Tema 3 - Criptografie

1. Demonstrați că dacă $n=\prod_{i=1}^{K} p_i^{\alpha_i}$ și $a^{p_i^{\alpha_i}} \equiv a \pmod{p_i}$, $\forall p_i$, atunci $a^n \equiv a \pmod{n}$

Pentru a demonstra acest exercițiu putem utiliza Teorema Chineză a resturilor.

În cazul nostru $n=\prod_{i=1}^{K} p_i^{\alpha_i}$ - unde p_i sunt prime distincte deoarece $p_i^{a_i}$ sunt puteri ale numerelor prime distincte fiind coprime

Demonstrație: Este suficient să arătăm că $a^n \equiv a \pmod{p_i^{\alpha_i}}$, $\forall i$

Pas 1: Avem $a^{p_i^{a_i}} \equiv a \pmod{p_i^{\alpha_i}}$ ①

$n=\prod_{i=1}^{K} p_i^{\alpha_i} \rightarrow$ putem rescrie ca $n = p_i^{a_i} \cdot m$ unde m este produs de $p_j^{\alpha_j}$, pt $i \neq j$

~~m~~

Pas 2: $n = p_i^{\alpha_i} \cdot m$ deci $a^n = a^{p_i^{\alpha_i} \cdot m}$

Folosim ① $\Rightarrow a^{p_i^{a_i}} = a + k \cdot p_i^{a_i}$

Pas 3: $a + k \cdot p_i^{\alpha_i} \,|^m = (a + k \cdot p_i^{\alpha_i})^m$

Aplicăm binomul lui Newton

$$(a + k \cdot p_i^{\alpha_i})^m = a^m + \binom{m}{1} a^{m-1}(k \cdot p_i^{\alpha_i}) + \dots + (k \cdot p_i^{\alpha_i})^m$$

observăm că orice termen este multiplu de $p_i^{\alpha_i}$ în afară de a^m

Pas 4: Deci $a^n \equiv a^m \pmod{p_i^{\alpha_i}}$

Pas 5: Prin TCR, există un ~~...~~ $x \pmod{n}$ care satisface toate aceste congruențe

observăm că acest $x = a \Rightarrow a^n = \boxed{a \pmod{n}}$

3) $2^n - 1$ prim $\Rightarrow$ n prim

Pt $n \leq 3$

$n = 0 \Rightarrow 2^0 - 1 = 0$ (nu este prim)

$n = 1 \Rightarrow 2^1 - 1 = 1$ (nu este prim)

$n = 2 \Rightarrow 2^2 - 1 = 3$ (este prim dar n nu este prim)

$n = 3 \Rightarrow 2^3 - 1 = 7$ (este prim și n prim)

Pt $n > 3$

Pp prin R.A că n nu este prim $\Rightarrow \exists\, k, m \in \mathbb{N}^* \setminus \{1\}$ a.î. $n = k \cdot m$

$2^n - 1 = 2^{k \cdot m} - 1 = (2^k)^m - 1 = (2^k - 1)\left((2^k)^{m-1} + (2^k)^{m-2} + \ldots + (2^k)\right)$

$k \in \mathbb{N}^* \setminus \{1\} \Rightarrow 2^k - 1 > 1$

$2^k < 2^m \Rightarrow 2^k - 1 < 2^n - 1$

$\Rightarrow 2^n - 1$ are divizor diferit de 1 și de el însuși

$\Rightarrow 2^n - 1$ nu e prim

4) Demonstrați Legea reciprocității pătratice

Pentru două numere prime impare distincte p și q, simbolurile $\left(\frac{p}{q}\right)$ și $\left(\frac{q}{p}\right)$ satisfac

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$$

Pentru a demonstra această teoremă, vom (~~[illegible]~~) aplica un argument bazat pe suma lui Gauss.

Demonstrație: Fie p un nr prim impar. Definim suma lui Gauss $G(a,p)$ pentru a un întreg:

$$G(a,p) = \sum_{n=0}^{p-1} e^{\frac{2\pi i a n^2}{p}}$$

Pas 2: ~~Propr~~ Suma lui Gauss are câteva proprietăți importante

$$G(1,p)=\sum_{n=0}^{p-1} e^{\frac{2\pi i n}{p}} = \sqrt{p} \text{ dacă } p \equiv 1 \pmod 4$$

$$\text{și } i\sqrt{p} \text{ dacă } p \equiv 3 \pmod 4$$

Pas 3: Suma lui Gauss poate fi folosită pentru a lega simbolul lui Legendre de reciprocitatea pătratică:

$$G(a,p)\,G(a,q)=\sum_{m=0}^{p-1}\sum_{n=0}^{q-1} e^{2\pi i\left(\frac{am^2}{p}+\frac{an^2}{q}\right)}$$

Pas 4: Calculăm produsul $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)$

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

Această relație se deduce din proprietățiile sumei lui Gauss și din comportamentul exponențialelor modulare.

Acesta este rezultatul cunoscut ca Legea Reciprocității Pătratice