① 23.04.24.

Elem TN I

89	7

$A \xrightarrow{76} B$.

$A \xleftarrow{87} B$

Alice alege ca exponentul „său" adică 3
Bob a ales pe al lui adică pe 4.

$B: 76^4 \equiv 81 \pmod{89}$

$A: 87^3 \equiv 81 \pmod{89}$

Def 1) Fie $n \in \mathbb{N}^*$, și fie $a \in \mathbb{Z}$ cu $(a,n)=1$. Numim GAUSSIANUL (sau ORDINUL) lui $a \pmod n$ ~~[illegible]~~ ordinul lui $\hat{a}$ în $U(\mathbb{Z}_n)$.

NOTĂM gaussianul lui $a \pmod n$ cu $\gamma_n(a)$.

Prop 2) Fie $n \in \mathbb{N}^*$ și fie $a \in \mathbb{Z}$ cu $(a,n)=1$. Atunci:

(i) $\forall k \in \mathbb{Z}\ (a^k \equiv 1 \pmod n \Leftrightarrow \gamma_n(a) \mid k)$

(ii) $\gamma_n(a) \mid \varphi(n)$

(iii) $\forall k, l \in \mathbb{Z}\ (a^k \equiv a^l \pmod n \Leftrightarrow k \equiv l \pmod{\gamma_n(a)})$

exemplu: Determinați $\gamma_{23}(2)$

Sol:

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
2·	2	4	6	8	10	12	14	16	18	20	22	1	3	5	7	9	11	13	15	17	19	21
$2^\wedge$	2	4	8	16	9	18	13	3	6	12	1											

Conform tabelului, $\gamma_{23}(2) = 11$.

Def 3 Fie $n \in \mathbb{N}^* \setminus \{1\}$ și fie $a \in \mathbb{Z}$ și $k \in \mathbb{N}^*$ cu $(a,n)=1$

(i) Spunem că a e RĂDĂCINĂ DE ORDIN k A LUI 1 (mod n) dacă $a^k \equiv 1 \pmod n$

(ii) ~~Dacă~~, în plus, $k \mid \varphi(n)$, spunem că a e RĂDĂCINĂ PRIMITIVĂ DE ORDIN k (mod n) dacă $\gamma_n(a) = k$.

(iii) Spunem că a e RĂDĂCINĂ PRIMITIVĂ modulo n dacă $\gamma_n(a) = \varphi(n)$.

ex: De mai sus, $\gamma_{23}(2) = 11$, deci 2 nu e rădăcină primitivă (mod 23)

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
3.	3	6	9	12	15	18	21	1	4	7	10	13	16	19	22	2	5	8	11	14	17	20
3¹	3	9	4	12	13	16	2	6	18	8	1											
5.	5	10	15	20	2	7	12	17	22	4	9	14	19	1	6	11	16	21	3	8	13	18
5¹	5	2	10	4	20	8	17	16	11	9	~~22~~	~~18~~	~~7~~	~~12~~	~~17~~	15	6	7	12	14		
											22	18	21	13	19	3	15	6	7	12	14	1

Conform tabelului, $\gamma_{23}(3) = 11$, deci 3 nu e rădăcină primitivă (mod 23),

iar $\gamma_{23}(5) = 22$, deci 5 e rădăcină primitivă (mod 23).

Def 4 Fie $n \in \mathbb{N}^*$. Presupunem că există rădăcini primitive (mod n) și fie b una dintre ele. Fie $a \in \mathbb{Z}$ cu $(a,n)=1$. Numim INDICELE LUI a ÎN BAZA b acel exponent k cu proprietatea

$b^k \equiv a \pmod n$ (3)

Prop 5 Fie $n \in \mathbb{N}$, $b \in \mathbb{Z}$ cu n def. 4. Atunci:

(i) Dacă $a_1, a_2, \dots, a_s \in \mathbb{Z}$ și $(a_i, n) = 1$, atunci

$$\operatorname{ind}_b (a_1 a_2 \dots a_s) \equiv \operatorname{ind}_b a_1 + \operatorname{ind}_b a_2 + \dots + \operatorname{ind}_b a_s \pmod{\varphi(n)}$$

(ii) Dacă $a \in \mathbb{Z}$, $(a, n) = 1$ și $k \in \mathbb{Z}$,

$$\operatorname{ind}_b a^k \equiv k \operatorname{ind}_b a \pmod{\varphi(n)}$$

(iii) Dacă b' e alt număr primitiv (mod n); iar $a \in \mathbb{Z}$, $(a, n) = 1$, atunci

$$\operatorname{ind}_{b'} a \cdot \operatorname{ind}_b b' \equiv \operatorname{ind}_b a \pmod{\varphi(n)}$$

Observăm că modulo 8 nu există rădăcini primitive. De ce, deci, interesează modulo cele numere n există rădăcini primitive?

Fie $n \in \mathbb{N}^*$. Presupunem că există rădăcini primitive (mod n); fie b una din ele. Atunci, descompunând n în factori primi, avem $U(\mathbb{Z}_n) \xrightarrow{\sim} U(\mathbb{Z}_{p_1^{\alpha_1}}) \times U(\mathbb{Z}_{p_2^{\alpha_2}}) \times \dots \times U(\mathbb{Z}_{p_r^{\alpha_r}})$

Atunci $\varphi(n) = \operatorname{ord} \varphi(b) = [\operatorname{ord}_{\mathbb{Z}_{p_1^{\alpha_1}}} \beta_1, \operatorname{ord}_{\mathbb{Z}_{p_2^{\alpha_2}}} \beta_2 \dots \operatorname{ord}_{\mathbb{Z}_{p_r^{\alpha_r}}} \beta_r]$

(β_j fiind componenta j a lui $\varphi(b)$).

Dar $|U(\mathbb{Z}_{p_j^{\alpha_j}})| = p_j^{\alpha_j - 1}(p_j - 1)$; și a arăta egalitatea de mai sus e necesar ca

(4) n → să nu aibă 2 factori primi impari
↘ Dacă are factorul prim 2 și un factor prim impar, 2 trebuie să apară în descompunere LA PUTEREA ÎNTÂI!!

Concluzie: Singurele numere naturale $n \geq 2$ modulo care mai e vreo șansă să existe rădăcini primitive sunt:

- puterile de 2
- puterile de prim impar
- $2p^{\alpha}$, p prim impar, $\alpha \in \mathbb{N}^*$.

Fie $\alpha \in 2\mathbb{Z}+1$,

Atunci $\alpha^2 \equiv 1 \pmod 8$,

deci $\exists \lambda \in \mathbb{Z}$ $\alpha^2 = 1 + 8\lambda$.

Pp. $\exists \lambda_k \in \mathbb{Z}$ $\alpha^{2^k} = 1 + 2^{k+2} \cdot \lambda$.

Atunci $\alpha^{2^{k+1}} = (\alpha^{2^k})^2 = (1 + 2^{k+2} \cdot \lambda)^2 =$

$= 1 + 2^{k+3} \cdot \lambda'$,

pt orice $L \geq 3$ $\begin{cases} \text{deci } \; \gamma_{2^{k+3}}(\alpha) \mid 2^{k+2} \\ \text{Dar } \; \varphi(2^{k+3}) = 2^{k+2} \end{cases}$

Morala: pt nicio valoare $L \geq 3$ nu există rădăcini primitive $(\bmod 2^L)$