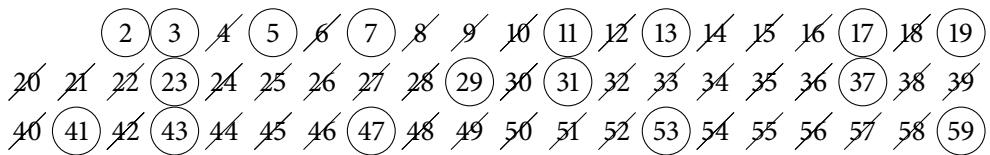
primos :: Integer -> [Integer]
primos n = cribar [2 .. n]

cribar :: [Integer] -> [Integer]
cribar []      = []
cribar (x : xs) = x : cribar [i | i <- xs, i `mod` x /= 0]

```

Programa 9.1. Una implementación de la criba de Eratóstenes en HASKELL. El valor de la expresión `primos n` es 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 primo 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.

hacer eso, lo que tenemos es:



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 estos son precisamente los números primos menores o iguales a 59.

Este procedimiento se llama la *criba¹ de Eratóstenes*, por Eratóstenes de Cirena, 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. En la computadora del autor, esta implementación determina la lista de los primos menores que 100 000, que son 9 592, en 20 segundos.

9.1.6. 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,

¹La palabra *criba* designa el utensilio que se usa para cribar, es decir, para filtrar y seleccionar semillas o minerales.

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.

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 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 esta proposición es 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 9.1.3 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

9.1.7. Otra consecuencia importante de la Proposición 9.1.3 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

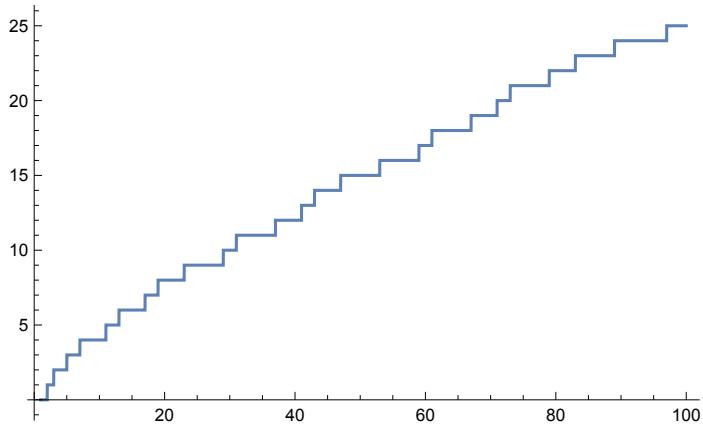


Figura 9.1. La función π en el intervalo $[0, 100]$.

k es igual a un producto de números primos con un sólo factor. Supongamos entonces que, por el contrario, k no es primo. La Proposición 9.1.3 nos dice que hay un número primo p menor k tal que $p \mid k$ y, en consecuencia, que hay entonces un entero positivo l tal que $k = pl$. Como $p \geq 2$ y, por lo tanto,

$$l = \frac{k}{p} \leq \frac{k}{2} < k,$$

tenemos que $1 \leq l < k$. En particular, nuestra hipótesis inductiva nos dice que la afirmación $P(l)$ vale, es decir, que l es igual a un producto de números primos: existen $r \in \mathbb{N}_0$ y números primos p_1, \dots, p_r tales que $l = p_1 \cdots p_r$. Como entonces $k = pl = pp_1 \cdots p_r$, vemos que k es igual a un producto de números primos, es decir, que $P(k)$ vale. Esto completa la inducción. \square

9.1.8. La Proposición 9.1.6 nos dice que hay infinitos números primos. Podemos ser más ambiciosos y hacernos la siguiente pregunta: si x es un número real positivo, ¿cuántos números primos que menores que x ? En otras palabras, esta pregunta pide determinar el entero

$$\pi(x) := |\{n \in \mathbb{N} : n \text{ es primo y } n \leq x\}|.$$

Notemos que de esta forma obtenemos una función $\pi : [0, +\infty) \rightarrow \mathbb{R}$. Si tenemos a nuestra disposición una tabla de números primos o, mejor, una computadora, podemos evaluar π fácilmente. En la Figura 9.1 podemos ver el gráfico de la función π en el intervalo $[0, 100]$.

La Proposición 9.1.6 nos dice que la función π no está acotada superiormente y si analizamos la forma en la que la probamos podemos obtener también una cota inferior para ella:

Proposición. Para todo $n \geq 2$ vale que $\pi(n) \geq \ln \ln n$.

Esta cota inferior crece de manera extremadamente lenta con n y resulta no ser particularmente buena. Nos dice, por ejemplo, que $\pi(10^{15}) \geq \ln \ln 10^{15} = 3,542\,082\dots$, lo que es cierto, ya que $\pi(10^{15}) = 29\,844\,570\,422\,669$, pero claramente no es muy informativo!

Demostración. Sea p_1, p_2, p_3, \dots , la lista en orden creciente de los números primos. Mostremos que para cada $n \in \mathbb{N}$ vale que

$$p_n \leq 2^{2^{n-1}}. \quad (2)$$

Esto ciertamente es cierto cuando n es 1, ya que $p_1 = 2 \leq 2^{2^{1-1}}$. Supongamos, por otro lado, que k es un elemento cualquiera de \mathbb{N} mayor que 1 y que sabemos que la desigualdad (2) es cierta siempre que $1 \leq n < k$. El número $p_1 \cdots p_{k-1} + 1$ es mayor que 1, así que es divisible por algún primo: como no es divisible por ninguno de los primos p_1, p_2, \dots, p_{k-1} , tiene que ser divisible por algún primo mayor o igual que p_k y, en particular,

$$p_k \leq p_1 p_2 \cdots p_{k-1} + 1 \leq 2^{2^{1-1}} 2^{2^{2-1}} \cdots 2^{2^{(k-1)-1}} + 1 = 2^{2^0 + 2^1 + \cdots + 2^{k-2}} + 1 = 2^{2^{k-1}-1} + 1.$$

Como $k \geq 2$, es $2^{k-1} - 1 \geq 2^1 - 1 = 1$, así que $2^{2^{k-1}-1} \geq 1 \geq 1$ y

$$2^{2^{k-1}-1} + 1 \leq 2^{2^{k-1}-1} + 2^{2^{k-1}-1} = 2 \cdot 2^{2^{k-1}-1} = 2^{2^{k-1}}.$$

Esto nos dice que la desigualdad (2) vale cuando n es k . Esa desigualdad es, por lo tanto, cierta para cualquier $n \in \mathbb{N}$. Notemos que esto nos dice que n es un elemento cualquiera de \mathbb{N} , entonces $p_n \leq 2^{2^{n-1}}$ y, por lo tanto, $\pi(2^{2^{n-1}}) \geq n$.

Sea ahora n un entero mayor que 2 y sea $m := \lfloor \log_2 \log_2 n \rfloor$. Es $m \leq \log_2 \log_2 n < m + 1$, así que $2^m \leq \log_2 n$, $2^{2^m} \leq n <$ y, por lo tanto,

$$\log_2 \log_2 n < m + 1 \leq \pi(2^{2^m}) \leq \pi(n). \quad (3)$$

Es $0 < \ln 2 < 1$, ya que $2 < e$, así que para todo número real x mayor que 1 es $\log_2 x = \ln x / \ln 2 > \ln x$. Como la función \log_2 es creciente, esto implica a su vez que para todo número real x tal que $\ln x$ es mayor que 1 es

$$\log_2 \log_2 x \geq \log_2 \ln x > \ln \ln x.$$

Combinando esta desigualdad con la de (3) obtenemos la de la proposición. \square

9.1.9. Un resultado fundamental de la teoría de números es el siguiente teorema, usualmente llamado el *teorema de los números primos*:

Teorema. Si x es un número real suficientemente grande, entonces $\pi(x) \sim \frac{x}{\ln x}$. □

Explícitamente, lo que queremos decir aquí es que cuando el número x es grande el cociente de $\pi(x)$ y de $x/\ln x$ se aproxima a 1, esto es, que

$$\lim_{x \rightarrow \infty} \frac{\pi(x)}{x/\ln x} = 1.$$

El primero en conjeturar que la función π puede aproximarse por una expresión como la que aparece en el teorema fue Adrien-Marie Legendre, en 1797, en base a la consideración de tablas de primos elaboradas por Anton Felkel y Jurij Bartolomej Vega²

El problema de aproximar π fue considerado desde entonces por muchos matemáticos — Carl Friedrich Gauss, Peter Gustav Lejeune Dirichlet, Pafnuty Chebyshev, Leonhard Euler, Bernhard Riemann, entre muchos otros — pero el teorema de los números primos fue probado por primera vez recién por Jacques Hadamard [Had1896] y Charles Jean de la Vallée Poussin [dLVP1896a, dLVP1896b, dLVP1896c, dLVP1897a, dLVP1897b] en trabajos independientes y casi simultáneos basados de manera esencial en ideas de Riemann. Hoy se conocen varias pruebas del teorema y todas son largas y complicadas. La más sencilla fue encontrada por Donald Joseph Newman en 1980 [New1980]; una versión de esta de Don Zagier puede encontrarse en [Zag1997].

Una consecuencia directa del teorema es la observación de que cuando n es un entero positivo grande podemos dar una aproximación para el n -ésimo primo p_n :

$$p_n \sim n \ln n. \tag{4}$$

Por ejemplo, el primo 10^{15} -avo es

$$p_{10^{15}} = 37\,124\,508\,045\,065\,437$$

mientras que

$$10^{15} \ln 10^{15} \sim 34\,538\,776\,394\,910\,685,260\,269\dots$$

La diferencia entre $p_{10^{15}}$ y $10^{15} \ln 10^{15}$ es grande, del orden de 10^{15} , pero el error relativo de la aproximación es pequeño y menor que el 7 %:

$$\frac{p_{10^{15}} - 10^{15} \ln 10^{15}}{p_{10^{15}}} = 0,069\,650\,3\dots$$

²Felkel había publicado entre 1776 y 1777 una tabla [Fel1776] que daba la factorización de todos los números coprimos con 30 entre 1 y 10 000 000. En la Figura 9.2 puede verse una página de este trabajo. El trabajo matemático más famoso de Vega, por su parte, es una serie de volúmenes con tablas de logaritmos decimales y funciones trigonométricas, en los que trabajó durante toda su vida. Además de eso, Vega se dedicó a la astronomía, a la física y a la balística. Hay un cráter en la luna que lleva su nombre, con coordenadas $45.4^\circ S$ $63.4^\circ E$.

	Factores ab 150001 usque 156000.																									
	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
150-1	$f \cdot g^2$	$151-1$	B	$152-1$	C	$153-1$	D	$154-1$	E	$155-1$	F	$156-1$	G	$157-1$	H	$158-1$	I	$159-1$	J	$160-1$	K	$161-1$	L	$162-1$	M	
150-2	$f \cdot g^2$	$151-2$	B	$152-2$	C	$153-2$	D	$154-2$	E	$155-2$	F	$156-2$	G	$157-2$	H	$158-2$	I	$159-2$	J	$160-2$	K	$161-2$	L	$162-2$	M	
150-3	$f \cdot g^2$	$151-3$	B	$152-3$	C	$153-3$	D	$154-3$	E	$155-3$	F	$156-3$	G	$157-3$	H	$158-3$	I	$159-3$	J	$160-3$	K	$161-3$	L	$162-3$	M	
150-4	$f \cdot g^2$	$151-4$	B	$152-4$	C	$153-4$	D	$154-4$	E	$155-4$	F	$156-4$	G	$157-4$	H	$158-4$	I	$159-4$	J	$160-4$	K	$161-4$	L	$162-4$	M	
150-5	$f \cdot g^2$	$151-5$	B	$152-5$	C	$153-5$	D	$154-5$	E	$155-5$	F	$156-5$	G	$157-5$	H	$158-5$	I	$159-5$	J	$160-5$	K	$161-5$	L	$162-5$	M	
150-6	$f \cdot g^2$	$151-6$	B	$152-6$	C	$153-6$	D	$154-6$	E	$155-6$	F	$156-6$	G	$157-6$	H	$158-6$	I	$159-6$	J	$160-6$	K	$161-6$	L	$162-6$	M	
150-7	$f \cdot g^2$	$151-7$	B	$152-7$	C	$153-7$	D	$154-7$	E	$155-7$	F	$156-7$	G	$157-7$	H	$158-7$	I	$159-7$	J	$160-7$	K	$161-7$	L	$162-7$	M	
150-8	$f \cdot g^2$	$151-8$	B	$152-8$	C	$153-8$	D	$154-8$	E	$155-8$	F	$156-8$	G	$157-8$	H	$158-8$	I	$159-8$	J	$160-8$	K	$161-8$	L	$162-8$	M	
150-9	$f \cdot g^2$	$151-9$	B	$152-9$	C	$153-9$	D	$154-9$	E	$155-9$	F	$156-9$	G	$157-9$	H	$158-9$	I	$159-9$	J	$160-9$	K	$161-9$	L	$162-9$	M	
150-10	$f \cdot g^2$	$151-10$	B	$152-10$	C	$153-10$	D	$154-10$	E	$155-10$	F	$156-10$	G	$157-10$	H	$158-10$	I	$159-10$	J	$160-10$	K	$161-10$	L	$162-10$	M	
150-11	$f \cdot g^2$	$151-11$	B	$152-11$	C	$153-11$	D	$154-11$	E	$155-11$	F	$156-11$	G	$157-11$	H	$158-11$	I	$159-11$	J	$160-11$	K	$161-11$	L	$162-11$	M	
150-12	$f \cdot g^2$	$151-12$	B	$152-12$	C	$153-12$	D	$154-12$	E	$155-12$	F	$156-12$	G	$157-12$	H	$158-12$	I	$159-12$	J	$160-12$	K	$161-12$	L	$162-12$	M	
150-13	$f \cdot g^2$	$151-13$	B	$152-13$	C	$153-13$	D	$154-13$	E	$155-13$	F	$156-13$	G	$157-13$	H	$158-13$	I	$159-13$	J	$160-13$	K	$161-13$	L	$162-13$	M	
150-14	$f \cdot g^2$	$151-14$	B	$152-14$	C	$153-14$	D	$154-14$	E	$155-14$	F	$156-14$	G	$157-14$	H	$158-14$	I	$159-14$	J	$160-14$	K	$161-14$	L	$162-14$	M	
150-15	$f \cdot g^2$	$151-15$	B	$152-15$	C	$153-15$	D	$154-15$	E	$155-15$	F	$156-15$	G	$157-15$	H	$158-15$	I	$159-15$	J	$160-15$	K	$161-15$	L	$162-15$	M	
150-16	$f \cdot g^2$	$151-16$	B	$152-16$	C	$153-16$	D	$154-16$	E	$155-16$	F	$156-16$	G	$157-16$	H	$158-16$	I	$159-16$	J	$160-16$	K	$161-16$	L	$162-16$	M	
150-17	$f \cdot g^2$	$151-17$	B	$152-17$	C	$153-17$	D	$154-17$	E	$155-17$	F	$156-17$	G	$157-17$	H	$158-17$	I	$159-17$	J	$160-17$	K	$161-17$	L	$162-17$	M	
150-18	$f \cdot g^2$	$151-18$	B	$152-18$	C	$153-18$	D	$154-18$	E	$155-18$	F	$156-18$	G	$157-18$	H	$158-18$	I	$159-18$	J	$160-18$	K	$161-18$	L	$162-18$	M	
150-19	$f \cdot g^2$	$151-19$	B	$152-19$	C	$153-19$	D	$154-19$	E	$155-19$	F	$156-19$	G	$157-19$	H	$158-19$	I	$159-19$	J	$160-19$	K	$161-19$	L	$162-19$	M	
150-20	$f \cdot g^2$	$151-20$	B	$152-20$	C	$153-20$	D	$154-20$	E	$155-20$	F	$156-20$	G	$157-20$	H	$158-20$	I	$159-20$	J	$160-20$	K	$161-20$	L	$162-20$	M	
150-21	$f \cdot g^2$	$151-21$	B	$152-21$	C	$153-21$	D	$154-21$	E	$155-21$	F	$156-21$	G	$157-21$	H	$158-21$	I	$159-21$	J	$160-21$	K	$161-21$	L	$162-21$	M	
150-22	$f \cdot g^2$	$151-22$	B	$152-22$	C	$153-22$	D	$154-22$	E	$155-22$	F	$156-22$	G	$157-22$	H	$158-22$	I	$159-22$	J	$160-22$	K	$161-22$	L	$162-22$	M	
150-23	$f \cdot g^2$	$151-23$	B	$152-23$	C	$153-23$	D	$154-23$	E	$155-23$	F	$156-23$	G	$157-23$	H	$158-23$	I	$159-23$	J	$160-23$	K	$161-23$	L	$162-23$	M	
150-24	$f \cdot g^2$	$151-24$	B	$152-24$	C	$153-24$	D	$154-24$	E	$155-24$	F	$156-24$	G	$157-24$	H	$158-24$	I	$159-24$	J	$160-24$	K	$161-24$	L	$162-24$	M	
150-25	$f \cdot g^2$	$151-25$	B	$152-25$	C	$153-25$	D	$154-25$	E	$155-25$	F	$156-25$	G	$157-25$	H	$158-25$	I	$159-25$	J	$160-25$	K	$161-25$	L	$162-25$	M	
150-26	$f \cdot g^2$	$151-26$	B	$152-26$	C	$153-26$	D	$154-26$	E	$155-26$	F	$156-26$	G	$157-26$	H	$158-26$	I	$159-26$	J	$160-26$	K	$161-26$	L	$162-26$	M	
150-27	$f \cdot g^2$	$151-27$	B	$152-27$	C	$153-27$	D	$154-27$	E	$155-27$	F	$156-27$	G	$157-27$	H	$158-27$	I	$159-27$	J	$160-27$	K	$161-27$	L	$162-27$	M	
150-28	$f \cdot g^2$	$151-28$	B	$152-28$	C	$153-28$	D	$154-28$	E	$155-28$	F	$156-28$	G	$157-28$	H	$158-28$	I	$159-28$	J	$160-28$	K	$161-28$	L	$162-28$	M	
150-29	$f \cdot g^2$	$151-29$	B	$152-29$	C	$153-29$	D	$154-29$	E	$155-29$	F	$156-29$	G	$157-29$	H	$158-29$	I	$159-29$	J	$160-29$	K	$161-29$	L	$162-29$	M	
150-30	$f \cdot g^2$	$151-30$	B	$152-30$	C	$153-30$	D	$154-30$	E	$155-30$	F	$156-30$	G	$157-30$	H	$158-30$	I	$159-30$	J	$160-30$	K	$161-30$	L	$162-30$	M	
150-31	$f \cdot g^2$	$151-31$	B	$152-31$	C	$153-31$	D	$154-31$	E	$155-31$	F	$156-31$	G	$157-31$	H	$158-31$	I	$159-31$	J	$160-31$	K	$161-31$	L	$162-31$	M	
150-32	$f \cdot g^2$	$151-32$	B	$152-32$	C	$153-32$	D	$154-32$	E	$155-32$	F	$156-32$	G	$157-32$	H	$158-32$	I	$159-32$	J	$160-32$	K	$161-32$	L	$162-32$	M	
150-33	$f \cdot g^2$	$151-33$	B	$152-33$	C	$153-33$	D	$154-33$	E	$155-33$	F	$156-33$	G	$157-33$	H	$158-33$	I	$159-33$	J	$160-33$	K	$161-33$	L	$162-33$	M	
150-34	$f \cdot g^2$	$151-34$	B	$152-34$	C	$153-34$	D	$154-34$	E	$155-34$	F	$156-34$	G	$157-34$	H	$158-34$	I	$159-34$	J	$160-34$	K	$161-34$	L	$162-34$	M	
150-35	$f \cdot g^2$	$151-35$	B	$152-35$	C	$153-35$	D	$154-35$	E	$155-35$	F	$156-35$	G	$157-35$	H	$158-35$	I	$159-35$	J	$160-35$	K	$161-35$	L	$162-35$	M	
150-36	$f \cdot g^2$	$151-36$	B	$152-36$	C	$153-36$	D	$154-36$	E	$155-36$	F	$156-36$	G	$157-36$	H	$158-36$	I	$159-36$	J	$160-36$	K	$161-36$	L	$162-36$	M	
150-37	$f \cdot g^2$	$151-37$	B	$152-37$	C	$153-37$	D	$154-37$	E	$155-37$	F	$156-37$	G	$157-37$	H	$158-37$	I	$159-37$	J	$160-37$	K	$161-37$	L	$162-37$	M	
150-38	$f \cdot g^2$	<																								

Figura 9.2. Una página de la tabla de Anton Felkel con la factorización de todos los enteros positivos coprimos con 30 y menores que 10 000 000. El libro puede encontrarse entero en versión electrónica en la URL incluida en la referencia [Fel1776]. La computadora del autor de estas notas puede generar esa tabla completa en 16 segundos.

Es en este sentido que debe entenderse la aproximación (4): el límite cuando n crece del error relativo de la aproximación es 0.

Es de notar que se conocen aproximaciones al n -ésimo primo mucho mejores que la de (4), que se deducen de resultados más precisos que el teorema de los números primos. Por ejemplo, Ernesto Cesàro probó en [Ces1894] que para cada entero positivo n es

$$\frac{p_n}{n} = \ln n + \ln \ln n - 1 + \frac{\ln \ln n - 2}{\ln n} - \frac{(\ln \ln n)^2 - 6 \ln \ln n + 11}{2(\ln n)^2} + \varepsilon_n,$$

con ε_n un número tal que

$$\lim_{n \rightarrow \infty} \frac{\varepsilon_n}{1/(\ln n)^2} = 0.$$

Esto nos dice que 10^{15} -avo primo $p_{10^{15}}$ es aproximadamente igual a

$$37\,124\,545\,467\,703\,341,527\,861\dots$$

Esta aproximación tiene un error relativo de 0,000 100 8 %, extraordinariamente mejor que la anterior.

Una segunda consecuencia del teorema es que si N es un entero positivo grande, entonces la proporción de números primos en el conjunto $\{1, \dots, N\}$ es aproximadamente

$$\frac{\pi(N)}{N} \sim \frac{N/\ln N}{N} = \frac{1}{\ln N}. \quad (5)$$

Esto nos dice que cuando N crece cada vez hay relativamente menos y menos primos en el conjunto $\{1, \dots, N\}$, porque sabemos que $\lim_{N \rightarrow \infty} \ln N = +\infty$. De todas formas, como la función \ln crece de manera muy lenta con su argumento, esta proporción decrece muy lentamente. Por ejemplo, hay $\pi(10^{15}) = 29\,844\,570\,422\,669$ y $\pi(10^{20}) = 2\,220\,819\,602\,560\,918\,840$ primos en los conjuntos $\{1, \dots, 10^{15}\}$ y $\{1, \dots, 10^{20}\}$, así que las proporciones de primos en esos conjuntos son

$$\frac{\pi(10^{15})}{10^{15}} = 0,029\,844\dots \qquad \qquad \frac{\pi(10^{20})}{10^{20}} = 0,022\,208\dots$$

mientras que las estimaciones dadas por (5) para esas proporciones son

$$\frac{1}{\ln 10^{15}} = 0,028\,953\dots \qquad \qquad \frac{1}{\ln 10^{20}} = 0,021\,714\dots$$

§9.2. El Teorema Fundamental de la Aritmética

9.2.1. En la sección anterior probamos la Proposición 9.1.7, que nos dice que todo entero positivo es igual a un producto de números primos. Nuestro objetivo en esta es mostrar que, de hecho, ese producto de primos es esencialmente único.

9.2.2. El primer paso para eso es establecer la siguiente caracterización de los números primos, usualmente conocida como el *Lema de Euclides* — es la Proposición 30 del libro VII de sus *Elementos*.

Proposición. *Un número p mayor que 1 es primo si y solamente si cada vez que divide al producto de dos enteros divide a alguno de ellos.*

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 al producto 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. Por otro lado, de acuerdo a la identidad de Bézout 6.4.10, 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.

Probemos ahora 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 parte 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 enteros. 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 es un elemento cualquiera de \mathbb{N} tal 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 $P(k)$ 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 9.1.7, 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

$$n = p_1 \cdots p_r. \quad (6)$$

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 $p_1 \leq p_2 \leq \cdots \leq p_r$. Mostraremos ahora que, bajo esta condición extra, hay exactamente *una* factorización de n como la de (6).

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

$$p_1 \leq \cdots \leq p_r, \quad q_1 \leq \cdots \leq q_s \quad y \quad p_1 \cdots p_r = q_1 \cdots q_s,$$

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 $p_1 \leq \cdots \leq p_r$, $q_1 \leq \cdots \leq q_s$ 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 que p_1, \dots, p_r y q_1, \dots, q_s son números primos tales que $p_1 \leq \cdots \leq p_r$, $q_1 \leq \cdots \leq q_s$ y $1 = p_1 \cdots p_r = q_1 \cdots q_s$. Si $r > 0$, entonces el número primo p_1 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.

Sea ahora k un elemento cualquiera de \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

$$k = p_1 \cdots p_r = q_1 \cdots q_s. \quad (7)$$

No puede ser que se tenga que $p_r < q_s$. En efecto, si fuera ese el caso, como q_s divide a $k = p_1 \cdots p_r$, el Corolario 9.2.3 nos diría que existe $i \in \{1, \dots, r\}$ tal que q_s divide a p_i , y esto es imposible porque $p_i \leq p_r < q_s$. De manera similar podemos ver que no puede ser que $p_r > q_s$, y concluir, en definitiva, que $p_r = q_s$. Si ponemos $l := k/p_r$, de la igualdad (7) deducimos, dividiendo en cada miembro por p_r , que

$$l = p_1 \cdots p_{r-1} = q_1 \cdots q_{s-1}. \quad (8)$$

Ahora bien, este entero l es positivo y estrictamente menor que k (porque $p_r \geq 2$), así que nuestra hipótesis inductiva nos dice que la afirmación $P(l)$ vale. Usándola en (8), 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

9.2.5. Podemos ahora enunciar y probar el llamado *Teorema fundamental de la aritmética*:

Proposición. Si n es un entero positivo, entonces existen

- un entero no negativo $s \in \mathbb{N}_0$,
- números primos p_1, \dots, p_s y
- enteros positivos a_1, \dots, a_s

tales que $p_1 < \dots < p_s$ y $n = p_1^{a_1} \cdots p_s^{a_s}$ y, más aún, todos ellos están únicamente determinados por n .

Demostración. Sea n un entero positivo. De la Proposición 9.1.7 sabemos que existen $r \in \mathbb{N}_0$ y números primos q_1, \dots, q_r tales que $n = p_1 \cdots p_r$. Más aún, como observamos en 9.2.4, podemos suponer sin pérdida de generalidad que $q_1 \leq \dots \leq q_r$, ya que si no es ese el caso basta reindexar apropiadamente los primos q_1, \dots, q_r .

Los primos q_1, \dots, q_r no son necesariamente distintos dos a dos. Sea s la cantidad de elementos del conjunto $\{q_1, \dots, q_r\}$, sean p_1, \dots, p_s los elementos de este conjunto listados en orden estrictamente creciente y para cada $i \in \{1, \dots, s\}$ sea a_i la cantidad de veces que el primo p_i aparece en la

lista q_1, \dots, q_r , es decir, el cardinal del conjunto $\{j \in \{1, \dots, r\} : q_j = p_i\}$. Es claro, entonces, que

$$n = q_1 \cdots q_r = \underbrace{p_1 \cdots p_1}_{a_1 \text{ factores}} \underbrace{p_2 \cdots p_2}_{a_2 \text{ factores}} \cdots \underbrace{p_s \cdots p_s}_{a_s \text{ factores}} = p_1^{a_1} \cdots p_s^{a_s}.$$

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 $a_1 + \cdots + a_r$ números primos y los factores están en orden no decreciente, mientras que a la derecha tenemos un producto de $b_1 + \cdots + b_s$ números primos también listados en orden no decreciente. De acuerdo a la Proposición 9.1.7, entonces, a ambos lados de la igualdad tenemos la misma cantidad de factores, así que $a_1 + \cdots + a_r = b_1 + \cdots + b_s$, 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

9.2.6. 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 9.1.4, que usamos 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 las dos partes de la Proposición 9.2.5 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 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, Leonhard 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 9.3 en la página siguiente reproducimos el pasaje relevante.

16.

THEOREMA. *Numerus compositus quicunque 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 alias primos quam a, b, c etc. ingredi non posse, quum quicunque alias 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 plures 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 9.3. 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».

En el trabajo [AO2001] puede encontrarse una descripción detallada de la historia de la Proposición 9.2.5 y en [AO1997] una revista de las muchas pruebas que han sido dadas de ella.

9.2.7. 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 2 en 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 nos proponemos factorizar el entero

29 822 375. Los primeros primos son

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, ...

29 822 375	5
5 964 475	5
1 192 895	5
238 579	11
21 689	23
943	23
41	41
1	

Probamos dividir nuestro número por 2 y por 3, sin éxito. Es divisible por 5, y el cociente es 5 964 475; este es otra vez divisible por 5, con

cociente 1192 895, y este 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 $29\ 822\ 375 = 5^3 \cdot 11 \cdot 23^2 \cdot 41$.

En la Figura 9.2 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.

9.2.8. Demos una aplicación sencilla y bonita del teorema fundamental de la aritmética:

Proposición. *Para todo $n \in \mathbb{N}$ el n -ésimo número primo p_n es menor que 4^n .*

Demostración. Sea n un entero positivo, sean p_1, \dots, p_n los primeros n números primos listados en orden creciente y sin repeticiones, y sea I el conjunto de todos los enteros de 1 a p_n .

Sea m un elemento cualquiera de I . Los primos que dividen a m pertenecen a I , porque son menores o iguales que p_n , así que hay enteros no negativos a_1, \dots, a_n tales que

$$m = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}.$$

Dividiendo estos enteros por 2 vemos que hay otros enteros no negativos b_1, \dots, b_n y elementos c_1, \dots, c_n del conjunto $\{0, 1\}$ tales que $a_i = 2b_i + c_i$ para cada $i \in \{1, \dots, n\}$ y, por lo tanto, que

$$m = p_1^{2b_1+c_1} p_2^{2b_2+c_2} \cdots p_n^{2b_n+c_n} = (p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n})^2 p_1^{c_1} p_2^{c_2} \cdots p_n^{c_n}.$$

Así, todo elemento de I es igual al producto de un cuadrado — necesariamente menor que p_n — y un elemento del conjunto

$$F := \{p_1^{c_1} p_2^{c_2} \cdots p_n^{c_n} : 0 \leq c_1, c_2, \dots, c_n \leq 1\}.$$

El número de cuadrados menores que p_n es, como mucho, $\sqrt{p_n}$, y el conjunto F tiene, de acuerdo al teorema fundamental de la aritmética, exactamente 2^n elementos. La cantidad de elementos de I es, por lo tanto,

$$p_n = |I| \leq \sqrt{p_n} \cdot 2^n.$$

```

module Factorizar where

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 = 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)

```

Programa 9.2. Una implementación en HASKELL del algoritmo trivial de 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 249.

Dividiendo por $\sqrt{p_n}$ a ambos lados de esta desigualdad y elevando luego al cuadrado vemos que $p_n \leq 4^n$, que es lo que la proposición afirma. \square

9.2.9. Usando la misma idea que usamos para probar esta proposición encontrar una cota para la función π :

Corolario. Para cada entero n es $\pi(n) \geq \frac{\ln n}{2 \ln 2}$.

Esta cota es mejor que la que nos da la Proposición 9.1.8. Por ejemplo, es posible calcular que $\pi(10^{15}) = 29\,844\,570\,422\,669$: la cota que nos da aquella proposición es

$$\pi(10^{15}) \geq \ln \ln 10^{15} = 3,542\,082\dots$$

mientras que el corolario nos dice que

$$\pi(10^{15}) \geq \frac{\ln 10^{15}}{2 \ln 2} = 24,914\,460\dots$$

De todas formas, vemos con esto que se trata de una cota muy grosera. Sin embargo, cuando n crece la nueva cota es mucho mejor que la que teníamos, ya que

$$\lim_{n \rightarrow \infty} \frac{\ln \ln n}{\frac{\ln n}{2 \ln 2}} = 0.$$

Demostración. Sea n un entero tal que $n \geq 2$, sea $N := \pi(n)$, y sean p_1, \dots, p_N los primos menores o iguales que n . En la demostración de la proposición vimos que todo elemento de $\{1, \dots, n\}$ puede escribirse como un producto de un cuadrado menor o igual que n , de los cuales hay como mucho \sqrt{n} , y un número que es un producto de la forma $p_1^{c_1} \cdots p_N^{c_N}$ con $c_1, \dots, c_N \in \{0, 1\}$, de los que hay 2^N . Esto implica, claro, que $n \leq \sqrt{n} \cdot 2^N$, así que $\sqrt{n} \leq 2^{\pi(n)}$: tomando logaritmos obtenemos la desigualdad del enunciado. \square

Tanto la Proposición 9.2.8 como el Corolario 9.2.9 son debidos a Paul Erdős [Erd1938].

9.2.10. Es importante notar que para probar el Teorema fundamental de la aritmética 9.2.5 no usamos nunca el hecho de que hay infinitos números primos. Leonhard Euler aprovechó esto en su célebre artículo [Eul1744] para dar una prueba alternativa de que hay infinitos números primos.

Supongamos, siguiendo a Euler, que, por el contrario, hay un número finito de ellos, y sea p_1, p_2, \dots, p_N la lista de todos en orden creciente y sin repeticiones.

Sea m un entero positivo. Si distribuimos el producto de N factores

$$\left(1 + \frac{1}{p_1} + \frac{1}{p_1^2} + \cdots + \frac{1}{p_1^m}\right) \left(1 + \frac{1}{p_2} + \frac{1}{p_2^2} + \cdots + \frac{1}{p_2^m}\right) \cdots \left(1 + \frac{1}{p_N} + \frac{1}{p_N^2} + \cdots + \frac{1}{p_N^m}\right) \quad (9)$$

el resultado es la suma de $(m+1)^N$ fracciones de la forma

$$\frac{1}{p_1^{b_1} p_2^{b_2} \cdots p_N^{b_N}},$$

una para cada forma de elegir elementos b_1, \dots, b_N en el conjunto $\{0, \dots, m\}$. Ahora bien, si n es un elemento de $\{1, \dots, m\}$, entonces según el teorema fundamental de la aritmética hay exactamente una forma de elegir a_1, \dots, a_N en \mathbb{N}_0 tales que $n = p_1^{a_1} p_2^{a_2} \cdots p_N^{a_N}$, y es claro que todos ellos pertenecen a $\{0, \dots, m\}$, ya que $n \leq m$: esto nos dice que exactamente una de las fracciones de la gran suma descripta arriba es igual a $1/n$. Esto prueba que el producto (9) es mayor o igual que la suma

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{m}.$$

Notando que cada uno de los factores de ese producto es una suma geométrica, concluimos así que

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{m} \leq \prod_{i=1}^N \frac{1 - 1/p_i^{m+1}}{1 - 1/p_i} \leq \prod_{i=1}^N \frac{1}{1 - 1/p_i}.$$

Esto es cierto cualquiera sea m en \mathbb{N} . Supongamos ahora que k es un entero positivo y pongamos $m = 2^k - 1$. Tenemos entonces que

$$\begin{aligned} 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{2^k - 1} \\ = 1 + \left(\frac{1}{2} + \frac{1}{3} \right) + \left(\frac{1}{4} + \frac{1}{5} + \frac{1}{6} + \frac{1}{7} \right) + \left(\frac{1}{8} + \cdots + \frac{1}{15} \right) + \cdots + \left(\frac{1}{2^{k-1}} + \cdots + \frac{1}{2^k - 1} \right). \end{aligned}$$

Para cada $i \in \{1, \dots, k\}$ el i -ésimo sumando de esta última suma es él mismo una suma de 2^{i-1} términos todos mayores o iguales que $1/2^i$, así que es mayor o igual a $2^{i-1} \cdot 1/2^i = 1/2$. Como hay en total k de esos sumandos, esto nos dice que

$$\frac{k}{2} \leq 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{2^k - 1} \leq \prod_{i=1}^N \frac{1}{1 - 1/p_i}.$$

Esto no puede ser cierto para toda elección de k en \mathbb{N} , por supuesto. Esta contradicción provino de haber supuesto que hay un número finito de números primos: podemos concluir, entonces, que hay infinitos, y esto es lo que queríamos.

Esta demostración de la Proposición 9.1.6 es considerablemente más compleja que todas las que vimos antes! El argumento de Euler es importante, sin embargo, porque es el inicio de la llamada *teoría analítica de números*, que consiste en el uso de técnicas del análisis real y complejo para estudiar propiedades de los números enteros. La elaboración de esas ideas es lo que eventualmente llevó a la prueba del teorema de los números primos.

9.2.11. Ejercicio. Sea p_1, p_2, p_3, \dots la lista en orden creciente y sin repeticiones de los números primos. Muestre que si k un entero positivo, entonces existe un entero positivo N tal que

$$e^{2k} \leq \prod_{i=1}^N \frac{1}{1 - 1/p_i}.$$

Tomando logaritmos y recordando que $-\ln(1-x) \leq 2x$ para todo $x \in (0, \frac{1}{2}]$, concluya que

$$k \leq \sum_{i=1}^N \frac{1}{p_i}$$

Esto nos dice que el conjunto $\{\sum_{i=1}^N \frac{1}{p_i} : N \in \mathbb{N}\}$ no está acotado superiormente y, en el lenguaje del análisis, que

$$\sum_{i=1}^{\infty} \frac{1}{p_i} = +\infty.$$

Este es un célebre teorema de Leonhard Euler publicado en [Eul1744].

9.2.12. Ejercicio. Sea p_1, p_2, p_3, \dots la lista en orden creciente y sin repeticiones de los números primos, y para cada $n \in \mathbb{N}$ sea

$$s_n := \sum_{i=1}^n \frac{1}{p_i}.$$

Pruebe que para ningún $n \in \mathbb{N}$ el número s_n , que es ciertamente racional, es entero. Para hacerlo, muestre haciendo inducción que si a_n/b_n es la expresión de s_n como cociente de dos enteros coprimos, entonces uno de los números a_n y b_n es par y el otro impar.

§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 . Se trata, de acuerdo a esta definiciones, del exponente más grande k tal que p^k divide a 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. Sea n un entero no nulo. 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. La valuación p -ádica $v_p(n)$ de n es el único entero no negativo k tal que hay un entero m no divisible por p tal que $n = p^k m$.*

Demostración. 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 un entero m tal que $n = p^{v_p(n)}m$. Supongamos por un momento que p divide a m , de manera que existe $u \in \mathbb{Z}$ tal que $m = pu$. En ese caso tenemos que $n = p^{v_p(n)+1}u$ 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 p no divide a m , y esto prueba que el número $v_p(n)$ tiene la propiedad descripta en el enunciado de la proposición.

Para ver que esa propiedad la caracteriza, supongamos ahora que $k \in \mathbb{N}_0$ es tal que existe $m \in \mathbb{Z}$ para el cual se tiene 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, que

$$k \leq v_p(n), \tag{10}$$

ya que $v_p(n)$ es el mayor elemento de $V_p(n)$. Supongamos que la desigualdad (10) 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 (10) era estricta y podemos concluir entonces que $k = v_p(n)$, como afirma el enunciado. \square

9.3.4. Si p es un número primo, entonces la valuación p -ádica es una función $v_p : \mathbb{Z} \setminus \{0\} \rightarrow \mathbb{N}_0$. La siguiente proposición describe sus propiedades fundamentales.

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 este 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 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 $k \leq v_p(m)$, sabemos que p^k divide a n y a m , y 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. Una de las razones por las que nos interesan las valuaciones de un número es que nos dicen exactamente cuáles son los exponentes en la factorización de este como producto de potencias de primos distintos dos a dos.

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. Sean p_1, \dots, p_r los números primos que dividen a n listados sin repeticiones y sea i un elemento de $\{1, \dots, r\}$. Sabemos que hay enteros positivos a_1, \dots, a_r tales que $n = p_1^{a_1} \cdots p_r^{a_r}$. Como p_i es distinto de todos los primos $p_1, \dots, p_{i-1}, p_{i+1}, \dots, p_r$, es coprimo con todos ellos, así que también es coprimo con los números $p_1^{a_1}, \dots, p_{i-1}^{a_{i-1}}, p_{i+1}^{a_{i+1}}, \dots, p_r^{a_r}$ y, finalmente, con el producto de todos estos,

$$m := p_1^{a_1} \cdots p_{i-1}^{a_{i-1}} p_{i+1}^{a_{i+1}} \cdots p_r^{a_r}.$$

Tenemos entonces que $n = p_i^{a_i} m$ y que $p_i \nmid m$, así que la Proposición 9.3.3 nos permite concluir que $a_i = v_{p_i}(n)$. Como esto es cierto cualquiera sea el elemento i de $\{1, \dots, n\}$, tenemos entonces que

$$n = p_1^{a_1} \cdots p_r^{a_r} = p_1^{v_{p_1}(n)} \cdots p_r^{v_{p_r}(n)},$$

como afirma la proposición. \square

9.3.6. Más generalmente, tenemos lo siguiente:

Corolario. *Sea n un entero positivo. Si p_1, \dots, p_r es una lista de primos dos a dos distintos que incluye a todo primo que divide a n , entonces*

$$n = p_1^{v_{p_1}(n)} \cdots p_r^{v_{p_r}(n)}.$$

A diferencia de lo que ocurre en la Proposición 9.3.5, los exponentes que aparecen en esta factorización pueden ser nulos.

Demostración. Supongamos que p_1, \dots, p_r es una lista de primos dos a dos distintos que incluye a todo primo que divide a n . Reordenándola si es que es necesario, podemos suponer que hay un entero s con $0 \leq s \leq r$ y tal que los primos p_1, \dots, p_s dividen a n y los primos p_{s+1}, \dots, p_r no lo hacen. Como p_1, \dots, p_s son entonces todos los primos que dividen a n listados sin repeticiones, sabemos que

$$n = p_1^{v_{p_1}(n)} \cdots p_s^{v_{p_s}(n)}.$$

Por otro lado, como ninguno de p_{s+1}, \dots, p_r divide a n , sabemos que $v_{p_i}(n) = 0$ para cada $i \in \{s+1, \dots, r\}$ y, por lo tanto, que

$$1 = p_{s+1}^{v_{p_{s+1}}(n)} \cdots p_r^{v_{p_r}(n)}.$$

Juntando todo, vemos que

$$n = n \cdot 1 = p_1^{v_{p_1}(n)} \cdots p_s^{v_{p_s}(n)} \cdot p_{s+1}^{v_{p_{s+1}}(n)} \cdots p_r^{v_{p_r}(n)},$$

y este último producto es el mismo que aparece en el enunciado del corolario. \square

9.3.7. Las valuaciones nos dan un criterio sencillo de divisibilidad:

Proposición. Sean n y m dos enteros. Una condición necesaria y suficiente para que n divida a m es que para todo número primo p se tenga que $v_p(n) \leq v_p(m)$.

Demostración. Sean p_1, \dots, p_r los primos que dividen a n listados sin repeticiones. 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, de manera que para cada elemento i de $\{1, \dots, r\}$ tenemos que $v_{p_i}(n) \leq v_{p_i}(m)$ y, por lo tanto, 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 6.5.8 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

9.3.8. De manera muy similar, podemos usar valuaciones para dar expresiones para el máximo común divisor y el mínimo común múltiplo de dos enteros que son muchas veces útiles.

Proposición. Sean n y m dos enteros positivos y sean p_1, \dots, p_r los primos que dividen a nm listados sin repeticiones. Se tiene entonces que

$$\text{mcd}(n, m) = p_1^{a_1} \cdots p_r^{a_r}, \quad \text{mcm}(n, m) = p_1^{b_1} \cdots p_r^{b_r}$$

con

$$a_i = \min\{v_{p_i}(n), v_{p_i}(m)\}, \quad b_i = \max\{v_{p_i}(n), v_{p_i}(m)\}$$

para cada $i \in \{1, \dots, r\}$.

Demostración. Sea $d := p_1^{a_1} \cdots p_r^{a_r}$. Para cada $i \in \{1, \dots, r\}$ pongamos

$$s_i := v_{p_i}(n) - a_i, \quad t_i := v_{p_i}(m) - a_i,$$

y observemos s_i y t_i son los dos 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 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

$$\begin{aligned} &= p_1^{v_{p_1}(n)} \cdots p_r^{v_{p_1}(n)} \cdot p_1^{v_{p_1}(m)} \cdots p_r^{v_{p_r}(m)} \\ &= n \cdot m. \end{aligned}$$

Así, tenemos que $\text{mcd}(n, m) \cdot e = n \cdot m$ y, gracias al Ejercicio 6.6.4(c), podemos concluir que $e = \text{mcm}(n, m)$. Esto prueba la segunda de las igualdades de la proposición. \square

9.3.9. La descripción que nos da la última proposición del máximo común múltiplo nos permite probar fácilmente el siguiente resultado, que nos será útil más tarde.

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

$$b_i := \begin{cases} v_{p_i}(m), & \text{si } v_{p_i}(n) < v_{p_i}(m); \\ 0, & \text{en caso contrario.} \end{cases}$$

Consideraremos finalmente 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 9.3.7 vemos que $u \mid n$ y que $v \mid n$. De la segunda y de la tercera, usando la Proposición 9.3.8, que $\text{mcd}(u, v) = 1$ y que $uv = \text{mcm}(n, m)$. La proposición queda así probada. \square

9.3.10. Antes de cambiar de tema, probemos un resultado bien conocido y útil de Adrien-Marie Legendre que determina las valuaciones de los factoriales. Se lo conoce habitualmente como *fórmula de Legendre* o *de Polignac*, por Alphonse de Polignac.

Proposición. Si n es un entero positivo y p un número primo, entonces

$$v_p(n!) = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor.$$

En esta situación es fácil ver que hay un entero positivo l tal que $n < p^l$, así que para todo entero k tal que $k \geq l$ se tiene que $\lfloor n/p^k \rfloor = 0$. Esto nos dice que en la suma de esta proposición hay un número finito de sumandos no nulos: es por eso que tiene sentido.

Demostración. De acuerdo a la segunda parte de la Proposición 9.3.4, tenemos que

$$v_p(n!) = v_p(1 \cdot 2 \cdots n) = v_p(1) + v_p(2) + \cdots + v_p(n). \quad (11)$$

Sabemos que hay un entero positivo l tal que $n < p^l$, y esto implica inmediatamente que todos los n sumandos de esta suma son menores que l .

Para cada $k \in \mathbb{N}_0$ escribimos m_k a la cantidad de términos de la suma de (11) que son mayores o iguales a k . Para cada $k \in \mathbb{N}_0$, entonces, el número de términos de esa suma que son *iguales* a k es exactamente $m_k - m_{k+1}$ y, por lo tanto, tenemos que

$$\begin{aligned} v_p(n!) &= 0 \cdot (m_0 - m_1) + 1 \cdot (m_1 - m_2) + 2 \cdot (m_2 - m_3) + \cdots + l \cdot (m_l - m_{l+1}) \\ &= 0 \cdot m_0 + (1 - 0) \cdot m_1 + (2 - 1) \cdot m_2 + \cdots + (l - (l - 1)) \cdot m_l - l \cdot m_{l+1} \end{aligned}$$

y como $m_{l+1} = 0$ por la forma que elegimos a l , esto es

$$= m_1 + m_2 + \cdots + m_l. \quad (12)$$

Ahora bien, si $k \in \mathbb{N}_0$, entonces un elemento i de $\{1, \dots, n\}$ tiene $v_p(i) \geq k$ si y solamente si i es divisible por p^k , y esto nos dice que m_k es el número de elementos del conjunto $\{1, \dots, n\}$ divisibles por p^k , esto es, $\lfloor n/p^k \rfloor$. La igualdad (12) es, por lo tanto, la que afirma la proposición. \square

9.3.11. Daremos una aplicación de la fórmula de Legendre. Para eso necesitamos la siguiente propiedad sencilla de la función «parte entera».

Ejercicio. Muestre que si x e y son dos números reales entonces

$$\lfloor x \rfloor + \lfloor y \rfloor \leq \lfloor x + y \rfloor \leq \lfloor x \rfloor + \lfloor y \rfloor + 1$$

y que, en particular, $0 \leq \lfloor 2x \rfloor - 2\lfloor x \rfloor \leq 1$.

9.3.12. La fórmula de Legendre nos da una expresión para la valuación p -ádica de un número factorial y usándola podemos obtener información sobre los números binomiales, que se expresan de manera sencilla usando factoriales. El siguiente resultado se ocupa de los llamados *números binomiales centrales*.

Corolario. Sea p un número primo. Si n es un entero positivo y $N := \binom{2n}{n}$, entonces

$$p^{v_p(N)} \leq 2n.$$

Si escribimos \log_p al logaritmo en base p , este corolario nos dice que $v_p(N) \leq \log_p 2n$.

Demostración. Sea n un entero positivo y sea $N := \binom{2n}{n} = (2n)!/n!^2$. La multiplicatividad de la valuación p -ádica implica que

$$2v_p(n!) + v_p(N) = v_p(n!^2 N) = v_p((2n)!),$$

así que usando la fórmula de Legendre 9.3.10 vemos que

$$v_p(N) = v_p((2n)!)) - 2v_p(n!) = \sum_{k=1}^{\infty} \left\lfloor \frac{2n}{p^k} \right\rfloor - 2 \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor = \sum_{k=1}^{\infty} \left(\left\lfloor \frac{2n}{p^k} \right\rfloor - 2 \left\lfloor \frac{n}{p^k} \right\rfloor \right) \quad (13)$$

Si l es un entero tal que $l > \log_p 2n$, entonces $p^l > 2n$, así que $0 \leq n/p^l < 2n/p^l < 1$ y, por lo tanto, $\lfloor 2n/p^l \rfloor - 2\lfloor n/p^l \rfloor = 0$. Esto nos dice que en la suma de (13) todos los términos que tienen $k > \log_p 2n$ se anulan y que, por lo tanto,

$$v_p(N) = \sum_{k=1}^{\lfloor \log_p 2n \rfloor} \left(\left\lfloor \frac{2n}{p^k} \right\rfloor - 2 \left\lfloor \frac{n}{p^k} \right\rfloor \right).$$

Por otro lado, el resultado del Ejercicio 9.3.11 nos dice cada uno de los $\lfloor \log_p 2n \rfloor$ términos de esta suma vale como mucho 1, así que $v_p(N) \leq \lfloor \log_p 2n \rfloor$ y, en definitiva,

$$p^{v_p(N)} \leq p^{\lfloor \log_p 2n \rfloor} \leq p^{\log_p 2n} = 2n,$$

como afirma el corolario. □

§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 $n = 172\,772$ 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 9.3.7 nos dice que

$$0 \leq a_1 \leq 3, \quad 0 \leq a_2 \leq 2, \quad 0 \leq a_3 \leq 4. \quad (14)$$

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 (14) 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

$$\sigma_0(300) = (2 + 1)(1 + 1)(2 + 1) = 3 \cdot 2 \cdot 3 = 18.$$

Esto coincide con nuestro ejemplo de 9.4.1. De manera similar, como $172\,772 = 2^3 \cdot 3^2 \cdot 7^4$, la proposición nos dice que

$$\sigma_0(172\,772) = (3 + 1)(2 + 1)(4 + 1) = 60,$$

como dijimos.

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 9.3.7 nos dice que $0 \leq v_{p_i}(d) \leq v_{p_i}(n)$ para todo $i \in \{1, \dots, r\}$, y entonces la r -upla $(v_{p_1}(d), \dots, v_{p_r}(d))$ pertenece al 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

$$\varphi : d \in D(n) \mapsto (v_{p_1}(d), \dots, v_{p_r}(d)) \in I_1 \times \cdots \times I_r$$

Mostremos que esta función es una biyección.

- Sea (a_1, \dots, a_r) un elemento de $I_1 \times \cdots \times I_r$ y consideremos 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 9.3.7 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

$$\text{para cada } i \in \{1, \dots, r\} \text{ se tiene que } v_{p_i}(d) = v_{p_i}(e). \quad (15)$$

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 (15) 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, su dominio y su codominio tienen el mismo cardinal, así 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 ciudadanos³ 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 los divisores positivos 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.

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

³Para Platón no todos los habitantes de una ciudad son ciudadanos.

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. \square

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 potencias de números primos distintos dos a dos:

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 6.5.9 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. \square

9.4.8. Vamos a necesitar un par de veces un resultado sencillo sobre divisores, que probamos ahora. Para cada entero positivo 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 d y e son divisores coprimos de nm y, por lo tanto, su producto de es un divisor positivo de nm . Esto nos dice que hay una función

$$P : (d, e) \in D(n) \times D(m) \mapsto de \in D(nm).$$

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. Sean n y m dos enteros coprimos. 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

$$Q : u \in D(nm) \mapsto (\text{mcd}(n, u), \text{mcd}(m, u)) \in D(n) \times D(m).$$

Mostremos que esta función Q es inversa de P .

- Si u es un elemento cualquiera de $D(nm)$, 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 $D(nm)$.

- Sea, por otro lado, (d, e) un elemento de $D(n) \times D(m)$. Es

$$Q(P(d, e)) = Q(de) = (\text{mcd}(n, de), \text{mcd}(m, de)). \quad (16)$$

Como e divide a m , el Corolario 6.5.2 nos dice que $\text{mcd}(n, e) | \text{mcd}(n, m) = 1$, 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 (16), 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, la función P es biyectiva. \square

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

$$\sigma_k(n) = \sigma_k(p_1^{v_{p_1}(n)}) \cdots \sigma_k(p_r^{v_{p_r}(n)}). \quad (17)$$

Ahora bien, si p es un número primo y $a \in \mathbb{N}_0$, entonces de acuerdo a la Proposición 9.3.7 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

$$\sigma_k(p^a) = 1^k + p^{2k} + \cdots + p^{ak}.$$

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 (17), vemos que

$$\sigma_k(n) = \frac{p_1^{k(v_{p_1}(n)+1)}}{p_1^k - 1} \cdots \frac{p_r^{k(v_{p_r}(n)+1)}}{p_r^k - 1}.$$

Esto completa la prueba de la proposición. □

9.4.10. Usando la Proposición 9.4.9 podemos calcular fácilmente las funciones σ_k . Por ejemplo, como $317\,765\,539 = 7^2 \cdot 13 \cdot 23^3 \cdot 41$, tenemos que

$$\begin{aligned}\sigma_3(317\,765\,539) &= \frac{7^{3(2+1)} - 1}{7^3 - 1} \cdot \frac{13^{3(1+1)} - 1}{13^3 - 1} \cdot \frac{23^{3(3+1)} - 1}{23^3 - 1} \cdot \frac{41^{3(1+1)} - 1}{41^3 - 1} \\ &= 117\,993 \cdot 2\,198 \cdot 1\,801\,300\,709\,520 \cdot 68\,922 \\ &= 32\,197\,935\,268\,666\,697\,933\,108\,160.\end{aligned}$$

§9.5. Números perfectos

9.5.1. 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. Así, 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

$$\begin{aligned}6, \quad 28, \quad 496, \quad 8\,128, \quad 33\,550\,336, \quad 8\,589\,869\,056, \quad 137\,438\,691\,328, \\ 2\,305\,843\,008\,139\,952\,128, \quad 2\,658\,455\,991\,569\,831\,744\,654\,692\,615\,953\,842\,176, \\ 191\,561\,942\,608\,236\,107\,294\,793\,378\,084\,303\,638\,130\,997\,321\,548\,169\,216\end{aligned}$$

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 dio cuenta que 8\,128 es perfecto. Los siguientes tres fueron encontrados más de mil años después por el matemático Ismail ibn Fallūs, quien también listó varios más, que ahora sabemos que no son perfectos.

El 29 de septiembre de 2023 se conocían 51 números perfectos⁴. El más grande de ellos es el número

$$2^{82\,589\,932} \cdot (2^{82\,589\,933} - 1),$$

que tiene 49 724 095 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 viendo de él esto es muy significativo!

9.5.2. 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. □

9.5.3. 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

$$2^1(2^2 - 1) = 6, \quad 2^2(2^3 - 1) = 28, \quad 2^4(2^5 - 1) = 496, \quad 2^6(2^7 - 1) = 8\,128$$

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

$$2^{12}(2^{13} - 1) = 33\,509\,381, \quad 2^{16}(2^{17} - 1) = 8\,589\,869\,056$$

⁴En una versión anterior de este libro decíamos que el 10 de enero de 2018 se conocían 50 números perfectos: el 7 de diciembre de ese año se encontró uno más. Hasta ese momento el más grande conocido era $2^{77\,232\,916} \cdot (2^{77\,232\,917} - 1)$ que tiene 46 498 850 dígitos.

y

$$2^{18}(2^{19} - 1) = 137\,438\,691\,328,$$

ya que $8\,191 = 2^{13} - 1$, $131\,071 = 2^{17} - 1$ 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 este no fue encontrado hasta el año 1772, cuando Euler pudo determinar que

$$2\,147\,483\,647 = 2^{31} - 1$$

es primo.

9.5.4. La Proposición 9.5.2 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.

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 6.6.6(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.

Desde 1996, un esfuerzo colaborativo y distribuido llamado *Great Internet Mersenne Prime Search* (GIMPS) busca primos de Mersenne y desde su fundación hasta septiembre de 2023 encontró 18 primos, el más grandes de los cuales es

$$2^{82\,589\,933} - 1,$$

que es, de hecho, el número primo más grande que conocemos — tiene 24 862 048 dígitos decimales.

9.5.5. Los números perfectos que nos permite construir la Proposición 9.5.2 son todos pares. Euler probó en 1899 que de esa forma obtenemos, de hecho, *todos* los números perfectos pares.



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.

Proposición. Si n es un número perfecto par, hay 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. Sabemos que hay 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

§9.6. Ejercicios

Números perfectos multiplicativos

9.6.1. Ejercicio. Muestre que un número a es igual al producto de sus divisores propios si y solamente si es de la forma p^3 para algún primo p , o de la forma pq para dos primos distintos p y q .

Esto nos dice que el análogo «multiplicativo» de la definición de números perfectos no es muy interesante.

La función de Möbius

9.6.2. Si n es un entero positivo y $p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$, con $r \in \mathbb{N}_0$, p_1, p_2, \dots, p_n primos distintos dos a dos y a_1, \dots, a_r enteros positivos, es su factorización usual, entonces escribimos

$$\mu(n) := \begin{cases} 0 & \text{si alguno de los números } a_1, a_2, \dots, a_r \text{ es mayor que 1;} \\ (-1)^r & \text{en caso contrario.} \end{cases}$$

Obtenemos de esta forma una función $\mu : \mathbb{N} \rightarrow \mathbb{Z}$ llamada la *función de Möbius*, por August Ferdinand Möbius que la estudió en 1832.

9.6.3. Ejercicio.

- (a) Muestre que $\mu(n) = 0$ si y solamente si n es divisible por un cuadrado mayor que 1.
- (b) Prueba que la función μ es multiplicativa, esto es, que si n y m son dos enteros positivos coprimos entonces $\mu(nm) = \mu(n)\mu(m)$.
- (c) Muestre que para todo entero positivo n vale que

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{si } n = 1; \\ 0 & \text{si } n > 1. \end{cases}$$

Notemos que esta suma tiene un término por cada divisor *positivo* de n .

- (d) Sea $f : \mathbb{N} \rightarrow \mathbb{R}$ una función cualquiera. Si $g : \mathbb{N} \rightarrow \mathbb{R}$ es la función que en cada entero

positivo n toma el valor

$$g(n) := \sum_{d|n} f(d),$$

entonces para todo entero positivo n vale que

$$f(n) = \sum_{d|n} \mu(d)g\left(\frac{n}{d}\right).$$

Esta es la llamada *fórmula de inversión de Möbius*.
