Capítulo 2

Aritmética modular

2.1. Relaciones de congruencia y aritmética modular

Definición 2.1.1. Sean $a, b, n \in \mathbb{Z}$, con $n > 1$. Diremos que a es *congruente con b módulo n*, y lo denotaremos por $a \equiv b \pmod{n}$, si $a - b$ es múltiplo de n.

Ejemplo 2.1.2.

- $23 \equiv 17 \pmod{3}$, ya que $23 - 17 = 6 = 2 \cdot 3$.
- $-12 \equiv 14 \pmod{13}$, ya que $-12 - 14 = -26 = (-2) \cdot 13$.

Observación 2.1.3. Recordemos que, en el ejemplo 1.1.65, vimos que la relación de congruencia era una relación de equivalencia.

Teorema 2.1.4. *Sean $a, b, n \in \mathbb{Z}$, con $n > 1$. Entonces se verifica:*

1. *$a \equiv b \pmod{n}$ si, y solo si, a y b tienen el mismo resto al dividirlos entre n.*
2. *Cada entero $a \in \mathbb{Z}$ es congruente módulo n con uno de los siguientes enteros: 0,1,2,..., $n-1$.*

Denotaremos por $[a]_n$ al conjunto de enteros congruentes con a módulo n, y lo denominamos *clase de a módulo n*:

$$[a]_n = \{b \in \mathbb{Z} : a \equiv b \pmod{n}\}.$$

Por lo tanto, como consecuencia de la observación anterior,

$$a \equiv b \pmod{n} \iff [a]_n = [b]_n.$$

Por el teorema precedente, hay exactamente n clases módulo n y son disjuntas dos a dos. Denotaremos por $\mathbb{Z}_n$ al conjunto de las clases módulo n,

$$\mathbb{Z}_n = \{[0]_n, [1]_n, [2]_n, ..., [n-1]_n\}.$$

En ocasiones, siempre que no haya confusión, escribiremos simplemente la clase de un cierto entero $a \in \mathbb{Z}$ módulo un cierto natural n, como $[a]$, en lugar de $[a]_n$.

Ejemplo 2.1.5. Consideremos la relación de congruencia módulo 5.

Empecemos mirando los números positivos. Como $a \equiv b \pmod 5$ si, y sólo si, a y b tienen el mismo resto al dividirlos entre 5, entonces tenemos 5 posibilidades, ésto es, el valor del resto puede variar desde 0 hasta 4. De esta manera, trabajando con la relación de congruencia módulo 5, nos aparecen cinco clases de equivalencia:

- $[0]_5 : 0 \equiv 5 \equiv 10 \equiv 15 \equiv 20 \equiv ... \pmod 5$,
- $[1]_5 : 1 \equiv 6 \equiv 11 \equiv 16 \equiv 21 \equiv ... \pmod 5$,
- $[2]_5 : 2 \equiv 7 \equiv 12 \equiv 17 \equiv 22 \equiv ... \pmod 5$,
- $[3]_5 : 3 \equiv 8 \equiv 13 \equiv 18 \equiv 23 \equiv ... \pmod 5$,
- $[4]_5 : 4 \equiv 9 \equiv 14 \equiv 19 \equiv 24 \equiv ... \pmod 5$.

Los números negativos también son de alguno de esos tipos:

- $[0]_5 : \quad 0 \equiv -5 \equiv -10 \equiv -15 \equiv -20 \equiv ... \pmod 5$,
- $[1]_5 : -4 \equiv -9 \equiv -14 \equiv -19 \equiv -24 \equiv ... \pmod 5$,
- $[2]_5 : -3 \equiv -8 \equiv -13 \equiv -18 \equiv -23 \equiv ... \pmod 5$,
- $[3]_5 : -2 \equiv -7 \equiv -12 \equiv -17 \equiv -22 \equiv ... \pmod 5$,
- $[4]_5 : -1 \equiv -6 \equiv -11 \equiv -16 \equiv -21 \equiv ... \pmod 5$.

El siguiente resultado afirma que podemos realizar sumas y productos módulo un entero mayor que 1.

Proposición 2.1.6. *Sean $a, b, c, d, n \in \mathbb{Z}$, con $n > 1$, tales que $a \equiv b \pmod n$ y $c \equiv d \pmod n$. Entonces se verifica:*

1. $a + c \equiv b + d \pmod n$.
2. $ac \equiv bd \pmod n$.

Observación 2.1.7. Esto indica que, para hacer operaciones con un entero a módulo un cierto número n, podemos utilizar el resto de dividir a entre n para simplificar operaciones. Además, se verifica

$$[a]_n + [b]_n = [a + b]_n, \text{ y } [a]_n \cdot [b]_n = [a \cdot b]_n.$$

Ejemplo 2.1.8.

- Volvamos al ejemplo anterior, es decir, consideremos el conjunto de las clases de todos los números módulo 5, $\mathbb{Z}_5$. Si queremos multiplicar módulo 5 los números 7421 y 124592, en lugar de hacer la multiplicación directamente, tomamos los restos módulo 5. Así, tenemos que

  $$7421 \cdot 124592 \equiv 1 \cdot 2 \equiv 2 \pmod 5,$$

  ya que $[7421] = [1]$ y $[124592] = [2]$ en $\mathbb{Z}_5$.

- Vamos a determinar el resto de dividir 795^{25} entre 11 aplicando las operaciones con clases de equivalencia. Empezaremos dividiendo 795 entre 11 para obtener la clase de 795 módulo 11:

$$795 = 72{\cdot}11 + 3.$$

Luego $[795]_{11} = [3]_{11}$. Ahora, descomponemos el exponente en sumas de potencias de 2, en este caso

$$[795^{25}] = [3^{25}] = [3^{1+2\cdot 12}] = [3(3^2)^{12}] = [3{\cdot}9^{12}].$$

Ahora bien, como $[9]_{11} = [-2]_{11}$, entonces

$$[3{\cdot}9^{12}] = [3{\cdot}(-2)^{12}] = [3(-2^4)^3] = [3{\cdot}16^3] = [3{\cdot}5^3],$$

ya que $[16]_{11} = [5]_{11}$. Por lo tanto

$$[795^{25}] = [3{\cdot}5^3] = ([(3 \cdot 5)5^2] = [15{\cdot}25] = [4{\cdot}3] = [12] = [1],$$

es decir, $795^{25} \equiv 1 \pmod{11}$, con lo que el resto de dividir 795^{25} entre 11 es 1.

2.2. Congruencias lineales y sistemas de congruencias

2.2.1. Congruencias lineales

Definición 2.2.1. Sean $a, b, c, n \in \mathbb{Z}$, con $n > 1$. Llamaremos *congruencia lineal* a una ecuación de la forma $ax + b \equiv c \pmod{n}$.

Ejemplo 2.2.2. Sea por ejemplo la congruencia lineal $3x + 3 \equiv 4 \pmod{5}$. Se trata entonces de buscar todos los números enteros x tales que al multiplicarlos por 3 y sumarles 3 sean congruentes con 4 módulo 5.

Si razonamos como si fueran ecuaciones de primer grado tradicionales, lo que hacemos primero es pasar el 3 restando al otro miembro, quedando así $3x \equiv 1 \pmod{5}$. Nótese que esta operación no supone ningún problema, ya que en el conjunto de los números enteros siempre podemos sumar o restar números enteros entre ellos sin problemas.

Sin embargo, ahora lo que querríamos es pasar el 3 dividiendo, lo que daría problemas ya que el inverso de 3 es $\frac{1}{3} \notin \mathbb{Z}$. La cuestión natural entonces es si al trabajar módulo 5 (o módulo un natural cualquiera n) el 3 tiene, o no, inverso para el producto módulo 5.

Teorema 2.2.3. *Sean $a, n \in \mathbb{Z}$, con $n > 1$. Si $\mathrm{mcd}(a, n) = 1$, entonces existe inverso de a para el producto en $\mathbb{Z}_n$, es decir, existe $b \in \mathbb{Z}$ tal que $a{\cdot}b \equiv 1 \pmod{n}$.*

Observación 2.2.4. Si existe un entero b en las condiciones del teorema anterior, entonces b es único módulo n (hay una sola clase de equivalencia).

Corolario 2.2.5. *Sean $a, n \in \mathbb{Z}$, con $n > 1$. Si el $\mathrm{mcd}(a, n) \neq 1$, entonces no existe inverso de a para el producto en $\mathbb{Z}_n$, es decir, no podemos encontrar ningún $b \in \mathbb{Z}$ tal que $a{\cdot}b \equiv 1 \pmod{n}$.*

Ejemplo 2.2.6. Volvamos al ejemplo anterior, donde teníamos la congruencia lineal $3x + 3 \equiv 4 \pmod 5$ o, equivalentemente, $3x \equiv 1 \pmod 5$.

Por el teorema anterior, como $\text{mcd}(3, 5) = 1$, entonces el 3 tiene inverso módulo 5. Al trabajar módulo 5, sabemos que todo número es congruente con uno del conjunto $\{0, 1, 2, 3, 4\}$. Podemos buscar el inverso entonces probando:

$$\begin{array}{l} 3{\cdot}0 \equiv 0 \pmod 5 \\ 3{\cdot}1 \equiv 3 \pmod 5 \\ 3{\cdot}2 \equiv 1 \pmod 5 \\ 3{\cdot}3 \equiv 4 \pmod 5 \\ 3{\cdot}4 \equiv 2 \pmod 5 \end{array} .$$

Es decir, el inverso de $[3]$ en $\mathbb{Z}_5$ es $[2]$, ya que $3{\cdot}2 \equiv 1 \pmod 5$.

Multiplicamos ambos miembros de la congruencia por 2 para obtener $x \equiv 2 \pmod 5$. Por lo tanto, todos los números enteros x solución de la congruencia lineal $3x + 3 \equiv 4 \pmod 5$ son de la forma

$$x = 5k + 2, \text{ con } k \in \mathbb{Z},$$

ya que, por la definición de relación de congruencia, $x - 2$ es múltiplo de 5, es decir, existe $k \in \mathbb{Z}$ tal que $x - 2 = k{\cdot}5$ o, equivalentemente, $x = 5k + 2$.

Ejemplo 2.2.7. Consideremos ahora la congruencia lineal $3x + 4 \equiv 5 \pmod 6$.

Como $3x + 4 \equiv 5 \pmod 6$, entonces $3x \equiv 1 \pmod 6$. Pero $\text{mcd}(3, 6) = 3 \neq 1$, con lo que 3 no tiene inverso módulo 6 y, por tanto, esta congruencia lineal no tiene solución.

Ejemplo 2.2.8. Sea ahora la congruencia lineal $6x - 3 \equiv 2 \pmod{17}$.

En primer lugar, como $\text{mcd}(6, 17) = 1$, entonces nuestra congruencia lineal tiene solución.

Sumando 3 en ambos lados de la congruencia, obtenemos $6x \equiv 5 \pmod{17}$. Nótese ahora que, como $6{\cdot}3 = 18$, entonces $[3]$ es el inverso de $[6]$ en $\mathbb{Z}_{17}$. Con lo que obtenemos

$$x \equiv 3{\cdot}5 \pmod{17} \Leftrightarrow x \equiv 15 \pmod{17}.$$

Luego, las soluciones de la congruencia lineal $6x-3 \equiv 2 \pmod{17}$ son todos los números enteros x de la forma

$$x = 17k + 15, \text{ con } k \in \mathbb{Z}.$$

Veamos ahora un procedimiento general para hallar el inverso de un número entero módulo n.

Definición 2.2.9. Definimos la *función de Euler* como la función $\phi : \mathbb{Z}^+ \longrightarrow \mathbb{Z}^+$ tal que a cada $n \in \mathbb{Z}^+$ le asigna el número de enteros positivos menores o iguales que n y coprimos con n.

Ejemplo 2.2.10. En la siguiente tabla se recogen los valores que toma la función de Euler sobre los primeros 12 números naturales:

n	1	2	3	4	5	6	7	8	9	10	11	12
$\phi(n)$	1	1	2	2	4	2	6	4	6	4	10	4

.

La forma más sencilla de evaluar esta función es utilizando el siguiente resultado.

Teorema 2.2.11. *Sea $\phi : \mathbb{Z}^+ \longrightarrow \mathbb{Z}^+$ la función de Euler. Entonces se verifica:*

1. *Si p es un número primo, entonces $\phi(p) = p - 1$.*
2. *Si p es un número primo, entonces $\phi(p^\alpha) = p^\alpha - p^{\alpha-1}$ para todo $\alpha \in \mathbb{N}$.*
3. *Si $m, n \in \mathbb{Z}^+$, con $\text{mcd}(m, n) = 1$, entonces $\phi(m{\cdot}n) = \phi(m){\cdot}\phi(n)$.*
4. *Si $n \in \mathbb{Z}^+$ se descompone en factores primos como $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, entonces*

$$\phi(n) = (p_1^{\alpha_1} - p_1^{\alpha_1 - 1})(p_2^{\alpha_2} - p_2^{\alpha_2 - 1}) \cdots (p_k^{\alpha_k} - p_k^{\alpha_k - 1}).$$

Ejemplo 2.2.12.

- $\phi(11) = 11 - 1 = 10$.
- $\phi(12) = \phi(2^2{\cdot}3) = (2^2 - 2^{2-1})(3^1 - 3^{1-1}) = (4-2)(3-1) = 2{\cdot}2 = 4$.
- $\phi(180) = \phi(2^2{\cdot}3^2{\cdot}5) = (2^2 - 2)(3^2 - 3)(5 - 1) = 2{\cdot}6{\cdot}4 = 48$.

Teorema 2.2.13. (de Euler-Fermat). *Sean $a, n \in \mathbb{Z}$, con $n > 1$, tales que $\text{mcd}(a, n) = 1$. Entonces $a^{\phi(n)} \equiv 1 \pmod{n}$. Es decir, en inverso de $[a]$ en $\mathbb{Z}_n$ es $[a^{\phi(n)-1}]$.*

Ejemplo 2.2.14. Vamos a usar el teorema de Euler-Fermat para resolver la congruencia lineal $2x + 3 \equiv 11 \pmod 9$.

En primer lugar, esta congruencia lineal es equivalente a la congruencia lineal $2x \equiv 8 \pmod 9$. Ahora bien, como $\text{mcd}(2, 9) = 1$ entonces, por el teorema de Euler-Fermat, el inverso de 2 módulo 9 será $2^{\phi(9)-1}$.

Como $\phi(9) = \phi(3^2) = (3^2 - 3) = 6$, entonces $2^{\phi(9)-1} = 2^5 = 32$, que es congruente con 5 módulo 9. Luego

$$2x \equiv 8 \pmod 9 \Leftrightarrow x \equiv 5{\cdot}8 \pmod 9 \Leftrightarrow x \equiv 40 \pmod 9 \Leftrightarrow x \equiv 4 \pmod 9.$$

Por lo tanto, todos los números enteros x solución de la congruencia lineal $2x + 3 \equiv 11 \pmod 9$ son de la forma

$$x = 9k + 4, \text{ con } k \in \mathbb{Z}.$$

En cualquier caso, el uso de esta función para calcular inversos solo es recomendable para números no demasiado grandes, ya que requiere de la factorización en números primos.

2.2.2. Sistemas de congruencias

En muchas ocasiones, la resolución de un problema supondrá la satisfacción de más de una congruencia lineal. Por ejemplo, si nos preguntamos por un número que tenga las siguientes características: al dividirse entre 3 tiene resto 1, al dividirse entre 5 tiene resto 2 y al dividirse

entre 7 tiene resto 3, estamos buscando un número que satisfaga simultáneamente las siguientes congruencias lineales:

$$\begin{array}{l} x \equiv 1 \pmod 3 \\ x \equiv 2 \pmod 5 \\ x \equiv 3 \pmod 7 \end{array}.$$

El teorema chino del resto, que vemos a continuacion, establece condiciones en las que podemos estar seguros de la existencia de soluciones.

Teorema 2.2.15. (Teorema chino del resto). *Sean $n_1, n_2, ..., n_k \in \mathbb{Z}$ enteros positivos mayores que 1 y primos relativos dos a dos, y sean $a_1, a_2, ..., a_k \in \mathbb{Z}$. Entonces el sistema de congruencias*

$$\begin{array}{l} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \\ \cdots \\ x \equiv a_k \pmod{n_k} \end{array}$$

tiene solución. Además, si x y x' son soluciones, entonces $x \equiv x' \pmod{n_1 n_2 \cdots n_k}$, es decir, la solución es única módulo $N = n_1 n_2 \cdots n_k$.

Ejemplo 2.2.16. Resolvamos el sistema planteado en la introducción de esta sección, es decir,

$$\begin{array}{l} x \equiv 1 \pmod 3 \\ x \equiv 2 \pmod 5 \\ x \equiv 3 \pmod 7 \end{array}.$$

En primer lugar, como $\text{mcd}(3,5) = \text{mcd}(3,7) = \text{mcd}(5,7) = 1$ entonces, por el teorema chino del resto, el sistema tiene solución.

1. De la primera ecuación, deducimos que $x = 3k+1$, con $k \in \mathbb{Z}$. Utilizamos esta igualdad para sustituir en la segunda ecuación, obteniendo

   $$3k + 1 \equiv 2 \pmod 5 \Leftrightarrow 3k \equiv 1 \pmod 5 \Leftrightarrow k \equiv 2{\cdot}1 \pmod 5 \Leftrightarrow k \equiv 2 \pmod 5),$$

   con lo que $k = 5m + 2$, con $m \in \mathbb{Z}$ y, por tanto,

   $$x = 3k + 1 = 3(5m + 2) + 1 = 15m + 7, \text{ con } m \in \mathbb{Z}.$$

2. A continuación, llevamos esta expresión de x a la última congruencia:

   $$x \equiv 3 \pmod 7 \Leftrightarrow 15m + 7 \equiv 3 \pmod 7 \Leftrightarrow m + 0 \equiv 3 \pmod 7 \Leftrightarrow m \equiv 3 \pmod 7),$$

   con lo que $m = 7n + 3$, con $n \in \mathbb{Z}$ y, por tanto,

   $$x = 15m + 7 = 15(7n + 3) + 7 = 105n + 52, \text{ con } n \in \mathbb{Z}.$$

   Es decir, $x \equiv 52 \pmod{105}$, donde $105 = 3{\cdot}5{\cdot}7$.

El teorema chino del resto establece condiciones suficientes para la existencia de soluciones, pero esas condiciones no son necesarias. El siguiente resultado es más general, pero solo se enuncia para dos ecuaciones.

Teorema 2.2.17. *Sean $n_1, n_2 \in \mathbb{Z}$ enteros positivos mayores que 1 y sean $a_1, a_2 \in \mathbb{Z}$. Sean $d = \text{mcd}(n_1, n_2)$ y $m = \text{mcm}(n_1, n_2)$. Entonces el sistema de congruencias*

$$\begin{array}{l} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \end{array}$$

tiene solución si, y sólo si, $a_1 \equiv a_2 \pmod{d}$. En tal caso, la solución es única módulo m.

Ejemplo 2.2.18. Vamos a estudiar ahora el siguiente sistema de congruencias:

$$\begin{array}{l} x \equiv 3 \pmod{14} \\ x \equiv 10 \pmod{35} \end{array}.$$

En primer lugar, como $\text{mcd}(14, 35) = 7$ ($14 = 2{\cdot}7$ y $35 = 5{\cdot}7$) y $3 \equiv 10 \pmod{7}$ entonces, por el teorema anterior, el sistema tiene solución.

De la primera ecuación, deducimos que $x = 14k + 3$, con $k \in \mathbb{Z}$. Utilizamos esta igualdad para sustituir en la segunda ecuación, obteniendo

$$14k + 3 \equiv 10 \pmod{35} \Leftrightarrow 14k \equiv 7 \pmod{35}.$$

Como la clase de 14 no tiene inverso módulo 35, ya que $\text{mcd}(14, 35) = 7 \neq 1$, entonces obtenemos que $14k = 35m + 7$, con $m \in \mathbb{Z}$ o, equivalentemente, $2k = 5m + 1$, con $m \in \mathbb{Z}$, es decir,

$$2k \equiv 1 \pmod{5} \Leftrightarrow k \equiv 3{\cdot}1 \pmod{5} \Leftrightarrow k \equiv 3 \pmod{5},$$

con lo que $k = 5m + 3$, con $m \in \mathbb{Z}$ y, por tanto,

$$x = 14k + 3 = 14(5m + 3) + 3 = 70m + 45, \text{ con } m \in \mathbb{Z},$$

es decir, $x \equiv 45 \pmod{70}$.

Ejercicios

1. Resuelve las siguientes congruencias lineales:

$$\text{a) } 3x \equiv 1 \pmod{12}; \qquad \text{b) } 3x \equiv 1 \pmod{11}, \qquad \text{c)} 64x + 11 \equiv 43 \pmod{84}.$$

2. Demostrar que los siguientes sistemas de congruencias tienen solución y resolverlos:

$$\text{a) } \begin{cases} x \equiv 3 \pmod{5} \\ x \equiv 5 \pmod{7} \end{cases}, \qquad \text{b) a) } \begin{cases} x \equiv 5 \pmod{11} \\ x \equiv 7 \pmod{13} \end{cases}.$$

3. Demostrar que el siguiente sistema de congruencias no tiene solución:

$$\begin{cases} x \equiv 2 \pmod{6} \\ x \equiv 3 \pmod{9} \end{cases}.$$

4. Encuentra el conjunto de enteros x que verifican el siguiente sistema de congruencias:

$$\begin{cases} x \equiv -2 \pmod{5} \\ 2x \equiv 1 \pmod{7} \\ x \equiv 3 \pmod{8} \end{cases}.$$

5. Resuelve, cuando sea posible, los siguientes sistemas de congruencias:

$$\text{a) } \begin{cases} x \equiv 5 \pmod{6} \\ x \equiv 3 \pmod{10} \\ x \equiv 8 \pmod{15} \end{cases}, \qquad \text{b) } \begin{cases} x \equiv 2 \pmod{14} \\ x \equiv 10 \pmod{30} \\ x \equiv 6 \pmod{21} \end{cases}.$$

6. ¿En qué condiciones podemos afirmar que el siguiente sistema de congruencias tiene solución?

$$\begin{cases} x \equiv a \pmod{n} \\ x \equiv b \pmod{m} \end{cases}.$$

7. Encuentra el menor entero positivo cuyo resto cuando se divide por 11 es 8, que tiene el último dígito igual a 4 y es divisible por 27.

8. Un tesoro escondido de monedas de oro pasa a "ser propiedad" de una banda de 15 piratas. Cuando empiezan a repartirse las monedas, les sobran 3 monedas. La discusión por el reparto se "anima" y solo quedan 7 piratas pero, cuando se reparten las monedas entre ellos, sobran 2. La discusión continua y el número de piratas se reduce a 4, que sí consiguen repartirse todas las monedas. ¿Cuál es el mínimo número de monedas que podía haber en el tesoro?

9. En los apartados siguientes, calcula el menor entero positivo x que verifique la relación:

$$\text{a) } 3^{201} \equiv x \pmod{11}; \qquad \text{b) } 2^{11} \cdot 3^{13} \equiv x \pmod{7}.$$

10. Calcula el resto de dividir 100^{101} entre 7.