Polinomios cuadráticos en $\mathbb{F}_p$

Mario Pineda Ruelas
Departamento de Matemáticas,
Universidad Autónoma Metropolitana-Iztapalapa
correo electrónico: mpr@xanum.uam.mx

Gabriel D. Villa Salvador
Departamento de Control Automático,
Centro de Investigación y de Estudios Avanzados, IPN
correo electrónico gvilla@ctrl.cinvestav.mx

1 Introducción

En la sección 2.4 (ver notas de congruencias) hicimos un estudio de las soluciones del polinomio $f(x) \in \mathbb{Z}_m[x]$ y observamos que todo se reduce a estudiar las soluciones en $\mathbb{F}_p$ en lugar de $\mathbb{Z}_m$ y donde $p \mid m$. Entre otras cosas, dimos un criterio-algoritmo para resolver congruencias lineales $ax \equiv b \pmod{m}$: Si $g = \text{mcd}(a, m)$ y $g \mid b$, entonces nuestra congruencia de grado 1 tiene g-soluciones diferentes o incongruentes. En el caso particular que el módulo es un primo p, entonces la solución es única, descartando por supuesto el caso $a \equiv 0 \pmod{p}$. Ahora nuestro objetivo es estudiar un polinomio de grado 2 en $\mathbb{F}_p[x]$.

Sea $f(x) = ax^2 + bx + c \in \mathbb{R}[x]$ de grado 2. Entonces con un argumento algebraico elemental se llega a que $f(x_0) = 0$ si y sólo si

$$x_0 = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

Este razonamiento no puede ser imitado en polinomios cuadráticos $f(x) \in \mathbb{F}_p[x]$ y las razones principales son:

1. Si $p = 2$, entonces $2a \equiv 0 \pmod{2}$.
2. No sabemos cómo interpretar la expresión $\sqrt{b^2 - 4ac}$ en $\mathbb{F}_p$.

El primer obstáculo lo podemos evitar simplemente pidiendo $p \neq 2$, al fin y al cabo es muy simple verificar si 0 ó 1 es raíz de cualquier polinomio. Para el segundo obstáculo tenemos el siguiente resultado:

Teorema 1.1. *Sea $a \in \mathbb{Z}$ y p un primo impar tal que $(a,p) = 1$. Entonces $ax^2 + bx + c \equiv 0 \pmod{p}$ es soluble si y sólo si $(2ax+b)^2 \equiv b^2 - 4ac \pmod{p}$ es soluble.*

Demostración: Sea $x_0 \in \mathbb{F}_p^*$ tal que $ax_0^2 + bx_0 + c \equiv 0 \pmod{p}$. Entonces

$$\begin{aligned} ax_0^2 + bx_0 + c &\equiv 0 \pmod{p} \text{ si y sólo si} \\ 4a(ax_0^2 + bx_0 + c) &\equiv 0 \pmod{p} \text{ si y sólo si} \\ 4a^2x_0^2 + 4abx_0 + 4ac &\equiv 0 \pmod{p} \text{ si y sólo si} \\ 4a^2x_0^2 + 4abx_0 + 4ac + b^2 &\equiv b^2 \pmod{p} \text{ si y sólo si} \\ 4a^2x_0^2 + 4abx_0 + b^2 &\equiv b^2 - 4ac \pmod{p} \text{ si y sólo si} \\ (2ax_0 + b)^2 &\equiv b^2 - 4ac \pmod{p}. \end{aligned}$$

□

Observemos que si en el teorema anterior ponemos $y = 2ax + b$ y $a_0 = b^2 - 4ac$, entonces resolver una congruencia de la forma $ax^2 + bx + c \equiv 0 \pmod{p}$ es equivalente a resolver la congruencia $y^2 \equiv a_0 \pmod{p}$. Esto motiva la siguiente definición.

Definición 1.2. *Sea p un primo impar y $a \in \mathbb{Z}$ tal que $\text{mcd}(a,p) = 1$. Diremos que a es un residuo cuadrático módulo p si y sólo si $x^2 \equiv a \pmod{p}$ es soluble. En caso contrario diremos que a no es un residuo cuadrático módulo p.*

Ejemplo 1.3. *Residuos cadráticos en $\mathbb{F}_7$. Se puede mostrar, por simple ensayo error, que los únicos elementos de $\mathbb{F}_7^*$ que son residuo cuadrático módulo 7 son: $1, 2, 4$. De paso observamos que exactamente la mitad de los elementos de $\mathbb{F}_7^*$ son un residuo cuadrático. Más adelante veremos que esto no es una simple casualidad.*

Al conjunto de residuos cuadráticos módulo p lo escribiremos como

$$GRC_p = \{a \in U_p : x^2 \equiv a \pmod{p} \quad \text{es soluble}\}$$

y éste no es vacio pues $1 \in GRC_p$ para todo p.

Teorema 1.4. *Sea $a \in GRC_p$. Si $b \in U_p$ es tal que $ab \equiv 1 \pmod{p}$, entonces $b \in GRC_p$.*

Demostración: Sólo hay que demostrar que la congruencia $x^2 \equiv b \pmod{p}$ es soluble. En efecto, sea c tal que $c^2 \equiv a \pmod{p}$. Entonces $x = cb$ es solución de $x^2 \equiv b \pmod{p}$. □

El teorema anterior es de singular importancia porque nos muestra que GRC_p es cerrado bajo productos y contiene al inverso multiplicativo de cada elemento en GRC_p. En pocas palabras, GRC_p es un subgrupo de $\mathbb{F}_p^*$. De ahora en adelante llamaremos a GRC_p con el nombre de *grupo de residuos cuadráticos* del campo $\mathbb{F}_p$.

2 Cuadrados en $\mathbb{F}_p$ y Símbolo de Legendre

De los problemas importantes en toda la matemática, resalta uno de manera sobresaliente: encontrar las raíces de un polinomio que tiene sus coeficientes en un campo dado. Si el campo es $\mathbb{Q}, \mathbb{R}$ ó $\mathbb{C}$, entonces ya hay métodos y técnicas muy estudiadas en cierta clase de polinomios y que no son aplicables al caso particular de $\mathbb{F}_p$. Precisamente en esta sección desarrollaremos la teoría necesaria para poder decidir si un polinomio cuadrático con coeficientes enteros tiene una raíz en el campo finito $\mathbb{F}_p$. Sea p un primo impar y $a \in \mathbb{Z}$ tal que $\text{mcd}(a, p) = 1$.

Definición 2.1. *Definimos el símbolo de Legendre*[1] *como*

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \textit{si } a \textit{ es residuo cuadrático módulo } p, \\ -1 & \textit{si } a \textit{ no es residuo cuadrático módulo } p. \end{cases}$$

Vale la pena mencionar que fue Legendre el que introdujo esta notación en su célebre trabajo *Essai sur la Théorie des Nombres* en el año 1798. De la definición anterior tenemos para $\text{mcd}(a, p) = 1$ que

1. $\left(\frac{a}{p}\right) = 1$ si y sólo si $x^2 - a \in \mathbb{F}_p[x]$ es soluble en $\mathbb{F}_p$.

2. $\left(\frac{a}{p}\right) = -1$ si y sólo si $x^2 - a \in \mathbb{F}_p[x]$ no es soluble $\mathbb{F}_p$.

Teorema 2.2. *Si* $a, b \in \mathbb{Z}$ *y* p *primo impar tal que* $\text{mcd}(a, p) = \text{mcd}(b, p) = 1$*, entonces:*

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

2. *Si* $a \equiv b \pmod{p}$*, entonces* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

[1] Adrien-Marie Legendre nació en 1752 en Toulouse, Francia. Su nombre va unido a un gran número de proposiciones, lo que atestigua la diversidad de sus investigaciones. Aunque sobresalió particularmente en teoría de números, contribuyó también de manera original en otros campos: ecuaciones diferenciales, cálculo de variaciones, teoría de funciones, geometría euclidiana e integrales elípticas. Sus trabajos matemáticos fueron durante mucho tiempo los clásicos por excelencia: Elementos de geometría(1794); Ensayo sobre la teoría de números(1798); Tratado de las funciones elípticas y de las integrales eulerianas(1825-1832) y Teoría de números(1830).

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

4. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

5. $\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)$.

Demostración: 1. La congruencia $x^2 \equiv a^2 \pmod{p}$ tiene solución $x_0 = a$.

2. Es inmediata.

3. Si $\left(\frac{a}{p}\right) = 1$, entonces existe $x_0 \in \mathbb{Z}$ tal que $x_0^2 \equiv a \pmod{p}$. Por lo anterior

$$a^{\frac{p-1}{2}} \equiv \left(x_0^2\right)^{\frac{p-1}{2}} \equiv x_0^{p-1} \equiv 1 \pmod{p},$$

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

Si $\left(\frac{a}{p}\right) = -1$, entonces $x^2 \equiv a \pmod{p}$ no es soluble. Si $r \in \mathbb{F}_p^*$, entonces la congruencia lineal $rx \equiv a \pmod{p}$ tiene solución única $r' \in \mathbb{F}_p^*$. Es claro que $r \neq r'$, pues de lo contrario $x^2 \equiv a \pmod{p}$ sería soluble. Así, al conjunto $\{1, 2, \ldots, p-1\}$ lo podemos partir en parejas $\{r, r'\}$ que satisfacen $rr' \equiv a \pmod{p}$ y $r \not\equiv r' \pmod{p}$. Con el Teorema de Wilson obtenemos

$$-1 \equiv (p-1)! = \prod (rr') \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

Por lo tanto, si $\left(\frac{a}{p}\right) = -1$, entonces $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$.

4. Usando la parte 3 tenemos

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

por tanto,

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \equiv \left(\frac{ab}{p}\right) \pmod{p}$$

y no sólo son congruentes, sino que son iguales.

5. Puesto que $\text{mcd}(a, p) = \text{mcd}(b^2, p) = 1$, entonces por 1) y 4) tenemos que

$$\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b^2}{p}\right) = \left(\frac{a}{p}\right).$$

□

Notemos que la parte 2 del teorema anterior puede ser muy útil en el siguiente sentido: Si $a = bp + r$ y $0 < r < p$, entonces $\left(\frac{a}{p}\right) = \left(\frac{r}{p}\right)$.

Corolario 2.3. *Si p es un primo impar, entonces*

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

Demostración: Si $p \equiv 1 \pmod 4$, entonces $\dfrac{p-1}{2}$ es par. Si $p \equiv 3 \pmod 4$, entonces $\dfrac{p-1}{2}$ es impar.

□

Ejemplo 2.4. *Como aplicación de la parte 3 (Euler) del Teorema 2.2 tenemos que* $\left(\frac{p}{3}\right) = p^{\frac{3-1}{2}} = p$. *Así:*

$$\left(\frac{p}{3}\right) = \begin{cases} 1 & si\ p \equiv 1 \pmod 3 \\ -1 & si\ p \equiv 2 \pmod 3 \end{cases}$$

Ejemplo 2.5. *Si* $p = 601$, *entonces* $\left(\dfrac{-1}{601}\right) = (-1)^{\frac{600}{2}} = 1$. *Por lo tanto* $x^2 \equiv -1 \pmod{601}$ *es soluble, luego el polinomio* x^2+1 *tiene una raíz en* $\mathbb{F}_{601}$, *es decir,* x^2+1 *es reducible en* $\mathbb{F}_{601}[x]$.

Ejemplo 2.6. *Si* $p = 47$, *entonces* $\left(\dfrac{-1}{47}\right) = -1$, *y así,* $x^2 \equiv -1 \pmod{47}$ *no tiene solución en el campo* $\mathbb{F}_{47}$, *lo cual significa que el polinomio* x^2+1 *es irreducible en* $\mathbb{F}_{47}[x]$.

Ejemplo 2.7. *Si p es cualquier primo, entonces es claro que* 1 *y* $p-1$ *son los únicos elementos de* U_p *que satisfacen* $1^2 \equiv (p-1)^2 \equiv 1 \pmod p$. *Esto significa que la congruencia* $x^2-1 \equiv 0 \pmod p$ *es soluble. Usando el Teorema del Factor* **??** *tenemos que la factorización de* x^2-1 *en* $\mathbb{F}_p[x]$ *es* $x^2-1 = (x-1)(x-p+1)$.

El Corolario 2.3 nos asegura que la congruencia $x^2+1 \equiv 0 \pmod p$ es soluble si $p = 4n+1$ y si $p \equiv 3 \pmod p$, entonces $x^2+1 \equiv 0 \pmod p$ no tiene solución. En el lenguaje de los polinomios tenemos que $f(x) = x^2+1$ es reducible en $\mathbb{F}_p[x]$ si $p \equiv 1 \pmod 4$ e irreducible si $p \equiv 3 \pmod 4$. Por lo pronto, podemos decidir con cierta facilidad si la congruencia $x^2 \equiv a \pmod p$ es o no soluble. Otro problema es encontrar explícitamente las soluciones.

PROBLEMAS

1. Puede el lector responder ¿por qué dejamos fuera de la definición de residuo cuadrático al primo $p = 2$ y por qué, en la definición de residuo cuadrático módulo p, sólo consideramos enteros que son primos relativos con p?

2. Consideremos el campo finito $\mathbb{F}_p$. Mostrar que para cada entero $n > 1$ existe $f(x) \in \mathbb{F}_p[x]$ irreducible de grado n.

3. Usar el Teorema 1.1 para transformar cada uno de los siguientes polinomios cuadráticos en uno de la forma $x^2 \equiv a \pmod{p}$:

   a) $f(x) = 2 - x + 3x^2$ en $\mathbb{F}_7[x]$.

   b) $f(x) = 1 + 2x - x^2$ en $\mathbb{F}_{13}[x]$.

   c) $f(x) = -2 - 7x + 14x^2$ en $\mathbb{F}_{17}[x]$.

4. Demostrar la parte 2 del Teorema 2.2.

5. ¿Para qué valores de p es -2 un residuo cuadrático?

6. ¿En qué campos $\mathbb{F}_p$ el polinomio $f(x) = x^2 + 1$ es irreducible?

7. Sea $f(x) \in \mathbb{F}_p[x]$ un polinomio de grado 2. Mostrar que si $f(x)$ no tiene raíces en $\mathbb{F}_p$, entonces $f(x)$ es irreducible en $\mathbb{F}_p[x]$.

8. Para los siguientes números primos, mostrar con una lista todos los residuos cuadráticos y el inverso multiplicativo de cada elemento en GRC_p.

   a) 17

   b) 13

   c) 79

   d) 137

   e) 251

9. Sea p un primo impar y $a \in \mathbb{Z}$ tal que $\text{mcd}(a, p) = 1$ y $x^2 \equiv a \pmod{p}$ es soluble. Entonces la congruencia $x^2 \equiv a \pmod{p}$ tiene dos soluciones incongruentes.

10. Sea $\mathbb{F}$ cualquier campo. Se sabe que si $f(x) \in \mathbb{F}[x]$ es irreducible en $\mathbb{F}[x]$ y $gr(f(x)) > 1$, entonces $f(x)$ no tiene raíces en $\mathbb{F}$. Si $f(x)$ es reducible o factorizable con polinomios de $\mathbb{F}[x]$ entonces ¿$f(x)$ debe tener al menos una raíz en $\mathbb{F}$?

11. Mostrar que el número de soluciones de $x^2 \equiv a \pmod{p}$ está dado por $1 + \left(\frac{a}{p}\right)$.

12. Sea p un primo impar. Encontrar los valores de c para que la congruencia $3x^2 - 2x + c \equiv 0 \pmod{p}$ tenga solución.

13. Usando el Corolario 2.3, demostrar que si un número primo impar p es suma de dos cuadrados, entonces $p = 4n + 1$.

14. Para los grupos de residuos cuadráticos GRC_p, con $p = 23, 37, 43$, encontrar $\alpha \in GRC_p$ tal que si $a \in GRC_p$, entonces $a = \alpha^j$ para algún $j \in \mathbb{N} \cup \{0\}$.

15. Supongamos que a es impar. Mostrar que:

    a) $x^2 \equiv a \pmod 2$ tiene exactamente una solución en $\mathbb{F}_2$.

    b) $x^2 \equiv a \pmod{2^2}$ es soluble si y sólo si $a \equiv 1 \pmod 4$. En este caso existen dos soluciones en $\mathbb{Z}_4$.

    c) $x^2 \equiv a \pmod{2^3}$ tiene solución si y sólo si $a \equiv 1 \pmod{2^3}$. En este caso existen exactamente cuatro soluciones en $\mathbb{Z}_8$.

    d) Supongamos que $s \geq 3$ y $x^2 \equiv a \pmod{2^s}$ tiene una solución c_s. Entonces $x^2 \equiv a \pmod{2^{s+1}}$ admite una solución de la forma $c_{s+1} = c_s + t2^{s-1}$.

    e) Para $n \geq 3$, $x^2 \equiv a \pmod{2^n}$ tiene solución si y sólo si $a \equiv 1 \pmod 8$. En este caso existen cuatro soluciones.

3 Ley de Reciprocidad Cuadrática (LRC)

El problema que estudiaremos ahora es ¿cómo evaluar el Símbolo de Legendre? Para valores grandes del primo p, calcular los cuadrados módulo p ofrece dificultades bastante serias. Así que lo primero que haremos en esta sección es encontrar leyes generales que nos simplifiquen nuestro problema.

Teorema 3.1. *Sea* $a = (-1)^{\mu(a)} 2^\alpha p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ *la factorización de* a*, donde* $\mu(a) = 1$ *si* $a < 0$ *y* $\mu(a) = 2$ *si* $a > 0$*. Si* p *es un primo impar y* $\mathrm{mcd}(a, p) = 1$*, entonces evaluar el símbolo* $\left(\frac{a}{p}\right)$ *se reduce a evaluar a lo más:*

$$\left(\frac{-1}{p}\right), \quad \left(\frac{2}{p}\right), \quad \left(\frac{p_i}{p}\right).$$

Demostración: Por la parte 2 del Teorema 2.2 tenemos que

$$\left(\frac{a}{p}\right) = \left(\frac{(-1)^{\mu(a)}}{p}\right)\left(\frac{2^\alpha}{p}\right)\prod_{i=1}^{r}\left(\frac{p_i^{\alpha_i}}{p}\right).$$

Si $\mu(a) = 1$, entonces el Corolario 2.3 nos da la respuesta para $\left(\frac{-1}{p}\right)$. El caso $\mu(a) = 2$ es evidente. Para los otros factores hagámoslo en general: Sea q

cualquier divisor primo de a y $\beta \in \mathbb{N}$. Si $\beta = 2t$, entonces $q^\beta = (q^t)^2$ y por lo tanto

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

Si $\beta = 2t + 1$, entonces

$$\left(\frac{q^\beta}{p}\right) = \left(\frac{(q^t)^2 q}{p}\right) = \left(\frac{q}{p}\right).$$

□

Ahora ya sabemos cuál es el camino para averiguar si un entero es un residuo cuadrático y sólo nos queda encontrar respuesta para $\left(\frac{2}{p}\right)$ y $\left(\frac{q}{p}\right)$.

La ley general que va a satisfacer el símbolo $\left(\frac{q}{p}\right)$ se conoce como *Ley de Reciprocidad Cuadrática* (LRC) y las dos primeras leyes $\left(\frac{-1}{p}\right)$ y $\left(\frac{2}{p}\right)$ se conocen como *Leyes Suplementarias*.

La LRC fue descubierta experimentalmente por Euler y Legendre y sin embargo, no pudieron dar una demostración de ella. En 1796, Gauss usa inducción y da la primera demostración completa. Esta demostración aparece publicada en su obra monumental [**?**] en los artículos 125-145. Parece ser que sus argumentos no eran tan disfrutables como para fascinar a sus lectores. Con el tiempo, llegó a dar al menos seis demostraciones diferentes, una de las cuales depende de la construcción con regla y compás de los polígonos regulares. En el siglo XIX se conocían cerca de 50 publicaciones de la LRC [**?**], incluyendo una demostración de G. Mathews[3] que era una variación de la primera demostración de Gauss.

En casi todos los libros donde se da una prueba de la LRC, la demostración corresponde a una variación de la tercera demostración de Gauss y fue hecha por Eisenstein, el estudiante más brillante de Gauss.

En esta sección estudiaremos el Lema de Gauss, en el cual se basó Eisenstein[2]. Para facilitar la prueba del Lema de Gauss comentaremos antes un ejemplo.

[2]Ferninand Gotthold Max Eisenstein nace el 16 de abril de 1823 en Berlín, Alemania. Eisenstein sufrió toda su vida de mala salud, de hecho, es el único sobreviviente de sus cinco hermanos, los cuales mueren todos de meningitis. Se sabe que Gauss era extremadamente difícil de impresionar, sin embargo Eisenstein lo cautiva con sus trabajos. Sus contribuciones más sobresalientes están en la teoría de formas cuadráticas, leyes de reciprocidad superior y en la teoría de Kummer de ideales. Las dos primeras lineas de investigación intentaban generalizar el trabajo de Gauss. En [**?**], Weil examina las anotaciones hechas por Eisenstein en su copia de *Disquisitiones Arithmeticae* y afirma que ahí Riemann recibió las ideas que lo condujeron a su célebre trabajo sobre la función zeta. Eisenstein muere de pulmonía a los 29 años de edad el 11 de octubre de 1852.

Ejemplo 3.2. *Sea* $p = 17,\ a = 6$ *y* $\dfrac{p-1}{2} = 8$. *Consideremos el conjunto*

$$S = \{1 \cdot a, 2 \cdot a, \ldots, \frac{p-1}{2} \cdot a\} = \{1 \cdot 6, 2 \cdot 6, 3 \cdot 6, 4 \cdot 6, 5 \cdot 6, 6 \cdot 6, 7 \cdot 6, 8 \cdot 6\}.$$

Reduciendo los elementos de S *módulo 17 obtenemos*

$$S' = \{6, 12, 1, 7, 13, 2, 8, 14\}.$$

Notemos que S' *contiene 3 elementos que exceden la cantidad de* $\dfrac{17}{2} = 8.5$, *a saber* $12, 13, 14$. *Por medio de ensayo error podemos mostrar que* $x^2 \equiv 6 \pmod{17}$ *no tiene solución. Esto significa que* $\left(\dfrac{6}{17}\right) = -1 = (-1)^3$. *Coincidentemente el exponente* 3 *es la cardinalidad del conjunto* $\{12, 13, 14\}$. *Veremos que este fenómeno no es una casualidad.*

Lema 3.3. [Lema de Gauss] *Sea* p *primo impar y* $a \in \mathbb{Z}$ *tal que* $p \nmid a$. *Consideremos el conjunto* $S = \{1 \cdot a, 2 \cdot a, \ldots, \dfrac{p-1}{2} \cdot a\}$. *Para* $i = 1, \ldots, \dfrac{p-1}{2}$, *sea* $ia = pq_i + r_i$ *con* $0 \leq r_i < p$. *Si* $S' = \{r_1, r_2, \ldots, r_{\frac{p-1}{2}}\}$ *denota al conjunto de residuos módulo* p *de los elementos de* S *y* n *es el número de elementos de* S' *que exceden la cantidad* $\dfrac{p}{2}$, *entonces*

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

Demostración: Primero observemos que $r_i \not\equiv r_j \pmod{p}$ para $i \neq j$. Así, S' está formado por elementos incongruentes dos a dos. Sean $r_1, r_2, \ldots, r_n \in S'$ tal que $r_i > \dfrac{p}{2}$, $i = 1, \ldots, n$ y $s_1, \ldots, s_m \in S$ tal que $s_i < \dfrac{p}{2}$. Entonces

$$n + m = \frac{p-1}{2},\ s_i \neq \frac{p}{2},\ r_j \neq \frac{p}{2}$$

pues p es un número primo impar. Es claro que los elementos

$$r_1, \ldots, r_n, s_1, \ldots, s_m$$

son distintos. Así que $p - r_1, p - r_2, \ldots, p - r_n$ son diferentes dos a dos y

$$0 < p - r_i < \frac{p}{2}.$$

Por lo tanto, los elementos $p - r_1, p - r_2, \ldots, p - r_n, s_1, s_2, \ldots, s_m$ son mayores que cero y menores que $\dfrac{p}{2}$. Afirmamos que ellos son diferentes. En efecto:

Si $p - r_i = p - r_j$ con $i \neq j$, entonces $r_i = r_j$, lo cual es absurdo.

Si $p - r_i = s_j$, entonces existen x_0, y_0 con $1 \leq x_0, y_0 \leq \dfrac{p-1}{2}$ tales que $r_i \equiv x_0 a \pmod{p}$ y $s_j \equiv y_0 a \pmod{p}$, así

$$s_j = p - r_i \equiv p - x_0 a \equiv y_0 a \pmod{p},$$

de donde $p \mid a(-y_0 - x_0)$ y por lo tanto $p \mid (x_0 + y_0)$, lo cual es imposible pues $2 \leq x_0 + y_0 \leq p - 1$.

Hasta este momento hemos visto que

$$\{p - r_1, p - r_2, \ldots, p - r_n, s_1, \ldots, s_m\} = \{1, 2, \ldots, \frac{p-1}{2}\},$$

donde $n + m = \dfrac{p-1}{2}$.

Para finalizar la prueba observemos que

$$\begin{aligned}
\left(\frac{p-1}{2}\right)! &= \prod_{j=1}^{n}(p - r_j)\prod_{j=1}^{m} s_j \\
&\equiv (-1)^n \prod_{j=1}^{n} r_j \prod_{j=1}^{m} s_j \\
&\equiv (-1)^n a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \pmod{p}
\end{aligned}$$

y como $\left(\dfrac{p-1}{2}\right)!$ y p son primos relativos, entonces cancelando se obtiene

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

De lo anterior concluimos que $\left(\dfrac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \equiv (-1)^n \pmod{p}$. Por lo tanto

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

□

Recordemos que si $a, b \in \mathbb{Z},\ a \neq 0$, entonces

$$b = a\left[\frac{b}{a}\right] + r, \qquad \text{y} \qquad 0 \leq r < |a|$$

donde [ ] es la función mayor entero. Este hecho fue discutido en el Teorema **??**. Usando lo anterior y las ideas de la prueba del Lema de Gauss tenemos el siguiente resultado.

Lema 3.4. *Sea p un primo impar y $a \in \mathbb{N}$ tal que $p \nmid a$. Consideremos n y S como en el* Lema de Gauss. *Si $t = \sum_{i=1}^{\frac{p-1}{2}} \left[\frac{ia}{p}\right]$, entonces*

$$(a-1)\frac{p^2-1}{8} \equiv t - n \pmod 2.$$

Demostración: Sean $r_1, r_2, \ldots, r_n, s_1, s_2, \ldots, s_m$ como en el lema de Gauss. Sabemos que:

$$\{p - r_1, p - r_2, \ldots, p - r_n, s_1, \ldots, s_m\} = \{1, 2 \ldots, \frac{p-1}{2}\}.$$

Sumando los elementos de cada lado tenemos

$$\sum_{i=1}^{n}(p - r_i) + \sum_{i=1}^{m} s_i = \sum_{i=1}^{\frac{p-1}{2}} i.$$

Pero

$$\sum_{i=1}^{\frac{p-1}{2}} i = \frac{p^2-1}{8},$$

así

$$\sum_{i=1}^{n}(p - r_i) + \sum_{i=1}^{m} s_i = np - \sum_{i=1}^{n} r_i + \sum_{i=1}^{m} s_i.$$

Por lo tanto

$$\frac{p^2-1}{8} = np - \sum_{i=1}^{n} r_i + \sum_{i=1}^{m} s_i \tag{1}$$

Usando el algoritmo de la división con p y ia tenemos

$$ia = \left[\frac{ia}{p}\right] p + R_i, \qquad i = 1, \ldots, \frac{p-1}{2},$$

donde los R_i son exactamente los elementos de $\{r_1, \ldots, r_n, s_1, \ldots, s_m\}$. Por lo tanto

$$a\Big(\frac{p^2-1}{8}\Big) = \sum_{i=1}^{\frac{p-1}{2}} ia = \sum_{i=1}^{\frac{p-1}{2}} \Big(\left[\frac{ia}{p}\right] p + R_i\Big) =$$

$$p\sum_{i=1}^{\frac{p-1}{2}} \left[\frac{ia}{p}\right] + \sum_{i=1}^{\frac{p-1}{2}} R_i = pt + \sum_{i=1}^{n} r_i + \sum_{i=1}^{m} s_i. \tag{2}$$

Restando la ecuación (1) de la ecuación (2) obtenemos

$$pt + \sum_{i=1}^{n} r_i + \sum_{i=1}^{m} s_i - \big(np - \sum_{i=1}^{n} r_i + \sum_{i=1}^{m} s_i\big) = p(t-n) + 2\sum_{i=1}^{n} r_i.$$

También

$$a\frac{p^2-1}{8} - \frac{p^2-1}{8} = (a-1)\frac{p^2-1}{8}.$$

De esta manera hemos obtenido que

$$(a-1)\frac{p^2-1}{8} = p(t-n) + 2\sum_{i=1}^{n} r_i.$$

Por lo tanto

$$(a-1)\frac{p^2-1}{8} \equiv p(t-n) \pmod 2.$$

El resultado se sigue al observar que $p \equiv 1 \pmod 2$.

□

Como decíamos con anterioridad, las *Leyes Suplementarias* son un antecedente importante para entender el Símbolo de Legendre.

Teorema 3.5. [Leyes Suplementarias] *Si p es un primo impar, entonces*

1. $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.
2. $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

Demostración: La primera afirmación es *verbatim* el Corolario 2.3. Para la segunda afirmación ponemos en el Lema 3.4 $a = 2$. Entonces

$$t = \sum_{i=1}^{\frac{p-1}{2}} \left[\frac{2i}{p}\right] = \left[\frac{2}{p}\right] + \left[\frac{4}{p}\right] + \cdots + \left[\frac{p-1}{p}\right] = 0.$$

Así que por el lema anterior

$$\frac{p^2-1}{8} \equiv -n \equiv n \pmod 2.$$

Esto último significa que $\frac{p^2-1}{8}$ y n tienen la misma paridad, i.e, ambos son pares o ambos son impares. Por lo tanto, aplicando el Lema de Gauss obtenemos

$$\left(\frac{2}{p}\right) = (-1)^n = (-1)^{\frac{p^2-1}{8}}.$$

□

Ahora podemos caracterizar los primos p para los cuales el polinomio $x^2 - 2$ es reducible o irreducible en $\mathbb{F}_p[x]$.

Corolario 3.6. $\left(\frac{2}{p}\right) = \begin{cases} 1 & si\ p \equiv 1,7 \pmod 8 \\ -1 & si\ p \equiv 3,5 \pmod 8). \end{cases}$

Demostración: Se sigue directamente del Teorema 3.5.

□

Corolario 3.7. $\left(\frac{-2}{p}\right) = 1$ *si y sólo si* $p \equiv 1,3 \pmod 8$.

Demostración: Cualquier primo impar p es de la forma $8n+1, 8n+3, 8n+5$ ó $8n+7$, entonces

$$\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) = (-1)^{\frac{p-1}{2}}(-1)^{\frac{p^2-1}{8}} = (-1)^{\frac{(p-1)(p+5)}{8}} = 1$$

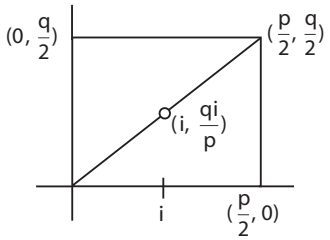
si y sólo si $p \equiv 1,3 \pmod 8$.

□

Lema 3.8. [Lema de Eisenstein] *Si p, q son primos impares con $p \neq q$, entonces*

$$\frac{p-1}{2}\frac{q-1}{2} = \sum_{i=1}^{\frac{p-1}{2}} \left[\frac{qi}{p}\right] + \sum_{i=1}^{\frac{q-1}{2}} \left[\frac{pi}{q}\right]$$

Demostración: Reproduciremos la prueba que dió Eisenstein y la cual es de naturaleza puramente geométrica. En $\mathbb{R} \times \mathbb{R}$ consideremos el rectángulo cuyos vértices se encuentran en los puntos $(0,0)$, $(\frac{p}{2},0)$, $(0,\frac{q}{2})$ y $(\frac{p}{2},\frac{q}{2})$. La idea es contar los puntos dentro de este rectángulo, sin considerar los lados, y cuyas coordenadas sean enteros.



Como p y q son impares, entonces queremos contar los puntos de la forma (m,n) con m,n enteros que satisfacen

$$1 \leq m \leq \frac{p-1}{2} \quad \text{y} \quad 1 \leq n \leq \frac{q-1}{2}.$$

Es claro que el número de tales puntos debe ser $\frac{p-1}{2}\frac{q-1}{2}$.

Primero veremos que sobre la diagonal no hay puntos de los que buscamos. La ecuación de la diagonal es $y = \frac{q}{p}x$ donde

$$0 < x < \frac{p}{2} \quad \text{y} \quad 0 < y < \frac{q}{2}.$$

Sea $x = i \in \mathbb{Z}$ tal que $0 < i < \frac{p}{2}$. Entonces $y = \frac{qi}{p}$ y el punto correspondiente sobre la diagonal es $(i, \frac{qi}{p})$. Notemos que $\frac{qi}{p} \notin \mathbb{Z}$. Por lo tanto la diagonal no contiene puntos con ambas coordenadas enteros. Todo lo anterior nos reduce el trabajo a contar sólo en el triángulo inferior y en el triángulo superior. Consideremos el triángulo con vértices en

$$(0,0), \qquad (\frac{p}{2}, 0), \qquad (\frac{p}{2}, \frac{q}{2}).$$

Para $i = 1, 2, \ldots, \frac{p-1}{2}$, consideremos la línea vertical dentro del triángulo en $x = i$. Este segmento empieza en $(i, 0)$ y termina en $(i, \frac{qi}{p})$. Recordemos que no debemos considerar estos puntos terminales. Debemos contar el número de enteros mayores que cero y menores que $\frac{qi}{p}$. Puesto que $\left[\frac{qi}{p}\right]$ es el mayor entero debajo de la diagonal, los puntos de la forma (i, j) con $1 \leq j \leq \left[\frac{qi}{p}\right]$ son los que andamos buscando. Por lo tanto, el número de puntos con ambas coordenadas enteras y dentro del triángulo inferior es

$$\sum_{i=1}^{\frac{p-1}{2}} \left[\frac{qi}{p}\right].$$

Por último, sólo nos falta contar en el triángulo superior. Para esto consideremos la familia de rectas horizontales

$$y = j, \quad j = 1, 2, \ldots, \frac{q-1}{2}$$

dentro del rectángulo cuyos vértices son: $(0,0),\ (0, \frac{q}{2}),\ (\frac{p}{2}, \frac{q}{2})$. De la misma manera que contamos en el triángulo inferior, encontramos que el número de puntos con ambas coordenadas enteros dentro del triángulo superior es

$$\sum_{i=1}^{\frac{q-1}{2}} \left[\frac{pi}{q}\right].$$

Por lo tanto, $\dfrac{p-1}{2}\dfrac{q-1}{2} = \displaystyle\sum_{i=1}^{\frac{p-1}{2}} \left[\frac{qi}{p}\right] + \sum_{i=1}^{\frac{q-1}{2}} \left[\frac{pi}{q}\right]$

□

Teorema 3.9. [Ley de Reciprocidad Cuadrática] *Sean p, q primos impares distintos. Entonces*

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

Demostración: Aplicamos el Lema 3.4 con p y $a = q$. Puesto que q es impar se tiene $q-1 \equiv 0 \pmod 2$. Así que $0 \equiv t-n \pmod 2$ o equivalentemente $t \equiv n \pmod 2$. Por el Lema de Gauss $\left(\dfrac{q}{p}\right) = (-1)^n = (-1)^t$, donde $t = \displaystyle\sum_{i=1}^{\frac{p-1}{2}} \left[\frac{qi}{p}\right]$. Intercambiando los papeles de q y p obtenemos $\left(\dfrac{p}{q}\right) = (-1)^{t'}$, con $t' = \displaystyle\sum_{i=1}^{\frac{q-1}{2}} \left[\frac{pi}{q}\right]$. Por lo tanto, usando el Lema de Eisenstein

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^t(-1)^{t'} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

□

Corolario 3.10. $\left(\dfrac{p}{q}\right)\left(\dfrac{q}{p}\right) = \begin{cases} 1 & \text{si } p \text{ o } q \equiv 1 \pmod 4 \\ -1 & \text{si } p \text{ y } q \equiv 3 \pmod 4. \end{cases}$

Demostración: Si $p \equiv 1 \pmod 4$, entonces $\dfrac{p-1}{2}$ es un número par y por tanto $\left(\dfrac{p}{q}\right)\left(\dfrac{q}{p}\right) = 1$. De la misma manera se obtienen los otros casos.

□

Corolario 3.11. *Si p, q primos impares diferentes, entonces*

$$\left(\frac{q}{p}\right) = \begin{cases} -\left(\dfrac{p}{q}\right) & \text{si } p \equiv q \equiv 3 \pmod 4 \\ \left(\dfrac{p}{q}\right) & \text{en otro caso.} \end{cases}$$

Demostración: Se sigue directamente del Corolario 3.10.

□

Corolario 3.12. *Sean p, q primos impares diferentes. Entonces*

1. *Si $p \equiv q \equiv 3 \pmod 4$, entonces q es residuo cuadrático módulo p si y sólo si p no es residuo cuadrático módulo q.*

2. *Si p ó $q \equiv 1 \pmod 4$, entonces q es residuo cuadrático módulo p si y sólo si p es residuo cuadrático módulo q.*

Demostración: Es una simple reformulación del Corolario 3.11.

□

El lector estará de acuerdo que el Corolario 3.11 es el que justifica propiamente el nombre de Ley de Reciprocidad Cuadrática.

Ejemplo 3.13. *¿Es reducible $f(x) = x^2 + 23$ en $\mathbb{F}_{41}[x]$? Se tiene que*

$$\left(\frac{-23}{41}\right) = \left(\frac{-1}{41}\right)\left(\frac{23}{41}\right) = \left(\frac{23}{41}\right) = \left(\frac{41}{23}\right) =$$
$$\left(\frac{18}{23}\right) = \left(\frac{3^2}{23}\right)\left(\frac{2}{23}\right) = \left(\frac{2}{23}\right) = 1,$$

pues $\left(\frac{-1}{41}\right) = 1$, $41 \equiv 1 \pmod 4$, $41 \equiv 18 \pmod{23}$ y $5^2 \equiv 2 \pmod{23}$. Por lo tanto, el polinomio $f(x) = x^2 + 23$ es reducible en $\mathbb{F}_{41}[x]$.

Ejemplo 3.14. *¿Es irreducible $f(x) = x^2 + 189$ en $\mathbb{F}_{491}[x]$? En este caso, tenemos*

$$\begin{aligned}
\left(\frac{-189}{491}\right) &= \left(\frac{-1}{491}\right)\left(\frac{3^2}{491}\right)\left(\frac{3}{491}\right)\left(\frac{7}{491}\right) \\
&= \left(\frac{-1}{491}\right)\left(\frac{3}{491}\right)\left(\frac{7}{491}\right) \\
&= (-1)(-1)\left(\frac{491}{3}\right)\left(\frac{7}{491}\right) \\
&= \left(\frac{2}{3}\right)\left(\frac{7}{491}\right) \\
&= \left(\frac{2}{3}\right)(-1)\left(\frac{491}{7}\right) \\
&= (-1)\left(\frac{2}{3}\right)\left(\frac{1}{7}\right) \\
&= (-1)(-1)(1) = 1
\end{aligned}$$

Por lo tanto, $x^2 \equiv -189 \pmod{491}$ es soluble y así $f(x) = x^2 + 189$ tiene una raíz en $\mathbb{F}_{491}$.

Ejemplo 3.15. *¿Para qué valores de p el polinomio $f(x) = x^2 - 3$ tiene una raíz en $\mathbb{F}_p$? Lo primero que debemos suponer es que $p > 3$. Aplicando la Ley de Reciprocidad Cuadrática tenemos*

$$\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = (-1)^{\frac{3-1}{2}\frac{p-1}{2}} = (-1)^{\frac{p-1}{2}}.$$

Multiplicando ambos lados por $\left(\frac{p}{3}\right)$ obtenemos, $\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right)$. Lo que queremos es que $\left(\frac{3}{p}\right) = 1$. Esto se da exactamente en dos situaciones:

$$(-1)^{\frac{p-1}{2}} = \left(\frac{p}{3}\right) = 1 \quad \text{ó} \quad (-1)^{\frac{p-1}{2}} = \left(\frac{p}{3}\right) = -1.$$

Puesto que

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

y para p impar, $p \neq 3$

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

entonces claramente tenemos

$$p \equiv 1 \pmod 4 \quad y \quad p \equiv 1 \pmod 3$$

ó

$$p \equiv 3 \pmod 4 \quad y \quad p \equiv 2 \pmod 3.$$

En el primer caso tenemos que $p \equiv 1 \pmod{12}$ y en el segundo caso

$$p \equiv 3 \equiv -1 \pmod 4 \quad y \quad p \equiv 2 \equiv -1 \pmod 3.$$

Por lo tanto $p \equiv -1 \pmod{12}$. Concluimos afirmando que

$$\left(\frac{3}{p}\right) = 1 \quad \textit{si y sólo si} \quad p \equiv \pm 1 \pmod{12}.$$

Ejemplo 3.16. *¿Para qué valores de p el polinomio $f(x) = x^2 + 3$ tiene una raíz en $\mathbb{F}_p$?*

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right) = \left(\frac{p}{3}\right).$$

Según el ejemplo 2.4 tenemos que: $\left(\frac{p}{3}\right) = 1$ si y sólo si $p \equiv 1 \pmod 3$.

Sumario: Encontrar las raíces en $\mathbb{Q}$ ó $\mathbb{R}$ de un polinomio cuadrático en una variable es una tarea relativamente sencilla: es suficiente con el conocimiento de un libro de álgebra elemental. La misma tarea en un campo con p elementos es un asunto más delicado. Si hacemos un recuento de los resultados que hasta ahora hemos demostrado, nos daremos cuenta que casi todos ellos son *simplemente* criterios para decidir si un polinomio cuadrático es soluble en algún campo con p elementos y ninguno de ellos nos indica exactamente cuál es la solución (si es que ésta existe). La forma natural de resolver cualquier problema es comenzar averiguando si el problema tiene solución. De esta manera son muy valiosos aquellos teoremas que dicen: *Existe* x tal que... y esto es un gran avance en la busqueda de una solución. La siguiente etapa es encontrar un método o algoritmo para encontrar las soluciones (si es que existen). Un método relativamente eficiente es el siguiente: Si $p \equiv 3 \pmod 4$ y $a \in GRC_p$, entonces $x = a^{\frac{p+1}{4}}$ es una solución de $x^2 \equiv a \pmod p$. El inconveniente es si p es demasiado grande, entonces una alternativa es usar una computadora. En cualquier caso es recomendable escribir un programa en algún lenguaje, inclusive para descubrir qué pasa con los primos de la forma $4n + 1$.

3.1 Aplicaciones de la LRC

El objetivo de esta sección es usar la LRC para demostrar el siguiente Teorema de Fermat:

Teorema 3.17. [Teorema de Fermat] *Sea p un número primo. Entonces existen $x, y \in \mathbb{Z}$ tales que:*

1. $p = x^2 + y^2$ *si y sólo si* $p \equiv 1 \pmod 4$.
2. $p = x^2 + 2y^2$ *si y sólo si* $p \equiv 1, 3 \pmod 8$.
3. $p = x^2 + 3y^2$ *si y sólo si* $p = 3$ *ó* $p \equiv 1 \pmod 3$.

La idea a seguir es la siguiente: Si p es un número primo tal que p divide a un número de la forma $x^2 + ny^2$, entonces p tiene la misma forma.

Teorema 3.18. *Sea p un número primo. Existen $x, y \in \mathbb{Z}$ tales que:*

1. $\left(\dfrac{-1}{p}\right) = 1$ *si y sólo si* $p \equiv 1 \pmod 4$.
2. $\left(\dfrac{-2}{p}\right) = 1$ *si y sólo si* $p \equiv 1, 3 \pmod 8$.

3. $\left(\frac{-3}{p}\right) = 1$ *si y sólo si* $p = 3$ *ó* $p \equiv 1 \pmod 3$.

Demostración: Es consecuencia directa de los Corolarios 2.3, 3.7 y el ejemplo 3.16.

□

Lema 3.19. *Sea* $n \in \mathbb{N}$ *y* p *un primo tal que* $p \nmid n$. *Existen* $x, y \in \mathbb{Z}$ *con* $\text{mcd}(x, y) = 1$ *tal que* $p \mid x^2 + ny^2$ *si y sólo si* $\left(\frac{-n}{p}\right) = 1$.

Demostración: Supongamos que existen enteros x, y primos relativos tal que $p \mid x^2 + ny^2$. Entonces $x^2 \equiv -ny^2 \pmod p$. Si $p \mid y$, entonces $p \mid x$, contrario a la suposición $\text{mcd}(x, y) = 1$. Por lo tanto, $\text{mcd}(y, p) = 1$. Sea b tal que $yb \equiv 1 \pmod p$. De la congruencia $x^2 \equiv -ny^2 \pmod p$ se sigue que

$$(xb)^2 \equiv -n(yb)^2 \equiv -n \pmod p.$$

y así $\left(\frac{-n}{p}\right) = 1$. Inversamente, si $x \in \mathbb{Z}$ es tal que $x^2 \equiv -n \pmod p$, entonces para $y \in \mathbb{F}^*$ tenemos $(xy)^2 \equiv -ny^2 \pmod p$. Por lo tanto $p \mid (xy)^2 + ny^2$.

□

Para $n = 1, 2, 3$, el Lema 3.19 queda como:

Corolario 3.20. *Sea* p *un número primo. Entonces existen enteros* a, b *tales que:*

1. $\left(\frac{-1}{p}\right) = 1$ *si y sólo si* $p \mid a^2 + b^2$.

2. $\left(\frac{-2}{p}\right) = 1$ *si y sólo si* $p \mid a^2 + 2b^2$.

3. $\left(\frac{-3}{p}\right) = 1$ *si y sólo si* $p \mid a^2 + 3b^2$.

□

Lema 3.21. *Sea* $n \in \mathbb{N}$ *y* $q = x^2 + ny^2$. *Supongamos que para ciertos enteros* a, b *primos relativos se tiene* $q \mid a^2 + nb^2$. *Si* q *es primo o* $q = 4$ *y* $n = 3$, *entonces existen* $c, d \in \mathbb{Z}$ *primos relativos tales que* $\frac{a^2 + nb^2}{q} = c^2 + nd^2$.

Demostración: Es claro que $q \mid x^2(a^2+nb^2)$ y $q \mid a^2(x^2+ny^2)$. Por lo tanto

$$q \mid (a^2x^2+nx^2b^2)-(a^2x^2+na^2y^2) = n(xb-ay)(xb+ay). \tag{1}$$

Si q es primo, entonces $q \mid n$ o $q \mid xb-ay$ o $q \mid xb+ay$. Si $q \mid n$, entonces de la desigualdad $q \leq n \leq x^2+ny^2 = q$ se sigue que $q=n$ y puesto que $n \mid a^2+nb^2$, se sigue $n \mid a$. Digamos que $a=nd$. Entonces

$$\frac{a^2+nb^2}{n} = \frac{n^2d^2+nb^2}{n} = nd^2+b^2.$$

Si $q \mid xb-ay$, entonces para algún $d \in \mathbb{Z}$ tenemos

$$xb-ay = d(x^2+ny^2) = dx^2+ndy^2.$$

Por lo tanto

$$xb-dx^2 = x(b-dx) = y(a+ndy). \tag{2}$$

Así, $x \mid y(a+ndy)$. Puesto que q es primo, necesariamente $\mathrm{mcd}(x,y)=1$. Lo anterior significa que $x \mid a+ndy$. Es decir, $a=cx-dny$ para algún $c \in \mathbb{Z}$. Sustituimos en (2) para obtener $b=dx+yc$. En la conocida igualdad

$$(c^2+nd^2)(x^2+ny^2) = (cx-ndy)^2+n(dx+cy)^2,$$

sustituimos los valores $a=cx-dny$, $b=dx+yc$ y $q=x^2+ny^2$ para obtener

$$(c^2+nd^2)q = a^2+nb^2.$$

Por lo tanto $\dfrac{a^2+nb^2}{q} = c^2+nd^2$. El caso $q \mid xb-ay$ es idéntico. Para ver que $\mathrm{mcd}(c,d)=1$ notemos que $1=az+bw$ para ciertos enteros z,w. Así tenemos

$$1 = az+bw = (cx-dny)z+(dx+yc)w = c(xz+yw)+d(-nyz+xw),$$

y por lo tanto $\mathrm{mcd}(c,d)=1$.

Finalmente, si $q=4$ y $n=3$, entonces $4 = 1^2+3\cdot 1^2$ y (1) funciona bien con $x=y=1$, es decir, $4 \mid b-a$ ó $4 \mid b+a$. Si $4 \mid b-a$, entonces $b-a = (1^2+3\cdot 1^2)d$ para algún $d \in \mathbb{Z}$ y así $b-d = a+3d$. Si escribimos $c=a+3d$, entonces

$$a = c-3d \quad \text{y} \quad b = c+d.$$

Sustituyendo el valor de c y b en la igualdad

$$(c^2+3d^2)(1^2+3\cdot 1^2) = (c-3d)^2+3(d+c)^2,$$

obtenemos

$$(c^2+3d^2)4 = a^2+3b^2,$$

y por lo tanto

$$\frac{a^2+3b^2}{4} = c^2+3d^2.$$

Si $4 \mid b+a$, entonces se repite el argumento anterior.

□

El Corolario 3.20 nos asegura que para $n = 1, 2, 3$, el primo p en cuestión satisface $p \mid a^2 + nb^2$. Veamos que esta afirmación ya nos garantiza que p es de la misma forma.

Teorema 3.22. *Sea $n = 1, 2, 3$ y p un primo impar tal que $p \mid a^2 + nb^2$ para ciertos enteros a, b con $\mathrm{mcd}(a, b) = 1$. Entonces p es de la forma $x^2 + ny^2$.*

Demostración: Supongamos que $p \mid a^2 + nb^2$ y al mismo tiempo que p no es de la forma x^2+ny^2. Es claro que para $k, l \in \mathbb{Z}$ se tiene $p \mid (a-kp)^2+n(b-lp)^2$. Por lo anterior, podemos elegir k, l de tal forma que

$$|a - kp| < \frac{p}{2} \quad \text{y} \quad |b - lp| < \frac{p}{2}.$$

Así que desde el principio podemos elegir a, b tal que

$$p \mid a^2 + nb^2 \quad \text{con} \quad |a| < \frac{p}{2} \quad \text{y} \quad |b| < \frac{p}{2}.$$

Puesto que $n \leq 3$, se tiene que $a^2 + nb^2 < \left(\frac{p}{2}\right)^2 + 3\left(\frac{p}{2}\right)^2 = p^2$. Tenemos así

$$a + nb^2 = 2^r p q_1 q_2 \cdots q_r,$$

donde $q_i < p$, para $i = 1, 2, ..., r$ son primos impares. Afirmamos que algún factor q_i no es de la forma $x^2 + ny^2$. Si logramos demostrar la afirmación anterior, entonces prácticamente ya tenemos la conclusión pues $q_i \mid a^2 + nb^2$ y repetimos el argumento que hicimos para el primo p. Obtendremos así, una sucesión infinita de primos positivos

$$0 < ..... < q_i < p,$$

lo cual es un absurdo. Bueno, supongamos que todos los q_i son de la forma $x^2 + ny^2$. Puesto que el producto es de la misma forma, aplicando el Lema 3.21 podemos cancelar y llegar a una expresión de la forma

$$\alpha^2 + n\beta^2 = 2^r p.$$

Si $n = 1, 2$, entonces $2 = 1^2 + 1 \cdot 1^2 = 0^2 + 2 \cdot 1^2$ y por lo tanto 2^r es de la misma forma. Aplicando nuevamente el Lema 3.21 llegamos a

$$\alpha_1^2 + n\beta_1^2 = p,$$

lo cual contradice la elección de p. Por lo tanto, algún q_i no es de la forma $x^2 + ny^2$.

Sólo nos queda el caso $n = 3$. Así tenemos $\alpha^2 + 3\beta^2 = 2^r p$ donde r es par o impar. Nuevamente vamos a aplicar el Lema 3.21 con $q = 4$ y $n = 3$. Si $r = 2t$, entonces $2^r = 2^{2t} = 4^t$ y por lo tanto

$$\frac{\alpha^2 + 3\beta^2}{4^t} = a'^2 + 3b'^2 = p,$$

lo cual no es posible por la elección de p. Si r es impar, entonces tenemos

$$\frac{\alpha^2 + 3\beta^2}{2^{r-1}} = a'^2 + 3b'^2 = 2p.$$

Por el Corolario 3.20 $\left(\frac{-3}{p}\right) = 1$. El Teorema 3.18 nos asegura que $p = 3$ ó $p \equiv 1 \pmod 3$. Cualquiera que sea el caso tenemos

$$2p = a'^2 + 3b'^2 \equiv 2 \equiv a^2 \pmod 3.$$

Si $p = 3$, entonces $2 \equiv 0 \pmod 3$ lo cual no es posible. Si $p \equiv 1 \pmod 3$, entonces 2 es un residuo cuadrático módulo 3, lo cual tampoco es posible. Lo anterior nos indica que no podemos llegar a la igualdad $\alpha^2 + n\beta^2 = 2^r p$ y por lo tanto, algún q_i no es de la forma $x^2 + ny^2$. La conclusión ya la sabemos. □

El Teorema 3.17, el Corolario 3.20 y el Teorema 3.22, aplicados en este orden, dan la justificación del Teorema de Fermat.

La aplicacion de la LRC que hemos estudiado es posiblemente el cimiento de una teoría abstracta que se llama *Leyes de Reciprocidad* y que seguramente, un antecedente se encuentra en el Teorema de Fermat que estudiamos en esta sección. Está fuera de nuestro alcance describir explícitamente cuál es el tema de estudio de esta teoría. Intentaremos dar una respuesta: Sea $f(x) \in \mathbb{Z}[x]$ mónico irreducible. Reducimos los coeficientes de $f(x)$ módulo un primo p. El polinomio resultante lo escribimos como $f_p(x)$. Si $f_p(x)$ se factoriza como producto de polinomios lineales en $\mathbb{F}_p[x]$ entonces diremos que $p \in Split(f)$. Entre otras cosas, esta teoría trata de encontrar el conjunto $Split(f)$. Para una espléndida exposición del tema invitamos al lector consultar [**?**].

PROBLEMAS

1. Calcular el símbolo de Legendre:

$$a)\ \left(\frac{2}{97}\right) \qquad b)\ \left(\frac{14}{97}\right) \qquad c)\ \left(\frac{-38}{29}\right)$$

$$d)\ \left(\frac{135}{67}\right) \qquad e)\ \left(\frac{-79}{97}\right) \qquad f)\ \left(\frac{-23}{59}\right)$$

2. En el Lema de Gauss, considerar las congruencias

$$r_i \equiv xa \pmod{p} \quad \text{y} \quad s_j \equiv ya \pmod{p}.$$

Supongamos que $p - r_i = s_j$. Mostrar que existen $x_0, y_0 \in \mathbb{Z}$ tales que

$$1 \leq x_0, y_0 \leq \frac{p-1}{2}$$

y

$$r_i \equiv x_0 a \pmod{p}, \qquad s_j \equiv y_0 a \pmod{p}.$$

3. Usar el Lema de Gauss 3.3 para decidir si las siguientes congruencias cuadráticas tienen solución en $\mathbb{F}_p$.

   a) $x^2 \equiv -5 \pmod{19}$

   b) $x^2 \equiv 9 \pmod{23}$

   c) $x^2 - 2x + 6 \equiv 0 \pmod{31}$

   d) $x^2 - 3x + 1 \equiv 0 \pmod{71}$

4. Considerar el rectángulo cuyos vértices son $(0,0), (\frac{p}{2}, 0), (0, \frac{q}{2}), (\frac{p}{2}, \frac{q}{2})$ y que aparecen en el Lema de Eisenstein 3.8. Se observa que la recta $y = \frac{q}{p}x$ divide al rectángulo en dos triángulos idénticos. Pareciera a simple vista que existe la misma cantidad de puntos con ambas coordenadas enteras en cada uno de estos triángulos. Sea $p = 11$ y $q = 13$. Mostrar geométricamente que en el triángulo inferior hay más puntos con ambas coordenadas enteras que en el triángulo superior. ¿Cómo explicar este fenómeno? ¿Siempre sucede lo mismo? ¿Es posible que en algún caso los triángulos tengan la misma cantidad de puntos con ambas coordenadas enteras?

5. Sean p, q primos impares distintos y $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) = -1$. Mostrar que el polinomio $f(x) = x^2 - a$ es irreducible en $\mathbb{Z}_{pq}[x]$. Esto último significa que $x^2 \equiv a \pmod{pq}$ no tiene solución en $\mathbb{Z}_{pq}$.

6. Sea p un primo impar y $a \in \mathbb{Z}$ tal que $\text{mcd}(a, p) = 1$. Mostrar que $a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$.

7. Mostrar que:

   a) Si a, b son residuos cuadráticos módulo p, entonces ab es residuo cuadrático módulo p.

   b) Si a y b no son residuos cuadráticos módulo p, entonces ab es residuo cuadrático módulo p.

   c) ¿Qué pasa si a es residuo cuadrático y b no es residuo cuadrático?.

d) Si $ab \equiv n \pmod{p}$, donde n es un residuo cuadrático módulo p, entonces a, b son ambos residuos cuadráticos o ambos no son residuos cuadráticos.

8. Mostrar que la cardinalidad de GRC_p es $\dfrac{p-1}{2}$.

9. Encontrar los residuos cuadráticos y los no residuos cuadráticos en $\mathbb{F}_{23}$ y $\mathbb{F}_{31}$.

10. Mostrar que $\displaystyle\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) = 0$.

11. Sea p un primo impar. Mostrar que $p \in GRC_3$ si y sólo si $p \equiv 1 \pmod{3}$.

12. ¿Se puedes usar la fórmula $\dfrac{-b \pm \sqrt{b^2 - 4ac}}{2a}$ para resolver una ecuación cuadrática en $\mathbb{F}_p$?

13. Consideremos la congruencia $ax^2 + bx + c \equiv 0 \pmod{p}$ y $\Delta = b^2 - 4ac$. Mostrar que:

    a) $ax^2+bx+c \equiv 0 \pmod{p}$ no tiene solución en $\mathbb{F}_p$ si y sólo si $\left(\dfrac{\Delta}{p}\right) = -1$.

    b) $ax^2 + bx + c \equiv 0 \pmod{p}$ tiene solución única en $\mathbb{F}_p$ si y sólo si $p \mid \Delta$.

    c) $ax^2 + bx + c \equiv 0 \pmod{p}$ tiene dos soluciones incongruentes en $\mathbb{F}_p$ si y sólo si $\left(\dfrac{\Delta}{p}\right) = 1$. ¿Puede decir cuáles son?

14. Reproducir toda la teoría de esta sección (o lo que se pueda) para $\left(\dfrac{a}{2}\right)$.

15. Sea $GRC_p = \{r_1, \ldots, r_{\frac{p-1}{2}}\}$. Mostrar que $\displaystyle\sum_{i=1}^{\frac{p-1}{2}} r_i$ es divisible por p.

16. Sea $p \equiv 3 \pmod{4}$ y $a \in GRC_p$. Mostrar que $x = a^{\frac{p+1}{4}}$ es una solución de $x^2 \equiv a \pmod{p}$. Este es un método eficiente para encontrar residuos cuadráticos.

17. Encontrar una solución de $f(x) = x^2 + 10$ en $\mathbb{F}_{971}$. Por supuesto que primero se debe decidir si existe tal solución.

18. Mostrar que si $p \equiv 1 \pmod{5}$, entonces $f(x) = x^2 - 5$ tiene una raíz en $\mathbb{F}_p$.

19. Mostrar que si $p \equiv 2 \pmod{5}$, entonces $f(x) = x^2 - 5$ no tiene soluciones en $\mathbb{F}_p$.

20. Acerca de la discusión final de la sección anterior, considerar los siguientes polinomios mónicos irreducibles: $f(x) = x^2 - 2, f(x) = x^2 - p$, con p un primo impar. Encontrar $Split(f)$.

4 Cuadrados en $\mathbb{Z}_m$ y Símbolo de Jacobi

El Símbolo de Legendre $\left(\frac{a}{p}\right)$ fue definido en todo $\mathbb{F}_p^*$, con p un primo impar. Jacobi[3] extendió el Símbolo de Legendre a otros denominadores impares.

Definición 4.1. *Sea $a, m \in \mathbb{Z}^*$ tal que $\text{mcd}(a, m) = 1$ y m impar. Si $m = p_1 p_2 \cdots p_r$ (los p_i no necesariamente distintos), definimos el Símbolo de Jacobi*

$$\left(\frac{a}{m}\right) = \prod_{i=1}^{r} \left(\frac{a}{p_i}\right),$$

donde $\left(\frac{a}{p_i}\right)$ denota el Símbolo de Legendre.

Si $m = p$, entonces el Símbolo de Jacobi y el Símbolo de Legendre coinciden.

Definición 4.2. *Sean a y m como en la definición anterior. Diremos que a es un residuo cuadrático módulo m si $f(x) = x^2 - a$ tiene solución en $\mathbb{Z}_m$.*

Claramente si a es residuo cuadrático módulo m y $p_i \mid m$, entonces a es residuo cuadrático módulo p_i. Así que $\left(\frac{a}{p_i}\right) = 1$ para todo primo p_i que divide a m y por lo tanto $\left(\frac{a}{m}\right) = 1$. El inverso del comentario anterior es falso. Por ejemplo

$$\left(\frac{2}{33}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{11}\right) = (-1)(-1) = 1$$

y se puede verificar fácilmente que $x^2 \equiv 2 \pmod{33}$ no tiene solución en $\mathbb{Z}_{33}$.

El Símbolo de Jacobi tiene las siguientes propiedades elementales.

[3]Carl Gustav Jacob Jacobi nació en Berlín en 1804. Estudia en la Universidad de Berlín. Su padre, rico banquero, le procuró cuanto era necesario para completar su formación filológica y matemática. Profesor nato, realizó una carrera brillante como docente y como investigador, pero renunció a sus funciones en 1842 por razones de salud y se retiró a Berlín con una pensión del gobierno prusiano. Jacobi es célebre en matemáticas principalmente por sus trabajos sobre las funciones elípticas y los determinantes funcionales, llamados también Jacobianos. Jacobi se interesó también por el cálculo de variaciones y su principal descubrimiento se refiere a la existencia de puntos conjugados. Finalmente, en teoría de números él es el que da la primera demostración sobre las leyes de reciprocidad bicuadrática y cúbica.

Proposición 4.3. *Si* $\text{mcd}(a,m) = \text{mcd}(a',m) = \text{mcd}(a,m') = \text{mcd}(a',m') = 1$, *entonces:*

1. *Si* $a \equiv a' \pmod{m}$, *entonces* $\left(\frac{a}{m}\right) = \left(\frac{a'}{m}\right)$.
2. $\left(\frac{aa'}{m}\right) = \left(\frac{a}{m}\right)\left(\frac{a'}{m}\right)$.
3. $\left(\frac{a}{mm'}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{m'}\right)$.
4. $\left(\frac{a^2}{m}\right) = \left(\frac{a}{b'^2}\right) = 1$.
5. $\left(\frac{a^2a'}{m^2m'}\right) = \left(\frac{a'}{m'}\right)$.

Demostración: 1. Si $a \equiv a' \pmod{m}$, entonces $a \equiv a' \pmod{p}$ para cualquier número primo p tal que $p \mid m$. Usando el Teorema 2.2 parte 2 tenemos

$$\left(\frac{a}{p}\right) = \left(\frac{a'}{p}\right)$$

y por lo tanto $\left(\frac{a}{m}\right) = \left(\frac{a'}{m}\right)$.

2. Usaremos la parte 4 del Teorema 2.2 acerca de la multiplicatividad del Símbolo de Legendre. Así tenemos

$$\left(\frac{aa'}{m}\right) = \left(\frac{aa'}{p_1}\right)\left(\frac{aa'}{p_2}\right)\cdots\left(\frac{aa'}{p_r}\right) = \prod_{i=1}^{r}\left(\frac{a}{p_i}\right)\left(\frac{a'}{p_i}\right) = \left(\frac{a}{m}\right)\left(\frac{a'}{m}\right).$$

3. Evidente.

4. $\left(\frac{a^2}{m}\right) = \prod_{p|m}\left(\frac{a^2}{p}\right) = 1$ y $\left(\frac{a}{m^2}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{m}\right) = \left(\frac{a}{m}\right)^2 = 1$.

5. $\left(\frac{a^2a'}{m^2m'}\right) = \left(\frac{a^2a'}{m^2}\right)\left(\frac{a^2a'}{m'}\right) = \left(\frac{a^2}{m^2}\right)\left(\frac{a'}{m^2}\right)\left(\frac{a^2}{m'}\right)\left(\frac{a'}{m'}\right) = \left(\frac{a'}{m'}\right)$.

□

Lema 4.4. *Sean* r, s *enteros impares. Entonces*

$$\frac{rs-1}{2} \equiv \frac{r-1}{2} + \frac{s-1}{2} \pmod{2} \quad y \quad \frac{r^2s^2-1}{8} \equiv \frac{r^2-1}{8} + \frac{s^2-1}{8} \pmod{2}.$$

Demostración: Puesto que

$$(r-1)(s-1) \equiv rs - r - s + 1 - 1 + 1 \equiv 0 \pmod 4,$$

entonces, $rs - 1 \equiv (r-1) + (s-1) \pmod 4$. Dividiendo entre 2 ambos lados de la congruencia obtenemos la primera afirmación de nuestro lema.

Para la segunda parte notemos primero que

$$r^2 - 1 \equiv 0 \pmod 4 \quad \text{y} \quad s^2 - 1 \equiv 0 \pmod 4.$$

Por lo tanto $(r^2-1)(s^2-1) \equiv 0 \pmod{16}$. Así

$$r^2 s^2 - 1 \equiv (r^2 - 1) + (s^2 - 1) \pmod{16}.$$

El resultado se sigue al dividir ambos lados de última congruencia entre 8.

□

Corolario 4.5. *Sean $r_1, r_2, \ldots, r_n$ enteros impares. Entonces*

$$\sum_{i=1}^{n} \frac{r_i - 1}{2} \equiv \frac{(\prod_{i=1}^{n} r_i) - 1}{2} \pmod 2 \quad y \quad \sum_{i=1}^{n} \frac{r_i^2 - 1}{8} \equiv \frac{\prod_{i=1}^{n} r_i^2 - 1}{8} \pmod 2.$$

Demostración: Usar el Lema 4.4 e inducción sobre n.

□

Como es de esperarse, el Símbolo de Jacobi también satisface Leyes Suplementarias y una Ley de Reciprocidad Cuadrática, las cuales generalizan las leyes correspondientes al Símbolo de Legendre.

Teorema 4.6. [Leyes Suplementarias] *Si m es un entero positivo impar, entonces:*

1. $\left(\dfrac{-1}{m}\right) = (-1)^{\frac{m-1}{2}}$.

2. $\left(\dfrac{2}{m}\right) = (-1)^{\frac{m^2-1}{8}}$.

3. *Si a es un entero positivo impar, entonces* $\left(\dfrac{a}{m}\right)\left(\dfrac{m}{a}\right) = (-1)^{\frac{a-1}{2}\frac{m-1}{2}}$.

Demostración: 1. Sea $m = p_1 p_2 \cdots p_r$. Usando la primera parte del Corolario 4.5 obtenemos

$$\left(\frac{-1}{m}\right) = \left(\frac{-1}{p_1}\right)\left(\frac{-1}{p_2}\right)\cdots\left(\frac{-1}{p_r}\right) =$$

$$(-1)^{\frac{p_1-1}{2}} \cdots (-1)^{\frac{p_r-1}{2}} = (-1)^{\sum_{i=1}^{r} \frac{p_i-1}{2}} = (-1)^{\frac{m-1}{2}}.$$

2. Análogo a 1.
3. Si $a = q_1 q_2 \cdots q_l$, entonces

$$\left(\frac{a}{m}\right)\left(\frac{m}{a}\right) = \prod_{i=1}^{l}\prod_{j=1}^{r}\left(\frac{q_i}{p_j}\right)\left(\frac{p_j}{q_i}\right) = (-1)^{\sum_{i=1}^{l}\sum_{j=1}^{r}\frac{q_i-1}{2}\frac{p_j-1}{2}}.$$

Usando el Corolario 4.5 obtenemos

$$\sum_{i=1}^{l}\sum_{j=1}^{r}\frac{p_j-1}{2}\frac{q_i-1}{2} \equiv \frac{a-1}{2}\sum_{i=1}^{l}\frac{p_i-1}{2} \equiv \frac{a-1}{2}\frac{m-1}{2} \pmod 2$$

y por lo tanto

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

□

PROBLEMAS

1. Calcular los siguientes símbolos de Jacobi:
   a) $\left(\frac{18}{35}\right)$
   b) $\left(\frac{126}{315}\right)$
   c) $\left(\frac{186}{234}\right)$
2. Mostrar que si $\left(\frac{a}{m}\right) = -1$, entonces a no es un cuadrado en $\mathbb{Z}_m$.
3. Mostrar que $x^2 \equiv 32 \pmod{33}$ no es soluble a pesar que $\left(\frac{32}{33}\right) = 1$.
4. Mostrar que $f(x) = x^2 - 2$ es irreducible en $\mathbb{Z}_{33}[x]$.
5. Sea $f(x) \in \mathbb{Z}[x]$. Diremos que un primo p es un divisor de $f(x)$ si existe un entero n tal que $p \mid f(n)$. Describir todos los divisores primos de x^2+1 y $x^2 - 2$.

6. Sea p un primo impar. Verificar que :
$$\left(\frac{2}{p}\right) = \left(\frac{8-p}{p}\right) = \left(\frac{p}{p-8}\right) = \left(\frac{8}{p-8}\right) = \left(\frac{2}{p-8}\right).$$

7. Sea $RC_m = \{a \in \mathbb{Z}_m : x^2 \equiv a \pmod{m} \text{ es soluble}\}$. ¿Es un grupo RC_m?

8. Sea $m \in \mathbb{Z}$ y consideremos su factorización de $m^2+1 = p_1 p_2 \cdots p_r$ tal que $p_i \neq p_j$ si $i \neq j$. ¿Puede ser alguno de los p_i's de la forma $4n+3$?

5 Generadores de U_n (raíces primitivas)

Uno de los conceptos de la aritmética que ha tenido más aplicaciones en las últimas décadas es el de *raíz primitiva*, por ejemplo, en métodos para encriptar mensajes. El Teorema de Euler **??** nos asegura que si $\text{mcd}(a,n) = 1$, entonces $a^{\varphi(n)} \equiv 1 \pmod{n}$. Por el momento, nada nos asegura que $\varphi(n)$ sea el menor entero con la propiedad $a^{\varphi(n)} \equiv 1 \pmod{n}$. Si $\text{mcd}(a,n) = 1$, escribiremos $o_n(a) = x$ para indicar que $a^x \equiv 1 \pmod{n}$ y x es el menor entero positivo con esta propiedad. Al entero $o_n(a)$ lo llamaremos *el orden* de a módulo n. Veamos un ejemplo. Sea $n = 8$. Consideremos $SRR(8) = \{1,3,5,7\}$. Escogemos, por ejemplo $a = 3$. Para encontrar $o_8(a)$ simplemente calculamos las potencias de a módulo 8. Así
$$3^1 \equiv 3 \pmod{8}, \;\; 3^2 \equiv 1 \pmod{8},$$
y por lo tanto $o_8(3) = 2$. Análogamente, $o_8(5) = 2$ y $o_8(7) = 2$. Obviamente $o_8(1) = 1$ y por lo tanto concluimos que si $a \in SRR(8)$, entonces $o_8(a) < |SRR(8)| = 4$.

Un ejemplo más interesante resulta al considerar $n = 7$. En este caso
$$SRR(7) = \{1,2,3,4,5,6\}.$$
Se verifica fácilmente que
$$o_7(1) = 1, \;\; o_7(2) = 3, \;\; o_7(3) = 6, \;\; o_7(4) = 3, \;\; o_7(5) = 6, \;\; o_7(6) = 2.$$
Los casos 3 y 5 son de interés para nosotros. Observemos que módulo 7
$$\{3, 3^2, 3^3, 3^4, 3^5, 3^6\} = \{1,2,3,4,5,6\} = SRR(7),$$
$$\{5, 5^2, 5^3, 5^4, 5^5, 5^6\} = \{1,2,3,4,5,6\} = SRR(7).$$

Los ejemplos anteriores nos llevan directamente a la definición de raíz primitiva.

Definición 5.1. *Sean a, n enteros positivos con* $\text{mcd}(a,n) = 1$. *Diremos que a es una raíz primitiva de n si* $o_n(a) = \varphi(n)$.

Usando el Teorema de Euler **??**, esta definición simplemente significa que a es una raíz primitiva de n si y sólo si

$$\{a, a^2, \ldots, a^{\varphi(n)}\} = SRR(n).$$

Es claro que no existe una raíz primitiva para $n = 8$ y $n = 7$ tiene exactamente dos. Podemos preguntarnos ¿qué enteros tienen raíces primitivas? Si un entero tiene raíces primitivas ¿podemos contarlas?

Corolario 5.2. *Si* $\text{mcd}(a,n) = 1$ *y* $a^x \equiv 1 \pmod{n}$, *entonces* $o_n(a) \mid x$.

Demostración: Usando el algoritmo de la división

$$x = o_n(a)q + r \quad \text{con} \quad 0 \leq r < o_n(a).$$

Entonces $a^x \equiv (a^{o_n(a)})^q a^r \equiv a^r \equiv 1 \pmod{n}$. Observemos que $0 < r$ no es posible pues $o_n(a)$ es el menor entero positivo con la propiedad $a^{o_n(a)} \equiv 1 \pmod{n}$. Por lo tanto $r = 0$.

□

¿En dónde usamos la hipótesis $\text{mcd}(a,n) = 1$?

Corolario 5.3. *Si* $\text{mcd}(a,n) = 1$, *entonces* $o_n(a) \mid \varphi(n)$.

Demostración: Si $\text{mcd}(a,n) = 1$, entonces por el Teorema de Euler **??** tenemos que $a^{\varphi(n)} \equiv 1 \pmod{n}$. Ahora aplicamos el corolario anterior.

□

El Teorema de Lagrange **??** nos asegura que si $f(x) \in \mathbb{Z}[x]$ y $gr(f(x)) = p-1$, entonces la congruencia

$$f(x) \equiv 0 \pmod{p}$$

tiene a lo más $p-1$ soluciones. Vamos a usar este hecho para deducir que cualquier primo p tiene raíces primitivas.

Teorema 5.4. *Si p es primo y $d \mid p-1$, entonces la congruencia* $x^d \equiv 1 \pmod{p}$ *tiene d soluciones distintas.*

Demostración: El Pequeño Teorema de Fermat **??** afirma que la congruencia

$$x^{p-1} \equiv 1 \pmod{p}$$

tiene exactamente $p-1$ soluciones distintas módulo p. Escribimos $p-1 = kd$ y usamos la igualdad

$$x^{p-1} - 1 = (x^d - 1)(x^{d(k-1)} + x^{d(k-2)} + \ldots + x^d + 1)$$

para deducir que la congruencia

$$(x^d - 1)(x^{d(k-1)} + x^{d(k-2)} + \ldots + x^d + 1) \equiv 0 \pmod{p}$$

también tiene $p-1$ soluciones distintas módulo p, sólo que ahora esas $p-1$ soluciones están repartidas en el producto

$$(x^d - 1)(x^{d(k-1)} + x^{d(k-2)} + \ldots + x^d + 1).$$

Por el Teorema de Lagrange **??** la congruencia $x^d - 1 \equiv 0 \pmod{p}$ tiene a lo más d soluciones y $x^{d(k-1)} + x^{d(k-2)} + \ldots + x^d + 1 \equiv 0 \pmod{p}$ tiene a lo más $d(k-1)$ soluciones. Por lo tanto $x^{p-1} - 1 \equiv 0 \pmod{p}$ tiene a lo más $d + d(k-1) = p-1$ soluciones distintas módulo p. Puesto que nuestra congruencia $x^{p-1} - 1 \equiv \pmod{p}$ tiene exactamente $p-1$ soluciones, entonces necesariamente $x^d - 1 \equiv 0 \pmod{p}$ tiene exactamente d soluciones y $x^{d(k-1)} + x^{d(k-2)} + \ldots + x^d + 1 \equiv 0 \pmod{p}$ tiene exactamente $d(k-1)$ soluciones.

□

El teorema anterior sólo nos confirma que la congruencia $x^d - 1 \equiv 0 \pmod{p}$ es soluble, pero hasta ahora, nada nos garantiza que existen enteros con la propiedad $o_p(x) = d$ para $d \mid p-1$.

Teorema 5.5. *Si p es primo y $d \mid p-1$, entonces existen $\varphi(d)$ enteros x tales que $o_p(x) = d$.*

Demostración: Si x satisface $x^d - 1 \equiv 0 \pmod{p}$, entonces $\text{mcd}(x, p) = 1$. Sea n el menor entero para el cual la afirmación del teorema es falsa. Así que, si $d < n$ y $d \mid p-1$, entonces la congruencia $x^d - 1 \equiv 0 \pmod{p}$ tiene exactamente $\varphi(d)$ soluciones con $o_p(x) = d$. Un entero a con $\text{mcd}(a, n) = 1$ es solución de $x^n \equiv 1 \pmod{p}$ si y sólo si $o_p(a) \mid n$. Así que el número de soluciones a con $o_p(a) < n$ de $x^n \equiv 1 \pmod{p}$ está dado por

$$\sum_{\substack{d \mid n \\ d < n}} \varphi(d).$$

Por el Corolario **??** tenemos $\displaystyle\sum_{\substack{d \mid n \\ d < n}} \varphi(d) = \sum_{d \mid n} \varphi(d) - \varphi(n) = n - \varphi(n)$. Por lo tanto, el número de soluciones a de $x^n \equiv 1 \pmod{p}$ y tal que $o_p(a) = n$ es $n - (n - \varphi(n)) = \varphi(n)$. Esto último contradice la elección de n.

□

Corolario 5.6. *Existen $\varphi(p-1)$ raíces primitivas de p, donde p es cualquier primo.*

Demostración: En el teorema anterior consideremos $d = p - 1$.

□

¡Qué romántico es el corolario anterior! Nos afirma que existen raíces primitivas para cualquier primo p y no nos dice cómo encontrarlas. En la siguiente sección veremos lo complicado que es este problema.

Bien, lo que sigue es mostrar que cualquier potencia de un primo impar p tiene raíces primitivas. Vamos por partes. Ya mostramos que cualquier primo p siempre tiene raíces primitivas. El siguiente paso es utilizar una raíz primitiva de p para mostrar que p^2 también tiene raíces primitivas. El paso siguiente consistirá en utilizar una raíz primitiva de p^2 para mostrar que p^k tiene raíces primitivas.

Teorema 5.7. *Sea p un primo impar. Si a es una raíz primitiva de p, entonces a o $a + p$ es una raíz primitiva de p^2.*

Demostración: Primero observemos que si a es una raíz primitiva de p, entonces también $a + p$ es una raíz primitiva de p. Sea $n = o_{p^2}(a)$. Entonces $a^n \equiv 1 \pmod{p^2}$ y n es el menor entero positivo con esta propiedad. Es claro que si $a^n \equiv 1 \pmod{p^2}$, entonces $a^n \equiv 1 \pmod{p}$. Puesto que a es raíz primitiva de p, entonces por el Corolario 5.2 tenemos que $p - 1 \mid n$. Por otro lado, $\text{mcd}(a, p^2) = 1$ y $a^n \equiv 1 \pmod{p^2}$, así que por el Corolario 5.3 tenemos $n \mid p(p-1)$. Estas dos afirmaciones nos llevan a que $n = p - 1$ ó $n = p(p-1)$. Estudiemos cada caso.

Si $n = p - 1$, entonces $a^{p-1} \equiv 1 \pmod{p^2}$. En este caso elegimos $r = a + p$. Así $r \equiv a \pmod{p}$ y por lo tanto r también es una raíz primitiva de p. Pongamos $m = o_{p^2}(r)$. Repitiendo el argumento anterior tenemos que $m = p - 1$ o $m = p(p-1)$. Veremos que $m = p - 1$ no es posible.

Tenemos la siguiente igualdad:

$$r^{p-1} = (a+p)^{p-1} = a^{p-1} + (p-1)a^{p-2}p + \frac{(p-1)(p-2)}{2}a^{p-3}p^2 + \ldots + p^{p-1}.$$

Así que

$$r^{p-1} \equiv a^{p-1} + (p-1)a^{p-2}p \equiv 1 + (p-1)a^{p-2}p \equiv 1 - pa^{p-2} \not\equiv 1 \pmod{p^2}$$

y por lo tanto $o_{p^2}(r) \neq p - 1$. De esta forma $o_{p^2}(r) = p(p-1) = \varphi(p^2)$.

El segundo caso es muy sencillo pues si $n = p(p-1)$, entonces $o_{p^2}(a) = \varphi(p^2)$ y a es una raíz primitiva de p^2.

□

La demostración del teorema anterior nos proporciona un recurso importante para construir raíces primitivas de p^2. Prácticamente es un algoritmo que se podría implementar fácilmente escribiendo algún programa para computadora. Concretamente tenemos: Si a es una raíz primitiva de p y $o_{p^2}(a) = p-1$, entonces necesariamente $a+p$ es una raíz primitiva de p^2. También, si $o_{p^2}(a) = p(p-1)$, entonces a es una raíz primitiva de p^2. Consideremos dos ejemplos sencillos con $p = 5, 29$. Una raíz primitiva de 5 es 2. Puesto que $o_{5^2}(2) = 5(5-1)$, entonces, como se puede comprobar fácilmente, 2 es una raíz primitiva de 25. También, 14 es una raíz primitiva de 29 y $o_{29^2}(14) = 29 - 1$. Así que $14 + 29 = 43$ es una raíz primitiva de 29^2. Ejemplos de éstos son difíciles de encontrar.

El siguiente resultado será fundamental para poder justificar que cualquier potencia de un número primo p tiene al menos una raíz primitiva,

Lema 5.8. *Si $k \geq 2$ y a es una raíz primitiva de p^2, entonces $a^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^k}$.*

Demostración: Inducción sobre k. Si $k = 2$, entonces el resultado es cierto pues a es una raíz primitiva de p^2. Supongamos que $a^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^k}$. Mostraremos que $a^{p^{k-1}(p-1)} \not\equiv 1 \pmod{p^{k+1}}$. Puesto que $\mathrm{mcd}(a,p) = 1$, entonces $\mathrm{mcd}(a, p^{k-1}) = 1$ y por el Teorema de Euler **??** tenemos

$$a^{\varphi(p^{k-1})} \equiv a^{p^{k-2}(p-1)} \equiv 1 \pmod{p^{k-1}}$$

y por lo tanto

$$a^{p^{k-2}(p-1)} = 1 + tp^{k-1}$$

para algún entero t. Por hipótesis de inducción $a^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^k}$, así que $p \nmid t$. Es claro que si $k \geq 3$ y $j \geq 2$, entonces $k(j-1) - (j+1) \geq 0$. Con la igualdad $p^{kj-j} = p^{k+1}p^{k(j-1)-(j+1)}$ obtenemos

$$(1 + tp^{k-1})^p =$$

$$1 + ptp^{k-1} + \frac{p(p-1)}{2}(tp^{k-1})^2 + \frac{p(p-1)(p-2)}{3!}(tp^{k-1})^3 + \ldots + (tp^{k-1})^p =$$

$$1 + tp^k + \frac{p(p-1)}{2}t^2p^{k+1}p^{k-3} + \ldots + t^pp^{k+1}p^{(p-1)k-(p+1)} \equiv 1 + tp^k \pmod{p^{k+1}}.$$

Lo anterior nos muestra que

$$a^{p^{k-1}(p-1)} = (a^{p^{k-2}(p-1)})^p = (1 + tp^{k-1})^p \not\equiv 1 \pmod{p^{k+1}}.$$

□

Ahora ya tenemos todo para justificar que cualquier potencia de un primo tiene raíces primitivas.

Teorema 5.9. *Si p es primo y $k \in \mathbb{N}$, entonces p^k tiene al menos una raíz primitiva.*

Demostración: Por el Teorema 5.7 sabemos que p y p^2 tienen una raíz primitiva en común. Así que podemos suponer que $k \geq 2$. Sea a una raíz primitiva en común de p y p^2. El entero a satisface $a^{p-1} \not\equiv 1 \pmod{p^2}$. Por el lema anterior tenemos

$$a^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^k}$$

para todo entero $k \geq 2$. Sea $r = o_{p^k}(a)$. Entonces $a^r \equiv 1 \pmod{p^k}$ y por el Corolario 5.3 tenemos $r \mid \varphi(p^k) = p^{k-1}(p-1)$. Puesto que $o_p(a) = p-1$ y $a^r \equiv 1 \pmod{p}$, entonces el Corolario 5.2 implica que $\varphi(p) \mid r$. Juntando las afirmaciones

$$r \mid p^{k-1}(p-1) \quad \text{y} \quad p-1 \mid r,$$

obtenemos $r = p^s(p-1)$, donde $0 \leq s \leq k-1$. Si $s \leq k-2$, entonces usando la igualdad $p^{k-2} = p^s p^{k-2-s}$ tenemos

$$a^{p^{k-2}(p-1)} \equiv (a^{p^s(p-1)})^{p^{k-2-s}} \equiv 1 \pmod{p^k},$$

lo que contradice el lema anterior. Por lo tanto $s = k-1$ y $r = \varphi(p^k)$.

□

Lema 5.10. *Si $o_n(a) = r$ y $m \in \mathbb{N}$, entonces $o_n(a^m) = \dfrac{r}{\text{mcd}(r,m)}$.*

Demostración: La prueba la haremos en tres casos:
Caso 1. $m|r$. Supongamos que $r = mq$. Es claro que $\text{mcd}(r,m) = m$ y

$$\frac{r}{\text{mcd}(r,m)} = \frac{r}{m}.$$

En este caso debemos probar que $o_n(a^m) = \dfrac{r}{m} = q$. Notemos primero que

$$(a^m)^q = a^r \equiv 1 \pmod{n}.$$

Así que $o_n(a^m) \leq q$. Supongamos que $o_n(a^m) < q$. Veremos que esta suposición nos conduce a una contradicción. Multiplicando ambos lados de la desigualdad $o_n(a^m) < q$ por m obtenemos $mo_n(a^m) < mq = r$, así que

$$(a^m)^{o_n(a^m)} \equiv 1 \pmod{n} \quad \text{y} \quad mo_n(a^m) < r = o_n(a),$$

y por lo tanto r no es el orden de a. Así que necesariamente $o_n(a^m) = q$.

Caso 2. $\text{mcd}(m,r) = 1$. Según la afirmación del teorema, debemos mostrar que $o_n(a^m) = r$. Sean $x, y \in \mathbb{Z}$ tal que $mx + yr = 1$. Multiplicando esta última igualdad por $o_n(a^m)$ obtenemos

$$mxo_n(a^m) + yro_n(a^m) = o_n(a^m),$$

de donde

$$a^{o_n(a^m)} = (a^m)^{xo_n(a^m)} \cdot (a^r)^{yo_n(a^m)} \equiv 1 \pmod{n},$$

y así $o_n(a^m) \geq r$ puesto que $o_n(a) = r$. Por otro lado

$$(a^m)^r = (a^r)^m \equiv 1 \pmod{n},$$

así que $r \geq o_n(a^m)$ y por lo tanto la igualdad.

Caso 3. Caso general. Si $\text{mcd}(m, r) = d$, entonces $m = dq_0, r = dq_1$ con $\text{mcd}(q_0, q_1) = 1$. Debemos probar que $o_n(a^m) = \dfrac{r}{d}$. Puesto que $d \mid r$, por el caso 1 tenemos $o_n(a^d) = q_1$ y ya que $\text{mcd}(q_0, q_1) = 1$, entonces por el caso 2 $(a^d)^{q_0}$ tiene orden $q_1 = \dfrac{r}{d}$.

□

Corolario 5.11. *Sea a una raíz primitiva de n. Entonces a^r es raíz primitiva de n si y sólo si* $\text{mcd}(r, \varphi(n)) = 1$.

Demostración: Por el lema anterior tenemos

$$o_n(a^r) = \frac{o_n(a)}{\text{mcd}(r, m)} = \frac{\varphi(n)}{\text{mcd}(r, \varphi(n))}.$$

Por lo tanto $o_n(a^r) = \varphi(n)$ si y sólo si $\text{mcd}(r, \varphi(n)) = 1$.

□

Vamos a precisar el número de raíces primitivas que tiene un entero n, generalizando así el Corolario 5.6.

Teorema 5.12. *Si n tiene una raíz primitiva, entonces n tiene $\varphi(\varphi(n))$ raíces primitivas.*

Demostración: Sea a una raíz primitiva de n. Entonces $\{a, a^2, \ldots, a^{\varphi(n)}\} = SRR(n)$. Por el Corolario 5.11 tenemos que a^r es una raíz primitiva de n si y sólo si $\text{mcd}(r, \varphi(n)) = 1$. Puesto que $|SRR(\varphi(n))| = \varphi(\varphi(n))$, entonces n tiene $\varphi(\varphi(n))$ raíces primitivas.

□

El Corolario 5.11 y el Teorema 5.12 presuponen que el entero n tiene al menos una raíz primitiva. Hasta ahora sabemos que cualquier potencia positiva de un primo p tiene raíces primitivas ¿Habrá otros enteros que tengan raíces primitivas? Un cálculo muy simple demuestra que los enteros 2 y 4 tienen raíces primitivas.

Teorema 5.13. *Sea p un primo impar y a una raíz primitiva de p^k. Si a es impar, entonces a es una raíz primitiva de $2p^k$. Si a es par, entonces $a+p^k$ es una raíz primitiva de $2p^k$.*

Demostración: Usaremos la igualdad $\varphi(2p^k) = \varphi(2)\varphi(p^k) = \varphi(p^k)$. Observemos primero que

$$a^{\varphi(2p^k)} \equiv a^{\varphi(p^k)} \equiv 1 \pmod{p^k}.$$

Por otro lado, si a es impar, entonces $a^{\varphi(2p^k)}$ es impar y por lo tanto $a^{\varphi(2p^k)} \equiv 1 \pmod 2$. Usando el Teorema **??** tenemos que $a^{\varphi(2p^k)} \equiv 1 \pmod{2p^k}$. Por lo anterior $o_{2p^k}(a) \leq \varphi(2p^k)$. Si la desigualdad fuera estricta, puesto que $a^{o_{2p^k}(a)} \equiv 1 \pmod{2p^k}$ y $\mcd(2, p^k) = 1$, entonces por el Teorema **??** $a^{o_{2p^k}(a)} \equiv 1 \pmod{p^k}$ lo cual es absurdo. Por lo tanto $o_{2p^k}(a) = \varphi(2p^k)$.

Si a es par, entonces $a+p^k$ es impar y $(a+p^k)^{\varphi(2p^k)}$ es impar. Por lo tanto $(a+p^k)^{\varphi(2p^k)} \equiv 1 \pmod 2$. Por otro lado tenemos que $a + p^k \equiv a \pmod{p^k}$. Así

$$(a+p^k)^{\varphi(2p^k)} \equiv a^{\varphi(2p^k)} \equiv a^{\varphi(p^k)} \equiv 1 \pmod{p^k}.$$

Por lo tanto $(a+p^k)^{\varphi(2p^k)} \equiv 1 \pmod{2p^k}$ y así $o_{2p^k}(a+p^k) \leq \varphi(2p^k)$. Para mostrar la igualdad entre estos dos números usamos el argumento del caso a impar.

□

Hasta ahora hemos mostrado que los enteros $2, 4, p^k, 2p^k$ tienen raíces primitivas. La pregunta inmediata es ¿serán todos?

Teorema 5.14. *Sea $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, donde $p_i \neq p_j$ si $i \neq j$. Si n tiene una raíz primitiva, entonces $n = p_1^{\alpha_1}$ ó $r = 2$ y $n = 2p^\alpha$ con p_1 y p primos impares.*

Demostración: Sea a una raíz primitiva de $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$. Entonces

$$\mcd(a, n) = \mcd(a, p_i^{\alpha_i}) = 1 \quad \text{y} \quad o_n(a) = \varphi(n).$$

Por el Teorema de Euler **??** tenemos para $1 \leq i \leq r$ que

$$a^{\varphi(p_i^{\alpha_i})} \equiv 1 \pmod{p_i^{\alpha_i}}.$$

Consideremos en entero $M = \mcm(\varphi(p_1^{\alpha_1}), \ldots, \varphi(p_r^{\alpha_r}))$. Puesto que $\varphi(p_i^{\alpha_i}) \mid M$, entonces

$$a^{\varphi(p_i^{\alpha_i})} \equiv a^M \equiv 1 \pmod{p_i^{\alpha_i}},$$

para $1 \leq i \leq r$. También para $i \neq j$ tenemos $\mcd(p_i^{\alpha_i}, p_j^{\alpha_j}) = 1$. Por lo tanto

$$a^M \equiv 1 \pmod{n}.$$

Así que $\varphi(n) \leq M$. Por otro lado $\varphi(n) = \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2}) \cdots \varphi(p_r^{\alpha_r})$ implica

$$\varphi(n) = \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2}) \cdots \varphi(p_r^{\alpha_r}) \leq M \leq \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2}) \cdots \varphi(p_r^{\alpha_r}).$$

Lo anterior significa que

$$\varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2}) \cdots \varphi(p_r^{\alpha_r}) = M$$

y para $i \neq j$ necesariamente tenemos

$$\text{mcd}(\ \varphi(p_i^{\alpha_i}),\ \varphi(p_j^{\alpha_j})\ ) = \text{mcd}(\ p_i^{\alpha_i - 1}(p_i - 1),\ p_j^{\alpha_j - 1}(p_j - 1)\ ) = 1.$$

Observemos que $\varphi(p_i^{\alpha_i})$ es par si p_i es un primo impar. Por lo tanto, la condición

$$\text{mcd}(\ p_i^{\alpha_i - 1}(p_i - 1),\ p_j^{\alpha_j - 1}(p_j - 1)\ ) = 1$$

no se cumple a menos que $r = 1$ ó $r = 2$ y $n = 2p^{\alpha}$ con p un primo impar.

□

El teorema anterior nos dice que si $n \neq p^{\alpha}$ ó $n \neq 2p^{\alpha}$, para algún primo p impar, entonces n no tiene raíces primitivas. Sólo nos queda considerar el caso $n = 2^{\alpha}$ con $\alpha \geq 3$ y esto lo abordaremos en la lista de problemas.

5.1 La conjetura de Artin acerca de las raíces primitivas

Para un entero $n > 1$, el conjunto $\mathbb{Z}_n$ tiene una estructura aritmética muy interesante. Podemos sumar cualesquiera dos elementos de $\mathbb{Z}_n$ y luego reducir módulo n. Observamos que esta suma da por resultado un elemento de $\mathbb{Z}_n$. Si $\overline{i} \in \mathbb{Z}_n$, entonces $\overline{i} + \overline{n - i} = \overline{0}$. Podemos pensar que cualquier elemento de $\mathbb{Z}_n$ tiene un *inverso aditivo* donde el *neutro aditivo* está representado por los enteros que dejan residuo 0 al ser divididos por n. También observemos que cualquier elemento de $\mathbb{Z}_n$ es suma de $\overline{1}$'s. En el lenguaje de la Teoría de Grupos se dice que $\mathbb{Z}_n$ es un grupo cíclico con generador $\overline{1}$. En pocas palabras, un grupo G es cíclico, si existe $a \in G$ tal que cualquier elemento x de G se puede escribir como ra ó a^r, dependiendo de la operación de G. Al elemento a se le llama generador de G y suele escribirse $G = \langle a \rangle$. En nuestro caso, $\mathbb{Z}_n$ es un grupo cíclico con la *suma* de clases. Se puede mostrar que si $k \in \mathbb{Z}_n$ y $\text{mcd}(k, n) = 1$, entonces cualquier elemento $j \in \mathbb{Z}_n$ se puede escribir como $k + \cdots + k$. Lo anterior es cierto puesto que existen enteros x_0, y_0 tal que $1 = kx_0 + ny_0$. Por lo tanto $j = kx_0(j) + ny_0(j)$ y así

$$j = kx_0(j) + ny_0(j) \equiv kx_0(j) \equiv \underbrace{k + \cdots + k}_{x_0 j - \text{veces}} \pmod{n}$$

En pocas palabras, $\mathbb{Z}_n = \langle k \rangle$ es un grupo cíclico con la suma módulo n y tiene al menos $\varphi(n)$-generadores. Se puede mostrar que $\mathbb{Z}_n$ tiene exactamente

$\varphi(n)$-generadores. Ahora, la multiplicación módulo n hace que U_n sea un grupo abeliano, es decir, si $x, y \in U_n$, entonces $xy = yx$. Si multiplicamos dos residuos en U_n y reducimos módulo n, entonces obtenemos un elemento de U_n, i,e, U_n es cerrado bajo la multiplicación módulo n. El "neutro multiplicativo" en U_n es $\overline{1}$ y el "inverso multiplicativo" de $a \in U_n$ es la solución única de la congruencia $ax \equiv 1 \pmod{n}$.

La pregunta que surge ahora es: ¿existe $a \in U_n$ tal que cualquier elemento $x \in U_n$ es de la forma $x = a^r$? El Corolario 5.5 nos afirma que en el caso particular de $U_p = \mathbb{Z}_p^*$, existen raíces primitivas de p. En nuestro nuevo lenguaje, una raíz primitiva de n es un generador de U_n y según el Teorema 5.14, no cualquier U_n es cíclico. Resaltamos la discusión anterior reescribiendo el Teorema 5.14:

Teorema 5.15. *El grupo $U(n)$ es cíclico si y sólo si $n = 1, 2, 4, p^\alpha, 2p^\alpha$, donde p es un primo impar y $\alpha \in \mathbb{N}$.*

Fijemos nuestra atención en U_p. En la práctica, con la ayuda de una computadora, es relativamente fácil encontrar una raíz primitiva de p. Sólo hay un pequeño inconveniente, p debe ser menor que 2^{28}.

En general, las computadoras trabajan a fuerza bruta: éstas toman un entero a módulo p y primo relativo con p, calculan todas sus potencias hasta que, para cierto entero r, obtienen $a^r \equiv 1 \pmod{p}$. Luego verifican si $p - 1 = r$ y si la respuesta es afirmativa, entonces han encontrado una raíz primitiva de p. Seguramente hay formas más eficientes de realizar esta tarea. Sin embargo, en ejemplos concretos, sin importar la forma en que se calcula una raíz primitiva, no hay un patrón a seguir para diferentes valores de p.

Según Dickson [1], fue Lambert, en 1769 el primero en establecer, sin demostrarlo, que existe una raíz primitiva para cualquier primo p. Siguiendo a Dickson, Euler da una prueba errónea de este resultado y es el que introduce el término de raíz primitiva. El mismo Euler reconoció que no tenía un método para calcularlas.

Gauss en sus *Disquisitiones Arithmeticae* [**?**], interesado en los períodos de fracciones de la forma $\frac{1}{p}$, con p primo, observa que si la fracción decimal $\frac{1}{p}$ tiene período k, entonces k debe satisfacer la congruencia

$$10^k \equiv 1 \pmod{p},$$

donde k debe ser el menor entero con esta propiedad. Por ejemplo, si $p = 53$, entonces $\frac{1}{53} = 0.\overline{0188679245283}$ y 13 es el menor entero positivo con la propiedad $10^{13} \equiv 1 \pmod{53}$. Gauss se preguntaba qué tan frecuentemente el número 10 aparece como una raíz primitiva de p, cuando p varía sobre los números primos. Sin embargo no formuló una conjetura específica.

En 1927, Emil Artin conjeturó que si un entero a es diferente de -1 y no es un cuadrado, entonces a es una raíz primitiva para una infinidad de primos.

En la actualidad, esta conjetura no ha sido resuelta, sólo se conocen resultados parciales.

A continuación mencionaremos algunos resultados que son comprensibles en este momento.

En 1945 P. Erdös [**?**] demostró que si g es una raíz primitiva de p, entonces

$$g < p^{\frac{1}{2}}(\log(p))^{17}$$

para primos grandes. Desafortunadamente su resultado no funciona si el número de factores primos de $p-1$ es pequeño.

En 1967 C. Hooley [**?**] demostró la conjetura de Artin junto con alguna fórmula que cuenta primos con cierta propiedad. En su demostración considera cierta la Hipótesis de Riemann Generalizada. Esta hipótesis es una extensión natural de la conocida Hipótesis de Riemann y aún no ha sido demostrada. Una implicación importante del trabajo de Hooley es que si la conjetura de Artin es falsa, entonces la Hipótesis de Riemann también es falsa.

En 1982 A. Ecker [**?**] usa métodos de conteo para demostrar resultados elementales conocidos acerca de las raíces primitivas de un primo p. Entre otras cosas demuestra que 3 y 6 son raíces primitivas de p si $p = 16q + 1$, donde q es un primo impar.

En el bello artículo expositorio de M. Ram Murty [**?**], entre otras cosas, se concluye que alguno de los números 2, 3 ó 5 es una raíz primitiva de p, para una infinidad de primos p. Desafortunadamente no se concluye de que forma debe ser p. En la práctica, si se busca una raíz primitiva de algún primo p, primero se debe ensayar con $2, 3, 5$. Con suerte y alguno de estos funciona.

Las investigaciones más recientes acerca de la conjetura de Artin involucran principalmente cuestiones de densidad de primos. Debemos prevenir al lector que las técnicas y teorías utilizadas en casi cualquier trabajo que trate la conjetura de Artin, están fuera del alcance de este libro. Éstas corresponden a la teoría analítica de los números y este libro es de teoría de números algebraicos. En todo caso, al lector interesado le recomendamos leer [**?**].

5.2 El logaritmo discreto

Consideremos el grupo $U_p = \{1, 2, ..., p-1\}$. Sabemos que U_p contiene al menos un elemento g tal que si $y \in U_p$, entonces existe $x \in \mathbb{Z}$ y $y \equiv g^x \pmod{p}$. El número g no es otra cosa que una raíz primitiva de p. Supongamos que g, y son conocidos. El problema de encontrar x es conocido como *el problema del logaritmo discreto* por su similitud con una ecuación exponencial. ¿Vemos cúal es la complicación que aparece?

Ejemplo 5.16. *En la congruencia* $2^x \equiv 10 \pmod{11}$ *una solución es* $x = 5$. *Observamos que* 2 *es una raíz primitiva del primo* 11.

En la práctica, calcular potencias dado un módulo, es complicado computacionalmente hablando. Es por esta razón que las investigaciones en criptografía han decidido usar logaritmos discretos.

PROBLEMAS

1. Mostrar usando inducción que si a es un entero positivo impar y $k \geq 3$, entonces $a^{2^{k-2}} \equiv 1 \pmod{2^k}$. Concluir que si $k \geq 3$, entonces 2^k no tiene raíces primitivas ¿y si a es par?

2. Sea $1 \leq a \leq n-1$. Encontrar $o_n(a)$ para los valores $n = 5, 6, 11, 15, 32$.

3. Sea $n \geq 2$ y $a \in SRR(n)$. Mostrar que $\{a, a^2, ..., a^{o_n(a)}\}$ es un grupo con $o_n(a)$ elementos.

4. Sea b solución de la congruencia $ax \equiv 1 \pmod{n}$. Mostrar que $o_n(a) = o_n(b)$.

5. Sea p un número primo impar. Mostrar que $o_p(a) = 2$ si y sólo si $a \equiv -1 \pmod{p}$.

6. Sea p primo y $k \in \mathbb{N}$. Demostrar que:

   a) Si $p-1 \nmid k$, entonces $\sum_{i=1}^{p-1} i^k \equiv 0 \pmod{p}$.

   b) Si $p-1 \mid k$, entonces $\sum_{i=1}^{p-1} i^k \equiv -1 \pmod{p}$.

7. Teorema de Wilson con raíces primitivas. Sea g una raíz primitiva de un primo p. Para $k = 0, 1, ..., p-1$, las potencias g^k satisfacen $(p-1)! = 1 \cdot 2 \cdot (p-1) \equiv g^{\frac{p-1}{2}} \pmod{p}$. Usar el Pequeño Teorema de Fermat **??** para justificar que $g^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.

8. Mostrar que si $\text{mcd}(o_n(a), o_n(b)) = 1$, entonces $o_n(ab) = o_n(a)o_n(b)$. Si $\text{mcd}(\, o_n(a), o_n(b)\,) > 1$ ¿será cierto que $o_n(ab) = o_n(a)o_n(b)$? ¿si $o_n(ab) = o_n(a)o_n(b)$, entonces $\text{mcd}(\, o_n(a), o_n(b)\,) = 1$?

9. Método para encontrar raíces primitivas de un primo p. Sea $\varphi(p) = q_1^{\beta_1} \cdots q_s^{\beta_s}$. Según el Teorema 5.9 existe a_i raíz primitiva de $q_i^{\beta_i}$. Demostrar que $a = a_1 \cdots a_s$ es una raíz primitiva de p. ¿Cuál es el inconveniente de este método?

10. Usar el problema anterior para encontrar una raíz primitiva de 17.

11. Sea p un primo de la forma $4n+1$ y a una raíz primitiva de p. Mostrar que $-a$ es una raíz primitiva de p.

12. Mostrar que si a es un residuo cuadrático de un primo impar p, entonces a no es una raíz primitiva de p.

13. Sea $p = 2q+1$ un primo con q primo impar. Mostrar que existen q residuos no cuadráticos y $q-1$ raíces primitivas módulo p. Concluir que las raíces primitivas son exactamente los no residuos cuadráticos con una excepción, $2q$.

14. Usar el problema 11 para encontrar las raíces primitivas de $p = 23, 47$.

15. Los números primos $p = 113$, 593 son de la forma $p = 16q + 1$. Verificar que 3 y 6 son una raíz primitiva para cada uno de ellos.

16. Encontrar todos los números primos ≤ 100 para los cuales 2, 3 ó 5 es una raíz primitiva.

17. Usar el Teorema 5.9 para demostrar que si a es una raíz primitiva de p^2, entonces a es una raíz primitiva de p^k para todo $k \geq 2$.

18. ¿Será cierto que si a es una raíz primitiva de p^2, entonces a es una raíz primitiva de p?

19. Sea $p = 3, 5, 7, 11, 13, 17, 19, 23$. Mostrar que si a es una raíz primitiva de p, entonces a es una raíz primitiva de p^2.

20. Considere un número primo $p \neq 2, 5$. Supongamos que la expansión decimal de $\dfrac{1}{p} = 0.\overline{a_1 a_2 \ldots a_r}$ tiene período r. Mostrar que $\dfrac{1}{p} = \dfrac{A}{10^r - 1}$. Sugerencia: La serie $\displaystyle\sum_{i=0}^{\infty} (10^{-r})^i$ converge. Usando lo anterior, demostrar que r es el menor entero positivo tal que $10^r \equiv 1 \pmod{p}$. En el lenguaje que hemos desarrollado en esta sección tenemos que $o_p(10) = r$. Problemas similares a éstos pensaba Gauss cuando se preguntó qué tan frecuentemente el número 10 es una raíz primitiva de p si p corre sobre el conjunto de números primos. Por ejemplo, 10 es raíz primitiva de $p = 7, 17, 19, 23, 29$.

21. Observar que los números primos 23 y 47 satisfacen $47 = 2 \cdot 23 + 1$. Demostrar que $(-1)^{\frac{23-1}{2}} \cdot 2 = -2$ es una raíz primitiva de 47. En general, demostrar que si p y $2p + 1$ son primos impares, entonces $(-1)^{\frac{p-1}{2}} \cdot 2$ es una raíz primitiva de $2p + 1$.

22. Encontrar una raíz primitiva para los primos $p = 7, 13, 29$.

23. Sea g una raíz primitiva para los primos del problema anterior. Resolver las siguientes congruencias:

    a) $g^x \equiv 25 \pmod{p}$.

    b) $g^x \equiv -1 \pmod{p}$.

    c) $g^x \equiv 4 \pmod{p}$.

d) $g^x \equiv -9 \pmod{p}$.

Bibliografía

[1] Dickson L. E., *History of the theory of numbers*, Vol. 1, Chelsea 1971.

[2] Hardy G.H., Wright E.M. *An introduction to the theory of numbers*. Oxford University Press 1979.

[3] Mathews G.B., *Theory of Numbers*, Cambridge, 1892.

[4] Nagell T. *Number theory*. Chelsea 1964.

[5] Morales Guerrero L.E., Rzedowski Calderón M., *Contando sobre números*. Avance y Perspectiva CINVESTAV-IPN vol. **18** (1999).

[6] Stark M.H., *An introduction to number theory*. MIT Press (1978).

[7] Zaldivar Cruz F., Fundamentos de álgebra, Editado por Fondo de Cultura Económica-Universidad Autónoma Metropolitana 2005.