Leyes suplementarias de reciprocidad cuadrática

Alexey Beshenov (cadadr@gmail.com)

14 de octubre de 2018

En esta breve nota voy a revisar pruebas de las leyes suplementarias de reciprocidad cuadrática. En Álgebra I hemos visto que el grupo $\mathbb{F}_p^\times$ (los restos no nulos módulo p respecto a la multiplicación) es cíclico (véase el capítulo 7). Esto significa que existe un generador $g \in \mathbb{F}_p^\times$ tal que

$$\mathbb{F}_p^\times = \{1, g, g^2, g^3, ..., g^{p-1}\}.$$

Para un número entero a tal que $p \nmid a$ definamos el **símbolo de Legendre** mediante

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

He aquí el resultado clave.

Lema (Criterio Euler)**.** *Para $p \neq 2$ y a tal que $p \nmid a$ se tiene*

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

Demostración. Tenemos $[a]_p = g^i$ para algún i, y esto es un cuadrado en $\mathbb{F}_p^\times$ si y solamente si i es un número par. Luego,

$$[a]_p^{\frac{p-1}{2}} = g^{i\frac{p-1}{2}}.$$

Si i es par, entonces $i\frac{p-1}{2}$ es divisible por $p-1 = \#\mathbb{F}_p^\times$, así que

$$g^{i\frac{p-1}{2}} = 1$$

(gracias al teorema de Lagrange: si $|G| \mid k$, entonces $g^k = 1$ para cualquier $g \in G$). Si i es impar, entonces $i\frac{p-1}{2}$ no es divisible por $p-1$ y por ende

$$g^{i\frac{p-1}{2}} \neq 1.$$

Sin embargo,

$$\left(g^{i\frac{p-1}{2}}\right)^2 = g^{i(p-1)} = 1,$$

lo que nos permite concluir que

$$g^{i\frac{p-1}{2}} = -1.$$

■

Corolario (Primera ley suplementaria)**.** *Para $p \neq 2$ se cumple*

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} +1, & p \equiv 1 \pmod{4}, \\ -1, & p \equiv 3 \pmod{4}. \end{cases}$$

Demostración. Basta sustituir $a = -1$ en el criterio de Euler. ■

Corolario (Segunda ley suplementaria)**.** *Para $p \neq 2$ se cumple*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} +1, & p \equiv 1,7 \pmod 8, \\ -1, & p \equiv 3,5 \pmod 8. \end{cases}$$

(Nota que $7 \equiv -1$ y $5 \equiv -3 \pmod 8$, así que los dos casos son $p \equiv \pm 1$ y $p \equiv \pm 3 \pmod 8$.)

Demostración. De nuevo, se puede aplicar el criterio de Euler

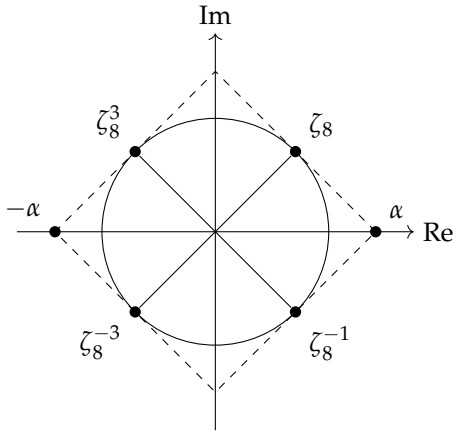
$$\left(\frac{2}{p}\right) \equiv 2^{\frac{p-1}{2}} \pmod p,$$

y hay que solo identificar el número a la derecha. Hay argumentos elementales, pero me gustaría presentar un cálculo con las raíces octavas de la unidad. Consideremos

$$\zeta_8 := e^{2\pi\sqrt{-1}/8}$$

y el número

$$\alpha := \zeta_8 + \zeta_8^{-1}.$$



Notamos que en el anillo $\mathbb{Z}[\zeta_8]$ se cumple

$$\alpha^p = (\zeta_8 + \zeta_8^{-1})^p \equiv \zeta_8^p + \zeta_8^{-p} \equiv \begin{cases} \zeta_8 + \zeta_8^{-1} = +\alpha, & p \equiv \pm 1 \pmod 8, \\ \zeta_8^3 + \zeta_8^{-3} = -\alpha, & p \equiv \pm 3 \pmod 8. \end{cases} \pmod p$$

(usando la identidad $(x+y)^p \equiv x^p + y^p \pmod p$). Puesto que $\alpha = \sqrt{2}$, calculamos

$$2^{\frac{p-1}{2}} = \alpha^{p-1} = \alpha^p\, \alpha^{-1} \equiv (\zeta_8 + \zeta_8^{-1})^p\, \alpha^{-1} \equiv \begin{cases} +1, & p \equiv \pm 1 \pmod 8, \\ -1, & p \equiv \pm 3 \pmod 8. \end{cases} \pmod p.$$

■