

Totălitatea problemelor din
universitate de Algebra (Sem I)

Cursul 2 și pregătire

1. Să se găsească inversul lui $\bar{30}$ în \mathbb{Z}_{61}

$$\bar{30} \cdot \bar{\text{inv}} \equiv 1 \pmod{61}$$

$\gcd(30, 61) = 1 \Rightarrow$ inversul există

Bézout: $61m + 30n = 1$

$$\begin{array}{l} 61 = 30 \cdot 2 + 1 \\ 30 = 1 \cdot 30 + 0 \text{ stop} \end{array} \quad \left| \begin{array}{l} 1 = 61 - 30 \cdot 2 \\ 1 = 61 \cdot 1 + 30 \cdot (-2) \end{array} \right.$$

Inversul lui $\bar{30}$ în \mathbb{Z}_{61} este $\underline{\underline{59}}$

2. Să se găsească inversul lui $\bar{14}$ în \mathbb{Z}_{61}

$$\bar{14} \cdot \bar{\text{inv}} \equiv 1 \pmod{61}$$

$\gcd(14, 61) = 1 \Rightarrow$ inversul există

Bézout: $61m + 14n = 1$

$$\begin{array}{l} 61 = 14 \cdot 3 + 10 \\ 14 = 10 \cdot 1 + 4 \\ 10 = 4 \cdot 2 + 0 \text{ stop} \end{array} \quad \left| \begin{array}{l} 10 = 61 - 14 \cdot 3 \\ 4 = 14 - 10 \cdot 1 \\ 3 = 10 - 4 \cdot 2 \\ 1 = 4 - 3 \cdot 2 \end{array} \right. \quad \hat{|}$$

$$\begin{aligned} 1 &= 7 - 2 \cdot (10 - 7 \cdot 1) \\ &= 7 - 2 \cdot 10 + 7 \cdot 2 \\ &= 7 \cdot 3 - 2 \cdot 10 \end{aligned}$$

$$\begin{aligned} 1 &= 3(14 - 10 \cdot 1) - 2 \cdot 10 \\ &= 3 \cdot 14 - 10 \cdot 3 - 2 \cdot 10 \\ &= 3 \cdot 14 + 10 \cdot (-5) \end{aligned}$$

$$\begin{aligned} 1 &= 3 \cdot 14 + (-5)(61 - 14 \cdot 3) \\ &= 3 \cdot 14 + 61 \cdot (-5) - 14 \cdot 3 \cdot (-5) \\ &= 61 \cdot (-5) + 14 \cdot \underline{\underline{18}} \end{aligned}$$

Inversul lui $\bar{14}$ în \mathbb{Z}_{61}
este 18

Obs: $(\mathbb{Z}_{61}, +)$ Care este inversul lui $\bar{14}$

$$\bar{14} + \bar{x} = \bar{0} \pmod{61}$$

$$\bar{14} + \bar{44} = \bar{0} \pmod{61}$$

$\bar{0}$ = elem neutru

$\bar{44}$ este inversul lui $\bar{14}$
pt adunare.

3. Care sunt ultimele 2 cifre ale lui 14^{203} ?

$$\begin{aligned} \mathbb{Z}_{100} &\\ \varphi(100) &= \varphi(2^2 \cdot 5^2) = \varphi(2^2) \cdot \varphi(5^2) = (2^2 - 2) \cdot (5^2 - 5) \\ &= 2 \cdot 20 = 40 \end{aligned}$$

$$\begin{aligned} \gcd(14, 100) &= 1 \Rightarrow \text{folosim T. Euler} \Rightarrow 14^{\varphi(100)} \equiv 1 \pmod{100} \\ &\Rightarrow 14^{40} \equiv 1 \pmod{100} \end{aligned}$$

$$\begin{aligned} \bar{14}^{203} &= (\bar{14}^{40})^5 \cdot \bar{14}^3 = \bar{1}^5 \cdot \bar{14}^3 = \bar{14}^3 = \bar{1} \cdot \bar{14}^2 \\ &= \bar{289} \cdot \bar{14} = \bar{89} \cdot \bar{14} = \bar{13} \end{aligned}$$

Ultimele 2 cifre sunt 1 și 3

4. Care sunt ultimele 2 cifre ale lui 17^{199} ?

\mathbb{Z}_{100}

$\gcd(17, 100) = 1 \Rightarrow$ folosim T. Euler

$$\varphi(100) = \varphi(2^2 \cdot 5^2) = 40$$

$$17^{\varphi(100)} \equiv 1 \pmod{100} \Rightarrow 17^{40} \equiv 1 \pmod{100}$$

$$\overline{17^{199}} = (\overline{17^{40}})^4 \cdot \overline{17^{39}} = \overline{1}^4 \cdot \overline{17^{39}} = \overline{17^{39}}$$

$$\overline{17^{39}} = + \text{ a. i. } \overline{17} \cdot \overline{x} = 1 \pmod{100}$$

Bézout: $100 \cdot m + 17 \cdot n = 1$

$$\begin{array}{l} 100 = 17 \cdot 5 + 15 \\ 17 = 15 \cdot 1 + 2 \\ 15 = 2 \cdot 7 + 1 \\ 2 = 1 \cdot 2 + 0 \text{ stop} \end{array} \quad \left| \begin{array}{l} 15 = 100 - 17 \cdot 5 \\ 2 = 17 - 15 \cdot 1 \\ 1 = 15 - 2 \cdot 7 \end{array} \right| \quad \begin{array}{l} 1 = 15 - 4(17 - 15) \\ = 15 - 4 \cdot 17 + 4 \cdot 15 \\ = 15 \cdot 8 - 4 \cdot 17 \\ = 15 \cdot 8 + 17 \cdot (-4) \end{array}$$

$$1 = 8(100 - 17 \cdot 5) + 17 \cdot (-4)$$

$$= 8 \cdot 100 - 17 \cdot 40 + 17 \cdot (-4)$$

$$= 100 \cdot 8 + 17 \cdot (-47)$$

$$100 - 47 = 53$$

Impresul "e..." al lui
 17 în \mathbb{Z}_{100} este 53
 \Rightarrow Ultimele 2 cifre
ale lui 17^{199} sunt
 $5 \text{ și } 3$.

5. Care sunt ultimele 2 cifre ale lui $18^{199}?$

$\gcd(18, 100) \neq 1$ nu putem folosi Teorema pt 18 dar:

$$18^{199} = (3 \cdot 3 \cdot 2)^{199} = \overline{3}^{199} \cdot \overline{3}^{199} \cdot \overline{2}^{199} = \\ = (\overline{3^4})^{49} \cdot \overline{3}^{39} \cdot (\overline{3^4})^{40} \cdot \overline{3}^{39} \cdot \overline{2}^{199} = \\ \Rightarrow 3^{40} \equiv 1 \pmod{100}$$

$$\gcd(100, 3) = 1 \Rightarrow T. Euler \quad 3^{e(100)} \equiv 1 \pmod{100}$$

$$= \overline{1}^{40} \cdot \overline{3}^{39} \cdot \overline{1}^{40} \cdot \overline{3}^{39} \cdot (\overline{2^4})^{199} \cdot \overline{2}^{199} \\ = \overline{67} \cdot \overline{67} \cdot \overline{24}^{199} \cdot \overline{12} = \overline{89} \cdot (\overline{24^2})^9 \cdot \overline{24} \cdot \overline{12}$$

$$\overline{3} \cdot \overline{x} = \overline{1} \pmod{100}$$

$$\text{Bezout: } 100m + 3n = 1$$

$$100 = 3 \cdot 33 + 1 \quad | \quad 1 = 100 - 3 \cdot 33 \\ 3 = 1 \cdot 3 + 0 \text{ stop} \quad | \quad 1 = 100 \cdot 1 + 3(-33)$$

$$100 - 33 = 67 \Rightarrow \text{Ultimile 2 cifre ale lui } \overline{3}^{39} \text{ sunt 67}$$

$$= \overline{32} \cdot \overline{46}^9 = \overline{32} \cdot (\overline{46^2})^4 \cdot \overline{46} = \overline{32} \cdot \overline{46} = \overline{32}$$

\Rightarrow Ultimile 2 cifre sunt 3 și 2

$$\underline{\text{Metoda 2:}} \quad (18^{199}) = (\overline{18^2})^{90} \cdot \overline{18}^{19} = \overline{24}^{90} \cdot (\overline{18^2})^{9} \cdot 18 \\ = (\overline{24^3})^{30} \cdot \overline{24}^{15} \cdot \overline{18} = \overline{24}^{30} \cdot (\overline{24^2})^3 \cdot \overline{18} = (\overline{24^2})^{15} \cdot \overline{24} \cdot \overline{18} \\ = \overline{46^{15}} \cdot \overline{32} = (\overline{46^2})^2 \cdot \overline{46} \cdot \overline{32} = \overline{46}^4 \cdot \overline{32} = (\overline{46^2})^3 \cdot \overline{46} \cdot \overline{32} \\ = \overline{46^3} \cdot \overline{32} = \overline{46} \cdot \overline{32} = \overline{32} \Rightarrow \text{Ultimile 2 cifre sunt 3 și 2}$$

(1.)

6. Care sunt ultimele 2 cifre ale lui 22^{2018} ?

$\gcd(100, 22) \neq 1$ nu putem folosi T. Euler pt $100 \nmid 22$ dar:

$$22^{2018} = (2 \cdot 11)^{2018} = 2^{2018} \cdot 11^{2018}$$

$$\gcd(100, 11) = 1 \Rightarrow \text{T. Euler } 11^{\varphi(100)} \equiv 1 \pmod{100}$$

$$\Rightarrow 11^{40} \equiv 1 \pmod{100}$$

$$= (\overline{2^{10}})^{20} \cdot \overline{2^{10}} \cdot \overline{2^8} \cdot (\overline{11^{40}})^{50} \cdot \overline{11}^{18} = \overline{2^4}^{20} \cdot \overline{2^4} \cdot \overline{56} \cdot$$

$$\cdot \overline{1}^{50} \cdot \overline{11}^{18} = (\overline{2^4})^{10} \cdot \overline{44} \cdot (\overline{11^2})^9 = \overline{46}^{10} \cdot \overline{44} \cdot \overline{21}^9$$

$$= (\overline{46^2})^5 \cdot \overline{44} \cdot \overline{21} \cdot (\overline{21^2})^4 = \overline{46}^2 \cdot \overline{46}^3 \cdot \overline{24} \cdot \overline{41}^4$$

$$= \overline{46} \cdot \overline{24} \cdot (\overline{41^2})^2 = \overline{24} \cdot \overline{81^2} = \overline{24} \cdot \overline{61} = \overline{64} \Rightarrow$$

\Rightarrow Ultimile 2 cifre sunt 6 și 4

7. Gasiti $a \in \{0, 1, 2, 3, \dots, 16\}$ stiind ca $17 \nmid a^{43} - 3$

$$a^{43} \equiv 3 \pmod{17}$$

$$\text{Obs: } \gcd(a, 17) = 1 \Rightarrow \text{T. Euler } a^{\varphi(17)} \equiv 1 \pmod{17}$$

$$\varphi(17) = p-1 = 16$$

$$\overline{a}^{43} = \overline{a}^{16} \cdot \overline{a}^{16} \cdot \overline{a}^{11} = \overline{1} \cdot \overline{1} \cdot \overline{a}^{11}$$

$$\overline{a}^{11} \equiv 3 \pmod{17} \Rightarrow (\overline{a}^{11})^3 \equiv 3^3 \pmod{17} \Rightarrow \overline{a}^{33} \equiv 27 \pmod{17}$$

$$\overline{a}^{33} = \overline{a}^{16} \cdot \overline{a}^{16} \cdot \overline{a} \Rightarrow a \equiv 10 \pmod{17}$$

$$\overline{a}^{33} = \overline{a} \Rightarrow a \text{ este } 10$$

8. Fie permutarea:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 1 & 7 & 10 & 3 & 6 & 9 & 2 & 5 & 8 & 1 \end{pmatrix}$$

Să se calculeze inversa σ^{-1}

$$\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 10 & 4 & 1 & 8 & 5 & 2 & 9 & 6 & 3 & 7 \end{pmatrix}$$

9. Fie permutările:

$$g = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad x = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad g^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

Să se calculeze $g \cdot x \cdot g^{-1}$

$$g \cdot x \cdot g^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

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

$$g \cdot g^{-1}(1) = g \cdot (2) = g(3) = 3$$

$$1 \rightarrow 2 \rightarrow 3 \rightarrow 3$$

$$2 \rightarrow 1 \rightarrow 2 \rightarrow 1$$

$$3 \rightarrow 3 \rightarrow 1 \rightarrow 2$$

10. Tip permutarea σ :

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 2 & 3 & 1 & 5 & 6 & 7 & 4 & 9 & 8 & 10 \end{pmatrix} \in S_{10}$$

Descmpune permutarea în produs de cicluri disjuncte.

$$\sigma = (1, 2, 3)(4, 5, 6, 7)(8, 9)(10) \quad 1 \not\sim 2 \not\sim 3 \not\sim 4 \not\sim 5 \not\sim 6 \not\sim 7 \not\sim 8 \not\sim 9 \not\sim 10$$

Sunt permutarea nici un produs de transpozitii.

$$\begin{matrix} 1 \rightarrow 2 \rightarrow 3 \\ 4 \rightarrow 5 \rightarrow 6 \rightarrow 7 \end{matrix}$$

$$8 \rightarrow 9$$

$$\textcircled{10}$$

$$\sigma = \left(\begin{array}{ccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 9 & 8 & 10 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 9 & 8 & 10 \\ 2 & 1 & 3 & 4 & 5 & 6 & 7 & 9 & 8 & 10 \\ 2 & 3 & 1 & 4 & 5 & 6 & 7 & 9 & 8 & 10 \\ 2 & 3 & 1 & 5 & 4 & 6 & 7 & 9 & 8 & 10 \\ 2 & 3 & 1 & 5 & 6 & 4 & 7 & 9 & 8 & 10 \\ 2 & 3 & 1 & 5 & 6 & 7 & 4 & 9 & 8 & 10 \\ 2 & 3 & 1 & 5 & 6 & 7 & 4 & 9 & 8 & 10 \\ 2 & 3 & 1 & 5 & 6 & 7 & 4 & 9 & 8 & 10 \end{array} \right)$$

$$\sigma = (4, 7)(4, 6)(4, 5)(1, 3)(1, 2)(8, 9)$$

11. Tip permutarea $\sigma \in S_{10}$

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 2 & 3 & 10 & 5 & 6 & 7 & 4 & 9 & 8 & 1 \end{pmatrix}$$

Să se descompună în produs de cicluri disjuncte și în produs de transpozitii. Să se afle și signatura.

$$= (1, 2, 3, 10)(4, 5, 6, 7)(8, 9)$$

~~A Z X K S D T R B J P C F~~

1 → 2 → 3 → 10

4 → 5 → 6 → 7

8 → 9

$$\underline{\text{transport}} \quad (1, 2)(2, 3)(3, 10)$$

$$(4, 5)(5, 6)(6, 7)(8, 9)$$

1	2	3	4	5	6	7	8	9	10
1	2	3	4	5	6	7	8	9	10
1	2	3	4	5	6	7	8	9	10
1	2	3	4	5	6	7	8	9	10
1	2	3	4	5	6	7	8	9	10
1	2	3	5	6	4	9	8	7	10
1	2	10	5	6	4	9	8	7	3
2	3	10	5	6	4	9	8	7	2
2	3	10	5	6	4	9	8	7	1
2	3	10	5	6	4	9	8	7	1

Signature ext:

$$\varepsilon(\sigma) = (-1)^7 = -1$$

Signature ext
în de transport
= (-1)

③ Se păstrează
pantărea în casul
produsului de transpa-
zită.

12. Găsiți inversa permutării:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 1 & 5 & 3 & 4 & 7 & 8 & 6 & 9 \end{pmatrix} \in S_9$$

$$\sigma^{-1} = ?$$

Inversăm linile și sortăm prima linie păstrând
corespondența.

$$\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 1 & 4 & 5 & 3 & 8 & 6 & 7 & 9 \end{pmatrix}$$

13. Găsiți ultimele 2 cifre ale lui 3^{49}

\mathbb{Z}_{100}

$$\gcd(3, 100) = 1 \Rightarrow$$
 folosim T. Euler $\Rightarrow 3^{\varphi(100)} \equiv 1 \pmod{100}$

$$\begin{aligned}\varphi(100) &= \varphi(2^2 \cdot 5^2) = \varphi(2^2) \cdot \varphi(5^2) \\ &= (2^2 - 2) \cdot (5^2 - 5) = 40\end{aligned}$$

$$\bar{3}^{49} = \bar{3}^{40} \cdot \bar{3}^{49} = \bar{1} \cdot \bar{3}^{49} = \bar{3}^{49}$$

$$\begin{aligned}\bar{3}^{49} &\equiv (\bar{3}^3)^{13} \equiv (\bar{27})^{13} \equiv \bar{27} + (\bar{27}^2)^6 \equiv \bar{27} + \bar{27}^6 \\ &\equiv \bar{27} + \bar{27}^3 + \bar{27}^3 \equiv \bar{27} + \bar{81} + \bar{81} \equiv \bar{67}\end{aligned}$$

\Rightarrow Ultimele 2 cifre sunt 6 și 7

Metoda 2:

$$\begin{array}{c} \bar{3}^{49} \\ \bar{3} \\ \times \end{array} \quad \bar{3} \cdot \bar{x} \equiv 1 \pmod{100} \quad 100 - 33 = 67$$

$$\text{Bézout: } 100m + 3n = 1$$

$$\begin{array}{l} 100 = 3 \cdot 33 + 1 \\ 3 = 1 \cdot 3 + 0 \text{ stop} \end{array} \quad \left| \begin{array}{l} 1 = 100 - 3 \cdot 33 \\ 1 = 100 \cdot 1 + 3(-33) \end{array} \right.$$

\Rightarrow Ultimele 2 cifre sunt 6 și 7

14. Găsiți ultimele 2 cifre ale lui 3^{2018}

$$\begin{aligned}\gcd(3, 100) &= 1 \Rightarrow \text{folosim T. Euler} \Rightarrow 3^{\varphi(100)} \equiv 1 \pmod{100} \\ \varphi(100) &= 40 \\ \Rightarrow \bar{3}^{40} &\equiv \bar{1} \pmod{100}\end{aligned}$$

$$\bar{3}^{2018} = (\bar{3}^{10})^{50} \cdot \bar{3}^{18} = \bar{1}^{50} \cdot \bar{3}^{18} = \bar{3}^{18}$$

$$\bar{3}^{18} = (\bar{3}^6)^3 = \bar{27}^3 = \bar{819}$$

Ultimile 2 cifre sunt 8 și 9

15. În $(\mathbb{Z}_{89}, +)$ inversul lui $\bar{32}$ = ?

$$\bar{32} + \bar{x} = \bar{0} \pmod{89}$$

$$\begin{array}{r} 89 - \\ 32 \\ \hline 57 \end{array}$$

$$\bar{x} = \bar{57}$$

16. În (\mathbb{Z}_{89}, \cdot) inversul lui $\bar{32}$ = ?

$$\gcd(89, 32) = 1 \Rightarrow \exists! x^{-1}$$

$$\text{Bézout: } 89m + 32n = 1$$

$$89 = 32 \cdot 2 + 25$$

$$32 = 25 \cdot 1 + 7$$

$$25 = 7 \cdot 3 + 4$$

$$7 = 4 \cdot 1 + 3$$

$$4 = 3 \cdot 1 + 1$$

$$3 = 1 \cdot 3 + 0 \text{ stop}$$

$$\left| \begin{array}{l} 25 = 89 - 32 \cdot 2 \\ 7 = 32 - 25 \cdot 1 \\ 4 = 25 - 7 \cdot 3 \\ 3 = 7 - 4 \cdot 1 \\ 1 = 4 - 3 \cdot 1 \end{array} \right.$$

$$\begin{aligned} 1 &= 4 - (7 - 4) \\ &= 4 - 7 + 4 \\ &= 4 \cdot 2 - 7 \end{aligned}$$

$$\begin{aligned} 1 &= 2(25 - 7 \cdot 3) - 7 \\ &= 2 \cdot 25 - 7 \cdot 6 - 7 \\ &= 2 \cdot 25 + 7(-7) \end{aligned}$$

$$\begin{aligned} 1 &= 2 \cdot 25 + (-7)(32 - 25) \\ &= 2 \cdot 25 + 32(-7) - 25 \cdot (-7) \\ &= 9 \cdot 25 + 32(-7) \end{aligned}$$

$$\begin{aligned} 1 &= 9 \cdot (89 - 32 \cdot 2) + 32(-7) \\ &= 9 \cdot 89 - 32 \cdot 18 + 32(-7) \\ &= 89 \cdot 9 + 32(-25) \end{aligned}$$

$$\begin{array}{r} 89 - \\ 25 \\ \hline 64 \end{array}$$

\Rightarrow Ultimile 2 cifre sunt 6 și 4

17. Care este următorul an după 2018 în care ziua de 10 noiembrie este sămbătă?

Anul = 365 zile

= 366 dacă este bisect

bisect \Leftrightarrow se divide la 4 (Dacă 4 | an \Rightarrow bisect)

Un număr este divizibil la 4 \Leftrightarrow Suma ultimelor 2 cifre este divizibile cu 4.

Lucrăm în \mathbb{Z}_7

$$365 \equiv 1 \pmod 4$$

$$366 \equiv 2 \pmod 4$$

Atunci când avem an nou și calculăm +1, când anul este bisect calculăm +2 și își

10 nov \rightarrow 2018 \rightarrow sămbătă

\rightarrow 2019 \rightarrow duminică

\rightarrow 2020 \rightarrow mardi (an bisect)

\rightarrow 2021 \rightarrow miercuri

\rightarrow 2022 \rightarrow joi

\rightarrow 2023 \rightarrow vineri

\rightarrow 2024 \rightarrow duminică (an bisect)

\rightarrow 2025 \rightarrow luni

\rightarrow 2026 \rightarrow marti

\rightarrow 2027 \rightarrow miercuri

\rightarrow 2028 \rightarrow vineri (an bisect)

\rightarrow 2029 \rightarrow sămbătă

Cursul 3 și pregătire

17

18. Calcularea ordinul lui $\bar{28}$ în grupul $(\mathbb{Z}_{200}, +)$

Elementul neutru = $\bar{0}$ în $(\mathbb{Z}_{200}, +)$

$$\bar{28} \cdot k = \bar{0} \quad \underbrace{\bar{28} + \bar{28} + \bar{28} + \dots + \bar{28}}_{k \text{ ori}} = \bar{0}$$

Formule: $\text{ord } \bar{m} = \frac{n}{(\text{m}, n)}$

Ondinul unui element, este cel mai mic număr mai mare ca 0 care împărează elementul = elem membru

$$\text{gcd}(200, 28) = 4$$

$$200 \rightarrow 1, 2, \boxed{4}, 5, 8, 10, 20, \dots \cancel{28} - \cancel{X} - \cancel{X}$$

$$28 \rightarrow 1, 2, \boxed{4}, 7, 14, \cancel{28}$$

\Rightarrow Ordinul lui $\bar{28}$ în $(\mathbb{Z}_{200}, +)$ este 50

19. Calculati ordinul lui $\bar{32}$ în grupul $(\mathbb{Z}_{152}, +)$

$$\text{ord } \bar{32} = \frac{n}{(\text{m}, n)} = \frac{152}{8} = 19$$

$$152 \& 32 \mid 8$$

\Rightarrow Ordinul lui $\bar{32}$ în grupul $(\mathbb{Z}_{152}, +)$ este 19.

$$19 \& 4$$

20. Calcularea ordinul lui $\bar{2}$ în grupul $(U(\mathbb{Z}_{55}), \cdot)$

$$U(\mathbb{Z}_{55}) = \{a \mid a \in \mathbb{Z}, \gcd(a, 55) = 1\} \quad (\text{Inversul})$$

Elementul neutru în $(U(\mathbb{Z}_{55}), \cdot)$ este 1

Vrem să găsim cel mai mic $k \in \mathbb{N}^*$ a. i. $\bar{2}^k = 1$

Hătâm ord $\bar{2}$ cu d

Proprietatea 3: $\text{ord } g \mid |G|$

Ondinul elementului d, divide cardinalul grupului.

Cardinalul lui $|U(\mathbb{Z}_{55})| = ?$

Folosim funcția lui Euler (ne arată căte elemente nu întregi de la 1 până la n sunt relativ prime cu n)

$$\varphi(55) = \varphi(11 \cdot 5) = \varphi(11) \cdot \varphi(5) = (11-1) \cdot (5-1) = 10 \cdot 4 = \underline{\underline{40}}$$

Deci, $\Rightarrow d \mid 40$ În acest caz d poate fi:

$d \in \{1, 2, 4, 5, 8, 10, 20, 40\}$ divizori lui 40

d nu poate fi 1, 2, 4, 5, 8, 10

$2^1 \not\equiv 1 \pmod{55}; 2^2 \not\equiv 1 \pmod{55}; \dots 2^{10} = 1024 \text{ și}$

$1024 \pmod{55} = 34 \text{ iar } 34 \not\equiv 1 \pmod{55}$

Nicăieri nu verificăm ca $2^0 \equiv 1$

$\bar{2}^{20} \equiv 1 \pmod{55} \Rightarrow (\bar{2}^{10})^2 \equiv 1 \pmod{55} \Rightarrow \bar{34}^2 \equiv 1 \pmod{55} \Rightarrow \bar{1} \equiv 1 \pmod{55} \Rightarrow \text{Ondinul lui } \bar{2} \text{ în grupul } (U(\mathbb{Z}_{55}), \cdot) \text{ este } 20$

21. Calcularea ordinului lui $\bar{32}$ în grupul $(\mathbb{Z}_{89}^*, \cdot)$,
 având elementul, din de cănd
 $\text{ord}_G | |G|$ grupul.

Notăm $\text{ord } \bar{32} = d$
 $\Rightarrow d | |\mathbb{Z}_{89}^*|$ adică, $d | 88$
 $d \in \{1, 2, 4, 8, 11, 22, 44, 88\}$

$$32^1 \not\equiv 1 \pmod{89}$$

$$32^2 = 1024 \Rightarrow 45 \not\equiv 1 \pmod{89}$$

$$32^4 = \overline{32^2} \cdot \overline{32^2} = \overline{45} \cdot \overline{45} = \overline{2025} \Rightarrow 67 \not\equiv 1 \pmod{89}$$

$$32^8 = \overline{32^4} \cdot \overline{32^4} = \overline{67} \cdot \overline{67} = \overline{4489} \Rightarrow 39 \not\equiv 1 \pmod{89}$$

$$32^{11} = \overline{32^8} \cdot \overline{32^3} = \overline{39} \cdot \overline{16} = \overline{624} \Rightarrow 1 \equiv 1 \pmod{89}$$

\Rightarrow Ordinul lui $\bar{32}$ în $(\mathbb{Z}_{89}^*, \cdot)$ este 11

22. Găsiți ordinul permutării $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 7 & 2 & 8 & 6 & 3 & 5 & 4 & 1 \end{pmatrix}$

Descompunem în produs de cicluri disjuncte:

$$\sigma = (1, 9) (2, 7, 5, 6, 3) (4, 8)$$

$$\text{ord } \sigma = \text{l.c.m.} (m_1, m_2, m_3) = \text{l.c.m.} (2, 5, 2) = 10$$

$$1 \rightarrow 9 \\ 2 \rightarrow 7 \rightarrow 5 \rightarrow 6 \rightarrow 3$$

Ordinul unei permutări a unor multimi finite $4 \rightarrow 8$
 număr de produs de cicluri disjuncte este cel mai mic multiplu
 comun a lungimii ciclurilor.

$$\frac{18}{18-12} \cdot 3 \cdot 3 \cdot \frac{12}{12-6} \cdot 2 \cdot 2 = 12$$

$$\text{l.c.m. } \frac{18}{12} = 2 \cdot 3 \cdot 3 \\ \frac{12}{12-6} = 2 \cdot 2 \cdot 3$$

$$\text{l.c.m. } 2 \cdot 3 \cdot 3 \cdot 2 = 36$$

23. Fie permutarea:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 \\ 2 & 3 & 4 & 1 & 6 & 7 & 8 & 9 & 10 & 5 & 12 & 13 & 11 \end{pmatrix}$$

Găsește ordinul permutării

$$(1, 2, 3, 4)(5, 6, 7, 8, 9, 10)$$

$$1 \neq 2 \neq 3 \neq 4 \neq 5 \neq 10 \neq 12 \neq 13$$

$$(11, 12, 13)$$

$$1 \rightarrow 2 \rightarrow 3 \rightarrow 4 \rightarrow 1$$

$$\text{ord } \sigma = [4, 6, 3] = 12$$

$$5 \rightarrow 6 \rightarrow 7 \rightarrow 8 \rightarrow 9 \rightarrow 10 \rightarrow 5$$

c.m.m.m.c

24. Calculati ordinul lui $\bar{2}$ in grupul $(U(\mathbb{Z}_{73}), \cdot)$

Notam ord $\bar{2}$ in d

$$d \mid |(U(\mathbb{Z}_{73}), \cdot)|$$

$$73 \rightarrow \text{prim} \quad \varphi(73) = (73 - 1) = 72$$

$$\Rightarrow d \mid 72 \quad \text{Deci } d \in \{1, 2, 3, 4, 6, 8, 9, 12, 18, \dots, 72\}$$

$$2^9 \equiv 1 \pmod{73} \Rightarrow 512 \equiv 1 \pmod{73}$$

$$\begin{array}{r} 512 \mid 73 \\ 511 \\ \hline = 1 \end{array}$$

$$\Rightarrow 1 \equiv 1 \pmod{73} \Rightarrow \text{ordinul lui}$$

$\bar{2}$ in grupul $(U(\mathbb{Z}_{73}), \cdot)$ este 9

25. Găsiți cel mai mic factor prim al lui $2^{23} - 1$

$$\text{prim} \rightarrow p \text{ deu } p \mid 2^{23} - 1 \quad 2^{23} \equiv 1 \pmod{p}$$

$$(\cup(\mathbb{Z}_p), \cdot) = (\mathbb{Z}_p^*, \cdot)$$

$\mathbb{Z}_p^* = \{\bar{a} \mid p \nmid a\}$ $\bar{1}$ = elem neutru al grupului
ordinul lui $\bar{2}$ în acest grup (Prop2: $g^m = e_{\text{ord } g \mid m}$)

$$\bar{2}^{23} = \bar{1} \Rightarrow \text{ord } \bar{2} \mid 23 \Rightarrow \text{ord } \bar{2} = 1 \text{ sau } \text{ord } \bar{2} = 23$$

$\xleftarrow[23 \text{ prim}]{\bar{2} \neq 1} \Rightarrow$

$$\Rightarrow \text{ord } \bar{2} = 23$$

$$\text{ord } \bar{2} \mid |\mathbb{Z}_p^*| = p-1 \quad \text{Deci:} \quad \begin{cases} 23 \mid p-1 \text{ adică,} \\ p-1 \text{ este multiplu de } 23 \end{cases}$$

$$23t = p-1 \Rightarrow p = 23t+1 \geq 47 \quad \xrightarrow{23} t \text{ nu poate fi } 1, \text{ deoarece } p \text{ număr prim} = 2$$

Trebui să arătem că $47 \mid 2^{23} - 1$

$$2^{11} = 2048 \stackrel{47}{\equiv} 27$$

$$2^{12} = 2^{11} \cdot 2 \stackrel{47}{\equiv} 27 \cdot 2 = 54 \stackrel{47}{\equiv} 7$$

$$\begin{aligned} & \Rightarrow 2^{23} = 2^{11} \cdot 2^{12} \stackrel{47}{\equiv} 27 \cdot 1 \stackrel{47}{=} 1 \Rightarrow \\ & = 189 \stackrel{47}{\equiv} 1 \Rightarrow \end{aligned}$$

$$\Rightarrow 47 \mid 2^{23} - 1 \Rightarrow 47 \text{ este cel mai mic factor al lui } 2^{23} - 1$$

26. Găsiți un factor prim al numărului $2^{2^3} - 1$
 p prim

$$(\cup(\mathbb{Z}_p), \cdot) = (\mathbb{Z}_p^*, \cdot)$$

$$2^3 = \text{ord } \bar{2} \quad | \quad |\mathbb{Z}_p^*| = p-1$$

$$p-1 = 2^3t \Rightarrow p = 2^3t+1$$

$$t=2 \Rightarrow p = 5^3 - \text{prim}$$

$$t=8 \Rightarrow p = 233 - \text{prim}$$

27. Găsiți $a \in \{1, 2, 3, \dots, 22\}$ a.i. $\text{ord } \bar{a} = 22$
 în grupul $(\cup(\mathbb{Z}_{23}), \cdot)$

$$\text{ord } \bar{1} = 1$$

$$\text{ord } \bar{2} = \bar{2}^2 + 1$$

$$2^{11} = 2048 \stackrel{23}{\equiv} 1$$

$$\Rightarrow \text{ord } \bar{2} = 11$$

Să folosește prop 5

$$\text{ord } \bar{2} \bar{2} = 2$$

$$\text{ord } \bar{2} \cdot \bar{2} \bar{2} = \bar{2} \bar{2} = \bar{44} = \bar{2} \bar{1}$$

$$\text{ord } \bar{3} = 11$$

$$\text{ord } \bar{5} = 11 \quad \Rightarrow a = 5$$

$$\text{ord } \bar{5} \neq 11$$

$$|\mathbb{Z}_{23}^*| = 22$$

$$\text{ord } \bar{a} | 22$$

$$\text{ord } \bar{a} \in \{1, 2, 11, 22\}$$

$$\text{ord } \bar{2} \bar{1} = 22$$

$$(3^{11} \stackrel{13}{\equiv} 1)$$

$$5^2 = 25 \equiv 2 \pmod{23}$$

$$5^{10} \equiv 2^5 = 32 \stackrel{23}{\equiv} 9$$

$$5^{11} = 5^{10} \cdot 5 \equiv 9 \cdot 5 \stackrel{23}{\equiv} 22$$

28. Calculati restul impartirii lui $79! \cdot 130!$
la 211

$$80x = 80! \cdot 130!$$

$$79 + 130 = 209$$

211 prim

$$x = 79! \cdot 130!$$

$$C_{211}^a \equiv 0 \pmod{211}$$

$$1 \leq a \leq 209$$

$$C_{210}^{130} = \frac{210!}{130! 80!}$$

$$C_{210}^{k+1} + C_{210}^k = \frac{210!}{(k+1)! (210-k)!} +$$

$$+ \frac{210!}{k! (210-k)!} = \frac{210!}{(k+1)! (210-k)!}$$

$$\left[(210-k) + (k+1) \right] \stackrel{211}{\equiv} 0$$

$$C_{210}^{k+1} \stackrel{211}{\equiv} -C_{210}^k \equiv C_{210}^{k-1}$$

$$C_{210}^{130} \stackrel{210}{\equiv} C_{210}^{129} \equiv \dots \stackrel{0}{\equiv} C_{210}^0 = 1$$

$$C_{210}^{1130} \equiv 1 \pmod{211} \quad \frac{210!}{130! 80!} \equiv 1 \pmod{211}$$

$$130! \cdot 80! \stackrel{211}{\equiv} 210! \equiv -1$$

↓ T. Wilson
211 prim

$$80x \stackrel{211}{\equiv} -1 \equiv 210$$

$$8x \stackrel{211}{\equiv} 21 \equiv 21 + 211 = 232$$

$$x \equiv 232 \pmod{211}$$