Ley de Reciprocidad Cuadrática

Alan Reyes-Figueroa

Teoría de Números (Aula 14) 31.agosto.2021

Congruencias de grado 2

Sea $p > 2$ un primo impar, y sean $a, b, c \in \mathbb{Z}$, con $p \nmid a$. Estamos interesados en resolver la ecuación cuadrática

$$ax^2 + bx + c \equiv 0 \pmod{p}. \tag{1}$$

Completando al cuadrado (esto es, multiplicando por $4a$, y luego sumando b^2), la ecuación anterior es equivalente a

$$(2ax + b)^2 \equiv b^2 - 4ac \pmod{p}. \tag{2}$$

(Observe que 2 y a no son divisíbles por p).

Así, estamos interesados en encontrar criterios para la existencia de soluciones de la ecuación

$$x^2 \equiv d \pmod{p}. \tag{3}$$

Definición

Si la ecuación (3) tiene solución, esto es, $\bar{d}$ es un cuadrado perfecto en $\mathbb{Z}/p\mathbb{Z}$, diremos que d es un ***residuo cuadrático*** *módulo p.*

Congruencias

Hay exactamente $\frac{p+1}{2}$ residuos cuadráticos módulo p, $p > 2$. A saber:

$$0^2, (\pm 1)^2, (\pm 2)^2, (\pm 3)^2, \ldots, \Big(\pm \frac{p-1}{2}\Big)^2 \pmod{p},$$

ya que $i^2 \equiv (-i)^2 \pmod{p}$. Observe que todos estos números son incongruentes módulo p, de manera que conforman un sistema completo de residuos cuadráticos módulo p, pues

$$\begin{aligned} i^2 \equiv j^2 \pmod{p} \quad &\iff \quad p \mid i^2 - j^2 = (i-j)(i+j) \\ &\iff \quad p \mid i-j \text{ ó } p \mid i+j \\ &\iff \quad i \equiv \pm j \pmod{p}. \end{aligned}$$

Así, si x es residuo cuadrático módulo p, debe ser congruente a alguno de estos números.

Ahora, aunque conozcamos la lista completa de residuos cuadráticos módulo p, en la práctica es difícil reconocer si un número d es o no residuo cuadrático módulo p.

Congruencias

Ejemplo: Módulo 23 tenemos

- $0^2 \equiv 0 \pmod{23}$,
- $1^2 \equiv 1 \pmod{23}$,
- $2^2 \equiv 4 \pmod{23}$,
- $3^2 \equiv 9 \pmod{23}$,
- $4^2 \equiv 16 \pmod{23}$,
- $5^2 \equiv 2 \pmod{23}$,
- $6^2 \equiv 13 \pmod{23}$,
- $7^2 \equiv 3 \pmod{23}$,
- $8^2 \equiv 18 \pmod{23}$,
- $9^2 \equiv 12 \pmod{23}$,
- $10^2 \equiv 8 \pmod{23}$,
- $11^2 \equiv 6 \pmod{23}$,

Así, los resíduos cuadráticos módulo 23 son:

$$0, 1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18.$$

Ejemplo: ¿Es 53 resíduo cuadrático módulo 101?
No.

Precisamos de una forma eficiente para determinar si un entero a cualquiera es residuo cuadrático módulo p.

Definición

*Sea $p > 2$ un número primo y $a \in \mathbb{Z}$ un entero cualquiera. Definimos el **símbolo de Legendre** como*

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

Proposición (Criterio de Euler)

Sea $p > 2$ un primo impar, y sea $a \in \mathbb{Z}$. Entonces

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

<u>Prueba</u>: Para $a \equiv 0 \pmod p$, el resultado es inmediato pues $\left(\frac{a}{p}\right) = 0 \equiv 0^{(p-1)/2} \pmod p$. Suponga entonces que $p \nmid a$. Por el Teorema de Fermat, sabemos que $a^{p-1} \equiv 1 \pmod p$.

Como

$$\begin{aligned} a^{p-1} - 1 \equiv 0 \pmod{p} &\iff (a^{(p-1)/2} - 1)(a^{(p-1)/2} + 1) \equiv 0 \pmod{p} \\ &\iff p \mid a^{(p-1)/2} - 1 \text{ ó } p \mid a^{(p-1)/2} + 1 \\ &\iff a^{(p-1)/2} \equiv \pm 1 \pmod{p}. \end{aligned}$$

Debemos ahora mostrar que $a^{(p-1)/2} \equiv 1 \pmod{p}$ si, y sólo si, a es un residuo cuadrático módulo p. Observe que si a es un residuo cuadrático módulo p, entonces $a \equiv j^2 \pmod{p}$, y por el Teorema de Fermat, se tiene

$$a^{(p-1)/2} \equiv (j^2)^{(p-1)/2} \equiv j^{p-1} \equiv 1 \pmod{p}.$$

Así, los residuos cuadráticos $1^2, 2^2, \ldots, (\frac{p-1}{2})^2$ son todos raíces del polinomio $f(x) = x^{(p-1)/2} - \bar{1}$ en $\mathbb{Z}/p\mathbb{Z}[x]$. Pero, $\mathbb{Z}/p\mathbb{Z}$ es un cuerpo, luego f puede tener a lo sumo $\deg f = \frac{p-1}{2}$ raíces en $\mathbb{Z}/p\mathbb{Z}$. Esto muestra que las raíces de $f(x)$ son exactamente los residuos cuadráticos no congruentes a cero módulo p.
Portanto, $a^{(p-1)/2} \equiv 1 \pmod{p} \Leftrightarrow a$ es residuo cuadrático módulo p. $\square$

Símbolo de Legendre

Corolario (Euler)

Sea $p > 2$ primo. Entonces $(-1)^{(p-1)/2} \equiv 1 \pmod{p}$ si, y sólo si, $p \equiv 1 \pmod{4}$.

Prueba: Como p es impar, sólo puede ser de la forma $p = 4k+1$ o de la forma $p = 4k+3$.

- Si $p = 4k+1 \;\Rightarrow\; \frac{p-1}{2} = \frac{4k}{2} = 2k$. Luego, $(-1)^{(p-1)/2} \equiv (-1)^{2k} \equiv 1 \pmod{p}$.
- Si $p = 4k+3 \;\Rightarrow\; \frac{p-1}{2} = \frac{4k+2}{2} = 2k+1$. Luego, $(-1)^{(p-1)/2} \equiv (-1)^{2k+1} \equiv -1 \pmod{p}$.

Corolario

El símbolo de Legendre satisface las siguientes propiedades:

1. *Si $a \equiv b \pmod{p}$, entonces $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.*
2. $\left(\frac{a^2}{p}\right) = 1$, *si $p \nmid a$.*
3. $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$. *Esto es, -1 es residuo cuadrático módulo $p \;\Leftrightarrow\; p \equiv 1 \pmod{4}$.*
4. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

Prueba: (1) y (2) son inmediatos a partir de la definición, o si lo prefieren, también se deducen a partir de Criterio de Euler:

$$a \equiv b \pmod p \;\Rightarrow\; \left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \equiv b^{(p-1)/2} \equiv \left(\frac{b}{p}\right) \pmod p \;\Rightarrow\; , \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right),$$

$$\left(\frac{1}{p}\right) \equiv (1)^{(p-1)/2} \equiv 1 \pmod p \;\Rightarrow\; \left(\frac{1}{p}\right) = 1.$$

(3) Del Criterio de Euler, junto con el corolario anterior, tenemos

$$\left(\frac{-1}{p}\right) \equiv 1 \pmod p \iff (-1)^{(p-1)/2} \equiv 1 \pmod p$$
$$\iff p = 4k+1 \iff p \equiv 1 \pmod 4.$$

(4) Finalmente, del Criterio de Euler tenemos que

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

lo que muestra que $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$, pues ambos lados son iguales a ± 1. $\square$

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,

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

<u>Prueba</u>: 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

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

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

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

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,

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

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

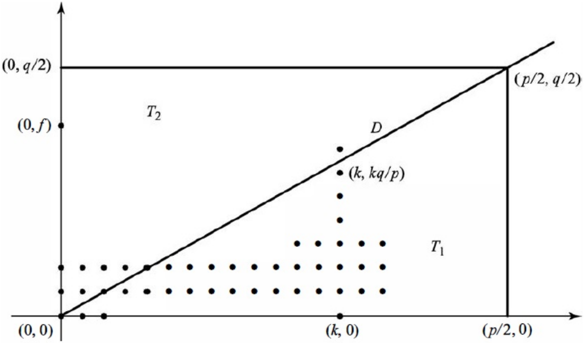
$$\frac{p-1}{2}\cdot\frac{q-1}{2} = \sum_{1\le i\le\frac{q-1}{2}} \left\lfloor \frac{ip}{q} \right\rfloor + \sum_{1\le i\le\frac{p-1}{2}} \left\lfloor \frac{iq}{p} \right\rfloor. \tag{4}$$

y que

$$\left(\frac{p}{q}\right) = (-1)^{\sum_{1\le i\le\frac{q-1}{2}} \left\lfloor \frac{ip}{q} \right\rfloor}, \qquad \text{y} \qquad \left(\frac{q}{p}\right) = (-1)^{\sum_{1\le i\le\frac{p-1}{2}} \left\lfloor \frac{iq}{p} \right\rfloor}. \tag{5}$$

La fórmula (4) 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 $y=\frac{p}{q}x$.



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 (5), 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

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

Ley de Reciprocidad Cuadrática

Corolario

Si p y q son primos impares distintos, entonces

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

<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

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

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.