

Tema 3 - Criptografie

1] dacă $n = \prod_{i=1}^k p_i^{\alpha_i}$ și $a^{\alpha_i} \equiv a \pmod{p_i^{\alpha_i}}$, at. $a^n \equiv a \pmod{n}$

$a^{p_i^{\alpha_i}} \equiv a \pmod{p_i^{\alpha_i}}$, ar. că această proprietate se extinde la n

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k} \Rightarrow p_i^{\alpha_i} | n \Rightarrow n = m \cdot p_i^{\alpha_i}, \forall i \in \overline{1, k}$$

$$\Rightarrow n = \frac{n}{p_i^{\alpha_i}}, \forall i \in \overline{1, k}$$

$$\Rightarrow a^n = \underbrace{a^m}_{\text{m, } p_i^{\alpha_i}} \cdot p_i^{\alpha_i} \Rightarrow (a^{p_i^{\alpha_i}})^m \equiv a^m \cdot a \equiv a \pmod{p_i^{\alpha_i}}$$

2] ar că 1729, 10585, 45861 → nr. Carmichael
numerele Carmichael = nr. care truc testul $b^u \equiv b \pmod{u}$
 $(\Leftrightarrow b^{u-1} \equiv 1 \pmod{u})$

$$\bullet n = 1729 \Rightarrow n-1 = 1728$$

$$\text{aleg } b = 2 \Rightarrow 2^{1728} \equiv (2^2)^{864} = (4^2)^{432} = (16^2)^{216} = (256^2)^{108}$$

$$= (1563^2)^{54} = (621^2)^{27} = 1290 \cdot (1290^2)^{13}$$

$$= 1290 \cdot 802 \cdot (802^2)^6$$

$$= 638 \cdot (16^2)^3 = 638 \cdot 256 \cdot 256^2$$

$$= (802) \cdot 1563 \equiv 1 \pmod{1729}$$

trece testul

↓

$n = 1729$ este număr Carmichael

$$\bullet n = 10585 \Rightarrow n-1 = 10584$$

$$\text{aleg } b = 2 \Rightarrow 2^{10584} \equiv (2^2)^{5292} = (4^2)^{2646} = (16^2)^{1323} = 256 \cdot (256^2)^{661}$$

$$= 256 \cdot 2026 \cdot (2026^2)^{330} = 10576 \cdot (8281^2)^{165}$$

$$= 10576 \cdot 5331 \cdot (5331^2)^{82} = 4946 \cdot (9421^2)^{41}$$

$$= 4946 \cdot 16 \cdot (16^2)^{20} = 5041 \cdot (256^2)^{10} = 5041 \cdot (2026^2)^5$$

$$= 5041 \cdot 8281 \cdot (8281^2)^2 = 4866 \cdot 5331^2$$

$$= 4866 \cdot 9421 \equiv 1 \pmod{10585} \Rightarrow \text{truc testul}$$

↓
 $n = 10585$ este nr. Carmichael.

$$\bullet n = 75361 \Rightarrow n-1 = 75360$$

$$\begin{aligned}
 b=2 \Rightarrow 2^{75360} &= (2^2)^{37680} = (4^2)^{18840} = (16^2)^{9420} = (256^2)^{4710} \\
 &= (65536^2)^{2855} = 68545 \cdot (68545^2)^{1177} \\
 &= 68545 \cdot 35480 \cdot (35480^2)^{588} \\
 &= 1769 \cdot (256^2)^{294} \\
 &= 1769 \cdot (65536^2)^{147} = 1769 \cdot 68545 \cdot (68545^2)^{73} \\
 &= 256 \cdot 35480 \cdot (35480^2)^{36} \\
 &= 39560 \cdot (256^2)^{18} \\
 &= 39560 \cdot (65536^2)^9 = 39560 \cdot 68545 \cdot (68545^2)^4 \\
 &= 698 \cdot (35480^2)^2 = 698 \cdot 256^2 = 698 \cdot 65536 \\
 &\equiv 1 \pmod{75361} \Rightarrow \text{truc testul}
 \end{aligned}$$

$n = 75361$ este nr. primă

3. At. că dacă $2^n - 1$ este prim, atunci n este prim

PpRA n este compus $\Rightarrow \exists a, b$ astfel încât $n = a \cdot b$, $a, b > 1$

$$\Rightarrow 2^n - 1 = 2^{a \cdot b} - 1$$

stim că $\forall k, \exists d \mid k$ astfel încât $2^d - 1 \mid 2^k - 1$

$$2^{a-1} \mid 2^{ab} - 1$$

$$2^{ab} - 1 = m(2^{a-1}) + m$$

pt că $a > 1 \Rightarrow 2^a - 1 > 1 \Rightarrow 2^a - 1$ divisor prim al lui $2^n - 1$
dar $2^n - 1$ este prim \Rightarrow contradicție $\Rightarrow n$ este prim

4. Legea reciprocării patratice: Fie p, q două numere prime impare, distincte. Atunci: $\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$

Demonstrație:

din Lemă lui Gauss avem $\left(\frac{p}{q}\right) = (-1)^k$, unde k este numărul punctelor planului (x, y) cu coordonate întregi care verifică relația $0 < x < \frac{q}{2}$ și $-\frac{q}{2} < px - qy < 0$

$$\Rightarrow y < \frac{px}{2} + \frac{1}{2} < \frac{p+1}{2}$$

dici, k este numărul punctelor cu coord. întregi din dreptunghiul $0 < x < \frac{p}{2}$ și $0 < y < \frac{p}{2}$, care verifică relația $-\frac{p}{2} < px - 2y < 0$.

Analog, $\left(\frac{2}{p}\right) = (-1)^l$, unde l este nr. punctelor din planul (x, y) cu coord. întregi, din dreptunghiul $0 < x < \frac{p}{2}$ și $0 < y < \frac{p}{2}$. Care verifică relația $-\frac{p}{2} < 2x - py < 0$.

Aș. că $\frac{(p-1)(q-1)}{4} - (k+l)$ este par.

obs. că $\frac{(p-1)(q-1)}{4}$ este tocmai numărul de puncte cu coord. întregi, care verifică inegalitatea $px - 2y < \frac{p}{2}$ sau $2x - py < -\frac{p}{2}$

Inegalitățile acestea au multe mulțimi de soluții disjuncte, și cauzează același nr. de puncte cu coord. întregi. De altfel, aspectul se deduce din faptul că relația $x = \frac{p+1}{2} - x'$ și $y = \frac{p+1}{2} - y'$ constituie o transf. bijectivă între aceste două mulțimi disjuncte.

8] simbolul lui Kronecker:

Este scris $\left(\frac{a}{n}\right)$ sau $(a|n)$ și reprez. generalizarea simbolului lui Jacobi pentru totuști întregii $n \neq 0$ cu factorizare primă.

$n = u \cdot p_1^{e_1} \cdots p_k^{e_k}$, unde u este o unitate ($u = \pm 1$), și p_i sunt prime. Practic simbolul Kronecker este definit pentru un întreg a , astfel: $\left(\frac{a}{n}\right) := \left(\frac{a}{u}\right) \prod_{i=1}^k \left(\frac{a}{p_i}\right)^{e_i}$. Când $p_i = 2$,

$$\text{avem: } \left(\frac{a}{2}\right) := \begin{cases} 0, & a \text{ par}, \\ 1, & a \equiv \pm 1 \pmod{8}, \\ -1, & a \equiv \pm 3 \pmod{8}. \end{cases}$$

Când $p_i = \text{impar} \Rightarrow \left(\frac{a}{p_i}\right)$ este chiar simbolul lui Legendre.

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & a \text{ rest patratic } (\pmod{p}) \\ -1, & a \text{ nu este rest patratic } (\pmod{p}) \\ 0, & a \equiv 0 \pmod{p} \end{cases}$$

Pentru că reprezentă numărul lui Jacobi generalizat, atunci $\left(\frac{a}{n}\right) = 1$ când $n=1$, iar când $n=-1$, avem: $\left(\frac{a}{-1}\right) := \begin{cases} -1, & a < 0 \\ 1, & a \geq 0 \end{cases}$.

Dacă $n=0$, atunci avem: $\left(\frac{a}{0}\right) := \begin{cases} 1, & a = \pm 1 \\ 0, & \text{altele} \end{cases}$

Proprietăți:

$$\rightarrow \left(\frac{a}{n}\right) = \pm 1, \text{ dacă } (a, n)=1, \text{ altfel } \left(\frac{a}{n}\right) = 0$$

$$\rightarrow \left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right) \left(\frac{b}{n}\right); \text{ dacă } n=-1, \text{ atunci } a=0 \text{ și } b \text{ negativ sau } b=0 \text{ și } a \text{ negativ}$$

$$\rightarrow \left(\frac{a}{m \cdot n}\right) = \left(\frac{a}{m}\right) \left(\frac{a}{n}\right); \text{ dacă } a=-1, \text{ atunci } m=0 \text{ și } n \text{ are parte impară congruentă cu } 3 \pmod{4} \text{ sau } m \neq 0 \text{ și } n \text{ are parte impară congruentă cu } 3 \pmod{4}.$$

partea impară a numărului n este $2^e n'$ unde n' este impară (dacă $n=0$, atunci $n'=1$)

$$\rightarrow \text{pentru } n>0, \text{ avem } \left(\frac{a}{n}\right) = \left(\frac{b}{n}\right) \text{ când:}$$

$$a \equiv b \pmod{\begin{cases} 4n, & n \equiv 2 \pmod{4} \\ n, & \text{altele} \end{cases}} \quad \text{dacă } a, b \text{ au}$$

ciclași sunte, atunci afirmația este valabilă și pentru $n<0$.

$$\rightarrow \text{pentru } a \not\equiv 3 \pmod{n}, a \neq 0 \text{ avem } \left(\frac{a}{n}\right) = \left(\frac{a}{m}\right), \text{ când:}$$

$$m \equiv n \pmod{\begin{cases} n | a \Rightarrow a \equiv 2 \pmod{n} \\ \text{ial, altfel.} \end{cases}}$$

g) Alg. de primalitate:

+ Verifică cu ajutorul lui Fermat dacă 461 este prim sau compus (cu multe 3 mărturi).

$$n = 461$$

$$\rightarrow b_1 = 2 \Rightarrow 2^{460} = (2^2)^{230} = (4^2)^{115} = 16 \cdot (16^2)^{57} = 16 \cdot 256 \cdot (256^2)^{28} = 16 \cdot (4096^2)^{14} = 16 \cdot (4095^2)^7 = 16 \cdot 340 \cdot (378^2)^3$$

$$= 213 \cdot 444 \cdot 444^6 = 67 \cdot 289 \equiv 1 \pmod{461} \Rightarrow n=461 \text{ este pseudoprime}$$

În raport cu $b_1 = 2$

$$\begin{aligned} b_3 &= 3 \Rightarrow 3^{160} = (3^2)^{230} = (9^2)^{113} = 81 \cdot (81^2)^{57} = 81 \cdot 107 \cdot (107^2)^{28} \\ &= 369 \cdot (885^2)^{14} = 369 \cdot (244^2)^7 = 369 \cdot 67 \cdot (67^2)^3 \\ &= 290 \cdot 340 \cdot 340^2 = 407 \cdot 350 \equiv 1 \pmod{461} \Rightarrow n=461 \text{ este pseudoprime} \end{aligned}$$

În raport cu $b_2 = 3$

10 Alg de factorizare. Folosind Q3 sau Fermat, factorizați:

+) 10807

$$\begin{array}{c|cc} \sqrt{10807} & 103 \\ \hline 1 & \\ 0 & 20 \cdot 0 = 0 \\ 0 & 20 \underline{3} \cdot \underline{3} = 609 \\ \hline 8 & \\ 609 & \\ \hline 198 \end{array}$$

$$[\sqrt{10807}] = 103$$

$$t = 104, t^2 - n = 104^2 - 10807$$

$$\begin{aligned} &= (103+1)^2 - 10807 = 103^2 - 10807 + 206 + 1 \\ &= -198 + 207 = 9 = \Delta^2 \end{aligned}$$

$$\Rightarrow 10807 = 104^2 - 3^2 = (104-3)(104+3) = 101 \cdot 107$$

11 Realizați o comparație între algoritmi de primătate studiați la seminar.

Alg lui Fermat	Alg Miller-Rabin	Alg Solovay-Strassen
- simplu și rapid de implementat	- mai puternic decât Fermat	- mai bun decât testul Fermat
- eficient și pt numere mari	- poate fi determinist și numere mici ($< 2^{64}$)	- mai rapid decât Miller-Rabin și anume în implementări
- vulnerabil la numerele Carmichael	- încă este probabilitate (poate da fals-positiv)	- poate da rezultate greșite (dar mai puțin decât Fermat)
- doar probabilistic (nu oferă certitudine)	- mai lent decât Fermat	- mai puțin utilizat în practică decât Miller-Rabin (nu este însoțitor lui Miller-Rabin în majoritatea casinilor)
- distul de mat	- des utilizat în criptografie (standarde)	

62) Studiați alg. de factorizare rho al lui Pollard și aplicați-l pt. 10909.

Alg rho al lui Pollard

→ vom să factorizăm $n = 10909$

$$g(x) = (x^2 - 1) \pmod{n} \text{ sau } (x^2 + 1) \pmod{n}$$

→ vom avea $g(x) = (x^2 + 1) \pmod{n}$

$$\Rightarrow g(x) = (x^2 + 1) \pmod{10909}$$

→ aleg $x_0 = 2$

→ folosim două secvențe:

1. x_n (se mișcă normal)

2. y_n (se mișcă cu două ori mai repede)

→ apoi verificăm la fiecare pas $(|x_n - y_n|, 10909)$.

→ primul set de valori

$$x_0 = 2$$

$$y_0 = 2$$

Aplicăm funcția:

$$x_1 = (2^2 + 1) \pmod{10909} = 5$$

$$y_1 = f(f(2)) = f(5) = (5^2 + 1) \pmod{10909} = 26$$

$$\text{Calc. } (|5 - 26|, 10909) = (21, 10909) = 1 \Rightarrow \text{nu am găsit factor}$$

Al doilea set de valori:

$$x_2 = (5^2 + 1) \pmod{10909} = 26$$

$$y_2 = f(f(y_1)) = f(26) = 677$$

Calculăm:

$$(|677 - 26|, 10909) = (651, 10909) = 1 \Rightarrow \text{nu am găsit factor}$$

Al treilea set de valori:

$$x_3 = (677^2 + 1) \pmod{10909} = 677$$

$$y_3 = f(f(y_2)) = f(677) = (677^2 + 1) \pmod{10909} = \cancel{4589} 4589$$

Calculăm:

$$(|677 - 4589|, 10909) = (3912, 10909) \Rightarrow \text{nu am găsit factor}$$