ESTALMAT ANDALUCIA ORIENTAL

Ley de reciprocidad cuadrática

Veteranos (5/mayo/2018)

2017–2018

Ponentes:
Pascual Jara
Blas Torrecillas

Resumen

Ley de reciprocidad cuadráticas y aplicaciones a la aritmética de números enteros.

Introducción

¿Qué es la ley de reciprocidad cuadrática y para qué se utiliza?

1. Factorización de enteros

La factorización de enteros positivos es uno de los retos de la Matemática Moderna. Existe un método factorización, atribuido a Fermat, de números enteros positivos impares, los pares son fácilmente factorizables.

Primero observamos que si n es un entero positivo impar, sea $n = 2h + 1$, entonces $n = (h + 1)^2 - h^2$, esto es, n es siempre una diferencia de dos cuadrados perfectos; llamamos a esta diferencia una diferencia impropia. Por otro lado todo número entero positivo tiene una factorización impropia: la dada por $n = 1 \cdot n$. El resultado sobre factorización atribuido a Fermat establece que diferencias de cuadrados perfectos propias determinan factorizaciones propias y viceversa.

Proposición. 1.1.
Sea n un entero positivo impar. Son equivalentes:

(a) n tiene una factorización propia.
(b) n es una diferencia propia de dos cuadrados perfectos.

Demostración. (a) $\Rightarrow$ (b). Si n tiene una factorización propia, existen $a, b \in \mathbb{Z}$, $a > b > 1$ tales que $n = ab$, entonces

$$n = \left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2$$

Si $\frac{a+b}{2} = \frac{n+1}{2}$ y $\frac{a-b}{2} = \frac{n-1}{2}$, entonces $a = n$ y $b = 1$, lo que es una contradicción.

(b) $\Rightarrow$ (a). Si $n = x^2 - y^2$ es una diferencia propia de cuadrados, entonces $n = (x + y)(x - y)$, si esta factorización es trivial, se tiene $x - y = 1$, $x + y = n$, por lo que $2x = n + 1$, $2y = n - 1$, lo que es una contradicción.

La diferencia de cuadrados perfectos es propia si, y sólo si, la factorización es propia. □

Si $n = ab$ y $n = \left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2$, entonces $n + \left(\frac{a-b}{2}\right)^2 = \left(\frac{a+b}{2}\right)^2$. Se trata entonces de tomar diversos valores de k y calcular $n + k^2$. Cuando éste es un cuadrado perfecto (tomamos el mínimo de ellos), entonces tendremos n expresado como una diferencia de cuadrados, y por tanto una factorización (que puede ser impropia). Si se tiene $n + k^2 = h^2$, planteamos entonces el siguiente sistema,

$$\frac{a+b}{2} = h, \quad \frac{a-b}{2} = k.$$

para calcular a y b; se tiene

$$a = h + k, \quad b = h - k, \quad n = ab.$$

Alternativamente podemos tomar h el mínimo entre los que verifican $\sqrt{n} < h$, y considerar la sucesión $h^2 - n$ hasta encontrar un cuadrado perfecto. Observa que se tiene $h = \lfloor\sqrt{n}\rfloor, \lfloor\sqrt{n}\rfloor + 1, \lfloor\sqrt{n}\rfloor + 2, \ldots, n$. Ya que $a, b \leq n$, por tanto $\frac{a+b}{2} < n$. Si en ella aparece un cuadrado perfecto k^2, procedemos como en el caso precedente.

Ejemplo. 1.2.
Estudia si el número $n = 4\,080\,319$ es primo, y si no lo es, calcular una factorización propia.

Solución. Tenemos $\lfloor\sqrt{n}\rfloor = \lfloor\sqrt{4\,080\,319}\rfloor = 2019$. Construimos la sucesión $h^2 - n$, para $h \geq \lfloor\sqrt{n}\rfloor = 2019$. Para $h = 2020$ se tiene: $h^2 - n = 2020^2 - 4\,080\,319 = 81 = k^2$.

Tenemos entonces $k = 9$, y $h = 2020$. Es necesario resolver el sistema $\left.\begin{array}{l} a+b = 2h \\ a-b = 2m \end{array}\right\}$, esto es, $\left.\begin{array}{l} a+b = 4040 \\ a-b = 18 \end{array}\right\}$, cuya solución es: $a = 2029$ y $b = 2011$, y por tanto $4\,080\,319 = 2029 \times 2011$. □

2. Símbolo de Legendre

Sea p un entero primo positivo, para cada $a \in \mathbb{Z}$, primo relativo con p, se define el **símbolo de Legendre** $\left(\frac{a}{p}\right)$ como

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{si } a \text{ es un cuadrado módulo } p \\ -1 & \text{si } a \text{ no es un cuadrado módulo } p \end{cases}$$

Lema. 2.1.
Dado un entero primo positivo p y enteros a, b, primos relativos con p, se verifica:

(1) $\left(\frac{1}{p}\right) = 1$
(2) $\left(\frac{a^2}{p}\right) = 1$.
(3) Si $a \equiv b \pmod{p}$, *entonces* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

Lema. 2.2. (Pequeño teorema de Fermat)
Para cada entero primo positivo p y cada entero a, primo relativo con p, se verifica $a^{p-1} \equiv 1 \pmod{p}$.

Demostración. Para $p = 2$ el resultado es cierto. Supongamos que $p > 2$ y $a > 0$. Como $p \nmid a$, la aplicación $f : \{1, \ldots, p-1\} \longrightarrow \{1, \ldots, p-1\}$, definida $f(x) = y$ tal que $y \equiv ax \pmod{p}$ es una

biyección. Tenemos entonces $\prod_{i=1}^{p-1} i \equiv \prod_{i=1}^{p-1}(ia) \equiv a^{p-1}\prod_{i=1}^{p-1} i \pmod p$. Como $p \nmid \prod_{i=1}^{p-1} i$, se tiene $a^{p-1} \equiv 1 \pmod p$. □

Para cada entero positivo n definimos $\varphi(n)$ como el número de enteros $0 < k < n$ que son primos relativos con n, y la llamamos la **función totiente de Euler**.

Lema. 2.3.
La función totiente de Euler verifica las siguientes propiedades:

(1) Si n, m son enteros positivos primos relativos, se verifica $\varphi(nm) = \varphi(n)\varphi(m)$,
(2) Para cada entero primo positivo p y cada entero positivo n, se verifica

$$\varphi(p^n) = p^n - p^{n-1} = p^{n-1}(p-1) = p^n\left(1 - \frac{1}{p}\right).$$

(3) Para $p_1, \ldots, p_t$, enteros primos positivos y $n_1, \ldots, n_t$, enteros positivos, se verifica

$$\varphi(p_1^{n_1}\cdots p_t^{n_t}) = p_1^{n_1-1}\cdots p_t^{n_t-1}(p_1-1)\cdots(p_t-1) = p_1^{n-1}\cdots p_t^{n_t}\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_t}\right).$$

Lema. 2.4. (Teorema de Euler)
Para cada entero positivo n y cada entero a, primo relativo con n, se verifica $a^{\varphi(n)} \equiv 1 \pmod n$.

Demostración. La demostración puede ser similar al Pequeño teorema de Fermat. □

Lema. 2.5. (Lema de Wilson)
Para cada entero primo positivo p se verifica $(p-1)! \equiv -1 \pmod p$.

Demostración. Para el caso $p = 2, 3$ el resultado es cierto. Supongamos que $p > 3$. Si p es un entero primo positivo, para cada $0 < a \leq p$ existe un único $a' \in \{1, 2, \ldots, p-1\}$ tal que $aa' \equiv 1 \pmod p$. Agrupamos los elementos de $\{2, \ldots, p-2\}$ por parejas $\{a, a'\}$, tenemos $\prod_{i=2}^{p-2} i \equiv 1 \pmod p$, y por tanto $(p-1)! = \prod_{i=1}^{p-1} i \equiv -1 \pmod p$. □

Lema. 2.6. (Recíproco del Teorema de Wilson)
Para cada entero positivo $n \in \mathbb{Z}$, $n > 1$, si $(n-1)! \equiv -1 \pmod{n}$, entonces n es primo.

Demostración. Si n no es primo, existen $a, b \in \mathbb{Z}$, $a, b > 1$, tales que $n = ab$; como $a, b \,|\, (-1)!$, resulta que $n \,|\, (n-1)!$, por lo que, al reducir módulo n se tiene $0 \equiv -1 \pmod{n}$, lo que es una contradicción. □

Teorema. 2.7. (Criterio de Euler)
Si p es un entero primo positivo impar y a es primo relativo con p, se verifica:

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

Demostración. Si $\left(\frac{a}{p}\right) = 1$, existe $x \in \mathbb{F}_p^{\times}$ tal que $x^2 \equiv a \pmod{p}$, entonces $a^{\frac{p-1}{2}} \equiv (x^2)^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \pmod{p}$. Si $\left(\frac{a}{p}\right) = -1$ la ecuación $X^2 - a \equiv 0 \pmod{p}$ no tiene soluciones en $\mathbb{Z}$; para cada $b \in \{1, \ldots, p-1\}$ la ecuación $bX - a \equiv 0 \pmod{p}$ tiene una única solución en $\{1, \ldots, p-1\}$, llamémosla b'; por la hipótesis se tiene $b \neq b'$, podemos entonces agrupar los elementos de $\{1, \ldots, p-1\}$ en pares $\{b, b'\}$, de los que tenemos exactamente $\frac{p-1}{2}$, su producto es congruente con $a^{\frac{p-1}{2}}$, y por otro lado es congruente con $(p-1)!$ Por el Teorema de Wilson se tiene $(p-1)! \equiv -1 \pmod{p}$. □

Ver el Ejercicio (5.10.).

Corolario. 2.8.
Sea p un entero primo positivo, y a, b enteros primos relativos con p, se tiene $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$.

Demostración. El caso en el que p es par es trivial. Para el caso de p impar se tiene:

$$\left(\frac{ab}{p}\right) = (ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right).$$

□

Corolario. 2.9.
Si p es un entero primo positivo impar, se verifica $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$. Como consecuencia

- *-1 es un residuo cuadrático si $p \equiv 1 \pmod 4$, y*
- *-1 no es un residuo cuadrático si $p \equiv 3 \pmod 4$.*

Este resultado puede aplicarse a probar cuando un entero primo positivo es suma de dos cuadrados, y en general a determinar cuando un entero primo p divide a una expresión del tipo $x^2 + ny^2$, o equivalentemente, cuando $-n$ es un residuo cuadrático módulo p.

Teorema. 2.10. (Lema de Gauss)
Sea p un entero primo positivo impar y $a \in \mathbb{Z}$ primo relativo con p, si se considera el conjunto $\{ha \mid h = 1, \ldots, \frac{p-1}{2}\}$ se tiene:

(1) Al reducir módulo p tenemos $\frac{p-1}{2}$ elementos distintos.
(2) Sean $y_1, \ldots, y_s$ los restos estrictamente menores que $\frac{p-1}{2}$, y $x_1, \ldots, x_t$ los restos mayores o iguales que $\frac{p-1}{2}$, entonces $p - x_i \not\equiv y_j \pmod p$ para todos i, j.
(3) $\left(\frac{a}{p}\right) = (-1)^t$.

Demostración. (1). Si dos restos son iguales, existen $h, k \in \{1, \ldots, \frac{p-1}{2}\}$ tales que $ha \equiv ka \pmod p$, por tanto $p \mid h - k$, lo que es imposible.

(2). Si $p - x \equiv y$, existen $h, k \in \{1, \ldots, \frac{p-1}{2}\}$ tales que $p - ha \equiv ka \pmod p$, entonces $p \mid h - k$ lo que es imposible.

(3). Por el apartado (2) se tiene que $\{y_1, \ldots, y_s, p - x_1, \ldots, p - x_t\} = \{1, \ldots, \frac{p-1}{2}\}$, entonces tenemos las siguientes igualdades módulo p:

$$\left(\tfrac{p-1}{2}\right)! \equiv y_1 \cdots y_s (p - x_1) \cdots (p - x_t) \equiv (-1)^t y_1 \cdots y_s x_1 \cdots x_t \equiv (-1)^t a(2a) \cdots (\tfrac{p-1}{2}a) \equiv (-1)^t a^{\frac{p-1}{2}} \left(\tfrac{p-1}{2}\right)!$$

Podemos simplificar por $\left(\frac{p-1}{2}\right)!$ ya que no es congruente con 0. Como consecuencia $\left(\frac{a}{p}\right) \equiv a^{\frac{a}{p}} \equiv (-1)^t$. □

Para cada número racional positivo r llamamos $[r]$ a la **parte entera** de r.

Proposición. 2.11.
Con la notación de lema de Gauss se tiene

$$t \equiv \sum_{j=1}^{\frac{p-1}{2}} \left[\frac{ja}{p}\right] + (a-1)\frac{p^2-1}{8} \pmod 2.$$

Demostración. Tenemos las relaciones

$$\sum_{j=1}^{\frac{p-1}{2}} ja = \sum_{j=1}^{\frac{p-1}{2}} p\left[\frac{ja}{p}\right] + \sum_{i=1}^{s} y_i + \sum_{h=1}^{t} x_t.$$

$$\sum_{j=1}^{\frac{p-1}{2}} j = \frac{\left(1+\frac{p-1}{2}\right)\frac{p-1}{2}}{2} = \frac{p^2-1}{8}.$$

$$\sum_{j=1}^{\frac{p-1}{2}} j = \sum_{i=1}^{s} y_i + \sum_{h=1}^{t}(p-x_h) = tp - \sum_{h=1}^{t} x_h + \sum_{i=1}^{s} y_i.$$

Tenemos entonces módulo 2 tenemos:

$$\begin{aligned}
(a-1)\tfrac{p^2-1}{8} &= (a-1)\textstyle\sum_{j=1}^{\frac{p-1}{2}} j \\
&= a\textstyle\sum_{j=1}^{\frac{p-1}{2}} j - \sum_{j=1}^{\frac{p-1}{2}} j \\
&= \textstyle\sum_{j=1}^{\frac{p-1}{2}} p\left[\frac{ja}{p}\right] + \sum_{i=1}^{s} y_i + \sum_{h=1}^{t} x_t - (tp - \sum_{h=1}^{t} x_h + \sum_{i=1}^{s} y_i) \\
&\equiv \textstyle\sum_{j=1}^{\frac{p-1}{2}} p\left[\frac{ja}{p}\right] - tp \\
&\equiv \textstyle\sum_{j=1}^{\frac{p-1}{2}} \left[\frac{ja}{p}\right] - t
\end{aligned}$$

De aquí se deduce la congruencia del enunciado. □

Corolario. 2.12.
Sea p un entero primo positivo impar, se verifica $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

Demostración. En la proposición anterior si tomamos $a = 2$ tenemos $\sum_{j=1}^{\frac{p-1}{2}} \left[\frac{j2}{p}\right] = 0$; todos son mayores que 0 y menores que 1. □

3. Ley de reciprocidad cuadrática

Tenemos ahora el resultado fundamental de la teoría.

Teorema. 3.1. (Ley de reciprocidad cuadrática)
Sean ahora p, q primos impares, distintos, se verifica:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Demostración. Consideramos $\left(\frac{q}{p}\right)$; se tiene $\left(\frac{q}{p}\right) = (-1)^t$, en donde t verifica $t \equiv \sum_{j=1}^{\frac{p-1}{2}} \left[\frac{jq}{p}\right] + (q-1)\frac{p^2-1}{8} \pmod 2$; como q es un primo impar, resulta $t \equiv \sum_{j=1}^{\frac{p-1}{2}} \left[\frac{jq}{p}\right] = a \pmod 2$. Análogamente, en el caso de $\left(\frac{p}{q}\right)$ tenemos $\left(\frac{p}{q}\right) = (-1)^r$, siendo $r \equiv \sum_{j=1}^{\frac{q-1}{2}} \left[\frac{jp}{q}\right] = b \pmod 2$. Tenemos por tanto la relación

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^t(-1)^r = (-1)^{t+s} = (-1)^{a+b}.$$

Se trata ahora de ver que se verifica $a + b = \frac{p-1}{2}\frac{q-1}{2}$.

Consideramos, en una retícula semientera los puntos $O = (0,0)$, $A = (\frac{p}{2}, 0)$, $B = (\frac{p}{2}, \frac{q}{2})$ y $C = (0, \frac{q}{2})$, y llamamos $\mathcal{P}$ al conjunto de puntos de la retícula entera en el interior del rectángulo $OABC$. La diagonal de este rectángulo es $\overline{OB}$, y son los puntos (x, y), de coordenadas enteras, que verifican $yp = xq$; observamos que no hay puntos en la diagonal, $\mathcal{D}$, y en $\mathcal{P}$. En efecto, si $(x, y) \in \mathcal{D} \cap \mathcal{P}$, entonces $p \mid x$, lo que es imposible ya que $1 \leq x \leq \frac{p-1}{2}$.

Tenemos que en $\mathcal{P}$ hay exactamente $\frac{p-1}{2}\frac{q-1}{2}$ puntos. Vamos ahora a contar los puntos de $\mathcal{P}$ calculando los puntos que hay en cada uno de los triángulos OAB y OBC.

Para contar los puntos en OAB consideramos una recta vertical de ecuación $X = h$, el número de puntos en esta recta es $\left|\{y \in \mathbb{Z} \mid \ (h, y) \in \mathcal{P},\ 1 \leq y < \frac{qh}{p}\}\right| = \left[\frac{hq}{p}\right]$. Por tanto el número de puntos en OAB es

$$\left[\frac{q}{p}\right] + \left[\frac{2q}{p}\right] + \cdots + \left[\frac{(\frac{p-1}{2})q}{p}\right] = a.$$

De la misma forma se tiene

$$\left[\frac{p}{q}\right] + \left[\frac{2p}{q}\right] + \cdots + \left[\frac{(\frac{q-1}{2})p}{q}\right] = b.$$

Tenemos por tanto la relación $\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{a+b} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$. □

4. Símbolo de Jacobi

El símbolo de Jacobi es una extensión del símbolo de Legendre y se define para $a, b \in \mathbb{Z}$, primos relativos, con b impar y $b = p_1 \cdots p_t$ una factorización en primos, como sigue:

$$\left(\frac{a}{b}\right) = \prod_{i=1}^{t} \left(\frac{a}{p_i}\right),$$

y $\left(\frac{a}{1}\right) = 1$.

Lema. 4.1.
Para $a, b \in \mathbb{Z}$ impares se verifica:

(1) $\frac{ab-1}{2} \equiv \frac{a-1}{2} + \frac{b-1}{2} \pmod 2$.
(2) $\frac{(ab)^2-1}{8} \equiv \frac{a^2-1}{8} + \frac{b^2-1}{8} \pmod 2$.

Proposición. 4.2.
El símbolo de Jacobi verifica las siguientes propiedades:

(1) Coincide con el símbolo de Legendre si b es primo.
(2) Si $\left(\frac{a}{b}\right) = -1$, entonces a no es un residuo cuadrático módulo b. El recíproco no es necesariamente cierto.
(3) $\left(\frac{aa'}{bb'}\right) = \left(\frac{a}{b}\right) \cdot \left(\frac{a}{b'}\right) \cdot \left(\frac{a'}{b}\right) \cdot \left(\frac{a'}{b'}\right)$ *cuando aa' y bb' son primos relativos.*
(4) $\left(\frac{a^2}{b}\right) = \left(\frac{a}{b^2}\right) = 1$ *cuando a y b son primos relativos.*
(5) $\left(\frac{-1}{b}\right) = (-1)^{\frac{b-1}{2}} = \begin{cases} +1 \ \textit{si } b \equiv 1 \pmod 4 \\ -1 \ \textit{si } b \equiv 3 \pmod 4. \end{cases}$
(6) $\left(\frac{2}{b}\right) = (-1)^{\frac{b^2-1}{8}} = \begin{cases} +1 \ \textit{si } b \equiv \pm 1 \pmod 8 \\ -1 \ \textit{si } b \equiv \pm 3 \pmod 8. \end{cases}$
(7) Si a y b son enteros impares primos relativos, se verifica

$$\left(\frac{a}{b}\right) \cdot \left(\frac{b}{a}\right) = (-1)^{\frac{a-1}{2}\,\frac{b-1}{2}}.$$

Demostración. (5). Supongamos que $b = p_1 p_2$; tenemos

$$\left(\frac{-1}{b}\right) = \left(\frac{-1}{p_1}\right) \cdot \left(\frac{-1}{p_2}\right) = (-1)^{\frac{p_1-1}{2}} \cdot (-1)^{\frac{p_2-1}{2}} = (-1)^{\frac{p_1-1}{2}+\frac{p_2-1}{2}} = (-1)^{p_1 p_2 - 1} 2.$$

(6). Supongamos que $b = p_1 p_2$; tenemos:

$$\left(\frac{2}{b}\right) = \left(\frac{2}{p_1}\right) \cdot \left(\frac{2}{p_2}\right) = (-1)^{\frac{p_1^2-1}{8}} \cdot (-1)^{\frac{p_2^2-1}{8}} = (-1)^{\frac{p_1^2-1}{8}+\frac{p_2^2-1}{8}} = (-1)^{(p_1p_2)^2-1}8.$$

(7). Supongamos que $a = q_1 \cdots q_s$ y $b = p_1 \cdots p_t$; se tiene:

$$\left(\frac{a}{b}\right) \cdot \left(\frac{b}{a}\right) = \text{prof}_{i,j} \left(\frac{q_i}{p_j}\right) \cdot \left(\frac{p_j}{q_j}\right) = \prod_{i,j} (-1)^{\frac{q_i-1}{2}\,\frac{p_j-1}{2}} = (-1)^{\sum_{i,j} \frac{q_i-1}{2}\,\frac{p_j-1}{2}}.$$

Por otro lado se tiene

$$\sum_{i,j} \frac{q_i-1}{2}\,\frac{p_j-1}{2} = \sum_j \left(\sum_i \frac{q_i-1}{2} \right) \frac{p_j-1}{2} \equiv_2 \frac{q_1 \cdots q_s - 1}{2} \sum_j \frac{p_j-1}{2} \equiv_2 \frac{a-1}{2}\,\frac{b-1}{2}.$$

□

La importancia del símbolo de Jacobi, con respecto al símbolo de Legendre es la rapidez de cálculo que éste permite. Tenemos algunos resultados de interés que sólo vamos a enunciar.

Proposición. 4.3.
Sean a, b enteros impares primos relativos.

(1) Si $\omega = \pm 1$, se tiene:

$$\left(\frac{\omega a}{b}\right) \cdot \left(\frac{b}{a}\right) = (-1)^{\frac{\omega a-1}{2}\,\frac{b-1}{2}}.$$

(2) Si $\omega_1 = \pm 1$ y $\omega_2 = \pm 1$, se tiene:

$$\left(\frac{\omega_1 a}{b}\right) \cdot \left(\frac{\omega_2 b}{a}\right) = (-1)^{\frac{\omega_1 a-1}{2}\,\frac{\omega_2 b-1}{2}+\frac{\omega_1-1}{2}\,\frac{\omega_2-1}{2}}.$$

En particular, si $\omega = \pm 1$, se tiene $\left(\frac{\omega}{b}\right) = (-1)^{\frac{\omega-1}{2}\,\frac{b-1}{2}}$.

Vemos un método de calcular el símbolo de Jacobi mediante la división euclídea.

Teorema. 4.4. (Teorema de Eisenstein)
Sean a y b enteros impares, siendo b positivo. Se define:

$$\begin{aligned} a_1 &= a, \\ a_2 &= b, \\ a_1 &= q_1 a_2 + \omega_1 a_3, \\ &\cdots \\ a_n &= q_n a_{n+1} + \omega_n a_{n+2}, \end{aligned}$$

siendo

(1) $a_2 > a_3 > \cdots > a_{n+2} = 1$,
(2) los a_i *todos impares y* $\omega_i = \pm 1$.

Se definen

$$s_i = \begin{cases} 0 & si\ a_{i+1} \equiv 1 \pmod 4\ ó\ \omega_i a_{i+2} \equiv 1 \pmod 4, \\ 1 & si\ a_{i+1} \equiv 3 \pmod 4\ y\ \omega_i a_{i+2} \equiv 3 \pmod 4, \end{cases}$$
$$s = \sum_{i=1}^{n} s_i.$$

Entonces se tiene $\left(\frac{a}{b}\right) = (-1)^s$.

Demostración. Tenemos las relaciones:

$$\begin{aligned}
\left(\tfrac{a}{b}\right) = \left(\tfrac{a_1}{a_2}\right) = \left(\tfrac{\omega_1 a_3}{a_2}\right) &= (-1)^{\frac{\omega_1 a_3 - 1}{2}\,\frac{a_2-1}{2}} = (-1)^{s_1}\left(\tfrac{a_2}{a_3}\right), \\
\left(\tfrac{a_2}{a_3}\right) = \left(\tfrac{\omega_2 a_4}{a_3}\right) &= (-1)^{\frac{\omega_2 a_4 - 1}{2}\,\frac{a_3-1}{2}} = (-1)^{s_2}\left(\tfrac{a_3}{a_4}\right), \\
&\cdots \\
\left(\tfrac{a_n}{a_{n+1}}\right) = \left(\tfrac{\omega_n a_{n+2}}{a_{n+1}}\right) &= (-1)^{\frac{\omega_n a_{n+2} - 1}{2}\,\frac{a_{n+1}-1}{2}} = (-1)^{s_n}\left(\tfrac{a_{n+1}}{1}\right),
\end{aligned}$$

Por tanto $\left(\frac{a}{b}\right) = \prod i = 1^n (-1)^{s_i} = (-1)^s$. □

Observa que en general se tiene:

$$\left(\frac{a}{b}\right) = (-1)^{s_1 + \cdots + s_j}\left(\frac{a_{j+1}}{a_{j+2}}\right),$$

para $j = 1, \ldots, n$.

5. Ejercicios

Ejercicio. 5.1.
Prueba, usando residuos cuadráticos, que $\sqrt{2}$ *no es un número racional.*

Solución. Si podemos escribir $\sqrt{2} = \frac{a}{b}$, con $a, b \in \mathbb{Z}$, entonces $2b^2 = a2$, y tomando módulo 3, y ya que $\overline{a}, \overline{b} \neq 0$, resulta $\overline{2} = \overline{a^2}\ \overline{b^2} = \overline{a^2 b^2} = \overline{(ab)^2}$, por lo que 2 debería ser un residuo cuadrático módulo 3, lo cual no es cierto. □

Ejercicio. 5.2.
Utilizando la ley de reciprocidad cuadrática, determina $\left(\frac{13}{31}\right)$.

DEMOSTRACIÓN. $\left(\frac{13}{31}\right) = (-1)^{\frac{13-1}{2}\frac{31-1}{2}}\left(\frac{31}{13}\right) = \left(\frac{5}{13}\right) = (-1)^{\frac{5-1}{2}\frac{13-1}{2}}\left(\frac{13}{5}\right) = \left(\frac{3}{5}\right) = -1.$ □

Ejercicio. 5.3.
Estudiar la ecuación cuadrática $X^2 - nY^2 = p$, *donde* p *es un entero primo positivo y* n *es un entero.*

SOLUCIÓN. Tomando módulo p tenemos la relación $X^2 - nY^2 = 0$, por lo que la ecuación tiene solución, módulo p, si y sólo si, n es un residuo cuadrático módulo p.

Una vez obtenida una solución módulo p, el problema es determinar una solución entera de la ecuación original. □

El **Teorema de Dirichlet** asegura que en cada sucesión aritmética $a_n = a_0 + nr$, con término inicial $a_0 \in \mathbb{Z}$ y razón $r \in \mathbb{Z}$, si a_0 y r son primos relativos, entonces existen infinitos valores de n tales que a_n es un entero primo.

Veamos cómo la ley de reciprocidad cuadrática permite probar casos particulares del Teorema de Dirichlet.

Ejercicio. 5.4.
Sea $f(X) \in \mathbb{Z}[X]$ *un polinomio no constante y* $P_f = \{p \in \mathbb{Z} \mid \ p \text{ es primo y } p \mid f(n) \text{ para algún } n \in \mathbb{Z}\}$, *entonces* P_f *es un conjunto infinito.*

SOLUCIÓN. Supongamos que $P_f = \{p_1, \ldots, p_t\}$. Si $f(0) \neq 0$, consideramos $\frac{f(f(0)p_1 \cdots p_t)}{f(0)}$. Tenemos

$$\frac{f(f(0)p_1 \cdots p_t)}{f(0)} = \frac{\sum_{i=1}^{n} c_i (f(0)p_1 \cdots p_t) + f(0)}{f(0)} = p_1 \cdots p_t k + 1,$$

que es primo relativo con $p_1, \ldots, p_t$, y por tanto $P_f \neq \{p_1, \ldots, p_t\}$. □

Ejercicio. 5.5.
Existen infinitos números primos.

SOLUCIÓN. Basta considerar el polinomio $f(X) = X + 1$. □

Ejercicio. 5.6.
Para cada $n \leq 2$ existen infinitos números primos p verificando $p \equiv 1 \pmod{n}$.

SOLUCIÓN. Si $n = 2$ el resultado es cierto. Si $n \leq 3$, consideramos el polinomio ciclotómico $\varphi_n(X)$ y el polinomio $g(X) = (X-1)(X^2-1)\cdots(X^{n-1}-1)$. Tenemos que $\varphi_n(X)$ y $g(X)$ son primos relativos, ya que no tienen raíces comunes en ninguna extensión de $\mathbb{Q}$. Existen polinomios $a(X), b(X) \in \mathbb{Q}[X]$ tales que $1 = a(X)\varphi_n(X) + b(x)g(X)$. Si d es el mínimo común múltiplo de los denominadores de $a(X)$ y $b(X)$, entonces $d = da(X)\varphi_n(X) + db(X)g(X)$. Como P_{φ_n} es infinito, existe $p \in P_{\varphi_n}$ tal que $p > d$, y existe $x \in \mathbb{Z}$ tal que $p \,|\, \varphi_n(x)$, por lo tanto $x^n \equiv 1 \pmod{p}$. Tenemos que $x^k \neq 1$ si $k < n$, ya que en caso contrario se tendría $g(x) = 0$, y por tanto $d = da(x)\varphi_n(x) + db(x)g(x) = 0$, lo que es una contradicción. Como consecuencia x tiene orden n en $\mathbb{Z}_p^\times$, esto es, $n \,|\, p-1$, y por tanto $p \equiv 1 \pmod{n}$ □

Ejercicio. 5.7.
Existen infinitos números primos p verificando $p \equiv 3 \pmod{8}$.

SOLUCIÓN. Se considera el polinomio $f(X) = X^2 + 2$. Si $p \,|\, f(n)$, entonces -2 es un residuo cuadrático módulo p, luego $\left(\frac{-2}{p}\right) = 1$. Tenemos $1 = \left(\frac{-2}{p}\right) = \left(\frac{-1}{0}\right)\cdot\left(\frac{2}{p}\right) = (-1)^{\frac{p-1}{2}}\cdot(-1)^{\frac{p^2-1}{8}} = (-1)^{\frac{(p-1)(p+5)}{8}}$. Esto significa que $p \equiv 1 \pmod{8}$ ó $p \equiv 3 \pmod{8}$.

Veamos que hay infinitos números primos de éstos que no son congruentes con 1 módulo 8. Supongamos que hay un número finito (todos son impares) Entonces $f(2p_1\cdots p_t) \equiv 6 \pmod{8}$. Como consecuencia hay infinitos números primos p verificando $\left(\frac{-2}{p}\right) = 1$ y $p \not\equiv 1 \pmod{8}$, y por tanto hay infinitos números primos p verificando $p \equiv 3 \pmod{8}$. □

Existen infinitos números primos p verificando $p \equiv 4 \pmod{5}$.

SOLUCIÓN. Se considera el polinomio $f(X) = X^2 - 5$. Si $p \,|\, f(n)$, entonces $\left(\frac{5}{p}\right) = 1$. Tenemos $1 = \left(\frac{5}{p}\right) = (-1)^{\frac{p-1}{2}\,\frac{5-1}{2}}\left(\frac{p}{5}\right) = \left(\frac{p}{5}\right)$, de aquí se tiene $\left(\frac{p}{5}\right) = p^{\frac{5-1}{2}} = p^2 \equiv 1 \pmod{5}$. Por tanto $p \equiv \pm 1 \pmod{5}$

Si sólo hay un número finito de estos números primos no congruentes con 1 módulo 5, y distintos de 5, sean éstos $p_1, \ldots, p_t$. Se verifica

$$f(p_1\cdots p_t) = (p_1\cdots p_t)^2 - 5 \quad \text{y} \quad f(2p_1\cdots p_t) = 4(p_1\cdots p_t)^2 - 5.$$

Si ambos con congruentes con 1 módulo 5, se tiene $(p_1 \cdots p_t)^2 \equiv 1 \equiv 4(p_1 \cdots p_t)^2 \equiv -(p_1 \cdots p_t)^2 \pmod 5$, lo que es imposible, luego $f(p_1 \cdots p_t) \not\equiv 1 \pmod 5$ ó $f(2p_1 \cdots p_t) \not\equiv 1 \pmod 5$, y por tanto hay infinitos números primos p verificando $p \equiv -1 \equiv 4 \pmod 5$. □

Ejercicio. 5.8.
Determina el valor de $\left(\frac{3}{p}\right)$, *para cada entero primo positivo* p.

Solución. Podemos suponer que $p > 3$, los otros casos son triviales. Tenemos $\left(\frac{3}{p}\right) = (-1)^{\frac{3-1}{2}\frac{p-1}{2}}\left(\frac{p}{3}\right) = (-1)^{\frac{p-1}{2}}\, p^{\frac{3-1}{2}}$. Como consecuencia tenemos

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & \begin{cases} p \equiv_4 1 \text{ y } p \equiv_3 1. \\ p \equiv_4 3 \text{ y } p \equiv_3 2. \end{cases} \\ -1 & \begin{cases} p \equiv_4 1 \text{ y } p \equiv_3 2. \\ p \equiv_4 3 \text{ y } p \equiv_3 1. \end{cases} \end{cases}$$

Por el Teorema Chino del Resto tenemos:

$$\begin{gathered} p \equiv_4 1 \text{ y } p \equiv_3 1 \Leftrightarrow p \equiv_{12} 1 \\ p \equiv_4 1 \text{ y } p \equiv_3 2 \Leftrightarrow p \equiv_{12} 5 \\ p \equiv_4 3 \text{ y } p \equiv_3 1 \Leftrightarrow p \equiv_{12} 7 \\ p \equiv_4 3 \text{ y } p \equiv_3 2 \Leftrightarrow p \equiv_{12} 11 \end{gathered}$$

Por lo tanto

$$\left(\frac{3}{p}\right) = \begin{cases} 1 \text{ si } p \equiv \pm 1 \pmod{12}. \\ -1 \text{ si } p \equiv \pm 5 \pmod{12}. \end{cases}$$

□

Ejercicio. 5.9.
Existen infinitos números primos p *verificando* $p \equiv 11 \pmod{12}$.

Solución. Se considera el polinomio $f(X) = 3X^2 - 1$, por tanto para cada $p \in P_f$ existe $x \in \mathbb{Z}$ tal que $3x^2 \equiv 1 \pmod p$, y por tanto $3^2x^2 \equiv 3 \pmod p$, esto es, 3 es un residuo cuadrático módulo p. Como consecuencia $1 = \left(\frac{3}{p}\right)$, y se tiene $p \equiv \pm 1 \pmod{12}$.

Vamos a ver que hay infinitos números primos verificando esta condición y $p \not\equiv 3 \pmod 4$. Si sólo hay un número finito $p_1, \ldots, p_t$, entonces se tiene $f(2p_1 \cdots p_t) \equiv 3 \pmod 4$ y es primo relativo con los $p_1, \ldots, p_t$, por tanto hay infinitos números primos p verificando $\left(\frac{3}{p}\right) = 1$ y $p \equiv 3 \pmod 4$, por tanto $p \equiv 2 \pmod 3$, esto es, $\left(\frac{p}{3}\right) = -1$. Luego existen infinitos números primos p verificando $p \equiv 11 \pmod{12}$. □

Ejercicio. 5.10. (Criterio de Euler)
Demostrar que para todo $m \in \mathbb{Z}$, verificando $m \not\equiv 0 \pmod{p}$, son equivalentes:

(a) La congruencia $X^2 \equiv m \pmod{p}$ tiene solución.
(b) $m^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.

Ref.: 5141e_084

Solución.

Traducido a $\mathbb{F}_p$ tenemos que probar la equivalencia de los siguientes enunciados para $m \neq 0$:

(a) m es un cuadrado en $\mathbb{F}_p$, esto es, el polinomio $X^2 - m$ tiene una raíz en $\mathbb{F}_p$.
(b) $m^{\frac{p-1}{2}} = 1$, esto es, m es una raíz $\frac{p-1}{2}$ de la unidad.

(a) $\Rightarrow$ (b). Supongamos que existe $x \in \mathbb{F}_p$ tal que $x^2 = m$, entonces

$$m^{\frac{p-1}{2}} = (x^2)^{\frac{p-1}{2}} = x^{p-1} = 1.$$

(b) $\Rightarrow$ (a). Consideramos un generador g del grupo $\mathbb{F}_p^\times$, entonces $m = g^j$, para $j \in \{0, \ldots, p-1\}$, entonces $1 = m^{\frac{p-1}{2}} = g^{\frac{j(p-1)}{2}}$, y por tanto $p-1$ divide a $\frac{i(p-1)}{2}$, esto es, j deber ser par, y tenemos $m = (g^{\frac{j}{2}})^2$. □

Pascual Jara. Departamento de Álgebra. Universidad de Granada
Blas Torrecillas. Departamento de Matemáticas. Universidad de Almería
.