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

matemático se considere inequívocamente bello es que establezca una conexión inesperada, que resuelva no trivialmente un problema natural, que posea un enunciado breve y simétrico, que tenga implicaciones profundas y que, aunque en ello habría menos acuerdo, admita la experimentación con ejemplos.

Todas estas cualidades se aplican al resultado principal de esta sección, uno de los teoremas más emblemáticos de la teoría de números.

Comencemos con alguna motivación. Una ecuación lineal $ax + b = 0$ en $\mathbb{Z}/p\mathbb{Z}$ tiene solución si a no es la clase de 0, esto es, $p \nmid a$. El siguiente paso es el cuadrático $ax^2 + bx + c = 0$. Practicando con algunos ejemplos se ven patrones inesperados. Por ejemplo, consideremos

$$x^2 + 4x - 1 = 0 \qquad \text{en} \quad \mathbb{Z}/p\mathbb{Z}.$$

Nos preguntamos para qué primos p tiene solución. Los casos $p = 2$ y $p = 5$ son especiales porque el polinomio para estos módulos resulta ser $(x-1)^2$ y $(x+2)^2$ obteniéndose solución única. No es difícil probar que son los únicos primos con esta particularidad. Para el resto, o bien hay dos soluciones o bien no hay ninguna. Con la ayuda de un pequeño programa, hagamos una tabla para ver cómo se distribuyen los primeros primos en estas categorías:

Sin sol.	$3, 7, 13, 17, 23, 37, 43, 47, 53, 67, 73, 83, 97, 103, 107, 113, 127, \ldots$
Dos sol.	$11, 19, 29, 31, 41, 59, 61, 71, 79, 89, 101, 109, 131, 139, 149, 151, \ldots$

Tras un vistazo, se infiere que hay dos soluciones si y solo si la última cifra (la menos significativa) de p es un 1 o un 9 y no hay solución si y solo si es un 3 o un 7. Esto es realmente sorprendente. Además el milagro reaparece para cada ecuación cuadrática cambiando las propiedades de la última cifra, que es el resto al dividir por 10, por condiciones de congruencia sobre p para algún módulo. Por ejemplo, para

$$x^2 + x - 3 = 0 \qquad \text{en} \quad \mathbb{Z}/p\mathbb{Z},$$

excluyendo los casos especiales $p = 2$ y $p = 13$ (en el primero no hay solución y en el segundo hay solución única) resulta que hay dos soluciones si y solo si p es congruente con ± 1, ± 3 o ± 4 módulo 13 y no hay solución en el resto de los casos.

L. Euler detectó experimentalmente patrones de este tipo e hizo algunos avances teóricos. Su trabajo fue complementado por el de A.-M. Legendre. Ambos enunciaron la ley correcta que explicaba los patrones, aunque ninguno de ellos fue capaz de probarla en su totalidad. Esta ley es la llamada *ley de reciprocidad cuadrática* y la primera demostración completa la obtuvo C.F. Gauss en su juventud y aparece en su obra maestra *Disquisitiones Arithmeticae* [20]. Además de contener notabilísimos resultados, dicha obra es un texto fundacional para la teoría de números tal como la entendemos

hoy. Es respecto a esta área algo así como los *Elementos* respecto a todas las matemáticas.

Antes de enunciar la ley de reciprocidad cuadrática, necesitaremos un poco de notación. Se dice que $a \in \mathbb{Z}$ es un *residuo cuadrático* módulo p (primo) si $p \nmid a$ y $x^2 \equiv a\ (p)$ tiene solución $x \in \mathbb{Z}$. Si $p \nmid a$ y $x^2 \equiv a\ (p)$ no tiene solución, se dice que a es un *no residuo cuadrático*. Nótese que los múltiplos de p están excluidos de esta clasificación. Con ello se define el *símbolo de Legendre*

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{si } a \text{ es residuo cuadrático módulo } p, \\ -1 & \text{si } a \text{ es no residuo cuadrático módulo } p, \\ 0 & \text{si } p \mid a. \end{cases}$$

Lleva solo un instante convencerse de que

$$\left|\{x \in \mathbb{Z}/p\mathbb{Z} \,:\, x^2 - a = 0\}\right| = 1 + \left(\frac{a}{p}\right) \qquad \text{para} \quad p > 2 \tag{1.3}$$

porque si x es solución, $-x$ también lo es. Aquí estamos abusando ligeramente de la notación, identificando a y su clase.

Utilizando que $(p-a)^2 \equiv a^2\ (p)$ es fácil ver que para $p > 2$

$$\left(\frac{a}{p}\right) = 1 \quad \Leftrightarrow \quad a \equiv r\ (p) \quad \text{con} \quad r \in \left\{1^2, 2^2, 3^2, \ldots ((p-1)/2)^2\right\}. \tag{1.4}$$

Además los elementos del último conjunto pertenecen a diferentes clases de congruencia porque $x^2 \equiv y^2\ (p)$ si y sólo si $x \equiv \pm y\ (p)$.

El resultado principal de esta sección, del que hemos hecho tanta propaganda, es:

▶ **Teorema 1.3.1** (Ley de reciprocidad cuadrática)**.** *Si $p, q > 2$ son primos distintos,*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}.$$

Se suele preferir este enunciado simétrico, aunque quizá sea más informativa la siguiente traducción:

$$\left(\frac{p}{q}\right) = \begin{cases} -\left(\frac{q}{p}\right) & \text{si } 4 \mid p+1 \text{ y } 4 \mid q+1 \\ \left(\frac{q}{p}\right) & \text{en el resto de los casos} \end{cases}$$

Normalmente se añaden un par de evaluaciones de evaluaciones del símbolo de Legendre que a veces se llaman "leyes suplementarias", aunque no tienen ni mucho menos la misma profundidad.

Proposición 1.3.2. *Si $p > 2$ es primo*

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} \qquad y \qquad \left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}.$$

En palabras, esto se traduce en que -1 es residuo cuadrático módulo p si y solo si p es de la forma $4k+1$ mientras que 2 lo es si y solo si p es de la forma $8k+1$ o $8k-1$.

Antes de seguir, veamos por qué la ley de reciprocidad cuadrática explica los ejemplos anteriores. Completando cuadrados, $x^2+4x-1 = (x+2)^2 - 5$. Según (1.3), para $p = 5$ hay una solución y para el resto de los $p > 2$ existe solución (de hecho dos) si y solo si $(5/p) = 1$. Aplicando el Teorema 1.3.1 con $q = 5$ se tiene

$$\left(\frac{p}{5}\right)\left(\frac{5}{p}\right) = 1 \qquad \text{o, equivalentemente,} \quad \left(\frac{5}{p}\right) = \left(\frac{p}{5}\right).$$

Los residuos cuadráticos módulo 5 son congruentes a 1^2 o a 2^2, por (1.4). Por tanto

$$\left(\frac{5}{p}\right) = 1 \quad \Longleftrightarrow \quad 5 \mid p - 1^2 \quad \text{o} \quad 5 \mid p - 2^2.$$

Ahora bien, un primo que al restarle 1 es divisible por 5, necesariamente acaba en 1 y si lo es al restarle 4, debe acabar en 9.

El segundo ejemplo es similar salvo un pequeño problema inicial al completar cuadrados, ya que $x^2 + x - 3 = (x + 1/2)^2 - 13/4$ en $\mathbb{Q}$ y debemos trabajar con congruencias o clases módulo p, no con fracciones. Si $p > 2$, se cumple $2 \cdot (p+1)/2 \equiv 1\ (p)$ y entonces $t = (p+1)/2$, que es entero, hace las veces de $1/2$. Con ello,

$$x^2 + x - 3 \equiv t^2\big((2x+1)^2 - 13\big) \quad (p).$$

Para $p = 13$ hay una solución módulo 13 y para el resto de los $p > 2$, procediendo como antes, habrá solución si y solo si $(p/13) = 1$ que equivale a $13 \mid p - k^2$ para algún $1 \leq k \leq 6$, por (1.4). De $1^2 \equiv -5^2 \equiv 1$, $2^2 \equiv -3^2 \equiv 4$ y $4^2 \equiv -6^2 \equiv 3$ módulo 13, se deduce que p es de la forma indicada.

Comencemos la teoría con un resultado de Euler que afina el pequeño teorema de Fermat (Corolario 1.2.7).

Proposición 1.3.3 (Criterio de Euler)**.** *Para $p > 2$ primo y $a \in \mathbb{Z}$, se tiene*

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \quad (p).$$

A costa de alargar la demostración, separemos el siguiente resultado que en realidad es consecuencia inmediata de algo que ya sabemos a partir de (1.4): hay $(p-1)/2$ clases que dan lugar a residuos y otras $(p-1)/2$ que dan lugar a no residuos.

Lema 1.3.4. *Si g es una raíz primitiva módulo $p > 2$, las clases que corresponden a residuos cuadráticos son las de g^k con $0 \leq k < p-1$ par y las que corresponden a no residuos las que tienen k impar, en el mismo rango.*

Demostración. Dado a no divisible por p, sea ℓ tal que $a \equiv g^\ell$. Escribiendo $x = g^k$ la existencia de solución de $x^2 \equiv a\ (p)$ equivale a que exista $0 \leq k < p-1$ con $g^{2k-\ell} = 1$ en $\mathbb{Z}/p\mathbb{Z}$, lo que se traduce en $2k = \ell + (p-1)m$, porque el orden de g es $p-1$, y k se puede despejar si y solo si ℓ es par. □

Demostración de la Proposición 1.3.3. Tanto las clases de los residuos como las de los no residuos anulan $x^{p-1} - 1$ en $\mathbb{Z}/p\mathbb{Z}$ por el pequeño teorema de Fermat. Teniendo en cuenta que $x^{p-1} - 1 = (x^{(p-1)/2} - 1)(x^{(p-1)/2} + 1)$, que los residuos cuadráticos anulan el primer factor (por el Lema 1.3.4) y que el número de ceros de un polinomio sobre un cuerpo no puede superar al grado (teorema de Lagrange), necesariamente los no residuos anulan el segundo factor. □

Corolario 1.3.5. *Para p primo y $a, b \in \mathbb{Z}$ se tiene*

$$\Big(\frac{ab}{p}\Big) = \Big(\frac{a}{p}\Big)\Big(\frac{b}{p}\Big).$$

Demostración. El caso $p = 2$ es trivial. Para el resto se aplica el criterio de Euler notando que la congruencia $(a/p)(b/p) \equiv (ab/p)$ módulo p implica la igualdad porque ambos miembros pertenecen a $\{-1, 0, 1\}$. □

Una consecuencia es que hay una aritmética del producto de residuos y no residuos similar a la de la suma de números pares e impares: el producto de dos residuos o de dos no residuos es un residuo mientras que el producto de un residuo y de un no residuo es no residuo. Por otro lado, si $aa^* \equiv 1\ (p)$ entonces $(a/p) = (a^*/p)$. En realidad esto último se obtiene también fácilmente de la definición.

Demostración de la Proposición 1.3.2. La primera parte se sigue directamente del criterio de Euler (Proposición 1.3.3). Para la segunda parte comenzamos aplicando el criterio de Euler para establecer

$$\Big(\frac{2}{p}\Big)\, t! \equiv \mathcal{P}\ \ (p) \qquad \text{donde} \qquad t = \frac{p-1}{2} \quad \text{y} \quad \mathcal{P} = \prod_{k=1}^{t} (2k).$$

Dividiendo el producto en $k < p/4$ y $k > p/4$, se tiene

$$\mathcal{P} \equiv \prod_{1 \leq k < p/4} (2k) \prod_{p/4 < k \leq t} (p-2k) \prod_{p/4 < k \leq t} (-1) = t!(-1)^{(p-1)/2 - \lfloor p/4 \rfloor}.$$

Para la última igualdad, nótese que en el primer producto, $2k$ recorre los enteros pares en $[1,t]$ y en el segundo, $p-2k$ recorre los impares en este mismo intervalo. Con ello deducimos

$$\Big(\frac{2}{p}\Big) = (-1)^{(p-1)/2-\lfloor p/4\rfloor}.$$

Solo resta justificar que el exponente se puede reemplazar por $(p^2-1)/8$. Esto se deduce de que ambas expresiones son pares para $p = 8k\pm 1$ e impares para $p = 8k \pm 3$. □

El propio Gauss dio ocho pruebas de la ley de reciprocidad cuadrática y hoy en día existen, sin exageración, centenares de pruebas (el autor de [38] mantiene una *web* en la que proporciona referencias a más de 300). En [3] y [55] hay dos recientes, relacionadas con una clásica de G. Eisenstein, que destacan por su brevedad. Aquí nos decidimos por la versión de [3] que es menos breve y, a cambio, tiene una línea argumental más clara. La idea es hallar de dos maneras distintas el valor de

$$N_d = \big|\{\vec{x} \in (\mathbb{Z}/p\mathbb{Z})^d \,:\, x_1^2 - x_2^2 + x_3^2 - \cdots - x_{d-1}^2 + x_d^2 = 1\}\big| \quad \text{con } 2 \nmid d.$$

La primera forma es por inducción.

Lema 1.3.6. *Si $p > 2$ es primo y $2 \nmid d$, se tiene $N_d = p^{d-1} + p^{(d-1)/2}$.*

Demostración. El resultado es cierto para $d = 1$. Para $d > 1$, haciendo el cambio de variable $x_d = y + x_{d-1}$ la ecuación se convierte en

$$x_1^2 - x_2^2 + x_3^2 - \cdots + x_{d-2}^2 = 1 - y^2 - 2yx_{d-1}.$$

Si $y = 0$, por la hipótesis de inducción hay $N_{d-2} = p^{d-3} + p^{(d-3)/2}$ soluciones para cada $x_{d-1} \in \mathbb{Z}/p\mathbb{Z}$. Si $y \neq 0$, podemos asignar a x_j, $1 \leq j \leq d-2$, valores arbitrarios en $\mathbb{Z}/p\mathbb{Z}$ y a y valores arbitrarios en $(\mathbb{Z}/p\mathbb{Z})^*$ y despejar x_{d-1}, lo que da lugar a $p^{d-2}(p-1)$ soluciones. Sumando ambos casos, en total hay $\big(p^{d-3} + p^{(d-3)/2}\big)p + p^{d-2}(p-1)$ soluciones. □

La segunda forma es con el símbolo de Legendre.

Lema 1.3.7. *Si $p > 2$ es primo y $2 \nmid d$, se tiene*

$$N_d = p^{d-1} + (-1)^{(d-1)(p-1)/4} \sum_{u_1+\cdots+u_d=1} \Big(\frac{u_1u_2\cdots u_d}{p}\Big)$$

donde los u_j recorren las clases módulo p.

Demostración. Llamando u_j a $(-1)^{j-1}x_j$ se tiene, por (1.3),

$$N_d = \sum_{u_1+\cdots+u_d=1} \left(1+\left(\frac{u_1}{p}\right)\right)\left(1+\left(\frac{-u_2}{p}\right)\right)\left(1+\left(\frac{u_3}{p}\right)\right)\cdots\left(1+\left(\frac{u_d}{p}\right)\right).$$

Al expandir el producto los términos que contienen a (u_1/p) pero sí al resto de los u_j contribuyen $\sum(-u_2/p)(u_3/p)\cdots(u_d/p)$ sin restricciones en la suma para los u_j, porque u_1 siempre se puede ajustar para que se cumpla $u_1 + \cdots + u_d = 1$. Esta suma es cero porque $\sum_{u=1}^{p}(u/p) = 0$, ya que hay tantos residuos como no residuos. El mismo razonamiento se aplica a los términos que no contienen a ciertos u_j y sí a otros. Por consiguiente,

$$N_d = \sum_{u_1+\cdots+u_d=1} \left(1+\left(\frac{u_1(-u_2)\cdots(-u_{d-1})u_d}{p}\right)\right).$$

Utilizando la primera parte de la Proposición 1.3.2 y notando que el número de soluciones de $u_1+\cdots+u_d = 1$ es p^{d-1}, se deduce al fórmula buscada. □

Demostración del Teorema 1.3.1. Tomemos $d = q$ en el Lema 1.3.6 y en el Lema 1.3.7. Al igualar los valores de N_q obtenidos en ellos, se deduce que el sumatorio del Lema 1.3.7 es $(-1)^{(p-1)(q-1)/4}p^{(q-1)/2}$ y, por el criterio de Euler, $p^{(q-1)/2} \equiv (p/q)$. Así basta probar que el sumatorio es congruente con (q/p) módulo q.

Si $(u_1, \ldots, u_q)$ no tiene todas sus coordenadas iguales, al permutar cíclicamente las variables obtenemos q vectores distintos $(u_q, u_1 \ldots, u_{q-1})$, etc. que contribuyen en total $q(u_1 \cdots u_q/p)$ al sumatorio. Por tanto, módulo q basta considera $u_j = u$ y el sumatorio es igual a (u^q/p) donde $qu \equiv 1\ (p)$. Usando que $q+1$ es par y el Corolario 1.3.5,

$$\left(\frac{u^q}{p}\right) = \left(\frac{q}{p}\right)^{q+1}\left(\frac{u^q}{p}\right) = \left(\frac{q}{p}\right)\left(\frac{(qu)^q}{p}\right) = \left(\frac{q}{p}\right)\left(\frac{1}{p}\right) = \left(\frac{q}{p}\right),$$

lo que concluye la prueba. □

Veamos con mayor profundidad por qué la ley de reciprocidad cuadrática permite decidir la solubilidad para p arbitrario de cualquier ecuación fijada de segundo grado

$$ax^2 + bx + c = 0 \quad \text{en } \mathbb{Z}/p\mathbb{Z}.$$

El caso $p = 2$ es trivial porque solo hay dos clases. Damos por hecho que $a \neq \overline{0}$ ya que la ecuación es de segundo grado. Multiplicando por $4a$ la ecuación equivale a $(2ax + b)^2 - \Delta$ con $\Delta = b^2 - 4ac$, el *discriminante*. Por (1.3) y el Corolario 1.3.5 el número de soluciones es

$$1 + \left(\frac{\Delta}{p}\right) = 1 + \left(\frac{\pm 1}{p}\right)\prod_{j=1}^{k}\left(\frac{q_j}{p}\right)^{\alpha_j} \qquad \text{si} \quad \Delta = \pm q_1^{\alpha_1}\cdots q_k^{\alpha_k},$$

con q_j los primos de la factorización de $\pm\Delta$. Cada símbolo se puede calcular dándole la vuelta con la ley de reciprocidad cuadrática o usando las leyes suplementarias (uno puede restringirse a α_j impar). Esto da lugar a condiciones de congruencia que se pueden resumir en otras respecto a un solo módulo por el teorema chino del resto.

Compárese la situación con el estudio de las ecuaciones de segundo grado en los reales. Allí, tras completar cuadrados, la existencia de dos soluciones reales era equivalente a que el discriminante Δ fuera positivo, para que se pudiera extraer su raíz cuadrada. La condición análoga en $\mathbb{Z}/p\mathbb{Z}$ para que Δ tenga "raíz cuadrada" es que sea un residuo cuadrático módulo p. Nuestro análisis se ha centrado en la existencia de soluciones y cabe preguntarse cómo se extraen estas raíces cuadradas en $\mathbb{Z}/p\mathbb{Z}$ cuando existen. Hay algoritmos eficientes con este propósito [6, §1.5], [40, §10.6]. Aquí solo mencionaremos un caso sencillo que es consecuencia inmediata del Criterio de Euler: si $p \equiv 3\ (4)$ se tiene que $x = \pm a^{(p+1)/4}$ resuelve $x^2 \equiv a\ (p)$ con a un residuo cuadrático.

La aplicación de la ley de reciprocidad cuadrática para decidir si cierta ecuación de segundo grado tiene solución módulo un primo dado puede resultar engorrosa por el requerimiento en su enunciado de que p y q sean primos, lo que fuerza a factorizar y a aplicar el Corolario 1.3.5, quizá varias veces. Una manera de aumentar la eficiencia del procedimiento es definir artificialmente una especie de símbolo de Legendre con módulo no primo. Concretamente, para $m > 2$ impar se define el *símbolo de Jacobi* como

$$\left(\frac{n}{m}\right) = \prod_{j=1}^{k} \left(\frac{n}{p_j}\right)^{\alpha_j}$$

con $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ la factorización en primos. Hay cosas importantes a tener en cuenta. La primera es que este símbolo no tiene nada que ver con la solubilidad de $x^2 - n \equiv 0\ (m)$ si m no es primo. Lo segundo, es que la condición $2 \nmid m$ no es caprichosa si se quieren respetar algunas propiedades básicas. La extensión a m par está relacionado con el llamado *símbolo de Kronecker*, más complicado [43, §9.3], que no introduciremos.

La gracia de este artificio teórico es que satisface una relación similar a la ley de reciprocidad cuadrática y las leyes suplementarias. Esto no es nada profundo, solo una consecuencia del caso m primo a traves de la factorización.

Proposición 1.3.8. *Si $n, m \in \mathbb{Z}_{>2}$ son impares y coprimos, se cumple*

$$\left(\frac{n}{m}\right)\left(\frac{m}{n}\right) = (-1)^{(n-1)(m-1)/4}.$$

Además

$$\left(\frac{-1}{m}\right) = (-1)^{(m-1)/2} \qquad y \qquad \left(\frac{2}{m}\right) = (-1)^{(m^2-1)/8}.$$

Demostración. Sustituyendo la definición y empleando la ley de reciprocidad cuadrática, todo se reduce a ver que los sumatorios en los exponentes de -1 que provienen de la factorización se pueden sustituir por los exponentes indicados $(n-1)(m-1)/4$, $(m-1)/2$ y $(m^2-1)/8$. Un poco de reflexión muestra que para ello basta probar que si $N = a_1 a_2 \cdots a_\ell$ con N impar, entonces

$$N-1 \equiv \sum_{j=1}^{\ell}(a_j-1) \ \ (4) \qquad \text{y} \qquad N^2-1 \equiv \sum_{j=1}^{\ell}(a_j^2-1) \ \ (16).$$

La primera congruencia se sigue de $N = \prod_j \big(1+2(a_j-1)/2\big)$, desarrollando el producto, y la segunda de $N^2 = \prod_j \big(1+8(a_j^2-1)/8\big)$, de la misma forma. □

Como ejemplo, comparemos el procedimiento para decidir si $x^2 \equiv 1569$ tiene solución módulo $p = 6353$ usando los símbolos de Legendre y los de Jacobi. Sea cual sea el procedimiento, nuestro objetivo es evaluar $(1569/6353)$.

Si aplicamos el Teorema 1.3.1 nos vemos obligados a factorizar $1569 = 3 \cdot 523$ (y quizá nos lleve un poco asegurarnos de que 523 es primo con cálculos a mano). Obtendríamos:

$$\Big(\frac{1569}{6353}\Big) = \Big(\frac{3}{6353}\Big)\Big(\frac{523}{6353}\Big) = \Big(\frac{2}{3}\Big)\Big(\frac{77}{523}\Big) = -\Big(\frac{77}{523}\Big).$$

De nuevo, 77 no es primo y no está cubierto por el Teorema 1.3.1, así que factorizamos de nuevo $77 \cdot 11$ y hacemos los cálculos por separado para 7 y 11. Teniendo en cuenta que $523 \equiv 5 \ (7)$, con dos aplicaciones de la ley de reciprocidad cuadrática,

$$\Big(\frac{7}{523}\Big) = -\Big(\frac{5}{7}\Big) = -\Big(\frac{2}{5}\Big) = 1.$$

Por otro lado, $523 \equiv 6 \ (11)$ y el cálculo para 11 requiere la factorización $6 = 2 \cdot 3$:

$$\Big(\frac{11}{523}\Big) = -\Big(\frac{6}{11}\Big) = -\Big(\frac{2}{11}\Big)\Big(\frac{3}{11}\Big) = -\Big(\frac{2}{11}\Big)(-1)\Big(\frac{2}{3}\Big) = 1.$$

En definitiva, hemos deducido $(1569/6353) = -1$ y la ecuación de partida no tiene solución.

Si procedemos con el símbolo de Jacobi, nos podemos ahorrar las factorizaciones. Como $6353 \equiv 77 \ (1569)$, obtenemos de la Proposición 1.3.8,

$$\Big(\frac{1569}{6353}\Big) = \Big(\frac{77}{1569}\Big).$$

Ahora usamos $1569 \equiv 29 \ (77)$ y después $77 \equiv 19 \ (29)$ y $29 \equiv -9 \ (19)$ para obtener

$$\Big(\frac{77}{1569}\Big) = \Big(\frac{29}{77}\Big) = \Big(\frac{19}{29}\Big) = \Big(\frac{-9}{19}\Big) = \Big(\frac{-1}{19}\Big) = -1$$

con la misma conclusión que antes. Escoger $29 \equiv -9\ (19)$ en vez de $29 \equiv 10\ (19)$ ha sido para no tener que separar el factor 2 de 10.

Más allá de este ejemplo, es fácil de entender que por medio del símbolo de Jacobi se podría programar un algoritmo para que un ordenador calcule (a/p) sin apelar a métodos de factorización, solo usando congruencias.

Sin entrar en detalles, con un procedimiento elemental [5, Th. 3.15], las soluciones módulo p se elevan a soluciones módulo p^α y utilizando la ley de reciprocidad cuadrática y el teorema chino del resto también podemos decidir la solubilidad de una ecuación cuadrática dada sobre $\mathbb{Z}/m\mathbb{Z}$ cuando m no es primo. Desde el punto de vista algebraico esto es un poco menos natural porque en estos anillos una ecuación de segundo grado puede tener más de dos soluciones. Un comentario al margen es que el procedimiento elemental para pasar de módulo p a p^α está íntimamente ligado a una construcción algebraica y analítica llamada los *números p-ádicos* [2], [33] que es crucial en la teoría de números contemporánea. En pocas palabras, cada número p-ádico integra clases de congruencia con respecto a todos los módulo p^k simultáneamente.

Teniendo en cuenta las conclusiones de esta sección, cabe preguntarse si hay un modo de caracterizar si un polinomio dado de grado $d > 2$ tiene d raíces en $\mathbb{Z}/p\mathbb{Z}$. Gauss y Eisenstein estudiaron los casos $x^d - a$ obteniendo algunos resultados difíciles de enunciar aquí [27, 38]. El caso de un polinomio general llega a los límites de la investigación contemporánea y tiene conexiones estrechas con la teoría de Galois [57].