Matemática Discreta I

Tema 3. Aritmética modular

Jesús Martínez Mateo jmartinez@fi.upm.es

Departamento de Matemática Aplicada a las TIC
E.T.S. Ingenieros Informáticos
Universidad Politécnica de Madrid

Grado en Ingeniería Informática
Curso 2020/21

Contenidos

Congruencias

Definición

Sean $n \in \mathbb{N}$ y $a, b \in \mathbb{Z}$. Decimos que a **es congruente con** b **módulo** n, y lo denotamos por $a \equiv b \pmod{n}$ si y sólo si $n \mid (a - b)$. Llamamos **congruencia** a la expresión $a \equiv b \pmod{n}$.

Teorema

Sean $n \in \mathbb{N}$ y $a, b \in \mathbb{Z}$ tales que

$$\begin{aligned} a &= qn + r \qquad 0 \leq r < n \\ b &= q'n + r' \qquad 0 \leq r' < n \end{aligned}$$

con $q, q', r, r' \in \mathbb{Z}$. Entonces $a \equiv b \pmod{n}$ si y sólo si $r = r'$.

Demostración.

Si $a \equiv b \pmod{n}$ entonces $n \mid a - b = n(q - q') + (r - r')$. Luego $n \mid (r - r')$, es decir, $r - r' = q''n$. Como además $0 \leq r, r' < n$ se tiene necesariamente que $q'' = 0$ y por lo tanto $r = r'$. Recíprocamente, si $a = qn + r$ y $b = q'n + r$ entonces $a - b = n(q - q')$, y por lo tanto $n \mid (a - b)$, es decir $a \equiv b \pmod{n}$. $\square$

Observación. Nótese que,

$$a \equiv a' \pmod{n} \Leftrightarrow n \mid (a - a') \Leftrightarrow \begin{cases} a = qn + r \\ a' = q'n + r \end{cases} \underbrace{\Leftrightarrow}_{q'=k+q} a' = kn + a$$

Relación de congruencia

La definición de congruencia dada es una relación de equivalencia, a la llamamos **relación de congruencia módulo** n, puesto que verifica las propiedades:

1. Reflexiva: $a \equiv a \pmod{n}$.
2. Simétrica: Si $a \equiv b \pmod{n}$ entonces $b \equiv a \pmod{n}$.
3. Transitiva: Si $a \equiv b \pmod{n}$ y $b \equiv c \pmod{n}$ entonces $a \equiv c \pmod{n}$.

Demostración.

1. $\forall a \in \mathbb{Z},\ n \mid (a-a) \Rightarrow a \equiv a \pmod{n}$.
2. $a \equiv b \pmod{n} \Rightarrow n \mid (a-b) = (b-a) \Rightarrow b \equiv a \pmod{n}$.
3. $$\left.\begin{array}{l} a \equiv b \pmod{n} \\ \end{array}\right\} \Rightarrow \left.\begin{array}{l} n \mid (a-b) \\ \end{array}\right\} \Rightarrow$$

Clases de congruencia

Definiciones

- Llamamos **clase de congruencias módulo** n a la clase de equivalencia de cada elemento de $\mathbb{Z}$:

$$\begin{aligned}[a]_n &= \{b \in \mathbb{Z} \mid a \equiv b \pmod{n}\} \\ &= \{\ldots, a-2n, a-n, a, a+n, a+2n, \ldots\}\end{aligned}$$

- Llamamos **conjunto de enteros módulo** n, y lo denotamos por $\mathbb{Z}_n$, al conjunto cociente de $\mathbb{Z}$ determinado por la relación de congruencia módulo n, es decir, el conjunto de clases de congruencia módulo n

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

Clases de congruencia

Ejemplo

$\mathbb{Z}_3$ es el conjunto formado por tres clases de congruencia

$$\mathbb{Z}_3 = \{[0]_3, [1]_3, [2]_3\},$$

donde

$$\begin{aligned}
[0]_3 &= \{x \in \mathbb{Z} \mid x \equiv 0 \pmod{3}\} = \{\ldots - 9, -6, -3, 0, 3, 6, 9, \ldots\} \\
[1]_3 &= \{x \in \mathbb{Z} \mid x \equiv 1 \pmod{3}\} = \{\ldots - 8, -5, -2, 1, 4, 7, 10, \ldots\} \\
[2]_3 &= \{x \in \mathbb{Z} \mid x \equiv 2 \pmod{3}\} = \{\ldots - 7, -4, -1, 2, 5, 8, 11, \ldots\}.
\end{aligned}$$

La relación de congruencia módulo 3 en $\mathbb{Z}$ produce una partición de $\mathbb{Z}$ en tres conjuntos $[0]_3$, $[1]_3$ y $[2]_3$ donde

Aritmética en $\mathbb{Z}_n$

Definición

Sean $[a]_n, [b]_n \in \mathbb{Z}_n$. Definimos las operaciones suma y producto como

$$[a]_n + [b]_n = [a+b]_n$$
$$[a]_n \cdot [b]_n = [ab]_n$$

Teorema

Sean $n \in \mathbb{N}$ y $a, a', b, b' \in \mathbb{Z}$ enteros cualesquiera tales que $a \equiv a' \pmod{n}$ y $b \equiv b' \pmod{n}$. Entonces $a + b \equiv a' + b' \pmod{n}$ y $ab \equiv a'b' \pmod{n}$.

Demostración.

Sean $a' = qn + a$, $b' = q'n + b$. Tenemos entonces que

$$a' + b' = (qn + a) + (q'n + b) = (q + q')n + (a + b) \Leftrightarrow$$

$$\Leftrightarrow n \mid ab - a'b' \Leftrightarrow ab \equiv a'b' \pmod{n}$$

Propiedades en $\mathbb{Z}_n$

Sean $[a]_n, [b]_n, [c]_n \in \mathbb{Z}_n$. Las operaciones suma y producto en $\mathbb{Z}_n$ verifican las siguientes propiedades:

- Asociativa: $\begin{cases} [a]_n + ([b]_n + [c]_n) = ([a]_n + [b]_n) + [c]_n \\ [a]_n \cdot ([b]_n \cdot [c]_n) = ([a]_n \cdot [b]_n) \cdot [c]_n \end{cases}$.
- Conmutativa: $[a]_n + [b]_n = [b]_n + [a]_n, \quad [a]_n \cdot [b]_n = [b]_n \cdot [a]_n$.
- Distributiva: $[a]_n \cdot ([b]_n + [c]_n) = ([a]_n \cdot [b]_n) + ([a]_n \cdot [c]_n)$.
- Existencia de elementos neutro y unidad (neutro para producto): $\exists\, [0]_n, [1]_n \in \mathbb{Z}_n$ tales que $[a]_n + [0]_n = [a]_n, \quad [a]_n [1]_n = [a]_n$.
- Existencia de elementos opuestos: $\exists\, [-a]_n \in \mathbb{Z}_n$ tal que $[a]_n + [-a]_n = [0]_n$.

Propiedades en $\mathbb{Z}_n$

Definición

Sea $[a]_n \in \mathbb{Z}_n$ con $[a]_n \neq 0$. Decimos que $[a]_n$ es un **divisor de cero** si existe $[b]_n \in \mathbb{Z}_n$ tal que $[a]_n \cdot [b]_n = [0]_n$.

Observación I. La existencia de divisores de cero hace que en $\mathbb{Z}_n$ no se siempre se cumpla la propiedad cancelativa del producto.

Ejemplo

Por ejemplo, $\mathbb{Z}_4$ el $[2]_4$ es un divisor de cero puesto que $[2]_4 \cdot [2]_4 = [0]_4$. Nótese por lo tanto que, en $\mathbb{Z}_4$ no se verifica la propiedad cancelativa. Por ejemplo, $[2]_4 \cdot [1]_4 = [2]_4 \cdot [3]_4 = [2]_4$ y sin embargo $[1]_4 \neq [3]_4$.

Observación II. En $\mathbb{Z}_n$ ...

Criterios de divisibilidad

Sea $x = (x_n x_{n-1} \ldots x_1 x_0)_{10}$ la representación en decimal del entero

$$x = x_n 10^n + x_{n-1}10^{n-1} + \ldots + x_1 10 + x_0 = \sum_{k=0}^{n} x_k 10^k$$

- En $\mathbb{Z}_2$ y Z_5 podemos escribir x como

$$x = 10(x_n 10^{n-1} + x_{n-1}10^{n-2} + \ldots + x_1) + x_0.$$

  Luego $x \equiv x_0 \pmod 2$ y $x \equiv x_0 \pmod 5$. Es decir, $2 \mid x$ si y sólo si $2 \mid x_0$, y análogamente, $5 \mid x$ si y sólo si $5 \mid x_0$
- En Z_4 podemos escribir x como

$$x = 100(x_n 10^{n-2} + x_{n-1}10^{n-3} + \ldots + x_2) + (x_1 10 + x_0)$$

Criterios de divisibilidad

- En $\mathbb{Z}_3$ y Z_9 tenemos que $10 \equiv 1 \pmod 3$ y $10 \equiv 1 \pmod 9$. Por lo tanto $x = x_n + x_{n-1} + \ldots + x_1 + x_0 \pmod 3$, y análogamente $x = x_n + x_{n-1} + \ldots + x_1 + x_0 \pmod 9$. Luego tenemos que, $3 \mid x$ si y sólo si $3 \mid (x_n + \ldots + x_0)$, y $9 \mid x$ si y sólo si $9 \mid (x_n + \ldots + x_0)$.
- En Z_{11} tenemos que $10 \equiv -1 \pmod{11}$, y por lo tanto $x \equiv \sum_{k=0}^{n} (-1)^k x_k \pmod{11}$. Es decir, $11 \mid x$ si y sólo si

$$11 \mid ((-1)^n x_n + \ldots - x_3 + x_2 - x_1 + x_0).$$

Unidades en $\mathbb{Z}_n$

Definición

Un elemento $[a]_n \in \mathbb{Z}_n$ es **unidad** o inversible en $\mathbb{Z}_n$ si existe $[b]_n \in \mathbb{Z}_n$ tal que $[a]_n \cdot [b]_n = [1]_n$. También decimos que el elemento $[a]_n \in \mathbb{Z}_n$ tiene inverso. Al elemento $[b]_n$ lo llamamos **inverso** de $[a]_n$ y lo denotamos por $[b]_n = [a]_n^{-1}$.

Teorema

El inverso de un elemento unidad es único.

Demostración.

Sea $[a]_n \in \mathbb{Z}_n$. Supongamos que $[b]_n, [b']_n \in \mathbb{Z}_n$ son ambos elementos inversos de $[a]_n$. Tenemos entonces que

Unidades en $\mathbb{Z}_n$

Teorema

Un elemento $[a]_n \in \mathbb{Z}_n$ es unidad, es decir, tiene inverso si y sólo si $\mathrm{mcd}(a, n) = 1$.

Demostración.
$[a]_n \in \mathbb{Z}_n$ es unidad en $\mathbb{Z}_n$ si existe $[b]_n \in \mathbb{Z}_n$ tal que $[a]_n \cdot [b]_n = [1]_n$, o equivalentemente $[a \cdot b]_n = [1]_n$, es decir, $ab \equiv 1 \pmod{n}$. Recordemos entonces que $ab \equiv 1 \pmod{n} \Leftrightarrow 1 = kn + ab$ con $a, b, k, n \in \mathbb{Z}$. Los enteros a y n son conocidos, y la ecuación diofántica anterior tiene solución si y sólo si $\mathrm{mcd}(a, n) = 1$. El recíproco es análogo. □

Observación. El resultado anterior nos proporciona además un método para el cálculo de inversos. Tan sólo tenemos que encontrar una solución particular para la ecuación diofántica

El elemento inverso será $[x]_n = [a]_n^{-1}$

Unidades en $\mathbb{Z}_n$

Teorema

Si p es primo, los únicos elementos que coinciden con su inverso en $\mathbb{Z}_p$ son $[1]_p$ y $[-1]_p$.

Demostración.

Sea $[a]_p \in \mathbb{Z}_p$ con p primo. Sabemos que el elemento $[a]_p$ tiene inverso en $\mathbb{Z}_p$ si $[a]_p \neq [0]_p$. Suponemos entonces que $[a]_p^{-1} = [a]_p$. Se cumple que

$$[a^2]_p = [a]_p \cdot [a]_p = [a]_p \cdot [a]_p^{-1} = [1]_p,$$

o equivalentemente $a^2 \equiv 1 \pmod{p}$. Es decir, $a^2 = kp + 1$ para algún $k \in \mathbb{Z}$, que también podemos expresar como $kp = a^2 - 1 = (a-1)(a+1)$, o como $p \mid (a-1)(a+1)$. Tenemos entonces que, si $p \mid (a-1)$ es porque

Unidades en $\mathbb{Z}_n$

Definición

Definimos el **conjunto de unidades** en $\mathbb{Z}_n$ como el conjunto

$$U_n = \{[a]_n \in \mathbb{Z}_n \mid \text{mcd}(a, n) = 1\}.$$

Es decir, U_n es el conjunto de los elementos de $\mathbb{Z}_n$ que tienen inverso.

Propiedades.

- Sean $[a]_n, [b]_n \in U_n$. Entonces, $[a \cdot b]_n \in U_n$.
- Sea $[a]_n \in U_n$. Entonces, $[a]_n \cdot U_n = \{[a]_b \cdot [b]_n \mid [b]_n \in U_n\} = U_n$.

Demostración.

- Sean $[a]_n, [b]_n \in U_n$. Existen $[a]_n^{-1}, [b]_n^{-1} \in U_n$. Tenemos entonces que $[a]_n \cdot [a]_n^{-1} = [1]_n$, y $[b]_n \cdot [b]_n^{-1} = [1]_n$, y por lo tanto

Unidades en $\mathbb{Z}_n$

Propiedades.

- Sea $[a]_n \in U_n$. Entonces, $[a]_n \cdot U_n = \{[a]_b \cdot [b]_n \mid [b]_n \in U_n\} = U_n$.

Demostración.

- Veamos en primer lugar que $[a]_n \cdot U_n \subseteq U_n$. Sea $[c]_n$ un elemento cualquiera de $[a]_n \cdot U_n$. Se tiene entonces que $[c]_n \in [a]_n \cdot U_n$ puesto que existe $[b]_n \in U_n$ tal que $[c]_n = [a]_n \cdot [b]_n$. Ahora bien, puesto que $[a]_n, [b]_n \in U_n$ se tiene también que $[a]_n \cdot [b]_n \in U_n$. En efecto,

$$[a]_n \cdot [a]_n^{-1} \cdot [b]_n [b]_n^{-1} = ([a]_n \cdot [b]_n) \cdot ([a]_n^{-1} [b]_n^{-1}) = [1]_n.$$

  Por lo tanto $[c]_n \in U_n$.

  Veamos en segundo lugar que $U_n \subseteq [a]_n \cdot U_n$. Sea $[c]_n \in U_n$ un elemento cualquiera. Podemos expresarlo como

$$[c]_n = ([a]_n \cdot [a]_n^{-1}) \cdot [c]_n = [a]_n \cdot ([a]_n^{-1} \cdot [c]_n).$$

Función de Euler

Definición

Llamamos **función de Euler** a la función $\phi\colon \mathbb{N} \to \mathbb{N}$ dada por $\phi(n) = |U_n|$, es decir, la función que asocia a cada $n \in \mathbb{N}$ el número de unidades en $\mathbb{Z}_n$.

Propiedades.

- Si p es primo, entonces $\phi(p) = p - 1$.
- Si p es primo, entonces $\phi(p^e) = p^e - p^{e-1}$.
- Si $\mathrm{mcd}(m, n) = 1$, entonces $\phi(m \cdot n) = \phi(m)\phi(n)$.

Demostración.

- Si p es primo, es evidente que el número de unidades en $\mathbb{Z}_p$ es $p - 1$.
- Si p es primo, podemos particionar el conjunto de las clases de congruencia de $\mathbb{Z}_{p^e}$ en p partes (o bloques) con $\frac{p^e}{p} = p^{e-1}$ elementos por bloque. Repartimos los elementos de $\mathbb{Z}_{p^e}$, comenzando por el

Función de Euler

Propiedades.

Demostración.

- Suponemos que $m, n > 1$ (en caso contrario el resultado es trivial). Particionamos el conjunto $\mathbb{Z}_{mn}$, y repartimos sus $m \cdot n$ elementos en m bloques de forma que los elementos de cada bloque son todos congruentes módulo m. Se tiene entonces que, exactamente $\phi(m)$ bloques contienen enteros todos ellos coprimos con m. Cada bloque contiene n elementos, y por lo tanto es de la forma $\{r, r+m, r+2m, \ldots, r+(n-1)m\}$. En $\mathbb{Z}_n$ podríamos a cada elemento del bloque restar r y multiplicar por $[m]_n^{-1}$ (puesto que $\mathrm{mcd}(m,n) = 1$) y nos quedaría $\{0, 1, \ldots, n-1\}$, por lo que cada bloque constituye un conjunto completo de restos módulo n, y por lo tanto contiene exactamente $\phi(n)$ enteros coprimos con n. Luego, los

Teorema de Wilson

Teorema

Si p es primo, entonces $(p-1)! \equiv (p-1) \pmod{p}$.

Demostración.

Si p es primo, los únicos elementos que coinciden con su inverso son $[1]_p$ y $[p-1]_n$. El resto de elementos se agrupan dos a dos siendo mutuamente inversos, y por lo tanto $[p-1]_n! = [p-1]_n \cdot [p-2]_n \cdots 2 \cdot 1 = [p-1]_n$. □

Ejemplo

En Z_7 los elementos que coinciden con su inverso son $[1]_7^{-1} = [1]_7$, y $[-1]_7 = [6]_7 = [6]_7$. Para el resto de elementos los inversos son $[2]_7^{-1} = [4]_7$, y $[3]_7^{-1} = [5]_7$. Luego,

$$[6]_7! = [6]_7 \cdot [5]_7 \cdot [4]_7 \cdot [3]_7 \cdot [2]_7 \cdot [1]_7$$

Teorema de Euler

Teorema (Teorema de Euler)

Sean $a, n \in \mathbb{Z}$ *con* $a \neq 0$ *y* $n > 1$. *Si* a *y* n *son coprimos, es decir, si* $\operatorname{mcd}(a, n) = 1$, *entonces*

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

Demostración.

Equivalentemente, si $[a]_n \in U_n$ entonces $[a]_n^{\phi(n)} = [1]_n$. Sea $U_n = \{[x_1]_n, [x_2]_n, \ldots, [x_k]_n\}$. Tenemos entonces que $\phi(n) = |U_n| = k$. Si $[a]_n \in U_n$, entonces $[a]_n U_n = U_n$ y por lo tanto

$$\{[ax_1]_n, [ax_2]_n, \ldots, [ax_k]_n\} = \{[x_1]_n, [x_2]_n, \ldots, [x_k]_n\}.$$

Luego $[ax_1]_n \cdot [ax_2]_n \cdots [ax_k]_n = [x_1]_n \cdot [x_2]_n \cdots [x_k]_n$, es decir,

y queda $[a]_n^{\phi(n)} = [1]_n$, o equivalentemente $a^{\phi(n)} \equiv 1 \pmod{n}$.

Teorema de Euler

Corolario (Pequeño teorema de Fermat)

Si p *es primo y* $\operatorname{mcd}(a, p) = 1$, *entonces* $a^{p-1} \equiv 1 \pmod{p}$.

Observación I. Nótese que este resultado es una consecuencia directa del teorema de Euler. Si p es primo, entonces $\phi(p) = p - 1$. Se tiene también entonces que un entero $a \in Z$ comprendido entre $0 < a < p$ es siempre coprimo con p, y por lo tanto $\operatorname{mcd}(a, p) = 1$.

Observación II. Nótese también que, si p es primo, para cualquier entero $a \in \mathbb{Z}$ se verifica que

$$a^p \equiv a \pmod{p}.$$

Congruencias lineales

Definición

Sean $n \in \mathbb{N}$ y $a, b \in \mathbb{Z}$. Llamamos **congruencia lineal** a una ecuación de la forma

$$a \cdot x \equiv b \pmod{n},$$

donde x es una variable entera, $x \in \mathbb{Z}$, la incógnita de la ecuación.

Resolver una congruencia lineal es por lo tanto encontrar los valores de x que verifican la congruencia.

Ejemplo

Dada la congruencia lineal $3 \cdot x \equiv 4 \pmod{7}$ es fácil comprobar que una solución de la ecuación es $x = 6$. Efectivamente, $3 \cdot 6 = 18$ y se tiene que

Congruencias lineales

También podemos reescribir una ecuación en congruencias como una ecuación en el conjunto de enteros módulo n de la forma

$$[a]_n \cdot [x]_n = [b]_n,$$

donde $[a]_n$, $[b]_n$, y la variable $[x]_n$ son ahora elementos de $\mathbb{Z}_n$.
Para resolver dicha ecuación en $\mathbb{Z}_n$ basta con encontrar el inverso de $[a]_n$, si existe, y despejamos la variable como $[x]_n = [b]_n \cdot [a]_n^{-1}$.

Ejemplo

Para resolver la ecuación $[3]_7 \cdot [x]_7 = [4]_7$ calculamos en primer lugar el inverso $[3]_7^{-1} = [5]_7$ (efectivamente, $[3]_7 \cdot [5]_7 = [3 \cdot 5]_7 = [15]_7 = [1]_7$), y despejamos en la ecuación $[x]_7 = [4]_7 \cdot [5]_7 = [4 \cdot 5]_7 = [20]_7 = [6]_7$.

Congruencias lineales

Existe todavía una tercera aproximación. Podemos interpretar la congruencia lineal $a \cdot x \equiv b \pmod{n}$ como una expresión de la forma

$$ax = b + ny.$$

Es decir, resolver una congruencia lineal es equivalente a resolver una ecuación diofántica donde sólo nos interesa conocer una de las incógnitas.

Teorema

Sea $d = \operatorname{mcd}(a, n)$. La congruencia lineal $a \cdot x \equiv b \pmod{n}$ tiene solución si y sólo si $d \mid b$, en cuyo caso tiene d soluciones distintas en $\mathbb{Z}_n$. Si x_0 es una solución particular, todas las soluciones de la congruencia son

Congruencias lineales

Ejemplos

- La congruencia
$$4x \equiv 3 \pmod{6},$$
no tiene solución puesto que $\operatorname{mcd}(4,6) = 2$, y no se cumple que $2 \mid 3$.
- En cambio, la siguiente congruencia sí tiene solución.
$$4x \equiv 2 \pmod{6}.$$
Resolvemos la ecuación diofántica $4x + 6y = 2$ y encontramos que $x_0 = -1$ es una solución particular. Todas las soluciones son $x = -1 + 3t, \forall t \in \mathbb{Z}$. Luego todas las soluciones constituyen dos clases de congruencia módulo 6, las clases $[2]$ y $[5]$:

Congruencias lineales

Observación. Nótese que, en el ejemplo anterior decíamos que todas las soluciones constituyen dos clases de congruencia módulo 6. En cambio, si observamos la expresión de todas las soluciones en $\mathbb{Z}$, $x = -1 + 3t, \forall t \in \mathbb{Z}$, vemos que podemos también decir que todas las soluciones constituyen una única clase de congruencia módulo 3, es decir, $[x]_3 = [-1]_3 = [2]_3$.

Ejemplo

- La congruencia
$$5x \equiv 3 \pmod{6},$$
tiene solución puesto que $\mathrm{mcd}(5,6) = 1$, y se tiene que $1 \mid 3$. Una solución particular de la ecuación diofántica $5x + 6y = 3$ es $x_0 = -3$, y todas las soluciones son $x = -3 + 6t, \forall t \in \mathbb{Z}$. En este caso, todas las soluciones constituyen una única clase de congruencia módulo 6

Congruencias lineales

Propiedades.

- Sea $m \in \mathbb{Z}$ tal que $m \mid a$, $m \mid b$ y $m \mid n$. Entonces,

$$ax \equiv b \pmod{n} \Leftrightarrow \frac{a}{m}x \equiv \frac{b}{m} \pmod{\frac{n}{m}}.$$

- Sea $m \in \mathbb{Z}$ tal que $m \mid a$ y $m \mid b$. Si a y n son primos entre sí, es decir, si $\mathrm{mcd}(a, n) = 1$ se tiene entonces que

$$ax \equiv b \pmod{n} \Leftrightarrow \frac{a}{m}x \equiv \frac{b}{m} \pmod{n}.$$

Demostración.

- $ax \equiv b \pmod{n} \Leftrightarrow ax + ny = b$ para algún $y \in \mathbb{Z}$
  $\Leftrightarrow \frac{a}{m}x + \frac{n}{m}y = \frac{b}{m} \Leftrightarrow \frac{a}{m}x \equiv \frac{b}{m} \pmod{\frac{n}{m}}$

Congruencias lineales

Observación. Nótese que, las propiedades anteriores nos proporcionan una herramienta para poder resolver una congruencia lineal $ax \equiv b \pmod{n}$ de forma algorítmica como sigue.

1. Calculamos $d = \operatorname{mcd}(a, n)$ y comprobamos si $d \mid b$. En caso contrario, no existen soluciones.
2. Calculamos $a' = \frac{a}{d}$, $b' = \frac{b}{d}$, y $n' = \frac{n}{d}$ y simplificamos la congruencia como $a'x \equiv b' \pmod{n'}$.
3. Buscamos un valor b'' congruente con b' tal que $d' = \operatorname{mcd}(a', b'')$ con $d' > 1$, observando que

$$b' \equiv b' + n' \equiv b' + 2n' \equiv \ldots \equiv b' + kn' \pmod{n'}, \quad k \in 0, \ldots, n' - 1.$$

Congruencias lineales

Ejemplo

Podemos volver a resolver la siguiente congruencia utilizando ahora las propiedades sobre congruencias lineales:

$$\begin{aligned} 4x &\equiv 2 \pmod{6} \\ 2x &\equiv 1 \pmod{3} \\ 2x &\equiv 4 \pmod{3} \\ x &\equiv 2 \pmod{3} \end{aligned}$$

Luego, todas las soluciones son $x = 2 + 3t, \forall t \in \mathbb{Z}$.

Sistemas de congruencias lineales

Definición

Sean $n_1, n_2, \ldots, n_k \in \mathbb{N}$, y $a_1, a_2, \ldots, a_k, b_1, b_2, \ldots, b_k \in \mathbb{Z}$. Un *sistema de congruencias lineales* es un sistema de la forma:

$$\begin{cases} a_1 x \equiv b_1 \pmod{n_1} \\ a_2 x \equiv b_2 \pmod{n_2} \\ \quad \vdots \\ a_k x \equiv b_k \pmod{n_k} \end{cases}$$

donde x es una variable entera, $x \in \mathbb{Z}$, la única incógnita del sistema.

Se trata de un sistema de k congruencias lineales con la misma incógnita.

Sistemas de congruencias lineales

El primer paso a realizar a la hora de resolver un sistema de congruencias lineales es, por lo tanto, resolver cada una de las k congruencias lineales hasta obtener un sistema equivalente de la forma:

$$\begin{cases} x \equiv a'_1 \pmod{n'_1} \\ x \equiv a'_2 \pmod{n'_2} \\ \quad \vdots \\ x \equiv a'_k \pmod{n'_k}. \end{cases}$$

El problema se reduce ahora a encontrar si todas las congruencias lineales tienen alguna solución en común.

Sistemas de congruencias lineales

Teorema chino del resto

Teorema

Sean $n_1, n_2, \ldots, n_k \in \mathbb{N}$, *y* $a_1, a_2, \ldots, a_k \in \mathbb{Z}$. *Si* $n_1, n_2, \ldots, n_k$ *son mutuamente coprimos, es decir,* $\operatorname{mcd}(n_i, n_j) = 1$ *para* $i \neq j$. *Entonces, el sistema de congruencias lineales*

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \\ \quad\vdots \\ x \equiv a_k \pmod{n_k}. \end{cases}$$

tiene solución, y las soluciones constituyen una única clase de congruencia

Sistemas de congruencias lineales

Demostración.
Hacemos $c_i = \frac{n}{n_i}$ para cada $i = 1, \ldots, k$. Puesto que $\mathrm{mcd}(n_i, n_j) = 1$ para $i \neq j$, se tiene entonces que $\mathrm{mcd}(n_i, c_i) = 1$ para todo $i = 1, \ldots, k$. Podemos resolver entonces la congruencia $c_i x \equiv 1 \pmod{n_i}$ para cada $i = 1, \ldots, k$. Las soluciones de cada congruencia constituyen una única clase de congruencia módulo n_i (inverso de c_i en $\mathbb{Z}_{n_i}$). Llamemos d_i a la solución, es decir, tal que $c_i d_i \equiv 1 \pmod{n_i}$ para todo $i = 1, \ldots, k$. Una solución particular del sistema es

$$x_0 = a_1 c_1 d_1 + a_2 c_2 d_2 + \ldots + a_k c_k d_k.$$

Efectivamente, $x_0 \equiv a_i \pmod{n_i}$ para todo $i = 1, \ldots, k$, puesto que:

- $a_i c_i d_i \equiv a_i \pmod{n_i}$ por ser $c_i d_i \equiv 1 \pmod{n_i}$, y

Sistemas de congruencias lineales

Demostración.

Veamos finalmente que x_0 es la única solución, y que el conjunto de todas las soluciones $x = x_0 + nt, \forall t \in \mathbb{Z}$ constituyen una única clase de congruencia módulo n. Supongamos que x es también solución. Tenemos entonces que

$$\left.\begin{aligned} x &\equiv a_i \pmod{n_i} \\ x_0 &\equiv a_i \pmod{n_i} \end{aligned}\right\} \Rightarrow x \equiv x_0 \pmod{n_i}.$$

Por lo tanto, $n_i \mid (x - x_0)$ para $i = 1, \ldots, k$. Como $\operatorname{mcd}(n_i, n_j) = 1$ para $i \neq j$, es decir, $n_1, n_2, \ldots, n_k$ son mutuamente coprimos, se tiene entonces que $n_1 \cdot n_2 \cdots n_k = n \mid (x - x_0)$ y por lo tanto $x \equiv x_0 \pmod{n}$.

Sistemas de congruencias lineales

Ejemplo

Resolvemos el siguiente sistema de congruencias mediante el teorema chico del resto.

$$\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \\ x \equiv 2 \pmod{7} \end{cases}$$

$c_1 = 5 \cdot 7 = 35$, $c_2 = 3 \cdot 7 = 21$, $c_3 = 3 \cdot 5 = 15$.

$$\begin{aligned} 35x &\equiv 1 \pmod{3} \\ 2x &\equiv 1 \pmod{3} \\ 2x &\equiv 4 \pmod{3} \\ x &\equiv 2 \pmod{3} \end{aligned} \qquad \begin{aligned} 21x &\equiv 1 \pmod{5} \\ x &\equiv 1 \pmod{5} \end{aligned} \qquad \begin{aligned} 15x &\equiv 1 \pmod{7} \\ x &\equiv 1 \pmod{7} \end{aligned}$$

Sistemas de congruencias lineales

Corolario

Sean $n \in \mathbb{N}$ *y* $a, b \in \mathbb{Z}$ *dos enteros cualquiera. Si descomponemos* n *en factores primos como*

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}.$$

Entonces,

$$a \equiv b \pmod{n} \Leftrightarrow \begin{cases} a \equiv b \pmod{p_1^{e_1}} \\ a \equiv b \pmod{p_2^{e_2}} \\ \quad \vdots \\ a \equiv b \pmod{p_k^{e_k}}. \end{cases}$$

Es una consecuencia directa del teorema chino del resto que nos asegura...

Sistemas de congruencias lineales

Ejemplo

Dada la congruencia

$$65x \equiv 45 \pmod{28}.$$

Sabemos que la congruencia lineal tiene solución puesto que $\operatorname{mcd}(65,28) = 1$. Para resolver la congruencia podemos entonces escribirla como un sistema de la forma

$$65x \equiv 45 \pmod{28} \Leftrightarrow \begin{cases} 65x \equiv 45 \pmod{7} \\ 65x \equiv 45 \pmod{2^2} \end{cases} \Leftrightarrow \begin{cases} 2x \equiv 3 \pmod{7} \\ x \equiv 1 \pmod{2^2} \end{cases}$$

$$\Leftrightarrow \begin{cases} x \equiv 5 \pmod{7} \\ x \equiv 1 \pmod{2^2} \end{cases}$$

Luego la solución de la congruencia es

Sistemas de congruencias lineales

Teorema chino del resto generalizado

Teorema

Sean $n_1, n_2, \ldots, n_k \in \mathbb{N}$, *y* $a_1, a_2, \ldots, a_k \in \mathbb{Z}$. *El sistema de congruencias lineales*

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \\ \quad \vdots \\ x \equiv a_k \pmod{n_k} \end{cases}$$

tiene solución si y sólo si $\mathrm{mcd}(n_i, n_j) \mid (a_i - a_j)$ *para todo* $i \neq j$. *De existir solución, todas las soluciones constituyen una única clase de congruencia módulo m*

Sistemas de congruencias lineales

Ejemplo (1)

Dado el sistema

$$\begin{cases} 6x \equiv 10 \pmod{16} \\ 7x \equiv 5 \pmod{12} \\ 2x \equiv 1 \pmod{33}. \end{cases}$$

Resolvemos en primer lugar cada una de las congruencias

$$\begin{aligned} 6x &\equiv 10 \pmod{16} \\ 3x &\equiv 5 \pmod{8} \\ 3x &\equiv 21 \pmod{8} \\ x &\equiv 7 \pmod{8} \end{aligned} \qquad \begin{aligned} 7x &\equiv 5 \pmod{12} \\ 55x &\equiv 5 \pmod{12} \\ 11x &\equiv 1 \pmod{12} \end{aligned} \qquad \begin{aligned} 2x &\equiv 1 \pmod{33} \\ 2x &\equiv 34 \pmod{33} \\ x &\equiv 17 \pmod{33} \end{aligned}$$

Sistemas de congruencias lineales

Ejemplo (1, continuación)

Luego, nos queda el sistema

$$\begin{cases} x \equiv 15 \pmod{8} \\ x \equiv 11 \pmod{12} \\ x \equiv 17 \pmod{33} \end{cases} \Leftrightarrow \begin{cases} x \equiv 7 \pmod{2^3} \\ \cancel{x \equiv 11} \pmod{2^2} \\ x \equiv 11 \pmod{3} \\ \cancel{x \equiv 17} \pmod{3} \\ x \equiv 17 \pmod{11} \end{cases} \Leftrightarrow \begin{cases} x \equiv 7 \pmod{2^3} \\ x \equiv 2 \pmod{3} \\ x \equiv 6 \pmod{11} \end{cases}$$

El sistema tiene solución puesto que $\mathrm{mcd}(8,12) \mid (15-11)$, $\mathrm{mcd}(8,33) \mid (15-17)$, y $\mathrm{mcd}(12,33) \mid (11-17)$. Y la solución es

$x = 7\cdot(33)\cdot(33)^{-1} + 2\cdot(88)\cdot(88)^{-1} + 6\cdot(24)\cdot(24)^{-1} + 264t$

Sistemas de congruencias lineales

Ejemplo (2)

Dado el sistema

$$\begin{cases} 46x \equiv 6 \pmod{140} \\ 65x \equiv 45 \pmod{28}. \end{cases}$$

Sabemos que ambas congruencias tienen solución puesto que $\operatorname{mcd}(46,140) = 2 \mid 6$ y $\operatorname{mcd}(65,28) = 1 \mid 45$. Resolvemos entonces el sistema equivalente

$$\begin{cases} 46x \equiv 6 \pmod{7} \\ 46x \equiv 6 \pmod{5} \\ 46x \equiv 6 \pmod{2^2} \end{cases} \Leftrightarrow \begin{cases} 4x \equiv 6 \pmod{7} \\ x \equiv 1 \pmod{5} \\ 2x \equiv 2 \pmod{2^2} \end{cases} \Leftrightarrow \begin{cases} x \equiv 5 \pmod{7} \\ x \equiv 1 \pmod{5} \\ \cancel{x \equiv 1} \pmod{2} \end{cases}$$

Sistemas de congruencias lineales

Ejemplo (2, continuación)

Luego nos queda el sistema

$$\begin{cases} x \equiv 5 \pmod{7} \\ x \equiv 1 \pmod{5} \\ x \equiv 1 \pmod{2^2} \end{cases}$$

que tiene solución puesto que $\operatorname{mcd}(7,5) = 1$, $\operatorname{mcd}(7,4) = 1$, y $\operatorname{mcd}(5,4) = 1$. Una solución particular es

$$x_0 = 1 \cdot 35 \cdot (-1) + 1 \cdot 28 \cdot 2 + 5 \cdot 20 \cdot (-1) = -79,$$

y todas las soluciones son