

Seminar 2

Se leau euro, pt. $p \in \mathbb{N}$ prim și $m \in \mathbb{N}^*$.

$$v_p(m) = \max \{ k \in \mathbb{N}^* : p^k \mid m \}$$

Prop: Fie $p \in \mathbb{N}$ prim. Atunci:

$$\text{i). } \forall m, n \in \mathbb{N}^* \quad v_p(mn) \geq \min \{ v_p(m), v_p(n) \}.$$

Dacă $v_p(mn) \leq v_p(m)$, atunci $m+n = p^{v_p(m)} \cdot \mu + p^{v_p(m)} \cdot \nu$, $m = p^{v_p(m)} \cdot \mu$, $n = p^{v_p(m)} \cdot \nu$. Cu $p \nmid \mu \wedge p \nmid \nu$.

$$(1) = p^{v_p(m)} (\mu + p^{v_p(m)} - v_p(m)) \quad (2)$$

Deci, $v_p(mn) \geq v_p(m) - \min \{ v_p(m), v_p(n) \}$.

Dacă $v_p(m) < v_p(n)$,

în (2) : $p \nmid \mu$ și $\mu \neq 0$

Deci $v_p(mn) = \min \{ v_p(m), v_p(n) \}$.

Cazul $v_p(m) \leq v_p(n)$ se tratează analog.

$$\text{ii). } \forall m, n \in \mathbb{N}^* \quad v_p(m) \neq v_p(n) \Rightarrow v_p(mn) = \min \{ v_p(m), v_p(n) \}.$$

Analog se procedează și;

$$\text{i'). } \forall m, n \in \mathbb{N}^* \quad (m > n \Rightarrow v_p(m-n) \geq \min \{ v_p(m), v_p(n) \})$$

$$\text{ii'). } \forall m, n \in \mathbb{N}^* \quad ((m > n \wedge v_p(m) \neq v_p(n)) \Rightarrow v_p(m-n) = \min \{ v_p(m), v_p(n) \})$$

Pf. $m \in \mathbb{N}^*$

$$\prod_{p \text{ prim}} p^{v_p(m)} \quad \{ p \in \mathbb{N}^* : p \text{ prim}\}$$

$$P_D = \prod_{\substack{p \text{ prim} \\ p \leq D}} p^{v_p(m)}$$

$$\text{Atunci: } P_m = P_{m+1} = P_{m+2} = \dots$$

(pt. că $p \in \mathbb{N}$ prim și $p > m \Rightarrow v_p(m) = 0$).

$$\text{Deci } \prod_{p \text{ prim}} p^{v_p(m)} = \lim_{D \rightarrow \infty} P_D = \lim_{D \rightarrow \infty} P_m = \prod_{\substack{p \text{ prim} \\ p \leq m}} p^{v_p(m)}$$

Dacă mai mult considerăm dec. standard $m = \prod_{p \text{ prim}} p^{\alpha_p}$, în acest produs

fiecare $p \leq m$ și avem pt. fiecare $p \leq m$, p prim

$$\left[\begin{array}{l} v_p(m) = v_p \left(\prod_{p \text{ prim}} p^{\alpha_p} \right) = \alpha_p \\ p \leq m \end{array} \right]$$

Deci în $\prod_{p \text{ prim}} p^{\alpha_p}$ fiecare α_p e de fapt, $v_p(m)$. Ca urmare, $m = \prod_{p \text{ prim}} p^{v_p(m)}$

Ca urmare, teorema fundam. a aritm. admite și formularea,

$$\forall m \in \mathbb{N}^* \quad m = \prod_{p \text{ prim}} p^{v_p(m)}.$$

$$\text{Fie } m = \prod_p p^{\nu_p(m)} \quad \text{și } m' = \prod_p p^{\nu'_p(m')}$$

$$\text{Considerăm } d = \prod_p p^{\min\{\nu_p(m), \nu'_p(m)\}}.$$

$$\text{Cum } \min\{\nu_p(m), \nu'_p(m)\} \leq \nu_p(m), \nu'_p(m).$$

Așa că $d \mid m \wedge d \mid m'$.

Dacă $d' = \prod_p p^{\nu_p(d')}$ are calitățile $d' \mid m \wedge d' \mid m'$, atunci

$$\nu_p(d') \leq \nu_p(m) \quad \text{și} \quad \nu_p(d') \leq \nu'_p(m) \quad \text{pt. } \forall p.$$

$$\text{Deci } \nu_p(d') \leq \min\{\nu_p(m), \nu'_p(m)\} \quad \text{pt. } \forall p$$

$$\text{Deci } \nu_p(d') \leq \nu_p(d) \quad \text{pt. } \forall p, \text{ deci } d' \mid d.$$

Morală:

$$\left(\prod_p p^{\nu_p(m)}, \prod_p p^{\nu'_p(m)} \right) = \prod_p p^{\min\{\nu_p(m), \nu'_p(m)\}}$$

$$\text{Analog, } [m, m'] = \prod_p p^{\max\{\nu_p(m), \nu'_p(m)\}}$$

$$\underline{\text{Dobz.}}: \dim \min\{u, v\} + \max\{u, v\} = u+v, \quad (m, m)[m, m] = mm.$$

1. Determinați nr. prime a, b pt. care $ab+1 \wedge ab-1$ sunt prime.
2. Dacă nr. m pt. care $m+1, m+3, m+7, m+9, m+13 \wedge m+15$ sunt prime.
3. Dim 10 nr. consecutive, cât de multe pot fi prime?
4. Dacă progresie aritmetică neconstanță de nr. nat. are o infinitate de termeni compusi.
5. $\frac{2^{4m+2}+1}{5} \in \mathbb{Z}$ și e compus pt. $\forall m \geq 2$.
6. $\forall m, n \in \mathbb{N} \quad m^{22} = m^4 + 4m^4$ e compus.
7. Dacă $\underbrace{11 \dots 1}_m$ e prim, atunci m e prim.
8. Dacă 2^m+1 e prim, $m=0$ sau $\forall k \in \mathbb{N}, m=2^k$.
9. Dacă 2^m-1 e prim, atunci m e prim.
10. Care sunt nr. nat. care nu sunt sume de două nr. compuse?

$$6) \quad m^4 + 4m^4 = m^4 + 4m^4 + 4m^2m^2 - 4m^2m^2 = \underbrace{(m^2 - 2mm + 2m^2)}_{\substack{'' \\ (m-m)^2 + m^2 \\ VI}} \underbrace{(m^2 + 2mm + 2m^2)}_{\substack{'' \\ (m+m)^2 + m^2 \\ VI}}$$

$$7) \quad \frac{2^{4m+2}+1}{5} = \frac{4^{2m+1}+1}{5} = \frac{(4+1)(4^{2m}-4^{2m-1}+4^{2m-2}-\dots+4^2-4+1)}{5} \in \mathbb{Z}.$$

$$1 + \sum_{j=1}^m (4^{2j} - 4^{2j-1}) = 1 + 3 \sum_{j=1}^m 4^{2j-1}.$$

- 2) Dacă restul împărțirii lui m la 5 este 0, $m+15 \geq 15$, deci $m+15$ nu e primă.
- 1: $m+9 \geq 9$, deci $m+9$ nu e prim, $\cancel{\text{X}}$
 - 2: $m+13 \geq 13$, deci $m+13$ nu e prim, $\cancel{\text{X}}$
 - 3: $m+7 \geq 7$, deci $m+7$ nu e prim, $\cancel{\text{X}}$
 - 4: $m+1 \geq 5$
- Dacă $m > 4$, $m+1$ nu e prim, $\cancel{\text{X}}$.

Rămâine $m=4$, pt. căre:

$$\begin{aligned} m+1 &= 5, \text{ e prim} \\ m+3 &= 7, \text{ ---} \\ m+7 &= 11, \text{ ---} \\ m+9 &= 13, \text{ ---} \\ m+13 &= 17, \text{ ---} \\ m+15 &= 19, \text{ ---} \end{aligned}$$

Deci singura valoare $m \in \mathbb{N}$ ce corespunde cerinței e $m=4$.

5) $\frac{(2^{2m+1} - 2^{m+1} + 1)(2^{2m+1} + 2^{m+1} + 1)}{5} \approx 2^{2m+1} - 2^{m+1} + 1 \geq 25$

6) Dacă $m = ab$ cu $a, b > 1$

$$2^m - 1 = 2^{ab} - 1 = (2^a)^b - 1 = \underbrace{(2^a - 1)}_{\geq 3} \underbrace{(2^{a(b-1)} + 2^{a(b-2)} + \dots + 2^a + 1)}_{\text{mai mult}}$$

7) Dacă $m = 2^k \cdot 2$, 2 impar

Așadar $2^m + 1 = 2^{2^k \cdot 2} + 1 = (\underbrace{2^{2^k} + 1}_{\geq 3})(2^{2^k(2-1)} - 2^{2^k(2-2)} + \dots - 2^{2^k} + 1)$

Evident, $2^{2^k(j+1)} > 2^{2^k j}$, deci $\sum (2^{2^k(j+1)} - 2^{2^k j}) \geq \sum \text{căstiguri} > 0$

8) $\underbrace{\frac{11 \dots 1}{m}} = \frac{10^m - 1}{9} = (1)$

9. $m = ab$ cu $a, b > 1$, atunci

$$(1) = \underbrace{(10^a - 1)(10^{a(b-1)} + 10^{a(b-2)} + \dots + 10 + 1)}_9 \in \mathbb{N}^* \setminus \{1\}$$

Seminar 3

Dacă cîntul și restul împărțirii lui -79 la 17

$$-79 : 17 = -5 \text{ r. } 6.$$

$$79 = 17 \cdot 4 + 11 \Rightarrow -79 = 17 \cdot (-4) - 11 \Rightarrow -79 = 17 \cdot (-5) + 6$$

evident $0 \leq 6 < 17 = |17|$.

Conform precizării de unicitate din TTR, cîntul împărțirii lui -79 la 17 e 5, iar restul acesteia e 6.

Dacă ale lui 79 la -17) $g = n =$

Dacă ale lui -79 la -17) $g = 5, n = 6$

• Căți pași are algoritmul lui Euclid?

$$\left. \begin{array}{l} a = bg_0 + n_0 \\ b = n_0 g_1 + n_1 \\ n_0 = n_1 g_2 + n_2 \\ n_1 = n_2 g_3 + n_3 \\ \vdots \\ n_{m-1} = n_m g_{m+1} + n_{m+1} \\ n_m = n_{m+1} g_{m+2} \end{array} \right\} m+2 \leq b.$$

Dacă $n_0 > \frac{b}{2}$ atunci $g_1 = 1$, deci $n_1 = b - n_0 < \frac{b}{2}$

Dacă $n_0 \leq \frac{b}{2}$ și $n_1 < n_0 < \frac{b}{2}$.

Mai general, $n_{j+2} \leq \frac{n_j}{2}$

Inductiv, $n_{2k+1} \leq \frac{b}{2^{k+1}}$ $\forall k \in \mathbb{N}, k \leq \left[\log_2 \left(\frac{b}{2} - 1 \right) \right] - 1$

Noi am vrăea ca restul să devină 0.

Dacă $\frac{b}{2^{k+1}} \leq 1$, atunci vom avea $n_{2k+1} = 0$

$$b \leq 2^{k+1} \Leftrightarrow k \geq \log_2 b - 1$$

Cu urmare, $\left[\log_2 b \right] + 1 = 0$

În consecință, algoritmul se termină cu certitudine după $2 \left[\log_2 b \right] + 2$ pași.

Considerăm sirul $F_0 = 1, F_1 = 1, F_m = F_{m-1} + F_{m-2}, \forall m \geq 2$.

(Def) : Sirul $(F_m)_m$ prezintă mai multe p.m. siruri lui Fibonacci.

Inductiv $(F_m)_{m \geq 1}$ este strict crescător.

Aplicăm alg. lui Euclid pt. $F_m \text{ și } F_{m-1}$:

$$F_m = F_{m-1} + F_{m-2}$$

$$F_{m-1} = F_{m-2} + F_{m-3}$$

$$F_3 = F_2 + F_1$$

$$F_2 = 2F_1$$

Ano m-1 pași

$$\text{Ec. caracter. } t^2 - t - 1 = 0 \Leftrightarrow t \in \left\{ \frac{1 \pm \sqrt{5}}{2} \right\}$$

$$\text{Vom avea } F_m = At_1^m + Bt_2^m$$

$$\begin{cases} A+B = F_0 = 1 \\ At_1 + Bt_2 = F_1 = 1 \end{cases} \Leftrightarrow$$

$$A = \frac{t_2 - 1}{t_2 - t_1} \wedge B = \frac{1 - t_1}{t_2 - t_1}$$

$$\Rightarrow A = \frac{\sqrt{5} - 1}{2\sqrt{5}} \wedge B = \frac{\sqrt{5} + 1}{2\sqrt{5}}$$

$$\text{Deci } F_m = \frac{1}{\sqrt{5}} \left[\left(\frac{\sqrt{5} + 1}{2} \right)^{m+1} - \left(\frac{1 - \sqrt{5}}{2} \right)^{m+1} \right].$$

$$\log_2 F_{m+1} \leq \log_2 \frac{1}{\sqrt{5}} \left(\frac{\sqrt{5} + 1}{2} \right)^m = \log_2 \sqrt{5} + m \log_2 \frac{1 + \sqrt{5}}{2} < m(\log_2(1 + \sqrt{5}) - 1) < m \log_2(1 + \sqrt{5})$$

637 ; 108

$$637 = 5 \cdot 108 + 97$$

$$108 = 1 \cdot 97 + 11$$

$$97 = 8 \cdot 11 + 9$$

$$11 = 1 \cdot 9 + 2$$

$$9 = 4 \cdot 2 + 1$$

$$2 = 1 \cdot 2$$

Varianta :

$$637 = 6 \cdot 108 - 11$$

$$108 = -10 \cdot (-11) - 2$$

$$-11 = 6 \cdot (-2) + 1.$$

$$-2 = (-2) \cdot 1.$$

$$a = b c_0 + d_0 \rightarrow |d_0| \leq \frac{|b|}{2}$$

$$b = d_0 c_1 + d_1 \rightarrow |d_1| \leq \frac{|d_0|}{2} \leq \frac{|b|}{4}$$

$$d_0 = d_1 c_2 + d_2 \rightarrow |d_2| \leq \frac{|d_1|}{2} \leq \frac{|b|}{8}$$

$$d_{m-2} := d_{m-1} c_m + d_m \quad \xrightarrow{\substack{= \\ \dots}} \quad d_{m+1} | d_{m-2}$$

$$d_{m-1} = d_m c_{m+1} + d_{m+1} \quad \xrightarrow{\substack{= \\ \dots}} \quad d_{m+1} | d_{m-1}$$

$$d_m = d_{m+1} c_{m+2}$$

$$d_{m+1} | d_m$$

$$|d_{m+1}| \leq \frac{|b|}{2^{m+1}}$$

Că nu firm riguri de $d_{m+1} = 0$

$$2^{m+2} \geq |b| \Leftrightarrow m+2 \geq \log_2 |b| \quad (= \log_2 b \text{ pt. } b \in \mathbb{N}^*)$$

De urmare, după $\log_2 b + 1$ parțială garantie că am ajuns la rezultat.

Teoria numerelor cu apl
în criptografie

Seminarul 4

T1 (Euler) $\forall m \in \mathbb{N}$ ($m \geq 2 \Rightarrow \forall a \in \mathbb{Z} / (a, m) = 1 \Rightarrow a^{\varphi(m)} \equiv 1 \pmod{m}$)

Denumire: $(a, m) = 1 \Rightarrow \hat{a} \in U(\mathbb{Z}_m) \Rightarrow \text{ord}_{U(\mathbb{Z}_m)} \hat{a} / |U(\mathbb{Z}_m)| = \varphi(m)$.

Că urmare, $\hat{a}^{\varphi(m)} = \hat{1}$, deci $a^{\varphi(m)} \equiv 1 \pmod{m}$.

T2 (Fermat): Pentru orice nr. natural prim p și pt. orice $a \in \mathbb{Z}$, $a^p \equiv a \pmod{p}$

T3 (Wilson): Pentru orice nr. natural prim p
 $(p-1)! \equiv -1 \pmod{p}$

1. Pentru ce $p \in \mathbb{N}$ prime avem $\frac{2^{p+1}}{p} \in \mathbb{Z}$?

2. Pentru orice $m \in \mathbb{N}$ restul împărțirii lui $10^m - 1$ la 37 e patrat perfect.

3. Determinați restul împărțirii lui $100!$ la 109 .

Obs: • Orice patrat de nr. par $\equiv 0 \pmod{4}$.
• Orice patrat de nr. impar $\equiv 1 \pmod{8}$.

T4 (Gauss-Legendre)

Um nr. natural se scrie ca suma de trei patrate de nr. întregi dacă el este de forma $4^K(8T+7)$ ($K, T \in \mathbb{N}$)

Fie $x \in \mathbb{Z}$, $x = a^2 + b^2 + c^2$ $a, b, c \in \mathbb{N}$.

Presupunem că $\exists K, T \in \mathbb{N}$ $x = 4^K(8T+7)$

Atunci $4^K(8T+7) = a^2 + b^2 + c^2$.

Dacă $K > 0$, fie a, b, c sunt pari, deci $4^K(8T+7) = 4(a_1^2 + b_1^2 + c_1^2) \Leftrightarrow$

$\Leftrightarrow 4^{K-2}(8T+7) = a_1^2 + b_1^2 + c_1^2$

Dacă continuăm "iesind numai pe acasă" varianta, obținem:

$\exists a_K, b_K, c_K \in \mathbb{Z}$ $8T+7 = a_K^2 + b_K^2 + c_K^2$.

În MD nu putem avea decât:

• 1 nr. impar și 2 pare

Atunci $MD \stackrel{?}{=} \underbrace{1+\alpha+\beta}_{\text{III}}, \text{ unde } \alpha, \beta \in \{0, 4\}$

sau $1 \text{ sau } 5 \pmod{8}$

• toate impare:

Atunci $MD \equiv 3 \pmod{8}$.

Dacă în $4^K(8T+7) = a^2 + b^2 + c^2$ în MD avem 1 nr. par și nr. pare, $MD \equiv 2 \pmod{4}$.

Dacă, am demonstrat „ \Rightarrow ” !!

$$\text{Sof. 3: } 100! \cdot (-8) \cdot (-7) \cdot (-6) \cdot (-5) \cdot (-4) \cdot (-3) \cdot (-2) \cdot (-1) \equiv -1 \pmod{109}$$

Cum calculăm inversul $(\bmod n)$ al unui element?

Ex.: Care e inversul lui $83 \pmod{601}$?

1. "La inspirație".

$$\begin{aligned} 83 \cdot 7 &\equiv -20 \\ (-20) \cdot (-30) &\equiv -1 \end{aligned} \quad \Rightarrow 83 \cdot 7 \cdot 30 \equiv 1$$

\Downarrow

$$83 \cdot 210 \equiv 1.$$

Deci inversul $(\bmod 601)$ al lui 83 e 210 .

2. Folosind algoritmul lui Euclid

De fapt, inversul lui $83 \pmod{601}$ e un nr. $\alpha \in \mathbb{Z}$ cu proprietatea că $83 \cdot \alpha \equiv 1 \pmod{601}$

$$\Leftrightarrow \exists m \in \mathbb{Z} \quad 83\alpha - 1 \equiv 601m \quad \Leftrightarrow \exists m \in \mathbb{Z} \quad 83\alpha - 601m = 1.$$

$$601 = 7 \cdot 83 + 20$$

$$83 = 4 \cdot 20 + 3$$

$$20 = 6 \cdot 3 + 2$$

$$3 = 1 \cdot 2 + 1$$

$$2 = 2 \cdot 1.$$

$$\alpha_j = \alpha_{j-2} - q_j \alpha_{j-1}$$

$$p_j = p_{j-2} - q_j p_{j-1}$$

$$a = b q_0 + r_0 \quad (\Rightarrow r_0 = a - q_0 b)$$

$$b = r_0 q_1 + r_1 \quad \alpha_0 = \pm$$

$$r_0 = q_1 r_1 \quad p_0 = -q_0$$

$$r_1 = q_2 r_2 + r_3$$

$$\dots$$

	-1	0	1	2	3
q	0	7	4	6	1
α	0	1	-4	25	-29
p	1	-7	29	-181	210

$$\begin{aligned} b &= 0 \cdot a + b \\ &\Downarrow \\ &\alpha_2 + \beta_2 b = r_1 \\ &\Downarrow \\ \alpha_{-1} &= \beta_{-1} \end{aligned}$$

Deci, $1 = r_3 = -29 \cdot 601 + 210 \cdot 83$.

Deci $83 \cdot 210 \equiv 1 \pmod{601}$, deci inversul lui $83 \pmod{601}$ e 210 .

3. Cu fracții continue.

$$\frac{601}{83} = 7 + \frac{20}{83} = 7 + \frac{1}{\frac{83}{20}} = 7 + \frac{1}{4 + \frac{3}{20}} = 7 + \frac{1}{4 + \frac{1}{6 + \frac{2}{3}}} = 7 + \frac{1}{4 + \frac{1}{6 + \frac{1}{1 + \frac{1}{2}}}}$$

fracția continuă asociată
lui $\frac{601}{83}$.

mat F
II

$$\text{Fractii continue } \frac{x}{R_0}, \frac{x+1}{R_1}, \frac{x+\frac{1}{4}}{R_2} ; \frac{x+\frac{1}{4+\frac{1}{6}}}{R_3} ; \frac{x+\frac{1}{4+\frac{1}{6+\frac{1}{4}}}}{R_4} \dots$$

REDUSELE lui \overline{F} .

$$R_3 = x + \frac{1}{29} = \frac{210}{29}$$

Obs: $210 \cdot 83 - 29 \cdot 601 = 1$, deci $210 \cdot 83 \equiv 1 \pmod{601}$, deci inversul lui $83 \pmod{601}$ este 210 .

4. Folosind T. Fermat.

#. Cf. T. Fermat, (obs: 601 e prim!!!)

$$83^{600} \equiv 1 \pmod{601}$$

deci inversul lui $83 \pmod{601}$ este 83^{599} .

$$599 = 512 + 64 + 16 + 4 + 2 + 1$$

$$\text{Deci } 83^{599} = 83 \cdot 83^2 \cdot 83^4 \cdot 83^{64} \cdot 83^{512} = (1)$$

$$\text{Dacă: } 83^2 \equiv 278$$

$$83^4 \equiv 278^2 \equiv 356$$

$$83^8 \equiv 356^2 \equiv 526$$

$$83^{16} \equiv 526^2 \equiv 216$$

$$83^{32} \equiv 216^2 \equiv 379$$

$$83^{64} \equiv 379^2 \equiv 2$$

$$83^{128} \equiv 4$$

$$83^{256} \equiv 4^2 \equiv 16$$

$$83^{512} \equiv 256$$

(toate $\rightarrow 0 \pmod{601}$)

$$\text{Deci, } (1) \equiv 83 \cdot 278 \cdot 356 \cdot 216 \cdot 2 \cdot 256 \equiv 210.$$

Că urmăre, inversul lui $83 \pmod{601}$ este 210 .

Semimarul 5

Care sunt numerele care admit reprezentări periodice în baza b ?

$$\begin{aligned}
 & \overline{0, a_1 a_2 \dots a_n (u_1 u_2 \dots u_0)}_{(b)} = \frac{a_1}{b} + \frac{a_2}{b^2} + \dots + \frac{a_n}{b^n} + \frac{u_1}{b^{n+1}} + \frac{u_2}{b^{n+2}} + \dots + \frac{u_0}{b^{n+0}} + \\
 & + \frac{u_1}{b^{n+0+1}} + \frac{u_2}{b^{n+0+2}} + \dots + \frac{u_0}{b^{n+20}} + \\
 & + \frac{u_1}{b^{n+20+1}} + \dots + \frac{u_0}{b^{n+30}} + \\
 & = \frac{a_1 b^{n-1} + a_2 b^{n-2} + \dots + a_{n-1} b + a_n}{b^n} + \frac{1}{b^{n+1}} \left(u_1 + \frac{u_2}{b} + \dots + \frac{u_0}{b^{0-1}} \right) \left(1 + \frac{1}{b^0} + \frac{1}{b^{20}} + \dots \right). = \\
 & = \frac{\overline{a_1 a_2 \dots a_n}_{(b)}}{b^n} + \frac{\overline{u_1 u_2 \dots u_0}_{(b)}}{b^{n+1}} \cdot \lim_{k \rightarrow \infty} \frac{1 - \frac{1}{b^{20}}}{1 - \frac{1}{b^0}} = \\
 & = \frac{\overline{a_1 a_2 \dots a_n}_{(b)}}{b^n} + \frac{\overline{u_1 u_2 \dots u_0}_{(b)}}{b^{n+1}} \cdot \frac{b^0}{b^{0-1}} = \frac{\overline{a_1 a_2 \dots a_n}_{(b)} (b^{0-1}) + \overline{u_1 u_2 \dots u_0}_{(b)}}{b^n (b^{0-1})} \\
 & = \frac{\overline{a_1 a_2 \dots a_n \underbrace{000 \dots 0}_{\text{ }}_{(b)}} + \overline{u_1 u_2 \dots u_0}_{(b)} - \overline{a_1 a_2 \dots a_n}_{(b)}}{b^n (b^{0-1})} = \\
 & = \frac{\overline{a_1 a_2 \dots a_n u_1 u_2 \dots u_0}_{(b)} - \overline{a_1 a_2 \dots a_n}_{(b)}}{b^n (b^{0-1})} = \frac{\overline{a_1 a_2 \dots a_n}_{(b)} \underbrace{\beta \beta \beta \dots \beta}_{\Delta} \underbrace{0 \dots 0}_{\Pi}}{b^n (b^{0-1})}
 \end{aligned}$$

Dacă avem nr. $\frac{u}{v}$, $u, v \in \mathbb{N}$ $v \neq 0, 1$?

$$x_1 = \frac{u}{v}$$

$$a_1 = [5x_1] = \left[\frac{5u}{v} \right]; \quad x_2 = \{5x_1\} = \frac{N_2}{v} \in \{0, 1, \dots, v-1\}$$

$$a_2 = [5x_2] = \left[\frac{5N_2}{v} \right]; \quad x_3 = \{5x_2\} = \frac{N_3}{v} \in \{0, 1, \dots, v-1\}$$

Continuând calculele, constatăm că:

$$\forall k \in \mathbb{N}^* \setminus \{1\} \quad \exists n_k \in \{0, 1, \dots, v-1\} \quad x_k = \frac{n_k}{v}$$

De aici, $\exists i, j \in \mathbb{N} \setminus \{1\}$, cu $i < j$ și $x_i = x_j$.

Așadar $x_{j+1} = \{5x_j\} = \{5x_i\} = x_{i+1}$ și inductiv $x_{j+k} = x_{i+k}$ $\forall k \in \mathbb{N}^*$.

Morală: $\forall k \geq i \quad x_k = x_{k+j-i}$

(dăm: inducție!)

Deci, reprezentarea lui $\frac{u}{v}$ în baza b e periodică.

Așa că obținem deci:

T1 Un nr. real x are reprezentare periodică în baza b dacă și numai dacă $x \in \mathbb{Q}$.

Care din nr. reale (de fapt, rationale, cf T1!!) admit reprezentări cu frație finită în baza b ?

$$\overline{0, a_1 a_2 \dots a_n}_{(b)} = \frac{\overline{a_1 a_2 \dots a_n}_{(b)}}{b^2} \Rightarrow u b^2 = v \cdot \overline{a_1 a_2 \dots a_n}_{(b)} \xrightarrow{(u,v)=1}$$

$$(u, v) = 1.$$

$\Rightarrow v \mid b^2$. Ca urmare, v nu are factori primi p care să nu împărtășească pe b . Deci, v este un produs de factori primi de-ai lui b .

Reciproc, dacă $b = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$, iar $v = p_1^{\beta_1} p_2^{\beta_2} \dots p_n^{\beta_n}$, atunci

$$\Leftrightarrow \beta_i \in \mathbb{N}$$

$$\frac{u}{v} = \frac{u}{p_1^{\beta_1} p_2^{\beta_2} \dots p_n^{\beta_n}} \text{ . } \text{Cu }\text{atunci } T = \max \left\{ \left[\frac{\beta_1}{\alpha_1} \right] + 1, \dots, \left[\frac{\beta_n}{\alpha_n} \right] + 1 \right\}, \text{ atunci}$$

$$\frac{u}{v} = \frac{u p_1^{T \alpha_1 - \beta_1} \dots p_n^{T \alpha_n - \beta_n}}{p^T}$$

care se reprezintă ca frație finită în baza b .

Ce urmare:

T2 Un nr. rational x admite reprezentare finită în baza b dacă și numai dacă $x = \frac{u}{v}$ cu $u, v \in \mathbb{Z}$, $v \neq 0$, $(u, v) = 1$, iar v este produs de factori primi de-ai lui b .

Obs3. Singurele nr. reale (memule!) care au mai mult de o reprez. în bazele sunt cele din T2.

Care numere reale (de fapt, rationale!) se scriu ca frație periodică simplă în baza b ?

$$\frac{u}{v} = \overline{0, (a_1 a_2 \dots a_n)}_{(b)} = \frac{\overline{a_1 a_2 \dots a_n}_{(b)}}{b^{n+1}-1} \Rightarrow u(b^{n+1}-1) = v \cdot \overline{a_1 a_2 \dots a_n}_{(b)} \xrightarrow{(u, v)=1}$$

$$\Rightarrow v \mid b^{n+1}-1 \Rightarrow (v, b) = 1.$$

Reciproc, dacă $(v, b) = 1$. cf TMR

$$b = g, v \mid M_1$$

$$b^2 = g_2, v \mid M_2$$

$$b^{n+1} = g_{n+1}, v \mid M_{n+1}$$

dor $M_1, M_2, \dots, M_{n+1} \in \{0, 1, \dots, n-1\}$, deci $\exists i, j \in \{0, 1, \dots, n+1\} \quad i < j \wedge M_i = M_j$

?t. acceptă i, j $(g_j - g_i)v = b^j - b^i \Rightarrow v \mid b^i(b^{j-i}-1) \xrightarrow{(v, b)=1} v \mid b^{j-i}-1$

Deci $\exists w \in \mathbb{Z} \quad vw = b^{j-i}-1$, adică $\exists w \in \mathbb{Z} \quad \frac{1}{v} = \frac{w}{b^{j-i}-1}$,

deci $\exists w \in \mathbb{Z} \quad \frac{u}{v} = \frac{uw}{b^{j-i}-1}$

$\frac{uw}{b^{j-i}-1}$ frație periodică simplă în baza b .

T Am obtinut deci:

T3 Un nr. real x se reprezinta ca fractie periodica simpla in baza b daca si $u, v \in \mathbb{Z}$ ($v \neq 0 \wedge (u, v) = 1 \wedge (v, b) = 1 \wedge x = \frac{u}{v}$)

Scrieti in baza 7 numarul $A_{31,5(4972)}_{(12)}$ (doi zeci)

$$A_{31}_{(12)} = 10 \cdot 12^2 + 3 \cdot 12 + 1 = 1477$$

$$\begin{array}{r} 1477 \\ \hline 14 \\ \hline 7 \\ \hline 211 \\ \hline 21 \\ \hline 1 \\ \hline 18 \\ \hline 4 \\ \hline 0 \\ \hline 2 \\ \hline 0 \\ \hline 1 \\ \hline a_1 \\ \hline a_2 \\ \hline a_3 \end{array}$$

$$\begin{aligned} 1477 &= a_0 + 7a_1 + 7^2a_2 + \dots \\ &\quad \vdots \\ &\quad 7 \cdot 211 \\ &= (a_0 + 7a_1 + 7^2a_2 + \dots) \\ &\quad \vdots \\ &\quad 7(a_2 + 7a_3 + \dots) \end{aligned}$$

$$\text{Deci } [x] = A_{31}_{(12)} = 1477 = 4210_7$$

$$\begin{aligned} \{x\} &= 0,5(4972)_{(12)} = \frac{(54972)_{(12)} - 5_{(12)}}{12(12^4 - 1)} = \frac{5 \cdot 12^4 + 4 \cdot 12^3 + 9 \cdot 12^2 + 7 \cdot 12 + 2 - 3}{12 \cdot 11 \cdot 13 \cdot 145} = \\ &= \frac{12^3 \cdot 64 + 1296 + 81}{12 \cdot 11 \cdot 13 \cdot 5 \cdot 29} = \frac{9 \cdot \frac{24}{4} (4096 + 48 + 3)}{12 \cdot 11 \cdot 13 \cdot 5 \cdot 29} = \frac{9 \cdot \frac{24}{4} \cdot 4144}{4 \cdot 11 \cdot 12 \cdot 5 \cdot 29} = \frac{9}{20} = 0,45. \end{aligned}$$

$$0,45 \cdot 7 = 3,15$$

$$0,15 \cdot 7 = 1,05$$

$$0,05 \cdot 7 = 0,35$$

$$0,35 \cdot 7 = 2,45$$

$$0,45 \cdot 7 = 3,15$$

$$\text{Deci } 0,5(4972)_{(12)} = 0,45 = 0, (3102)_7.$$

$$\text{Ca urmare, } x = [x] + \{x\} = 4210_7 + 0, (3102)_7 = 4210, (3102)_7.$$

$$\left. \begin{array}{l} x_1 = 2 \\ [10x_1] = 2; \quad x_2 = \{10x_1\} = 0,291 \\ [10x_2] = 9 \\ x_1 = [5x_2]; \quad x_2 = \{5x_2\} \\ x_2 = [5x_2]; \quad x_3 = \{5x_2\} \end{array} \right\}$$

Seminarul 7

Criptosistem liniian pe dignituri vectoriale pe te alfabetul $A = \text{criptosistem în care textul e împărțit în perechi (ordonate) de litere care sunt interpretate ca elemente din } \mathbb{Z}_m^2$ (unde $m = |\text{alf}|$), și în care funcția de criptare e de tipul:

$$c : \mathbb{Z}_m^2 \rightarrow \mathbb{Z}_m^2, c(x) = M \cdot x, \text{ unde } M \text{ e o matrice inversabilă din } M_2(\mathbb{Z}_m).$$

(Obs.: Aplicația de decriptare e în ea de același formă.)

CKG-BAL CGYINJA.

Notând cu D matricea de decriptare, $D = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}_{28})$, informațile de mai sus se concretizează în:

$$\begin{aligned} D\begin{pmatrix} 8 \\ 5 \end{pmatrix} &= \begin{pmatrix} 19 \\ 7 \end{pmatrix} \Leftrightarrow \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 8 \\ 5 \end{pmatrix} = \begin{pmatrix} 19 \\ 7 \end{pmatrix} \quad \left. \right\} (1) \\ D\begin{pmatrix} 17 \\ 16 \end{pmatrix} &= \begin{pmatrix} 7 \\ 4 \end{pmatrix} \Leftrightarrow \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 17 \\ 16 \end{pmatrix} = \begin{pmatrix} 7 \\ 4 \end{pmatrix} \quad \left. \right\} (2) \end{aligned}$$

$$\begin{matrix} a & b & c & d & e & f & g & h & i & j & k & l & m & n & o & p & q & r & s & t & u & v & w & x & y & z & - & ! \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 & 20 & 21 & 22 & 23 & 24 & 25 & 26 & 27 \end{matrix}$$

$$(1) \Leftrightarrow \begin{cases} 8a + 5b = 19 \\ 17a + 16b = 7 \\ 8c + 5d = 7 \\ 17c + 16d = 4 \end{cases}$$

$$\begin{vmatrix} 8 & 5 \\ 17 & 16 \end{vmatrix} = -96 + 55 = -41 = 15$$

$$a = -13 \begin{vmatrix} -9 & 5 \\ 7 & 16 \end{vmatrix} = -13 \cdot 73 = -13 \cdot (-11) = 3,$$

$$b = -13 \begin{vmatrix} 8 & -9 \\ -11 & 7 \end{vmatrix} = -13 \cdot (-43) = -13 \cdot 13 = -169 = -1.$$

$$c = -13 \begin{vmatrix} 7 & 5 \\ 4 & 16 \end{vmatrix} = -13 \cdot 8 = -104 = 8$$

$$d = -13 \begin{vmatrix} 8 & 7 \\ -21 & 4 \end{vmatrix} = -13 \cdot (4 - 7) = 39 = 11$$

$$\text{Deci } D = \begin{pmatrix} 3 & -1 \\ 8 & 11 \end{pmatrix}$$

Acum desfășurăm mesajul:

$$\begin{pmatrix} 3 & -1 \\ 8 & 11 \end{pmatrix} \begin{pmatrix} 2 & 6 & 1 & 11 & 6 & 8 & 9 \\ 10 & 26 & 0 & 2 & 24 & 13 & 0 \end{pmatrix} = \begin{pmatrix} 24 & 20 & 3 & 3 & 22 & 11 & 27 \\ 14 & 26 & 8 & 26 & 4 & 11 & 16 \end{pmatrix},$$

deci mesajul inițial e you-did-well!

Semimmar 8 - 311

Rezolvări congruență:

$$2x^3 - x - 4 \equiv 0 \pmod{125}$$

Pb. "prelext"

H. a o rezolvare me trebuie să rezulte.

* LEMEA CHINEZĂ A RESTURILOR

Îf $m_1, m_2, \dots, m_m \in \mathbb{N}^* \setminus \{1\}$ ($m \geq 2$) cu prop. $(m_i, m_j) = 1$, $\forall i \neq j \in \mathbb{N}$ și $a_1, a_2, \dots, a_m \in \mathbb{Z}$. Atunci sistemul de congruențe

$$(S) \quad \begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_m \pmod{m_m} \end{cases}$$

are soluție.

Mai mult, dacă $x_0 \in \mathbb{Z}$ e o soluție a lui (S) , atunci $x \in \mathbb{Z}$ e soluție pt. (S) dacă $x \equiv x_0 \pmod{m_1 m_2 \dots m_m}$.

Derm.: Notăm $m = m_1 m_2 \dots m_m$ și $M_i = \frac{m}{m_i}$, $i = \overline{1, m}$.

Obs.: $(M_i, m_i) = 1$, deci congruența

$M_i y \equiv 1 \pmod{m_i}$ are soluții.

Îf y_i e soluție a $M_i y \equiv 1 \pmod{m_i}$ notăm $e_i = M_i y_i$. Atunci $e_i \equiv \delta_{ij} \pmod{m_j}$ $\forall i, j \in \{1, 2, \dots, m\}$.

Atunci $\underbrace{a_1 e_1 + a_2 e_2 + \dots + a_m e_m}_{\parallel \text{not}} = a_i \pmod{m_i}$ $\forall i \in \{1, 2, \dots, m\}$

(deci a e sol. pt. (S)).

Îf $x \in \mathbb{Z}$ e o soluție a lui (S) .

Atunci $x \equiv a_i \equiv a \pmod{m_i}$ $\forall i = \overline{1, m}$, deci $x \equiv a \pmod{[m_1, m_2, \dots, m_m]}$

$$\delta_{ij} = \begin{cases} 0, & j \neq i \\ 1, & j = i. \end{cases}$$

d.m. SIMBOLUL LUI KRONECKER.

$$\parallel (m_i, m_j) = 1$$

Reciproc, dacă $x \in \mathbb{Z}$ e apă încât $x \equiv a \pmod{m_i}$, atunci $x - a \equiv 0 \pmod{m_i}$ $\forall i = \overline{1, m}$, deci $x \equiv a \pmod{[m_1, m_2, \dots, m_m]}$.

Exemplu: Verificați dacă sistemul

$$S: \begin{cases} 3x \equiv 10 \pmod{5} \\ 7x \equiv 8 \pmod{4} \\ 5x \equiv 3 \pmod{9} \end{cases}$$

are soluții. În caz afirmativ, rezolvă-l!

Soluție: $S \Leftrightarrow \begin{cases} 3x \equiv 2 \pmod{5} \\ 3x \equiv 1 \pmod{4} \\ 8x \equiv 7 \pmod{9} \end{cases} \Leftrightarrow \begin{cases} x \equiv 4 \pmod{5} \\ x \equiv 3 \pmod{4} \\ x \equiv 2 \pmod{9} \end{cases}$

Cum $(5, 4) = 1$, $(4, 9) = 1$, $(9, 5) = 1$, cf. lemea chineză a resturilor 5 are soluții.

Ca măsurări dim LCR, $m_1=5$, $m_2=4$, $m_3=9$, $M_1=36$, $M_2=45$, $M_3=20$.

$M_1 y \equiv 1 \pmod{m_1} \Leftrightarrow 36y \equiv 1 \pmod{5} \Leftrightarrow y \equiv 1 \pmod{5}$.

Luăm $y_1=1$, deci $e_1=M_1 y_1=36$.

$M_2 y \equiv 1 \pmod{m_2} \Leftrightarrow 45y \equiv 1 \pmod{4} \Leftrightarrow y \equiv 1 \pmod{4}$

Luăm $y_2=1$, deci $e_2=M_2 y_2=45$.

$M_3 y \equiv 1 \pmod{m_3} \Leftrightarrow 20y \equiv 1 \pmod{9} \Leftrightarrow 2y \equiv 1 \pmod{9} \Leftrightarrow y=5 \pmod{9}$;

Luăm $y_3=-4$, deci $e_3=M_3 y_3=-80$.

Cf. LCR, numărul $4 \cdot 36 + 3 \cdot 45 + 2 \cdot (-80) = 119$ e soluție a lui S.

Că urmăre, cf. LCR, soluția sistemului S conată în valoare $x \in \{119 + 180\lambda : \lambda \in \mathbb{Z}\}$.

Teorema chineză a resturilor

Fie m_1, m_2, \dots, m_n ca-n LCR și fie $f \in \mathbb{Z}[x]$. Dacă pt. fiecare $i=\overline{1, n}$ congruența $f(x) \equiv 0 \pmod{m_i}$ are $d_i \in \mathbb{N}$ soluții, atunci congruența $f(x) \equiv 0 \pmod{\prod_{i=1}^n m_i}$ are $d_1 d_2 \dots d_n$ soluții.

Denum.: Se notează $f = \sum_{i=0}^n c_i x^i$.

Fie a_1, a_2, \dots, a_m căte o soluție pentru $f(x) \equiv 0 \pmod{m_1}$, și. Fie $a = \sum_{i=1}^m a_i e_i$, e_i dim dom LCR. Atunci $f(a) = \sum_{i=0}^n c_i \left(\sum_{j=1}^m a_j e_j \right)^i \stackrel{\text{mod } m_1}{=} \sum_{i=0}^n c_i a_1^i = f(a_1) \equiv 0 \pmod{m_1}$, $\forall i=\overline{1, n}$.

Că urmăre, $f(a) \equiv 0 \pmod{[m_1, m_2, \dots, m_n]}$.

Reciproc, dacă $a \in \mathbb{Z}$ e soluție pentru $f(x) \equiv 0 \pmod{m_i}$, atunci a e sol. pt. $f(x) \equiv 0 \pmod{m_i}$ pentru fiecare $i=\overline{1, n}$.

Așa pus astfel în evidență funcțiile

$$\{(a_1, a_2, \dots, a_n) \in \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \dots \times \mathbb{Z}_{m_n} : f(a_i) \equiv 0 \pmod{m_i} \quad \forall i=\overline{1, n}\}$$

$$\begin{array}{c} \phi \downarrow \uparrow \psi \\ \{(a \in \mathbb{Z}_m : f(a) \equiv 0 \pmod{m})\} \end{array}, \text{ multimea soluțiilor lui } f(x) \equiv 0 \pmod{m}$$

$$\phi((a_1, a_2, \dots, a_n)) = a_1 e_1 + a_2 e_2 + \dots + a_n e_n$$

$$(a, a, \dots, a) = \psi(a)$$

$$\psi \phi((a_1, a_2, \dots, a_n)) = \psi(a_1 e_1 + a_2 e_2 + \dots + a_n e_n) = (\underbrace{a_1 e_1 + \dots + a_n e_n}_{\in \mathbb{Z}_{m_1}}, \dots, \underbrace{a_1 e_1 + \dots + a_n e_n}_{\in \mathbb{Z}_{m_n}}) =$$

$$= (a_1, a_2, \dots, a_n)$$

$$\phi \psi(a) = \phi((a, a, \dots, a)) = a e_1 + a e_2 + \dots + a e_n \stackrel{m_i}{=} a \quad \forall i=\overline{1, n}.$$

Că urmăre, $\phi \psi(a) \equiv a \pmod{m}$, deci $\phi \psi(a) = a$.

Morală: $\psi = \phi^{-1}$, deci ϕ e inv., deci ϕ e bijectie, ceea ce furnizează imediat concluzie.

Teorema Morala: Dacă considerăm o soluție a congruenței $f(x) \equiv 0 \pmod{p^{k+1}}$, ($f \in \mathbb{Z}[x]$, $p \in \mathbb{N}$ prim, $k \in \mathbb{N}^*$), atunci a e soluție și pt. $f(x) \equiv 0 \pmod{p^k}$.
 În plus, $x^p \equiv a \in \{0, 1, \dots, p^k - 1\}$, deci $\exists \lambda \in \{0, 1, \dots, p-1\}$ $a = a + \lambda p^k$.
 Prin urmare $f = c_0 + c_1 x + \dots + c_k x^k$, $f(a + \lambda p^k) \equiv 0 \pmod{p^{k+1}}$

$$c_0 + c_1 a + c_2 a^2 + c_3 a^3 + \dots + c_k a^k + \lambda p^k + c_2 a^2 \lambda p^k + c_3 a^3 \lambda p^k + \dots + c_k a^k \lambda p^k$$

$$\Leftrightarrow f(a) + f'(a) p^k \lambda \equiv 0 \pmod{p^{k+1}} \quad \xleftarrow[f(a) \equiv p^k]{\text{termeni}} \quad f'(a) \lambda \equiv -\frac{f(a)}{p^k} \pmod{p} \quad \text{(mod } p^{k+1})$$

De aici obținem

LEMĂ LUI HENSEL

Fie $f \in \mathbb{Z}[x]$ și fie $a \in \mathbb{Z}$ o soluție a congruenței $f(x) \equiv 0 \pmod{p^k}$ (p prim, $k \in \mathbb{N}^*$). Atunci:

- (i) Dacă $p \nmid f'(a)$, există o unică valoare $\lambda \in \{0, 1, \dots, p-1\}$ astfel că $f(a + \lambda p^k) \stackrel{p}{\equiv} 0$.
- (ii) Dacă $p \mid f'(a)$ dar $p \nmid \frac{f(a)}{p^k}$, atunci nu există nicio valoare $\lambda \in \{0, 1, \dots, p-1\}$ cu $f(a + \lambda p^k) \equiv 0 \pmod{p^{k+1}}$.
- (iii) Dacă $p \mid f'(a)$ și $p \mid \frac{f(a)}{p^k}$, atunci $f(a + \lambda p^k) \equiv 0 \pmod{p^{k+1}} \quad \forall \lambda \in \{0, 1, \dots, p-1\}$.

Rămăși să rezolvem congruența inițială:

• Rezolvăm mai întâi congruențe

$$(1) : 2x^3 - x - 4 \equiv 0 \pmod{25}$$

$$\pmod{5} : 2x^3 - x - 4 \equiv 0 \pmod{5} \Leftrightarrow x \in \{2, 4\}.$$

Considerăm soluția $a \equiv 2 \pmod{5}$

Incercați să "rădăcați" la ad $\pmod{25}$.

$$2(2+5\lambda)^3 - (2+5\lambda) - 4 \equiv 0 \pmod{25} \Leftrightarrow 16 + 120\lambda + 25\lambda^2 - 2 - 5\lambda - 4 \equiv 0 \pmod{25} \Leftrightarrow$$

$$\Leftrightarrow 115\lambda \equiv -10 \pmod{25} \Leftrightarrow 23\lambda \equiv -2 \pmod{5} \Leftrightarrow 3\lambda \equiv -2 \pmod{5} \Leftrightarrow \lambda = 1.$$

Că urmăre, 2 "rădăci" le soluție $a' \equiv ? \pmod{25}$.

Incercați să "rădăcați" $a' \equiv ? \pmod{25}$ la ad $\pmod{125}$

$$2(1+25\lambda)^3 - (1+25\lambda) - 4 \equiv 0 \pmod{125} \Leftrightarrow 686 + 25\lambda - 1 + 25\lambda^2 - 4 \equiv 0 \pmod{125}$$

$$\Leftrightarrow 675 \equiv 0 \pmod{125}, \text{ care nu are soluții.}$$

Deci congruența $2x^3 - x - 4 \equiv 0 \pmod{125}$ nu are soluții obținute prin "rădăcarea" soluției $x \equiv 2 \pmod{5}$.

Germinal 9

1. Determinăm $i \text{ mod}_5 (19) \pmod{23}$

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

Conform tabelului, $i \text{ mod}_5 (19) = 15$.

- Rezolvări congruențe:
 - $x^6 \equiv 7 \pmod{23}$
 - $x^6 \equiv 6 \pmod{23}$.

Să notăm $y = i \text{ mod}_5 x \pmod{23}$

$$\text{a)} x^6 \equiv 7 \pmod{23} \Leftrightarrow (5y)^6 \equiv 5^{19} \pmod{23} \Leftrightarrow 5^6y^6 \equiv 5^{19} \pmod{23} \Leftrightarrow 6y \equiv 19 \pmod{22} \quad (\underbrace{(6,22)=2}_{\Rightarrow y \in \mathbb{Z}}) \Rightarrow y \in \emptyset.$$

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

$$\text{b)} x^6 \equiv 6 \pmod{23} \Leftrightarrow (5y)^6 \equiv 5^{18} \pmod{23} \Leftrightarrow 6y \equiv 18 \pmod{22} \Leftrightarrow 3y \equiv 9 \pmod{11} \Leftrightarrow y \equiv 3 \pmod{11} \Leftrightarrow y \equiv 3 \text{ sau } 14 \pmod{22} \Leftrightarrow 5^6y \equiv 10 \text{ sau } 13 \pmod{23} \Rightarrow x \equiv 10 \text{ sau } 13 \pmod{23}.$$

Continuare curs:

Dacă $p \in 2N+1$ este prim, considerăm $U(\mathbb{Z}_p) = \mathbb{Z}_p \setminus \{0\}$

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

Numărănd $p-1 = q_1^{\alpha_1} q_2^{\alpha_2} \cdots q_n^{\alpha_n}$ (deosebit de standard), elementele $\bar{a} \in U(\mathbb{Z}_p)$ ce nu au ordin $p-1$ trebuie că aibă cel puțin un divizor al lui $\frac{p-1}{2^1}$ sau al lui $\frac{p-1}{2^2}, \dots$ sau al lui $\frac{p-1}{2^n}$, deci trebuie că fie rădăcini pt. $x^{\frac{p-1}{2^1}} - 1$ sau pt. $x^{\frac{p-1}{2^2}} - 1, \dots$ sau pt. $x^{\frac{p-1}{2^n}} - 1$, deci aceste elemente \bar{a} de ordin < $p-1$ constituie multimea $R = \bigcup_{j=1}^n R_{\frac{p-1}{2^j}}$, unde R_k e multimea rădăcinilor lui $x^k - 1 \in \mathbb{Z}_p[x]$.

$$\text{Dacă } |R| = \sum_{j=1}^n |T_j| - \sum_{1 \leq i < j \leq n} |T_i \cap T_j| + \dots$$

Dacă elementele lui $T_i \cap T_j$ sunt rădăcinile comune ale pol. $x^{\frac{p-1}{2^i}} - 1$ și $x^{\frac{p-1}{2^j}} - 1$, adică red. lui $(x^{\frac{p-1}{2^i}} - 1, x^{\frac{p-1}{2^j}} - 1) = x^{(\frac{p-1}{2^i}, \frac{p-1}{2^j})} = x^{\frac{p-1}{2^{\min(i,j)}}} - 1$.

Continuând analog obținem

$$|R| = (p-1) \left(\sum_{j=1}^n \frac{1}{2^j} - \sum_{1 \leq i < j \leq n} \frac{1}{2^i 2^j} + \sum_{1 \leq i < j < k \leq n} \frac{1}{2^i 2^j 2^k} - \dots \right) \Rightarrow$$

$$|\mathbb{Z}_p^\times \setminus R| = (p-1) \left(1 - \sum_{j=1}^n \frac{1}{2^j} + \sum_{1 \leq i < j \leq n} \frac{1}{2^i 2^j} - \dots \right) = (p-1) \left(1 - \frac{1}{2^1} \right) \left(1 - \frac{1}{2^2} \right) \cdots \left(1 - \frac{1}{2^n} \right) = \varphi(p-1)$$

Morală: Modulo orice nr. prim p există $\varphi(p-1)$ nădejdești primitive.

Ria numărelor cu epl.
în criptografie

Seminarul 10 - 311

1. Descompuneti în factori primi numărul $2^{48} + 1$.
2. Câte cifre are în perioadă numărul $\frac{1}{2023}$?

Sol.: 1) $N \stackrel{\text{not.}}{=} 2^{48} + 1 = (2^{16} + 1)(2^{32} - 2^{16} + 1)$

• $\exists p$ prim cu $p | 2^{16} + 1$

Așa că $\begin{cases} 2^{16} \equiv -1 \pmod{p} \\ 2^{32} \equiv 1 \pmod{p}, \end{cases} \Rightarrow \varphi_p(2) = 32$

Dar $32 = \varphi_p(2) | p-1 \Rightarrow p \equiv 1 \pmod{32}$

$N = 65537$

$97 \cancel{| N}$

$193 \cancel{| N}$

$257^2 = (2^8 + 1)^2 = 2^{16} + 2^8 + 1 > 2^{16} + 1 = N$

Întrucât pt. orice nr. prim $p \in \mathbb{N}$, $p < \sqrt{N}$ avem $p \nmid N$, N este prim.

$N = 2^2 + 1. \quad F_0 \stackrel{\text{not.}}{=} 2^2 + 1 = 3,$

$F_1 = 2^2 + 1 = 5$

$F_2 = 2^2 + 1 = 17$

$F_3 = 2^2 + 1 = 257$

$F_4 = N$

Formulă: Toate $F_m = 2^{2^m} + 1$ sunt prime.

Euler: $F_5 = 2^{32} + 1 = 2^{32} + 2^{20} \cdot 5^4 - 2^{20} \cdot 5^4 + 1 = 2^{20} \left[\underbrace{2^4 + 5^4}_{641} \right] = (1 - 5 \cdot 2^4) \left(\underbrace{(1 + 5 \cdot 2^4)}_{641} \right) \left(1 + 5 \cdot 2^4 \cdot 2^{14} \right) > 641$

• $\exists p$ prim cu $p | 2^{32} - 2^{16} + 1 \stackrel{\text{not.}}{=} M | 2^{48} + 1$.

Așa că $\begin{cases} 2^{48} \equiv -1 \pmod{p} \\ 2^{32} \equiv 1 \pmod{p} \end{cases} \Rightarrow (\varphi_p(2) | 96 \wedge \varphi_p(2) \nmid 48) \Leftrightarrow \varphi_p(2) \in \{32, 96\}$.

$\varphi_p(2) = 32 \Rightarrow \begin{cases} 2^{32} \equiv 1 \pmod{p} \\ 2^{48} \equiv -1 \pmod{p} \end{cases} \xrightarrow[\substack{2 \in U(\mathbb{Z}_p) \\ \text{deci}}]{(\varphi_p(p) = 1)} 2^{16} \equiv -1 \pmod{p} \Rightarrow p | 2^{16} + 1 = N \xrightarrow[\substack{\text{prim}}]{N_p} p = N$

Așa că $2^{16} + 1 = N (2^{32} - 2^{16} + 1) = (2^{16} + 1)2 - 32 \cdot 2^{16} \Rightarrow 2^{16} + 1 | 3 \cdot 2^{16}$, astfel (generată de TF Aritm), sau de consecință imediată $2^{16} + 1 | 3$)

Rămâne, deci, că $\gamma_p(2) = 96$.

Că urmăre, $96 = \gamma_p(2)/p-1$ deci $p \equiv 1 \pmod{97}$

$$M = 2^{32} - 2^{16} + 1 = 65536 \cdot 65535 + 1 = 4.294.901.761 = 193 \cdot \underline{\underline{22.253.377}} \quad \text{not. L}$$

$193XL$; $481XL$; $577XL$; $673XL$; $769XL$; $1057XL$; $1153XL$; $1249XL$; $1441XL$; $1537XL$; $1633XL$; $1729XL$; $1825XL$; $1821XL$; $2017XL$; $2113XL$; $2497XL$; $2593XL$; $2689XL$; $2881XL$; $2947XL$; $3043XL$; $3169XL$; $3361XL$; $3457XL$; $3553XL$; $3649XL$; $3841XL$; $3937XL$; $4033XL$; $4129XL$; $4321XL$; $4417XL$; $4513XL$; $4609XL$; $4703XL$; $4799 > \sqrt{L}$, deci amănăvile se pot opri aici și concluzia e că L e prim.

Că urmăre, descompunerea lui $2^{48} + 1$ în factori primi este $193 \cdot 65537 \cdot 22253377$

2. $\exists t, a_1, a_2, \dots, a_t$

$$\begin{aligned} 2) \sqrt{\frac{1}{2023}} = 0, (\overline{a_1 a_2 a_3 \dots a_t}) &= \overline{\frac{a_1 a_2 \dots a_t}{10^{t-1}}} \quad \begin{matrix} \exists t, a_1, a_2, \dots, a_t \\ \downarrow \\ 2023 \cdot \overline{a_1 a_2 \dots a_t} = 10^{t-1} \end{matrix} \quad (\Rightarrow) \\ \Leftrightarrow 2023 | 10^{t-1} \quad (\Rightarrow) \quad 10^t \equiv 1 \pmod{2023} \quad (\Rightarrow) \quad \gamma_{2023}(10) | t \end{aligned}$$

De fapt, însă, "numărul de cifre din perioada" lui 2023 înseamnă CEL MAI MIC astfel de $t \in \mathbb{N}^*$, adică $\gamma_{2023}(10)$.

Mai trebuie, deci, să găsim pe $\gamma_{2023}(10)$.

Dar

$$\gamma_{2023}(10) = \text{ord}_{U(\mathbb{Z}_{2023})} 10 = \text{ord}_{U(\mathbb{Z}_7) \times U(\mathbb{Z}_{17^2})} (10) = [\text{ord}_{U(\mathbb{Z}_7)} (10), \text{ord}_{U(\mathbb{Z}_{17^2})} (10)]$$

căci, dacă $(a, b) = 1$,
 $\mathbb{Z}_a \times \mathbb{Z}_b \xrightarrow{\cong} \mathbb{Z}_{ab}$
 $(\bar{a}, \bar{b}) \longleftarrow \bar{a}^{-1}$
e izomorfism.

$$= [6, \text{ord}_{U(\mathbb{Z}_{17^2})} (10)].$$

Nărmă $\gamma = \text{ord}_{U(\mathbb{Z}_{17^2})} (10)$.

Atunci $10^8 \equiv 1 \pmod{17^2} \Rightarrow 10^8 \equiv 1 \pmod{17} \Rightarrow \gamma \mid \text{ord}_{U(\mathbb{Z}_{17})} (10) = \gamma_{17}(10)$

$$\text{Dacă } 10^2 \equiv 17 \pmod{17^2} \Rightarrow 10^2 \equiv -2 \pmod{17} \Rightarrow 10^4 \equiv 4 \pmod{17} \Rightarrow 10^8 \equiv 16 \equiv -1 \pmod{17} \Rightarrow 10^{16} \equiv 1 \pmod{17}$$

Că urmăre $\gamma_{17}(10) = 16$.

De mai sus, $16 \mid \gamma$

$$\text{Dacă } \gamma \mid |\text{U}(\mathbb{Z}_{17^2})| = \varphi(17^2) = 16 \cdot 17 \quad \Rightarrow \gamma \in \{16, 16 \cdot 17\}. \quad (1)$$

$$10^2 \equiv 100 \pmod{17^2}; \quad 10^4 \equiv 100^2 \equiv 174 \pmod{17^2}; \quad 10^8 \equiv 174^2 \equiv 220 \equiv -69 \pmod{17^2}, \quad 10^{16} \equiv 69^2 \equiv 137 \not\equiv 1 \pmod{17^2}$$

Că urmăre, $\gamma \neq 16 \quad \Rightarrow \quad (1) \quad \Rightarrow \quad \gamma = 16 \cdot 17$.

În consecință, $\frac{1}{2023}$ are în perioada $\gamma_{2023}(10) = [6, 16 \cdot 17] = 10 \cdot 51 = 816$ cifre.