Preliminares matemáticos

Cifrado afín I
Divisibilidad. Números primos

eman ta zabal zazu
Universidad del País Vasco
Euskal Herriko Unibertsitatea

KISA

Cifrado afín I

Supongamos que tenemos un alfabeto de N letras.

La función de cifrado *afín* es

$$\begin{array}{rccc} f: & \mathcal{M} & \longrightarrow & \mathcal{C} \\ & M & \mapsto & C \equiv aM + b \mod N \end{array}$$

donde M es el equivalente numérico de cada letra.

La *clave* de cifrado es: (a, b).

Observación: $0 \leq M \leq N - 1$, $0 \leq C \leq N - 1$. Es decir,

$$M, C \in \{0, 1, \ldots N - 1\} = \mathbb{Z}_N.$$

Por tanto

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

Ejemplo

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

$N = 26$

Clave de cifrado: $a = 5,\ b = 2$

$$\text{“HOLA”} \rightarrow (7, 14, 11, 0).$$

$$a \cdot 7 + b = 5 \cdot 7 + 2 = 37 \equiv 11 \quad \text{mód } 26$$

$$a \cdot 14 + b = 5 \cdot 14 + 2 = 72 \equiv 20 \quad \text{mód } 26$$

$$\text{“HOLA”} \rightarrow (7, 14, 11, 0) \rightarrow (11, 20, 5, 2) \rightarrow \text{“LUFC”}$$

Descifrado

$$C \equiv aM + b \mod N \;\Leftrightarrow\; aM \equiv C - b \mod N$$

$$\Leftrightarrow\; M \equiv a^{-1}C - a^{-1}b \mod N.$$

Observación:

$$\text{Existe } a^{-1} \mod N \Leftrightarrow \mathrm{mcd}(a, N) = 1.$$

Si $\mathrm{mcd}(a, N) \neq 1$, puede ocurrir que textos en claro diferentes den lugar al mismo cifrado.

Ejemplo

$$N = 26, \quad a = 2,\ b = 1.$$

$$\mathrm{mcd}(a, N) = \mathrm{mcd}(2, 26) = 2.$$

- "YA" $\rightarrow (24, 0)$

$$2 \cdot 24 + 1 = 49 \equiv 23 \pmod{26}, \quad 2 \cdot 0 + 1 = 1 \equiv 1 \pmod{26}.$$

$$\text{“YA”} \rightarrow (24, 0) \rightarrow (23, 1) \rightarrow \text{“XB”}$$

- "LA" $\rightarrow (11, 0)$

$$2 \cdot 11 + 1 = 23 \equiv 23 \pmod{26}, \quad 2 \cdot 0 + 1 = 1 \equiv 1 \pmod{26}.$$

$$\text{“LA”} \rightarrow (11, 0) \rightarrow (23, 1) \rightarrow \text{“XB”}$$

Divisibilidad. Números primos

Definición

Sean a y b dos números enteros, con $a \neq 0$.

- *Se dice que a* divide *a b o que a es un* divisor *de b, o que b es un* múltiplo *de a si existe un número entero k tal que $b = ak$. Se denota*
$$a \mid b.$$
- *Si a, b son positivos, $a \mid b$, $a \neq 1$ y $a \neq b$, se dice que a es un* divisor propio *de b.*

Ejemplo

Divisores de 12: $1, 2, 3, 4, 6, 12, -1, -2, -3, -4, -6, -12$.
Divisores propios de 12: $2, 3, 4, 6$.

Definición

Un número entero $n > 1$ es primo si no tiene divisores propios.

Teorema (Teorema fundamental de la aritmética)

Todo número entero puede descomponerse de manera única como producto de primos, salvo orden de los factores.

Ejemplo

$$490 = 2 \cdot 5 \cdot 7^2 = 5 \cdot 2 \cdot 7^2 = 7 \cdot 5 \cdot 7 \cdot 2 = \ldots.$$

Teorema (Euclides: La infinitud de los números primos)

Dado un número primo p, siempre existe otro primo mayor.

Definición

Dados dos enteros a y b con $a \neq 0$ *o* $b \neq 0$*, el* máximo común divisor *de a y b,* $\mathrm{mcd}(a, b)$*, es un entero positivo d tal que*

1. *d es un divisor común de a y b:* $d \mid a$ *y* $d \mid b$*.*
2. *Cualquier divisor común de a y b divide a d (d es el "máximo" entero cumpliendo la propiedad anterior).*

Para el cálculo del máximo común divisor de dos enteros, $d = \mathrm{mcd}(a, b)$, utilizaremos el **algoritmo de Euclides**.

Teorema

Dados dos números enteros a y b, sea $d = \mathrm{mcd}(a, b)$. Entonces existen números enteros u y v tales que

$$au + bv = d.$$

Se suele decir que d es una "combinación lineal" de a y b con *coeficientes* u y v. Además, d es el mínimo entero positivo que puede expresarse como una combinación lineal de a y b.

Ejemplo

$$\mathrm{mcd}(90, 70) = 10 = (-3) \cdot 90 + 4 \cdot 70. \qquad u = -3,\ v = 4.$$

Para el cálculo de los números enteros u y v utilizaremos el **algoritmo de Euclides extendido**.

Definición

Se dice que dos números enteros a y b son primos relativos *si*

$$\mathrm{mcd}(a, b) = 1.$$

Si a y b son primos relativos, entonces 1 es una combinación lineal de a y b. Recíprocamente, si 1 es una combinación lineal de a y b, entonces es el mínimo entero positivo que se puede expresar de esta forma.

Por tanto, a, b son primos relativos si y sólo si existen enteros u y v tales que

$$au + bv = 1.$$

Ejemplo

$$1 \cdot 78 + (-1) \cdot 77 = 1 \Rightarrow \mathrm{mcd}(78, 77) = 1.$$

78 y 77 son primos relativos.

Algoritmo de Euclides para el cálculo de $\mathrm{mcd}(a, b)$

Sean a, b números enteros, $a \geq 0$, $b > 0$. Comenzamos dividiendo a entre b y después sucesivamente dividimos cada divisor por el resto

$$\begin{array}{r|l} a & \underline{\ b\ } \\ r_1 & \ q_1 \end{array} \qquad a = q_1 b + r_1, \qquad 0 < r_1 < b$$

$$\begin{array}{r|l} b & \underline{\ r_1\ } \\ r_2 & \ q_2 \end{array} \qquad b = q_2 r_1 + r_2, \qquad 0 < r_2 < r_1$$

$$\begin{array}{r|l} r_1 & \underline{\ r_2\ } \\ r_3 & \ q_3 \end{array} \qquad r_1 = q_3 r_2 + r_3, \qquad 0 < r_3 < r_2$$

$$\vdots \qquad\qquad \vdots \qquad\qquad\qquad \vdots$$

$$\begin{array}{rl} \vdots & \quad\vdots \\ r_i & \left|\, \underline{\quad r_{i+1} \quad}\right. \\ r_{i+2} & \quad q_{i+2} \\ \vdots & \quad\vdots \end{array} \qquad \begin{array}{c} \vdots \\ r_i = q_{i+2} r_{i+1} + r_{i+2}, \quad 0 < r_{i+2} < r_{i+1} \\ \\ \vdots \end{array}$$

Como cada vez obtenemos restos más pequeños, alguna vez obtendremos resto 0:

$$\begin{array}{rl} r_{k-1} & \left|\, \underline{\quad r_k \quad}\right. \\ 0 & \quad q_{k+1} \end{array} \qquad r_{k-1} = q_{k+1} r_k + 0$$

$$b > r_1 > r_2 > \cdots > r_{k-1} > r_k > 0 \; (= r_{k+1}).$$

Entonces, r_k, el último resto distinto de 0, es el $\mathrm{mcd}(a, b)$:

$$r_k = \mathrm{mcd}(a, b).$$

<u>Observación</u>: Si $a < 0$ o $b < 0$,

$$\mathrm{mcd}(a, b) = \mathrm{mcd}(|a|, |b|).$$

Ejemplo

Para calcular $\mathrm{mcd}(560, 427)$:

$$\begin{array}{r|l} 560 & \underline{\;427\;\;\;\;} \\ 133 & \;1 \end{array} \qquad \begin{array}{r|l} 427 & \underline{\;133\;\;\;\;} \\ 28 & \;3 \end{array} \qquad \begin{array}{r|l} 133 & \underline{\;28\;\;\;\;} \\ 21 & \;4 \end{array}$$

$$\begin{array}{r|l} 28 & \underline{\;21\;\;\;\;} \\ 7 & \;1 \end{array} \qquad \begin{array}{r|l} 21 & \underline{\;7\;\;\;\;} \\ 0 & \;3 \end{array}$$

$$\mathrm{mcd}(560, 427) = 7, \quad \mathrm{mcd}(-560, 427) = 7,$$

$$\mathrm{mcd}(560, -427) = 7, \quad \mathrm{mcd}(-560, -427) = 7.$$

Algoritmo de Euclides extendido

Ejemplo

$$\mathrm{mcd}(560, 427) = 7 \Rightarrow \text{ existen } u, v \text{ tales que } 7 = u560 + v427.$$

$$\begin{array}{r|l} 560 & 427 \\ \cline{2-2} 133 & 1 \end{array} \qquad 560 = 1 \cdot 427 + 133 \qquad 133 = 560 - 1 \cdot 427$$

$$\begin{array}{r|l} 427 & 133 \\ \cline{2-2} 28 & 3 \end{array} \qquad 427 = 3 \cdot 133 + 28 \qquad 28 = 427 - 3 \cdot 133$$

$$\begin{array}{r|l} 133 & 28 \\ \cline{2-2} 21 & 4 \end{array} \qquad 133 = 4 \cdot 28 + 21 \qquad 21 = 133 - 4 \cdot 28$$

$$\begin{array}{r|l} 28 & 21 \\ \cline{2-2} 7 & 1 \end{array} \qquad 28 = 1 \cdot 21 + 7 \qquad 7 = 28 - 1 \cdot 21$$

$$\begin{array}{r|l} 21 & 7 \\ \cline{2-2} 0 & 3 \end{array} \qquad 21 = 3 \cdot 7$$

$$133 \overset{(1)}{=} 560 - 1 \cdot 427, \quad 28 \overset{(2)}{=} 427 - 3 \cdot 133$$

$$21 \overset{(3)}{=} 133 - 4 \cdot 28, \quad 7 \overset{(4)}{=} 28 - 1 \cdot 21$$

$$\begin{aligned}
{\color{magenta}7} &\overset{(4)}{=} 28 + (-1) \cdot 21 \\
&\overset{(3)}{=} 28 + (-1) \cdot (133 - 4 \cdot 28) \\
&= (-1) \cdot 133 + (1 + 4) \cdot 28 = (-1) \cdot 133 + 5 \cdot 28 \\
&\overset{(2)}{=} (-1) \cdot 133 + 5 \cdot (427 - 3 \cdot 133) \\
&= 5 \cdot 427 + (-1 - 15) \cdot 133 = 5 \cdot 427 + (-16) \cdot 133 \\
&\overset{(1)}{=} 5 \cdot 427 + (-16) \cdot (560 - 1 \cdot 427) \\
&= (-16) \cdot 560 + (5 + 16) \cdot 427 = (-16) \cdot {\color{blue}560} + 21 \cdot {\color{blue}427}
\end{aligned}$$

Fin de la sección