UVG UNIVERSIDAD DEL VALLE DE GUATEMALA

Lema de Gauss

Alan Reyes-Figueroa

Teoría de Números

(Aula 19) 05.septiembre.2023

Lema (Gauss)

Sea $p > 2$ un primo impar, y $a \in \mathbb{Z}^+$ un entero positivo, primo relativo con p. Sea s el número de elementos del conjunto

$$S = \{a, 2a, 3a, \ldots, \tfrac{p-1}{2}\, a\},$$

tales que su residuo módulo p es mayor que $\frac{p-1}{2}$. Entonces,

$$\left(\frac{a}{p}\right) = (-1)^s.$$

Prueba: Imitamos la prueba del Teorema de Euler-Fermat. Como $\{\pm 1, \pm 2, , \pm\frac{p-1}{2}\}$ es un sistema completo de invertibles módulo p, para cada $j = 1, 2, \ldots, \frac{p-1}{2}$ podemos escribir $ja \equiv \varepsilon_j m_j \pmod{p}$, con $\varepsilon_j \in \{-1, 1\}$, y $m_j \in \{1, 2, \ldots, \frac{p-1}{2}\}$.
Observe que si $i \neq j$, entonces $m_i \neq m_j$, donde $\{m_1, m_2, \ldots, m_{(p-1)/2}\} = \{1, 2, \ldots, \frac{p-1}{2}\}$. De hecho, si $m_i \equiv m_j \pmod{p}$, tendríamos $ia \equiv ja \pmod{p}$ ó $ia \equiv -ja \pmod{p}$; y como a es

Lema de Gauss

invertible módulo p y $0 \leq i, j \leq \frac{p-1}{2}$, entonces el primer caso implica $i = j$, mientras que el segundo caso es imposible.

Multiplicando las congruencias $ja \equiv \varepsilon_j m_j \pmod{m}$, resulta

$$\begin{aligned} (a)(2a)(3a)\cdots\left(\tfrac{p-1}{2}\,a\right) &\equiv \varepsilon_1\varepsilon_2\cdots\varepsilon_{(p-1)/2}\, m_1 m_2 \cdots m_{(p-1)/2} \pmod{p} \\ \iff \quad a^{(p-1)/2}\left(\frac{p-1}{2}\right)! &\equiv \varepsilon_1\varepsilon_2\cdots\varepsilon_{(p-1)/2}\left(\frac{p-1}{2}\right)! \pmod{p} \\ \iff \quad a^{(p-1)/2} &\equiv \varepsilon_1\varepsilon_2\cdots\varepsilon_{(p-1)/2} \pmod{p}. \end{aligned}$$

Luego, $a^{(p-1)/2} = \varepsilon_1\varepsilon_2\cdots\varepsilon_{(p-1)/2}$, ya que ambos términos son iguales a ± 1.

De ahí concluímos que $a^{(p-1)/2} = (-1)^s$, donde s es exactamente el número de términos $j \in \{1, 2, \ldots, p-12\}$ tales que $\varepsilon_j = -1$.
Este número es precisamente la cardinalidad $|S|$. $\square$

Ley de Reciprocidad Cuadrática

El Criterio de Euler ya produce un mecanismo para identificar residuos cuadráticos. Vamos a mostrar ahora un resultado más general.

Teorema (Ley de Reciprocidad Cuadrática)

1. *Sea p un primo impar. Entonces*

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

2. *Sean p, q primos impares distintos. Entonces*

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

Prueba: (1) La propiedad es consecuencia del Lema de Gauss. Si $p \equiv 1 \pmod 4$, entonces $p = 4k+1$ y $\frac{p-1}{2} = 2k$. Como $1 \leq 2j \leq \frac{p-1}{2}$ para $j \leq k$ y $\frac{p-1}{2} < 2j \leq p-1$ para $k+1 \leq j \leq 2k$,

Ley de Reciprocidad Cuadrática

hay exactamente k elementos en el conjunto $S = \{1 \leq j \leq 2k : \ 2j > \frac{p-1}{2}\}$. Pero $p = 4k+1 \ \Rightarrow p$ es de la forma $p = 8q+1$ ó $p = 8q+5$. En el primer caso, $k = \frac{p-1}{4} = \frac{8q}{4} = 2q$, mientras que en el segundo caso, $k = \frac{p-1}{4} = \frac{8q+4}{4} = 2q+1$.
Así,

$$\left(\frac{2}{p}\right) = (-1)^k = \begin{cases} (-1)^{2q} \\ (-1)^{2q+1} \end{cases} = \begin{cases} 1, & \text{si } p \equiv 1 \pmod 8; \\ -1, & \text{si } p \equiv 5 \pmod 8. \end{cases}$$

Si $p \equiv 3 \pmod 4$, entonces $p = 4k+3$ y $\frac{p-1}{2} = 2k+1$. Para $1 \leq j \leq k$, tenemos $j \leq 2j \leq \frac{p-1}{2}$ y para $k+1 \leq j \leq 2k+1$, tenemos $\frac{p-1}{2} \leq 2j \leq p-1$.
Ahora, hay exactamente $k+1$ elementos en el conjunto $S = \{1 \leq j \leq 2k+1 : \ 2j > \frac{p-1}{2}\}$.
Como $p = 4k+3 \ \Rightarrow p$ es de la forma $p = 8q+3$ ó $p = 8q+7$. En el primer caso, $k = \frac{p-3}{4} = \frac{8q}{4} = 2q$, mientras que en el segundo caso, $k = \frac{p-3}{4} = \frac{8q+4}{4} = 2q+1$.
De ahí,

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