23.04.24

Tema TNG_312

• Determinați $ind_5(19) \pmod{23}$.

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

Conform tabelului, $ind_5(19) = 15$.

• Rezolvați congruențele: a) $x^6 \equiv 7 \pmod{23}$

b) $x^6 \equiv 6 \pmod{23}$

Sol: Notăm $y = ind_5 x \pmod{23}$

a) $x^6 \equiv 7 \pmod{23} \iff$

$(5^y)^6 \equiv 5^{19} \pmod{23} \Rightarrow 5^{6y} \equiv 5^{19} \pmod{23} \iff$

$6y \equiv 19 \pmod{22} \overset{(6,22)=2 \nmid 19}{\Longleftrightarrow} y \in \emptyset$.

Ca urmare, congruența $x^6 \equiv 7 \pmod{23}$ nu are soluții.

b) $x^6 \equiv 6 \pmod{23} \iff$

$(5^y)^6 \equiv 5^{18} \pmod{23} \iff 6y \equiv 18 \pmod{22} \iff$

$3y \equiv 9 \pmod{11} \iff y \equiv 3 \pmod{11} \iff$

$y \equiv 3$ sau $14 \pmod{22} \iff 5^y \equiv 10$ sau $13 \pmod{23}$

$\iff x \equiv 10^1$ sau $13 \pmod{23}$

Dacă $p \in 2\mathbb{N}+1$ e prim,

Considerăm $U(\mathbb{Z}_p) = \mathbb{Z}_p \setminus \{\hat{0}\}$.

Elementele $\hat{a} \in U(\mathbb{Z}_p)$ sunt rădăcinile polinomului $X^{p-1} - \hat{1}$ (cf T. Fermat)

Punând $p-1 = q_1^{\alpha_1} q_2^{\alpha_2} \dots q_r^{\beta_r}$ (desc. standard), elementele $\hat{a} \in U(\mathbb{Z}_p)$ ce n-au ordin $p-1$ trebuie să aibă ordinul un divizor al lui $\frac{p-1}{q_1}$ sau al lui $\frac{p-1}{q_2}, \dots,$ sau al lui $\frac{p-1}{q_r}$,

deci trebuie să fie rădăcini pt $X^{\frac{p-1}{q_1}} - 1$ sau pt $X^{\frac{p-1}{q_2}} - 1, \dots,$ sau pt $X^{\frac{p-1}{q_r}} - 1$, deci aceste elemente $\hat{a}$ de ordin $< p-1$ constituie mulțimea

$R \overset{not}{=} \bigcup_{j=1}^{r} R_j$, $\left(R_{\frac{p-1}{q_j}}\right)$, unde R_h e mulțimea rădăcinilor lui $X^h - 1 \in \mathbb{Z}_p[X]$

dar $|R| = \sum_{j=1}^{r} |R_j| - \sum_{1 \le i < j \le r} |R_i \cap R_j| + \dots$

Dar elementele lui $T_i \cap T_j$ sunt rădăcinile comune ale pol. $X^{\frac{p-1}{q_i}} - 1$ și $X^{\frac{p-1}{q_j}} - 1$, adică răd lui $\left(X^{\frac{p-1}{q_i}} - 1, X^{\frac{p-1}{q_j}} - 1\right) = X^{\left(\frac{p-1}{q_i}, \frac{p-1}{q_j}\right)} - 1 = X^{\frac{p-1}{q_i q_j}} - 1$

continuând analog, obținem

$$|R| = (p-1)\left(\sum_{j=1}^{r} \frac{1}{q_j} - \sum_{1 \le i < j \le r} \frac{1}{q_i q_j} + \sum_{1 \le i < j < k \le r} \frac{1}{q_i q_j q_k} - \dots\right) \Rightarrow$$

$$|\mathbb{Z}_p^\times R| = (p-1)\left(1 - \sum_{j=1}^{r} \frac{1}{q_j} + \sum_{1\le i<j\le r} \frac{1}{q_i q_j} - \cdots\right) =$$

$$= (p-1)\left(1-\frac{1}{q_1}\right)\left(1-\frac{1}{q_2}\right)\cdots\left(1-\frac{1}{q_r}\right) = \varphi(p-1).$$

Morala Modulo orice număr prim p există $\varphi(p-1)$ rădăcini primitive!

Fie p prim impar.
Atunci există rădăcini primitive $\bmod p$.
Fie a una dintre ele.
Presupunem că $a^{p-1} \equiv 1 \pmod{p^2}$
Atunci $a^{p-1} \equiv (a+p)^{p-1} \pmod{p^2}$

$$a^{p-1} \equiv a^{p-1} + p(p-1)a^{p-2} + \text{un multiplu de } p^2 \pmod{p^2}$$

$$\equiv a^{p-1} + p(p-1)a^{p-2} \pmod{p^2} \Rightarrow$$

$$p^2 \mid p(p-1)a^{p-2}, \text{ A}$$

Notăm cu b acel element din $\{a, a+p\}$ care are proprietatea $b^{p-1} \not\equiv 1 \pmod{p^2}$ (3)

$$\gamma_{p^2}(b) \mid \varphi(p^2) = p(p-1) \quad (1)$$

Dar $\gamma_p(b) = \gamma_p(a) = p-1$

$$b^{\gamma_{p^2}(1)} \equiv 1 \pmod{p^2} \Rightarrow b^{\gamma_{p^2}(1)} \equiv 1 \pmod{p} \Rightarrow$$

$$\gamma_p(1) \mid \gamma_{p^2}(1) \Rightarrow p-1 \mid \gamma_{p^2}(1) \Rightarrow \gamma_{p^2}(1) = p(p-1),$$

(A), (3)

Deci b e rădăcină primitivă $(\mathrm{mod}\ p^2)$

Dar $\left.\begin{array}{l} b^{p-1} \equiv 1 \ (\mathrm{mod}\ p) \\ b^{p} \not\equiv 1 \ (\mathrm{mod}\ p^2) \end{array}\right\} \Rightarrow \exists \lambda \in \mathbb{Z} \setminus p\mathbb{Z}$ $b^{p-1} = 1 + \lambda p$.

Se știe că $b^{p^k(p-1)} = 1 + \lambda_k p^{k+1}$, cu $(\lambda_k, p) = 1$.

Demonstrăm

Atunci $b^{p^{k+1}(p-1)} = \left(1 + \lambda_k p^{k+1}\right)^p =$

$= 1 + \lambda_k p^{k+2} +$ un multiplu de p^{k+3}

$= 1 + \lambda_{k+1} \cdot p^{k+2}$, cu $(\lambda_{k+1}, p) = 1$.

Ca urmare, ~~$\forall n \in \mathbb{N}$ $\exists \lambda_n \in \mathbb{Z} \setminus p\mathbb{Z}$~~ $b^{p^n(p-1)} = 1 + \lambda_n p^{n+1}$.

Ca urmare, $b^{p^n(p-1)} \equiv 1 \ (\mathrm{mod}\ p^{n+1})$,

dar $b^{p^{n-1}(p-1)} = 1 + \lambda_{n-1} p^n \not\equiv 1 \ (\mathrm{mod}\ p^{n+1})$.

Deci:

$$\gamma_{p^{n+1}}(b) \mid p^n(p-1) \qquad (10)$$

$$\gamma_{p^{n+1}}(b) \nmid p^{n-1}(p-1) \qquad (11)$$

$b^{\gamma_{p^{n+1}}(b)} \equiv 1 \ (\mathrm{mod}\ p^{n+1})$ (9)

$b^{\gamma_{p^{n+1}}(1)} \equiv 1 \ (\mathrm{mod}\ p)$ (1)

$p - 1 = \gamma_p(1) \mid \gamma_{p^{n+1}}(b)$ (12)

(10), (11), (12) $\Rightarrow \gamma_{p^{n+1}}(b) = p^n(p-1) = \varphi(p^{n+1})$.

Ca urmare, b e rădăcină primitivă $(\mathrm{mod}\ p^{n+1})$

Obs: $\varphi(2p^\alpha) = \varphi(2)\cdot\varphi(p^\alpha) = \varphi(p^\alpha)$ pt orice p prim impar și orice $\alpha \in \mathbb{N}^*$.

Știm că există o rădăcină primitivă b (mod p^α).

Atunci: –

$b^u \equiv 1 \pmod{2p^\alpha} \Rightarrow b^u \equiv 1 \pmod{p^\alpha} \Rightarrow$

$u \,\vdots\, \varphi(p^\alpha) = p^{\alpha-1}(p-1)$.

Deci, presupunând că b e impar (ca să fie prim cu $2p^\alpha$ și să putem vorbi de ordinul său (mod $2p^\alpha$)),

$$\left.\begin{array}{l} \gamma_{2p^\alpha}(b) \,\vdots\, p^{\alpha-1}(p-1) \\ \text{Dar } \gamma_{2p^\alpha}(b) \mid \varphi(2p^\alpha) = p^\alpha(p-1) \end{array}\right\} \Rightarrow \gamma_{2p^\alpha}(b) = p^{\alpha-1}(p-1),$$

deci b e rădăcină primitivă (mod $2p^\alpha$).

Dacă, însă, b e par, atunci refacem considerațiile anterioare pt $c \stackrel{not}{=} b + p^\alpha$ și constatăm că c e rădăcină primitivă (mod $2p^\alpha$).

În concluzie, singurele numere naturale n în raport cu care există rădăcini primitive sunt: 2, 4,

- cele de forma p^α cu p prim impar și $\alpha \in \mathbb{N}^*$

și

- cele de forma $2p^\alpha$ — " — "

Cutăm ex. de descifrare RSA de la seminarul de mai devreme:

nr. citrat e 6347.

pb a-l descifra, știm că 943 (mod 6767) după care interpretăm rezultatul via ASCII

$943 = 512+256+128+32+8+4+2+1$.

$6347^2 \equiv 458$ (toate congruențele sunt (mod 6767))

$6347^4 = 458^2 \equiv 6754$

$6347^8 \equiv 6754^2 \equiv 169$

$6347^{16} \equiv 169^2 \equiv 1493$

$6347^{32} \equiv 1493^2 \equiv 2706$

$6347^{64} \equiv 2706^2 \equiv 542$

$6347^{128} \equiv 542^2 \equiv 2783$

$6347^{256} \equiv 2783^2 \equiv 3641$

$6347^{512} \equiv 3641^2 \equiv 328$

Deci

$6347^{943} \equiv 328 \cdot 3641 \cdot 2783 \cdot 2706 \cdot 169 \cdot 6754 \cdot 458 \cdot 6347$

$\equiv 435 \cdot 3111 \cdot 458 \cdot 3883 \equiv 77 \xleftrightarrow{\text{ASCII}} M$.