

CHESTIUNI COMPLEMENTARE MANUALELOR

Mica teoremă a lui Fermat

Mihai CRĂCIUN¹

"Ce dorești să afli
e adânc ca marea și ca cerul ..."
Mihail SADOVEANU

Presupunem cunoscute numai acele noțiuni și rezultate din teoria divizibilității cu care elevul se întâlnește în ciclul gimnazial.

Teoremă (Mica teoremă a lui Fermat). *Dacă p este un număr prim și n un număr natural nenul astfel încât $(n, p) = 1$, atunci avem*

$$n^{p-1} - 1 \vdots p \quad . \quad (1)$$

Demonstrație. Considerăm primii $p - 1$ multipli ai numărului n : $1 \cdot n, 2 \cdot n, 3 \cdot n, \dots, (p - 1) \cdot n$. Resturile împărțirii acestora la p sunt respective: $r_1, r_2, r_3, \dots, r_{p-1}$. Așadar, avem relațiile:

$$i \cdot n = p \cdot c_i + r_i, \quad 0 \leq r_i < p \quad (i = 1, 2, \dots, p - 1). \quad (2)$$

Observăm că $r_i \neq 0$ pentru orice $i = 1, 2, \dots, p - 1$; în caz contrar, ar urma că $p \mid i \cdot n$, deci $p \mid n$, ceea ce contravine ipotezei $(n, p) = 1$. Mai observăm că resturile r_1, r_2, \dots, r_{p-1} sunt diferențe între ele; dacă am avea $r_i = r_j$, atunci ar rezulta $(i - j)n = p(c_i - c_j)$, de unde $p \mid n$, din nou în contradicție cu ipoteza. Aceste afirmații permit să concluzionăm că r_1, r_2, \dots, r_{p-1} sunt numerele 1, 2, ..., $p - 1$ aranjate într-o anumită ordine.

Înmulțind egalitățile (2), vom obține

$$1 \cdot 2 \cdot \dots \cdot (p - 1) n^{p-1} = (pc_1 + r_1) \cdot (pc_2 + r_2) \cdot \dots \cdot (pc_{p-1} + r_{p-1})$$

sau

$$1 \cdot 2 \cdot \dots \cdot (p - 1) n^{p-1} = p \cdot t + r_1 r_2 \dots r_{p-1}, \quad t \in \mathbb{N}^*,$$

deci

$$1 \cdot 2 \cdot \dots \cdot (p - 1) n^{p-1} = p \cdot t + 1 \cdot 2 \cdot \dots \cdot (p - 1),$$

adică

$$1 \cdot 2 \cdot \dots \cdot (p - 1) (n^{p-1} - 1) = pt, \quad t \in \mathbb{N}^*,$$

de unde $n^{p-1} - 1 \vdots p$, q.e.d.

Observații. 1) Relația (1) se poate scrie sub forma

$$n^p - n \vdots p \quad (3)$$

(ce rezultă imediat, dacă înmulțim $n^{p-1} - 1 = u \cdot p$ cu $n \neq 0$).

2) Mica teoremă a lui Fermat poate fi demonstrată și prin metoda inducției complete, cu ajutorul binomului lui Newton etc.

¹ Profesor, Grupul școlar "Unirea", Pașcani

Problema 1. Să se arate că $E = 1848^{18n} + 96^{14n} - 2 \vdots 19$ pentru orice $n \in \mathbb{N}$.

Soluție. Avem $E = (1848^{18n} - 1) + (96^{14n} - 1)$. Dar

$$1848^{18n} - 1 = (1848^{18})^n - 1 = m(1848^{18} - 1) = m(1848^{19-1} - 1) = m' \cdot 19, \quad m' \in \mathbb{N}^*$$

(ultima egalitate are loc conform teoremei lui Fermat) și

$$96^{14n} - 1 = t(96 - 1) = t \cdot 95 = t \cdot 5 \cdot 19 = t' \cdot 19, \quad t' \in \mathbb{N}^*.$$

Deci $E \vdots 19$.

Problema 2. Să se demonstreze că $A = 3^{1966} + 5^{1966} - 34 \vdots 1966$.

Soluție. Deoarece 983 este număr prim, conform teoremei lui Fermat avem: $3^{982} = t \cdot 983 + 1, t \in \mathbb{N}^*$. Ridicând la pătrat, obținem: $3^{1964} = m \cdot 983 + 1, m \in \mathbb{N}^*$, sau, prin înmulțire cu $3^2, 3^{1966} = u \cdot 983 + 9, u \in \mathbb{N}^*$. În mod analog, se obține: $5^{1966} = v \cdot 983 + 25, v \in \mathbb{N}^*$. Prin adunarea ultimelor două relații, vom avea:

$3^{1966} + 5^{1966} = (u + v) \cdot 983 + 34$, deci $A \vdots 983$. De aici și din faptul că A este număr par, rezultă că $A \vdots 1966$.

Problema 3. Să se afle restul împărțirii numărului 17^{219} la 73.

Soluție. Deoarece $(17, 73) = 1$, conform cu mica teoremă a lui Fermat, avem

$$17^{73} - 17 \vdots 73, \text{ adică } 17^{73} = 73t + 17, t \in \mathbb{N}^*$$

$$17^{219} = (73t + 17)^3 = u \cdot 73 + 17^3 = u \cdot 73 + 4913 = u \cdot 73 + 67 \cdot 73 + 22 = v \cdot 73 + 22.$$

Deci $17^{219} = v \cdot 73 + 22, v \in \mathbb{N}^*$, adică restul împărțirii este 22.

Problema 4. Să se arate că, dacă $a \in \mathbb{N}^*$ nu este multiplu de 5 sau 7, atunci $E = (a^4 - 1)(a^4 + 15a^2 + 1)$ se divide cu 35.

Soluție. În condițiile problemei $a^4 - 1 = a^{5-1} - 1 \vdots 5$; deci $E \vdots 5$. Putem scrie

$$E = (a^4 - 1)[(a^4 + a^2 + 1) + 14a^2] = (a^4 - 1)(a^4 + a^2 + 1) + 14a^2(a^4 - 1) = \\ = (a^2 + 1)[(a^2 - 1)(a^4 + a^2 + 1)] + 14a^2(a^4 - 1) = (a^2 + 1)(a^6 - 1) + 14a^2(a^4 - 1).$$

Deoarece $a^6 - 1 \vdots 7$ (mica teoremă a lui Fermat) și $14a^2(a^4 - 1) \vdots 7$ rezultă că $E \vdots 7$.

Din $(5, 7) = 1$, $E \vdots 5$ și $E \vdots 7$, deducem că, în ipotezele din enunț, $E \vdots 35$.

Probleme propuse.

1. Să se arate că, dacă n nu este multiplu de 5, atunci

$$A = (11^{2n} - 2^{6n})(n^4 - 1) \vdots 285.$$

2. Să se demonstreze că:

(i) $7^{1994} + 5^{1994} - 74 \vdots 1994$,

(ii) $13^{1983} + 17^{1983} - 458 \vdots 1982$.

3. Să se găsească restul împărțirii numărului 439^{72} la 13.

4. Să se afle restul împărțirii numărului $A = 8^{183} + 13^{211}$ la 15.

5. Să se determine numărul prim x astfel încât $7^{x^3} + 5 \vdots x$.

① Calculate ordinal div $\bar{8}$ in group $(\mathbb{Z}_{100}, +)$.

Ex 2/June
2021

$$K = \text{ord}(\bar{8}) = \text{ord max nr. natural rem. pwr. of } 8$$

$$\bar{8}k = \bar{0} \Rightarrow 100 \cdot 2 \Rightarrow 100 \mid 8k \Leftrightarrow 25 \mid 2k \Rightarrow \boxed{K=25}$$

$$\text{verifcate: } 8 \cdot 25 = 200 \checkmark$$

Ex 2(b) Calculate ordinal div $\bar{52}$ in group $(\mathbb{Z}_{100}, +)$.

$$K = \text{ord}(\bar{52}) = \text{ord max nr. natural rem. pwr. of } 52$$

$$= 100 \cdot 2 \Rightarrow 100 \mid 52k \Leftrightarrow 50 \mid 26k \Leftrightarrow 25 \mid 13k \Rightarrow \boxed{K=25}$$

Ex 2(c) Calculate ordinal div $\bar{3}$ in group $(\mathbb{Z}_{47}, +)$.

$$K = \text{ord}(\bar{3}) = \underbrace{\dots}_{\text{nr. pwr.}} \Rightarrow \bar{3}k = \bar{0} = 61 \cdot 2 \Rightarrow$$

$$\Rightarrow 61 \mid 3k \Rightarrow \boxed{K=61}$$

② Calculate $\text{ord}(\bar{2})$ in group $(U(\mathbb{Z}_{47}), \cdot)$.

Ex 1/June 3. Notam $K = \text{ord}(\bar{2})$

Dim propertee 3 $\Rightarrow k \mid \text{ord}(6)$

$$\text{ord}(6) = |U(\mathbb{Z}_{47})| = \phi(47) \Rightarrow \phi(47) = \frac{47-1}{K} = 46 \Rightarrow$$

47 - prim

$$\Rightarrow K \in \{1, 2, 23, 46\}$$

Dim propertee 1 $\Rightarrow \bar{2}^k \equiv \bar{1} \pmod{47}$

$$\bar{2}^1 \equiv \bar{2} \not\equiv \bar{1} \pmod{47}$$

$$\bar{2}^2 \equiv \bar{4} \not\equiv \bar{1} \pmod{47}$$

$$\Rightarrow \bar{2}^{23} \equiv \bar{1} \pmod{47} \Rightarrow \boxed{K=23 = \text{ord}(\bar{2})}$$

③ Calculate $\text{ord}(\bar{8})$ in group $(U(\mathbb{Z}_{103}), \cdot)$.

$$102 = 2 \cdot 3 \cdot 17$$

$$\text{Notam } K = \text{ord}(\bar{8})$$

$$\text{Dim propertee 3} \Rightarrow K \mid \text{ord}(6) \Rightarrow \phi(103) = 103-1 = 102 \Rightarrow$$

$$\text{ord}(6) = |U(\mathbb{Z}_{103})| = \phi(103) \Rightarrow K \in \{1, 2, 3, 6, 17, 34, 51, 102\}$$

103 - prim

$$\bar{8}^1 \equiv \bar{8} \not\equiv \bar{1}$$

$$\bar{8}^2 \equiv \bar{16} \not\equiv \bar{1} \pmod{103}$$

$$\bar{8}^3 \equiv \bar{512} \equiv \bar{-3} \pmod{103} \equiv 105 \not\equiv \bar{1} \pmod{103}$$

$$\bar{8}^6 \equiv (\bar{8}^3)^2 \equiv (\bar{105})^2 \equiv 10,000 \equiv 9 \pmod{103} \not\equiv \bar{1}$$

$$\bar{8}^{17} \equiv \bar{8}^{18} \cdot \bar{8}^{-1} = \bar{8} \cdot \bar{8}^{-1} = \bar{8} \cdot \bar{13} = \bar{104} \pmod{103} \equiv \bar{1} \Rightarrow \boxed{\text{ord } \bar{8} = 17}$$

$$\bar{8}^{18} = \bar{8}^{6 \cdot 3} = (\bar{8}^6)^3 = (\bar{9})^3 = \bar{729} \equiv \bar{8} \pmod{103} \cancel{\Rightarrow K=17}$$

$$\begin{array}{r} 512 \\ 515 \\ \hline z=3 \end{array} \mid 103$$

$$\begin{array}{r} 10000 \\ 927 \\ \hline z=730 \end{array} \mid 103$$

$$\begin{array}{r} 721 \\ 721 \\ \hline z=9 \end{array} \mid 103$$

$$\begin{array}{r} 729 \\ 721 \\ \hline z=8 \end{array} \mid 103$$

$$\bar{8}^{-1} \pmod{103}$$

$$\bar{8} \cdot \bar{x} = \bar{1} \pmod{103}$$

$$\bar{8} \cdot \bar{x} = \bar{1} \mid \cdot \bar{13} \quad \text{in } (\mathbb{U}(103), \cdot)$$

$$\bar{103} \cdot \bar{x} = \bar{13} \Rightarrow \bar{1} \cdot \bar{x} = \bar{13} \Rightarrow \boxed{\bar{x} = \bar{13}}$$

$$\bar{103} \equiv \bar{1} \quad \text{verifizieren: } 13 \cdot 8 = 104 \equiv 1 \pmod{103}$$

dann: $103 = 8 \cdot \boxed{12} + 7$

2: $8 = 7 \cdot \boxed{1} + 1$

3: $7 = 1 \cdot \boxed{7}$

Algorithmus von Euclid

$$\begin{array}{l} A \\ B \end{array} = 12 + \frac{1}{1} = \frac{13}{1}$$

$$\frac{103}{8} - \frac{13}{1} = \frac{(-1)^3}{8 \cdot 1} = \frac{(-1)}{8}$$

$$103 \cdot 1 - 13 \cdot 8 = (-1) \Rightarrow \begin{aligned} &(-8) \cdot (\bar{13}) = \bar{1} \mid (-1) \\ &\bar{8} \cdot \bar{13} = \bar{1} \Rightarrow \boxed{\bar{x} = \bar{13}} \end{aligned}$$

durchteile
multipliziere 103

$$8^{-1} = \bar{13} \quad \text{in } (\mathbb{U}(7403), \cdot)$$

④ Calculate ordmul($\bar{52}$) in group $(\mathbb{U}(759), \cdot)$.

cursus: $\text{ordmul } K = \text{ordmul}(\bar{52}) = \text{ord}(\bar{52})$

Dm properties 3 $\Rightarrow K \mid \text{ord}(6)$

$$\begin{aligned} \text{ord}(6) &= |\mathbb{U}(759)| = \phi(59) \Rightarrow \phi(59) = 59 - 1 = 58 \\ 59 &\text{-prim} \end{aligned} \Rightarrow K \in \{1, 2, 29, 58\}$$

Dm properties 1 $\Rightarrow \bar{52}^K = \bar{1} \pmod{59}$

$$\bar{52}^1 = \bar{52} \not\equiv 1 \pmod{59}$$

$$\bar{52}^2 = (-7)^2 = \bar{49} = -\bar{10} \pmod{59} \not\equiv 1$$

$$\bar{52}^{29} = (\bar{52}^2)^{14} \cdot \bar{52}$$

$$\bar{52}^4 = (\bar{52}^2)^2 = (-\bar{10})^2 = \bar{100} = \bar{51} \pmod{59} = -18 \pmod{59}$$

$$\bar{52}^8 = (\bar{52}^4)^2 = (-18)^2 = \bar{324} = \bar{29} \pmod{59}$$

$$\bar{52}^{16} = \bar{52}^8 \cdot \bar{52}^8 \cdot \bar{52}^2 = \bar{29} \cdot (-18) \cdot (-\bar{10}) = \bar{29} \cdot \bar{180} = \frac{29}{29 \cdot 3} = \frac{180}{177} \pmod{59}$$

$$\bar{52}^{29} = (\bar{29})^2 \cdot \bar{52} \cdot (-\bar{7}) = \bar{784} \cdot (-\bar{7}) =$$

$$= \bar{14} \cdot (-\bar{7}) \cdot (-\bar{18}) = -\bar{1} \not\equiv 1 \pmod{59}$$

$$\Rightarrow (\bar{52}^{29})^2 = \bar{52}^{58} = (-\bar{1})^2 = 1 \pmod{59}$$

$$\boxed{K = \text{ord}(\bar{52}) = 58}$$

$$\begin{array}{r} 180 \\ 59 \\ \hline 29 \end{array}$$

$$\begin{array}{r} 324 \\ 295 \\ \hline 5 \end{array}$$

$$\begin{array}{r} 29 \\ 29 \cdot 3 \\ \hline 177 \\ 2 \cdot 3 \\ \hline 180 \\ 177 \\ \hline 3 \end{array}$$

$$\begin{array}{r} 87 \\ 59 \\ \hline 28 \end{array}$$

$$\begin{array}{r} 784 \\ 59 \\ \hline 194 \\ 177 \\ \hline 17 \end{array}$$

$$\begin{array}{r} 119 \\ 118 \\ \hline 2 \end{array}$$

⑤ Calculate ord 2 in $U(\mathbb{Z}_{43})$.

Notiz: $d = \text{ord } 2$

Din proprietatea 3 $\Rightarrow d \mid \text{ord}(6) \Rightarrow \phi(43) = 43 - 1 = 42$

$$\text{ord}(6) = |U(\mathbb{Z}_{43})| = \phi(43)$$

$$43 - \text{prim}$$
$$2^1 \equiv 2 \pmod{43}$$

$$2^2 \equiv 4 \not\equiv 1$$

$$2^3 \equiv 8 \cdot 2 = 16 \not\equiv 1$$

$$2^4 \equiv (2^2)^2 = 16$$

$$2^6 = 2^4 \cdot 2^2 = 16 \cdot 4 = 64 \equiv 21 \pmod{43}$$

$$2^8 = 2^6 \cdot 2 = 21 \cdot 2 = 42 = -1 \pmod{43}$$

$$\Rightarrow (2^8)^2 = 2^{16} = (-1)^2 = 1 \Rightarrow \text{ord } 2 = 16 \pmod{43}$$

⑥ Calculate ord 7 in $U(\mathbb{Z}_{31})$.

Notiz: $d = \text{ord } 7$

Din proprietatea 3 $\Rightarrow d \mid \text{ord}(6) \Rightarrow \phi(31) = 31 - 1 = 30$

$$\text{ord}(6) = |U(\mathbb{Z}_{31})| = \phi(31)$$

31 - prim

$$|U(\mathbb{Z}_{31})| = 30 =$$

$$(31-7)/2 \mid 30 \Rightarrow \text{ord } 7 \mid 30$$
$$\Rightarrow d \in \{1, 2, 3, 5, 6, 10, 15, 30\}$$

$$7^1 \equiv 7 \not\equiv 1$$

$$7^2 = 49 \equiv 18 \pmod{31}$$

$$\begin{array}{c} 126 \\ 125 \mid 31 \\ \hline 1 \end{array}$$

$$7^3 = 7^2 \cdot 7 = 18 \cdot 7 = 126 \equiv 2 \not\equiv 1 \pmod{31}$$

$$7^5 = 7^3 \cdot 7^2 = 2 \cdot 18 = 36 \equiv 5 \not\equiv 1 \pmod{31}$$

$$7^6 = 7^5 \cdot 7 = 5 \cdot 7 = 35 \equiv 5 \not\equiv 1 \pmod{31}$$

$$7^{10} = (7^5)^2 = (5)^2 = 25 \not\equiv 1 \pmod{31}$$

$$7^{15} = (7^3)^5 = (2)^5 = 32 \equiv 1 \pmod{31} \Rightarrow d = \text{ord } 7 = 15$$

⑦ Calculate ord 3 in group $(U(\mathbb{Z}_{61}), \cdot)$.

Notiz: $d = \text{ord } 3$

Din proprietatea 3 $\Rightarrow d \mid \text{ord}(6) \Rightarrow \phi(61) = (61 - 1) = 60$

$$\text{ord}(6) = |U(\mathbb{Z}_{61})| = \phi(61)$$

61 - prim

$$|U(\mathbb{Z}_{61})| = 60 = 2^2 \cdot 3 \cdot 5$$

$$(61-3)/2 \mid 60 \Rightarrow \text{ord } 3 \mid 60$$

$$\Rightarrow d \in \{1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60\}$$

$$3^1 \equiv 3 \not\equiv 1$$

$$3^2 \equiv 9 \not\equiv 1$$

$$\begin{aligned}3^3 &\equiv 27 \not\equiv 1 \quad \text{---} \\3^4 &\equiv \cancel{81} = \cancel{1} \pmod{61} \\3^5 &\equiv (\cancel{1})^2 = \cancel{1} \pmod{61} \\3^6 &\equiv \cancel{1} \cdot \cancel{3} = \cancel{3} \pmod{61} \\3^{10} &\equiv (3^5)^2 \equiv (\cancel{1})^2 = \cancel{1} \end{aligned}$$

$$\begin{array}{r} 169 \mid 61 \\ 61 \mid 1 \\ \hline 169 \end{array}$$

$$\begin{array}{r} 2209 \mid 61 \\ 143 \mid 36 \\ 36 \mid 9 \\ \hline 2209 \end{array}$$

81

(8) Să se arate că cel mai mare divizor prim impar al numărului $2019^8 + 1$.

Baza

$$2019^8 + 1 \equiv p \cdot k \pmod{\varphi(p)}$$

$$2019^8 + 1 \equiv 0$$

$$2019^8 \equiv -1 \pmod{\varphi(p)} \Rightarrow ((2019)^8)^2 \equiv (-1)^2 \equiv 1 \Rightarrow (2019)^{16} \equiv 1$$

$$\varphi(2019) = 16 \Rightarrow 16 \mid \varphi(p) \Rightarrow p-1 \mid 16 \Rightarrow$$

$$\Rightarrow p-1 = 16n \Rightarrow p = 16n+1 \Rightarrow p \in \{17, 37, 53, 65, 89, 97, 113\}$$

$$\begin{array}{ll} \text{In } U(\mathbb{Z}_{17}) & 2019 = 17 \cdot 118 + 13 = 13 \quad \text{In } U(\mathbb{Z}_{47}), 13^2 = 169 \equiv 170 - 1 \equiv -1 \\ & \text{se aranjează} \quad \Rightarrow (13)^8 \equiv (-1)^4 \equiv 1 \quad \text{In } U(\mathbb{Z}_{47}) \end{array}$$

$$\begin{array}{ll} \text{In } U(\mathbb{Z}_{97}) & 2019 = 97 \cdot 20 + 79 = 79 \quad \text{In } U(\mathbb{Z}_{97}) \\ & 79^2 = 6241 \quad \text{se aranjează} \quad 79 = 97 \cdot 64 + 33 = 33 \end{array}$$

$$(79)^8 = (33)^2 = 1089 = 97 \cdot 11 + 22 = 22$$

$$(79)^8 = (22)^2 = 484 = 485 - 1 = 97 \cdot 5 - 1 = -1$$

$$\Rightarrow 2019^8 + 1 \equiv 0 \pmod{\varphi(p)}, \text{ deoarece } 2019^8 + 1 \text{ se divide cu 97.}$$

Algebră ID

Fie G o mulțime și $*$ o operație pe G (adică $*$ este o funcție definită pe $G \times G$ cu valori în mulțimea G ; în loc de $*((x, y))$ se notează tradițional $x * y$).

Definiție: Mulțimea G împreună cu operația $*$ formează un grup (notat cu $(G, *)$) dacă au loc următoarele proprietăți:

1) $x * (y * z) = (x * y) * z$, pentru orice $x, y, z \in G$. Această proprietate a operației $*$ se numește asociativitate.

2) Există un element $e \in G$ astfel încât $e * x = x * e = x$ pentru orice $x \in G$. [e se numește elementul neutru al grupului G ; el este unic]

3) Pentru orice $x \in G$, există $y \in G$ astfel încât $x * y = y * x = e$. [y se numește inversul lui x ; el este unic]

Dacă în plus $x * y = y * x$, pentru orice $x, y \in G$, grupul se numește comutativ.

Observație: Dacă avem $g * x = g * y$, într-un grup $(G, *)$, atunci $x = y$.

Exemple de grupuri:

1) $(\mathbb{R}, +)$, (\mathbb{Q}^*, \cdot) , unde $+$ și \cdot sunt adunarea și înmulțirea obișnuită de numere reale (respectiv rationale). Inversul lui 3 în primul grup este -3 iar inversul lui 3 în al doilea grup este $\frac{1}{3}$. *Mu Q Mu R*

2) Fie $n \geq 2$ un număr natural. Vom descrie în continuare grupul $(\mathbb{Z}_n, +)$ (grupul claselor de resturi modulo n cu adunarea). Fie $a, b \in \mathbb{Z}$. Scriem $a \equiv b \pmod{n}$ (și spunem că "a este congruent cu b modulo n") dacă n divide $a - b$. Același lucru îl notăm și cu $\bar{a} = \bar{b}$ (spunem că "clasa lui a modulo n este egală cu clasa lui b modulo n"). Vom nota cu $\mathbb{Z}_n = \{\bar{a} | a \in \mathbb{Z}\}$. Aceasta este o mulțime cu n elemente. Pe ea se definește următoarea operație:

$$\bar{a} + \bar{b} = \overline{a + b}, \forall a, b \in \mathbb{Z}.$$

Este ușor de văzut că $(\mathbb{Z}_n, +)$ este un grup comutativ cu n elemente. Elementul neutru este $\bar{0}$.

Exercițiu: Inversul lui $\bar{3}$ în grupul $(\mathbb{Z}_{10}, +)$ este $\bar{7}$. *10 - 3 = 7 ✓*

3) Cu notăriile de mai sus, vom considera mulțimea

$$U(\mathbb{Z}_n) = \{\bar{m} | m \in \mathbb{Z}, (m, n) = 1\}.$$

Se definește următoarea operație pe $U(\mathbb{Z}_n)$:

$$\bar{a} \cdot \bar{b} = \overline{a \cdot b}, \forall \bar{a}, \bar{b} \in U(\mathbb{Z}_n).$$

$U(\mathbb{Z}_n, \cdot)$ este un grup comutativ cu $\phi(n)$ elemente; elementul neutru este $\bar{1}$. Funcția ϕ se numește funcția lui Euler. Avem următoarea formulă:

$$\boxed{\phi(n) = n \cdot \prod_{p \text{ prim}, p|n} \left(1 - \frac{1}{p}\right), \forall n \in \mathbb{N}^*}$$

Exemplu: $\phi(100) = 100(1 - \frac{1}{2})(1 - \frac{1}{5}) = 40$.

Exemplu: Să se calculeze inversul lui $\overline{37}$ în $U(\mathbb{Z}_{100}, \cdot)$. Inversul căutat este $\overline{73}$ deoarece

$$\boxed{\overline{37} \cdot \overline{73} = \overline{2701} = \bar{1}.}$$

Procedură de calcul pentru inversul lui \bar{a} în grupul $(U(\mathbb{Z}_n), \cdot)$ (unde $a < n$ este un număr natural, prim cu n):

Se scrie algoritmul lui Euclid pentru a și n . Ultimul rest nenul va fi 1. Avem egalitățile:

$$n = a \cdot q_1 + r_1,$$

$$a = r_1 \cdot q_2 + r_2,$$

⋮

$$r_{m-2} = r_{m-1} \cdot q_m + r_m,$$

$$r_{m-1} = r_n \cdot q_{m+1},$$

unde cîturile și resturile sunt numere naturale cu

$$a > r_1 > r_2 > \dots > r_{m-1} > r_m = 1.$$

Se calculează fracția ireductibilă

$$\boxed{\frac{A}{B} = q_1 + \frac{1}{q_2 + \frac{1}{\vdots + q_{m-1} + \frac{1}{q_m}}}.}$$

Avem următorul rezultat:

$$\frac{n}{a} - \frac{A}{B} = \frac{(-1)^{m+1}}{a \cdot B}.$$

De aici deducem ușor că

$$\overline{a} \cdot \overline{(-1)^{m+1} \cdot A} = \bar{1}.$$

Ne întoarcem la exemplul anterior: calculul inversului lui $\overline{37}$ în $U(\mathbb{Z}_{100}, \cdot)$. Urmăram procedura descrisă anterior:

$$\begin{aligned}100 &= 37 \cdot \cancel{2+26}, \\37 &= 26 \cdot \cancel{1+11}, \\26 &= 11 \cdot \cancel{2+4}, \\11 &= 4 \cdot \cancel{2+3}, \\4 &= 3 \cdot \cancel{1+1}. \\3 &= 1 \cdot 3.\end{aligned}$$

Calculăm fractia

Avem

$$\frac{100}{37} - \frac{27}{10} = \frac{(-1)^6}{37 \cdot 10}$$

$$100 \cdot 10 - 37 \cdot 27 = 1,$$

$$\overline{37} \cdot \overline{(-27)} = \overline{1}.$$

Deoarece $\overline{-27} = \overline{73}$ în \mathbb{Z}_{100} , regăsim rezultatul anterior: inversul lui $\overline{37}$ este $\overline{73}$ în grupul $U(\mathbb{Z}_{100}, \cdot)$.

4) Fie $n \in \mathbb{N}^*$. Se notează cu S_n mulțimea permutărilor cu n elemente (adică funcțiile bijective

$$\sigma : \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, n\}.$$

Se definește operația \circ pe S_n în felul următor:

$$\sigma \circ \tau(j) = \sigma(\tau(j)), \forall \sigma, \tau \in S_n, j = \overline{1, n}.$$

(S_n, \circ) este un grup cu $n!$ elemente. Dacă $n \geq 3$, acest grup nu este comutativ. O permutare σ din S_n se notează în mod tradițional ca o matrice cu două linii și n coloane. Pe prima linie se pun în ordine numerele $1, 2, \dots, n$. Pe linia a doua se pune sub j numărul $\sigma(j)$. Cum se calculează inversa unei permutări în grupul (S_n, \circ) ? Se inversează cele două linii și apoi se ordonează numerele de pe prima linie.

Exemplu: să se calculeze inversa matricii $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \in S_4$. Inversarea celor două linii produce permutarea $\tau = \begin{pmatrix} 2 & 3 & 4 & 1 \\ 1 & 2 & 3 & 4 \end{pmatrix} \in S_4$. Ordonând numerele din prima linie (și valorile care le corespund în a doua), găsim următoarea descriere pentru τ , inversa lui σ :

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} \in S_4.$$

Pentru permutări se definește conceptul de signatură al permutării $\sigma \in S_n$. Pentru aceasta, definim întâi ce înseamnă o inversiune a permutării σ ; o pereche (i, j) , cu

i, j numere naturale din mulțimea $\{1, 2, \dots, n\}$ astfel încât $i < j$ și $\sigma(i) > \sigma(j)$. Notăm cu m numărul de inversiuni ale permutării σ . Signatura permutării σ se notează cu $\epsilon(\sigma)$ și este numărul

$$\epsilon(\sigma) = (-1)^m.$$

Signatura unei permutări are următoarea proprietate:

$$\epsilon(\sigma \circ \tau) = \epsilon(\sigma) \cdot \epsilon(\tau), \forall \sigma, \tau \in S_n.$$

$$\begin{pmatrix} 2 & 3 & 4 & 1 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

Exemplu: calculați signatura permutării $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \in S_4$. Inversiunile permutării σ sunt perechile: $(1, 4), (2, 4), (3, 4)$. Deci $m = 3$ și $\epsilon(\sigma) = (-1)^3 = -1$.

Teoreme:

1) (Lagrange) Într-un grup finit $(G, *)$, avem că $g^{|G|} = e$, pentru orice $g \in G$. Prin g^n înțelegem $g * g * \dots * g$, unde semnul $*$ apare de $n - 1$ ori. Prin convenție, $g^0 = e$. Am notat cu e elementul neutru al grupului G și prin $|G|$ cardinalul mulțimii G .

2) Dacă n este un număr natural nenul și a este un număr întreg prim cu n , atunci n divide $a^{\phi(n)} - 1$ (Teoremă lui Euler). Acest rezultat este o consecință a teoremei lui Lagrange.

3) Dacă p este un număr prim și a este un număr întreg care nu se divide cu p , atunci p divide $a^{p-1} - 1$ (Mica Teoremă a lui Fermat). Acest rezultat este un caz particular al teoremei lui Euler.

4) Dacă p este un număr prim, atunci p divide $(p - 1)! + 1$ (teorema lui Wilson).

Exerciții:

1) Care sunt ultimele două cifre ale numărului 37^{79} ? Din teorema lui Euler stim că

$$\overline{37}^{\phi(100)} = \overline{1}$$

în $U(\mathbb{Z}_{100})$. Dar $\phi(100) = 40$ (vezi un calcul anterior). Deducem că $\overline{37}^{79}$ este inversul lui $\overline{37}$ în grupul $(U(\mathbb{Z}_{100}), \cdot)$. Acest invers era $\overline{73}$ (vezi exercițiu anterior). Deducem că ultimele două cifre ale numărului 37^{79} sunt 73.

2) Care este restul împărțirii lui $n = 2^{39} + 3^{39}$ la 41?

Din Mica teoremă a lui Fermat stim că $2^{40} \equiv 3^{40} \equiv 1 \pmod{41}$. Atunci

$$6n \equiv 3 + 2 \equiv 5 \equiv -36 \pmod{41}.$$

Deducem că

$$n \equiv -6 \equiv 35 \pmod{41}.$$

Restul căutat este 35.

3) Care este restul împărțirii lui $n = 38! + 1$ la 41? Din teorema lui Wilson știm că

$$40! \equiv -1 \pmod{41}.$$

Avem că $39 \cdot 40 \cdot n \equiv -1 + 39 \cdot 40 \pmod{41}$. Dar

$$39 \cdot 40 \equiv (-2) \cdot (-1) \equiv 2 \pmod{41}$$

și deci

$$2n \equiv 1 \equiv 42 \pmod{41}.$$

De aici rezultă imediat că $n \equiv 21 \pmod{41}$.

Definiție: Fie $(G, *)$ un grup finit (cu elementul neutru e) și $g \in G$. Se notează cu $\text{ord}(g)$ cel mai mic număr natural nenul k cu proprietatea că $g^k = e$ (se numește ordinul lui g în grupul $(G, *)$). Proprietățile ordinului:

- 1) $g^{\text{ord } g} = e$.
- 2) Dacă $g^k = e$ (unde k este un număr natural), atunci $\text{ord}(g)$ divide k .
- 3) Ordinul lui g divide întotdeauna cardinalul lui G .
- 4) $\text{ord}(g^k) = \frac{\text{ord}(g)}{(\text{ord}(g), k)}$, pentru orice $k \in \mathbb{N}$.
- 5) Dacă $g * h = h * g$, $\text{ord}(g) = n$, $\text{ord}(h) = m$ și $(m, n) = 1$ atunci

$$\text{ord}(g * h) = \text{ord}(g) \cdot \text{ord}(h).$$

Exerciții:

1) Să se calculeze ordinul lui $\bar{52}$ în grupul $(\mathbb{Z}_{100}, +)$. Notăm $k = \text{ord}(\bar{52})$. k este cel mai mic număr natural nenul pentru care $\bar{52}k = \bar{0}$. Deci $k = 25 = \text{ord}(\bar{52})$.

2) Să se calculeze $\text{ord}(\bar{52})$ în grupul $(U(\mathbb{Z}_{59}), \cdot)$. Să notăm cu k acest ordin. Din proprietatea 3) știm că k divide $|U(\mathbb{Z}_{59})| = \phi(59) = 58$. Deci

$$k \in \{1, 2, 29, 58\}.$$

Singurul element de ordin 1 este elementul neutru, deci $k \neq 1$. Avem $\bar{52}^2 = (\bar{-7})^2 = \bar{49} = \bar{-10}$; deci $k \neq 2$. Trebuie să calculăm $\bar{52}^{29}$. Avem

$$\bar{52}^4 = \bar{100} = \bar{-18}, \bar{52}^8 = \bar{324} = \bar{29},$$

$$\bar{52}^{14} = \bar{52}^8 \cdot \bar{52}^4 \cdot \bar{52}^2 = \bar{29} \cdot \bar{(-18)} \cdot \bar{(-10)} = \bar{29} \cdot \bar{3} = \bar{28},$$

$$\bar{52}^{29} = (\bar{52}^{14})^2 \cdot \bar{52} = \bar{28}^2 \cdot \bar{(-7)} = \bar{-7} \cdot \bar{17} = \bar{-1}.$$

Din calculele anterioare deducem că $k \neq 29$; deci $\text{ord}(\bar{52}) = k = 58$.

3) Cum se calculează ordinul unei permutări?

a) se descompune în cicli disjuncți b) se calculează cel mai mic multiplu comun al lungimilor cicilor; acesta este ordinul permutării

a) Scriem $\sigma = \sigma_1 \circ \sigma_2 \circ \dots \circ \sigma_m$, unde $\sigma_j = (a_1, a_2, \dots, a_k)$ este următoarea permutare (a_1, a_2, \dots, a_m) sunt numere naturale distincte din intervalul $\{1, 2, \dots, n\}$):

$$\sigma_j(a_i) = a_{i+1}, \forall i = \overline{1, k-1}, \sigma_j(a_k) = a_1; \sigma_j(x) = x, \forall x \neq a_i.$$

Descompunerea în cicli disjuncți presupune că un număr a_t din ciclul σ_j este diferit de orice număr b_s dintr-un ciclu σ_u , cu $u \neq j$. Ciclul $\sigma_j = (a_1, a_2, \dots, a_k)$ are lungimea k .

b) $ord(\sigma)$ este cel mai mic multiplu comun al lungimilor cicilor disjuncți din descompunerea lui σ .

Exemplu: să se calculeze ordinul permutării $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 4 & 1 & 6 & 7 & 5 \end{pmatrix} \in S_7$.

Găsim descompunerea în cicli disjuncți $\sigma = (1, 2, 3, 4) \circ (5, 6, 7)$.

$$ord(\sigma) = [4, 3] = 12.$$

4) Cum să găsești factori primi ai unui număr mare?

Exemplu: arătați că $65537 = 2^{16} + 1$ este număr prim. Deoarece $[\sqrt{2^{16} + 1}] = 2^8 = 256$, trebuie să arătăm că numărul 65537 nu are factori primi mai mici decât 256. Fie p un număr prim care-l divide pe 65537. Atunci

$$2^{16} \equiv -1 \pmod{p} \quad (1)$$

și

$$2^{32} \equiv 1 \pmod{p}. \quad (2)$$

Notăm cu k ordinul lui $\bar{2}$ în grupul $(U(\mathbb{Z}_p), \cdot)$. Din formula (2) și din proprietatea 2) a ordinului știm că k este un divizor al lui 32. Dacă cumva k divide 16, atunci

$$2^{16} \equiv (2^k)^{\frac{16}{k}} \equiv 1 \pmod{p};$$

am folosit proprietatea 1) a ordinului. Combinând această informație cu formula (1) ajungem la o contradicție:

$$-1 \equiv 2^{16} \equiv 1 \pmod{p}, p = 2.$$

Deci k nu divide 16 și divide 32. Neapărat $k = 32$. Din proprietatea 3) a ordinului știm că $32 = k = ord(\bar{2})$ este un divizor al cardinalului grupului $(U(\mathbb{Z}_p), \cdot)$. Acest număr este $\phi(p) = p - 1$. Am descoperit deci că $p = 1 + 32 \cdot t$, pentru un număr natural t . Inspectând numerele prime $p = 1 + 32 \cdot t < 256$, găsim doar două: $p = 97$ și $p = 193$. Verificăm dacă 65537 se divide cu 97 sau 193:

$$65537 = 97 \cdot 675 + 62, 65537 = 193 \cdot 339 + 110.$$

Din toate argumentele precedente deducem că $65537 = 2^{16} + 1$ este număr prim.

Lucrarea nr. I

1) Găsiți numărul $x \in \{0, 1, 2, \dots, 2020\}$ astfel încât $97 \cdot x \equiv 1 \pmod{2021}$.

- Exerciții
- 2) Găsiți acel număr $x \in \{0, 1, 2, \dots, 428\}$ astfel încât să fie îndeplinite simultan condițiile $x \equiv 2 \pmod{3}$, $x \equiv 2 \pmod{11}$, $x \equiv 8 \pmod{13}$.
 - 3) Câte submulțimi $A \subseteq \{1, 2, 3, 4, 5, 6\}$ au proprietatea că nu conțin "vecini" (adică nu există j natural cu $\{j, j+1\} \subseteq A$)?
 - 4) Decriptați DNSDDDS, criptat cu metoda Vigenère (cu alfabetul standard latin de 26 de litere, ordonate în mod obișnuit); cuvântul cheie are 2 litere.

Lucrarea nr. II

- Înțeles
- 1) Cât este restul împărțirii lui 2^{149} la 323 (formulare echivalentă: criptați litera C folosind RSA cu $n = 323$, $e = 149$ și alfabetul latin standard de 26 de litere)?
 - 2) Calculați restul împărțirii lui $6^{99} + 3^{99} + 2^{99}$ la 101.
 - 3) Fie $(G, *)$ un grup cu 211 elemente. Câte elemente $g \in G$ au proprietatea că $g^3 = e$?

- Merk 4) Fie $\sigma \in S_{36}$ definită prin faptul că $\sigma(x)$ este unicul număr din $\{1, 2, 3, \dots, 36\}$ astfel încât $\sigma(x) \equiv 3x \pmod{37}$. Să se calculeze ordinul permutării σ .

Lucrarea nr. III

- Înțeles
- 1) Să se calculeze $\text{ord}(\bar{2})$ în grupul $(U(\mathbb{Z}_{47}), \cdot)$.
 - 2) Găsiți $a \in \{1, 2, 3, \dots, 22\}$ cu proprietatea că $\text{ord}(\bar{a}) = 22$ în grupul $(U(\mathbb{Z}_{23}), \cdot)$.
 - 3) Care este cel mai mic factor prim al numărului $2^{24} + 1$?
 - 4) Găsiți cel mai mare ordin al unei permutări din S_{12} .

Lucrarea nr. IV

- Construcție 1) Rezolvați ecuația $\sigma^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 3 & 4 & 1 & 6 & 7 & 8 & 9 & 5 \end{pmatrix}$, în S_9 .

$$\text{ord}\sigma = 20$$

$$\text{ord}\sigma = 20 \Rightarrow \text{ord}\sigma = [15] = 20$$

- Merk 2) Găsiți $x \in \{1, 2, 3, \dots, 58\}$ astfel încât $2^x \equiv 29 \pmod{59}$.

- 3) Să se calculeze cardinalul mulțimii $A = \{x \in \mathbb{N} | x \leq 200, (x, 30) = 1\}$.

$$(2^2)^{10} = 20$$

- 4) Câte submulțimi $A \subseteq \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ au proprietatea că nu conțin "vecini" (adică nu există j natural cu $\{j, j+1\} \subseteq A$)?

Probleme de aritmética și teoreme numeroase. Iată ajutorul de
rezolvare - I. Parțială pol, Alexandru Stro

Complemente de aritmética și teoreme elementare a numerelor - Autor: Bogdan
Dănilă?

① $p > 3$ este prim. Să rezolvă $7^p - 6^p \equiv 63$

(+) și prim $p > 3$ $6n+1, 6n+5$

$$\text{dcl } p = 6n+1 \Rightarrow \text{modul } 63 \rightarrow 7^p - 7^{6n} \equiv 7^{6n} - 7^{6n} \equiv 7(63+6) \stackrel{3n}{\equiv}$$

$$7 \cdot 6^{3n} - 7 \cdot 216^n \equiv 7(63 \cdot 5 + 1)^n \equiv 7 \cdot 1 \equiv 6 \cdot 6^n \equiv 6 \cdot 216^{2n} \equiv 6 \cdot (5 \cdot 37)^{2n} \equiv$$

$$\equiv 6 \pmod{63} \Rightarrow 7^p - 6^p \equiv 6 - 1 \equiv 0 \pmod{63}$$

$$\text{dcl } p = 6n+5 \Rightarrow 7^{6n} \equiv 1 \pmod{63} \text{ și } 6^n \equiv 1 \pmod{63}$$

$$7^{6n+5} - 6^{6n+5} \equiv 7^5 - 6^5 \equiv 1 \pmod{63}$$

Altă metodă

$$\text{dcl } (m, n) = 1 \Rightarrow a \equiv b \pmod{m} \Leftrightarrow an \equiv bn \pmod{m}$$

$$\Rightarrow 7^5 - 6^5 \equiv 0 \pmod{63} \Leftrightarrow 42(7^5 - 6^5) \equiv 0 \pmod{63}$$

$$7^6 \equiv 6^6 \equiv 1 \pmod{63} \Leftrightarrow 6 - 7 \equiv 0 \pmod{63} \text{ - evident}$$

galelini numărul 1010 ; fronte 1010

zoom bătrânește 1010 galelini ; fronte 1010
univac → 1010 CNP 10-10-1973

Şifra foto bătrânește 1010 → 445x531f8fc22k2
wA5wF9

rezolvare bătrânește 1010 galelini numărul
1010 galelini numărul

ord off numărul 1010!

nupe bătrânește curthelius

id 892469 fronte 1010

Megawie 072397623 numărul 1010
galelini dyhovac

curthelius bătrânește

galelini

curthelius

curthelius

numărul 1010

of sh ok2 numărul 1010!

Facebook galelini dyhovac numărul 1239

ale galelini dyhovac fronte 1010

eng-galelini dyhovac curthelius

louis n-n - fronte

Algebră I

GIC

restanță 5.09.2021

info ✓

1) Găsiți $x \in \{0, 1, 2, 3, \dots, 106\}$ astfel încât $17x \equiv 1 \pmod{107}$. ✓

Consult ✓ 2) Găsiți $x \in \{0, 1, 2, 3, \dots, 104\}$ astfel încât (simultan) $x \equiv 1 \pmod{3}$, $x \equiv 3 \pmod{5}$, $x \equiv 5 \pmod{7}$.

Consult ✓ 3) Fie $\sigma \in S_{46}$ permutarea definită astfel: $\sigma(n)$ este restul împărțirii lui $2n$ la 47, pentru orice $n \in \{1, 2, 3, \dots, 46\}$. Să se calculeze ordinul permutării σ .

Info 4) Fie $\sigma \in S_{46}$ permutarea definită astfel: $\sigma(n)$ este restul împărțirii lui n^3 la 47, pentru orice $n \in \{1, 2, 3, \dots, 46\}$. Să se calculeze signatura permutării σ .

Info 5) Să se arate că numărul $739 \cdot 2^{102} + 1$ nu este prim.

Notă: 1) Trebuie să trimiteți lucrările până la ora 20 la adresele: alexgica@yahoo.com și alexandru.gica@unibuc.ro

2) Pentru a trece examenul cu nota 5 trebuie să rezolvați corect una dintre primele trei probleme. Dacă rezolvați mai multe probleme dintre primele 3 nu primiți o notă mai mare. Pentru o notă mai mare, trebuie să rezolvați una din problemele 4 și 5.

3) Veți primi notele astăzi. Dacă aveți neclarități privind nota primită, trebuie să-mi comunicați acest lucru în 24 de ore pentru a discuta eventualele nelămuriri.

Algebră ID

Gica

6 iunie 2021

1) a) Calculați inversul lui $\bar{8}$ în grupul $(\mathbb{Z}_{100}, +)$. ✓

b) Calculați inversul lui $\bar{8}$ în grupul $(U(\mathbb{Z}_{103}), \cdot)$.

c) Calculați inversa permutării $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 2 & 5 & 1 & 4 \end{pmatrix}$ din grupul (S_6, \circ) . ✓

2) a) Calculați ordinul lui $\bar{8}$ în grupul $(\mathbb{Z}_{100}, +)$. ✓

b) Calculați ordinul lui $\bar{8}$ în grupul $(U(\mathbb{Z}_{103}), \cdot)$. ✓

c) Calculați ordinul permutării $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 2 & 5 & 1 & 4 \end{pmatrix}$ în grupul (S_6, \circ) .

3) a) Care este restul împărțirii lui $75!$ la 79 ?

b) Pentru ce numere prime p avem $4^{p-2} + 3^{p-2} + 2^{p-2} \equiv 57 \pmod{p}$?

c) Să se găsească un factor prim al numărului $2^{83} - 1$.

4) a) Există o funcție bijectivă $f : U(\mathbb{Z}_{103}) \rightarrow \mathbb{Z}_{102}$ cu proprietatea că $f(\hat{x} \cdot \hat{y}) = f(\hat{x}) + f(\hat{y})$, pentru orice \hat{x}, \hat{y} din $U(\mathbb{Z}_{103})$?

b) Există o funcție bijectivă $f : U(\mathbb{Z}_{100}) \rightarrow \mathbb{Z}_{40}$ cu proprietatea că $f(\hat{x} \cdot \hat{y}) = f(\hat{x}) + f(\hat{y})$, pentru orice \hat{x}, \hat{y} din $U(\mathbb{Z}_{100})$?

Notă: Rezolvările trebuie trimise până la ora 10.15 la adresele alexgica@yahoo.com și alexandru.gica@unibuc.ro

Dacă aveți nelămuriri în privința subiectelor, îmi puteți trimite întrebări pe adresa alexgica@yahoo.com până la ora 8.15.

Veți primi rezultatele cel târziu mâine. Cei care doresc să conteste nota, trebuie să-și declare această intenție până mâine, ora 20. Pentru aceste persoane, voi iniția o sesiune Zoom, mâine, ora 20.

Algebră II

Gra

1 septembrie 2020

b) 1) Care este inversul lui $\bar{17}$ în corpul \mathbb{Z}_{19} ? (găsiți \bar{x} astfel încât $\bar{x} \cdot \bar{17} = \bar{1}$ în corpul \mathbb{Z}_{19}) ✓

- A) 7 B) 8 C) 9 D) 10

2) Care este valoarea determinantului matricii $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 4 \\ -1 & 0 & 1 \end{pmatrix}$? verso

- A) -1 B) 0 C) 1 D) 2

3) Fie x, y numere reale care satisfac simultan ecuațiile $3x+4y=10$ și $8x+11y=27$.

Valoarea lui $x+y$ este

- A) 7 B) 6 C) 4 D) 3

verso

4) Câte rădăcini reale are ecuația $x^{2020}=1$?

- A) 2 B) 4 C) 0 D) 2020

5) Pentru câte valori $n \in \{0, 1, 2, \dots, 41\}$ are loc congruența $2^n \equiv 21 \pmod{43}$?

Dacă p este un număr prim impar, câte soluții $n \in \{0, 1, 2, \dots, p-2\}$ are ecuația $2^n \equiv 1 \pmod{p}$?

6) Fie $A, B \in M_2(\mathbb{Z})$ (matrici cu două linii și două coloane, cu coeficienți întregi) astfel încât $A, A+B, A+2B, A+3B, A+4B$ sunt inversabile în inelul $M_2(\mathbb{Z})$. Să se arate că și $A+5B$ este inversabilă.

Observații: 1) Fotografiati sau scanati rezolvările. Soluțiile vor fi transmise prin e-mail la adresele alexgica@yahoo.com și alexandru.gica@unibuc.ro până cel mai târziu la ora 11.15

2) Veți primi astăzi notele prin e-mail. Contestațiile se rezolvă tot astăzi. Voi iniția o sesiune Zoom în acest scop (în caz că este nevoie).

3) Primiți un punct din oficiu. Nu trebuie să mai scrieți enunțurile problemelor. La problemele din testul grilă (primele patru), transmiteți doar numărul problemei și litera corespunzătoare răspunsului pe care îl considerați corect. Doar una dintre cele patru variante de răspuns este corectă. Dacă răspundeți corect la o problemă din testul grilă, primiți un punct. În caz contrar primiți 0 puncte.

4) Problema 5 se punctează cu 2 puncte iar problema 6 cu 3 puncte. Aceste două probleme necesită redactarea amănunțită a demonstrațiilor.

$$\textcircled{3} \quad \left\{ \begin{array}{l} 3x+4y=10 \\ 8x+11y=27 \end{array} \right| \cdot 8 \quad \left| \cdot 3 \right.$$

$$\left\{ \begin{array}{l} 27x+32y=80 \\ 27x+33y=27 \end{array} \right. \quad \textcircled{4}$$

$$T \quad y = 81 - 80$$

$$\boxed{y=1} \Rightarrow 3x + 4 = 10$$

$$\Rightarrow 3x = 6$$

$$\boxed{x=2}$$

$$\Rightarrow \boxed{x+y=3}$$

$$\textcircled{2} \quad \left| \begin{array}{ccc|c} 1 & 2 & 3 & 1 \\ 2 & 3 & 4 & 0 \\ 1 & 0 & 1 & 1 \end{array} \right| \quad 23 - 0 - 8 + 9 - 0 - 4 = -5 + 5 = 0$$

(B)

$$\textcircled{1} \quad \overline{x-14} \equiv 1 \pmod{19}$$

$$\overline{x-(-2)} \equiv 1$$

~~x~~

$$\begin{aligned} 1: 19 &\equiv 1 + 17 \pmod{2} \\ 2: 17 &\equiv 2 + 15 \pmod{2} \\ 3: 15 &\equiv 1 \cdot 15 \pmod{2} \end{aligned}$$

$$\frac{15}{17} \equiv 1 + \frac{1}{8} \pmod{\frac{9}{8}}$$

$$\frac{19}{17} - \frac{9}{8} \equiv \frac{(-1)^3}{17+8} =$$

$$19 \cdot 8 - 17 \cdot 9$$

$$152 - 153 \equiv -1 \pmod{19}$$

According to
 $-17 \cdot 9 \equiv -1 \pmod{19}$

$$17 \cdot 9 \equiv 1 \pmod{19}$$

$$\Rightarrow \text{Residual mod 9}$$

$$\boxed{x \equiv 9 \pmod{19}}$$

SUBSTITUITE EXAMEN - IRINA

-1-

Indre

Exercitii 5.9.21

$$\text{Se stă } x \in \{9, 12, 3, 1, 106\} \text{ și } 17x \equiv 1 \pmod{107}$$

~~$17 \cdot x = 1 \pmod{107}$~~

$$\text{① } 17x \equiv 1 \pmod{107}$$

~~$17x \equiv 1 \pmod{107}$~~

~~$5 \equiv 102 \cdot x \equiv 6 \pmod{107}$~~

~~$17x \equiv 1 \pmod{107}$~~

$$\begin{array}{l} \text{Soluție: } \\ 12x \equiv 19 \pmod{107} \end{array}$$

$$1 = 108 \cdot x \equiv 63 \pmod{107}$$

$$\boxed{x = 63}$$

~~$\text{Dacă: } 107 : 17 = 6 \quad 107 : 17 = 17 \cdot 6 + 5$~~

~~$17 : 5 = 3 \quad 17 : 5 = 5 \cdot 3 + 2$~~

~~$5 : 2 = 2 \quad 5 : 2 = 2 \cdot 2 + 1$~~

~~$2 : 1 = 2 \quad 2 : 1 = 1 \cdot 2 + 0$~~

$$\frac{b}{a} = 6 + \frac{1}{3 + \frac{1}{2}} = 6 + \frac{2}{7} = \frac{45}{7}$$

$$\frac{107}{17} - \frac{45}{7} = \frac{(-1)^5}{17 \cdot 7} \Leftrightarrow 107 \cdot 7 - 45 \cdot 17 = 1$$

$$17 \cdot (-5) = 1$$

$$\text{De unde } (-5) \cdot 17 = 1 \Rightarrow$$

$$\text{② } \begin{cases} x \equiv 1 \pmod{3} \\ x \equiv 3 \pmod{5} \\ x \equiv 5 \pmod{7} \end{cases} \Rightarrow 3|x-1 \Rightarrow x \in \{4, 7, 10, 13, 16, 19, 23, 26, 28, 31\}$$

Soluție

~~$x = 3a + 1 = 5n + 3$~~

$$5a = -2 \pmod{3}$$

$$2a = -2$$

$$a = -1 \equiv 2 \pmod{3}$$

$$x = 5 \cdot 2 + 3 = 13$$

$$\begin{cases} x \equiv 13 \pmod{15} \\ x \equiv 5 \pmod{7} \end{cases}$$

$$\Rightarrow x = 15a + 13 = 15a + 5 \pmod{7}$$

$$\begin{cases} x \equiv 13 \pmod{15} \\ x \equiv 5 \pmod{7} \end{cases} \quad 15|x-13 \Rightarrow$$

$$x \in \{28, 43, 58, 73, 88, 103, \dots\}$$

$$\boxed{x = 103} \quad 15 \mid 103 \quad 30 \mid 103 \quad 103 \equiv 5 \pmod{7}$$

$$108 : 3 = 36 \quad \checkmark$$

$$\begin{array}{r} 9 \\ 12 \\ \hline 0 \end{array}$$

$$\begin{array}{r} 103 \\ 12 \\ \hline 0 \end{array}$$

$$\begin{array}{r} 103 \\ 12 \\ \hline 0 \end{array}$$

$$x = 15 \cdot 6 + 13 = 103 \Rightarrow \boxed{x = 103} \quad \checkmark$$

$$a = -1 \equiv 6 \pmod{7}$$

$$x = 15 \cdot 6 + 13 = 103 \Rightarrow \boxed{x = 103} \quad \checkmark$$

④ $T(n)$ restet n mit $\underline{\underline{n^3}}$ und $\underline{\underline{64}}$

$$n^3 = 1, 2^3 = 8, 3^3 = 27, 4^3 = 64, 5^3 = 125, 6^3 = 216$$

$$8^3 = 512, 9^3 = 729, 10^3 = 1000, 11^3 = 1331, 12^3 = 1728$$

$$31^3 = 29512$$

$$33^3 = 35937$$

$$T(n) = \underbrace{(1)}_1 \circ \underbrace{(2, 8, 16, 27, 13, 18, 5, 17, 28, 21)}_{11} \circ \underbrace{(3, 27, 35, 33, 13, 36, 32, 9, 25, 6, 28)}_{11}$$

$$\text{ord}(T(n)) = [1, 11] = 11$$

⑤ $739 \cdot 2^{102} + 1$ mit p-film

p-film

$739 \rightarrow$ p-film

$$\begin{aligned} 2^0 &= 1 \\ 2^1 &= 2 \\ 2^2 &= 4 \\ 2^3 &= 8 \\ 2^4 &= 16 \\ 2^5 &= 32 \\ 2^6 &= 64 \end{aligned}$$

5

$$\frac{102}{5} = 20 \text{ r } 2$$

ultimo cifra 2^{102} este 4.

$$\text{ultimo cifra } 739 \cdot 2^{102} + 1 = 9 \cdot 4 + 1 = 6 + 1 = 7, \text{ neg. le}$$

prime: 1
neg. prime: 3
neg. digit: 7
digit: 9

$p = 73$

$p = 73$

$$2 \mid 739 \cdot 2^{102} + 1 ?$$

$$p = 2t + 1$$

$$739 \cdot 2^{102} \equiv 9 \cdot 8 + 1 = 73 \rightarrow$$

$$73 \mid 73 \Rightarrow 73 \mid 739 \cdot 2^{102} + 1$$

Ex. Sommer 2024

$$\textcircled{1} \text{ a) } \overline{8} + \overline{x} = \overline{0} (\mathbb{Z}_{100}, +) \Rightarrow \overline{x} = \overline{100 - 8} = \overline{92}$$

$$\text{b) } \overline{8} \cdot \overline{x} = \overline{1} (\mathbb{U}(\mathbb{Z}_{103}), \cdot) \quad , \quad \overline{8} = \cancel{\overline{8}}$$

$$\overline{8} \cdot \overline{x} = \overline{1} \cdot \overline{13}$$

$$\overline{102} \cdot \overline{x} = \overline{13} \Rightarrow \boxed{x=13}$$

II

verif: 13:

$$\frac{8}{103} \equiv 1 \pmod{103}$$

$$\textcircled{2} \text{ a) } \sigma_2 \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 2 & 5 & 1 & 4 \end{pmatrix} \Rightarrow \sigma^{-1} = \begin{pmatrix} 3 & 6 & 2 & 5 & 1 & 4 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} =$$

$$\textcircled{2} \text{ b) } z = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 1 & 6 & 4 & 2 \end{pmatrix}$$

$$\textcircled{2} \text{ c) } \text{ord } \overline{8} \text{ in } (\mathbb{Z}_{100}, +)$$

$$\overline{8k} = \overline{0} = 100 \cdot 2 \Rightarrow 100 | 8k \Leftrightarrow 25 | 2k \Rightarrow k=25$$

$$\overline{8 \cdot 25} = \overline{200} \checkmark$$

$$\text{d) } \text{ord } \overline{8} \text{ in } (\mathbb{U}(\mathbb{Z}_{103}), \cdot)$$

$$d = \text{ord } \overline{8} \quad 102 = 2 \cdot 3 \cdot 17$$

$$\varphi(103) = 102 \quad \Rightarrow d | 102 \Rightarrow d \in \{1, 2, 3, 6, 17, 34, 51, 102\}$$

$$8^2 \neq 1 \Rightarrow 64$$

$$8^3 = 512 \equiv 100 \pmod{103}$$

$$8^6 = 8^{3 \cdot 2} = (100)^2 \equiv 9 \pmod{103}$$

$$8^8 = 8^{6 \cdot 3} = 9^3 = 8 \Rightarrow 729$$

$$8^{17} = 8^{13} \cdot 8^4 = 8^{18} \cdot 8^{-1} = 8^{18} \cdot 13 \equiv 8 \cdot 13 = 104 \equiv 1 \pmod{103} \Rightarrow$$

$$\Rightarrow \boxed{\text{ord } \overline{8} = 17}$$

deler(17)

$$\begin{array}{r} 512 \mid 103 \\ 515 \mid 5 \\ \hline 3 \end{array}$$

$$\begin{array}{r} 729 \mid 103 \\ 721 \mid 7 \\ \hline 2 \end{array}$$

$$\text{P) } \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 2 & 5 & 1 & 4 \end{pmatrix} \text{ Ad } J = ?$$

$$J = (1, 3, 2, 6, 4, 5) \Rightarrow \text{longime 6} \Rightarrow \underline{\text{Ad } J = 6}$$

(3) a) nicht invertierbar bei $J! \cdot 6 \neq 1$

$$79\text{-prim} \xrightarrow{\text{T. Wilson}} 78! \equiv -1 \pmod{79}$$

$$78 \cdot 77 \cdot 76 \cdot 75 \equiv -1 + 78 \cdot 77 \cdot 76 \pmod{79}$$

$$= -1 = -2 = -3 \quad = -1 = -2 = -3$$

$$-6 \cdot 75! = -1 - 6 = -7 \equiv 72 \pmod{79} \quad \begin{matrix} 79 \\ (6, 79) = 1 \end{matrix} \Rightarrow 75! \equiv -12 \equiv 67 \pmod{79}$$

b) p ist reelle Zahl mit p auen $4p^2 + 3p^2 + 2p^2 \equiv 57 \pmod{p}$?

$$\left. \begin{array}{l} p \text{-prim} \\ (7, p) = 1 \\ (3, p) = 1 \\ (2, p) = 1 \end{array} \right\} \begin{array}{l} \text{MTF} \\ \text{MTF Fehler} \\ \text{auen} \\ \text{faktur} \end{array} \left. \begin{array}{l} 4p^{-1} \equiv 1 \pmod{p} \\ 3p^{-1} \equiv 1 \pmod{p} \\ 2p^{-1} \equiv 1 \pmod{p} \end{array} \right.$$

$$4p^{-2} + 3p^{-2} + 2p^{-2} \equiv 57 \pmod{p} \quad | \cdot 4 \cdot 3 \cdot 2$$

$$4p^{-1} \cdot 6 + 3p^{-1} \cdot 8 + 2p^{-1} \cdot 12 \equiv 57 \cdot 4 \cdot 3 \cdot 2 \stackrel{B68}{=} 1368 \pmod{p}$$

$$26 \cdot 6 + 8 + 12 \equiv 1368 \pmod{p} \Rightarrow p \mid 1368 - 26 = 1342 \Rightarrow$$

$$\Rightarrow p \in \{2, 11, 61\}$$

~~13422/11461~~

auskl p \in \{2, 3, 7\} \Rightarrow

meine prim

$$\Rightarrow p = 2 \Rightarrow 1^0 + 3^0 + 2^0 = 3 \equiv 57 \pmod{2} \Leftrightarrow 2 \mid 57 - 3 = 54 \vee$$

$$p = 3 \Rightarrow 1^1 + 3^1 + 2^1 = 9 \equiv 57 \pmod{3} \Leftrightarrow 3 \mid 57 - 9 = 48 \vee$$

-3-

c) factor prim p in $2^{83}-1$

$$\text{Se } p \mid 2^{83}-1 \Rightarrow 2^{83} \equiv 1 \pmod{p}$$

prim

$\text{ord } 2 = 83$, weil 83 e prim $\Rightarrow \text{ord } 2 \in \{1, 83\}$

$$\text{ord } 2 \mid |\mathbb{U}(\mathbb{Z}_p)| = p-1 \Rightarrow p = 1 + 83 \cdot t$$

$$p \in \{1, 83, 167, 200, \dots\}$$

$$p = 167 \Rightarrow \text{prim} : 2^{83} \equiv 1 \pmod{167} \quad \checkmark$$

$$\textcircled{3} \text{ a) } 75! \equiv x \pmod{79} \Leftrightarrow 75! - x \equiv 0 \pmod{79}$$

$$\text{Wilson: } (p-1)! \equiv -1 \pmod{p}$$

$$78! \equiv -1 \pmod{79}$$

$$78! = \underbrace{78}_{z=1} \cdot \underbrace{77}_{z=2} \cdot \underbrace{76}_{z=3} \cdot \underbrace{75}_{z=4} \equiv -1 \pmod{79} \Rightarrow \underbrace{(-6)}_{78} \cdot \underbrace{75!}_{79} \equiv -1 \pmod{79}$$

$$\Rightarrow \text{durchsetzen in } \overline{73} \text{ in } \mathbb{U}(\mathbb{Z}_{79}), \cdot \rightarrow \overline{13}$$

$$\begin{aligned} (6, 79) &= 1 \\ (73, 79) &= 1 \quad \text{Separate complete} \end{aligned}$$

$$1: 79 : 73 = \boxed{1} \text{ r } 6$$

$$1 + \frac{1}{12} = \frac{13}{12}$$

$$2: 73 : 6 = \boxed{12} \text{ r } 1$$

$$\frac{79}{73} = \frac{13}{12} \underset{73 \cdot 12}{=} \frac{(-1)^3}{13 \cdot 12} \quad \checkmark$$

$$3: 12 : 2 = \boxed{6} \text{ r } 0$$

$$\overline{73} \cdot \overline{13} = \overline{1} \Rightarrow \overline{73}^{-1} = \overline{13}$$

$$\Rightarrow \overline{73} \cdot \overline{13} \cdot \overline{75!} \equiv \overline{-1 \cdot 13} \Rightarrow \overline{75!} \equiv \overline{-13} = 66 \pmod{79}$$

103 \rightarrow Lösung; Rechnungen

(2) Since $\alpha \in \mathbb{Z}_{23} - \{-22\}$ and $\text{ord} \bar{\alpha} = 22$ in $\mathbb{U}(\mathbb{Z}_{23})$

$\alpha \in \mathbb{Z}_{23}, -22$

$\text{ord} \bar{\alpha} = 22 \Rightarrow \bar{\alpha}^{22} = 1$ in $\mathbb{U}(\mathbb{Z}_{23})$

$\text{ord}(\bar{\alpha}) \mid \text{ord } \mathbb{U}(\mathbb{Z}_{23}) = \varphi(23) \Rightarrow \text{ord}(\bar{\alpha})^{2^k} \in \{1, 2, 11, 22\}$
23 prime

$1^k \equiv 1 \pmod{23}$

$2^k \not\equiv 1 \pmod{23}$

$2^2 \equiv 4 \not\equiv 1 \pmod{23}$

$2^{11} = 2048 \equiv 1 \pmod{23} \Rightarrow \text{ord} 2 = 11$

Observe $-2 \equiv +\bar{2} \pmod{23}$ & $(-2)^{11} = 2^{11} = -1 \pmod{23}$

verifying that $k < 11$ & $\bar{\alpha} = -\bar{2} = \bar{2}^{-1}$

$-2^1 \equiv -2 \not\equiv 1 \pmod{23}$

$-2^2 \equiv 4 \not\equiv 1 \pmod{23}$

$-2^{11} \equiv -1 \not\equiv 1 \pmod{23}$

$(-2)^{11} = 2^{22} \equiv (-1)^2 = 1 \pmod{23} \Rightarrow \text{ord } \bar{2} = 22$

After multiplying: 5, 7, 10, 11, 13, 15, 17, 19, 20, 21

Considereaza SAI

-1-

2) $x \in \{50, 53, 56, 59, 62, 65\}$ astfel încât $x \equiv 1 \pmod{3}$, $x \not\equiv 3 \pmod{5}$ și $x \not\equiv 5 \pmod{7}$

$$\begin{cases} x \equiv 1 \pmod{3} \\ x \equiv 3 \pmod{5} \\ x \equiv 5 \pmod{7} \end{cases}$$

3, 8, 13

$$x \equiv 13 + 15t \equiv 5 + 7s \pmod{7}$$

$$13 + 1 \cdot t \equiv 5 + 0 \Rightarrow t \equiv -8 \equiv 6 \pmod{7} \quad t = 7a + 6$$

$$\begin{cases} 103 = x = 13 + 15t = 13 + 15(7a + 6) = 105a + \boxed{13 + 15 \cdot 6} \\ x \equiv 1(3) \\ x \equiv 3(5) \end{cases} \Rightarrow 15t + 13 \Rightarrow x \equiv 13 \pmod{103}$$

103

(5) Pe carelelori $\{50, 51, \dots, 59\}$ sunt loc congruenta $2^n \equiv 21$
 $\pmod{43}$?

1) $\text{ord}_2 2 \in \langle U(\mathbb{Z}_{43}) \rangle$

$$d | 42 \quad d \in \{1, 2, 3, 6, 7, 14, 21, 42\}$$

$$2^2 \not\equiv 1 \pmod{43}$$

$$2^3 \not\equiv 1 \pmod{43}$$

$$43 | 2^6 - 1 = 63$$

$$2^7 \equiv 128 \equiv -1 \pmod{43}$$

$$129 \equiv 3 \cdot 43$$

$$2^{15} \equiv (2^7)^2 \equiv 1 \pmod{43}$$

$$\frac{14}{2} = 7$$

$$2^n \equiv 21 \equiv 2^6 \pmod{43}$$

$$2^{n-6} \equiv 1 \pmod{43}$$

Prop. ord₂(2) $\rightarrow g^n = e \Rightarrow \text{ord } g | n$

$$14 = \text{ord } 2 | n-6 \Rightarrow 14 | n-6$$

$$\begin{array}{c|cc} 128 & 43 \\ 125 & 3 \\ \hline 2 & -1 \end{array}$$

$$2^7 \equiv 42 \pmod{43} \quad | :2$$

$$2^6 \equiv 21 \pmod{43},$$

$$\begin{array}{c} \text{me}\{6, 20, 35\} \\ \text{adm}(43) \end{array} \rightarrow 3 \text{ soluții} \quad \boxed{\boxed{}}$$

6+15

b) Dacă p este prim impar, cuțit $m \in \mathbb{N} \setminus \{0, 1\} \rightarrow p-2$, au proprietatea
 $\forall 2^m \equiv 1 \pmod{p}$

$$2^m \equiv 1 \pmod{p}$$

$d = \text{ord } 2 \text{ în } U(\mathbb{Z}_p)$ $\Rightarrow d \mid p-1 \quad p-1 = d \cdot k$
 Proprietatea 2: $\text{ord } 2 \mid m$

Numelele $0, d, 2d, \dots, (k-1)d$
 care se
 dividă
 cu d sunt
 $\frac{d}{n}$

$$K = \frac{p-1}{d} \quad | \quad d = \text{ord } 2$$

Lucrare Exercițiu 1
 Permutare din locuri de curs.

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 3 & 1 & 6 & 7 & 8 & 9 & 5 & 4 \end{pmatrix} \stackrel{\text{m.sg}}{=} (1, 2, 3, 5, 6, 7, 8, 9)$$

signatura $\text{sgn} = -1$

$$\sum (\sigma) = (-1)^{\text{nr inversions}}$$

$(i, j) \in S_{1, 2, \dots, n}, \quad \sigma \in S_n.$
 $i, j \in S_{1, 2, \dots, n}, \quad \sigma \in S_n.$

$$\sum (\sigma \circ \tau) = \sum (\sigma) \cdot \sum (\tau)$$

$$\sum (\sigma^2) = (-1)^{\text{nr inversions}} \quad \text{Contradicție că nu este } \sigma^2.$$

$$\sum (\sigma)^2 = (-1)^{\text{nr inversions}} = (-1)^0 = 1$$

Inversori $(1, 2) - 1$
 $(2, 3) - 1$
 $(3, 4) - 1$
 $(5, 9) - 1$
 $(6, 9) - 1$
 $(7, 9) - 1$
 $(8, 9) - 1$

+ inversori

Cum calculă poziția unei permutări

$\sigma \in S_n$

$\sigma = \text{produs de cicluri disjuncte} = \sigma_1 \sigma_2 \dots \sigma_r$
 cicluri
 de
 comută

-2-

$$\Gamma^2 = \overline{z_1}^2 \overline{z_2}^2 \dots \overline{z_k}^2$$

Calculăm potențialul unui ciclu.

$$(a_1, a_2, \dots, a_k)^2 = (a_1, a_3, a_5, a_7, \dots)$$

$$(a_1, a_2) \rightarrow a_k \circ (a_1, a_2, \dots, a_k)$$

Lemătoare - ciclu de lungime după
potențial.

$$|C_{\text{cic}}| = k = \text{lung} \approx 2n+1$$

$$(a_1, a_2, \dots, a_k)^2 = (a_1, a_3, a_5, a_7, \dots, a_{2n+1}, a_2, a_4, a_6, \dots, a_{2n})$$

$\boxed{k=2n+1}$ ciclu

$$|C_{\text{cic}}| = k = 2n = \text{lung} \approx$$

$$(a_1, \dots, a_k)^2 = (a_1, a_3, \dots, a_{2n-1})(a_2, a_4, a_6, \dots, a_{2n})$$

Produs de cicluri diferențiale, ceea ce înseamnă:

- 2 cicluri diferențiale $\approx 1/2$ de

$$\text{Exercițiul } 3) \quad \Gamma \in S_{46} \quad m \in \{1, 2, \dots, 46\}$$

$\Gamma(m)$ este reședința imparitatei lui m din Γ . Se calculează permutarea

$$\Gamma = (1, 2, 7, 8, 16, 32, 64, 17, 2, 17, 2, 21, 42, 37, 74, 14, 28, 9, 18, 36, 25, 32^2, 64, 47, 17) \quad \text{criteriu initial}$$

$$32^2 = 64 : 47 = \text{restul } 17$$

$$\begin{array}{ccccccccc} 68 & - & 84 & - & 74 & - & 56 & - & 72 \\ \cancel{47} & & \cancel{47} & & \cancel{47} & & \cancel{47} & & \cancel{47} \\ \cancel{21} & \cancel{9} & \cancel{2} & \cancel{37} & \cancel{22} & \cancel{7} & \cancel{37} & \cancel{22} & \cancel{11} \\ 56, 6, 12, 27 \end{array}$$

$$\cancel{47} : 2 = 23$$

$$\text{Exercițiul } 3) \quad \text{Ce lungime are acest } \Gamma? \quad 46 : 2 = \underline{\underline{23}} \text{ fără r.m. } U(\Gamma_{47})$$

$$(5, 10, \dots, 23) \rightarrow \text{lungime } 23$$

cicluri care nu se intersectează → tot 23 elemente.

$$\sqrt[4]{2^k} = 5$$

$\sqrt[4]{(k=23)}$
Produs de 2 cicluri de acces, lungime.

$$\Sigma(\Gamma) = \Sigma(z_1) \cdot \Sigma(z_2) = 1$$

$$\boxed{\text{sign}(a_1, a_2, \dots, a_k) = (-1)^{k-1}}$$

Ex. 7) a) $\tilde{U}(\mathbb{Z}_{103}) \xrightarrow{\sim} (\mathbb{Z}_{102}, +)$ ad. $f(x \cdot y) = f(x) + f(y)$
 Aproape există f bijectorie $\forall x, y \in \tilde{U}(\mathbb{Z}_{103})$

T: Dacă p prim $\Rightarrow \exists q \in S(p) \rightarrow p-1$ ad. și $\bar{a} = p-1$
 în $\tilde{U}(\mathbb{Z}_p)$ —

$$\frac{\tilde{U}(\mathbb{Z}_{103})}{\text{ord } 102}.$$

$$\uparrow \bar{a}, \sim, \bar{x}^{101}$$

$$f(\bar{a} \bar{j}) = \bar{j} \text{ acesta e izomorfism}$$

b) $\exists f: \tilde{U}(\mathbb{Z}_{100}) \xrightarrow{\sim} (\mathbb{Z}_{100}, +)$ ad. $f(x \cdot y) = f(x) + f(y)$
 f bijectorie. $\forall x, y \in \tilde{U}(\mathbb{Z}_{100})$

$$\mid \tilde{U}(\mathbb{Z}_{100}) \mid \geq 100 \text{ un element de ordin } 100$$

ordinul

$$\forall x \in \tilde{U}(\mathbb{Z}_{100}) \rightarrow \overbrace{x^{20}}^{\text{un element de ordin } 5} = 1$$

$$(x, 100) = 1 \quad 100 \mid x^{20} - 1$$

$$(x \text{ prim cu } 100) \quad 100 = 5 \cdot 25$$

$$5 \mid x^{20} - 1$$

$$x \text{ impar} \rightarrow x = 2t+1$$

$$x^2 = 4t^2 + 4t + 1 \equiv 1 \pmod{5}$$

$$(x, 25) = 1$$

$$x^{20} \equiv 1 \pmod{5}$$

$$x^{4(25)} \equiv 1 \pmod{25}$$

$$\varphi(25) = 25 \left(1 - \frac{1}{5}\right) = 20 \rightarrow 20 \mid x^{20} - 1$$

$$\Rightarrow \boxed{100 \mid x^{20} - 1}$$

$$\overbrace{1 + \dots + 1}^{20} = 20 \neq 0 \rightarrow \text{nu sunt izomorfe}$$

$$\text{Rp. 62 (3) f}$$

f surjetiva $\Rightarrow \exists \hat{x} \in U(\mathbb{Z}_{100})$ a.s. $f(\hat{x}) = I$

calcultem $f(\hat{x}^{20}) = f(\hat{x}) + f(\hat{x}) + \dots + f(\hat{x}) = \underbrace{[20]}_{\text{de } 20 \text{ add}} = f(I) = \overline{0}$

$$\hat{x} = \hat{y} = \hat{1}$$

$$f(\hat{1}) = f(1) + f(\hat{1}) \Rightarrow f(\hat{1}) = 0$$

$f: G_1 \rightarrow G_2$, f bijectivo

$$f(x+y) = f(x) + f(y).$$

$$\frac{1}{20}/20 \neq 0$$

contradictio,

contradiction

2.2.4 Wohin vermittet diese
 $\Gamma(36) \rightarrow$ der untere rechte Teil von $S_{42} \cong 36$ ist $\Gamma(x) \equiv 3x \pmod{37}$

$\text{ord } \Gamma = ?$

$\Gamma(1) \equiv 3 \cdot 1 \pmod{37} \Rightarrow$ Divisibel durch 3 $\pmod{37}$

$\Gamma(3) \equiv 3 \cdot 3 \equiv 9 \pmod{37}$

$\Gamma(9) \equiv 27 \cdot 3 \equiv 27 \pmod{37}$

$\Gamma(27) \equiv 27 \cdot 3 \equiv 81 \equiv 7 \pmod{37}$

$\Gamma(36) \equiv 36 \cdot 3 \equiv 108 \equiv 34 \pmod{37}$

$\Gamma(34) \equiv 34 \cdot 3 \equiv 102 \equiv 28 \pmod{37}$

$\circ \quad \Gamma(28) \equiv 28 \cdot 3 \equiv 84 \equiv 10 \pmod{37}$

$\Gamma(10) \equiv 10 \cdot 3 \equiv 30 \pmod{37}$

$\Gamma(30) \equiv 30 \cdot 3 \equiv 90 \equiv 16 \pmod{37}$

$\Gamma(16) \equiv 16 \cdot 3 \equiv 48 \equiv 11 \pmod{37}$

$\Gamma(11) \equiv 11 \cdot 3 \equiv 33 \pmod{37}$

$\Gamma(33) \equiv 33 \cdot 3 \equiv 99 \equiv 25 \pmod{37}$

$\Gamma(25) \equiv 25 \cdot 3 \equiv 75 \equiv 1 \pmod{37} \rightarrow$ so Mehl's Regel \Rightarrow Länge 18

Bei nicht mehr einer Zahl im Kreislaufprecedente 2.

$\Gamma(2) \equiv 3 \cdot 2 \equiv 6 \pmod{37}$

$\Gamma(6) \equiv 3 \cdot 6 \equiv 18 \pmod{37}$

$\Gamma(18) \equiv 18 \cdot 3 \equiv 54 \equiv 5 \pmod{37}$

$\Gamma(5) \equiv 5 \cdot 3 \equiv 15 \pmod{37}$

$\Gamma(8) \equiv 8 \cdot 3 \equiv 24 \pmod{37}$

$\Gamma(35) \equiv 35 \cdot 3 \equiv 105 \equiv 31 \pmod{37}$

$\Gamma(19) \equiv 19 \cdot 3 \equiv 57 \equiv 20 \pmod{37}$

$\Gamma(23) \equiv 23 \cdot 3 \equiv 69 \equiv 32 \pmod{37}$

$\Gamma(22) \equiv 22 \cdot 3 \equiv 66 \equiv 28 \pmod{37}$

$\Gamma(13) \equiv 13 \cdot 3 \equiv 39 \equiv 2 \pmod{37}$

$\text{ord } \Gamma(x) \in [18, 18] = 18$

Länge 18

Sense privata delle costituzioni: da Γ dopo regole $\Gamma(x) \equiv 3x \pmod{37}$

$\Gamma(10) \equiv 3 \cdot 10 \equiv 30 \pmod{37}$

\rightarrow per 2.10 depe I llore

~~$\Gamma_4 \equiv 4 \cdot 3 \equiv 21 \pmod{37}$~~

$\Gamma(21) \equiv 21 \cdot 3 \equiv 63 \equiv 26 \pmod{37}$

$\Gamma(26) \equiv 26 \cdot 3 \equiv 78 \equiv 4 \pmod{37}$

$\Gamma(4) \equiv 4 \cdot 3 \equiv 12 \pmod{37}$

$\Gamma(12) \equiv 12 \cdot 3 \equiv 36 \pmod{37}$

① Calculați signature permutării $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ & 2 & 3 & 1 \end{pmatrix} \in S_4$.

Suntem permuteate de produs de cicluri disjuncte.

$$\cancel{\tau = (14)}$$

$$\cancel{\tau = (1,2,3) \circ (4)} = \cancel{(14)} \cancel{(2,3)} \cancel{(3,4)}$$

Inversa permutării $\tau = \tau_1 = \begin{pmatrix} 2 & 3 & 4 & 1 \\ 1 & 2 & 3 & 4 \end{pmatrix} \in S_4$.

$$\tau_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} \in S_4, \quad \text{în același ordine}$$

$\tau_2 = (1,3,2)$ este permutarea $\tau_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \in S_4$. Observăm că produsul de cicluri disjuncte.

$$\tau_2 \underbrace{(1,2,3)}_{\text{lung. 3}} \circ \underbrace{(4)}_{\text{lung. 1}} = (1,2) \circ (2,3) \circ (4) = 3 \text{ transpozitii}$$

$$\text{Nr. de inversions} (\tau) = 1 + 1 + 1 = 3 = \underline{\underline{m}}$$

(neutramos la τ) → acoperă pe 2 → numărul de elem pe stânga pe 2 este mai mare ca el.

Vedem pe 1 la 4 ⇒ 3 inversions

+ 1 inversions pt 3 - care este 1

+ 1 - care este 1

$$\boxed{\epsilon(\tau) = (-1)^m} = (-1)^3 = -1$$

$$\text{Deci } \boxed{\epsilon(\tau) = -1}$$

② Come si sostituisce nelle 2 cifre alle numerarie 37⁷⁹?

$$n=100 \quad \varphi(n) = 100 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{5}\right) = 100 \cdot \frac{1}{2} \cdot \frac{4}{5} = 40. \quad \Rightarrow \\ (37, 100) = 1$$

$$\hat{37}^{40} = 1$$

$$\hat{37}^{49} = \hat{37}^{40} \cdot \hat{37}^9 = \hat{37}^{40} \cdot \hat{37}^{40-1} = \hat{37}^{40} \cdot \hat{37}^{-1} = 1 \cdot 1 \cdot \hat{37}^{-1} = \hat{37}^{-1}$$

Tribute so often measured and 37. Pm $U(K_{100})$

$$100 = 37 - \boxed{12} + 26$$

$$SF = 26 \cdot \boxed{11} + 11$$

$$26 = 11 + 15$$

$$11 = 7 - \boxed{2} + 3$$

$$h = 3 - \sqrt{11} + 8$$

3=1-3 se omiste

$$\Rightarrow \frac{100}{37} - \frac{27}{10} = \frac{(-1)^6}{37 \cdot 10}$$

$$37 \cdot 10 - 37 \cdot 27 = 1 \Rightarrow +\widehat{37}(-\widehat{27}) = 1 \Rightarrow \widehat{37}^{-1} = \widehat{27} \text{ mod } 100$$

\Rightarrow Whole coffee beans 37^{+9} ~~amt~~ (73)

Sisteme reprezentări

1) 5 \boxed{a}

4 \boxed{b}

Găiti acel unic nr $x \in \{0, 1, 2, \dots, 100\}$ astfel încât $\overline{x} + \overline{11} = 0$ în $(\mathbb{Z}_{101}, +)$.

$$x \in \{1, 2, \dots, 100\}$$

$$-11$$

D) 3 \boxed{a} Calculati $\overline{6^2}$ în grupul $(\mathbb{Z}_{32}, +)$.
3 \boxed{b} Calculati $\overline{6^2}$ în grupul $(\mathbb{Z}_{23}, +)$.
3 \boxed{c}) Arătați că $6^{11} - 1$ nu e prim

2) Găiti rădăcinile polinomului $X^2 + X + 1 = 0$ în corpul $\langle a \rangle$ $(\mathbb{Z}_{103}, +, \cdot)$

$$\overline{11} \cdot \overline{X} = \overline{1}$$

$$\overline{X} + \overline{11} = \overline{0}$$

$$\overline{X} = \overline{-11}$$

$$\overline{X} = \overline{11}$$

$$\boxed{10}$$

$\overline{0} \rightarrow \text{in } (\mathbb{Z}_{101}, +)$.

$\overline{1} \rightarrow \text{in } (\cup(\mathbb{Z}_{101}), +)$

4) Fie $H \subseteq G$ în operație

• pe G astfel încât (G_i) în
 (H_i) sunt grupuri. Stiu că

$$|H| = 50 \text{ și } |G| = 100.$$

Fie $x, y \in G \setminus H$ ($x, y \in G$)
 $x, y \notin H$

Așa că $x, y \in H$.

a) $(\mathbb{Z}_{103}, +)$ 4
b) $(\mathbb{Z}_{101}, +)$ 5

10



① a) Să se calculeze cel mai mic nr. $x \in \{0, 1, 2, \dots, 100\}$ astfel încât $\bar{x} + \bar{11} = \bar{0}$ în $(\mathbb{Z}_{101}, +)$.

$$\bar{x} + \bar{11} = \bar{0} (\mathbb{Z}_{101}, +) \Rightarrow \bar{x} = \bar{101 - 11} = \bar{90} \Rightarrow$$

$\boxed{\bar{x} = \bar{90}}$ numărul căutat x în $(\mathbb{Z}_{101}, +)$ este 90.

b) Să se calculeze cel mai mic $x \in \{1, 2, \dots, 100\}$ astfel încât $\bar{11} \cdot \bar{x} = \bar{1}$ în $(U(\mathbb{Z}_{101}), \cdot)$.

$$\bar{11} \cdot \bar{x} = \bar{1} (U(\mathbb{Z}_{101}))$$

Algoritmul lui Euclid:

$$101 = 11 \cdot \boxed{9} + 2$$

$$11 = 2 \cdot \boxed{5} + 1$$

$$2 = 1 \cdot \boxed{2}$$

$$\frac{A}{B} = \frac{5}{9+1} = \frac{5}{10} \text{ redus la fracție}$$

$$\frac{5}{10} - \frac{11}{5} = \frac{(-1)^3}{11 \cdot 5} = \frac{(-1)}{55}$$

$$505 - 46 \cdot 11 = (-1)$$

$$505 - 506 = (-1) \quad \checkmark$$

$$\underbrace{505 - 46 \cdot 11 = (-1)}_{\text{dispare}} \Rightarrow -\bar{46} \cdot \bar{11} = \bar{(-1)} \mid \cdot (-1) \Rightarrow$$

$$\bar{46} \cdot \bar{11} = \bar{1} \Rightarrow \text{Inversul lui } \bar{11} = \bar{x} = \bar{46} \pmod{101}$$

$$\text{Deci, } \boxed{\bar{x} = \bar{46}} \pmod{101}$$

Numărul căutat x în $U(\mathbb{Z}_{101})$ este 46

$$\text{verificare: } \bar{11} \cdot \bar{46} = \bar{506} = \bar{1} \quad \checkmark$$

$$\begin{array}{r} 506 \\ 505 \\ \hline z=1 \end{array}$$

② a) Calculați $\text{ord}(\bar{6})$ în grupul $(\mathbb{Z}_{32}, +)$.

$$d = \text{ord}(\bar{6}) = \text{cel mai mic nr. natural nenul pt. că}$$

$$\bar{6k} = \bar{0} = 32 \cdot 2 \Rightarrow 32 \mid 6k \stackrel{(:2)}{\Rightarrow} 16 \mid 3k \Rightarrow \boxed{d=16} \quad \text{folosind}$$

$$\text{verificare: } 6 \cdot 16 = 96 \quad \checkmark$$

ord($\bar{6}$) în grupul $(\mathbb{Z}_{32}, +)$ este 16.

b) Calculați ord $\hat{6}$ în grupul $(\mathbb{U}(\mathbb{Z}_{23}), \cdot)$

Notăm $d = \text{ord}(\hat{6})$

$d | |\mathbb{U}(\mathbb{Z}_{23})| = \phi(23)$ $\phi_{23} = 23 - 1 = 22$
 $\hat{6}^{23} \equiv 1 \pmod{23}$ $d | 22 \Rightarrow d \in \{1, 2, 11, 22\}$

$$\hat{6}^1 \equiv \hat{6} \not\equiv 1$$

$$\hat{6}^2 \equiv \hat{36} \equiv \hat{13} \pmod{23} \not\equiv 1$$

$$\hat{6}^{11} = \hat{6}^{12} \cdot \hat{6}^{-1} = \hat{6} \cdot \hat{6}^{-1} \equiv 1 \pmod{23}$$

$$\begin{array}{r|l} 169 & 23 \\ 161 & \\ \hline 2 & \end{array}$$

$$(\hat{6}^2)^2 = (\hat{13})^2 = \hat{169} \equiv \hat{8} \pmod{23} \Rightarrow \hat{6}^{12} = (\hat{6}^2)^6 \equiv \hat{8}^3 = \hat{512} \equiv \hat{6}$$

$$\hat{6}^4 \cdot \hat{6}^{-1} \equiv 1 \pmod{23}$$

$$\hat{6}^4 \cdot \hat{6}^4 \equiv \hat{25} \equiv 1 \pmod{23} \quad \checkmark$$

din urmă $\hat{6} \pmod{23}$.

$$\begin{array}{r|l} 512 & 23 \\ 36 & \\ \hline 22 & \\ 36 & \\ \hline 20 & \end{array}$$

Deci, $\boxed{\text{ord } \hat{6} = \text{ord}(\hat{6}) = 11} \quad \checkmark$

c) Arătați că $6^{11} - 1$ nu e prim.

$$p \neq 2 \Rightarrow p \mid 6^{11} - 1 \text{ în } \mathbb{U}(\mathbb{Z}_p)$$

$$d = \hat{6}^{11} - 1 \mid 11 \Rightarrow \text{divizorul lui } 11, d \in \{1, 11\}$$

$\text{ord } \hat{6}$ în $\mathbb{U}(\mathbb{Z}_p) \Rightarrow \text{ord } \hat{6} \in \{1, 11\}$.

$$\hat{6}^4 = 1$$

$$\underline{\text{ord } \hat{6} = 11 \Rightarrow}$$

$$|\mathbb{U}(\mathbb{Z}_p)| = p - 1$$

$$\Rightarrow 6 \mid |\mathbb{U}(\mathbb{Z}_p)| \Rightarrow p - 1 = 11 \cdot t \Rightarrow p = 11t + 1 \geq 23 \Rightarrow$$

$$\Rightarrow 23 \mid 6^{11} - 1$$

Așa arătat mai sus la exercițiu 2b) că $\hat{6}^{11} - 1 \equiv 1 \pmod{23} \Rightarrow$

$$\Rightarrow 6^{11} - 1 \mid 23 \Rightarrow \underline{6^{11} - 1 \text{ nu e prim.}} \quad \checkmark$$