UNIVERSIDAD DEL VALLE DE GUATEMALA

Solución de Congruencias Cuadráticas

Alan Reyes-Figueroa

Teoría de Números (Aula 16) 20.septiembre.2022

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*

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

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 $k+1 \leq j \leq 2k$,

hay exactamente k elementos en el conjunto $S = \{1 \le j \le 2k : \ 2j > \frac{p-1}{2}\}$. 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 $1 \le j \le k$, tenemos $j \le 2j \le \frac{p-1}{2}$ y para $k+1 \le j \le 2k+1$, tenemos $\frac{p-1}{2} \le 2j \le p-1$.
Ahora, hay exactamente $k+1$ elementos en el conjunto $S = \{1 \le j \le 2k+1 : \ 2j > \frac{p-1}{2}\}$.
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,

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

(2) Para la segunda parte, vamos a mostrar que

Ley de Reciprocidad Cuadrática

$$\frac{p-1}{2}\cdot\frac{q-1}{2} = \sum_{1\leq i\leq \frac{q-1}{2}} \left\lfloor \frac{ip}{q} \right\rfloor + \sum_{1\leq i\leq \frac{p-1}{2}} \left\lfloor \frac{iq}{p} \right\rfloor. \tag{1}$$

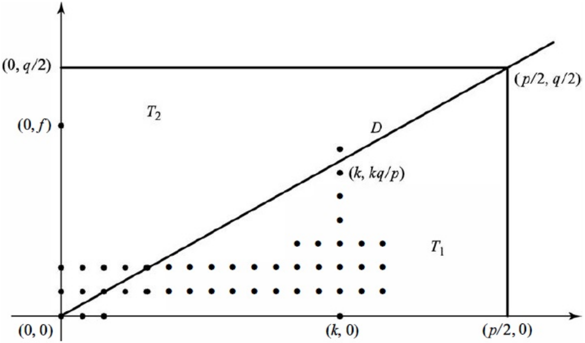
y que

$$\left(\frac{p}{q}\right) = (-1)^{\sum_{1\leq i\leq \frac{q-1}{2}} \left\lfloor \frac{ip}{q} \right\rfloor}, \qquad \text{y} \qquad \left(\frac{q}{p}\right) = (-1)^{\sum_{1\leq i\leq \frac{p-1}{2}} \left\lfloor \frac{iq}{p} \right\rfloor}. \tag{2}$$

La fórmula (1) es apenas un conteo: el lado izquierdo es el número de puntos con coorenadas enteras, en el interior del rectángulo con vértices $(0,0)$, $(\frac{p}{2},0)$, $(0,\frac{q}{2})$ y $(\frac{p}{2},\frac{q}{2})$. Por otro lado, la primer suma del lado derecho cuenta el número de tales puntos que están arriba de la diagonal $y=\frac{p}{q}x$ en dicho rectángulo, mientras que la segunda suma cuenta el número de puntos abajo de esta diagonal.

(Como p y q son primos distintos, no hay puntos con coordenadas enteras sobre la diagonal). Por ejemplo, en la primera suma, la cantidad $\left\lfloor \frac{ip}{q} \right\rfloor$ representa la cantidad de puntos sobre la recta $y=i$, arriba de la diagonal $y=\frac{p}{q}x$.

Ley de Reciprocidad Cuadrática



Conteo de puntos enteros en la Ley de Reciprocidad Cuadrática.

El número de puntos enteros en el intervalo $0 < x < \frac{iq}{p}$ es $\lfloor \frac{iq}{p} \rfloor$. Así, hay $\lfloor \frac{iq}{p} \rfloor$ puntos sobre $y = i$, arriba de la diagonal (en la región T_2. La otra cuenta es similar.

Ley de Reciprocidad Cuadrática

Finalmente, para mostrar (2), basta verificar que $\sum_{1\leq i\leq \frac{p-1}{2}} \left\lfloor \frac{iq}{p} \right\rfloor \equiv s \pmod 2$, donde s es como en el lema de Gauss, aplicado para $a = q$.
Sea r_i el residuo de la división de iq entre p, de modo que $iq = \left\lfloor \frac{iq}{p} \right\rfloor p + r_i$. Sumando y usando la notación en el Lema de Gauss, obtenemos

$$q \sum_{1\leq i\leq \frac{p-1}{2}} i = p \sum_{1\leq i\leq \frac{p-1}{2}} \left\lfloor \frac{iq}{p} \right\rfloor + \sum_{r_i<p/2} m_i + \sum_{r_i>p/2} (p - m_i).$$

Como p y q son impares, módulo 2 tenemos

$$\sum_{1\leq i\leq \frac{p-1}{2}} i \equiv \sum_{1\leq i\leq \frac{p-1}{2}} \left\lfloor \frac{iq}{p} \right\rfloor + \sum_{r_i<p/2} m_i + \sum_{r_i>p/2} (1 - m_i) \pmod 2,$$

y como $\{m_1, m_2, \ldots, m_{\frac{p-1}{2}}\} = \{1, 2, \ldots, \frac{p-1}{2}\}$, se concluye que

$$\sum_{1\leq i\leq \frac{p-1}{2}} i \equiv \sum_{1\leq i\leq \frac{p-1}{2}} \left\lfloor \frac{iq}{p} \right\rfloor + \sum_{1\leq i\leq \frac{p-1}{2}} i + \sum_{r_i>p/2} 1 \pmod 2 \iff \sum_{1\leq i\leq \frac{p-1}{2}} \left\lfloor \frac{iq}{p} \right\rfloor \equiv s \pmod 2. \square$$

Corolario

Si p y q son primos impares distintos, entonces

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \begin{cases} 1, & \text{si } p \equiv 1 \pmod 4, \text{ó } q \equiv 1 \pmod 4; \\ -1, & \text{si } p \equiv q \equiv 3 \pmod 4. \end{cases}$$

<u>Prueba</u>: Basta ver que si $p = 4k + 1$, el exponente $\frac{p-1}{2} = 2k$ es par. Similarmente para el caso $q = 4k + 1$. Por el contrario, si $p = 4k + 3$ y $q = 4j + 3$, ambos exponentes son impares. $\square$

Corolario

Si p y q son primos impares distintos, entonces

$$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right), & \text{si } p \equiv 1 \pmod 4, \text{ó } q \equiv 1 \pmod 4; \\ -\left(\frac{q}{p}\right), & \text{si } p \equiv q \equiv 3 \pmod 4. \end{cases}$$

Ejemplo: Calcular $\left(\frac{29}{53}\right)$.

De la Ley de Reciprocidad Cuadrática, tenemos -0.1cm

$$\begin{aligned}
\left(\frac{29}{53}\right) &= \left(\frac{53}{29}\right)(-1)^{\frac{29-1}{2}\cdot\frac{53-1}{2}} = \left(\frac{53}{29}\right)(-1)^{14\cdot 26} = \left(\frac{53}{29}\right) \\
&= \left(\frac{24}{29}\right) = \left(\frac{2^3\cdot 3}{29}\right) = \left(\frac{2}{29}\right)^3\left(\frac{3}{29}\right) = \underbrace{\left(\frac{2}{29}\right)^2}_{=1}\left(\frac{2}{29}\right)\left(\frac{3}{29}\right) \\
&= \left(\frac{2}{29}\right)\left(\frac{3}{29}\right) = \left(\frac{2}{29}\right)\left(\frac{29}{3}\right)(-1)^{\frac{3-1}{2}\cdot\frac{29-1}{2}} = \left(\frac{2}{29}\right)\left(\frac{29}{3}\right)(-1)^{1\cdot 14} \\
&= \left(\frac{2}{29}\right)\left(\frac{29}{3}\right) = \left(\frac{2}{29}\right)\left(\frac{2}{3}\right) = (-1)^{\frac{29^2-1}{8}}(-1)^{\frac{3^2-1}{2}} \\
&= (-1)^{105}(-1)^{1} = (-1)^{106} = 1.
\end{aligned}$$

Esto muestra que 29 es residuo cuadrático módulo 53.

Ejemplo: Determinar si 90 es residuo cuadrático módulo 1019.

Como $90 = 2 \cdot 3^2 \cdot 5$, tenemos que

$$
\begin{aligned}
\left(\frac{90}{1019}\right) &= \left(\frac{2 \cdot 3^2 \cdot 5}{1019}\right) = \left(\frac{2}{1019}\right) \underbrace{\left(\frac{3^2}{1019}\right)}_{=1} \left(\frac{5}{1019}\right) \\
&= \left(\frac{2}{1019}\right)\left(\frac{5}{1019}\right) = \left(\frac{2}{1019}\right)\left(\frac{1019}{5}\right)(-1)^{\frac{5-1}{2}\cdot\frac{1019-1}{2}} \\
&= \left(\frac{2}{1019}\right)\left(\frac{1019}{5}\right)(-1)^{2\cdot 509} = \left(\frac{2}{1019}\right)\left(\frac{1019}{5}\right) = \left(\frac{2}{1019}\right)\left(\frac{4}{5}\right) \\
&= \left(\frac{2}{1019}\right)\underbrace{\left(\frac{2^2}{5}\right)}_{=1} = \left(\frac{2}{1019}\right) = (-1)^{\frac{1019^2-1}{8}} = (-1)^{129{,}795} \\
&= -1.
\end{aligned}
$$

Esto muestra que 90 no es residuo cuadrático módulo 1019.

Ley de Reciprocidad Cuadrática

Ejemplo: Resolver la ecuación $x^2 + x \equiv 0 \pmod{13}$.

Ejemplo: Resolver la ecuación $x^2 - 3x + 2 \equiv 8 \pmod{17}$.

Ejemplo: Resolver la ecuación $x^2 \equiv 196 \pmod{1357}$.

Ejemplo: Resolver la ecuación $x^2 + x + 7 \equiv 0 \pmod{189}$.
Hay 6 soluciones. ¿Cómo encontrarlas?