Capítulo 10

Potencias

§10.1. El pequeño teorema de Fermat

10.1.1. Nuestro primer objetivo en este capítulo es probar el llamado *pequeño teorema de Fermat*. Se conocen varias formas de llegar a ese resultado — aquí elegiremos una que es puramente algebraica. Empezamos con una observación puramente aritmética.

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. □

10.1.2. Una consecuencia inmediata de esta proposición y de la fórmula de Newton es que esta última se simplifica considerablemente si trabajamos módulo un número primo:

Corolario. *Sea p un número primo. Si a y b son dos enteros, entonces*

$$(a+b)^p \equiv a^p + b^p \mod p.$$

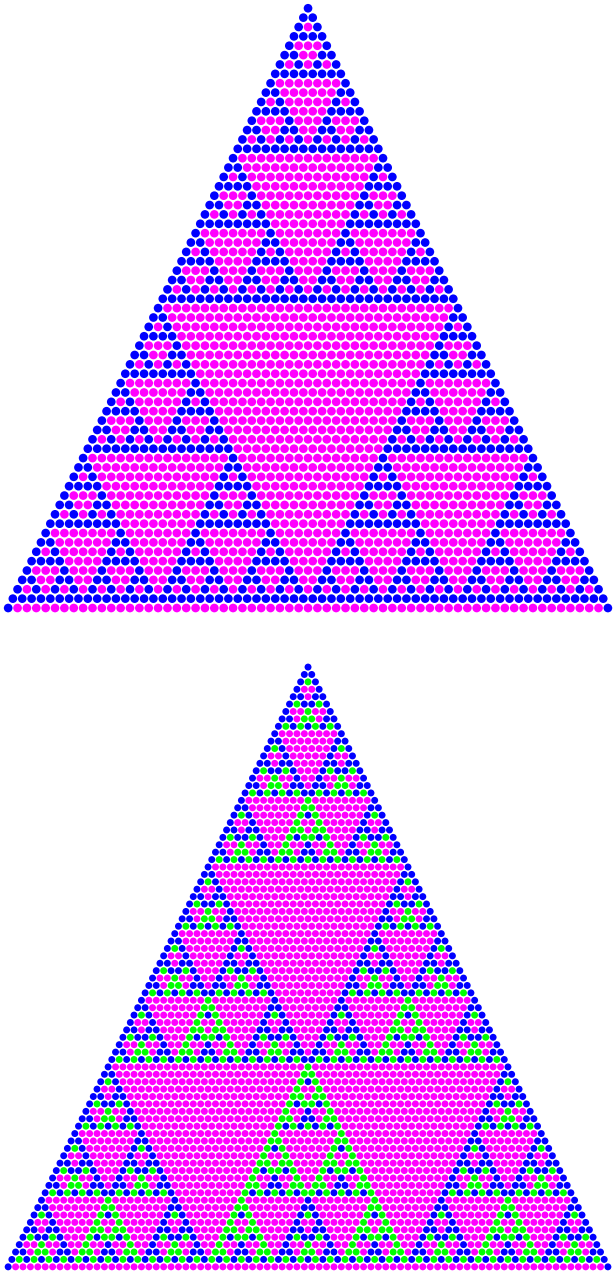

Figura 10.1. El triángulo de Pascal módulo 2 y módulo 3. Se trata de las primeras 64 y 81 filas del triángulo, respectivamente, y en los dos casos el magenta representa los números que tienen resto 0.

Demostración. Sean a y b dos enteros. La fórmula de Newton para las potencias de un binomio nos dice que

$$(a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^{p-i} b^i.$$

Ahora bien, de acuerdo a la Proposición 10.1.1 el número 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:

$$(a+b)^p \equiv a^p + b^p \mod p.$$

Esto es precisamente lo que afirma el corolario. □

10.1.3. Gracias a esta simplificación de la fórmula de Newton podemos probar lo que es casi el teorema que estamos buscando.

Proposición. *Sea p un número primo. Para todo entero a se tiene que $a^p \equiv a \mod p$.*

Demostración. Para cada $a \in \mathbb{Z}$ sea $P(a)$ la afirmación «$a^p \equiv a \mod p$». 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

$$(a+1)^p \equiv a^p + 1 \mod p$$

y la hipótesis inductiva nos dice que $a^p \equiv a \mod p$ así que, juntando todo, vemos que

$$(a+1)^p \equiv a + 1 \mod p,$$

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

$$a^p \equiv (a-ap)^p \equiv a - ap \equiv a \mod p,$$

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, 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*

$$a^{p-1} \equiv 1 \mod p.$$

Demostración. De acuerdo a la Proposición 10.1.3 tenemos que $a^p \equiv a \mod p$, es decir, que p divide a $a^p - a = a(a^{p-1} - a)$. Como p no divide a a y sí a este producto, tiene que dividir a $a^{p-1} - 1$: esto significa, precisamente, que $a^{p-1} \equiv 1 \mod p$. □

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

$$a^n = (a^{p-1})^q a^r \equiv a^r \mod p,$$

ya que, de acuerdo al teorema de Fermat 10.1.4, es $a^{p-1} \equiv 1 \mod p$. Por ejemplo, 11 es primo y coprimo con 2, y es $100 = 9(11-1) + 4$, así que

$$2^{104} = (2^{11-1})^9 2^4 \equiv 2^4 = 16 \equiv 5 \mod 11,$$

De manera similar, el número 541 es primo y coprimo con 123, así que el teorema de Fermat nos dice que $132^{541-1} \equiv 1 \mod 541$ y, por lo tanto, que

$$132^{999\,548} \equiv 132^{1\,851\cdot(541-1)+8} \equiv 132^8 \equiv ((132)^2)^2)^2 \equiv (112^2)^2 \equiv 101^2 \equiv 463 \mod 541.$$

10.1.6. El teorema de Fermat solo se aplica cuando estamos trabajando módulo un número primo, pero junto con el teorema chino del resto podemos extender su aplicabilidad.

Por ejemplo, supongamos que queremos calcular el resto de dividir a 2^{123} por 15. Se trata del único entero r tal que $2^{123} \equiv r \mod 15$ y $0 \leq r < 15$, como sabemos, y esa congruencia implica que también es $2^{123} \equiv r \mod 3$ y $2^{123} \equiv r \mod 5$. El teorema de Fermat nos permite calcular que

$$2^{123} \equiv (2^{3-1})^{61} \cdot 2 \equiv 2 \mod 3, \qquad 2^{123} \equiv (2^{5-1})^{30} \cdot 2^3 \equiv 8 \equiv 3 \mod 5,$$

y entonces el número r es una solución del sistema de congruencias

$$\begin{cases} x \equiv 2 \mod 3, \\ x \equiv 3 \mod 5. \end{cases}$$

Claramente 8 es una solución de este sistema, y esto implica que el conjunto de todas las soluciones es la clase de congruencia de 8 módulo 15. La única de esas soluciones que pertenece al conjunto $\{0, \ldots, 14\}$ es 8, y podemos concluir entonces que el resto que buscamos es $r = 8$.

De manera similar, podemos calcular el resto r de dividir a 5^{99} por $1178 = 2 \cdot 19 \cdot 31$. En efecto, es $r \equiv 5^{99} \mod 2 \cdot 19 \cdot 31$, así que

$$\begin{aligned} r &\equiv 5^{99} \equiv 1 \mod 2, \\ r &\equiv 5^{99} \equiv 5^{5\cdot(19-1)+9} \equiv 5^9 \equiv 1 \mod 19, \\ r &\equiv 5^{99} \equiv 5^{3\cdot(31-1)+9} \equiv 5^9 \equiv 1 \mod 31, \end{aligned}$$

y esto nos dice que r es una solución del sistema de congruencias

$$\begin{cases} x \equiv 1 \mod 2, \\ x \equiv 1 \mod 19, \\ x \equiv 1 \mod 31. \end{cases}$$

Ahora bien, es evidente que 1 es una solución de este sistema de congruencias, y sabemos que todas sus soluciones son entonces congruentes a 1 módulo $2 \cdot 19 \cdot 31$. La única de esas soluciones que está en el conjunto $\{0, \ldots, 2 \cdot 19 \cdot 31 - 1\}$ es 1 y, por lo tanto, ese es el resto que buscamos.

10.1.7. Debería ser claro para el lector en este punto que esta idea funciona siempre que queremos calcular el resto de dividir una potencia por un número que es producto de primos distintos dos a dos. Usando la misma idea, por otro lado, podemos probar la siguiente generalización del teorema de Fermat:

Proposición. *Sean p y q dos primos distintos. Si a es un entero coprimo con pq, entonces*

$$a^{(p-1)(q-1)} \equiv 1 \mod pq.$$

Demostración. Sea a un entero coprimo con pq. Como a es a la vez coprimo con p y con q, el teorema de Fermat nos dice que $a^{p-1} \equiv 1 \mod p$ y que $a^{q-1} \equiv 1 \mod q$, así que tenemos que $a^{(p-1)(q-1)} \equiv (a^{p-1})^{q-1} \equiv 1 \mod p$ y $a^{(p-1)(q-1)} \equiv (a^{q-1})^{p-1} \equiv 1 \mod q$. Esto nos dice que el entero $a^{(p-1)(q-1)}$ es una solución del sistema de congruencias

$$\begin{cases} x \equiv 1 \mod p, \\ x \equiv 1 \mod q. \end{cases}$$

Es claro que 1 es una solución de este sistema y, como p y q son primos distintos, sabemos que entonces todas las soluciones del sistema son congruentes entre sí módulo pq: podemos concluir entonces que $a^{(p-1)(q-1)} \equiv 1 \mod pq$, como afirma la proposición. □

10.1.8. Por supuesto, podemos generalizar esto a la situación en que tenemos más que dos primos:

Ejercicio. Sea r un entero positivo y sean $p_1, p_2, \dots, p_r$ números primos distintos dos a dos. Muestre que si a es un entero coprimo con el producto $p_1 p_2 \cdots p_r$, entonces

$$a^{(p_1-1)(p_2-1)\cdots(p_r-1)} \equiv 1 \mod p_1 \cdots p_r.$$

10.1.9. Veamos qué podemos decir cuando trabajamos módulo un número que no es producto de primos distintos dos a dos. Empecemos considerando un ejemplo.

Calculemos el resto de dividir a 7^{29} por 5^2, que es el único entero r tal que

$$r \equiv 7^{29} \mod 5^2, \qquad 0 \le r < 5^2. \tag{1}$$

Como vale esa congruencia, también es $r \equiv 7^{29} \mod 5$ y el teorema de Fermat nos permite calcular que $7^{29} \equiv 7^{7(5-1)+1} \equiv 7 \equiv 2 \mod 5$, así que es $r = 5s + 2$ para algún entero s. Volviendo a la congruencia de (1) vemos que $5s + 2 \equiv 7^{29} \mod 5^2$, así que $5s \equiv 7^{29} - 2 \mod 5^2$.

§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

$$C(n) := \{i \in \mathbb{N} : 1 \le i \le n, \mathsf{mcd}(i, n) = 1\}.$$

Esa cantidad es positiva, ya que $1 \in C(n)$. De esta manera obtenemos una función $\varphi : \mathbb{N} \to \mathbb{N}$, a la que llamamos ***función de Euler***. Por ejemplo, los enteros positivos que no superan a 20 son

$$\boxed{1}\ 2\ \boxed{3}\ 4\ 5\ 6\ \boxed{7}\ 8\ \boxed{9}\ 10\ \boxed{11}\ 12\ \boxed{13}\ 14\ 15\ 16\ \boxed{17}\ 18\ \boxed{19}\ 20$$

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, $\varphi(p) = p - 1$.

10.2.2. 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:

Proposición. *La función de Euler $\varphi : \mathbb{N} \to \mathbb{N}$ 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. Probaremos la afirmación de la proposición en varios pasos.

Primer paso. Empezamos construyendo dos funciones

$$f : C(n) \times C(m) \to C(nm), \qquad g : C(nm) \to C(n) \times C(m).$$

Sabemos que existen dos enteros x e y tales que $xn + ym = 1$.

- Sean $a \in C(n)$ y $b \in C(m)$, de manera que $1 \leq a < n$, $1 \leq b < m$, $\mathsf{mcd}(a, n) = 1$ y $\mathsf{mcd}(b, m) = 1$, y consideremos el entero $c = xnb + yma$. Se tiene que

  $$\mathsf{mcd}(c, n) = \mathsf{mcd}(xnb + yma, n) = \mathsf{mcd}(yma, n) = 1,$$

  ya que cada uno de los enteros y, m y a es coprimo con n. De manera similar, tenemos que $\mathsf{mcd}(c, m) = 1$ y, por lo tanto,

  $$\mathsf{mcd}(c, nm) = \mathsf{mcd}(c, n)\,\mathsf{mcd}(m) = 1.$$

  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 $f : C(n) \times C(m) \to C(nm)$ 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

  $$\mathsf{mcd}(r_n(c), n) = \mathsf{mcd}(r_n(c) + qn, n) = \mathsf{mcd}(c, n) \mid \mathsf{mcd}(c, nm) = 1,$$

  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 $g : C(nm) \to C(n) \times C(m)$ 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 $p_1, \ldots, p_r$ los primos que dividen a n, listados sin repeticiones, y sean $a_1, \ldots, a_r \in \mathbb{N}$ tales que $n = p_1^{a_1} \cdots p_r^{a_r}$. Se tiene que*

$$\varphi(n) = (p_1^{a_1} - p_1^{a_1 - 1}) \cdot \ldots \cdot (p_r^{a_r} - p_r^{a_r - 1}), \qquad \varphi(n) = n\left(1 - \frac{1}{p_1}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_r}\right).$$

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 $k \in \{1, \ldots, p^a - 1\}$ tiene $\mathsf{mcd}(k, p^a) \neq 1$ si y solamente si es divisible por p, y esto ocurre si y solamente es de la forma pm con $m \in \{1, \ldots, p^{a-1}\}$. Esto nos dice que en $\{1, \ldots, p^a - 1\}$ 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 $n = p_1^{a_1} \cdot \ldots \cdot p_r^{a_r}$ 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

$$\varphi(n) = \varphi(p_1^{a_1}) \cdot \ldots \cdot \varphi(p_r^{a_r}) = (p_1^{a_1} - p_1^{a_1-1}) \cdot \ldots \cdot (p_r^{a_r} - r_r^{a_r-1}).$$

Esta es la primera igualdad que aparece en el enunciado. Para ver la segunda observamos simplemente que esta última expresión es igual a

$$p_1^{a_1}\left(1 - \frac{1}{p_1}\right) \cdot \ldots \cdot p_r^{a_r}\left(1 - \frac{1}{p_r}\right)$$

y reordenamos los factores, recordando que el producto $p_1^{a_1} \cdot \ldots \cdot p_r^{a_r}$ es igual a n. □

10.2.4. Si n es un entero positivo y $p_1, \ldots, p_r$ son los primos que dividen a n listados sin repeticiones, la proposición que acabamos de probar nos dice que

$$\frac{\varphi(n)}{n} = \left(1 - \frac{1}{p_1}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_r}\right). \tag{2}$$

La fracción que aparece a la izquierda en esta igualdad es el cociente entre el número de enteros coprimos con n de $\{1, \ldots, n\}$ 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 $\{1, \ldots, n\}$. Podemos hacer algunas observaciones sencillas sobre esta proporción:

- Para cada $i \in \{1, \ldots, r\}$ el factor $1 - 1/p_i$ que aparece en (2) es menor que 1 pero mientras más grande es p_i mas 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 (2) 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 $p_1, \ldots, p_r$ 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 y menores que él es tan baja como queramos. Es posible cuantificar esto de manera muy precisa: para todo número positivo ε hay infinitos positivos n para los que

$$\frac{\varphi(n)}{n} \cdot \log\log n \geq \frac{1}{e^\gamma} - \varepsilon$$

y el número $1/e^\gamma$ es el mas chico con esta propiedad. Aquí $\gamma \approx 0{,}577\,216\ldots$ la llamada constante de Euler–Mascheroni, de manera que $e^\gamma \approx 1{,}781\,072\ldots$ Puede encontrarse una prueba de esto, junto con mucha más información sobre la función φ, en [HW2008, §18.4].

10.2.5. La siguiente observación es debida a Gauss, y describe una propiedad de la función de Euler que resulta ser fundamental.

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 $\psi : \mathbb{N} \to \mathbb{N}$. Mostremos que es multiplicativa.

Sean n y m dos enteros positivos coprimos. 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) es un elemento del conjunto $D(n) \times D(m)$, entonces $d \mid n$ y $e \mid m$, así que $\mathsf{mcd}(d,e) \mid \mathsf{mcd}(n,m) = 1$ y, 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, y recordando las funciones P y Q del Lema 9.4.8, vemos que

$$\begin{aligned}\psi(n)\psi(m) &= \sum_{(d,e)\in D(n)\times D(m)} \varphi(de) = \sum_{(d,e)\in D(n)\times D(m)} \varphi(P(d,e)) \\ &= \sum_{u\in D(nm)} \varphi(P(Q(u))) = \sum_{u\in D(nm)} \varphi(u) = \psi(nm).\end{aligned}$$

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 $1, p, p^2, \ldots, p^{a-1}, p^a$ así que

$$\begin{aligned}\psi(p^a) &= \varphi(1) + \varphi(p) + \varphi(p^2) + \cdots + \varphi(p^{a-1}) + \varphi(p^a) \\ &= 1 + (p-1) + (p^2 - p) + \cdots + (p^{a-1} - p^{a-2}) + (p^a - p^{a-1}) = p^a.\end{aligned}$$

Finalmente sea n un entero positivo cualquiera, sean $p_1, \ldots, p_r$ los primos que dividen a n listados sin repeticiones, y sean $a_1, \ldots, a_r$ los enteros tales que $n = p_1^{a_1} \cdots p_r^{a_r}$. Usando la multiplicatividad de la función ψ podemos calcular ahora que

$$\psi(n) = \psi(p_1^{a_1} \cdots p_r^{a_r}) = \psi(p_1^{a_1}) \cdots \psi(p_r^{a_r}) = p_1^{a_1} \cdots p_r^{a_r} = n.$$

Esto prueba la proposición. □

10.2.6. Una consecuencia importante de la proposición que acabamos de probar es la siguiente relación de la función φ de Euler y la función μ de Möbius que vimos en 9.6.2.

Corolario. *Para todo entero positivo n se tiene que*

$$\varphi(n) = \sum_{d\mid n} \mu(d) \cdot \frac{n}{d}.$$

Demostración. Consideremos la función $\mathrm{id} : n \in \mathbb{N} \mapsto n \in \mathbb{N}$. La Proposición 10.2.5 nos dice que para todo $n \in \mathbb{N}$ es

$$g(n) = \sum_{d\mid n} \varphi(d),$$

y entonces la fórmula de inversión de Möbius que vimos en en Ejercicio 9.6.3 nos dice que para

todo $n \in \mathbb{N}$ es

$$\varphi(n) = \sum_{d|n} \mu(d) \cdot g\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d) \cdot \frac{n}{d},$$

y esto es lo que afirma el corolario. □

§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 $a^{p-1} \equiv 1 \mod p$. Esto no es cierto si p no es primo: por ejemplo, 3 es coprimo con 4 pero $3^{4-1} \equiv 3 \not\equiv 1 \mod 4$. 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 $a^{\varphi(m)} \equiv 1 \mod m$.*

Observemos que como $\varphi(p) = p - 1$ para todo primo p, este resultado tiene como caso particular al Teorema de Fermat 10.1.4. De manera similar, si $m = p_1 p_2 \cdots p_r$ es un producto de r primos distintos dos a dos, entonces $\varphi(m) = (p_1 - 1)(p_2 - 1)\cdots(p_r - 1)$, y esta proposición tiene entonces también como casos particulares los resultados de la Proposición 10.1.7 y del Ejercicio 10.1.8

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

$$C(m) \coloneqq \{k \in \mathbb{N} : 1 \leq k \leq m, \mathsf{mcd}(k, m) = 1\}.$$

Si $k \in C(m)$, entonces $k = kxa + kym$ y, por lo tanto,

$$\mathsf{mcd}(ka, m) \mid \mathsf{mcd}(kxa, m) = \mathsf{mcd}(k - kym, m) = \mathsf{mcd}(k, m) = 1,$$

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 $\pi : C(m) \to C(m)$ 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

$$\mathsf{mcd}(kx, m) \mid \mathsf{mcd}(kxa, m) = \mathsf{mcd}(k - kym, m) = \mathsf{mcd}(k, m) = 1,$$

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.

Sean ahora

$$u_1, \quad u_2, \quad \ldots, \quad u_{\varphi(m)} \tag{3}$$

los $\varphi(m)$ elementos del conjunto $C(n)$ listados sin repeticiones. Como la función π es biyectiva, tenemos entonces que

$$r_m(au_1), \quad r_m(au_2), \quad \ldots, r_m(au_{\varphi(m)})$$

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

$$au_1, \quad au_2, \quad \ldots, \quad au_{\varphi(m)}. \tag{4}$$

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

$$u_1u_2\cdots u_{\varphi(m)} \equiv au_1au_2\cdots au_{\varphi(m)} \mod m.$$

Si llamamos w al producto $u_1\cdots u_{\varphi(m)}$, esto nos dice que

$$w \equiv wa^{\varphi(m)} \mod m. \tag{5}$$

El número w es coprimo con m. Existen entonces enteros α y β tales que $\alpha w + \beta m = 1$ y, en particular, $\alpha w \equiv 1 \mod m$. Multiplicando ahora a cada lado de la congruencia (5) por α vemos que

$$1 \equiv \alpha w \equiv \alpha w a^{\varphi(m)} \equiv a^{\varphi(m)} \mod m$$

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 cuyas cifras decimales son periódicas, esto es, tal que si escribimos

$$\frac{a}{b} = 0.d_1d_2d_3d_4\cdots d_nd_{n+1}\cdots$$

al desarrollo decimal de a/b, hay un entero positivo N tal que $d_{i+N} = d_i$ para todo $i \in \mathbb{N}$. Esto nos dice que lo que está después de la coma en la escritura decimal de a/b se obtiene repitiendo indefinidamente el bloque de dígitos $d_1d_2\cdots d_N$, al que llamamos un ***periodo*** del número a/b. Por ejemplo, con

$$\frac{9}{37} = 0.\underbrace{234}\,\underbrace{234}\,\underbrace{234}\,\underbrace{234}\ldots$$

podemos tomar $N = 3$, de manera que el periodo es 234, y con

$$\frac{1}{2\,439} = 0.\underbrace{00041}\,\underbrace{00041}\,\underbrace{00041}\,\underbrace{00041}\ldots$$

elegir $N = 5$, con periodo 00041. Notemos que el número N no está completamente determinado — en el primer ejemplo podríamos haber elegido también $N = 6$ — aunque es fácil ver que siempre hay un periodo más corto que todos los otros y que la longitud de este 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

$$\frac{1}{2} = 0.5000\ldots$$

Ahora bien, si multiplicamos a a/b por 10^N, obtenemos

$$10^N \cdot \frac{a}{b} = d_1\cdots d_N.\underbrace{d_1\cdots d_N}\,\underbrace{d_1\cdots d_N}\,\underbrace{d_1\cdots d_N}\ldots$$

así que si llamamos c al número $(d_1,\cdots,d_N)_{10}$, 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 $0 < c < 10^N - 1$. 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

$$0.d_1 d_2 d_3 \ldots, \tag{7}$$

entonces la de $10^N \cdot q$ es

$$d_1 \cdots d_N . d_{N+1} d_{N+2} \ldots$$

Esto es, de acuerdo a (6), igual a $c + q$: como c es un entero y $0 < q < 1$, es claro que debe ser $c = (d_1, \ldots, d_N)_{10}$ y

$$q = 0.d_{N+1} d_{N+2} d_{N+3} \ldots$$

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. □

10.3.3. Aunque la Proposición 10.3.2 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 $2/18 = 0{,}111\,111\ldots$ 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 $10^{\varphi(b)} \equiv 1 \mod b$ 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 $d = \mathsf{mcd}(b, 10)$, 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. □

§10.4. Dos aplicaciones al problema de decisión de primalidad

El algoritmo de decisión de primalidad de Fermat

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 $a^{p-1} \equiv 1 \mod p$. 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 5.4.20 para calcular potencias, podemos ver — haciendo unas $2 \log_2 n \approx 62.47\ldots$ multiplicaciones, que en la computadora del autor toman 0,000 2 segundos — que

$$2^{2\,534\,968\,907-1} \equiv 1\,475\,261\,599 \not\equiv 1 \mod n.$$

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 hicimos[1].

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 $a^{n-1} \not\equiv 1 \mod n$, 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

10.4.2. En la Figura 10.1 en la página siguiente damos una implementación sencilla de esa idea en Haskell. Con esas definiciones, podemos evaluar

```
*Main> fermatRandom 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> fermatRandom 3 10209288027285050745821549405241 17
False
```

vemos que ese número, que tiene 34 dígitos, es compuesto. De hecho, usando Mathematica podemos ver que su factorización como producto de primos es

$$32452843 \cdot 86028121 \cdot 179424673 \cdot 2038074743.$$

[1] De hecho, armamos el ejemplo eligiendo primero estos dos primos y multiplicándolos para construir el número n.

```
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

fermat :: Integer -> Integer -> Bool
fermat n a = gcd n a == 1 && potencia n a (n - 1) == 1

fermatRandom :: Int -> Integer -> IO Bool
fermatRandom k n = fmap (all (test n) . take m . randomRs (2, n-2)) newStdGen
```

Programa 10.1. El algoritmo de Fermat para decidir si un número es primo.

Por otro lado, podemos calcular:

```
*Main> fermatRandom 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.

10.4.3. Si a es un entero positivo mayor que 1, decimos que un entero positivo n es un ***pseudo-primo*** en base a si es compuesto y divide a $a^{n-1} - 1$. Esto significa precisamente que a es una base que no sirve para certificar usando el algoritmo de Fermat que n es compuesto. Por ejemplo, 341 es un pseudo-primo en base 2: es $341 = 11 \cdot 31$ y usando el teorema de Fermat podemos ver que

$$2^{341-1} \equiv 2^{34(11-1)} \equiv 1 \mod 11, \qquad 2^{341-1} \equiv 2^{11(31-1)+10} \equiv 1 \mod 31,$$

ya que $2^{10} \equiv 1 \mod 31$, y usando el teorema chino del resto podemos concluir que $2^{341-1} \equiv 1 \mod 11 \cdot 31$. Por el contrario, 341 no es un pseudo-primo en base 3, así que 3 sirve para certificar que 341 no es primo: es

$$3^{341-1} \equiv 3^{34(11-1)} \equiv 1 \mod 11, \qquad 3^{341-1} \equiv 3^{11(31-1)+10} \equiv 25 \mod 31,$$

porque $3^{10} \equiv 25 \mod 31$, y de esto podemos deducir que $3^{341-1} \equiv 56 \mod 11 \cdot 31$. El primero en observar la existencia de números pseudo-primos fue Pierre Frédéric Sarrus, que encontró el ejemplo del 341 que acabamos de analizar. Con una computadora es fácil ver que los primeros pseudo-primos en base 2 son

$$341, 561, 645, 1105, 1387, 1729, 1905, 2047, 2465, 2701, 2821, 3277, 4033, 4369, 4371,$$

4681, 5461, 6601, 7957, 8321, 8481, 8911, . . .

En [OEI2023, A001567] puede encontrarse más información sobre esta sucesión de números, que se llaman también ***números de Sarrus*** o ***de Poulet***, por Paul Poulet.

10.4.4. La existencia de números pseudo-primos implica que para un número compuesto n no necesariamente todo número entre 1 y n es un certificado de que n es compuesto. Más aún, nuestro siguiente lema implica inmediatamente que cualquiera sea el entero a mayor que 1 hay infinitos pseudo-primos en base a, y como consecuencia de esto podemos concluir que no hay ningún número a que tenga la propiedad de que para todo $n \in \mathbb{N}$ valga

$$a^{n-1} \equiv 1 \mod n \implies n \text{ es primo},$$

y, de hecho, que ni siquiera hay un entero a para el que esto sea cierto salvo para finitos elecciones de n. En otras palabras, no hay ningún número que sirva como certificado para casi todos los números compuestos. Es esto lo que nos fuerza, si queremos usar el algoritmo de Fermat para decidir que un número es compuesto, a usar muchos valores distintos de a.

Lema. *Si a es un entero mayor que 1, entonces para cada primo p mayor que $a+1$ el número*

$$\frac{a^p - 1}{a-1} \cdot \frac{a^p + 1}{a+1} \tag{8}$$

es un pseudo-primo en base a.

Por ejemplo, si elegimos $a = 2$ y $p = 5$, el pseudo-primo en base 2 que nos da el lema es 341. Este resultado es debido a Michele Cipolla [Cip1904]. En la sección 2 del capítulo VIII del libro [Rib1996] de Paulo Ribenboim se describen varios otros resultados de este tipo.

Demostración. Sea p un número primo mayor que $a+1$, que necesariamente es impar. Escribamos n_{+1} y n_{-1} a los dos factores del producto (8) y pongamos $n := n_{+1}n_{-1}$.

Sea $\varepsilon \in \{\pm 1\}$. Es

$$\frac{a^p - \varepsilon}{a - \varepsilon} = \varepsilon^{p-1} + \sum_{i=1}^{p-1} a^i \varepsilon^{p-1-i}.$$

La suma que aparece aquí tiene $p-1$ sumandos todos congruentes a a módulo 2, así que es un número par: esto implica que el cociente $(a^p - \varepsilon)/(a - \varepsilon)$ es impar. Por otro lado, como $p > a+1 \geq a - \varepsilon$, el entero $a - \varepsilon$ es coprimo con p y existe un entero u tal que $(a-\varepsilon)u \equiv 1 \mod p$. Usando esto y el teorema de Fermat vemos que

$$\frac{a^p - \varepsilon}{a - \varepsilon} \equiv \frac{a^p - \varepsilon}{a - \varepsilon} \cdot (a-\varepsilon)u \equiv (a^p - \varepsilon)u \equiv (a-\varepsilon)u \equiv 1 \mod p,$$

Vemos así que $n_\varepsilon \equiv 1 \mod 2$ y que $n_\varepsilon \equiv 1 \mod p$, así que $n_\varepsilon \equiv 1 \mod 2p$.

Esto implica, claro, que $n = n_{+1}n_{-1} \equiv 1 \mod 2p$ y, por lo tanto, que hay un entero q tal que $n-1 = 2pq$. Ahora bien, es

$$\frac{a^{2p}-1}{a^2-1} = n,$$

así que $a^{2p} \equiv 1 \mod n$, y esto nos permite concluir que $a^{n-1} = (a^{2p})^q \equiv 1 \mod n$, es decir, que n es un pseudo-primo en base a. □

10.4.5. Hemos visto que si un número n es compuesto no necesariamente todo entero entre 1 y n sirva como certificado de que lo es. De todas formas, podemos ilusionarnos y esperar que para cada número compuesto n exista algún certificado de que lo es. Lamentablemente esto no es así.

Decimos que un entero positivo n es un ***número de Carmichael*** si es compuesto y para todo entero a tal que $1 < a < n$ y coprimo con n se tiene que $a^{n-1} \equiv 1 \mod n$. Estos números fueron estudiados originalmente por Alwin Reinhold Korselt en [Kor1899] y por Robert Daniel Carmichael en [Car1912]. El más chico de estos números fue encontrado por Carmichael: es el 561, que tiene por factorización a $3 \cdot 11 \cdot 17$. Mostremos que este número tiene esa propiedad.

Sea a un entero coprimo con 561. Del teorema de Fermat sabemos que $a^2 \equiv 1 \mod 3$, de manera que $a^{10} \equiv (a^2)^5 \equiv 1 \mod 3$, y $a^{10} \equiv 1 \mod 11$, y entonces $a^{10} \equiv 1 \mod 3 \cdot 11$ y

$$a^{80} = (a^{10})^8 \equiv 1 \mod 3 \cdot 11. \tag{9}$$

Por otro lado, el teorema de Fermat nos dice que $(a^8)^2 = a^{16} \equiv 1 \mod 17$ y es fácil[2] ver que entonces $a^8 \equiv \pm 1 \mod 17$ y, por lo tanto, $a^{80} \equiv 1 \mod 17$. Esta congruencia junto con (9) nos permiten concluir que

$$a^{80} \equiv 1 \mod 3 \cdot 11 \cdot 17.$$

Por otro lado, el resultado del Ejercicio 10.1.8 nos permite concluir que

$$a^{320} = a^{(3-1)(11-1)(17-1)} \equiv 1 \mod 3 \cdot 11 \cdot 17$$

y entonces que

$$a^{561-1} \equiv a^{560}a^{80} \equiv a^{640} \equiv (a^{320})^2 \equiv 1 \mod 3 \cdot 11 \cdot 17.$$

Esto prueba que 561 es un número de Carmichael, como queremos. En particular, el algoritmo de Fermat no nos permite certificar que se trata de un número compuesto.

[2] Si x es un entero tal que $x^2 \equiv 1 \mod 17$, entonces 17 divide a $x^2 - 1 = (x-1)(x+1)$ y, como es primo, divide a $x-1$ o a $x+1$, de manera que $x \equiv 1$ o $x \equiv -1 \mod 17$.

10.4.6. En [AGP1994] William Robert Alford, Andrew Granville y Carl Pomerance probaron que existen infinitos números de Carmichael. Los primeros son

561, 1 105, 1 729, 2 465, 2 821, 6 601, 8 911, 10 585, 15 841, 29 341, 41 041, 46 657,

52 633, 62 745, 63 973, 75 361, 101 101, 115 921, 126 217, 162 401, 172 081, 188 461, ...

En [OEI2023, A002997] puede encontrarse más información sobre esta sucesión. El número de Carmichael más grande conocido fue encontrado por William Robert Alford, Jon Grantham, Steven Hayman y Andrew Shallue en [AGHS2014]: tiene 295 486 761 787 dígitos y es el producto de 10 333 229 505 primos distintos dos a dos.

No solamente hay infinitos números de Carmichael sino que, en cierto sentido, hay muchos. En [Har2008] Glyn Harman probó, por ejemplo, que cuando n es grande hay al menos $n^{1/3}$ números de Carmichael menores o iguales que n. Se conocen, además, varios resultados sobre la distribución de los números de Carmichael. Recientemente, Daniel Larsen probó en 2021 [Lar2023] para estos números un resultado similar al llamado *postulado de Bertrand* — Larsen tenía 17 años en ese momento.

10.4.7. La existencia de números de Carmichael implica que el algoritmo de Fermat no puede responder con certeza la pregunta de si un número es primo o no. Ahora bien, si suponemos que n es compuesto y *no es* un número de Carmichael, entonces sabemos que existen certificados de que es compuesto: ¿cuántos hay?

Proposición. *Sea n un entero positivo compuesto que no es un número de Carmichael. Entre los $\varphi(n)$ elementos de $\{1, \dots, n\}$ que son coprimos con n al menos la mitad son certificados de que n es compuesto.*

Demostración. Consideremos los conjuntos

$$A \coloneqq \{a \in \{1, \dots, n\} : \mathsf{mcd}(a, n) = 1, a^{n-1} \not\equiv 1 \mod n\}$$

y

$$B \coloneqq \{a \in \{1, \dots, n\} : \mathsf{mcd}(a, n) = 1, a^{n-1} \equiv 1 \mod n\}.$$

Claramente A y B son disjuntos, y su unión es el conjunto de elementos de $\{1, \dots, n\}$ que son coprimos con n, así que $|A| + |B| = |A \cup B| = \varphi(n)$.

Como n no es un número de Carmichael, el conjunto A no es vacío. Sea x uno de sus elementos. Si y pertenece a B, entonces $(xy)^{n-1} \equiv x^{n-1}y^{n-1} \equiv x^{n-1} \not\equiv 1 \mod n$, así que $xy \in A$. Esto nos dice que hay una función

$$f : y \in B \mapsto xy \in A.$$

Esta función es inyectiva. En efecto, como $\mathsf{mcd}(x, n) = 1$, hay un entero u tal que $ux \equiv 1 \mod n$: si y e y' son dos elementos de B tales que $f(y) = f(y')$, entonces $y \equiv uxy \equiv uxy' \equiv y' \mod n$ y,

como $1 \leq y, y' \leq n$, $y = y'$. Ahora bien, como la función f es inyectiva claramente tenemos que $|B| \leq |A|$ y, por lo tanto, que $2|A| \geq |A| + |B| = \varphi(n)$, de manera que $|A| \geq \varphi(n)/2$. Esto es lo que afirma la proposición. □

Esta proposición nos dice que si n es un entero positivo que es compuesto y no es un número de Carmichael y elegimos al azar un elemento de $\{1, \ldots, n\}$ coprimo con n, entonces la probabilidad de que no sea un certificado de que n es compuesto es como mucho $1/2$. Se sigue de esto que si elegimos k tales elementos la probabilidad de que ninguno de ellos sea un certificado es como mucho $1/2^k$ y esta probabilidad decrece exponencialmente con k. Así, por ejemplo, es suficiente elegir 34 candidatos para que la probabilidad de que ninguno sea un certificado sea menor que 0,000 000 000 1. En 10.4.2 hicimos 10 000 intentos de encontrar un certificado de que 2 038 074 743 es compuesto y no lo encontramos: si suponemos que este número no es un número de Carmichael (y no lo es), entonces la probabilidad de que no sea primo es menor[3] que $1/2^{10\,000} \sim 10^{-3000}$.

De todas formas, hay — como observamos arriba — relativamente muchos números de Carmichael y no es fácil determinar si un numero es o no de estos. Esto hace que, en la práctica, no usemos solamente el algoritmo de Fermat para decidir si un número es *probablemente* primo y que, entonces, lo combinemos con otro posiblemente más costoso computacionalmente pero que no tenga «excepciones».

El algoritmo de decisión de primalidad de Miller–Rabin

10.4.8. En [Mil1976] Gary Miller describió un algoritmo completamente determinístico para decidir si un número es primo o no, pero que es «condicional»: esto significa que su corrección depende de la validez una conjetura — la llamada *hipótesis de Riemann generalizada* — que no está probada. Cuatro años más tarde, Michael Oser Rabin mostró en [Rab1980] cómo modificar el algoritmo para que funcione incondicionalmente pero en forma probabilística.

10.4.9. Para describir este algoritmo necesitamos la siguiente observación bien sencilla:

Lema. *Sea p un número primo. Si x es un entero tal que $x^2 \equiv 1 \mod p$, entonces x es congruente a 1 o a -1 módulo p.*

En otras palabras, 1 tiene como mucho dos raíces cuadradas módulo p — y, de hecho, tiene exactamente dos si p es impar, ya que en ese caso $1 \not\equiv -1 \mod p$.

[3] En realidad, para poder afirmar esto con toda certeza habría que analizar en detalle la forma en que elegimos los candidatos al azar.

Demostración. Si x es un entero tal que $x^2 \equiv 1 \mod p$, entonces $p \mid x^2 - 1 = (x-1)(x+1)$ y, como p es primo, esto nos dice que p divide a $x-1$ o a $x+1$. La afirmación del lema sigue inmediatamente de esto. □

10.4.10. En base a este lema podemos probar el resultado que está en la base del algoritmo de Miller–Rabin

Proposición. *Sea p un número primo impar y sean s y d enteros positivos tales que $p = 2^s d + 1$ y d es impar. Para todo entero positivo a menor que p vale alguna de las siguientes dos afirmaciones:*

(*a*) *Es $a^d \equiv 1 \mod p$.*

(*b*) *Hay exactamente un elemento r de $\{0, \dots, s-1\}$ tal que $a^{2^r d} \equiv -1 \mod p$.*

En la Figura 10.2 ilustramos este resultado cuando $p = 41$.

Demostración. Sea a un entero positivo menor que p. Como p es primo a es coprimo con p y, de acuerdo al teorema de Fermat 10.1.4, tenemos que $a^{2^s d} \equiv a^{p-1} \equiv 1 \mod p$. Esto nos dice que el conjunto

$$S \coloneqq \{i \in \{0, \dots, s\} : a^{2^i d} \equiv 1 \mod p\}$$

no es vacío, ya que contiene a s: podemos entonces considerar su menor elemento. Si $\min S = 0$, es $a^d \equiv 1 \mod p$ y vale la primera de las dos afirmaciones de la proposición. Si, por el contrario, es $\min S > 0$, entonces el número $r \coloneqq \min S - 1$ pertenece a $\{0, \dots, s-1\}$ y no a S, y $r+1 \in S$: esto nos dice que $a^{2^r d} \not\equiv 1 \mod p$ y que $(a^{2^r d})^2 \equiv a^{2^{r+1} d} \equiv 1 \mod p$, y el Lema 10.4.9 nos permite concluir que $a^{2^r d} \equiv -1 \mod p$, de manera que vale la afirmación de existencia de (*b*).

Para verificar la afirmación de unicidad de (*b*) supongamos ahora que hay dos elementos distintos r y r' de $\{0, \dots, s-1\}$ tales que $a^{2^r d} \equiv -1 \mod p$ y $a^{2^{r'} d} \equiv -1 \mod p$, y, sin pérdida de generalidad, que $r < r'$, de manera que $u \coloneqq r' - r$ es un entero positivo. Tenemos entonces que

$$-1 \equiv a^{2^{r'} d} \equiv (a^{2^r d})^{2^u} = (-1)^{2^u} \equiv 1 \mod p,$$

y esto es absurdo, ya que p es un entero impar. □

10.4.11. Esta proposición nos da una condición necesaria para que el número p sea primo, y podemos entonces usarla para probar que un número no lo es. Por ejemplo, si tomamos

$$n = 28\,393\,021 = 2^2 \cdot 7\,098\,255 + 1$$

podemos calcular fácilmente que módulo n es

$$2^{7\,098\,255} \not\equiv 1, \qquad 2^{7\,098\,255} \not\equiv -1, \qquad 2^{2 \cdot 7\,098\,255} \not\equiv -1$$

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
	$\varnothing$	1	2	0	1	2	2	1	1	$\varnothing$	2	2	2	2	2	$\varnothing$	2	$\varnothing$	2	1

a	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
	1	2	0	2	0	2	2	2	2	2	0	1	1	2	2	1	$\varnothing$	2	1	0

Figura 10.2. Elegimos aquí $p = 41 = 2^3 \cdot 5 + 1$ y para cada entero positivo a menor que p tabulamos el entero $s \in \{0, 1, 2\}$ tal que $a^{2^s d} \equiv -1 \mod p$, si es que hay alguno, o ponemos un símbolo $\varnothing$.

y esto es suficiente para concluir que n no es primo. De manera similar, si

$$n = 9\,629\,970\,333\,103 = 2 \cdot 4\,814\,985\,166\,551 + 1,$$

entonces módulo n es

$$2^{4\,814\,985\,166\,551} \equiv 8\,956\,534\,393\,410,$$

y esto no es congruente ni con 1 ni con -1, así que podemos concluir que n no es primo. Notemos que el cálculo de esta potencia puede hacerse haciendo solamente 44 productos y divisiones entre números menores que n, lo que lleva menos de un milisegundo con una computadora moderna.

10.4.12. El ***algoritmo de Miller–Rabin*** para determinar si un entero positivo impar n es primo consiste en elegir un entero positivo a menor que n y verificar que alguna de las dos afirmaciones de la Proposición 10.4.10 se cumple. Si esto no es así, entonces tenemos certeza de que n no es primo — decimos en ese caso que a es un ***certificado*** de Miller–Rabin para n. Si, por el contrario, alguna de esas afirmaciones se cumple entonces no podemos decir nada, claro.

A diferencia de lo que ocurre con el algoritmo de Fermat — debido a la existencia de números de Carmichael — todo número compuesto impar posee un certificado de Miller–Rabin. No se conoce, de todas formas, una forma de encontrar uno. Miller [Mil1976] y Eric Bach [Bac1990] probaron — asumiendo la verdad de la hipótesis de Riemannn generalizada — que si n es compuesto e impar entonces hay un certificado a que cumple la desigualdad $1 < a < 2(\ln n)^2$, y esto nos dice que es suficiente buscar uno entre los enteros que satisfacen estas desigualdades: esto es conocido como el ***algoritmo de Miller*** y es completamente determinístico. Por ejemplo, si

$$n = 54\,299\,051\,326\,517 = 2^2 \cdot 13\,574\,762\,831\,629 + 1$$

entonces $2(\ln n)^2 = 2\,000{,}348\,02\ldots$ así que estamos seguros de que, si es que es compuesto, podemos encontrar un certificado entre 1 y 2000. En el peor de los casos, entonces, podremos decidir si n es primo o no calculando 2000 potencias de exponente menor que n módulo n.

10.4.13. En la práctica este algoritmo de Miller no suele usarse. En su lugar, simplemente se elige al azar un número k de enteros positivos menores que n y para cada uno de ellos se verifica si se cumplen o no alguna de las afirmaciones de la proposición. Si para alguno esto no ocurre, entonces podemos concluir que n es compuesto. En el caso contrario, claro, no podemos decir nada, pero Rabin probó en [Rab1980] que

> *si n es compuesto e impar, entonces como mucho $1/4$ de los enteros positivos menores que n no son certificados de Miller–Rabin para n.*

Esto implica que si hacemos k intentos con números elegidos al azar entonces la probabilidad de que n sea compuesto pero no lo podamos certificar con ninguno de ellos es menor que $1/4^k$, y esto decrece rápidamente cuando k aumenta. El algoritmo de Miller–Rabin nos permite establecer que n es primo con mucha probabilidad — que es lo que se llama un ***primo probable***.

10.4.14. Exactamente como con el algoritmo de Fermat es posible probar que no hay ningún entero que sirva como certificado de Miller–Rabin para todo entero compuesto, y esto es lo que nos fuerza a tener que buscar para cada n un certificado. De todas formas, si uno solamente está interesado en enteros n en un rango fijo esta situación puede mejorarse.

Por ejemplo, Carl Pomerance, John Lewis Selfridge y Samuel Wagstaff [PSW1980] y Gerhard Jaeschke [Jae1993] probaron que

- todo entero compuesto impar menor que 2 047 tiene a 2 como certificado de Miller–Rabin,
- todo entero compuesto impar menor que 341 550 071 728 321 tiene a alguno de 2, 3, 5, 7, 11, 13, o 17 como certificado.

Todo esto significa que podemos decidir si un número menor que 341 550 071 728 321 de manera completamente determinística y muy rápido. Más recientemente, Jonathan Sorenson y Jonathan Webster probaron en [SW2017] que

> *todo entero compuesto impar menor que* 3 317 044 064 679 887 385 961 981 *tiene uncertificado de Miller–Rabin que pertenece al conjunto* $\{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41\}$.

Esto nos da una forma extremadamente rápida de decidir la primalidad de cualquier número de a lo sumo 24 dígitos.

10.4.15. En la Figura 10.2 damos una implemenación sencilla del algoritmo de Miller-Rabin. Usando esas definiciones, podemos evaluar

```
ghci> millerRabin 1475261599 2
False
```

```
import System.Random

valuación :: Integer -> Integer -> Integer
valuación b n
  | n `mod` b == 0 = valuación b (n `div` b) + 1
  | otherwise      = 0

potencia :: Integer -> Integer -> Integer -> Integer
potencia n a 0 = 1
potencia n a d
  | even d     = potencia n a (d `div` 2) ^ 2 `mod` n
  | otherwise  = a * (potencia n a ((d - 1) `div` 2)) ^ 2 `mod` n

millerRabin :: Integer -> Integer -> Bool
millerRabin n a = p == 1 || (n - 1) `elem` ps
  where s = valuación 2 (n - 1)
        d = (n - 1) `div` (2 ^ s)
        p = potencia n a d `mod` n
        ps = take (fromIntegral s) (iterate (\x -> x^2 `mod` n) p)

millerRabinRandom :: Int -> Integer -> IO Bool
millerRabinRandom k n
        = fmap (all (millerRabin n) . take k . randomRs (2, n-2)) newStdGen
```

Programa 10.2. El algoritmo de Miller–Rabin para decidir si un número es primo.

y esto nos dice que 2 es un certificado de que el número 1 475 261 599 es compuesto. Por otro lado, evualuando

```
ghci> millerRabin 2038074743 2
True
```

vemos que 2 no es un certificado de que 2 038 074 743 es compuesto. Finalmente, evaluando

```
ghci> millerRabinRandom 1000 2038074743
True
```

generamos 1 000 enteros entre 2 y 2 038 074 743 − 2 al azar y verificamos que ninguno de ellos es un certificado de que 2 038 074 743 es compuesto.

§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 $a^{\varphi(m)} \equiv 1 \mod m$, así que, en particular, el conjunto

$$S_a = \{k \in \mathbb{N} : a^k \equiv 1 \mod m\} \tag{10}$$

no es vacío. Podemos entonces considerar su menor elemento, al que llamamos el ***orden*** de a módulo m y escribimos $\mathsf{ord}_m(a)$. Notemos que definimos el orden módulo m de un entero a sólo cuando este último es coprimo con m y por una buena razón: si no es ése el caso, el conjunto S_a que definimos arriba es vacío.

El orden de a nos permite describir el conjunto S_a completamente:

Proposición. *Sea $m \in \mathbb{N}$ y sea a un entero coprimo con m. Tenemos que $a^{\mathsf{ord}_m(a)} \equiv 1 \mod m$ y, más aún, un entero positivo t es tal que $a^t \equiv 1 \mod m$ si y solamente si es divisible por $\mathsf{ord}_m(a)$.*

Demostración. La primera afirmación es inmediata, ya que $\mathsf{ord}_m(a)$ pertenece al conjunto S_a de (10). Veamos la segunda.

Sea t un entero positivo. Supongamos primero que $a^t \equiv 1 \mod m$ y sean q y r el cociente y el resto de la división de t por $\mathsf{ord}_m(a)$, de manera que $t = q\,\mathsf{ord}_m(a) + r$ y $0 \leq r < \mathsf{ord}_m(a)$. Tenemos entonces que

$$1 \equiv a^t \equiv a^{q\,\mathsf{ord}_m(a)+r} \equiv (a^{\mathsf{ord}_m(a)})^q a^r \equiv a^r \mod m,$$

así que o bien $r = 0$ o bien $r \in S_a$. Como la segunda opción no puede ocurrir, ya que $r < \mathsf{ord}_m(a)$

y $\mathsf{ord}_m(a)$ es el menor elemento de S_a, vemos que $r = 0$, esto es, que r es divisible por $\mathsf{ord}_m(a)$. Esto muestra que la condición del enunciado es necesaria.

Su suficiencia, por otro lado, es casi evidente: si t es un múltiplo de $\mathsf{ord}_m(a)$, de manera que existe $s \in \mathbb{N}$ tal que $t = s\,\mathsf{ord}_m(a)$, entonces $a^t = (a^{\mathsf{ord}_m(a)})^s \equiv 1^s \equiv 1 \mod m$. □

10.5.2. Combinando esta proposición con el teorema de Euler obtenemos lo siguiente:

Corolario. *Si $m \in \mathbb{N}$ y a es un entero coprimo con m, entonces $\mathsf{ord}_m(a)$ divide a $\varphi(m)$. En particular, si m es primo, entonces $\mathsf{ord}_p(a)$ divide a $m - 1$.*

Demostración. De acuerdo al teorema de Euler 10.3.1, es $a^{\varphi(m)} \equiv 1 \mod m$, así que la Proposición 10.5.1 nos dice que $\mathsf{ord}_m(a)$ 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 $\varphi(m) = m - 1$. □

10.5.3. 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*

$$1,\ a,\ a^2,\ \ldots,\ a^{n-1} \tag{11}$$

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 $k \in \mathbb{N}_0$ y r es el resto de la división de k por n, entonces $a^k \equiv a^r \mod m$.

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 $0 \le i < j < n$ y $a^i \equiv a^j \mod m$. 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 $a^{j-i} \equiv 1 \mod m$: esto es imposible, ya que la diferencia $j - i$ es positiva y estrictamente menor que n, el orden de a.

Sea ahora $k \in \mathbb{N}_0$ y sean q y r el cociente y el resto de la división de k por n, de manera que $k = qn + r$ y $0 \le r < n$. Es $a^k = (a^n)^q a^r \equiv a^r \mod m$, así que a^k es congruente a uno de los enteros listados en (11). Sólo puede ser congruente a uno de ellos, ya que sabemos que no hay ahí dos que sean congruentes entre sí. □

10.5.4. La siguiente observación es importante: nos dice cómo calcular el orden de una potencia de un entero cuando conocemos el de este.

Proposición. *Sea $m \in \mathbb{N}$, sea a un entero coprimo con m, y sea $k \in \mathbb{N}_0$. El orden de a^k módulo m es*

$$\mathsf{ord}_m(a^k) = \frac{\mathsf{ord}_m(a)}{\mathsf{mcd}(\mathsf{ord}_m(a), k)}.$$

Demostración. Escribamos $n \coloneqq \mathsf{ord}_m(a)$ y $t \coloneqq \mathsf{ord}_m(a^k)$. 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 $d \coloneqq \mathsf{mcd}(n, k)$ y sean n_1 y k_1 enteros tales que $n = n_1 d$ y $k = k_1 d$; sabemos que es entonces $\mathsf{mcd}(n_1, k_1) = 1$. Como

$$k_1 dt = kt = nm = n_1 dm$$

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

$$(a^k)^{n_1} = a^{kn_1} = a^{k_1 d n_1} = a^{k_1 n} = (a^n)^{k_1} \equiv 1 \mod m,$$

así que $t = \mathsf{ord}_m(a^k) \mid n_1$ y, por lo tanto, $t \leq n_1$. Concluimos de esta forma que

$$t = n_1 = \frac{n}{d} = \frac{\mathsf{ord}_m(a)}{\mathsf{mcd}(\mathsf{ord}_m(a), k)},$$

que es lo que afirma la proposición. □

10.5.5. 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 $\mathsf{ord}_m(a)$, entonces el orden de a^k es $\mathsf{ord}_m(a)/k$.*

(*ii*) *Si k es coprimo con $\mathsf{ord}_m(a)$, entonces $\mathsf{ord}_m(a^k) = \mathsf{ord}_m(a)$.*

Demostración. Ambas afirmaciones son consecuencia inmediata de la proposición: en el primer caso $\mathsf{mcd}(\mathsf{ord}_m(a), k)$ es k y en el segundo es 1. □

10.5.6. Buscamos ahora información sobre el orden de un producto de dos números.

Proposición. *Sea $m \in \mathbb{N}$ y sean a y b dos enteros coprimos con m.*

(*i*) *El orden de ab es un divisor $\mathsf{mcm}(\mathsf{ord}_m(a), \mathsf{ord}_m(b))$.*

(*ii*) *Si los órdenes $\mathsf{ord}_m(a)$ y $\mathsf{ord}_m(b)$ son coprimos, entonces $\mathsf{ord}_m(ab) = \mathsf{ord}_m(a)\,\mathsf{ord}_m(b)$.*

Por supuesto, si a y b son coprimos con m también lo es ab, y es por esto que podemos hablar del orden de ab módulo m.

Demostración. Escribamos $x \coloneqq \mathsf{ord}_m(a)$, $y \coloneqq \mathsf{ord}_m(b)$ y $z \coloneqq \mathsf{ord}_m(ab)$.

(*i*) Sea $s \coloneqq \mathsf{mcm}(x, y)$, de manera que hay enteros positivos x_1 e y_1 tales que $s = xx_1$ y $s = yy_1$. Usando esto, vemos que

$$(ab)^s = a^s b^s = (a^x)^{x_1}(b^y)^{y_1} \equiv 1 \mod m$$

y, en particular, que $\mathsf{ord}_m(ab)$ divide a s.

(*ii*) Supongamos que $\mathsf{mcd}(x, y) = 1$. Como

$$(ab)^{xy} = (a^x)^y (b^y)^x \equiv 1^y 1^x \equiv 1 \mod m,$$

se tiene que $z \mid xy$. Por otro lado, tenemos que

$$a^z b^z = (ab)^z \equiv 1 \mod m,$$

así que

$$1 \equiv (a^z b^z)^y = a^{yz}(b^y)^z \equiv a^{yz} \mod m$$

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. □

10.5.7. En la situación de la Proposición 10.5.6(*i*) no se tiene en general que el orden de ab sea igual a $\mathsf{mcm}(\mathsf{ord}_m(a), \mathsf{ord}_m(b))$. 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 $\mathsf{mcm}(12, 6) = 12$.

El siguiente resultado nos dice, de todas formas, que podemos construir en la situación de la Proposición 10.5.6(*i*) a partir de a y b un número de orden igual a $\mathsf{mcm}(\mathsf{ord}_m(a), \mathsf{ord}_m(b))$, 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 $\mathsf{mcm}(\mathsf{ord}_m(a), \mathsf{ord}_m(b))$.*

Demostración. Sean $x \coloneqq \mathsf{ord}_m(a)$ e $y \coloneqq \mathsf{ord}_m(b)$. De acuerdo a la Proposición 9.3.9, existen enteros positivos u y v tales que $\mathsf{mcd}(u, v) = 1$, $\mathsf{mcd}(x, y) = uv$, $u \mid x$ y $v \mid y$. Como x/u divide a x, el Corolario 10.5.5(*i*) nos dice que $\mathsf{ord}_m(a^{x/u}) = \mathsf{ord}_m(a)/(x/u) = u$ y, de manera similar y como y/v divide a y, que $\mathsf{ord}_m(b^{y/v}) = v$. Ahora bien, como u y v son coprimos, la Proposición 10.5.6(*ii*) nos dice que el orden de $a^{x/u} b^{y/v}$ es uv, que es igual a $\mathsf{mcm}(x, y)$. Esto prueba la proposición: basta elegir $r = x/u$ y $s = y/v$. □

10.5.8. Como es habitual, podemos extender la afirmación de la Proposición 10.5.7 al caso en que

tenemos un número arbitrario de enteros:

Corolario. *Sea $m \in \mathbb{N}$. Si $n \in \mathbb{N}$ y $a_1, \ldots, a_n$ son enteros coprimos con m, entonces existen enteros positivos $r_1, \ldots, r_n$ tales que $a_1^{r_1} \cdots a_n^{r_n}$ tiene orden*

$$\mathsf{mcm}(\mathsf{ord}_m(a_1), \ldots, \mathsf{ord}_m(a_n))$$

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 10.5.7. Supongamos entonces que $n \geq 3$ y sean $a_1, \ldots, a_n$ enteros coprimos con n. De acuerdo a la Proposición 10.5.7 existen enteros positivos r y s tales que el orden de $a_1^r a_2^s$ es $\mathsf{mcm}(\mathsf{ord}_m(a_1), \mathsf{ord}_m(a_2))$. Por otro lado, la hipótesis inductiva obvia nos dice que existen enteros positivos $b_1, \ldots, b_{n-1}$ 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

$$\mathsf{mcm}(\mathsf{mcm}(\mathsf{ord}_m(a_1), \mathsf{ord}_m(a_2)), \mathsf{ord}_m(a_2), \ldots, \mathsf{ord}_m(a_n)),$$

que, de acuerdo al Ejercicio 6.6.4(*e*), es igual a

$$\mathsf{mcm}(\mathsf{ord}_m(a_1), \mathsf{ord}_m(a_2), \mathsf{ord}_m(a_2), \ldots, \mathsf{ord}_m(a_n)).$$

Esto completa la inducción y, por lo tanto, la prueba del corolario. □

§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 $a^n \equiv 1 \mod p$ 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

$$R(n) \coloneqq \{a \in \mathbb{Z} : 1 \leq a < p,\ a^n \equiv 1\}$$

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 $a_1, \ldots, a_t$ todos los elementos de $R(n)$, listados sin repeticiones, de manera que $t > n$, y sea $n' = \mathsf{mcm}(\mathsf{ord}_p(a_1), \ldots, \mathsf{ord}_p(a_t))$. Afirmamos que n' es igual a n.

En efecto, si i es un elemento cualquiera de $\{1, \ldots, t\}$, entonces $a_i^n \equiv 1$, así que $\mathsf{ord}_p(a_i)$ divide a n: como n' es el mínimo común múltiplos de los órdenes $\mathsf{ord}_p(a_1), \ldots, \mathsf{ord}_p(a_t)$, esto nos dice que n' divide a n. Por otro lado, si i pertenece a $\{1, \ldots, t\}$ entonces $\mathsf{ord}_p(a_i)$ divide a n', así que $a_i^{n'} \equiv 1$. Vemos así que todos los elementos $a_1, \ldots, a_t$ 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 10.5.8, vemos que hay enteros positivos $\alpha_1, \ldots, \alpha_t$ 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 $\mathsf{ord}_p(x) = n$. En particular, la Proposición 10.5.3 nos dice que los n enteros

$$1,\ x,\ x^2,\ \ldots,\ x^{n-1} \tag{12}$$

son no congruentes dos a dos. Si $i \in \{0, \ldots, n-1\}$, entonces $(x^i)^n = (x^n)^i \equiv 1$ y por lo tanto los restos de los n números de la lista (12) son n elementos distintos de $R(n)$. Más aún, tenemos que

> *si d es un divisor propio de n, entonces $R(d)$ tiene exactamente d elementos, que son los restos de los enteros $1,\ x^{n/d},\ x^{2n/d},\ \ldots,\ x^{(d-1)n/d}$.* (13)

Para verlo, basta observar que si d es un divisor propio de n, entonces los restos de los d enteros $1,\ x^{n/d},\ x^{2n/d},\ \ldots,\ x^{(d-1)n/d}$ 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 (12) tiene orden n.*

Para verlo, supongamos que y es un elemento de $R(n)$ que no es congruente con ninguno de los números de (12) y sea m el orden de y. Como $y^n \equiv 1$, 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 (13), los

elementos de $R(m)$ son entonces los restos de 1, $x^{n/m}$, $x^{2n/m}$, …, $x^{(m-1)n/m}$: 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 (12); 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 $(y^q)^{n/q} = y^m \equiv 1$, el entero y^q es congruente a un elemento de $R(n/q)$. Como n/q es menor que n, nuestra observación (13) nos dice que los elementos de $R(n/q)$ son los restos de los enteros 1, x^q, x^{2q}, …, $x^{(n/q-1)q}$ y esto implica que y^q es congruente con uno de ellos. En otras palabras, existe $i \in \{0, \ldots, n/q - 1\}$ 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, $x^{n/q}$, …, $x^{(q-1)n/q}$ 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 en 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

$$f(u) \coloneqq (1-u)(x-u)(x^2-u)\cdots(x^{n-1}-u). \tag{14}$$

En particular, tenemos que

$$f(xu) = (1-xu)(x-xu)(x^2-xu)\cdots(x^{n-1}-xu) \tag{15}$$

Ahora bien, para cada $j \in \{1, \ldots, n-1\}$ 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 (15), 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 (14) 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, …, $x^{n-2}u$, en orden, vemos inmediatamente que para todo entero u se tiene que

$$f(u) \equiv f(xu) \equiv f(x^2u) \equiv \cdots \equiv f(x^{n-1}u). \tag{16}$$

Quinto paso. Volvamos ahora a considerar el producto $f(u)$ de (14): 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

$$f(u) = c_0 + c_1u + c_2u^2 + \cdots + c_nu^n \tag{17}$$

para ciertos enteros $c_0, \ldots, c_n$, cada uno de los cuales es una suma con signos de productos de las potencias $1, x, \ldots, x^{n-1}$. 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 (16), tenemos que

$$\begin{aligned} nf(u) &= \underbrace{f(u) + f(u) + f(u) + \cdots + f(u) + \cdots + f(u)}_{n \text{ sumandos}} \\ &\equiv f(u) + f(xu) + f(x^2u) + \cdots + f(x^i) + \cdots + f(x^{n-1}u) \end{aligned}$$

Si usamos ahora la expresión (17) 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 $i \in \{0, \ldots, n-1\}$ 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 (12). Esta contradicción nos dice que nuestra hipótesis de partida es insostenible y, en consecuencia, que la proposición es cierta. □

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 positivo d de $p-1$ consideremos el conjunto

$$\Psi(d) \coloneqq \{a \in \mathbb{Z} : 1 \leq a < p,\ \mathsf{ord}_p(a) = d\}$$

y sea $\psi(d) \coloneqq |\Psi(d)|$ su cardinal. Como cada entero entre 1 y $p-1$ tiene un orden módulo p que es un divisor de $p-1$, tenemos que

$$\{a \in \mathbb{Z} : 1 \leq a < p\} = \bigcup_{d \mid p-1} \Psi(d),$$

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

$$p - 1 = \sum_{d \mid p-1} \psi(d). \tag{18}$$

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 $\mathsf{ord}_p(y) = d$. En ese caso, sabemos que los restos módulo p de los enteros $1,\ y,\ y^2,\ \ldots,\ y^{d-1}$ 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 $i \in \{0, \ldots, d-1\}$, sabemos que el orden de y^i es $d/\mathsf{mcd}(d, i)$: 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

$$\psi(d) \leq \varphi(d) \tag{19}$$

y, por lo tanto, que

$$\sum_{d|p-1} \psi(d) \leq \sum_{d|p-1} \varphi(d), \tag{20}$$

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 (18), (19), (20) 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. □

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 $p-1$ módulo p 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 $n = p-1$. □

10.6.4. Cuando m es un entero positivo y a es un entero coprimo con m tal que $1 \leq a < m$ y $\mathsf{ord}_m(a) = \varphi(m)$ 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 $\varphi(p-1)$ raíces primitivas módulo p. Si a es una raíz primitiva módulo p, sabemos de la Proposición 10.5.3 que las $p-1$ potencias

$$1,\ a,\ a^2,\ \ldots,\ a^{p-2}$$

son coprimas con p y no congruentes módulo p dos a dos, así que sus restos módulo p son precisamente los elementos de $\{1, \ldots, p-1\}$, listados en algún orden.

Por ejemplo, 3 es una raíz primitiva módulo 7, ya que sus primeras potencias son

$$3^0 \equiv 1, \quad 3^1 \equiv 3, \quad 3^2 \equiv 2, \quad 3^3 \equiv 6, \quad 3^4 \equiv 4, \quad 3^5 \equiv 5, \quad 3^6 \equiv 1 \mod 7.$$

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

$$5^0 \equiv 1, \quad 5^1 \equiv 5, \quad 5^2 \equiv 4, \quad 5^3 \equiv 6, \quad 5^4 \equiv 2, \quad 5^5 \equiv 3, \quad 5^6 \equiv 1 \mod 7.$$

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 $q_1, \ldots, q_r$ los divisores primos de $p-1$ y sea a un entero tal que $1 \leq a < p-1$. Si $a^{(p-1)/q_i} \not\equiv 1 \mod p$ para cada $i \in \{1, \ldots, r\}$, 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 $a^{(p-1)/q} = (a^n)^k \equiv 1 \mod p$. Esto prueba la implicación contrarrecíproca a la del enunciado. □

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**,

$$\frac{\varphi(p-1)}{p-1} = \left(1 - \frac{1}{q_1}\right) \cdots \left(1 - \frac{1}{q_r}\right)$$

con $q_1, \ldots, q_r$ 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 $\{1, \ldots, p-1\}$ es relativamente alta.

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.

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

$$\frac{\varphi(p-1)}{p-1} = \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = \frac{4}{15} \approx 0{,}266\,666\ldots,$$

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 $(p-1)! \equiv -1 \mod p$.*

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

$$1,\ a,\ a^2,\ \ldots,\ a^{p-2} \tag{21}$$

son los números

$$1,\ 2,\ 3,\ \ldots,\ p-1 \tag{22}$$

listados en algún orden. En particular, el producto de los $p - 1$ enteros de (21) es congruente módulo p con el producto de los de (22), esto es,

$$(p-1)! \equiv a^0 \cdot a^1 \cdot a^2 \cdot \ldots \cdot a^{p-2} = a^{(p-1)(p-2)/2} \mod p. \tag{23}$$

Sabemos que en $\{1, \ldots, p-1\}$ 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

$$(a^{(p-1)/2})^2 = a^{p-1} \equiv 1 \mod p,$$

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

$$a^{(p-1)(p-2)/2} = (a^{(p-1)/2})^{p-2} \equiv (-1)^{p-2} \equiv -1 \mod p.$$

Esto junto con (23) nos dice que $(p-1)! \equiv -1 \mod p$, 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 $(p-1)! \not\equiv -1 \mod p$. □

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 $a^{(p-1)/2} \equiv 1 \mod p$.*

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 $a \equiv b^2 \mod p$, entonces el teorema de Fermat 10.1.4 nos dice que

$$a^{(p-1)/2} \equiv (b^2)^{(p-1)/2} = b^{p-1} \equiv 1 \mod p.$$

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 $a \equiv r^i \mod p$. Si suponemos que la condición del enunciado vale, entonces tenemos que

$$1 \equiv a^{(p-1)/2} \equiv r^{i(p-1)/2} \mod p.$$

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 $a \equiv r^i \equiv (r^j)^2 \mod p$ y a es congruente a un cuadrado módulo p. □

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. Hay un entero x tal que $x^2 \equiv -1 \mod p$ si y solamente si $p \equiv 1 \mod 4$.*

Demostración. De acuerdo al criterio de Euler 10.6.8, el entero -1 es congruente a un cuadrado módulo p si y solamente si $(-1)^{(p-1)/2} \equiv 1 \mod p$. 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, $-1 \not\equiv 1 \mod p$. Esto prueba el corolario. □

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 $x^2 \equiv 2 \mod p$ 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

$$s! = \prod_{1\le k\le s} k = \prod_{1\le k\le s} \left((-1)^k k \cdot (-1)^k\right) = \prod_{1\le k\le s} ((-1)^k k) \cdot \prod_{1\le k\le s} (-1)^k. \tag{24}$$

Sabemos que

$$\prod_{1\le k\le s} (-1)^k = (-1)^{1+2+\cdots+s} = (-1)^{s(s+1)/2}. \tag{25}$$

Por otro lado,

$$\prod_{1\le k\le s} ((-1)^k k) = \prod_{\substack{1\le k\le s\\ k \text{ par}}} ((-1)^k k) \cdot \prod_{\substack{1\le k\le s\\ k \text{ impar}}} ((-1)^k k) = \prod_{\frac{1}{2}\le l\le \frac{s}{2}} (2l) \cdot \prod_{0\le l\le \frac{s-1}{2}} (-(2l+1)).$$

Como $-(2l+1) \equiv 2(s-l) \mod p$ para todo entero l, este último producto es congruente módulo p con

$$\prod_{\frac{1}{2}\le l\le \frac{s}{2}} (2l) \cdot \prod_{0\le l\le \frac{s-1}{2}} (2(s-l)).$$

Cambiando el índice del segundo producto, podemos reescribir esto en la forma

$$\prod_{\frac{1}{2}\le l\le \frac{s}{2}} (2l) \cdot \prod_{\frac{s+1}{2}\le l\le s} (2l)$$

y si consideramos ahora con cuidado qué factores aparecen aquí vemos que este producto es igual a $2^s s!$. Usando esto y (25) en la igualdad (24) vemos que

$$s! \equiv (-1)^{s(s+1)/2} 2^s s! \mod p.$$

Como $s!$ es coprimo con p, esto implica inmediatamente que

$$2^s \equiv (-1)^{s(s+1)/2} = (-1)^{(p^2-1)/8} \mod p.$$

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. □

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 $p \equiv 1 \mod 4$, 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 $p \equiv 1 \mod 4$ 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 o 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 $\mathsf{ord}_q(2)$ 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 $p \equiv 1 \mod 4$, 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 $2^p \not\equiv 1 \mod q$ y, por lo tanto, $\mathsf{ord}_q(2) \neq p$. 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. □

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, 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; puede encontrarse más información sobre esta sucesión de números

en [OEI2023, A005384]. 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 — 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 situación.

A lo largo de su vida Germain 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 Friedrichs 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 corresponsal 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 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.*