Congruencias Cuadráticas

Alan Reyes-Figueroa

Teoría de Números (Aula 18) 02.septiembre.2024

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 divisibles 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

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

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.

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 residuos cuadráticos módulo 23 son:

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

Ejemplo: ¿Es 53 residuo 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 $a^{p-1} \equiv 1 \pmod{p}$.

Símbolo de Legendre

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. $\square$

Corolario (Euler)

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

<u>Prueba</u>: 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. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

Símbolo de Legendre

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 $|S|$. $\square$

Lema de Gauss

El Criterio de Euler ya produce un mecanismo para identificar residuos cuadráticos. Vamos a mostrar ahora un resultado que ilustra el uso práctico del Lema de Gauss.

Teorema (Gauss)

Sea p un primo impar. Entonces

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

Prueba: La propiedad es consecuencia directa 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 $k + 1 \leq j \leq 2k$.

Entonces 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, $k = \frac{p-1}{4} = \frac{8q+4}{4} = 2q + 1$.

Lema de Gauss

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