donde $(b_0, d_0) = \pm(b_-, d_-)$, eligiendo el signo para que el determinante sea 1.

Por la Proposición 1.1.8, necesariamente $b = b_0 + at$ y $d = d_0 + ct$, de modo que posmultiplicando por T^t se obtiene M en términos de T y S. □

Siguiendo los pasos de la prueba, expresemos

$$M = \begin{pmatrix} 18 & -31 \\ 7 & -12 \end{pmatrix}$$

como producto de potencias de T y S. Sabíamos de un ejercicio anterior que al aplicar el algoritmo de Euclides a 18 y 7 se tenía $c_0 = 2$, $c_1 = c_2 = 1$, $c_3 = 3$, así que consideramos

$$T^2UTUTUT^3U = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 3 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 18 & 5 \\ 7 & 2 \end{pmatrix}$$

donde el último cálculo se ha hecho con el algoritmo de la fracción continua. Podemos reemplazar $UT^{c_j}U$ por $-ST^{c_j}S$, así pues

$$T^2ST^{-1}STST^{-3}S = \begin{pmatrix} 18 & 5 \\ 7 & 2 \end{pmatrix}.$$

Para ajustar la última columna, posmultiplicamos por T^{-2} y así se obtiene

$$M = T^2ST^{-1}STST^{-3}ST^{-2}.$$

Nótese que procediendo de esta forma el número de factores que resultan es aproximadamente el doble de los pasos que requiere el algoritmo de Euclides.

1.2. El anillo de clases de congruencias

La estructura de anillo. La función φ. El teorema chino del resto. Las congruencias de Euler-Fermat y de Wilson. Raíces primitivas.

En el marco de las estructuras algebraicas, $\mathbb{Z}$ tiene estructura de anillo conmutativo con unidad cuando se consideran la suma y el producto habituales. Dado un entero m, el conjunto de múltiplos de m, que indicaremos con $m\mathbb{Z}$, es un *ideal* de este anillo. Es decir, es un subgrupo respecto a la suma y es imposible salirse de él multiplicando por elementos del anillo. Según la teoría general [50, §3.5], el conjunto cociente $\mathbb{Z}/m\mathbb{Z}$ hereda la estructura de anillo. Notando que $m\mathbb{Z} = (-m)\mathbb{Z}$ y escapando de los ideales impropios $\{0\}$ y $\mathbb{Z}$, que dan cocientes triviales, es natural restringirse a $m > 1$.

Este cociente tiene una interpretación en términos de congruencias porque $a \equiv b\ (m)$ equivale a $a - b \in m\mathbb{Z}$. Entonces $\mathbb{Z}/m\mathbb{Z}$ es lo mismo que identificar cada entero con su *clase de congruencia*, el conjunto de los que son

congruentes con él módulo m. La estructura de anillo de $\mathbb{Z}/m\mathbb{Z}$ se traduce en que hay una aritmética coherente de restos: si a y b dejan, respectivamente, restos r y s al ser divididos por m, entonces $a+b$ y ab dejan restos $r+s$ y rs salvo un múltiplo de m.

En un ámbito básico se abrevia a veces $\mathbb{Z}/m\mathbb{Z}$ con $\mathbb{Z}_m$. Esta abreviatura tiene la desventaja de que para m primo se solapa con otra notación que aparece en temas más avanzados de teoría de números. La evitaremos aquí. Por lo dicho anteriormente, es natural suponer $m > 1$ y así lo haremos en toda la sección sin repetirlo cada vez. La clase de congruencia de $n \in \mathbb{Z}$ la indicaremos también con n o excepcionalmente con $\overline{n}$ en estas primeras líneas o si hay posibilidad de confusión.

En $\mathbb{Z}/m\mathbb{Z}$ la existencia del inverso multiplicativo no está garantizada. Por el Teorema 1.1.1, si a y m son coprimos existen $x, y \in \mathbb{Z}$ con

$$ax + by = 1, \qquad \text{entonces} \quad \overline{ax} = \overline{1}.$$

Esto es, la clase $\overline{a}$ tiene inverso. Es muy fácil completar el resultado a:

Lema 1.2.1. *La clase $\overline{a}$ tiene inverso en $\mathbb{Z}/m\mathbb{Z}$ si y solo si a y m son coprimos.*

Demostración. Si $\gcd(a,m) = d > 1$ entonces $ax \equiv 1\ (m)$ es imposible porque d divide a m pero no a $ax - 1$. □

A los elementos invertibles en un anillo R se les llama *unidades*. Forman un grupo abeliano con la multiplicación que se suele denotar mediante R^* o $\mathcal{U}(R)$. Usaremos la primera opción escribiendo $(\mathbb{Z}/m\mathbb{Z})^*$.

Se define la *función φ de Euler* como la que cuenta el número de unidades en $\mathbb{Z}/m\mathbb{Z}$ o, según el Lema 1.2.1, la cantidad de enteros coprimos con m en $\{1, 2, \ldots, m\}$, que es un conjunto completo de representantes de las clases. En una fórmula:

$$\varphi(m) = \left|(\mathbb{Z}/m\mathbb{Z})^*\right| = \left|\{1 \le a \le m \,:\, \gcd(a,m) = 1\}\right|.$$

Dados $m_1, m_2, \ldots, m_N \in \mathbb{Z}_{>1}$ coprimos dos a dos, esto es, $\gcd(m_j, m_k) = 1$ para $1 \le i < j \le N$, se tiene que $\gcd(m_j, M/m_j) = 1$ con $M = \prod_{j=1}^{N} m_j$, por el Lema 1.1.6. El Lema 1.2.1 asegura que existen $u_j \in \mathbb{Z}$ con $u_j(M/m_j) \equiv 1\ (m)$. La función $F : \mathbb{Z}^N \longrightarrow \mathbb{Z}$ dada por

$$F(n_1, \ldots, n_N) = n_1 u_1 M/m_1 + n_2 u_2 M/m_2 + \cdots + n_N u_N M/m_N$$

permite combinar las congruencias módulo m_j para obtener una congruencia módulo M.

Proposición 1.2.2. *Si $m_1, m_2, \ldots, m_N \in \mathbb{Z}_{>1}$ son coprimos dos a dos entonces la función F induce, al pasar a las clases, un isomorfismo de anillos de $(\mathbb{Z}/m_1\mathbb{Z}) \oplus (\mathbb{Z}/m_2\mathbb{Z}) \oplus \cdots \oplus (\mathbb{Z}/m_N\mathbb{Z})$ a $\mathbb{Z}/M\mathbb{Z}$.*

Demostración. En primer lugar hay que notar que al sumar a n_j, en los argumentos de F, un múltiplo de m_j, el resultado cambia por un múltiplo de M, entonces F está bien definida al pasar a las clases. Además la función inducida en las clases es un homomorfismo: preserva las sumas por ser lineal y también los productos porque M divide a $(M/m_j)(M/m_k)$ para $j \neq k$ y a $(u_jM/m_j)^2 - u_jM/m_j$, ya que $m_j \mid u_jM/m_j - 1$ por la elección de u_j.

El cardinal de ambos anillos es M, por tanto basta comprobar la inyectividad. Si $F(n_1, n_2, \ldots, n_N)$ es múltiplo de M, como $m_j \mid M$ y $m_j \mid M/m_k$ para $k \neq j$, se deduce $m_j \mid n_j u_j M/m_j$ para cada j, lo que implica $m_j \mid n_j$ por el Lema 1.1.6, esto es, $\overline{n}_j = \overline{0}$. Por tanto el núcleo es trivial. □

La traducción de este resultado a congruencias es lo que se llama *teorema chino del resto*:

Corolario 1.2.3. *Si $m_1, m_2, \ldots, m_N \in \mathbb{Z}_{>1}$ son coprimos dos a dos, dados $a_1, \ldots, a_N \in \mathbb{Z}$ cualesquiera, existe $x \in \mathbb{Z}$ tal que $x \equiv a_j\ (m_j)$ para todo $1 \leq j \leq N$. Además tal x es único módulo $M = \prod_{j=1}^{N} m_j$.*

Por ejemplo, para resolver

$$x \equiv 1\ (3), \qquad x \equiv 2\ (4), \qquad x \equiv 3\ (7),$$

tenemos que usar $F(1,2,3)$ con $m_1 = 3$, $m_2 = 4$, $m_3 = 7$, lo que lleva a $M/m_1 = 28$, $M/m_2 = 21$, $M/m_3 = 12$, de los que tenemos que hallar inversos módulo m_1, m_2, m_3, que son $u_1 = 1$, $u_2 = 1$, $u_3 = 3$. Con ello,

$$F(1,2,3) = 1 \cdot 1 \cdot 28 + 2 \cdot 1 \cdot 21 + 3 \cdot 3 \cdot 12 = 178$$

que módulo $M = 3 \cdot 4 \cdot 7 = 84$ es 10. Por tanto, el sistema de las tres congruencias equivale a $x \equiv 10\ (84)$.

Corolario 1.2.4. *Para $m_1, m_2 \in \mathbb{Z}_{>1}$ coprimos, $\varphi(m_1)\varphi(m_2) = \varphi(m_1 m_2)$.*

Demostración. Basta notar $(\mathbb{Z}/m_1\mathbb{Z} \oplus \mathbb{Z}/m_2\mathbb{Z})^* = (\mathbb{Z}/m_1\mathbb{Z})^* \times (\mathbb{Z}/m_2\mathbb{Z})^*$ e igualar su cardinal con el de $(\mathbb{Z}/m_1m_2\mathbb{Z})^*$. □

Corolario 1.2.5. *Para $n \in \mathbb{Z}_{>1}$ se tiene*

$$\varphi(n) = \prod_{j=1}^{k} p_j^{\alpha_j}\big(1 - \frac{1}{p_j}\big)$$

con p_j y α_j como en el Teorema 1.1.7.

Demostración. Se tiene $\varphi(p_j^{\alpha_j}) = p_j^{\alpha_j} - p_j^{\alpha_j - 1}$ porque hay $p_j^{\alpha_j - 1}$ múltiplos de p_j menores o iguales que $p_j^{\alpha_j}$. Sustituyendo esta evaluación en una aplicación iterada del resultado anterior, se obtiene la fórmula. □

Por ejemplo, $\varphi(1000000) = \varphi(2^6 5^6) = 2^6(1-1/2)\cdot 5^6(1-1/5) = 400000$.

La abstracción que requiere dotar a las congruencias de una estructura algebraica se compensa con elegantes pruebas sintéticas de resultados clásicos.

▶ **Proposición 1.2.6** (Congruencia de Euler)**.** *Si $a \in \mathbb{Z}$ y $m \in \mathbb{Z}_{>1}$ son coprimos,*

$$a^{\varphi(m)} \equiv 1 \quad (m).$$

También se llama a este resultado *congruencia de Euler-Fermat* por el siguiente caso particular:

Demostración. El orden de a en $(\mathbb{Z}/m\mathbb{Z})^*$ divide al orden de este grupo, por el teorema de Lagrange. □

▶ **Corolario 1.2.7** (Pequeño teorema de Fermat)**.** *Si $a \in \mathbb{Z}$ y p es primo,*

$$a^p \equiv a \quad (p)$$

Demostración. Si $p \mid a$ es trivial y si $p \nmid a$, se sigue de la Proposición 1.2.6 porque $\varphi(p) = p - 1$. □

Proposición 1.2.8 (Congruencia de Wilson)**.** *Si p es primo,*

$$(p-1)! \equiv -1 \quad (p).$$

Demostración. Si $1 \leq n < p$ y $p \mid n^2 - 1 = (n-1)(n+1)$ se tiene $n = 1$ o $n = p - 1$. Esto significa que $\overline{1}$ y $\overline{p-1}$ son las únicas clases en $\mathbb{Z}/p\mathbb{Z}$ que coinciden con su inversa. El resto, por tanto, se deben cancelar por parejas al multiplicar. Es decir, $\overline{1}$ es la clase de $(p-1)!/\big(1\cdot(p-1)\big)$, lo que equivale al resultado. □

De hecho no es difícil obtener un recíproco: si $(n-1)! \equiv -1$ (n) entonces n es primo.

Si $m = p$ es primo, todas las clases en $\mathbb{Z}/m\mathbb{Z}$ excepto $\overline{0}$ poseen inverso (Lema 1.2.1) y se obtiene un cuerpo, que en un contexto más amplio se denota con $\mathbb{F}_p$.

Un resultado general de álgebra [25, §7.1] afirma que para cualquier cuerpo finito el grupo de unidades (formado por todos los elementos menos el cero) es cíclico, esto es, $(\mathbb{Z}/p\mathbb{Z}) \cong C_{p-1}$ donde C_n es el grupo cíclico de n elementos. Con herramientas aritméticas básicas se prueba el siguiente resultado que permite establecer la estructura del grupo de unidades para cualquier módulo (véase [45, Th.2.6,2.7] [46, §8.3] para su prueba).

Teorema 1.2.9. *Sea $p > 2$ primo y $\alpha \in \mathbb{Z}^+$. Se tiene*

$$(\mathbb{Z}/p^\alpha\mathbb{Z})^* \cong C_{\varphi(p^\alpha)} \qquad y \qquad (\mathbb{Z}/2^\alpha\mathbb{Z})^* \cong \begin{cases} C_{\varphi(2^\alpha)} & si\ \alpha = 1, 2, \\ C_2 \times C_{2^{\alpha-2}} & si\ \alpha > 2. \end{cases}$$

Se dice que $g \in \mathbb{Z}$ coprimo con m es una *raíz primitiva* módulo m si $\overline{g}$ genera $(\mathbb{Z}/m\mathbb{Z})^*$. En particular, la existencia de raíces primitivas equivale a que $(\mathbb{Z}/m\mathbb{Z})^*$ sea cíclico. En términos más elementales, las raíces primitivas son los enteros tales que sus potencias generan dan lugar a todos los restos coprimos con m al dividir por m.

▶ **Proposición 1.2.10.** *Los módulos para los que existen raíces primitivas son exactamente $m = 2$, 4, p^α y $2p^\alpha$ con $p > 2$ primo y $\alpha \in \mathbb{Z}^+$. Además en cada caso el número de raíces primitivas $1 \leq g \leq m$ es $\varphi\big(\varphi(m)\big)$.*

Demostración. Si $m = 2$, 4, p^α la existencia de raíces primitivas se sigue del teorema anterior. También se sigue para $2p^\alpha$ porque $(\mathbb{Z}/2p^\alpha\mathbb{Z})^* \cong (\mathbb{Z}/2\mathbb{Z})^* \times (\mathbb{Z}/p^\alpha\mathbb{Z})^*$ y el primer factor es el grupo trivial. Para otros módulos m que no sean una potencia de dos, se cumple que $p^\alpha q^\beta \mid m$ con $q > 2$ primo, $\beta \in \mathbb{Z}^+$ o $q = 2$ y $\beta \in \mathbb{Z}_{>1}$. En esta situación $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$ y $(\mathbb{Z}/q^\beta\mathbb{Z})^*$ aparecen como factores de $(\mathbb{Z}/m\mathbb{Z})^*$ y no es cíclico porque los cardinales de estos factores, $\varphi(p^\alpha)$ y $\varphi(q^\beta)$, son ambos pares. Finalmente, el teorema asegura que $(\mathbb{Z}/2^\alpha\mathbb{Z})^*$ no es cíclico para $m = 2^\alpha$ con $\alpha > 2$.

Una vez supuesta la existencia de raíces primitivas, $(\mathbb{Z}/m\mathbb{Z})^* \cong C_{\varphi(m)}$ y es fácil ver que C_n tiene $\varphi(n)$ generadores, de donde se deduce la parte final. □

Por ejemplo, consideremos $m = 2 \cdot 3^2 = 18$. El grupo $(\mathbb{Z}/18\mathbb{Z})^*$ tiene $\varphi(18) = 6$ elementos, $\{1, 5, 7, 11, 13, 17\}$. Obviamente 1 y 17, que es -1, no dan lugar a raíces primitivas porque tienen orden 1 y 2. Los cálculos $5^2 \equiv 7$ y $5^3 \equiv -1$ (18) muestran que 5 tiene orden mayor que 3 y como tal orden debe dividir a 6, es exactamente 6. De ello deducimos que 5 es raíz primitiva. Por otro lado, 7 no lo es porque $7^3 \equiv 1$ (18). Notando que 13 y -5 están en la misma clase y 11 y -7 también lo están, los mismos cálculos cambiando signos muestran que 13 no es raíz primitiva y 11 sí lo es. En definitiva, solo hay dos raíces primitivas $1 \leq g \leq 18$, lo cual es coherente con la Proposición 1.2.10 porque $\varphi(\varphi(18)) = \varphi(6) = 2$.

1.3. La ley de reciprocidad cuadrática

Símbolo de Legendre. Criterio de Euler. Una prueba rápida.

Tanto en el arte como en las matemáticas es difícil caracterizar la belleza, sin embargo hay bastante más consenso acerca de la belleza matemática, incluso entre los expertos de diferentes generaciones, que acerca de la belleza artística. Algunos rasgos que usualmente contribuyen a que un resultado