Preliminares matemáticos

Inversos modulares
Teorema chino del resto
Cifrado afín II

eman ta zabal zazu

Universidad del País Vasco
Euskal Herriko Unibertsitatea

KISA

Inversos modulares

$(\mathbb{Z}_n, +, \cdot)$ es un anillo conmutativo unitario. ¿Es $(\mathbb{Z}_n, +, \cdot)$ cuerpo?

Un anillo conmutativo unitario $(\mathbb{F}, +, \cdot)$ es *cuerpo* si todo elemento distinto de 0 tiene simétrico para el producto (inverso):

$$0 \neq a \in \mathbb{F} \Rightarrow \exists a^{-1} \in \mathbb{F} \text{ tal que } a \cdot a^{-1} = 1.$$

Es decir, $(\mathbb{F} \setminus \{0\}, \cdot)$ es un grupo conmutativo.

Ejemplos de cuerpos: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.

$\mathbb{Z}$ no es cuerpo: no existe $2^{-1} \in \mathbb{Z}$.

Ejemplo

$$\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}.$$

$\cdot$	0	1	2	3	4
0					
1		1	2	3	4
2		2	4	1	3
3		3	1	4	2
4		4	3	2	1

$$1^{-1} \equiv 1 \quad \text{mód } 5,$$
$$2^{-1} \equiv 3 \quad \text{mód } 5,$$
$$3^{-1} \equiv 2 \quad \text{mód } 5,$$
$$4^{-1} \equiv 4 \quad \text{mód } 5.$$

$(\mathbb{Z}_5, +, \cdot)$ cuerpo.

$$\mathbb{Z}_2 = \{0, 1\}.$$

$\cdot$	0	1
0		
1		1

$$1^{-1} \equiv 1 \quad \text{mód } 2.$$

$(\mathbb{Z}_2, +, \cdot)$ cuerpo.

Ejemplo

$$\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}.$$

$\cdot$	0	1	2	3	4	5
0						
1		1	2	3	4	5
2		2	4	0	2	4
3		3	0	3	0	3
4		4	2	0	4	2
5		5	4	3	2	1

$$1^{-1} \equiv 1 \pmod 6,$$
$$5^{-1} \equiv 5 \pmod 6,$$
$$\text{No existen } 2^{-1}, 3^{-1}, 4^{-1} \pmod 6.$$

$(\mathbb{Z}_6, +, \cdot)$ no es cuerpo.

Teorema (Existencia de inversos modulares)

Existe $a^{-1} \mod n$ *si y sólo si* $\mathrm{mcd}(a, n) = 1$.

El conjunto de elementos invertibles en $\mathbb{Z}_n$ se llama *conjunto reducido de residuos módulo n y se representa* $\mathbb{Z}_n^*$.

$$\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n \,:\, \mathrm{mcd}(a, n) = 1\}$$

$(\mathbb{Z}_n^*, \cdot)$ es grupo conmutativo.

Ejemplo

$$\mathbb{Z}_2^* = \{1\}, \quad \mathbb{Z}_5^* = \{1, 2, 3, 4\}, \quad \mathbb{Z}_6^* = \{1, 5\}.$$

Corolario

$(\mathbb{Z}_n, +, \cdot)$ *es cuerpo si y sólo si n primo.*

Definición

Dado un entero $n > 1$, se llama función (indicatriz) de Euler de *n y se representa $\phi(n)$ al número de elementos del conjunto de residuos reducido de n.*

$$\begin{aligned}\phi(n) &= \mathrm{card}(\mathbb{Z}_n^*)\\ &= \textit{ número de enteros } a \textit{ t. q. } 0 < a < n \textit{ y } \mathrm{mcd}(a, n) = 1.\end{aligned}$$

- Si n primo, $\phi(n) = n - 1$.
- Si $n = pq$, p, q primos distintos, $\phi(n) = (p - 1)(q - 1)$.
- Si $n = p_1^{e_1} \cdots p_r^{e_r}$, $p_1, \ldots, p_r$ primos distintos,

$$\begin{aligned}\phi(n) &= p_1^{e_1-1}(p_1 - 1) \cdots p_r^{e_r-1}(p_r - 1)\\ &= \tfrac{n}{p_1 \ldots p_r}(p_1 - 1) \ldots (p_r - 1).\end{aligned}$$

Ejemplo

$$5 \text{ primo}, \quad \phi(5) = 4, \quad \mathbb{Z}_5^* = \{1, 2, 3, 4\}.$$

$$6 = 2 \cdot 3, \quad \phi(6) = (2-1)(3-1) = 2, \quad \mathbb{Z}_6^* = \{1, 5\}.$$

$$100 = 2^2 \cdot 5^2, \quad \phi(100) = \frac{100}{2 \cdot 5}(2-1)(5-1) = 40.$$

Cálculo de inversos modulares

$$\text{Existe } a^{-1} \mod n \text{ si y sólo si } \mathrm{mcd}(a, n) = 1.$$

Si $\mathrm{mcd}(a, n) = 1$, veremos dos métodos para calcular $a^{-1} \mod n$:

- A partir del Algoritmo extendido de Euclides.
- A partir del Teorema de Euler-Fermat.

A partir del Algoritmo extendido de Euclides

$$\mathrm{mcd}(a, n) = 1 \Leftrightarrow \text{existen enteros } u, v \text{ tales que } au + nv = 1.$$

$$au + nv = 1 \Rightarrow au = 1 + (-v)n \Rightarrow au \equiv 1 \pmod{n}$$

$$\Rightarrow \boxed{a^{-1} \equiv u \pmod{n}}.$$

Podemos calcular u con el Algoritmo extendido de Euclides.

Ejemplo

$$1 = (-1) \cdot 26 + 3 \cdot 9 \Rightarrow 9^{-1} \equiv 3 \pmod{26}.$$

$$9 \cdot 3 \equiv 1 \pmod{26}.$$

A partir del Teorema de Euler-Fermat

Teorema (Pequeño Teorema de Fermat)

Sea n un número primo. Entonces, para cualquier entero positivo a tal que $\mathrm{mcd}(a, n) = 1$*,*

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

Teorema (Teorema de Euler-Fermat)

Sean a, n números enteros positivos tales que $\mathrm{mcd}(a, n) = 1$*. Entonces,*

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

Consecuencia

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

<u>Observación</u>: Para calcular inversos por este método debemos ser capaces de calcular $\phi(n)$.

Teorema chino del resto

El Teorema chino del resto permite resolver ciertos sistemas de congruencias.

Teorema (Teorema chino del resto)

Sea $n = p_1 \cdots p_r$ *con* $p_1, \ldots, p_r$ *primos entre sí y sean* $a_1, \ldots, a_r$ *números enteros. Entonces existe un único (*$\text{mód}\, n$*)* entero* x *tal que*

$$x \equiv a_i \mod p_i, \quad i = 1, \ldots, r.$$

Este entero x *es:*

$$x \equiv \sum_{i=1}^{r} \frac{n}{p_i} y_i a_i \mod n,$$

donde $y_i \equiv (\frac{n}{p_i})^{-1} \mod p_i,\ i = 1, \ldots, r.$

*La unicidad ($\text{mód}\, n$) significa que existe una única solución en $\mathbb{Z}_n$ y, que si x es una solución entonces también lo es $x + kn$ para cuaquier entero k.

Ejemplo

$$\left.\begin{array}{l} x \equiv 5 \pmod 8 \\ x \equiv 4 \pmod 5 \\ x \equiv 2 \pmod 3 \end{array}\right\} \qquad n = 8 \cdot 5 \cdot 3 = 120,$$

$$\frac{120}{8} = 15, \quad y_1 \equiv 15^{-1} \equiv 7 \pmod 8,$$

$$\frac{120}{5} = 24, \quad y_2 \equiv 24^{-1} \equiv 4 \pmod 5,$$

$$\frac{120}{3} = 40, \quad y_3 \equiv 40^{-1} \equiv 1 \pmod 3,$$

$$15 \cdot 7 \cdot 5 + 24 \cdot 4 \cdot 4 + 40 \cdot 1 \cdot 2 = 989 \equiv 29 \pmod{120}.$$

Solución:

$$x \equiv 29 \pmod{120}.$$

Efectivamente:

$$\begin{array}{lll} 29 \equiv 5 \pmod 8, & 29 \equiv 4 \pmod 5, & 29 \equiv 2 \pmod 3, \\ 149 \equiv 5 \pmod 8, & 149 \equiv 4 \pmod 5, & 149 \equiv 2 \pmod 3, \\ & \vdots & \end{array}$$

Caso particular: $r = 2$

Sea $n = pq$ con p, q primos relativos y sean a, b números enteros. Existe un único $(\text{mód}\, n)$ entero x tal que

$$\begin{aligned} x &\equiv a \mod p, \\ x &\equiv b \mod q. \end{aligned}$$

Este entero x es:

$$x \equiv (qq_1 a + pp_1 b) \mod n,$$

donde

$$\begin{aligned} q_1 &\equiv q^{-1} \mod p, \\ p_1 &\equiv p^{-1} \mod q. \end{aligned}$$

Ejemplo

$$\left.\begin{aligned} x &\equiv 4 \mod 7 \\ x &\equiv 2 \mod 3 \end{aligned}\right\} \quad n = 7 \cdot 3 = 21,$$

$$q_1 \equiv 3^{-1} \equiv 5 \mod 7, \qquad p_1 \equiv 7^{-1} \equiv 1 \mod 3.$$

Solución:

$$x \equiv (3 \cdot 5 \cdot 4 + 7 \cdot 1 \cdot 2) \equiv 11 \mod 21.$$

Cifrado afín II

Cifrado afín sobre letras

Recordemos la transformación afín: a cada letra del alfabeto le asignamos un número.

Si el número de letras del alfabeto es N, entonces

$$\mathcal{M} = \mathcal{C} = \mathbb{Z}_N.$$

La función de cifrado es

$$C \equiv aM + b \mod N, \qquad \text{con } \operatorname{mcd}(a, N) = 1.$$

Clave de cifrado: (a, b).

Como $\mathrm{mcd}(a, N) = 1$, existe $a^{-1} \mod N$ y la función de descifrado es

$$\begin{aligned} M &\equiv a^{-1}C - a^{-1}b \mod N \\ &\equiv a'C + b' \mod N, \end{aligned}$$

donde

$$a' \equiv a^{-1} \mod N; \quad b' \equiv -a^{-1}b \mod N.$$

Clave de descifrado: (a', b').

El cifrado afín es fácil de romper:

- Probando todas las claves posibles hasta encontrar un mensaje que tenga sentido.
- Con *análisis de frecuencias.*

Cifrado afín sobre k-gramas

Transformación afín (k-gramas): $\mathcal{M} = \mathcal{C} = \mathbb{Z}_{N^k}$.

Las funciones de cifrado y descifrado son como en el caso de la transformación afín sobre las letras, pero módulo N^k.

Función de cifrado:

$$C \equiv aM + b \pmod{N^k} \quad \text{con } \operatorname{mcd}(a, N) = 1.$$

$$\operatorname{mcd}(a, N) = 1 \Rightarrow \operatorname{mcd}(a, N^k) = 1 \Rightarrow \text{ existe } a^{-1} \pmod{N^k}.$$

Función de descifrado:

$$M \equiv a'C + b' \pmod{N^k},$$

donde

$$a' \equiv a^{-1} \pmod{N^k}; \quad b' \equiv -a^{-1}b \pmod{N^k}.$$

Ejemplo

$$N = 26, \quad k = 2, \quad a = 159, \quad b = 580$$

$$\text{“ADIOS”} \rightarrow \text{“AD”},\ \text{“IO”},\ \text{“SQ”}$$

$$\text{“AD”} \rightarrow (0, 3) \rightarrow 26 \cdot 0 + 3 = 3$$

$$\text{“ADIOS”} \ \rightarrow (3,\ 222,\ 484)$$

$$159 \cdot 3 + 580 = 1057 \equiv 381 \pmod{676}$$

$$(3,\ 222,\ 484) \rightarrow (381,\ 50,\ 472)$$

$$381 = 26 \cdot 14 + 17, \quad (14, 17) \rightarrow \text{“OR”}$$

$$50 = 26 \cdot 1 + 24, \quad (1, 24) \rightarrow \text{“BY”}$$

$$472 = 26 \cdot 18 + 4, \quad (18, 4) \rightarrow \text{“SE”}$$

$$\text{“ADIOS”} \ \rightarrow \ \text{“ORBYSE”}$$

Descifrado: $N = 26, \quad k = 2, \quad a = 159, \quad b = 580$

$$a' \equiv 159^{-1} \equiv 659 \mod 676, \quad b' \equiv -580 \cdot 659 \equiv 396 \mod 676$$

$$\text{“YYDI”} \rightarrow \text{“YY”}, \text{“DI”}$$

$$\text{“YY”} \rightarrow (24, 24) \rightarrow 26 \cdot 24 + 24 = 648$$

$$\text{“YYDI”} \rightarrow (648,\ 86)$$

$$659 \cdot 648 + 396 = 427428 \equiv 196 \mod 676$$

$$(648,\ 86) \rightarrow (196,\ 286)$$

$$196 = 26 \cdot 7 + 14, \quad (7, 14) \rightarrow \text{“HO”}$$

$$286 = 26 \cdot 11 + 0, \quad (11, 0) \rightarrow \text{“LA”}$$

$$\text{“YYDI”} \rightarrow \text{“HOLA”}$$

Fin de la sección