ARITMETICĂ MODULARĂ

Notație:

$$a \equiv b(\text{mod } m) \Leftrightarrow m/(a-b) \Leftrightarrow a \text{ mod } m = b \text{ mod } m$$

Proprietăți:

- $a \equiv a(\text{mod } m)$ -> reflexivitate
- $a \equiv b(\text{mod } m) \Longrightarrow b \equiv a(\text{mod } m)$ -> simetrie
- $\left.\begin{matrix} a \equiv b(\text{mod } m) \\ b \equiv c(\text{mod } m) \end{matrix}\right\} \Longrightarrow a \equiv c(\text{mod } m)$ -> tranzitivitate
- $a \equiv b(\text{mod } m) \Longrightarrow a+k \equiv b+k(\text{mod } m)$
- $a \equiv b(\text{mod } m) \Longrightarrow a \cdot k \equiv b \cdot k(\text{mod } m)$
- $a \equiv b(\text{mod } m) \Longrightarrow a^k \equiv b^k(\text{mod } m)$
- $\left.\begin{matrix} a \equiv b(\text{mod } m) \\ c \equiv d(\text{mod } m) \end{matrix}\right\} \Longrightarrow a+c \equiv b+d(\text{mod } m)$
- $\left.\begin{matrix} a \equiv b(\text{mod } m) \\ c \equiv d(\text{mod } m) \end{matrix}\right\} \Longrightarrow a-c \equiv b-d(\text{mod } m)$
- $\left.\begin{matrix} a \equiv b(\text{mod } m) \\ c \equiv d(\text{mod } m) \end{matrix}\right\} \Longrightarrow a \cdot c \equiv b \cdot d(\text{mod } m)$

Mica teoremă a lui Fermat (1640):

Dacă p este un număr prim și $a \in \mathbb{Z}$, atunci $a^p \equiv a(\text{mod } p)$.

$20^7 \equiv 20(\text{mod } 7) \Longrightarrow 7 \,/\, (20^7 - 20)$

Corolar:

Dacă p este un număr prim și $a \in \mathbb{Z}$ a.î. $(a,p) = 1$, atunci $a^{p-1} \equiv 1(\text{mod } p)$.

(a, b) = cmmdc(a, b)

Definiție: Numărul a este *coprim* cu b dacă (a, b) = 1

Indicatorul lui Euler (1760):

$\varphi(n) =$ numărul numerelor mai mici decât n și coprime cu n

$\varphi(12) = 4$ (deoarece numerele 1,5,7,11 sunt coprime cu 12)

$\varphi(12) = \varphi(2^2 \cdot 3) = 12\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) = 12 \cdot \frac{1}{2} \cdot \frac{2}{3} = \frac{24}{6} = 4$

Proprietăți:

- Dacă $n = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_m^{k_m}$, unde $p_1, p_2, \ldots, p_m$ sunt numere prime, atunci:

$$\varphi(n) = n \prod_{p/n} \left(1 - \frac{1}{p}\right)$$

- Dacă p este un număr prim, atunci $\varphi(p) = p - 1$.
- Dacă $(a, b) = 1$, atunci $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$.
  $\varphi(12) = \varphi(3 \cdot 4) = \varphi(3) \cdot \varphi(4) = (3 - 1) \cdot 2 = 2 \cdot 2 = 4$

Teorema lui Euler (1736):

Dacă $a, n \in \mathbb{Z}$ astfel încât $(a, n) = 1$, atunci $a^{\varphi(n)} \equiv 1 (\mathrm{mod}\, n)$.

Mica teoremă a lui Fermat (1640):

Dacă p este un număr prim și $a \in \mathbb{Z}$ a.î. $(a, p) = 1$, atunci $a^{p-1} \equiv 1 (\mathrm{mod}\, p)$.

Corectitudinea cifrului RSA:

- **Generarea cheilor:**
  - se aleg două numere naturale prime p şi q
  - se calculează produsul $n = p \cdot q$
  - se calculează indicatorul lui Euler $\varphi(n) = (p-1) * (q-1)$
  - se alege un număr natural $1 < e < \varphi(n)$ astfel încât $cmmdc(\varphi(n), e) = 1$
  - se calculează numărul natural $d \equiv e^{-1}\big(\mathrm{mod}\ \varphi(n)\big)$
  - *cheia publică* sunt numerele e și n
  - *cheia privată* este numărul d
- **Criptarea:** $C \equiv M^e (\mathrm{mod}\ n)$
- **Decriptarea:** $M \equiv C^d (\mathrm{mod}\ n)$

Trebuie să demonstrăm faptul că $M \equiv (M^e)^d (\mathrm{mod}\ n) \Leftrightarrow M \equiv M^{e \cdot d} (\mathrm{mod}\ n) \Leftrightarrow$ $M^{e \cdot d} \equiv M (\mathrm{mod}\ n)$.

Deoarece $n = p \cdot q$ și $(p, q) = 1$ este suficient să demonstrăm că:

- $M^{e \cdot d} \equiv M (\mathrm{mod}\ p)$
- $M^{e \cdot d} \equiv M (\mathrm{mod}\ q)$

Cazul 1: $p | M \Longrightarrow M \equiv 0 (\mathrm{mod}\ p) \Longrightarrow M^{e \cdot d} \equiv 0 (\mathrm{mod}\ p) \Longrightarrow M^{e \cdot d} \equiv M (\mathrm{mod}\ p)$

Cazul 2: $p \nmid M \xRightarrow{Th.\ Fermat} M^{p-1} \equiv 1 (\mathrm{mod}\ p)$

Dar $e \cdot d \equiv 1\big(\mathrm{mod}\ \varphi(n)\big) \equiv 1\big(\mathrm{mod}\ (p-1) \cdot (q-1)\big) \Longrightarrow$

$\Longrightarrow \exists k \in \mathbb{N}$ a.î. $e \cdot d = 1 + k \cdot (p-1) \cdot (q-1) \Longrightarrow$

$$\Longrightarrow M^{e \cdot d} = M^{1 + k \cdot (p-1) \cdot (q-1)} = M \cdot \underbrace{(M^{p-1})}_{\equiv 1 (\mathrm{mod}\ p)}{}^{k \cdot (q-1)} \equiv M (\mathrm{mod}\ p) \Longrightarrow$$

$\Longrightarrow M^{e \cdot d} \equiv M (\mathrm{mod}\ p)$

Analog demonstrăm faptul că $M^{e \cdot d} \equiv M (\mathrm{mod}\ q)$.