Capítulo 3

Congruencias

3.1. Clases residuales

En su obra Disquisitiones Arithmeticae, publicada en el año 1801, Gauss introdujo el concepto de congruencia.

Supongamos que a, b y $m > 0$ son números enteros. Diremos que a y b son congruentes módulo m si m divide a $a - b$ y designaremos esta situación mediante el símbolo $a \equiv b \pmod{m}$.

La congruencia es una relación de equivalencia puesto que verifica las propiedades reflexiva, simétrica y transitiva. Esto nos permite agrupar a los enteros en familias disjuntas de manera que dos números son congruentes módulo m si y sólo si están en la misma. Estas familias se denominan clases residuales módulo m, y se designa por $\mathbb{Z}_m$ al conjunto formado por ellas.

De la definición anterior se deducen inmediatamente las siguientes propiedades.

Proposición 3.1.1. *Si* $a \equiv b \pmod{m}$ *y* $c \equiv d \pmod{m}$, *entonces*

i) $a + b \equiv c + d \pmod{m}$.

ii) $ka \equiv kb \pmod{m}$ *para todo entero* $k \in \mathbb{Z}$.

iii) $ac \equiv bd \pmod{m}$.

iv) $a^n \equiv b^n \pmod{m}$

v) $f(a) \equiv f(b) \pmod{m}$ *para todo polinomio* f *con coeficientes enteros.*

Los enteros $0, 1, \ldots, m - 1$ están en clases residuales distintas. Como todo entero n puede escribirse de manera única de la forma $n = mc + r$ con c entero

y $0 \leq r \leq m-1$, resulta que todo entero es congruente módulo m con uno de los enteros $0, 1, \ldots, m-1$. En particular existen exactamente m clases residuales módulo m y cualquier conjunto de enteros incongruentes módulo m constituyen un sistema residual completo.

El conjunto $\mathbb{Z}_m,\ m \geq 2$, dotado de las operaciones suma y producto emanadas de la proposición anterior es un anillo conmutativo cuyo elemento neutro aditivo, clase 0, es $0 = (m) = m\mathbb{Z}$ y cuya unidad multiplicativa es $1 + (m)$.

Proposición 3.1.2. *Si $\{a_1, \ldots, a_m\}$ es un sistema residual completo y $(k, m) = 1$, entonces el conjunto $\{ka_1, \ldots, ka_m\}$ también es un sistema residual completo.*

Demostración. Si $ka_i \equiv ka_j \pmod{m}$ entonces $m \mid k(a_i - a_j)$. Pero al ser k y m primos entre sí, necesariamente $m \mid (a_i - a_j)$. Es decir, los ka_i son incongruentes entre sí módulo m y por lo tanto forman un sistema residual completo. □

De una manera análoga podemos definir un sistema residual reducido como todo conjunto de $\phi(m)$ residuos incongruentes módulo m, cada uno de ellos primo con m. De manera similar se demuestra la siguiente proposición.

Proposición 3.1.3. *Si $\{a_1, \ldots, a_{\phi(m)}\}$ es un sistema residual reducido y $(k, m) = 1$, entonces el conjunto $\{ka_1, \ldots, ka_m\}$ también es un sistema residual reducido.*

Se designa por $\mathbb{Z}_m^*$ al conjunto de las clases residuales primas con m. Es fácil ver que constituyen un grupo multiplicativo de orden $\phi(m)$.

3.2. Congruencias lineales

En esta sección intentaremos resolver la ecuación en congruencias más sencilla de todas: la congruencia lineal.

Teorema 3.2.1. *Si $(a, m) = 1$, la congruencia $ax \equiv b \pmod{m}$ tiene exactamente una solución módulo m.*

Demostración. Por la proposición 3.1.2, el conjunto $\{a, 2a, \ldots, ma\}$ es un sistema residual completo. En particular uno y sólo uno de los residuos será congruente con b módulo m. □

Lema 3.2.2. *Si $ac \equiv bc \pmod{m}$ y $d = (m, c)$, entonces $a \equiv b \pmod{m/d}$.*

Demostración. Como $m \mid c(b-a)$, entonces $(m/d) \mid (c/d)(a-b)$. Pero como $(m/d, c/d) = 1$, entonces $(m/d) \mid a - b$. □

Teorema 3.2.3. *Supongamos que* $(a, m) = d$. *Si* $d \nmid b$ *la congruencia*

$$ax \equiv b \pmod{m}$$

no tiene soluciones, mientras que si $d \mid b$ *la congruencia tiene exactamente* d *soluciones módulo* m *que vienen dadas por*

$$x_1, x_1 + m_1, \ldots, x_1 + (d-1)m_1,$$

donde $m_1 = m/d$, $a_1 = a/d$, $b_1 = b/d$ *y* x_1 *es la solución de la congruencia* $a_1 x \equiv b_1 \pmod{m_1}$.

Demostración. Si la congruencia tiene alguna solución entonces, como $d \mid a$ y $d \mid m$, necesariamente d tiene que dividir a b.

Cualquier solución x de $ax \equiv b \pmod{b}$ debe serlo también de $a_1 x \equiv b_1 \pmod{m_1}$. Pero como $(a_1, m_1) = 1$ la solución x_1 es única módulo m_1. Sin embargo la clase residual módulo m_1 a la que pertenece x_1 consta de d clases residuales distintas módulo m: las clases a las que pertenecen los números $x_1, x_1+m_1, \ldots, x_1+(d-1)m_1$. Por lo tanto la congruencia $ax \equiv b \pmod{m}$ tiene exactamente las d soluciones descritas en el enunciado. □

El teorema anterior nos muestra cmo las congruencias lineales se reducen a resolver congruencias donde el módulo y el coeficiente de la x son primos entre sí.

La manera más económica de resolver esta la congruencia $ax \equiv b \pmod{m}$ con $(a, m) = 1$ consiste en resolver primero la ecuación $ax \equiv 1 \pmod{m}$ utilizando el algoritmo de Euclides y multiplicar dicha solución por b.

Ejemplo: Resolver la ecuación $51x \equiv 27 \pmod{123}$.

Observemos primero que $(51, 123) = 3$ y que 3 divide a 27. Luego esta congruencia tendrá exactamente 3 soluciones que serán $x_1, x_1 + 41, x_1 + 82$ donde x_1 es la solución de la congruencia $17x \equiv 9 \pmod{41}$. Para resolver esta congruencia resolvemos primero la congruencia $17x \equiv 1 \pmod{41}$ con el algoritmo de Euclides:

$$\begin{aligned} 41 &= 2 \cdot 17 + 7 \\ 17 &= 2 \cdot 7 + 3 \\ 7 &= 2 \cdot 3 + 1 \end{aligned}$$

Yendo hacia atrás tenemos que $1 = 7 - 2 \cdot 3 = 7 - 2(17 - 2 \cdot 7) = 5 \cdot 7 - 2 \cdot 17 = 5(41 - 2 \cdot 17) - 2 \cdot 17 = 5 \cdot 41 - 12 \cdot 17$. Es decir, $17 \cdot (-12) \equiv 1 \pmod{41}$ y por lo tanto $17 \cdot (-12 \cdot 9) \equiv 9 \pmod{41}$.

Luego $x_1 \equiv -108 \equiv 15 \pmod{41}$, y las tres soluciones de la congruencia original son $15, 56$ y 97.

Teorema 3.2.4 (Euler-Fermat)**.** *Si* $(a, m) = 1$*, entonces* $a^{\phi(m)} \equiv 1 \pmod{m}$.

Demostración. Sea $r_1, \ldots, r_{\phi(m)}$ un sistema residual reducido módulo m. Entonces, por la proposición 3.1.3, $ar_1, \cdots, ar_{\phi(m)}$ es también un sistema residual reducido módulo m. Los productos de todos los elementos en cada sistema tienen que coincidir módulo m,

$$r_1 \cdots r_{\phi(m)} \equiv a^{\phi(m)} r_1 \cdots r_{\phi(m)} \pmod{m}$$

y como $r_1 \cdots r_{\phi(m)}$ es primo con m, podemos cancelarlo (ver lema 3.2.2) para obtener $a^{\phi(m)} \equiv 1 \pmod{m}$. □

Teorema 3.2.5 (Fermat)**.** *Para todo primo* p *y para todo entero* a *tal que* $(a, p) = 1$*, se verifica la congruencia* $a^{p-1} \equiv 1 \pmod{p}$.

Demostración. Basta con observar que $\phi(p) = p - 1$. □

El teorema de Euler-Fermat nos proporciona la solución explícita $x = ba^{\phi(m)-1}$ para la congruencia $ax \equiv b \pmod{m}$ cuando $(a, m) = 1$.

En el ejemplo anterior tendríamos que $x_1 \equiv 9 \cdot 17^{39} \pmod{41}$. Para calcular $17^{39} \pmod{41}$ calculamos

$$\begin{aligned}
17^{2^0} &\equiv 17 \pmod{41} \\
17^{2^1} &\equiv 2 \pmod{41} \\
17^{2^2} &\equiv 4 \pmod{41} \\
17^{2^3} &\equiv 16 \pmod{41} \\
17^{2^4} &\equiv 10 \pmod{41} \\
17^{2^5} &\equiv 18 \pmod{41}
\end{aligned}$$

y como $39 = 2^5 + 2^2 + 2^1 + 2^0$ entonces $17^{39} \equiv 18 \cdot 4 \cdot 2 \cdot 17 \equiv 29 \pmod{41}$. Luego $x_1 \equiv 29 \cdot 9 \equiv 15 \pmod{41}$ y a partir de aquí se procede como antes.

Se advierte y se aconseja utilizar el algoritmo de Euclides para resolver las congruencias lineales por ser un método más sencillo y eficiente que este que acabamos de ver.

3.3. Congruencias polinómicas. Teorema de Lagrange

El estudio de congruencias polinómicas de grado superior resulta más complicado. Únicamente para las congruencias de grado 2 existe un método razonable (que se verá en el siguiente capítulo) para decidir cuándo tienen solución.

Cuando el módulo es primo tenemos, sin embargo, el siguiente teorema.

Teorema 3.3.1 (Lagrange)**.** *Dado un primo p, sea $f(x) = c_0 + c_1x + \cdots + c_nx^n$ un polinomio de grado n con coeficientes enteros tal que $p \nmid c_n$. Entonces la congruencia polinómica $f(x) \equiv 0 \pmod{p}$ tiene, a lo más, n soluciones.*

Demostración. Vamos a proceder por inducción sobre el grado del polinomio.

El caso $n = 1$ ha sido estudiado anteriormente. La congruencia $c_0 + c_1x \equiv 0 \pmod{p}$ tiene una solución si $(c_1, p) = 1$.

Hagamos la hipótesis de que el teorema es cierto para $n-1$: si x_1 es una solución de $c_0+\cdots+c_nx^n \equiv 0 \pmod{p}$, la ecuación $c_1(x-x_1)+\cdots+c_n(x^n-x_1^n) \equiv 0 \pmod{p}$ debe ser verificada por cualquier otra solución.

Es decir, existen enteros $a_2, a_3, \ldots, a_n$ tales que

$$(x - x_1)(c_nx^{n-1} + a_2x^{n-2} + \cdots + a_n) \equiv 0 \pmod{p}$$

debe ser satisfecha por todas las soluciones de nuestra ecuación.

Como p es primo, las soluciones distintas de x_1 deben serlo también de $c_nx^{n-1} + a_2x^{n-2} + \cdots + a_n \equiv 0 \pmod{p}$ y, por hipótesis de inducción, existen, a lo sumo, $n - 1$ soluciones de esta ecuación, lo cual completa la demostración del teorema de Lagrange. □

Corolario 3.3.2. *Si la congruencia*

$$c_nx^n + c_{n-1}x^{n-1} + \cdots + c_0 \equiv 0 \pmod{p}$$

tiene más de n soluciones, entonces los coeficientes $c_0, c_1, \ldots, c_n$ deben ser múltiplos de p.

Demostración. Supongamos que no es cierto y sea r el mayor entero tal que $p \nmid c_r$. La congruencia del corolario es equivalente a la congruencia $c_rx^r + \cdots + c_0 \equiv 0 \pmod{p}$, que tiene a lo más r soluciones. La contradicción surge porque estamos suponiendo que tiene por lo menos $n + 1$ soluciones. □

Teorema 3.3.3 (Wilson)**.**

$$(p - 1)! + 1 \equiv 0 \pmod{p}.$$

Demostración. Consideremos la congruencia

$$(x - 1)(x - 2)\cdots(x - (p - 1)) - (x^{p-1} - 1) \equiv 0 \pmod{p}.$$

El grado de esta congruencia es $p - 2$ y, sin embargo, tiene $p - 1$ soluciones por el teorema de Euler-Fermat. Por lo tanto, todos los coeficientes deben ser múltiplos de p y en particular el término independiente. □

Observación: Toda congruencia de la forma

$$a_n x^n + \cdots + a_0 \equiv 0 \pmod{p}$$

es equivalente a una de grado menor o igual que $p-1$. Para verlo basta con aplicar el teorema de Fermat $x^p \equiv x \pmod{p}$.

3.4. Congruencias simultaneas. Teorema Chino del resto

A continuación vamos a cambiar de tercio y en vez de una sola congruencia vamos a considerar un sistema de ellas.

Teorema 3.4.1 (Chino del resto)**.** *Si los números $m_1, \ldots, m_k$ son primos entre sí, entonces el sistema*

$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{m_2} \\ \cdots \\ x \equiv b_k \pmod{m_k} \end{cases}$$

tiene una única solución módulo $m = m_1 \cdots m_k$ y ésta viene dada por

$$x' = M_1 M_1' b_1 + \cdots + M_k M_k' b_k,$$

donde para todo $j = 1, \ldots, k$, $M_j = m/m_j$ y M_j' es el inverso de M_j mdulo m_j.

Demostración. Es claro que $x' \equiv M_j M_j' b_j \equiv b_j \pmod{m_j}$ para todo j, ya que M_i' es un múltiplo de m_j para $i \neq j$ y $M_j M_j' \equiv 1 \pmod{m_j}$.

Por otra parte, si x es otra solución del sistema entonces $x \equiv x' \pmod{m_j}$ para todo j y, como los números $m_1, \ldots, m_k$ son primos entre sí, resulta que $x \equiv x' \pmod{m}$.

□

Veamos ahora una aplicación del teorema chino del resto para resolver congruencias polinmicas donde el módulo es compuesto.

Teorema 3.4.2. *Sea $m = m_1 \cdots m_k$ con $(m_i, m_j) = 1$ para $i \neq j$. El número de soluciones de la congruencia*

$$a_n x^n + \cdots + a_0 \equiv 0 \pmod{m}$$

es el producto del nmero de soluciones de cada una de las congruencias

$$a_n x^n + \cdots + a_0 \equiv 0 \pmod{m}_j, \ j = 1, \ldots, k.$$

Demostración. En primer lugar es claro que cada solución de la congruencia mdulo m satisface cada una de las congruencias mdulo $m_j,\ j = 1, \ldots, k$.

Por otro lado, si para cada k-upla $(r_1, \ldots, r_k)$ donde r_j es una solución de la congruencia $a_n x^n + \cdots + a_0 \equiv 0 \pmod{m)_j}$ y si x es la solución del sistema

$$\begin{cases} x \equiv r_1 \pmod{m_1} \\ \cdots \\ \cdots \\ x \equiv r_k \pmod{m_k} \end{cases}$$

dada por la proposición anterior, entonces

$$a_n x^n + \cdots + a_0 \equiv a_n r_j^n + \cdots + a_0 \equiv 0 \pmod{m_j}$$

para todo j y, por tanto,

$$a_n x^n + \cdots + a_0 \equiv 0 \pmod{m_1 \cdots m_k}.$$

El número de k-uplas $(r_1, \ldots, r_k)$ es precisamente el producto del número de soluciones de la congruencia $a_n x^n + \cdots + a_0 \equiv 0 \pmod{m)_j}$ ara cada $j = 1, \ldots, k$ y cada una de ellas da lugar a una solución distinta de la congruencia original. □

Ejemplo: Para resolver $x^3 + 2x - 3 \equiv 0 \pmod{45}$ escribimos el sistema

$$\begin{cases} x^3 + 2x - 3 \equiv 0 \pmod{5} \\ x^3 + 2x - 3 \equiv 0 \pmod{9} \end{cases}.$$

La primera de estas ecuaciones tiene soluciones $x = 1, 3, 4$ módulo 5 y la segunda $x = 1, 2, 6$ módulo 9.

Por lo tanto, la ecuación $x^3 + 2x - 3 \equiv 0 \pmod{45}$ tiene 9 soluciones. Para encontrarlas teneos que resolver los 9 sistemas

$$\begin{cases} x \equiv a \pmod{5} \\ x \equiv b \pmod{9} \end{cases} \qquad a = 1, 3, 4 \qquad b = 1, 2, 6.$$

Utilizando el Teorema Chino del resto se halla fácilmente que las soluciones son $x = 1, 6, 11, 19, 28, 29, 33, 34, 38 \pmod{45}$.

Según lo visto hasta ahora, el problema de encontrar las soluciones de

$$P(x) = a_n x^n + \cdots + a_0 \equiv 0 \pmod{p_1^{\alpha_1} \cdots p_r^{\alpha_r}}$$

queda reducido a estudiar congruencias de la forma $P(x) \equiv 0 \pmod{p^\alpha}$, donde p es un número primo.

A continuación vamos a presentar una estrategia que nos permite reducir dicho estudio al caso sencillo $\alpha = 1$.

Si

$$f(a) \equiv 0 \pmod{p^\alpha}, \qquad 0 \leq a < p^\alpha,$$

entonces $f(a) \equiv 0 \pmod{p^{\alpha-1}}$ y a será de la forma $a = qp^{\alpha-1} + r$ con $0 \leq r < p^{\alpha-1}$ para algún q, $0 \leq q < p$.

Claramente $f(a) \equiv f(r) \equiv 0 \pmod{p^{\alpha-1}}$ y decimos que r ha sido generado por a.

Es decir, cada solución de $f(x) \equiv 0 \pmod{p^\alpha}$ genera otra de $f(x) \equiv 0 \pmod{p^{\alpha-1}}$.

Pero precisamente estamos buscando el proceso contrario. Si $f(r) \equiv 0 \pmod{p^{\alpha-1}}$, ¿cuándo existe un a tal que $f(a) \equiv 0 \pmod{p^\alpha}$ y que genere r? Cuando esto ocurra diremos que r puede subirse de $p^{\alpha-1}$ a p^α.

Teorema 3.4.3. *Sea $\alpha \geq 2$ y r una solución de*

$$f(x) \equiv 0 \pmod{p^{\alpha-1}}, \quad 0 \leq r < p^{\alpha-1.}$$

a) Si $f'(r) \not\equiv 0 \pmod{p}$, entonces r se sube de manera única de $p^{\alpha-1}$ a p^α.

b) $f'(r) \equiv 0 \pmod{p}$

b_1) Si $f(r) \equiv 0 \pmod{p^\alpha}$, entonces r puede subirse de $p^{\alpha-1}$ a p^α de p formas diferentes.

b_2) Si $f(r) \not\equiv 0 \pmod{p^\alpha}$, entonces r no puede subirse de $p^{\alpha-1}$ a p^α.

Demostración. Si a genera r, a tiene que ser de la forma

$$a = r + qp^{\alpha-1}, \quad 0 \leq r < p^{\alpha-1}, \quad 0 \leq q < p$$

y además $f(a) \equiv 0 \pmod{p^\alpha}$.

Por lo fórmula de Taylor en el punto r tenemos

$$f(r + qp^{\alpha-1}) = f(r) + qp^{\alpha-1}f'(r) + (qp^{\alpha-1})^2\frac{f''(r)}{2} + \cdots$$

Observemos que todos los sumandos a partir del tercero son múltiplos de p^α. Luego

$$0 \equiv f(r + qp^{\alpha-1}) \equiv f(r) + qp^{\alpha-1}f'(r) \pmod{p^\alpha}.$$

Como $f(r) = kp^{\alpha-1}$ para algún entero k, deberemos encontrar q tal que

$$k + qf'(r) \equiv 0 \pmod{p}.$$

Si $f'(r) \not\equiv 0 \pmod{p}$ dicho q existe y es único y por tanto r puede subirse de manera única.

Si $f'(r) \equiv 0 \pmod{p}$ y $f(r) \equiv 0 \pmod{p^\alpha}$ entonces $p \mid k$ y $k + qf'(r) \equiv 0 \pmod{p}$ para todo $q,\ 0 \leq q < p$. Es decir, r se puede subir de p maneras diferentes.

Si $f'(r) \equiv 0 \pmod{p}$ y $f(r) \not\equiv 0 \pmod{p^\alpha}$ entonces $p \nmid k$ y r no se puede subir porque no existe ningún q tal que $k + qf'(r) \equiv 0 \pmod{p}$. □

EJEMPLO. Hallar las soluciones de la congruencia $x^3 - x^2 + 3x + 1 \equiv 0 \pmod{121}$.

Como $121 = 11^2$, primero buscamos las soluciones de la congruencia $f(x) \equiv 0 \pmod{11}$ donde $f(x) = x^3 - x^2 + 3x + 1$. Se comprueba a mano que las nicas soluciones son $r_1 = 2$ y $r_2 = 8$. Veamos si estas soluciones se pueden subir de $\pmod{11}$ a $\pmod{121}$.

Calculamos $f'(x) = 3x^2 - 2x + 3$. Entonces $f'(2) = 11 \equiv 0 \pmod{11}$ y $f'(8) = 179 \equiv 3 \pmod{11}$.

La solucin 8 $\pmod{11}$ se puede subir de manera única y la solución $\pmod{11}$ será $a = 8 + 11q$ donde q es un entero tal que $k + qf'(8) \equiv 0 \pmod{11}$ y k se define como $k = f(8)/11 = 473/11 = 43$. Finalmente la congruencia $43 + 3q \equiv 0 \pmod{11}$ tiene como solución $q = 4$. Así que $a = 52$ es la solución $\pmod{121}$ que se sube desde la solución 8 $\pmod{11}$.

La solucin 2 $\pmod{11}$ se puede subir de 11 maneras. La razn es que $f(2) \equiv f'(2) \equiv 0 \pmod{11}$. Siguiendo el teorema anterior, las 11 maneras corresponden a las soluciones $a = 2 + 11q,\ 0 \leq q < 11$.

Hemos demostrado que la congruencia original tiene 12 soluciones y las hemos calculado todass.

3.5. Raíces primitivas

Supomgamos que $(a, m) = 1$. El teorema de Euler nos asegura que $a^{\phi(m)} \equiv 1 \pmod{m}$, pero es posible que $\phi(m)$ no sea necesariamente el entero positivo más pequeño x que verifica la ecuación $a^x \equiv 1 \pmod{m}$.

Definicion 3.5.1. *Dados dos números primos entre sí, a y m, llamaremos exponente de a módulo m al menor entero positivo e tal que* $a^e \equiv 1 \pmod{m}$. *Usaremos la notación* $e = \exp_m(a)$.

Claramente si $a \equiv b \pmod{m}$ se verifica que $\exp_m(a) = \exp_m(b)$. Esto nos permite considerar, indistintamente, exponentes de enteros o de clases residuales primas módulo m.

Teorema 3.5.2. *Si $e = exp_m(a)$ entonces los números $a^0, a^1, \ldots a^{e-1}$ son incongruentes entre sí módulo m.*

Además $a^k \equiv a^j \pmod{m}$ si y sólo si $k \equiv j \pmod{e}$; en particular $a^k \equiv 1 \pmod{m}$ si y sólo si k es divisible por e.

Demostración. Sean $k = c_1 e + r_1,\ j = c_2 e + r_2,\ 0 \leq r_1 \leq r_2 < e$ y supongamos que $a^k \equiv a^j \pmod{m}$. Entonces $a^{r_1} \equiv a^{r_2} \pmod{m}$, lo que implica que $a^{r_2 - r_1} \equiv 1 \pmod{m}$ y, por tanto, $r_1 = r_2$ debido a la propia definición del exponente e. □

Los números $\exp_m(a)$ son, por tanto, divisores del número $\phi(m)$.

Puede darse el caso de que exista g de manera que $\exp_m(g) = \phi(m)$. Es este un caso importante que recibe un nombre especial, se dice que g es una raíz primitiva módulo m.

La existencia de una raíz primitiva g es equivalente a que el grupo multiplicativo $\mathbb{Z}_m^*$ sea cíclico y generado por las potencias de g. Por ejemplo $g = 3$ es una raíz primitiva módulo 7: $\{3^1, 3^2, 3^3, 3^4, 3^5, 3^6\} = \{3, 2, 6, 4, 5, 1\}$. Sin embargo 2 no es raíz primitiva porque $exp_7(2) = 3$; es decir, $2^3 = 1$. .

A continuación vamos a caracterizar los módulos m para los que existen raíces primitivas.

Teorema 3.5.3. *Existen raíces primitivas módulo m si y sólo si $m = 1, 2, 4, p^k, 2p^k$, donde p designa a un número primo impar y $k \geq 1$.*

Demostración. Veremos primero que si m es de la forma $1, 2, 4, p^k$ o $2p^k$ con p primo impar, entonces $\mathbb{Z}_m^*$ es cíclico. Lo haremos en varios pasos:

(1) Los casos $m = 1, 2$ son triviales. $\mathbb{Z}_4^* = \{1, 3\}$ y es claro que 3 es una raíz primitiva.

(2) Consideremos ahora $\mathbb{Z}_p^*$ con p primo impar.

Sea $f(d) = \#\{a \in \mathbb{Z}_p^* :\ \exp_m(a) = d\}$, donde d es un divisor de $\phi(p) = p - 1$. Es claro que $\sum_{d|p-1} f(d) = p - 1$.

Por otro lado sabemos que $\sum_{d|p-1} \phi(d) = p - 1$. Si probamos la desigualdad $f(d) \leq \phi(d)$ para todo $d \mid p - 1$, las dos identidades anteriores fuerzan la igualdad $f(d) = \phi(d)$ para todo divisor de $p - 1$. En particular $f(p - 1) = \phi(p - 1)$. Es decir, existen $\phi(p - 1)$ raíces primitivas módulo p.

Para completar el argumento sólo nos queda demostrar la desigualdad $f(d) \leq \phi(d)$:

Dado $d \mid p-1$, si $f(d) \neq 0$ necesariamente existe un elemento $a \in \mathbb{Z}_p^*$ tal que $d = \exp_p(a)$ y, en particular, $a^d \equiv 1 \pmod{p}$.

La congruencia $x^d \equiv 1 \pmod{p}$ admite, a lo más, d soluciones módulo p y como la colección $1, a, \ldots, a^{d-1}$ la satisface y son, además, incongruentes entre sí módulo p, constituyen un conjunto completo de soluciones.

Sólo nos queda contar cuántas de entre ellas tienen exponente igual a d. Es claro que si $\exp_p(a^k) = d$ entonces $(k, d) = 1$ y, por tanto, su cardinal es a lo más $\phi(d)$ como queríamos demostrar.

(3) Sea g una raíz primitiva módulo p. Es claro que $g + tp$ es también una raíz primitiva módulo p cualquiera que sea el entero t.

Consideremos

$$\begin{aligned}(g+tp)^{p-1} &= g^{p-1} + (p-1)g^{p-2}tp + Ap^2 \\ &= 1 + sp - g^{p-2}tp + Bp^2 \\ &= 1 + p(s - gp^{p-2}t) + Bp^2,\end{aligned}$$

donde A, s, B son enteros y $g^{p-1} = 1 + sp$.

Podemos elegir el entero t de manera que $s - g^{p-2}t \not\equiv 0 \pmod{p}$, es decir, $(g+tp)^{p-1} = 1 + pu, \quad u \not\equiv 0 \pmod{p}$.

Vamos a probar que, con dicha elección, $g + tp$ es una raíz primitiva módulo p^k, para todo $k \geq 1$.

Supongamos que $(g+tp)^d \equiv 1 \pmod{p^k}$, siendo d un divisor de $\phi(p^k) = p^k(p-1)$.

Como $g^d \equiv 1 \pmod{p}$ y g es una raíz primitiva módulo p, d habrá de ser un múltiplo de $p-1$ y, por ser además un divisor de $pp^k(p-1)$ podemos suponer que tiene la forma $d = p^l(p-1)$ para algún l con $0 \leq l \leq k-1$.

Ahora bien, como

$$(g+tp)^{p^l(p-1)} = (1+up)^{p^l} = 1 + vp^{l+1}$$

para algún $v \not\equiv 0 \pmod{p}$, necesariamente tiene que ocurrir que $l = k-1$.

(4) En el caso restante, $m = 2p^k$, p primo impar, podemos proceder de la manera siguiente:

Sea g una raíz primitiva módulo p^k. Obviamente $g + p^k$ también lo es. Sea h el elemento impar del conjunto $\{g, g+p^k\}$. Vamos a ver que h es raíz primitiva módulo $2p^k$.

Como $h^{\phi(2p^k)} \equiv h^{\phi(p^k)} \equiv 1 \pmod{p^k}$ y obviamente $h^{\phi(2p^k)} \equiv 1 \pmod 2$, entonces $h^{\phi(2p^k)} \equiv 1 \pmod{2p^k}$.

Por otro lado, si d divide a $\phi(2p^k) = \phi(p^k)$ y es tal que $h^d \equiv 1 \pmod{2p^k}$, al ser h impar, también será cierto que $h^d \equiv 1 \pmod{p^k}$ y por tanto $g^d \equiv 1 \pmod{p^k}$. Pero como g es una raíz primitiva módulo p^k entonces $\phi(p^k) \mid d$, lo que implica que $d = \phi(2p^k)$. Luego h es una raíz primitiva.

Para concluir la demostración del teorema tenemos que probar que $\mathbb{Z}_m^*$ no es cíclico si m no es uno de los enteros considerados en los casos anteriores. Lo haremos en dos pasos.

(5) Caso $m = 2^k,\ k \geq 3$.

Es una consecuencia de la observación siguiente: Si a es un número impar, entonces $a^{\frac{\phi(2^n)}{2}} \equiv 1 \pmod{2^k}$.

Lo demostraremos por inducción en k. El caso $k = 3$ se comprueba directamente. Observemos que $\frac{\phi(2^3)}{2} = 2$ y que $1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \pmod{2^3}$.

Supongamos el resultado cierto para k: $a^{\frac{\phi(2^k)}{2}} = 1 + 2^k n$. Elevando ambos miembros al cuadrado obtenemos

$$a^{\phi(2^k)} = 1 + (n + n^2 2^{k-1})2^{k+1} \equiv 1 \pmod{2^{k+1}}.$$

Basta, pues, observar que $\phi(2^k) = 2^{k-1} = \frac{1}{2}\phi(2^{k+1})$.

(6) En el caso general $m = 2^k p_1^{a_1} \cdots p_r^{a_r}$, donde $k \geq 2$ si $r = 1$ y $r \geq 2$ si $k = 0$ o $k = 1$, también demostraremos que si $(a, m) = 1$ entonces $a^{\frac{\phi(m)}{2}} \equiv 1 \pmod m$.

Sea g una raíz primitiva módulo $p_1^{a_1}$, y sea n un entero positivo tal que $g^n \equiv a \pmod{p_1^{a_1}}$.

Tenemos que

$$a^{\frac{\phi(m)}{2}} \equiv g^{n\frac{\phi(m)}{2}} \equiv g^{\phi(p_1^{a_1})\frac{1}{2}n\phi(2^k)\phi(p_2^{a_2})\cdots\phi(p_r^{a_r})} \pmod{p_1^{a_1}}.$$

Es claro que bajo nuestras hipótesis sobre el número m, podemos afirmar que el exponente $\frac{1}{2}n\phi(2^k)\phi(p_2^{a_2})\cdots\phi(p_r^{a_r})$ es un entero.

En particular la congruencia anterior nos indica que

$$a^{\frac{\phi(m)}{2}} \equiv 1 \pmod{p_1^{a_1}}.$$

De manera análoga podemos probar que

$$a^{\frac{\phi(m)}{2}} \equiv 1 \pmod{p_i^{a_i}}, \qquad i = 1, \ldots, r.$$

Nos queda por probar que la congruencia anterior también se verifica para el módulo 2^k.

Si $k \geq 3$ aplicamos la misma demostración del caso (5) para obtener que

$$a^{\frac{\phi(2^k)}{2}} \equiv 1 \pmod{2^k}.$$

Y como $\frac{\phi(2^k)}{2}$ es un divisor de $\frac{\phi(m)}{2}$ habríamos acabado.

Si $k \leq 2$ tenemos que $\phi(m) = \phi(2^k)\phi(p_1^{a_1}) \cdots \phi(p_r^{a_r}) = 2n\phi(2^k)$ para algún entero n. Por tanto, también es cierto que

$$a^{\frac{\phi(m)}{2}} = a^{n\phi(2^k)} \equiv 1 \pmod{2^k},$$

como queríamos probar.

□

En el apartado (2) hemos observado que existen exactamente $\phi(p-1) = \phi(\phi(p))$ raíces primitivas módulo el primo impar p. Esto sigue siendo cierto para el caso general.

Sea g una raíz primitiva módulo m. Es claro que el conjunto

$$\{g^k : \ 1 \leq k \leq \phi(m), \ (k, \phi(m)) = 1\}$$

consiste, precisamente, de todas las raíces primitivas módulo m. Por lo tanto, si $m = 1, 2, 4, p^k$ ó $2p^k$, p primo impar, existen exactamente $\phi(\phi(m))$ raíces primitivas módulo m o, lo que es igual, el grupo cíclico $\mathbb{Z}_m^*$ tiene $\phi(\phi(m))$ generadores.

Observemos también que, fijada una raíz primitiva g módulo m, entonces $\{1, g, \ldots, g^{\phi(m)-1}\}$ es un sistema residual reducido módulo m.

Por lo tanto, dado a, primo con m, podemos asignarle un único número k, $\quad 0 \leq k \leq \phi(m) - 1$ de manera que $a \equiv g^k \pmod{m}$.

3.6. Ley de reciprocidad cuadrática

En el capítulo anterior hemos desarrollado con detalle la teoría de las congruencias lineales $ax + b \equiv 0 \pmod{m}$. Ahora vamos a considerar las congruencias cuadráticas $x^2 \equiv a \pmod{m}$.

Definicion 3.6.1. *Dada una clase residual prima módulo m, representada por el entero a, diremos que es un residuo cuadrático si la congruencia $x^2 \equiv a \pmod{m}$ tiene solución. En caso contrario diremos que a es un residuo no cuadrático.*

Es claro que el carácter cuadrático es independiente del representante elegido.

En lo sucesivo mantendremos la ambigüedad consistente en hablar de un entero particular como residuo cuadrático o residuo no cuadrático, en vez de mencionar a la clase residual que lo contiene.

Proposición 3.6.2. *Sea p un número primo impar. Existen exactamente $\frac{p-1}{2}$ residuos cuadráticos y $\frac{p-1}{2}$ residuos no cuadráticos módulo p.*

Demostración. Consideremos el siguiente sistema residual completo módulo p:

$$\left\{-\frac{p-1}{2}, \ldots, -1, 0, 1, \ldots, \frac{p-1}{2}\right\}.$$

Como $(-k)^2 = k^2$, existen, a lo más, $\frac{p-1}{2}$ residuos cuadráticos.

Por otro lado, la congruencia $k^2 \equiv j^2 \pmod{p},\ 1 \leq k, j \leq \frac{p-1}{2}$, necesariamente implica la igualdad $k = j$:

$(k-j)(k+j) \equiv 0 \pmod{p}$ implica que $k - j \equiv 0 \pmod{p}$ o bien $k + j \equiv 0 \pmod{p}$, lo que junto con la relación $1 \leq k, j \leq \frac{p-1}{2}$ nos da $k = j$.

Por lo tanto, los números $1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$ son incongruentes entre sí módulo p. □

Definicion 3.6.3. *Dado un número primo impar p, el símbolo de Legendre $\left(\frac{a}{p}\right)$ es la función aritmética definida de la forma siguiente:*

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{si } a \equiv 0 \pmod{p} \\ +1, & \text{si } a \text{ es un residuo cuadrático} \\ -1, & \text{si } a \text{ es un residuo no cuadrático} \end{cases}$$

Proposición 3.6.4 (Criterio de Euler)**.** *Sea p un número impar. Tenemos que*

$$\left(\frac{n}{p}\right) \equiv n^{\frac{p-1}{2}} \pmod{p}, \text{ para todo entero } n.$$

Demostración. Si $n \equiv 0 \pmod{p}$, entonces el resultado es inmediato.

Supongamos que $(n, p) = 1$. El Teorema de Fermat nos dice que $n^{p-1} \equiv 1 \pmod{p}$.

Es decir, $(n^{\frac{p-1}{2}} - 1)(n^{\frac{p-1}{2}} + 1) \equiv 0 \pmod{p}$ y por lo tanto, una de las dos relaciones siguientes debe ser verificada:

i) $n^{\frac{p-1}{2}} - 1 \equiv 0 \pmod{p}$.

ii) $n^{\frac{p-1}{2}} + 1 \equiv 0 \pmod{p}$.

Si $\left(\frac{n}{p}\right) = 1$, la ecuación $x^2 \equiv n \pmod{p}$ tiene solución. En particular $n^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \pmod{p}$: es decir, n verifica i): $n^{\frac{p-1}{2}} \equiv 1 = \left(\frac{n}{p}\right) \pmod{p}$.

Observemos que la ecuación $x^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ tiene como soluciones los $\frac{p-1}{2}$ residuos cuadráticos y que, por el teorema de Lagrange, no puede tener más soluciones.

Si $\left(\frac{n}{p}\right) = -1$, entonces n no es un residuo cuadrático y por tanto $n^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. Necesariamente $n^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. □

Corolario 3.6.5. *El símbolo de Legendre es, para cada primo p una función completamente multiplicativa.*

Demostración.

$$\left(\frac{mn}{p}\right) \equiv (mn)^{\frac{p-1}{2}} \equiv m^{\frac{p-1}{2}} n^{\frac{p-1}{2}} \equiv \left(\frac{m}{p}\right)\left(\frac{n}{p}\right) \pmod{p}.$$

Pero como los valores que toma el símbolo de Legendre son $+1, 0, -1$, necesariamente tenemos la igualdad

$$\left(\frac{mn}{p}\right) = \left(\frac{m}{p}\right)\left(\frac{n}{p}\right).$$

□

3.6.1. Cálculo de los símbolos $\left(\frac{-1}{p}\right)$ y $\left(\frac{2}{p}\right)$

Proposición 3.6.6. *Sea p un número impar. Tenemos que*

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

Demostración. Basta con aplicar el criterio de Euler y observar, como antes, que ambos miembros de la congruencia toman los valores $+1$ o -1 y, por tanto, la congruencia implica la igualdad. □

Proposición 3.6.7. *Para todo primo impar p tenemos la identidad:*

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

Demostración. Consideremos las $\frac{p-1}{2}$ congruencias siguientes:

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

donde r es $\frac{p-1}{2}$ ó $p - \frac{p-1}{2}$ según el caso.

Multipliquemos estos sistemas de congruencias y observemos que cada entero situado en los miembros de la parte izquierda es necesariamente par. Resulta que:

$$2 \cdot 4 \cdot 6 \cdots (p-1) \equiv \left(\frac{p-1}{2}\right)!(-1)^{1+2+\cdots+\frac{p-1}{2}} \pmod{p}.$$

Es decir,

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

Podemos dividir por $(\frac{p-1}{2})!$ para obtener

$$\left(\frac{2}{p}\right) \equiv 2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p^2-1}{8}} \pmod{p}$$

que, por la misma razón de la proposición anterior, implica la igualdad:

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

□

3.6.2. Ley de reciprocidad cuadrática

La ley de reciprocidad cuadrática fue descubierta por Euler en torno al año 1745. Gauss, a su vez, también la descubrió y produjo la primera demostración completa en 1796, varios años después de sus *Disquisitiones Arithmeticae*.

Hoy en día se conocen muchas demostraciones distintas. A continuación vamos a presentar una de las más sencillas conceptualmente, que está basada en el siguiente lema de Gauss.

Lema 3.6.8 (de Gauss)**.** *Sea p un primo impar y a un entero no divisible por él. Dado $x = 1, \ldots, \frac{p-1}{2}$, sea $ax \equiv \epsilon_x u_x \pmod{p}$, donde u_x es un entero del conjunto $\{1, 2, \ldots, \frac{p-1}{2}\}$ y $\epsilon_x = \pm 1$. Entonces*

$$\left(\frac{a}{p}\right) = \epsilon_1 \cdots \epsilon_{\frac{p-1}{2}}.$$

Demostración. En primer lugar observemos que dado $x,\ 1 \leq x \leq \frac{p-1}{2}$, tanto el entero $u_x,\ 1 \leq u_x \leq \frac{p-1}{2}$ como el número ϵ_x están unívocamente determinados por la relación

$$ax \equiv \epsilon_x u_x \pmod{p}.$$

En efecto, si $ax_1 \equiv u \pmod{p}$ y $ax_2 \equiv -u \pmod{p}$, entonces $a(x_1 + x_2) \equiv 0 \pmod{p}$, lo que es imposible por ser $1 \leq x_1, x_2 \leq \frac{p-1}{2}$.

Multiplicando las congruencias para cada $x,\ 1 \leq x \leq \frac{p-1}{2}$ obtenemos

$$a^{\frac{p-1}{2}} 1 \cdot 2 \cdots \left(\frac{p-1}{2}\right) \equiv \epsilon_1 \cdots \epsilon_{\frac{p-1}{2}} 1 \cdot 2 \cdots \left(\frac{p-1}{2}\right) \pmod{p}.$$

Es decir

$$a^{\frac{p-1}{2}} \equiv \epsilon_1 \cdots \epsilon_{\frac{p-1}{2}} \pmod{p}.$$

Basta entonces con aplicar el criterio de Euler para concluir la demostración del lema. □

Teorema 3.6.9 (Ley de reciprocidad cuadrática)**.** *Sean p y q números primos impares distintos. Tenemos que*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

Demostración. Sean $p = 2n + 1,\ q = 2m + 1$. Apliquemos el lema de Gauss para $a = q$ con respecto al conjunto $\{1, 2, \ldots, n\},\ n = \frac{p-1}{2}$.

Tenemos, para cada $x,\ 1 \leq x \leq n$,

$$qx \equiv \epsilon_x u_x \pmod{p} \text{ con } 1 \leq u_x \leq n, \qquad \epsilon_x \in \{-1, +1\}.$$

Es decir, $qx = \epsilon_x u_x + py$ donde ϵ_x, u_x, y están unívocamente determinados por estas condiciones cuando x está dado.

En particular ϵ_x toma el valor -1 si y sólo si

$$py = qx + u_x, \text{ con } 1 \leq u_x \leq n.$$

Ello implica que $y > 0$ y, además,

$$y \leq \frac{1}{p}(qx + u_x) \leq \frac{1}{p}(q+1)n < \frac{q+1}{2} = m + 1.$$

En otras palabras, $\epsilon_x = -1$ si y sólo si podemos fijar un y tal que la pareja (x, y) satisface las condiciones

$$\begin{cases} 1 \leq x \leq n \\ 1 \leq y \leq m \\ 1 \leq py - qx \leq n. \end{cases}$$

Consiguientemente, si N designa al número de tales parejas, el lema de Gauss nos dice que

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

Análogamente

$$\left(\frac{p}{q}\right) = (-1)^M,$$

donde M es el número de parejas (x, y) que verifican

$$\begin{cases} 1 \leq x \leq n \\ 1 \leq y \leq m \\ 1 \leq qx - py \leq m. \end{cases}$$

Ahora como p y q son primos entre sí y $1 \leq x < p$ entonces $qx - py$ no puede ser nunca cero y podemos escribir

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{M+N},$$

donde ahora $M + N$ es el número de parejas que satisfacen las condiciones

$$\begin{cases} 1 \leq x \leq n \\ 1 \leq y \leq m \\ -n \leq qx - py \leq m. \end{cases}$$

Sea S el número de parejas (x, y) tales que

$$\begin{cases} 1 \leq x \leq n \\ 1 \leq y \leq m \\ qx - py < -n. \end{cases}$$

Sea T el número de parejas (x', y') que verifican

$$\begin{cases} 1 \leq x' \leq n \\ 1 \leq y' \leq m \\ qx' - py' > m. \end{cases}$$

Entre estos conjuntos existe una correspondencia biyectiva dada por

$$\begin{cases} x' = n + 1 - x \\ y' = m + 1 - y. \end{cases}$$

Por lo tanto $S = T$. Por otro lado $M+N+S+T = mn$, entonces $(-1)^{M+N} = (-1)^{mn}$ y el teorema queda demostrado. □

3.6.3. Ejemplos y aplicaciones

La ley de reciprocidad cuadrática es uno de los resultados más notables de la Teoría de los Números: una relación sorprendente y a la vez sencilla entre las propiedades de las congruencias $x^2 \equiv q \pmod{p}$ y $x^2 \equiv p \pmod{q}$. Es también pieza importante de otras teorías aritméticas.

a) La ley de reciprocidad cuadrática nos permite calcular el valor de $\left(\frac{m}{p}\right)$ en muchos casos.

EJEMPLO: Supongamos que queremos estudiar si la congruencia $x^2 \equiv 315 \pmod{65537}$ tiene solución, sabiendo de antemano que 65537 es rimo.

Por supuesto podríamos ir comprobando todos los restos módulo 65537, pero la ley de reciprocidad cuadrática nos proporciona un método mucho más rápido. Recordemos que el símbolo de Legendre es una función multiplicativa.

$$\left(\frac{315}{65537}\right) = \left(\frac{3^2 \cdot 5 \cdot 7}{65537}\right) = \left(\frac{3^2}{65537}\right)\left(\frac{5}{65537}\right)\left(\frac{7}{65537}\right)$$
$$= \left(\frac{5}{65537}\right)\left(\frac{7}{65537}\right) = (-1)^{\frac{4 \cdot 65536}{4}}\left(\frac{65537}{5}\right)(-1)^{\frac{6 \cdot 65536}{4}}\left(\frac{65537}{7}\right)$$
$$= \left(\frac{2}{5}\right)\left(\frac{3}{7}\right) = (-1)(-1) = 1.$$

Es decir, la congruencia $x^2 \equiv 315 \pmod{65537}$ tiene solución. De hecho tiene exactamente dos soluciones pero la Ley de reciprocidad cuadrática no nos da una pauta para encontrarlas.

b) Otro ejemplo interesante de aplicaciones es el siguiente. Queremos saber para qué primos, la congruencia $x^2 \equiv 3 \pmod{p}$ tiene solución. Es decir, para qué valores de p se tiene que $\left(\frac{3}{p}\right) = 1$.

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

Como

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

y

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

resulta que

$$\left(\frac{3}{p}\right) = \begin{cases} +1 & \text{si } p \equiv \pm 1 \pmod{12} \\ -1 & \text{si } p \equiv \pm 5 \pmod{12}. \end{cases}$$

3.7. Ejercicios del capítulo 3

3.7.1. *Se ha escrito un número. Luego se ha escrito otro, permutando las cifras del primero. La diferencia de los dos números es* $391738X$ *¿Qué dígito es la última cifra representada por* X*?*

3.7.2. *Sea* S *un conjunto de* n *enteros no necesariamente distintos. Demostrar que algún subconjunto no vacío de* S *posee una suma divisible por* n*.*

3.7.3. *Demostrar que* $\sum_{k=1}^{n} k10^k$ *es múltiplo de* 3 *si y sólo si* $n \not\equiv 1 \pmod{3}$*.*

3.7.4. *Hallar el resto al dividir el número* 999 998 997 ...003 002 001 000 *entre* 13*.*

3.7.5. *El número* n *expresado en base* 2 *se escribe* 10010100111010100011*, Decir si es múltiplo de* 3*.*

3.7.6. *Probar el recíproco del teorema de Wilson: Si* $(n-1)! + 1 \equiv 0 \pmod{n}$*, entonces* n *es primo.*

3.7.7. *Demostrar que si* $n+2$ *es primo,* $n > 1$*, entonces* $n2^n + 1$ *no es primo.*

3.7.8. *Sea la función* $f(x,y) = \frac{y-1}{2}\{|B^2-1| - (B^2-1)\} + 2$ *donde* $B = x(y+1) + y! + 1$.

a) Demostrar que $f(x,y)$ *es primo para todo* $x, y \in \mathbb{Z}$.

b) Demostrar que para todo primo $p \neq 2$, *existen unos únicos* x *e* y *tales que* $f(x,y) = p$.

3.7.9. *Demostrar que para todo* $n \geq 3$,

$$\pi(n) = 1 + \sum_{j=3}^{n} \left\{ (j-2)! - j \left\lfloor \frac{(j-2)!}{j} \right\rfloor \right\}.$$

3.7.10. *Sean* a, b, x_0 *enteros positivos, y sea* $x_n = ax_{n-1} + b$ *para todo* $n \geq 1$. *Demostrar que* x_n *no puede ser primo para todo* n.

3.7.11. *D. José estudió en un colegio que tenía entre* 150 *y* 300 *colegiales. Ahora, aunque no recuerda el número de colegiales que eran, sí se queja de no haber podido practicar ni fútbol, ni baloncesto, ni balonmano porque, cuando en cada deporte se intentaba organizar el colegio en equipos, siempre faltaba o sobraba uno. ¿Podrías recordar a D.José cuántos colegiales eran?*

3.7.12. *Caracterizar los enteros* x *que satisfacen simultaneamente las congruencias* $x \equiv 7 \pmod{k}$, $2 \leq k \leq 10$. *¿Puede alguno de estos enteros ser un cuadrado?*

3.7.13. *Hallar todas las soluciones de la congruencia* $x^3 + 2x^2 - x + 6 \equiv 0 \pmod{98}$.

3.7.14. *Demostrar que si* $a^h \equiv 1 \pmod{n}$ *para todo* a, $(a,n) = 1$, *entonces* h *divide a* $\phi(n)$.

3.7.15. *Demostrar que el conjunto de puntos de coordenadas visibles desde el origen contiene cuadrados vacíos tan grandes como queramos.*

3.7.16. *Demostrar que* $a^{560} \equiv 1 \pmod{561}$ *para todo* a *con* $(a, 561) = 1$.

3.7.17. *Para cada entero positivo* n *encontrar la última cifra de* $13^{n!}$.

3.7.18. *Demostrar que existen infinitos enteros positivos que no son suma de tres cuadrados.*

3.7.19. *Sea* F_n *un número de Fermat y* p *un primo. Demostrar que si* p *divide a* F_n *entonces* $p = 2^{n+1}k + 1$ *para algún entero* k.

3.7.20. *Probar que todo entero satisface alguna de las congruencias*

$x \equiv 0 \pmod{2}$, $x \equiv 3 \pmod{3}$, $x \equiv 1 \pmod{4}$,

$x \equiv 3 \pmod{8}$, $x \equiv 7 \pmod{12}$, $x \equiv 23 \pmod{24}$.

3.7.21. *Sea g una raíz primitiva módulo p y sea $A = \{a_1, \ldots, a_{p-1}\}$ el subconjunto de $\mathbb{Z}_{(p-1)p}$ donde cada a_i se define como la única solución módulo $(p-1)p$ al sistema $x \equiv i \pmod{p-1},\ x \equiv g^i \pmod{p}$.*

Demostrar que A tiene la propiedad de que todas las diferencias $a_i - a_j,\ i \neq j$ son distintas. Demostrar también que no puede haber un conjunto A con p elementos que tenga esta misma propiedad.

3.7.22. *Demostrar que existen infinitos primos de la forma $4n + 1$.*

3.7.23. *Hallar los primos p para los cuales la ecuación $x^2 \equiv 5 \pmod{p}$ tiene solución.*

3.7.24. *a) Dar una condición necesaria y suficiente para que la progresión aritmética $an + b$ tenga infinitos cuadrados.*

b) Utilizar el apartado anterior para estudiar la existencia de infinitos cuadrados en la progresión $160 + 103n$.

3.7.25. *Dar una condición necesaria y suficiente, en función de a, b y c, para que la congruencia $ax^2 + bx + c \equiv 0 \pmod{p}$ tenga solución. Aplicar esto último para estudiar la existencia de soluciones de la congruencia $5x^2 - 13x + 8 \equiv 0 \pmod{37}$.*

3.7.26. *Caracterizar los primos para los que tiene solución la congruencia $5x^2 - 3x + 1 \equiv 0 \pmod{p}$.*

3.7.27. *Demostrar que para todo polinomio $Q(x) = ax^2+bx+c$, no constante, existen infinitos primos p para los que la congruencia $Q(x) \equiv 0 \pmod{p}$ tiene solución.*

3.7.28. *Demostrar que el producto de todos los residuos cuadráticos positivos y menores que p es congruente con $(-1)^{\frac{p+1}{2}} \pmod{p}$.*

3.7.29. *Demostrar que la congruencia $x^5 \equiv 300x \pmod{101}$ tiene una única solución.*

3.7.30. *Demostrar que la suma de tres cuadrados consecutivos no puede ser múltiplo de 19.*

3.7.31. *Demostrar que si $(x, y) = 1$ entonces $x^2 + y^2$ no es divisible por ningún primo $p \equiv 3 \pmod{4}$.*

3.7.32. *Demostrar que n puede escribirse como suma de dos cuadrados si y sólo si en su factorización en números primos,*

$$n = 2^{\nu} \prod_{p_j \equiv 1 \pmod 4} p_j^{\alpha_j} \prod_{q_k \equiv 3 \pmod 4} q_k^{\beta_k}$$

todos los β_k son pares.

3.7.33. *Considérese la congruencia* $x^2 \equiv p^t b \pmod{p^s}$ *con* p *primo impar,* $s \geq 1$, $(b, p) = 1$. *Probar que*

a) si $t \geq s$, *la congruencia tiene solución.*

b) si $t < s$, *la congruencia tiene solución si y sólo si* t *es par y* b *es un residuo cuadrático módulo* p.

3.7.34. *Probar que* $\sum_{x=1}^{p} \left(\frac{x}{p}\right)\left(\frac{x+1}{p}\right) = -1$ *si* p *es cualquier primo impar.*