Cum se calculează inversul modular?

Exemplu $21^{-1} \pmod{26} = a \qquad a \cdot 21 \equiv 1 \pmod{26}$

Există pentru că $\gcd(21, 26) = 1$.

Avem (cel puțin) două metode!

① **Teoremă** (Euler) $n \in \mathbb{N}^*$, $a \in \mathbb{N}$ cu $\gcd(a, n) = 1$

$$\Rightarrow a^{\varphi(n)} \equiv 1 \pmod{n}$$

$$\varphi(n) = \text{card}\{\xi \mid \xi < n, \xi \text{ divizor al lui } n, \gcd(\xi, n) = 1\}$$

$1 \le \xi \le n$

- $\varphi(p) = p - 1$
- $n = p \cdot \xi \Rightarrow \varphi(n) = (p-1)(\xi - 1)$
- $\varphi(n) = n \prod_{p \mid n} \left(1 - \frac{1}{p}\right)$

p prim.

$$n = p_1^{k_1} \cdots p_{\ell}^{k_\ell} \Rightarrow \varphi(n) = (p_1 - 1) p_1^{k_1 - 1} \cdots (p_\ell - 1) p_\ell^{k_\ell - 1}.$$

Corolar $\gcd(a, n) = 1 \Rightarrow a$ e inversabil $\pmod{n}$

$$\Rightarrow \boxed{a^{-1} \equiv a^{\varphi(n) - 1} \pmod{n}}$$

Revenind la exemplu $\varphi(26) = \varphi(2 \cdot 13) = 1 \cdot 12 = 12$

$\Rightarrow 21^{-1} \equiv 2^{11} \pmod{26}$. Acum am transformat problema la o exponențiere. Nu e complicat dacă numerele nu mari!

Exponențierea rapidă

$(G, \cdot)$ monoid $g \in G$ și $a \in \mathbb{N}$. Vrem să calculăm eficient g^a (în monoidul G).

- Scriem $a = \sum_{i=0}^{k} a_i \cdot 2^i$ (scrierea binară a lui a), $a_i \in \{0,1\}$

$$\Rightarrow g^a = g^{\sum_{i=0}^{k} a_i 2^i} = \prod_{i=0}^{k} (g^{2^i})^{a_i} = \prod_{\substack{i=0 \\ a_i=1}}^{k} g^{2^i}.$$

Deci avem:

1. - calculăm succesiv puterile (puterile) g^{2^i} $i = \overline{0,k}$
   observăm $g^{2^{i+1}} = (g^{2^i})^2$ deci ridicăm la pătrat pe cea precedentă!
2. recalculează produsul acelor g^{2^i} pentru care $a_i = 1$.

Exemplu (continuare)

$$11 = 2^3 + 2 + 1 \Rightarrow 21^{11} = 21^{2^3} \cdot 21^2 \cdot 21 \equiv$$
$$\equiv 25 \cdot 1 \cdot 21 \equiv 5 \pmod{26}$$

$21^2 = 25$

$21^{2^2} = 25^2 = 1$

$21^{2^3} = 1$.

Alt exemplu $107^{101} \pmod{131}$

$$101 = 2^6 + 2^5 + 2^2 + 1$$

$107^2 = 52$, $107^{2^2} = 84$ $107^{2^3} = 113$

$107^{2^4} = 62$, $107^{2^5} = 45$ $107^{2^6} = 60$

$\Rightarrow 60 \cdot 45 \cdot 84 \cdot 107 = 112$.

(2) (alfele)

Teorema (algoritmul lui Euclid extins)

Fie $R_0, R_1 \in \mathbb{N}$, $R_0 > R_1$

$$\begin{cases} R_0 = Q_1 \cdot R_1 + R_2 & 0 < R_2 < R_1 \\ R_1 = Q_2 \cdot R_2 + R_3 & 0 < R_3 < R_2 \\ \vdots \\ R_{m-2} = Q_{m-1} \cdot R_{m-1} + R_m & 0 < R_m < R_{m-1} \\ R_{m-1} = Q_m \cdot R_m \end{cases}$$

$\rightsquigarrow$ alg lui Euclid $\gcd(R_0, R_1) = R_m$.

Vrem $a^{-1} \pmod n$, $a < n$, $\gcd(a, n) = 1$

Facem $n = R_0$ și $a = R_1$

- Definim recurent $t_0, t_1, \dots, t_m$ prin.

$t_0 = 0$, $t_1 = 1$, $t_j = t_{j-2} - Q_{j-1} t_{j-1} \pmod{R_0}$ $j \geq 2$

unde Q_j sunt câturile definite mai sus.

Teoremă $\forall j = \overline{1, m}$ $R_j \equiv t_j \cdot R_1 \pmod{R_0}$ unde Q_j, R_j sunt definite de alg Euclid iar t_j de relațiile de recurență de mai sus.

Demonstrație inducție după i

$i=0 \quad R_0 \equiv t_0 R_1 \pmod{R_0}$ $(t_0 = 0$ pt-ca$)$

$i=1 \quad R_1 \equiv t_1 R_1 \pmod{R_0}$ $(t_1 = 1)$

$$R_i = R_{i-2} - q_{i-1} \cdot R_{i-1} \equiv (t_{i-2} - q_{i-1} t_{i-1}) R_1 \pmod{R_0}$$
$$= t_i R_1 \pmod{R_0}$$

Corolar $\gcd(R_0, R_1) = 1 \Rightarrow 1 \equiv t_m \cdot R_0 \pmod{R_0}$

$$\Rightarrow t_m = R_1^{-1} \pmod{R_0}$$

Revenim la exemplu

k	R_k	q_k	t_k
0	26	-	0
1	21	1	1
2	5	4	-1
3	1	5	5
	0		

$t_0 = 0, t_1 = 1$

$t_i = t_{i-2} - t_{i-1} \cdot q_{i-1}$.

Cifrul afin

- este un caz particular de afin cu substituție monoalfabetică
- $M = C = \mathbb{Z}_{26}$; $K \subset \mathbb{Z}_{26} \times \mathbb{Z}_{26}$ $\exists (a,b)$ (cheile)
- funcția de criptare $e_{(a,b)} : \mathbb{Z}_{26} \to \mathbb{Z}_{26}$

$$e_{(a,b)}(x) = ax + b \pmod{26}$$

funcție afină

- Obs pentru $a = 1$ avem cifrul Caesar
- $e_{(a,b)}$ trebuie să fie injectivă $\Leftrightarrow$ a e inversabil (în $\mathbb{Z}_{26}$)

$\Updownarrow$

$\gcd(a, 26) = 1$

Câte chei are cifrul afin?

$\varphi(26) = \varphi(2 \cdot 13) = 12$. $\Rightarrow$ avem 12×26 chei

- funcția de decriptare $d_{(a,b)} : \mathbb{Z}_{26} \to \mathbb{Z}_{26}$

$$d_{(a,b)}(y) = a'(y - b) \pmod{26}$$

Cifrul Hill.

- exemplu de cifru cu substituție polialfabetică
- inventat de Lester S. Hill în 1929

$M = C = \mathbb{Z}_{26}^n$ (fixăm n)

$K \subset M_n(\mathbb{Z}_{26}) \times \mathbb{Z}_{26}^n$

$e_{(A,b)} : \mathbb{Z}_{26}^n \to \mathbb{Z}_{26}^n$

$e_{(A,b)}(x) = A \cdot x^t + b^t$

$$\begin{pmatrix} A \end{pmatrix} \begin{pmatrix} x_1 \\ x_n \end{pmatrix} + \begin{pmatrix} b_1 \\ b_n \end{pmatrix} = \begin{pmatrix} y_1 \\ y_n \end{pmatrix}$$

- Vrem $e_{(A,b)}$ injectivă $\Leftrightarrow$ $A \in M_n(\mathbb{Z}_{26})$ inversabilă

$\Updownarrow$

$\gcd(\det A, 26) = 1$.

- Obs Pentru a evita "complicații" cu $\det A$ se recomandă mulțimi cu număr prim de elemente ai Ainversabilă $\Leftrightarrow \det A \neq 0$.