

$$\textcircled{1} \quad 37 \cdot x = \uparrow \quad \cup(7_{45}) \quad x?$$

$$1) \quad 151 = 37 \cdot \boxed{4} + 3$$

$$2) \quad 37 = 3 \cdot \boxed{12} + 1$$

$$3) \quad 3 = 1 \cdot \boxed{3}$$

se divide  
3opătă!

$$4 + \frac{1}{12} = \frac{49}{12} = 4,08$$

$$\frac{151}{37} - \frac{49}{12} = \frac{(-1)^3}{37 \cdot 12} = -\frac{1}{37 \cdot 12}$$

$$151 \cdot 12 - 37 \cdot 49 = -1$$

despre (e multiplu de)

$$-37 \cdot 49 = \uparrow$$

$$37 \cdot 49 = \uparrow$$

Lema chineză a resturilor:

$\forall a, b \in \mathbb{Z}, m, n \in \mathbb{N}^* \quad (m, n) = 1 \Rightarrow$  există un unic nr.  
 $x \in \{0, 1, \dots, m_1 - 1\}$  astfel încât  $x = m_1 a + r$   
 $x = m_2 b + s$  și  $r, s \in \mathbb{N}$

nr. prime între ele

Algoritm de cizură RSA

$(n, e)$   $n = p \cdot q \Rightarrow p, q$  prime distințoare,  $(e, (p-1)(q-1)) = 1$   
 $(899, 59)$

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

Mesajul  $M$ . În general se poate  $26^k < n < 26^{k+1}$

$$26^2 < 899 < 26^3 \quad (26^2 \rightarrow)$$

$$a_{k-1} a_{k-2} \dots a_1 a_0 \rightarrow a_{k-1} 26^k + a_{k-2} 26^{k-1} + \dots + a_1 26 + a_0$$

$$x = 13 \cdot 26 + 20 = \underline{\underline{358}}$$

$\frac{26}{13}$

$+ a_1 26 + a_0$

reziduu imprimabil  $x \pmod{n}$

Care este reziduu imprimabil

$$[\underline{\underline{358}}] \pmod{899} \quad \begin{array}{r} 29 \\ 31 \end{array} \quad \begin{array}{r} 26 \\ 338 \end{array} \quad \text{Operatii}$$

Se obține reziduu de un patrat

$$899 = 900 - 1 = 900 - 1^2 = 30^2 - 1^2 = 29 \cdot 31$$

Se te exponențializează scris în baza 2

$$x_2 \\ x_5 \\ x_8 \\ x_{16} \\ \text{---} \\ x_{32}$$

$$\frac{59 = 32 + 16 + 8 + 2 + 1}{(\text{poten additiv } x)}$$

-2-

Summe  $\wedge$   $\mathbb{Z}_{29}$

- mit  $\mathbb{Z}_{31}$ .

$$y = 358 \cdot 59 \quad \text{Restul importans to } 29.$$

$$358 \cdot 59 = 10^2 \cdot 59 = (10^2 \cdot 59) \cdot 32 \cdot 1000^{-1} \cdot \text{in } \mathbb{Z}_{29}$$

$$10^2 \equiv 1 \quad \text{mehr feste } a \text{-lin. Faktor}$$

$$U(\mathbb{Z}_{29})$$

$$\Rightarrow y \equiv 15$$

$$\text{ist } y \text{ in } \mathbb{Z}_{31} ? \quad \bar{y} \cdot 358 = 14^{59} \equiv 14^{30} \cdot 14^{29} \equiv 1 \cdot 14^{29} \rightarrow$$

$$\text{Importans zu } 358 \text{ do } 31$$

$$\text{dor } 14^{30} = 1 \text{ mehr feste a-lin. Faktor}$$

$$\Rightarrow 1 = 14^{30} = 14 \cdot \bar{y} \text{ in } U(\mathbb{Z}_{31})$$

$$\begin{aligned} 3 \cdot \bar{y} &= 2 \Rightarrow \bar{y} = 2 \cdot 3^{-1} = 2 \cdot 33 \Rightarrow \bar{y} = 11 \\ &\Rightarrow \bar{y} = 33 \cdot 3 = 11 \end{aligned}$$

$$\hat{y} = 11^3$$

$$y = 29a + 11 = 31b + 11, \quad a, b \in \mathbb{N}$$

$11, 11+29, 11+29, \dots, 11+30 \cdot 29 \rightarrow$  and symmetric polyphonic  
andante

modulo mt. not. note

$$\begin{aligned} \hat{y} &= 29a + 11 = 31b + 11 \rightarrow \text{in } \mathbb{Z}_{29} \\ \text{dispreo} &\Rightarrow \hat{b} = 2 \cdot \hat{a} + 11 \Rightarrow \\ 2\hat{a} &= 3 = 32 \text{ in } \mathbb{Z}_{29} \\ \Rightarrow \hat{a} &= 16 \text{ in } \mathbb{Z}_{29} \Rightarrow \end{aligned}$$

31:292

$$b = 29c + 16$$

$$\begin{aligned} y &= 31(29c + 16) + 11 = 899c + 31 \cdot 16 + 11 \\ &\Rightarrow y = 899c + 31 \cdot 16 + 11 \\ &\quad \text{droppe} \end{aligned}$$

$$\begin{array}{r} 31 \\ 16 \\ \hline 186 \\ 186 \end{array}$$

$$\frac{496}{11}$$

$$\Rightarrow y = 2504$$

$$\text{Sistem je SOF m } \frac{\log_2 26}{c=3} \text{ cu 3 cifre} \\ \text{SOF} = q \cdot 26^2 + b \cdot 26 + c, \quad a, b, c \in \{0, \dots, 25\} \\ = 0 \cdot 26^2 + 19 \cdot 26 + 13 \\ 2676$$

$$\begin{array}{r} \overline{0} & \overline{19} & \overline{13} \\ \text{NU} \curvearrowright \overline{A} & \overline{T} & \overline{N} \end{array} \quad \begin{array}{l} \text{lo} \\ \text{antide} \end{array}$$

$$\begin{array}{r}
 807 \\
 \times 26 \\
 \hline
 247 \\
 161 \\
 \hline
 2073
 \end{array}$$

## Decryptare - de gât pâinii!

$$\begin{cases} x = 25k + 1 \\ x = 25l + 3 \\ x \in S_{91}, \sim 99 \end{cases}$$

— and sign satisfies condition (53) so the result /

$$\text{Sekundenfsg} \Leftrightarrow a \cdot 26^2 + b \cdot 26 + c = 26^2 + 26 + 1$$

$$\begin{array}{r} 209 \\ - 676 \\ \hline 233 \end{array} \quad \boxed{D} 26 + \boxed{Y}$$

wedekin A — B — an-Open 1 — pto numeri ncl!  
W wedekin — (underlined) (underlined)

Met amalte simboluri

Sechzehn

- 1) Să se scrie  $p_{22} < \frac{p=29}{2=31}$  (element).
   
 2)  $e-f = 1 + (p-1) \cdot (2-1)t, t \in \mathbb{N}$  (element)
   
 3) ~~Restul împărțirii la  $y^f$  este~~.

$$AT \text{ intercept } (Y) = ATN = 50\%$$

(m, e)

Alice Bok  
the  
Osker

Ultim 358<sup>29</sup> = 507  
punkt am jüngste

$$59. \tilde{f} = 1 \text{ m } U(K_{870})$$

$$\begin{array}{r} 870 \\ | 59 \\ 59 \\ \hline 250 \\ 236 \\ \hline 21 \end{array}$$

$$1: 870 = 59 \cdot \boxed{15} + 15$$

$$2: \cancel{59 \cdot 15} + 15$$

$$3: 59 = 15 \cdot \boxed{3} + 14$$

$$4: 14 = 3 \cdot \boxed{4} + 2$$

$$5: 3 = 1 \cdot \boxed{3} + 0$$

$$6: 2 = 1 \cdot \boxed{2} \text{ se omete}$$

$$(27) (5-1)$$

$$28 \cdot 30$$

$$870 \text{ m } U(K_{870})$$

$$15 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1}}} =$$

$$= 15 + \frac{1}{1 + \frac{1}{5}} = 15 + \frac{5}{21} =$$

$$\frac{870}{59} - \frac{299}{21} = \frac{(-1)^{\text{jüngst}}}{55 \cdot 21}$$

$$\frac{870 \cdot 21}{59 \cdot 21} - 59 \cdot 299 = -1 \Rightarrow 59 \cdot \cancel{299} \tilde{f}$$

$$\Rightarrow \tilde{f} = 299$$

Ultimale pos

Amt Intercept ATN  $\rightarrow$  cusp line 507

$$507^{299} = 899 \cdot 2 + \frac{(358)(\frac{2}{2})}{\text{restl. Hypoth. } 29 \times 31}$$

Cu linea chiusa  $\Rightarrow$  c' restante

$$507^{299} = 17 \cdot (-7) \cdot 19 = -99 \cdot 15 = \boxed{10}$$

$$\begin{array}{r} 507 \\ | 29 \\ 29 \\ \hline 217 \\ 203 \\ \hline 17 \end{array}$$

$$\begin{array}{r} 126 \\ | 29 \\ 116 \\ \hline 10 \end{array}$$

$$\begin{array}{r} 299 \\ | 28 \\ 28 \\ \hline 1 \end{array}$$

$\cancel{219}$  rest

$$\begin{array}{r} 507 \\ | 31 \\ 31 \\ \hline 16 \end{array}$$

$$\begin{array}{r} 197 \\ | 186 \\ 186 \\ \hline 11 \end{array}$$

$\cancel{219}$  rest

Am  $K_{31}$  -

$$\begin{array}{r} 507^{299} - 299 \\ \hline 11 = 11 \cdot 29 = 17 \end{array}$$

am  $K_{31}$

$$11 \cdot 11 = 11^{30} = 1 \text{ dm } U(K_{31})$$

$$\begin{array}{r} 29 \\ | 11 \\ 11 \end{array}$$

$$\begin{array}{r} 2 \cdot 11 = 21 \cdot 3 \\ 21 \end{array}$$

$$28 = 3 = 35 \Rightarrow \boxed{\tilde{z} = 17}$$

$$\begin{array}{r} 308 \\ \times 31 \\ \hline 308 \\ + 98 \\ \hline 948 \end{array}$$

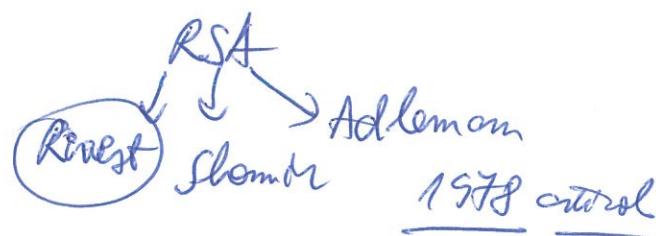
22-5

$$\begin{array}{r} \widehat{15}^2 = \widehat{196} = \widehat{22} = -\widehat{7} \\ m \geq 29 \\ \hline \widehat{15}^4 = \widehat{99} = \widehat{20} = -\widehat{9} \end{array}$$

$$\begin{array}{r} \overset{1}{\cancel{1}} \overset{8}{\cancel{5}} \overset{2}{\cancel{8}} \overset{1}{\cancel{1}} = -6 \\ \overset{1}{\cancel{1}} \overset{1}{\cancel{6}} \overset{2}{\cancel{3}} \overset{6}{\cancel{6}} = 4 \end{array} \quad 87 = 3 \cdot 29$$

$$-\hat{g} = \hat{g} \quad \text{wt } \omega \text{ is } 58 = 2 \cdot 29$$

$$\begin{array}{r}
 38 \quad | \quad 29 \\
 29 \quad | \quad 12 \\
 \hline
 268 \\
 -268 \\
 \hline
 0 \quad 15 \text{ goes into } 12 \text{ zero times} \\
 \hline
 0
 \end{array}$$



$A, B$  множества  $f: A \rightarrow B$  функция

Definitie 1) f este injectivă dacă  $f(x) = f(y) \Leftrightarrow x = y$  (dacă și numai dacă  $x \neq y$ )

$x, y \in A \Rightarrow f(x) \neq f(y)$

2) f surjective dec  $\Rightarrow \exists x \in A$  cu  $f(x) = b$

3) f) objectivé docē e simultānei inspekcijai / inspekcijai

Q.  $\begin{cases} \text{Soar } A, B \text{ finite} \\ f: A \rightarrow B \text{ bijective} \end{cases} \Rightarrow |A| = |B|$   
 (coordinate for sum egde)

2 groups:  $(6_1, +_1)$ ,  $(6_2, +_1)$

Spiraea grisea sunt grisea doce 30 fructu grisea intere 2 miliaria

$$f: G_1 \rightarrow G_2 \text{ A } f(x * y) = \overline{f(x) \sqcup f(y)} \quad \forall x, y \in G_1$$

$6_1 \approx 6_2$  Note (notre deux groupes sont identiques)

Exemple       $6_1 = (\mathbb{Z}_{10}, +)$   
                       $6_2 = (\cup(\mathbb{Z}_{11}), \cdot)$

First derivative also zero?  
 $b_1 \approx b_2$

$$\begin{array}{l} G_1 (\mathbb{Z}_{10}, +) \rightarrow \text{ordind } |\mathbb{Z}_6| = 6 \\ G_2 (\mathbb{U}(\mathbb{Z}_8), \cdot) \end{array}$$

ordine differente  
 $\Rightarrow$  nu sunt izomorfie

Controexemplu - deci nu e izomorfie

$$(\mathbb{U}(\mathbb{Z}_8), \cdot) \quad \{1, 3, 5, 7\} \quad \text{nu e grup}$$

$$\mathbb{U}(\mathbb{Z}_8) = \{1, 3, 5, 7\} \quad (\mathbb{U}(\mathbb{Z}_8), \cdot) \text{ grup cu 4 elemente}$$

$$(\mathbb{Z}_4, +) \quad \{0, 1, 2, 3\} \quad \text{un ordind 4}$$

acestea nu sunt izomorfie

$$\mathbb{U}(\mathbb{Z}_8) \not\cong \mathbb{Z}_4$$

$$\begin{array}{l} 3 \cdot 3 = 1 \text{ (elemt neutru)} \\ 1 \cdot 1 = 1 \\ 5 \cdot 5 = 1 \\ 7 \cdot 7 = 1 \end{array}$$

$$\begin{array}{l} \text{In } \mathbb{Z}_4 \\ 0+0=0 \\ 2+2=0 \\ 1+1 \neq 0 \\ 3+3 \neq 0 \end{array}$$

- elemt neutru. De se păstrează proprietatea fel nu e!

$$f(e_1) = e_2 \text{ (elemt neutru din alt grup)}$$

elemt neutru

din I grup cu 4 multimi

De ce  $\mathbb{U}(\mathbb{Z}_8) \not\cong \mathbb{Z}_4$ ? nu sunt izomorfie

$$\text{Presupun că } \exists f: \mathbb{U}(\mathbb{Z}_8) \rightarrow \mathbb{Z}_4 \text{ bijectiv} \quad f(x \cdot y) = f(x) + f(y)$$

$$\exists \hat{a} \in \mathbb{U}(\mathbb{Z}_8) \text{ a.s. } f(\hat{a}) = 1 \text{ (deoarece } f \text{ e surjectiv)}$$

$$(2) \quad 1+1 = f(\hat{a}) + f(\hat{a}) = f(\hat{a} \cdot \hat{a}) = f(1) = 0$$

$\times$  în  $\mathbb{Z}_4$  contradictie

$$\bar{a} = b \text{ în } \mathbb{Z}_8 \text{ nu ar fi } \frac{1}{2} - 0 \text{ în } \mathbb{Z}_4$$

- orice grup cu 2 elemt este izomorf cu  $\mathbb{U}(\mathbb{Z}_8)$ , și cu  $\mathbb{Z}_4$ .  
 Nu poate ca cele 2 să nu fie izomorfie.

Comutativitate:  $a \cdot b = b \cdot a \quad \forall a, b \in G$ . nu toate grupurile sunt comutative.

$(\mathbb{Z}_{10}, +) \cong (\mathbb{U}(\mathbb{Z}_{11}), \cdot)$  este izomorfie

$\text{ex 4 -}$

$U(\mathbb{Z}_{11})$

$\mathbb{Z}_{10}$

$\xrightarrow{0 \rightarrow} \text{elemente cloz de } 0.$

$1+1=2$

$1+1+1=3$

$\vdots$

$1+1+1+\dots+1=9$

9 ast

$$f(1) = 2$$

$$\boxed{f(j) = 2^j}$$

bijectivă

$$f(x+y) = f(x) + f(y),$$
  
 $x, y \in \mathbb{Z}_{10}$

$$f(x+y) = 2^{x+y} = 2^x \cdot 2^y = f(x) + f(y) \quad \begin{matrix} \text{-} \\ \text{conditie} \end{matrix} \quad \begin{matrix} \text{demonstrare} \\ \text{Teoreme lui Lagrange} \end{matrix}$$

(G formula)

$$(6, \cdot) \text{ grup finit}, g^{16} = e$$

$$\begin{matrix} 2^0 = 1 \\ 2^1 = 2 \\ 2^2 = 4 \\ 2^3 = 8 \\ 2^4 = 16 = 5 \text{ in } \mathbb{Z}_{11} \\ 2^5 = 10 = 9 \\ 2^6 = 20 = 9 \text{ in } \mathbb{Z}_{11} \\ 2^7 = 18 = 7 \\ 2^8 = 15 = 3 \\ 2^9 = 6 \end{matrix}$$

De ce e surjectiv? Incep din punct de vedere

- surjectiv - elem apar o singură dată.

Fiecare e bijectiv, nu e nicio d.

• E particular  $\rightarrow$  de  $10 \rightarrow$  reprezentanțe  $\frac{1}{2^k}$  - nu e o se! (Analog).

$$\text{Grupuri } (R, +) \cong (M_1, \cdot) \quad \forall r \in R, r > 0 \quad (M_1, \cdot) \text{ grup}$$

$$x - \frac{1}{x}$$

Numărul lui  $x$

De ce? - o bijectivă care să transforme o operare  
ce operare să nu să devină în anumite?

Ridicarea la o putere.

$$f(x) = 2^x$$

$$f(x+y) = 2^{x+y} = 2^x \cdot 2^y = f(x) \cdot f(y) \quad \text{Se arată că } f \text{ este o bijectionă.}$$

Surjectivitate

Surjectivitate.

$$f(x) = f(y) \Rightarrow 2^x = 2^y \Rightarrow x = y \quad \text{Bijectivă}$$

nu se rede  
mai și  
repetată!

$$x = \log_2 a \quad \text{pt } a > 0$$

(6.) grup finit, e-elementul neutral al grupului

ge 6.  $\nearrow$  ordinul lui  $g$

Notam  $\text{ord } g = m \in \mathbb{N}^* / g^m = e \}$  cel mai mic  $k \in \mathbb{N}^*$ .

$$g \cdot g \cdot g \cdots g = e$$

$k$  ord

elementul neutral

closed de  $\mathbb{Z}$ ,

Exemple:  $(\mathbb{Z}_{100})^+$

ord  $\bar{75} \Rightarrow l$

ord  $\bar{75} = l$

$$\bar{75} = \bar{75} + \bar{75} + \cdots + \bar{75} = \bar{0}$$

$\bar{75}k$   $k$  ord

$$\begin{array}{r} 100 \\ | \quad \text{divide} \\ 7 \quad 3k \end{array}$$

$\bar{l} \cdot \bar{75}$

$$\text{ord } \hat{3} \in \mathbb{N} (\cup (\mathbb{Z}_{11}), \cdot)$$

$$\hat{3} \cdot \hat{3} \cdots \hat{3} = \hat{1}$$

dekoN  $\quad$  kumon

$$\hat{3}^1 = \hat{3}$$

$$\hat{3}^2 = \hat{9}$$

$$\hat{3}^3 = 2\hat{7} \text{ in } \mathbb{Z}_{11} - \hat{5}$$

$$\hat{3}^4 = \hat{15} = \hat{3}$$

$$\begin{array}{r} 27 \\ 22 \\ \hline 25 \end{array} \quad \begin{array}{r} 11 \\ \hline 2 \end{array}$$

$$\text{ord } \hat{3} = 5 \text{ in }$$

$$(\cup (\mathbb{Z}_{11}), \cdot)$$

Proprietate:

$$1) \text{ } g^{\text{ord } g} = e$$

$$2) \text{ } g^n = e \Rightarrow \text{ord } g \mid n \quad \text{divide}$$

$$3) \text{ } \text{ord } g \mid \mid 6 \quad \text{divide}$$

$$|\cup (\mathbb{Z}_4)| = 10 \quad \text{codule}$$

$$\Delta_{10}(1, 2, 5, 10) \quad \text{not possible ztva ord 5}$$

$$2 \times 2$$

$$2^2 \times 2$$

$$2^5 \times 2^2 \cdot 2 \cdot 2 \cdot 5 \cdot 10 = 16 \cdot 2 \cdot 32 \cdot 2$$

$$32 \frac{1}{3}$$

dezord 2 in  $(\cup (\mathbb{Z}_{31}), \cdot)$

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

$$2^2 = 4 \neq 1$$

$$2^3 = 8 \neq 1$$

$$d \mid 30$$

$$\{1, 2, 3, 5, 6, 10, 15, 30\} \quad \text{not possible}$$

$$2^5 = 32 \neq 1 \rightarrow \text{ord } 2 = 5$$

$$\text{ord } 2 \text{ in } (\mathbb{U}(\mathbb{Z}_{100}), \cdot) \stackrel{?}{=} 9$$

$|\mathbb{U}(\mathbb{Z}_{100})| = 40$  (b-a mod 100)

$d \mid 40$

$\{1, 2, 3, 5, 7, 8, 10, 20, 50\}$

$$2^2 = 49$$

$$2^2(49) = (50-1)^2 = 2500+1 = 1 \Rightarrow \text{ord multiple of } 4.$$

- calculatia de buzunare (AA),

Test 2

$$\text{1. Se arata ca cel mult } x \in \{0, 1, \dots, 899\} \text{ are } \begin{cases} x = 31a + 11 \\ x = 29b + 20 \end{cases}, \forall a, b \in \mathbb{N}$$

$$\textcircled{2} \text{ Calculati ord 2 in } (\mathbb{U}(\mathbb{Z}_{43}), \cdot)$$

$$3. \text{ Verificati daca } (\mathbb{U}(\mathbb{Z}_{25}), \cdot) \cong (\mathbb{U}(\mathbb{Z}_{33}), \cdot)$$

b. Cate functii f inverse exista  $f: S_{1,2,3} \rightarrow S_{1,2,3,4,5}$ ?

c. Cate functii f surjective exista  $f: S_{1,2,3,4,5} \rightarrow S_{1,2,3}$ ?

Rezolvare

$$\textcircled{1} \quad \boxed{31a + 11 = 29b + 20} \Rightarrow \begin{cases} 31a + 11 = 20 \\ \mathbb{U}(\mathbb{Z}_{29}) \wedge \end{cases}$$

despre

$$31a = 20 - 11 \Rightarrow 2a = 20 - 11 = 9 = 38 \Rightarrow \boxed{\hat{a} = 19} \Rightarrow$$

$$\Rightarrow a = 29c + 19$$

$$x = 31a + 11 = 31(29c + 19) + 11 = 899c + \boxed{31 \cdot 19 + 11} \Rightarrow$$

$$\Rightarrow x = 31 \cdot 19 + 11 = 589 + 11 = 600$$

$$\boxed{x = 600} \text{ este numarul}$$

$$\begin{array}{r} 31 \\ 19 \\ \hline 275 \\ 89 + 11 \end{array}$$

$$\textcircled{2} \quad d = \text{ord } 2$$

$$|\mathbb{U}(\mathbb{Z}_{43})| = 2 \cdot 2 \cdot 3 \cdot 7 \Rightarrow$$

$$d \in \{1, 2, 3, 6, 7, 14, 21, 42\} \rightarrow \underline{8 \text{ divizori}}$$

$$\overline{2}^1 = 2 \neq 1$$

-10-

$$\overline{2}^2 = 4 \neq 1$$

$$\overline{2}^3 = 8 \neq 1$$

$$\overline{2}^6 = 64 \equiv 21 \neq 1$$

$$\overline{2}^7 = 52 \neq 1 = -1$$

$$\overline{2}^7 = (-1)^2 \rightarrow \text{nu este le poter} \quad \overline{2}^{15} = (-1)^2 = 1 \Rightarrow \boxed{\begin{array}{l} \text{ordналul } 2 \\ = 15 \end{array}}$$

③ Vom demonstra că  $\phi(U(\mathbb{Z}_{25})) \cong U(\mathbb{Z}_{33})$

$$|U(\mathbb{Z}_n)| = \phi(n) = n \cdot \prod_{p|n} (1 - \frac{1}{p}) \quad |U(\mathbb{Z}_{33})| = 33 \cdot (1 - \frac{1}{3})(1 - \frac{1}{11}) = 20$$
$$|U(\mathbb{Z}_{25})| = 25 \left(1 - \frac{1}{5}\right) = 20 = 25 \cdot \frac{4}{5}$$

Le  $\overline{0}, \overline{1}, \dots, \overline{24} \rightarrow 25 \text{ mod } 5$  → numerele cu 25  
sunt  $\overline{0}, \overline{5}, \overline{10}, \overline{15}, \overline{20}$  → multipli de 5 →  $\overline{0}, \overline{1}, \dots, \overline{32}$

$$|U(\mathbb{Z}_{33})| = \phi(33) = 33 \cdot (1 - \frac{1}{3})(1 - \frac{1}{11}) = 20$$

$\overline{0}, \overline{3}, \dots, \overline{30}$  sunt multe de 3

$\overline{11}, \overline{22}$

au sunt izomorfe. Așa că ordinalul nu fiecare!

$$d = \text{ord } 2 \text{ în } U(\mathbb{Z}_{25}) \quad \underline{d/20} = |U(\mathbb{Z}_{20})|$$

d ∈ {1, 2, 4, 5, 10, 20}

$$\overline{2}^1 \neq 1$$

$$\overline{2}^2 \neq 1$$

$$\overline{2}^4 = \overline{16} \neq 1$$

$$\overline{2}^5 = \overline{32} = \overline{7} \neq 1$$

$$\overline{2}^{10} = (\overline{2}^5)^2 = (\overline{7})^2 = \overline{49} = -1 \Rightarrow \text{ordinalul } 20.$$

Deci dă  $\mathbb{Z}_{20}$  este izomorfă  $U(\mathbb{Z}_{20}) \cong \{2^n \mid n \in \mathbb{N}\}$

în  $\mathbb{Z}_{33}$  să existe un elem. de ordin 20

~~$\text{decat}(U(\mathbb{Z}_{20}), U(\mathbb{Z}_{33}), \cdot)$~~  etenel există  $x \in U(\mathbb{Z}_{33})$  astfel încât  $x^2 = 20$  în  $U(\mathbb{Z}_{33})$ ,  $\cdot$ )  $\rightarrow$  FALSE  
 Dacă nu există  $x \in U(\mathbb{Z}_{33})$ . Atunci  $x^{10} = 1$   
 $(x_{33}) = \overline{1} \quad (x \in \text{prim cu } 33)$

$$3|x \Rightarrow x^2 = 3^2 + 1 \quad \left. \begin{array}{l} \text{(Mai multe ca div termot),} \\ |x| = 1121 + 1 \end{array} \right\} \Rightarrow 3|x^{10}-1$$

$$11|x \Rightarrow |x^{10} = 11^2 + 1 \quad \left. \begin{array}{l} \\ 33|x^{10}-1 \end{array} \right\} \Rightarrow 11|x^{10}-1$$

Contradictie

Nu există primul.

Q. Aleg  $f(1) = 5$  valori posibile

$f(1)$  fixat

Aleg  $f(2) = 4$  valori posibile

$S_{1,2,3,4,5} \setminus \{f(1)\}$

Aleg  $f(3) = 3$  valori posibile

$S_{1,2,3,4,5} \setminus \{f(1), f(2)\}$

Răspuns -  $5 \times 4 \times 3 = 60$  valori posibile

5)  $f$  surjective.  $f: S_{1,2,3,4,5} \rightarrow S_{1,2,3}$

Cate funcții f există  $f: S_{1,2,3,4,5} \rightarrow S_{1,2,3}$

$f(1) \rightarrow 3$  valori  $\rightarrow \boxed{3^5 = 243}$   
 $f(2) \rightarrow 3$  valori

Mai multe funcții nesurjective există  $f: S_{1,2,3,4,5} \rightarrow S_{1,2,3}$

E nesurjective  $\rightarrow$  nu există 1 dom funcție 1, 2, 3 nu e  $f(1)$  etc

Cate funcții  $f: S_{1,2,3,4,5} \rightarrow S_{1,2}$   $\rightarrow 2^5 = 32$   
 $\rightarrow S_{1,3}$   $\rightarrow 3^2 = 9$   
 etc  
 valori constante

$243 - 96$  nu e prima moștenire cu dom constantă

$$f(j) = 1 + j$$

$$243 - 96 + 3 = 243 - 93 = \boxed{150}$$

Numeri prime mari → date valoarele NUMERE PRIME

Euclid - (J) o informație de nr. prime. MAR!

2 82 5 89 9 3 3 - 1 cel mai mare număr prim cunoscut

Mersenne prime

Cel mai mare nr prim cunoscut astăzi explorat

Nr prim:

$2^{16} + 1$  și văd că e prim  $2^{16} + 1 = 65537$

$$\sqrt{2^{16} + 1} = 256, \dots$$

$p | 2^{16} + 1$  p prim  $\cup(\mathbb{Z}_p)$  1  $\Rightarrow p$  prim  $\Rightarrow p | 2^{16} + 1$  dñ  
 $2^{16} = -1$  Rădăcinea patrată  $2^{32} = 1$   $\downarrow$   $\cup(\mathbb{Z}_p)^n$   
dă ord  $\bar{2} \in \cup(\mathbb{Z}_p)$  :

1)  $g^{\text{ord } g} = e$

2)  $\text{dă } g^n = e \Rightarrow \text{ord } g | n$  - faza teorema  $\Rightarrow$

3)  $\text{ord } g | 16$  ordinalul grupului

$$2^{32} = 1 \xrightarrow{②} d | 32$$

$$\text{Prop 2: } \Rightarrow d | 32 \Rightarrow$$

$$\text{d} \in \{1, 2, 4, 8, 16, 32\} \leftarrow \text{Avem } \bar{2} \in \mathbb{Z}_{32}$$

$$\text{Resupunză } d \neq 32 \Rightarrow d | 16 \rightarrow \text{d } \cancel{32} \times \cancel{16}$$

$$2^{16} \left(2^d\right)^{16/d} = \left(2^{\text{ord } \bar{2}}\right)^{16/d} = 1^{16/d} = 1$$

$$1 = -1$$

$$p | 2 \Rightarrow p = 2$$

$$p \text{ impar} \Rightarrow p \neq 2 \text{ Contradicție}$$

$$\text{Deci } \text{ord } \bar{2} = 32 \in \cup(\mathbb{Z}_p)$$

$$32 \mid |\cup(\mathbb{Z}_p)| = p - 1 \quad p - 1 = 32 \cdot t$$

$$③ \text{ord } g | 16$$

$$1, 33, 65, 97, 129, 161 = 723, 193, 225, 257, 289, 321$$

nu e prim se divide cu 3

$$193 + \frac{32}{32} \frac{129}{161}$$

$$\begin{array}{r}
 65537 \\
 579 \\
 \hline
 = 763 \\
 579 \\
 \hline
 1844 \\
 1437 \\
 \hline
 = 110 \\
 65537 \text{ e prim}
 \end{array}$$

$$\begin{array}{r}
 -13- \\
 65537 \\
 582 \\
 \hline
 = 733 \\
 679 \\
 \hline
 = 554 \\
 485 \\
 \hline
 = 62
 \end{array}$$

Ord din 12 ordindell mult

Numeri primi mod - se situație (legate de mult. de 8&16).

$$\begin{array}{l}
 \cancel{\text{Fiz}} \text{ Stm } \bar{z}^2 \stackrel{d}{=} -1 \text{ contradicte } \Rightarrow \boxed{\frac{d \in \mathbb{Z}_2}{d \mid 2}} \Rightarrow
 \end{array}$$

$$\Rightarrow d = 32$$

$$\begin{array}{l}
 \text{Prop. 3} \Rightarrow 32 \mid N(\mathbb{Z}_p) \Rightarrow p-1 = 32k \Rightarrow \\
 \boxed{p = 32k+1} \Rightarrow
 \end{array}$$

primi. prime: 1, 3, 5, 6, ~~7~~, 11, ~~13~~, 17, ~~19~~, ~~23~~, ~~25~~, ~~27~~, ~~29~~, ~~31~~

$$\Rightarrow 65537 = 2^{16} + 1$$

$$\begin{array}{l}
 65537 = \boxed{193} \cdot 339 + 110 \\
 65537 = \boxed{97} \cdot 675 + 62
 \end{array}
 \Rightarrow \boxed{2^{16} + 1 \text{ e prim}}$$

nu sunt d 1  
fara  $\frac{p-1}{2}$   $\Leftrightarrow$   $\exists$  divizor al lui

Scrie: scriere divizor primul al lui  $2^{16} + 1$  nu poate fi divizor  $2^{16} + 1$  de nr. prim

$$\Rightarrow \boxed{2^{16} + 1 \text{ prim}}$$



② Calculați ordinul lui  $\langle \text{U}(\mathbb{Z}_{43}) \rangle$

$$|\text{U}(\mathbb{Z}_{43})| = 42 \quad D_{42} = \{1, 2, 3, 6, 7, 13, 21, 32\}$$

$\text{ord } 2 | 42 \Rightarrow \text{ord } 2 \in D_{42} \quad e=1$

$$\overline{2^2} = \overline{4}$$

$$\overline{2^3} = \overline{8}$$

$$\overline{2^4} = \overline{16}$$

$$\overline{2^6} = \overline{2^4} \cdot \overline{2^2} = \overline{16} \cdot \overline{4} = \overline{64} = \overline{21}$$

$$\overline{2^7} = \overline{21} \cdot \overline{2} = \overline{52} = -1$$

$$\overline{2^{15}} = (\overline{2^7})^2 = (-1)^2 = \overline{1} \Rightarrow \underline{\overline{1}}$$

$$\begin{array}{c|cc} 67 & 43 \\ \hline 43 & 1 \\ \hline 21 \end{array}$$

④ Cate funcții f injective există  $f: \{1, 2, 3\} \rightarrow \{1, 2, 3, 4, 5\}$ ?

$f(1) \in \{1, 2, 3, 4, 5\} \Rightarrow f(1)$  poate lua 5 valori

$f(2) \neq f(1) \Rightarrow f(2) \in \{1, 2, 3, 4, 5\} - \{f(1)\} \Rightarrow f(2)$  poate lua 4 valori

$f(3) \neq f(1) \wedge f(3) \neq f(2) \Rightarrow f(3) \in \{1, 2, 3, 4, 5\} - \{f(1), f(2)\} \Rightarrow$

$\Rightarrow f(3)$  poate lua 3 valori

$(f(1), f(2), f(3))$  - triplet de valori poate lua

$5 \cdot 4 \cdot 3 = 60$  valori, deci există 60 de astfel de funcții injective

⑤ Cate funcții f surjective există  $f: \{1, 2, 3, 4, 5\} \rightarrow \{1, 2, 3\}$ ?

$$3^5 = 243$$

$\{1, 2, 3\}$  are 3 submulțimi de cte 2 elemente, 3 submulțimi de cte 1 element, deci funcțiile de la  $\{1, 2, 3, 4, 5\}$  la  $\{1, 2, 3\}$  nu sunt surjective.

-2-  
Definiția de funcție surjectivă este

$$3^5 - 2^5 - 1^5 = 243 - 32 - 1 = 210 \Rightarrow \underline{\underline{210}}$$

① Se arată că numărul  $x \in \mathbb{Z}_{29} \sim [898]$  este astfel

$$\begin{cases} x = 31a + 11 \\ x = 29b + 20 \end{cases} \Rightarrow 31a + 11 = 29b + 20 \Rightarrow$$
$$\Rightarrow 31a = 29b + 9 \Rightarrow \hat{2}a = \hat{9} \pmod{29}$$
$$\hat{a} = \hat{19} \text{ și } \hat{2} \cdot \hat{19} = \hat{38} = \hat{9}$$
$$a = 19 \Rightarrow x = 31 \cdot 19 + 11 = \underline{\underline{600}} \Rightarrow \underline{\underline{600}}$$

③ Verifică că  $(U(\mathbb{Z}_{25}), \cdot) \cong U(\mathbb{Z}_{33})^\circ$

ele sunt izomorfe

card

Pentru grupul  $(U(\mathbb{Z}_{25}), \cdot)$  (cu ~~card~~  $U(\mathbb{Z}_{25}) = 20$ ),

elemente  $\underline{20} = \{1, 2, 3, 5, 10, 20\}$ , deoarece ordinele elementelor este  $20$ .

$$\underline{2}^1 = \underline{2}$$

$$\underline{2}^{10} = (\underline{2}^5)^2 = \underline{4}^2 = -\underline{1}$$

$$\underline{2}^2 = \underline{4}$$

$$\underline{2}^{20} = \underline{1}$$

$$\underline{2}^3 = \underline{8}$$

$$\underline{2}^5 = \underline{32} = \underline{4}$$

Dacă în grupul  $(U(\mathbb{Z}_{25}), \cdot)$  elementul  $\underline{2}$  generează toate elementele grupului.

Dacă în grupul  $(U(\mathbb{Z}_{33}), \cdot)$

$$\underline{2}^{10} = (\underline{2}^5)^2 = (\underline{32})^2 = (-\underline{1})^2 = \underline{1}$$

$$\underline{5}^{10} = (\underline{5}^5)^2 = (\underline{3125})^2 = (\underline{23})^2 = (-\underline{10})^2 = \underline{100} = \underline{1} = \underline{1}$$

Așadar, toate elementele grupului sunt generate de  $\underline{2}$  și nu există altun element de ordin 20?

$$\text{ord } \underline{2} = 20 \quad (U(\mathbb{Z}_{28}), \cdot)$$

$(\mathbb{Z}/x)$ , ord  $\hat{x} = 20$  ( $U(\mathbb{Z}_{33})$ )<sup>-3-</sup>  $\Rightarrow (U(\mathbb{Z}_{20}), \cdot) \not\cong (U(\mathbb{Z}_{33}), \cdot)$

the same isomorfe

2  
3  
4

5

6

Stup

$(G, \cdot)$  grup,  $G$  se numește comutativă, dacă  $x \cdot y = y \cdot x \quad \forall x, y \in G$ .

Exemplu - de grup necomutativ

- Grupul de permutări;  $n \in \mathbb{N}, n \geq 3$

$(S_n, \circ)$   
cordind but  $S_n = \{S_n\} = m!$

Dacă  $f, g \in S_n$ ,  $f \circ g \in S_n$ ,  $(f \circ g)_j = f(g(j)) \quad \forall j = 1, n$

$(S_n, \circ)$  grup necomutativ

Notătire:  $\tau = (1, 2, \dots, n)$

$\tau \in S_n \quad (\tau(1), \tau(2), \dots, \tau(n))$  - valoare funcției

Inversa unei permutări - cum se calculează? și cum se calculează ordinul?

$\tau^{-1} = \begin{pmatrix} \tau(1) & \tau(2) & \dots & \tau(n) \\ 1 & 2 & \dots & n \end{pmatrix}$  - se calculează linie

inverse  
linie

Exemplu  $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 2 & 5 & 7 & 3 & 1 & 6 \end{pmatrix} \in S_7$

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

= inversa permutării

le redoinăz.

ordinul unei permutări

cicli ale unei permutări

$(a_1, a_2, \dots, a_k) \rightarrow k \geq 2$

$a_j \in \{1, 2, \dots, n\} \quad \forall j$

K este  $a_i \neq a_j$  pt că  $i \neq j$   $\frac{\tau(x)=x}{\tau(a_i)=a_{i+1}} \quad \forall i=1, k-1$

lungime ciclu al permutării  $\tau$ :

$$\tau(a_1) = a_2$$

$$\tau(a_2) = a_3$$

$$\tau(a_3) = a_4$$

$$\tau(a_{k-1}) = a_k$$

$$\tau(a_k) = a_1$$

$\tau = (a_1, a_2, \dots, a_k) \circ (a_1, a_2, \dots, a_k) \circ \dots \circ (a_1, a_2, \dots, a_k)$

ciclu compus

$\tau = (1 \ 2 \ 3 \ 4 \ 5 \ 6 \ 7)$

Scris ca produs de cicli disjuncti pentru o permutare

Btr k=1 (a)  $\sigma(a) = a$

(6.) grupă finită, e-element neutru,  $g \in G$ .

$$\text{ord } g = \min \{k \in \mathbb{N}^* \mid g^k = e\}$$

$$(6,+) \quad g^n = g + g + \dots + g$$

Elementul neutru  $e$  din ord.

$$\sigma_{02} \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}$$

1) Notăm lungimele ciclilor

$$\text{ord } \sigma = \{k_1, k_2, \dots, k_m\} \quad \underline{k_1, k_2}$$

$$\text{ord } \sigma = \{1, 2\} \quad \text{comun comun}$$

Exemplu, scrieți o permutare în S<sub>6</sub> care să aibă ordinul maxim

$$k_1 + k_2 + \dots + k_m = 7 \quad k_j \in \mathbb{N}^* \\ [k_1, k_2, \dots, k_m] = \text{maxim}$$

~~(2, 3, 4, 5, 6, 7)~~ → permutare de ordin 7.

$$\text{ord } \sigma = 7$$

$$7 = 3 + 4$$

$$[3, 4] = 12$$

$$(1, 2, 3, 4) \quad (5, 6, 7)$$

- 13 este prim - numărul de 13. și  $k_i \leq 7$

11

27

2+7>7  
comună - numerabilă 7

8

15 - numărul  $\equiv 3 \cdot 5$

$$3+5=8 (>7)$$

① Pechet de 52 (ord 1), oranj este un alt lucru să fie lăsat.

1  
2  
3  
4  
52

$\frac{52(3k+1)}{49 \cdot 320 \text{ rest}}$	50	51
4	5	6
1	2	3
T	T	T

Anastorește o pochețelul de cizme,

$\frac{\text{III}}{\text{I}}$

Astăzi elnuște  $3k+2 \rightarrow 7$  elnuște

-3-

Se poate ordona treptele sa mențină <sup>c3</sup> poziția de corp pînă la sfîrșitul său?

Tratarea efectivă a ordinului  $S_{52}$  - o permutare.

$\sigma_2$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
	52	34	17	31	33	16	00	32	15	49	31	14	48	30	13	47	29	12	46	28
	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36				
	11	48	27	10	44	26	8	43	25	8	42	24	4	41	23	6				
	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52				
	40	22	5	39	21	4	38	20	3	37	19	<u>scule</u>	<u>36</u>	<u>18</u>	<u>1</u>	<u>35</u>				
	cartea	ord. 18 = 50 (dm 3m 3)																		

ordine disjunctă  $\rightarrow$  ordine

○  $\sigma_2(1, 52, 35, 23, 27, 9, 15, 13, 48, 2, 34, 41, 21, 11, 31, 42, 4, 57)$

~~(3, 17, 29, 25, 44, 20, 28, 43, 38, 22, 45) (5, 33, 45, 18, 12, 13, 30, 43, 24, 10, 49, 36, 6, 63, 47, 19, 46, 37, 50, 39)~~ (26)

lungimea ciclilor  $18, 11, 22$  Are 29 elemente.  $207 \text{ m.}$

$\text{ord}(\sigma_2[18, 11, 22]) = 3^2 \cdot 2 \cdot 11 = 198$

După 198 operații poziția se va întoarce la ordinea initială.

$$\begin{array}{r} 18 \\ 11 \\ \hline 18 \\ \hline 198 \end{array}$$

Se numește permutare pînă la  $n \geq 3$

○ Există 2 permutări  $\sigma_1, \sigma_2 \in S_n$  a.s.t.

$$\sigma_0 \sigma_1 \neq \sigma_1 \sigma_0$$

$$\sigma_2 \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ 2 & 1 & 3 & \dots & n \end{pmatrix}$$

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ 3 & 2 & 1 & \dots & n \end{pmatrix}$$

$$\sigma_0 \sigma_1 = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ 2 & 1 & 3 & \dots & n \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ 3 & 2 & 1 & \dots & n \end{pmatrix} =$$

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

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

dm desfășurăt

$c_3 \leftarrow$

$$\Gamma \circ \bar{\sigma}(j) = \Gamma(\bar{\sigma}(j))$$

$$\Gamma \circ \bar{\sigma}(1) = \Gamma(\bar{\sigma}(1)) = \Gamma(3) = 3$$

$$\Gamma \circ \bar{\sigma}(2) = \Gamma(\bar{\sigma}(2)) = 1$$

$$\text{Zo}\Gamma = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ 3 & 2 & 1 & \dots & n \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ 2 & 1 & 3 & \dots & n \end{pmatrix}$$

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

$$\Gamma \circ \bar{\sigma}(1) = 3$$

$$\Gamma \circ \bar{\sigma} \neq \text{Zo}\Gamma$$

$$\text{Zo}\Gamma(1) = 2$$

Proprietate ordine:

(G) grup finit

e-element neutru

$$\text{ord } g = \min \{ k \in \mathbb{N}^* \mid g^k = e \}$$

$$1) g^{\text{ord } g} = e$$

$$2) g^n = e \Rightarrow \boxed{\text{ord } g \mid n}$$

$$3) \text{ord } g \mid |G|$$

= Ordinele  
grupului

$$4) \text{ord } g^k = \frac{\text{ord } g}{(k) \text{ord } g}$$

Importante!

$$5) a \cdot b = b \cdot a \quad (\text{az comute ale 2 elem. intre ele})$$

$$(\text{ord } a, \text{ord } b) = 1 \Rightarrow \text{ord } a \cdot b = (\text{ord } a) \cdot (\text{ord } b)$$

Dacă ordinele sunt prime intre ele!

Exemplu:  $\text{ord } \overline{d}_2 \nmid m \cup (\mathbb{Z}_{31})^\times$

⇒ unul dintre el este grupul

$$\frac{|m \cup (\mathbb{Z}_{31})^\times| = 30}{d \mid 30}$$

$$|\langle U(\mathbb{Z}_n) \rangle| = \varphi(n) = n \cdot \prod_{p \mid n} \left(1 - \frac{1}{p}\right)^{\text{ord}_p}$$

Dacă  $n$  prim  $\Rightarrow |\langle U(\mathbb{Z}_n) \rangle| = n \cdot \left(1 - \frac{1}{n}\right) = n-1 \Rightarrow |\langle U(\mathbb{Z}_{31}) \rangle| = 30$

$$d \mid 30$$

$$\text{de } \langle 1, 2, 3, 5, 6, 10, 15, 30 \rangle$$

$$\text{elen. neutru} = \overline{1} \rightarrow \text{clasa de } 1$$

$$\overline{7}^2 = \overline{49} = \overline{18} \neq \overline{1}$$

$$\overline{7}^3 = \overline{7} \cdot \overline{7} = \overline{18} \cdot \overline{7} = \overline{126} = \overline{2} \neq \overline{1}$$

$$\overline{7}^4 = \overline{7} \cdot \overline{7}^3 = \overline{18} \cdot \overline{2} = \overline{36} = \overline{5} \neq \overline{1}$$

$$\overline{7}^5 = \overline{7} \cdot \overline{7}^4 = \overline{5} \cdot \overline{7} = \overline{35} = \overline{5} \neq \overline{1}$$

$$(\overline{7}^3)^5 = \overline{2}^5 = 32 = \overline{1} \quad \text{ordinul e cel mult } 15.$$

$$(\overline{7}^5)^2 = \overline{5} \cdot \overline{5} = \overline{25} \neq \overline{1}$$

Detectarea primei noile.

$2^p - 1$  - de aceeași formă

$p$  prim

$2^{ab} - 1$

$$(2^a - 1)^b \mid 2^{ab} - 1 \quad \text{dacă și numărul este prim}$$

$$2^{82589} - 1 \quad \text{Record Mersenne prime}$$

$$2^{13} - 1 = 8191$$

$$\sqrt{8191} \approx 90, -$$

$$8191 = 90^2 + 1^2$$

- nr primă 90 doar se divizează Mult 111

$$\text{iar } p \mid 2^{13} - 1 \quad p \text{ prim } (\langle U(\mathbb{Z}_p) \rangle, \cdot)$$

$$\overline{2^{13}} = \overline{1}$$

$$\text{care e odd 2 din } (\langle U(\mathbb{Z}_p) \rangle, \cdot)$$

ordinul este 1

prin care  $\neq \overline{1}$

$$\begin{array}{r} 126 : 31 = 4 \\ 124 \\ \hline 2 \end{array}$$

25-a putere de 31

ordinul este 15

Există subrotore, - cu subputere  
(grupă 2 subrotore); Atâtodată,  
(2h) din cești).  
2pm

C3

Proprietà 2)  $d \mid 13 \Rightarrow d > 1 \text{ e } d \neq 13$

$2 \neq 1 \Rightarrow d \neq 1$

Proprietà 3)  $13 \mid N(\mathbb{Z}_p)$  è cardinale  
divide  $p-1$  (dove  $p = \text{primo}$ )

$$p-1 = 13t + 1 \quad \boxed{+13t} = 1 + 26t$$

$\frac{p-1}{13}$

$$p \text{ primo} \Rightarrow p = 26t + 1$$

$$4, 24, \cancel{53} \text{ (stabilmente)} \\ \cancel{2}(26+1) \downarrow \\ \text{non è primo} \quad \text{è primo}$$

$$\frac{277}{26} \\ \cancel{53}$$

Concl - verifica delle 2mt. (numero min. primo per le 2mt)

$$\begin{array}{r} 8191 \\ 53 \\ \hline 289 \\ 245 \\ \hline 2241 \\ 212 \\ \hline 29 \end{array}$$

$$\begin{array}{r} 8191 \\ 79 \\ \hline 2251 \\ 227 \\ \hline 203 \end{array}$$

entrambi sono primi  $\Rightarrow$  vero  
~~ma non è primo~~

Numeri  $2^{16} + 1$  è primo. (non tranne 1).

Dimostrazione  $p_m^{2^m} 2^n + 1$

$$n = 0, 1, 2, 3, \dots, 2^m - 1 \\ \text{vedere } p \in \{3, 5, 17, 257, 65537\} \\ n \geq 0$$

Fermat

$2^{32} + 1$  non è primo

Dimostrazione

$$\lfloor 2^{32} \rfloor + 1 \approx 2^{16} = 65536.$$

$$p \mid 2^{32} + 1 \quad U(\mathbb{Z}_p)$$

$p$  primo,  $p \neq 2$

$$\frac{2^{32}}{2} = -1 \quad \text{Radicile per Fermat}$$

$$\frac{2^{64}}{2} = (\frac{2^{32}}{2})^2 = 1$$

$$2^{64} = T \text{ (from neutrality)} \Rightarrow d | 64.$$

Prop 2

Exponentul se divide cu 32,  $\frac{64}{32} = 2$

$$2^{32} = (2^d)^{32/d} = (2^{32/d})^{32/d} = 1^{32/d} = 1$$

dar  $2^{32} = -1 \Rightarrow$  contradicție,  $-1 = 1 \times$

$$\Rightarrow \text{ord}_2 \ln(U(z_p)) = 64 \quad \text{Prop 3} \quad 64 | p-1 \Rightarrow p = 1 + 64t$$

$$p = 1 + 64t$$

$$1, 65, 129, 193$$

$$257$$

nu e prim

(se divide cu 3)

$$257 = 2^8 + 1 = \\ \text{Proprietație } \text{dul } 193 \rightarrow 2^8 = 256 \equiv 63 \\ (2^8)^2 = 2^{16} = 63^2 \equiv 109 \equiv -87$$

$$2^{32} = 87^2$$

$$\begin{array}{r} 1266 \\ 1158 \\ \hline 108 \end{array}$$

$$2^8 \equiv -1 \pmod{107} \Rightarrow$$

$$2^{32} \equiv 1 \pmod{107}$$

$$2^{32} + 1 \equiv 2 \pmod{107} \quad \text{nu se imparte la } 107 \\ (\text{restul } 2)$$

$$\begin{array}{r} 63 \\ 63 \\ \hline 189 \\ 378 \\ 3565 \\ 3968 \\ \hline 193 \\ 193 \\ \hline 0 \end{array}$$

$$\begin{array}{r} 87 \\ 87 \\ \hline 336 \\ 672 \\ 7056 \\ 549 \\ \hline 1266 \end{array}$$

$$\begin{array}{r} 257 + \\ 63 \\ \hline 320 \\ 63 \\ \hline 257 \\ 257 \\ \hline 0 \end{array} \quad \text{se imparte la 3 nu e rest}$$

$$\begin{array}{r} 449 \\ 67 \\ \hline 512 \\ 512 \\ \hline 0 \end{array}$$

513 nu e divizibil cu 3

$449$  nu e prim deoarece nu e prim

$577$  - condicție.

$$641 | 2^{32} + 1 \quad \text{nu e prim}$$

cum e cunoscut că  $641 | 2^{32} + 1$  (Euler).

$$\begin{array}{r} 577 + \\ 63 \\ \hline 640 \end{array}$$

$$641 = 625 + 16 = 2^5 + 5^4$$

$$641 = 1 + 640 = 1 + 5 \cdot 2^7$$

$$2^{32} + 1 = \underbrace{2^{32} + 2^{28} \cdot 5^4}_{+ \text{rest}} + (1 - 2^{28} \cdot 5^4) \quad \text{selector cu care } 2^{28}$$

$$= 2^{28} \left( \underbrace{2^4 + 5^4}_{= 261} \right) + (1 + 2^{15} \cdot 5^2) \overbrace{\left( 1 - 2^{15} \cdot 5^2 \right)}^{(1-2^7 \cdot 5)(1+2^7 \cdot 5)} =$$

Subtract

$m \in \mathbb{N}, m \geq 3$

$a \in \mathbb{S}(1, 2, \dots, m-1)$  &  $n \nmid a^n - a \Rightarrow n \text{ mu e prim}$   
(divide) direkt auf Teiltot

Denn  $n \nmid a^n - a \forall a \in \mathbb{S}(1, 2, \dots, m-1) \Rightarrow n \text{ mu e prim oder}$

Exemplum denn  $\mathbb{N}$  kommt aus.  $n \nmid a^n - a \forall a \in \mathbb{S}(1, 2, \dots, m-1)$

M. Michael.  $561$  se divide an  $3$ .

$$561 = 3 \cdot 187 = \cancel{(3 \cdot 11) \cdot 17} \quad \text{mu e prim}$$

$$\begin{array}{r} 3 \cdot 11 \cdot 17 = 561 \\ \hline a^{561} - a \end{array} \quad \begin{array}{l} 11 \cdot 17 \\ \hline \text{divide} \end{array}$$

$$3 \nmid (a^{560} - 1) = a^{561} - a$$

Drittenteil  $3 \mid a$

$$\begin{array}{r} 3 \mid a^2 - 1 \mid a^{560} - 1 \\ \hline \end{array}$$

T denn  $3 \nmid a \Rightarrow 3 \mid a^2 - 1 \mid a^{560} - 1$  - denn  $p = \text{prim } p \in \mathbb{Z}, p \nmid a \Rightarrow$   
Mitteilen calci Teiltot - denn  $p = \text{prim } p \in \mathbb{Z}, p \nmid a \Rightarrow$

$$\Rightarrow p \nmid a^{p-1} - 1$$

T  $11 \mid a$  ok

$$\begin{array}{r} 11 \nmid a \Rightarrow 11 \mid a^{10} - 1 \mid a^{560} - 1 \\ \hline \end{array}$$

$$x-1 \mid x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + \dots + x + 1)$$

$$\text{Denn} \quad x = a^{10}$$

$$x-1 \mid x^{561} - 1$$

T  $17 \mid a$

$$\begin{array}{r} 17 \nmid a \Rightarrow 17 \mid a^{16} - 1 \mid a^{560} - 1 \\ \hline \end{array}$$

$$\Rightarrow 561 \mid a^{561} - a, \forall a \in \mathbb{Z}$$

$$\begin{array}{r} 560 \mid 16 \\ 58 \mid 30 \\ \hline 280 \end{array}$$

Denn ganz, 561 mu e prim

$n \nmid a^n - a \Rightarrow n \text{ mu e prim}$

Rejshere test 3

39-



$$\boxed{\begin{matrix} \text{J} & 3 \\ \text{Z} & 2 \end{matrix} \left( \begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 4 & 5 & 1 & 2 & 3 & 9 & 6 & 7 & 8 & 11 & 10 \end{matrix} \right)} \quad \frac{2020}{101}$$

de 3rd

Opmerk:

$$\begin{aligned} \Gamma^3(1) &= \Gamma^2(\Gamma(1)) = \Gamma(\Gamma(2)) = \Gamma(3) = 5 \\ (1, 4, 25, 3) \circ (6, 9, 8, 7) \circ (10, 11) &= \underbrace{\text{several more steps}}_{\text{in the solution}} \end{aligned}$$

$$\checkmark 5) x^{2023} = \sqrt[2023]{2023} \quad (x \in S_{11}) \Rightarrow \boxed{x=0} \text{ ist die ptturale} \\ \text{Lsg} \text{ der Gleichung.}$$

$$\text{Aplicam formula } \Theta \rightarrow \boxed{\begin{array}{l} \text{ord } x \\ (2023, \text{ord } x) = 20 \end{array}} \Rightarrow \cancel{x=20}$$

$$\Rightarrow 20 \cdot (\underbrace{2023}_{\text{descomponer}} \operatorname{Ad} X) = \operatorname{Ad} X \left( \frac{\text{Ap. 1204 Ad } x = 20}{\text{in S11}} \right) \quad \text{|| element mR}$$

$$2023 = 7 \cdot 11 \cdot 17 = 7 \cdot 14 \cdot 17$$


---

↑ 4  $\Rightarrow \operatorname{ord} X = [k_1 \dots k_m] \quad k_1 + k_2 + k_m = 11$

↑ 1  $\Rightarrow \operatorname{ord} X \neq 14 > 11$

7 depositos y 11

7.2023/140  $k_1 \geq 7; k_2 \geq 5$  (sino  $\operatorname{ln} = 12$  no es el).  $\Rightarrow \operatorname{ord} X = 20$

$$\text{flam} \ L \ X^{2023} = \overline{J}^{2023}$$

~~odd~~  $X = \overline{J} \Rightarrow$

~~odd~~  $X = \overline{J} \cdot \overline{J} = \overline{J}$

$\overline{J}^3 = \overline{J}^3$

3/10

dece odd  $X = \overline{J} \Rightarrow J \cdot 2023 \mid p$

$K_1 = J, K_2 = 5 \Rightarrow K_1 + K_2 = 12 \geq 11$

$(2023, \text{odd } X) = 1 \Rightarrow$

odd  $X = 2023$

$J \cdot 2023 = \overline{J} \cdot 2023 \rightarrow \text{even number} = 0$

$\star \overline{J}^{2023} = \overline{J}^{20} = \overline{e}$

---

~~$\overline{J}^{20} = \overline{J}$~~

④  $2^{23} - 1$  m.e. nt. prim

$p$  prim  $p \mid 2^{23} - 1$  m.u.  $(\mathbb{Z}_p)$

$d \mid 2^{23} - 1$   $\left\{ \begin{array}{l} d \mid 23 \\ d \mid 23 \end{array} \right. \Rightarrow \text{div by all div } 23 \rightarrow 1, 23$

odd 2  $\rightarrow$  m.u.  $(\mathbb{Z}_p)$   $\Rightarrow \cancel{d \neq 1} \quad 2 \neq 1$

Bsp 3.  $23 \mid 2^{23} - 1$   $\frac{\text{and } d=23}{\text{m.u. } (\mathbb{Z}_p)} \Rightarrow \text{odd } 2 \in S(1, 23)$

$23 \mid |U(\mathbb{Z}_p)| \Rightarrow 23 \mid p-1 \Rightarrow p-1 = 23t$

$p = 1 + 23t$

$1 + 23t + 1 \geq 57$

$57 \mid 2^{23} - 1$

$2^{10} = 1024 \mid 57 \cdot 21 + 37 \stackrel{m}{=} U(\mathbb{Z}_{57})$

$95 = 2 \cdot 47$

$2^{23} = 2^{10} \cdot 2^{10} \cdot 2^3 = (-10)(-10) \cdot 8 =$

$57 = 100 \cdot 8 = 6 \cdot 8 = 48 = 1 \Rightarrow 57 \mid 2^{23} - 1$

②  $p > 7$  a.d.  $p \mid 5^{15} + 1$

$p$  prim  $5^{15} + 1, p > 7 \mid U(\mathbb{Z}_p)$

$\frac{5^{15}}{5^{30}} = \frac{-1}{1}$

$d \text{ ord } 5 \nmid 30 \Rightarrow d \in \{2, 6, 10, 30\}$

$\# \text{ divisors of } 30$

$d \neq 15$

$d \in \{1, 2, 3, 5, 6, 10, 15, 30\}$ , step down to  $\{1, 3, 5, 10\} \rightarrow$

$d \in \{1, 6, 10, 30\}$

Case I  $d=2 \Rightarrow p \nmid 5^2 - 1 \Rightarrow (p \nmid 27)$ .  $p \nmid 7$  Contradict,

Case II  $d=6 \Rightarrow p \mid 5^6 - 1 \Rightarrow p \nmid 3$ .  $p \neq 3$  exclude

$$p \mid 5^6 - 1 = (5^3 - 1)(5^3 + 1) \Rightarrow$$

$$\Rightarrow p \mid 5^3 + 1 = 126 = 2 \cdot 3^2 \cdot 7 \text{ make sum } p \nmid 27 \text{ Contradict}$$

III  $d=10$

$$p \mid 5^{10} - 1 \stackrel{\text{ord } 5 = 10}{=} (5^5 - 1)(5^5 + 1) \Rightarrow$$

$$\Rightarrow p \mid 5^5 + 1 = (5+1)(5^4 + 5^3 + 5^2 + 5 + 1) \Rightarrow p \mid 521 \text{ prim}$$

$$625 = 125 + 21254$$

$$5^5 \equiv -1 \pmod{521}$$

$$5^{15} \equiv -1 \pmod{521}$$

IV  $d=30 \Rightarrow 30 \mid p-1 \quad p=1+30t \geq 31$

$$\begin{aligned} & 61 \quad 5^3 = 125 \equiv 61t + 3 \Rightarrow \\ & \Rightarrow 5^{15} \equiv 61t + 3^5 = 61t + 61 \Rightarrow \begin{array}{c} 263 \mid 61 \\ 183 \mid 3 \\ \hline 260 \end{array} \quad \left. \begin{array}{l} 61 \mid 5^{15} + 1 \\ 521 \mid 5^{15} + 1 \end{array} \right\} \text{ Reasons} \\ & 521 \mid 5^{15} + 1 \quad 5^3 = 125 \mid 31 \quad \frac{125}{25} \mid 31 \quad 61 \mid 5^{15} + 1 \quad \text{and } 5 \mid 31 \quad 0 \pmod{31} \end{aligned}$$

③ Given 2 nr. prime  $p_2$  s.t.  $5 < p_2 < 11$  and  $5p_2 \mid a^5 p_2 - a$

$$5p_2 \mid a(a^{5p_2-1} - 1) \quad \begin{array}{c} a-1 \\ \hline 5-1 \\ \hline 4 \end{array} \quad \begin{array}{c} p=13, 2=17 \\ \hline 13-1 \\ \hline 12 \end{array}$$

Nr. se div by 5,  $p_2 \mid 2$   $\Rightarrow$   $a \mid 5p_2 - 1$   $\Rightarrow$   $5 \mid a$   $\Rightarrow$   $5 \mid a^{5p_2-1} - 1$   $\Rightarrow$   $5 \mid a(a^{5p_2-1} - 1)$

$$\begin{array}{c} 5p_2-1 = 63-5 \\ 2-1 = 16-2 \\ \hline 52-1 = 81-2 \end{array}$$

$$p \nmid a \Rightarrow p \mid a^{p-1} - 1 \Rightarrow \frac{p-1}{(p-1)} \mid 5p_2 - 1$$

$$2 \nmid a \Rightarrow 2 \mid a^{\frac{p-1}{2}} - 1 \Rightarrow \frac{2-1}{(2-1)} \mid 5p_2 - 1$$

$$p-1 \mid 5p_2 - 1 \Leftrightarrow 5(p-1+1)2-1 = 5(p-1) \cdot 2 + 52-1 \Rightarrow \\ \Rightarrow p-1 \mid 52-1$$

$$2-1 \mid 5p_2 - 1 = 5(2-1+1)p-1 = 5(2-1)p + 5p-1 \Rightarrow \\ \text{divide} \quad \frac{5p-1}{2-1} \mid 5p-1$$

$$\boxed{p-1 \mid 52-1 \\ 2-1 \mid 5p-1}$$

$$\begin{array}{l} p=13 \\ 2=17 \\ 13, 17 \end{array}$$

p < 2

$$\frac{5p-1}{2-1} < \frac{52-1}{2-1} < 6$$

$$52-1 < 62-6 \quad \text{mit } (-)5p=2 \\ \underline{5 < 2} \quad (2 > 5) \quad \text{dell}(p, 2)=1$$

$$\frac{5p-1}{2-1} = 1 \quad 5p-1 = 2-1 \Rightarrow 2 = 5p \quad \text{num se parte - co'e} \\ \text{den se parte / form} \\ \text{num moltip}$$

Resumem

$$\frac{2 = 5p-1}{2-1} \Rightarrow \frac{2-2 = 5p-1}{2-1} \quad \boxed{2 = \frac{5p+1}{2}}$$

$$\downarrow p-1 \mid 52-1 = 5 \cdot \frac{5p+1}{2} - 1 = \frac{25p+3}{2} \quad \left| \begin{array}{l} \text{num moltip da 2} \\ \cdot 2 \Rightarrow \end{array} \right.$$

$$\Rightarrow p-1 \mid 25p+3 = 25(p-1)+28 : p-1 \Rightarrow$$

$$\Rightarrow p-1 \mid 28 \\ p=29$$

$$2 = \frac{5p+1}{2} = \frac{146}{2}$$

$$\begin{array}{l} \text{gcd } 2 = 73 \\ \boxed{p=29 \\ 2=73} \end{array}$$

crudeza rezolv!

$$\begin{array}{l} p=13 \\ 2=14 \end{array}$$

$$\boxed{2 \mid 5p_2 - 1}$$

$$5 \cdot 13 \cdot 17 - 1 = 21$$

$$\frac{5p-1}{2-1} = \frac{67}{16} = 4$$

$$\frac{52-1}{2-1} = \frac{5-17-1}{12} = \frac{84}{12} = 7$$

Totte solutioile la problema  $\rightarrow$  modelli

-1-

### Test 3

$$\textcircled{1} \quad \Gamma = (1, 2, 3, 4, 5) \circ (6, 7, 8, 9) \circ (10, 11)$$

$k_1=5$        $k_2=7$        $k_3=2$

$$[5, 7, 2]_{220} \Rightarrow \Gamma^{20} = e \Rightarrow \Gamma^{2020} = e \Rightarrow$$

$$\Rightarrow \Gamma^{2023} = \Gamma = (1, 2, 3, 4, 5)^3 \circ (6, 7, 8, 9)^3 \circ (10, 11)^3$$

$$(1 \ 2 \ 3 \ 4 \ 5 \ 6 \ 7 \ 8 \ 9 \ 10 \ 11)$$

$$(5 \ 4 \ 3 \ 2 \ 1 \ 9 \ 8 \ 7 \ 6 \ 11 \ 10)$$

$$\textcircled{2} \quad \widehat{2^{23}-1} = 0 \pmod{p}$$

$$\frac{2^{23}-1=0}{2^{23}-1=0} \Leftrightarrow 2^{23} \equiv -1 \quad ?$$

$$2^6 \equiv 1$$

$$\text{ord } 2 \mid 46 \Leftrightarrow \text{ord } 2 \mid 23 \nmid 23, 46$$

$$23 \mid p-1 \Rightarrow 46 \mid p-1$$

p impor

$$p \in \{47, 93, 139, \dots\}$$

$$\textcircled{2}^{23} = 1024 \cdot 8 \cdot 1024$$

$$37 = -10 \pmod{47}$$

$$2^{23} = 1024 \cdot 8 \cdot 1024 = (-10) \cdot 8 \cdot (-10) = \frac{64}{37}$$

$$= 800$$

$$\begin{array}{c|cc} 800 & 47 \\ \hline 47 & 17 \\ \hline 330 & 34 \\ \hline 329 & 21 \end{array} \Rightarrow 2^{23} \equiv 1 \pmod{47}$$

$$\Rightarrow 2^{23} - 1 \equiv 0 \pmod{47}$$

$$\begin{array}{l} 6^{11} \equiv 1 \\ 6^6 \equiv 1 \quad 6^{22} \equiv 1 \\ \text{ord } 6 \mid 22 \\ \text{ord } 6 \in \{1, 7, 11, 22\} \\ 11 \mid p-1 \Rightarrow \end{array}$$

$$\begin{array}{c|cc} 1024 & 47 \\ \hline 47 & 21 \\ \hline 327 & 34 \\ \hline 329 & 21 \end{array}$$

25

$$\textcircled{2} \quad 5^{15} + 1 = (5+1)(1-5+5^2-5^3+\dots-5^{13}+5^{15})$$

$$1-5+5^2-5^3+5^4=521, \text{ este prim}$$

$$5^{15} + 1 = 6 \cdot 521 \cdot (1-5+25) = 2 \cdot 3^2 \cdot 521$$

(521)

{ 3-7 }

curs 4 - SA)

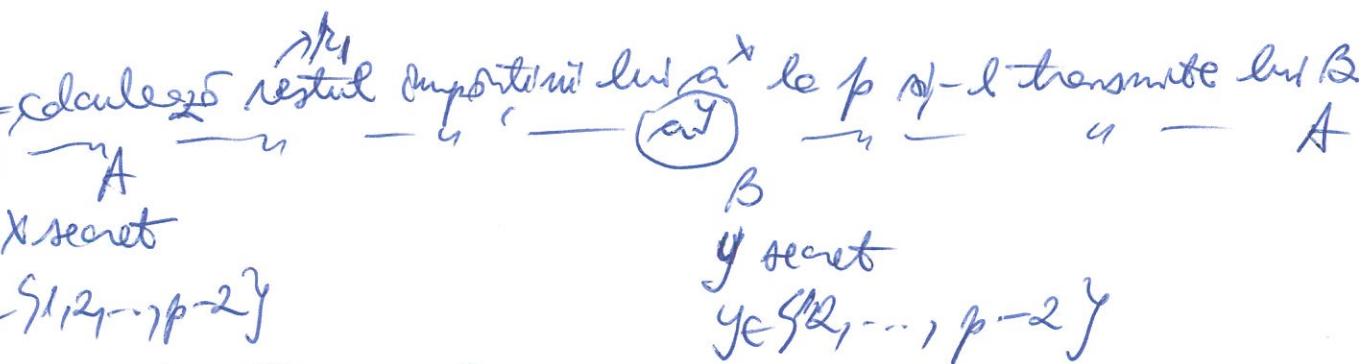
-1  
a<sup>p-1</sup>

21.01.2024

Teorema

- $p$  prim,  $p > 2$ . Atunci există  $a \in \mathbb{Z}_{p^2} \setminus \{1, 2, \dots, p-1\}$  astfel încât  $\text{ord } a = p-1$  în grupul  $(\mathbb{Z}_p^\times, \cdot) \Rightarrow$  grup cyclic
- $\mathbb{Z}_p^\times = \{1, \bar{a}, \bar{a}^2, \dots, \bar{a}^{p-2}\}$
- Diffie-Hellman 1976 RSA
  - (se bazează pe această teoremă)
  - Cum schimbă  $A$  pers. și către "A" și "B"?

acest lucru de:  
o p. mare ) și se numește  
 $a @$  publice



$$a^x = p \cdot x + r, r \in \{1, 2, \dots, p-1\}$$

Deși și el stiu pe  $r$ , nu e simplu să-l găsească pe  $x$ .  
 Problema logaritmului discret.

$\mathbb{Z}_p^\times$   $\bar{a}^x = \bar{r}$  (deosebit de  $r$ )

$$\boxed{x = \log_{\bar{a}} \bar{r} \text{ Analogie}}$$

Bsol 2

Obținem cheia comună

$$A: r_2^x = p \cdot x + r \quad \text{calculăm restul împărțirii la } p$$

$$B: r_1^y = p \cdot y + s$$

Aceeași rest = cheie comună

$$r = \text{restul împărțirii lui } \frac{(\bar{a}^y)^x}{p} \text{ la } p.$$

că de multă A există? (este  $\frac{2}{m}$ . ac  $\in \{1, 2, \dots, p-1\}$ ) cu proprietatea că

$$\text{ord } \bar{a} = p-1 \text{ în } (\mathbb{U}(\mathbb{Z}_p), \cdot)$$

$$\text{Rezolvare: } |\varphi(p-1)|$$

$$\varphi(n) = n \cdot \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

$$p \text{ prim}$$

$$p \mid n$$

$$\varphi(1) = 1$$

$$\text{Exemplu: } p=23$$

$$\varphi(22) = 22 \cdot \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{11}\right) = 10 \text{ numere au această proprietate.}$$

Să găsim explicit lnr. pătratul acesta.

Pe 1 -ul sistem; Le luăm tot mod de verificare cu 2, cu 3,

$$\text{d} \text{ord } 2 \text{ în } (\mathbb{U}(\mathbb{Z}_{23}), \cdot)$$

$$d \mid 22$$

de  $\{1, 2, \dots, 22\}$  să verifică,

$$\overline{2}^2 \neq \overline{1}$$

$$\overline{2}^{11} = \overline{2048} = \overline{1}$$

nu posibile pătrat - deci că?

$$\overline{3}^2 \neq \overline{1}$$

$$\overline{3}^{11}$$

$$\overline{3}^3 = \overline{24} = \overline{5} \text{ în } \mathbb{Z}_{23}$$

$$\overline{3}^9 = \overline{5}^3 = \overline{65} = \overline{18} \not\equiv$$

$$\overline{3}^{10} = \overline{3}^9 \cdot \overline{3} = \overline{81} = \overline{8}$$

$$\overline{3}^{11} = \overline{3} \cdot \overline{8} = \overline{1} \text{ nu e numărul } \overline{3},$$

$$\text{cu } \overline{3} \text{ nu avem } \overline{5}^{11} = (\overline{24})^2 = \overline{1}$$

$$\begin{array}{r} 2048 \\ 185 \\ \hline 208 \\ 208 \\ \hline 0 \end{array} \quad \begin{array}{r} 23 \\ \hline 89 \\ 89 \\ \hline 0 \end{array}$$

$$\begin{array}{r} 2048 \\ \hline 89 \\ 89 \\ \hline 0 \end{array}$$

$$67 \cdot 23 \equiv \text{rest } 18$$

$$\text{d} = \text{ord } 5 \quad \text{ord } 2 \mid n$$

$$\overline{5}^2 = \overline{25} = \overline{2} \neq \overline{1}$$

$$\overline{5}^{10} = \overline{5}^5 \cdot (\overline{5}^2)^5 = \overline{25} \cdot \overline{32} = \overline{9} \text{ modulo } 23$$

$$\overline{5}^{11} = \overline{9} \cdot \overline{5} = \overline{45} \Rightarrow \overline{-1} \neq \overline{1}$$

$$\boxed{\text{ord } \bar{5} = 22}$$

$$\bar{5}^3$$

Discrimenat. ac  $\{1, 2, \dots, 22\}$  a.s.  $\text{ord } \bar{a} = 22$

$$\bar{a} = \bar{5}^k$$

$$\text{Elementele } U(\mathbb{Z}_{23}) = \{ \bar{5}^0, \bar{5}^1, \bar{5}^2, \dots, \bar{5}^{21} \}$$

$$\text{ord } \bar{a} = 22 \Leftrightarrow \boxed{(22) = 1}$$

Proprietate  $\text{ord } g^k = \frac{\text{ord } g}{(\text{ord } g, k)}$

$$22 = \text{ord } \bar{5}^k = \frac{\text{ord } (\bar{5})}{(5, k)} = \frac{22}{(22, k)} \Leftrightarrow \boxed{(22, k) = 1}$$

Proprietate <sup>similitudine</sup> a lui Fermatelor

$$\text{ord } \bar{2} \text{ în } U(\mathbb{Z}_{23}) \text{ a.s. } \text{ord } \bar{2} = 11$$

Proprietate 5)  $a \cdot b \equiv b \cdot a$

$$(\text{ord } a, \text{ord } b) = 1 \Rightarrow \text{ord } a \cdot b = \text{ord } a \cdot \text{ord } b$$

$\text{ord } \bar{x} = 2$  prime între ele

$$\bar{x}^2 = \bar{1} \quad 23 \mid \frac{(\bar{x}-1)(\bar{x}+1)}{2} \quad (2, 11) = 1$$

$$\bar{x} \neq \bar{1} \quad 23 \nmid \bar{x}-1 \quad \Rightarrow 23 \mid \bar{x}+1$$

$$\text{ord } \bar{22} = 2 \xrightarrow{\text{Proprietate 5}} \text{ord } \bar{4}^2 = 2 \cdot 11 = 22$$

$$\boxed{\text{ord } \bar{22} = 22}$$

Exercițiu ușor de rezolvare

Să se arate că toate numerele prime  $p_{12}$  a.s.  $5p_2 | a^{5p_2} - a$  și  $5 < p_2 < 2$

$$5 \mid 2^{5p_2} - 2 \Rightarrow 2(2^{5p_2-1} - 1) \Rightarrow 5 \mid 2^{5p_2-1} - 1$$

Care este  $\text{ord } \bar{2}$  în  $U(\mathbb{Z}_{5})$

$$\bar{2}^2 \neq \bar{1} \quad \text{ord } \bar{2} = 4$$

$$\bar{2}^{(5p_2-1)} = \bar{1}$$

Proprietate 2)  $g^n = e \Rightarrow \text{ord } g | n$

$$\Rightarrow 4 \mid 5p_2 - 1 \Rightarrow 4 \nmid -$$

$$4 \mid p_2 - 1 \quad \text{I conditie}$$

Algo  $a \in \{1, 2, \dots, p-1\}$  a.s. ord  $\bar{a} = p-1$

$$p \mid 5p_2 \mid a(a^{5p_2-1}-1) \Rightarrow p \nmid a \Rightarrow p \mid a^{5p_2-1}-1$$

$$\overline{a^{5p_2-1}} = \overline{1} \text{ m } U(\mathbb{Z}_p)$$

$$\text{Follows Prop 2} \Rightarrow p-1 \mid 5p_2 - 1$$

$$g^m \equiv 1 \Rightarrow \text{ord } g \mid m$$

$$\text{Analog demonstrate } 2-1 \mid 5p_2 - 1$$

Algo  $b \in \{1, 2, \dots, 2-1\}$  a.s. ord  $\bar{b} = 2-1$  m  $U(\mathbb{Z}_2)$

$$b^{5p_2-1} = \overline{1} \text{ m } U(\mathbb{Z}_p) \xrightarrow{\text{Prop 2}} 2-1 \mid 5p_2 - 1$$

$$\Rightarrow 4 \mid 5p_2 - 1$$

$$\begin{array}{c} \boxed{p-1 \mid 5p_2 - 1} \\ \boxed{2-1 \mid 5p_2 - 1} \end{array} \xrightarrow{p-1 \mid 5p_2 - 1} \boxed{5(p-1)_2 + 5_2 - 1} \xrightarrow{\text{divide}} p-1 \mid 5_2 - 1$$

$$\text{Analog } 2-4 \mid 5p-1$$

3 conditie

$$1) 4 \mid p_2 - 1$$

$$2) p-1 \mid 5_2 - 1$$

$$3) 2-1 \mid 5p-1$$

$$\frac{5p-1}{2-1} < \frac{5_2 - 1}{2-1} < 6$$

mt. natural.  $p < 2$

$$\Leftrightarrow 5_2 - 1 < 6_2 - 6 \Leftrightarrow \underline{5 < 2} \Rightarrow$$

$$\frac{5p-1}{2-1} \in \{1, 2, 3, 4, 5\}$$

nd l m e parabola

$$\frac{5p-1}{2-1} \geq 1 \Rightarrow 5p-1 \geq 2-1 \Rightarrow$$

$$\Rightarrow 2 = 5p \quad \text{X} \quad \text{contradictie}$$

$$\frac{5p-1}{2-1} = 5$$

$$5 \mid 4$$

$$5p-1=52-5 \Rightarrow p \in \underline{\text{m.e.n.c.5}} \rightarrow \text{pazde.}$$

m.e.n.c.2 - res. formata

$$\frac{5p-1}{2-1} = 2 \Rightarrow p=29 \\ 2=73$$

$$\text{cauza 3} \quad \frac{5p-1}{2-1} = 3 \Rightarrow 5p-1=32-3 \Rightarrow 2 = \underline{\frac{5p+2}{3}}$$

(n.2) - Folosim  $p-1 \mid 52-1 = 5 \cdot \frac{5p+2}{3} - 1 = \frac{25p+7}{3} \Rightarrow$   
 ○ Duhocuse pe 2  $\Rightarrow$  ~~88~~

$$p-1 \mid 25p+7 \quad \cancel{\underline{25(p-1)+32}}$$

$$\Rightarrow p-1 \mid 32 \quad p-1 \in \{1, 2, 4, 8, 16, 32\} \Rightarrow$$

$$p \in \{2, 3, 5, 8, 17, 33\} \quad \text{m.e.paz}$$

Dar  $p > 5$

$$2 = \frac{84}{3} = 229$$

$$\boxed{p=17 \\ 2=229}$$

verstare cu 7

$$5p-1=42-5 \Rightarrow 2 = \underline{\frac{5p+3}{7}}$$

$$p-1 \mid 52-1 \Rightarrow = 5 \cdot \frac{5p+3}{7} - 1 = \frac{25p+11}{7} \mid 5$$

$$p-1 \mid 25p+11 = 25(p-1) + 36 \Rightarrow$$

$$p-1 \mid 36 \Rightarrow p \in \{1, 2, 3, 6, 12, 9, 18, 36\} \Rightarrow$$

$$p \in \{2, 3, 5, 7, 13, 10, 19, 37\}$$

$p > 5$   $\downarrow$   $\text{e.paz}$   $\downarrow$   $\text{m.e.paz}$

$$5 \mid 5p+3 \Rightarrow 5p+3 \Rightarrow \frac{5 \mid p+3}{p=5t+1} \quad (\downarrow 5 \rightarrow 3 \rightarrow 8 \rightarrow 1)$$

$\frac{5}{10} \text{ fără numere cardinale}$

6-  
c)

$\#$  numere cardinale.

$$\text{Deci } p=37, \text{ și } \frac{5 \cdot 37 + 3}{5} = \frac{185 + 3}{5} = \frac{188}{5} = 37$$

- nu se respectă condiția  $\frac{p}{5} \in \mathbb{N}$

$\frac{5}{10} \text{ păș-1}$

$$37 - 37 - 1 = 37 + 3 - 1 = 37 + 2 \Rightarrow$$

$$\frac{p}{5} \stackrel{4}{2} \Rightarrow \text{restul } 2$$

$$\text{restul } 2 \stackrel{5}{2} \\ = \text{restul } 2$$

$\rightarrow \frac{5}{10} \text{ nu } +2$

nu se respectă condiția

$$\text{Deci } p=13 ; \text{ și } \frac{5 \cdot 13 + 3}{5} = \frac{68}{5} = 13 \Rightarrow \boxed{p=13}, \boxed{s=13}$$

Sunt 3 perechi de nr.  $\begin{cases} p=29 \\ s=73 \end{cases}, \begin{cases} p=17 \\ s=29 \end{cases}, \begin{cases} p=13 \\ s=17 \end{cases}$  Toate!

Definitie - Inel.

A)  $(R, +, \cdot)$  se numește inel dacă:

1)  $(R, +)$  grup comutativ 0-element neutru  $\forall r, s \in R : r + s = s + r =$

2) asociativitate  $(x \cdot (y \cdot z)) = ((x \cdot y) \cdot z), \forall x, y, z \in R$   $= r, \forall r \in R$

3) pre-element neutru  $(\exists) 1 \in R. r \cdot 1 = 1 \cdot r = r \quad \forall r \in R$

$$3) x \cdot (y + z) = x \cdot y + x \cdot z \quad \forall x, y, z \in R$$

$$(x + y) \cdot z = x \cdot z + y \cdot z$$

$R \rightarrow$  multime (inel)

$(Z_n, +, \cdot)$

$$U(R) = \{k \in R \mid \exists s \in R \text{ a.s. } k \cdot s = s \cdot k = 1\}$$

unitate (element inversabil)

$(k, +, \cdot)$  corp dacă: 1)  $(k, +, \cdot)$  inel

$$2) U(k) = k \setminus \{0\}$$

Observații:

1) Deci sunt în inel,  $x \cdot 0 = 0 = 0 \cdot x$  (nu în inel  $\Rightarrow 0 \cdot x \neq x \cdot 0 \quad (\forall x \in R)$ )

Denumirea lui 0 și 1 în corpuri

$$\forall x \in K \quad x \cdot 0 = x + 0 = x \quad \text{distanță} \quad \text{Prop 3} \quad | \quad \text{scop de } x \neq 0$$

2)  $x, y \in K \quad x \cdot y = 0 \Rightarrow x = 0 \text{ sau } y = 0 \quad | \quad \text{nu mulțime cu 2.} \Rightarrow$   
 $x \cdot y = 0$   
 Prezumem că  $x \neq 0$ . Fiecare def. ca  $U(K) = K \setminus \{0\} \Rightarrow$   
 $\exists z \in K \text{ astfel încât } z \cdot x = x \cdot z = 1$   
 $\Rightarrow z(x \cdot y) = z \cdot 0 = 0$

$$0 = z \cdot (x \cdot y) \stackrel{\text{Prop 2}}{=} (z \cdot x) \cdot y = 1 \cdot y = y$$

În  $\mathbb{Z}_2$   $\begin{cases} 2 \cdot 2 = 0 \\ 2 \neq 0 \end{cases}$  O să

Exemplu:  $(\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot), (\mathbb{C}, +, \cdot)$

$(\mathbb{Z}, +, \cdot)$  este nu mulțime, nu este corp.  $a \cdot b = 1 \quad \text{în } \mathbb{Z}$   
 $(A, +, \cdot) \quad U(\mathbb{Z}) = \{ \pm 1 \}$

$(\mathbb{Z}_m, +, \cdot)$  este mulțime, nu este corp?

Ziceți  $\Rightarrow$  nu este

mulțime de polinoame

Luat în  $K$  corp comutativ ( $x \cdot y = y \cdot x, \forall x, y \in K$ )

Deoarece există comutativitate

$K[X] =$  mulțime de polinoame cu coeficienți în corpul  $K$

$$f(x) = a_k x^k + a_{k-1} x^{k-1} + \dots + a_0 \in K[X].$$

$$g(x) = b_n x^n + b_{n-1} x^{n-1} + \dots + b_0 \in K[X]$$

$$f \equiv g \Leftrightarrow \begin{array}{l} K = n \\ a_j = b_j \quad \forall j = 0, n \end{array}$$

Cum se adună 2 polinoame?

$$(f+g)(x) = (a_0 + b_0) + (a_1 + b_1) + \dots$$

$$f(x) = 1 + x + x^2 + x^3 \cdot 0 \quad \mathbb{R}$$

$$g(x) = 2 + 3x + x^3 + 0 \cdot x^2$$

$$\text{Sumă} \quad (f+g)(x) = 3 + 4x + x^2 + x^3$$

$$(f \cdot g)(x) = \sum_{j=0}^{k+m} c_j x^j \quad c_j = \sum_{t+s=j} a_t b_s$$

$$f \cdot g = 2 + \overbrace{5x + 5x^2 + 5x^3 + x^4 + x^5}^{(3x+1+2x)} + x^6 + x^7 + x^8 \quad \mathbb{R}$$

$$2x^2 + 3x^2 \\ 1 - x^3 + 3x^3 = 6x^3$$

grad f = k dacă  $a_k \neq 0$

$$\text{grad}(0) = -\infty$$

$$\underline{\underline{|f(x)|=1 \quad \text{grad } f=0}}$$

$$\text{grad } f \cdot g = \text{grad } f + \text{grad } g \quad -\text{cu coeficienti} \text{ \underline{\underline{intre un corp}}}$$

Rădăcina număr polinom

$$\exists k \text{ astfel că } f(x) = 0$$

$$f(x) = a_k \cdot x^k + \dots + a_1 x + a_0$$

$$\text{Fie } x^3 - x \in \mathbb{K}[x]$$

$$f(0) = 0 \quad \rightarrow \text{nu e rădăcine} \quad (\text{nu e rădăcine})$$

$$f(1) = 0$$

$$f(2) = 8 - 2 = 6 \neq 0$$

$$f(3) = 27 - 3 = 24 \neq 0$$

$$f(4) = 64 - 4 = 60 \neq 0$$

$$f(5) = 125 - 5 = 120 \neq 0$$

$$g(x) = 0$$

$$f \neq g$$

Ce funcții sunt egale ce polinoame sunt egale

Fracție polinomială: coracate sunt egale.

Teorema Nr. de rădăcini în  $\mathbb{K}$  pării în polinomul  $f$  cu gradul  $f \geq 1$  este cel mult  $n$ . (nu nu este egal cu  $n$ ).

$\frac{n}{4}$

$x^3 - x \stackrel{e de}{=} \text{produl } 3$  din  $\mathbb{Z}_6$  cu gradul 3. Gradul = 2 (mod 3), numărătoare;

### Formulele lui Viète

$x_1 x_2 \dots x_m$  roădăcini dintr-o ecuație

$$\text{grad } f(x) = m$$

$$f(x) = a_m x^m + a_{m-1} x^{m-1} + \dots + a_1 x + a_0 \neq 0.$$

— m. denotădăcă coincide cu gradul polinomului,  $m \in \mathbb{N}^*$   $\Rightarrow$  (ceva patru)

$$x_1 + x_2 + \dots + x_m = -\frac{a_{m-1}}{a_m} = -a_{m-1} \cdot \underbrace{(a_m)}_{\text{numărătoare}}^{-1}$$

$$x_1 x_2 + x_1 x_3 + \dots + x_{m-1} x_m = \frac{a_{m-2}}{a_m} \quad \text{numărătoare}$$

$$x_1 x_2 x_3 + \dots = -\frac{a_{m-3}}{a_m} \quad \text{numărătoare}$$

$$x_1 x_2 \dots x_m = \underbrace{(-1)^m}_{a_m} \cdot \underbrace{a_0}_{\text{numărătoare}}$$

### Teorema (fundamentală a algebrei)

Polinom cu coeficienți în  $\mathbb{C}[x]$ , grad  $f = n \Rightarrow$  are  $n$  roădăci complexe. Altă formulă: lui Viète. (se typează cu de multiplicitate).

De exemplu dacă avem  $(x-1)^2(x+1)^3 =$  folosim formulele lui Viète.

$$\text{grad } 5. \quad \begin{matrix} \text{roădăcini} \\ < 1 \\ f(1) \end{matrix} \quad \begin{matrix} \text{rez } 1 \\ \text{rez } 2 \\ \text{rez } 3 \end{matrix}$$

$$\overbrace{1, 1, -1, -1, -1}^{\text{combin.}}.$$

$$= (x-1)^2(x+1) = (x^2 - 2x + 1)(x+1) = x^5 - 2x^3 + x + x^4 - 2x^2 + 1$$

$$= x^5 + x^4 - 2x^3 - 2x^2 + x + 1$$

hypotheticele coeficienți  $x^5$

$$-2 : 1 \Rightarrow -2$$

Sunt roădăcini = -1.

Formule = 2 - 2  $\rightarrow$  produse de cinci 2

$$\sum x_i x_j = (-2)^{-3 + 2 + 1} = -2 \quad \text{correct!}$$

Exemplu:  $x^2 - 2 \in \mathbb{Q}[x] \rightarrow$  nu are roădăcini în  $\mathbb{Q}$

$$\pm \sqrt{2} \quad \text{în } \mathbb{R}[x]$$

roădăcini

$x^2 + 1 \in \mathbb{R}[x] \rightarrow$  nu are roădăzile în  $\mathbb{R}$   
 $\pm i$  în  $\mathbb{C}$ .  
 nu sunt reale

Exemplu  
 $x^2 + 1$  - nu are roădăzile în  $\mathbb{R}$

$$f(x) = x^2 + 1 = (x^2 + 1)^2 - 2x^2 = (x^2 + 1 + \sqrt{2}x)(x^2 + 1 - \sqrt{2}x)$$

$\forall x \in \mathbb{R} \quad f(x) = x^2 + 1 \geq 1 > 0$  nu are roădăzile.

Are roădăzile complexe.

$\begin{matrix} 2 & 1 & 3 \\ 2 & 2 \end{matrix} \rightarrow$  grad 1 are roădăzile  $ax + b$  unde  $a \neq 0$   
 Atunci suntem ceva mai departe de grad 2  
 și putem avea și roădăzile complexe cu coeficienți complexi.

$f(x) = x^4 + x^3 + x^2 + 2023x + 2023$  care roădăzile reale ale  $f$ ?

Roădăzile complexe sunt ca formulele lui Viète să fie astfel că nu sunt roădăzile reale

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = (x_1 + x_2 + x_3 + x_4)^2 - 2 \sum_{i < j} x_i x_j =$$

Din formulele lui Viète

$$x_1 + x_2 + x_3 + x_4 = -1$$

$$x_1 x_2 + x_1 x_3 + \dots + x_3 x_4 = 1$$

$$-1 - 2 - 1 < 0 \Rightarrow$$

Nu există roădăzile reale.

Să căutăm  $f \in \mathbb{R}[x]$ ,  $\lambda \in \mathbb{C} \setminus \mathbb{R}$

$$\underbrace{\begin{array}{l} f(\lambda) = 0 \rightarrow f(\bar{\lambda}) = 0 \\ \lambda \end{array}}_{\text{(conjugat)}} \quad$$

$$a_k \bar{\lambda}^k + a_{k-1} \bar{\lambda}^{k-1} + \dots + a_1 \bar{\lambda} + a_0 = 0$$

$$\overline{a_k \lambda^k + \dots + a_1 \lambda + a_0} = 0$$

conjugatul lui 0 este 0

$$\overline{x+y} = \bar{x} + \bar{y}$$

$$\overline{x \cdot y} = \bar{x} \cdot \bar{y}$$

$$\lambda = a + bi \quad a, b \in \mathbb{R}$$

$$\bar{\lambda} = a - bi \quad (\text{conjugatul lui } \lambda)$$

$\alpha \neq \bar{\alpha}$

$\alpha \in \mathbb{C} \setminus \mathbb{R} \Leftrightarrow \text{Re } \alpha \neq 0$

$\alpha \neq \bar{\alpha}$

$\alpha \neq -\bar{\alpha}$

-11-  
es

- 2 complexe reale, 2 reale

Proprietatea  $f$  cont  $f(c) \cdot f(d)$  negativ  $\Rightarrow$   $f$  un elev. c.c.

$f \geq 0$

2 m. reale între care se află nodul de pe axa.

$$f(-1) = 2 > 0$$

$$f(-2) = 16 - 8 + 4 - 50/16 + 2024 < 0$$

Dacă val. c.c.  $f \leq 0$

$\exists (J) x_0 \in (-2, -1)$  a.s.  $f(x_0) = 0$ .

- Alt interval. m.c.e. -

$$f(-\infty) = +\infty$$

nu crește și nu scade în  $(-\infty, -2]$ .

Truncare

$$x^4 + T \in \mathbb{Z}_{13}[x]$$

(close de 1)

Descompunem ca produs de 2 polini de grad 2

$$(x^2 + \bar{c}x + b)(x^2 + \bar{c}x + d)$$

$$T = -\bar{a}^2$$

$$\text{Scrim c.c. p.t. că } x^4 + T = x^4 - \bar{a}^2$$

$$= (x^2 - \bar{a})(x^2 + \bar{a})$$

$$-T = \bar{a}^2 = \bar{5}^2 = 25 = -1 \text{ în } \mathbb{Z}_{13}$$

$$T = -25 \quad 25 = 2 \cdot 13 \quad \frac{x^4 + T}{x^4 - 5^2} = x^4 - 5^2$$

$$(x^2 + 5)(x^2 - 5) = x^4 + T \text{ în } \mathbb{Z}_{13} \text{ scor}$$

În  $\mathbb{Z}_{11}[x]$  se scriu 25 reale

$T \neq \bar{a}^2$  în  $\mathbb{Z}_{11}$  De ce nu e posibil?

Prin deosebită proprietatea lui  $\mathbb{Z}_{13}$

482 587  
47 57  
46 56

$$\text{Def of } f \text{ egibt } -\bar{t} = \bar{a}^2 = \bar{a}^{12} = (\bar{a}^5)^2$$

482

$$Z_{11}(x) \quad -\bar{t} = \bar{t} \quad \text{M.T.F.} \quad \times$$

Möglichkeit um ein Faktor zu R

$$f(x) = (x^2 - \bar{t})^2 + 2x^2 = (x^2 - \bar{t})^2 - 3 \cdot x^2 = (x^2 - \bar{t} + 3x) \cdot$$

$$\begin{aligned} & x^2 + 1 \\ & \bar{t} = -9 \quad \text{in } Z_{11} \text{ (ader)} \end{aligned}$$

$x^2 = 2x^2 + 1 + 2x^2$

$\frac{4}{3}x^2$

$$\int \underbrace{(x^2 - \bar{t} - 3x)}_{\text{produkt}} \text{d}x$$

~~adefaktore~~

~~adefaktore~~

Test 3

-13

Ibioring = 83

(1) Să se arate că dacă  $x \in S_{(1, \dots, 8)}$  atunci  $2^x = 31$  în  $\mathbb{U}(\mathbb{Z}_{83})$

2) Să se arate că dacă  $x^5 + 1$  este divizor de grad 2 al lui  $x^5 + 1$  în  $\mathbb{Z}_{101}$ .

(3) Să se arate că există 2 polinoame de grad 2 fără găsi

$$f \cdot g = x^5 + 1 \text{ în } \mathbb{Z}_{83}[x].$$

4) Să se arate că există un polinomul  $x^5 + x^3 + x^2 + x + 1$  în corpul  $\mathbb{Z}_{71}$ .

Răspuns:

$$\textcircled{1} \quad 2^x = 31 \mid .8$$

$$2^{x+3} = \cancel{2^{58}} = -1 \cdot \cancel{2} \quad \text{ridică la patrat}$$

ord 2 în grup

$$2^{2x+6} = 1$$

ord 2 în  $\mathbb{Z}_{83}$

$$\mathbb{Z}_{83}.$$

$$\text{Ad 2} = 82$$

$$2x+6 = 82$$

$$2x = 76$$

$$\boxed{x = 38}$$

$$\text{Dacă } x+3=51$$

$$\boxed{x = 38}$$

(2)  $x^5 + 1$  este divizor de grad 2 al lui  $x^5 + 1$  în  $\mathbb{Z}_{101}$

Pretezumem că  $\exists x \in \{1, 2, \dots, 100\}$  astfel că  $x^5 = -1 \Rightarrow$

$$\cancel{x^5} = 1$$

ord  $x$  în  $\mathbb{U}(\mathbb{Z}_{101})$

$$\cancel{\text{ord } x = 8}$$

$$|\mathbb{U}(\mathbb{Z}_{101})| = 100$$

$$8 \nmid 100$$

Contradicție

Contradicție

$$(3) \quad x^5 + 1 = (x^2 + 1)^2 - 2x^2 = (x^2 + 1)^2 - (7x)^2 = (x^2 + 1 + 7x)(x^2 + 1 - 7x)$$

$$2 = 2 + 5 = 59 = 7^2$$

$$(x^2 + 1 - 7x)$$

(4) Arătați că  $x^5 + x^3 + x^2 + x + 1$  este divizor de grad 2 al lui  $x^5 - 1$  în  $\mathbb{Z}_{71}$ .

$$x^5 - 1$$

$$x^5 + x^3 + x^2 + x + 1 = 0 \quad | \cdot (x - 1)$$

$$x^5 - T = 0$$

Anătudină  $L^{14}$ ; să se dă o formă

$$x^5 = T \quad \text{Ce mă putere a 5-ă a da } L?$$

$$\frac{x^5}{T} = 1 \quad \text{dacă } x \neq 0 \quad \text{nu } \exists x_1$$

$$\frac{x^5}{T} = 5 \cdot 14$$

$$\frac{2^{14}}{2^5} \cdot \left(\frac{2^5}{2}\right)^5 = 2^{70} = 1$$

$$\text{nu } \exists x_1 \quad 2^{14} \cdot (2^7)^2 = 128 = (-14)^2$$

$$\text{șoarecă } \frac{196}{5^4} = 196 = 5^4$$

$$\frac{5^4}{5^4} \cdot \frac{5}{5} = 25, \quad \frac{5^4}{5^4}$$

$$x^5 = 1 \Rightarrow x^{10} = 1$$

nu există soluție și  $5^5 = 3125$

$$(x^5)^5 = 1$$

$$\frac{125}{71} \mid 71$$

$$71 = 5 \cdot 5 = 25$$

$$57 = -15$$

$$\begin{array}{r} 128 \\ \hline 71 & 1 \\ \hline 57 & \\ \text{rest} & \end{array}$$

$$57 = -15 \quad \frac{71}{15}$$

$$\begin{array}{r} 196 \\ \hline 152 & 12 \\ \hline 204 & \\ \hline 52 & \\ \hline 216 & \\ \hline 270 & \\ \hline 256 & \\ \hline 14 & \\ \hline \end{array}$$

$$\begin{array}{r} 256 \\ \hline 205 & 51 \\ \hline 270 & \\ \hline 256 & \\ \hline 14 & \\ \hline \end{array}$$

$$\begin{array}{r} 270 \\ \hline 213 & 3 \\ \hline 57 & \\ \hline 0 & \\ \hline \end{array}$$

Exemplu - 2 h 18' 30 min.

$$\begin{array}{r} 3700 \rightarrow 90000 \text{ metrii distanță} \\ \text{Master} \rightarrow \text{solo AS mediu} \end{array}$$

$$9 \frac{\infty}{\infty} ; 11 \frac{\infty}{\infty}; 11 \frac{30}{11} \frac{14}{14} \rightarrow 12 \frac{\infty}{\infty} V$$

- în metri și turn

- exponență

consultativ

Test

$$\text{Găsim 2 polinome de grad 2 f și g astfel încât } f \cdot g = x^4 + 1 \text{ din } \mathbb{Z}_{37}[x]$$

$$\textcircled{3} \quad x^4 + 1 = (x^2 + 1)^2 - 2 \cdot x^2 = (x^2 + 1)^2 - 4g \cdot x^2 = (x^2 + 1 - 4x) \cdot$$

$$(x^2 + 1 + 4x)$$

$$\text{din } \mathbb{Z}_{37}[x]$$

$$\checkmark \cdot (x^2 + \overline{1} + \overline{7}x)$$

$$f = x^2 - \frac{4x+1}{x^2+4x+1}$$

U.S. GOVERNMENT

$$\textcircled{2} \quad \frac{\text{Gravity neglectable and } x^4 + 1 \text{ on } K_{1016}}{\frac{25}{2} = 2 \cdot 2 \cdot 2 = \overline{512} \cdot \overline{512} \cdot \overline{128} =}$$

$$= \cancel{49} \cdot \cancel{27} = \cancel{1323} = 10$$

$$\left(\frac{99}{99}\right)^{25} = \left(-\frac{1}{2}\right)^{25} = -\frac{1}{2^{25}} = -\frac{1}{32768}$$

$$x^4 + 1 = x^4 - 100 = (x^2 - 10)(x^2 + 10)$$

① Ganzes Feld mit  $x \in [9, 81]$  und  $\overline{2}^x = \overline{31}$  muß  $(K_{83})$ .

$$\sqrt{31} \cdot \sqrt{8} = \sqrt{248} = \sqrt{249} - 1 = \sqrt{83} \cdot \sqrt{3} - 1 = -1 \Rightarrow \sqrt{31}^{-1} = -\frac{1}{8}$$

$$\checkmark \quad 2^x \cdot (-8) = 1 \Rightarrow 2^x \cdot (-2^3) = 1 \Rightarrow -2^{x+3} = 1$$

$\text{ord}_2 | 82 \Rightarrow \text{ord}_2 \in \{1, 82\}$

$$\frac{-1}{2^{11}} = \left(2^{10}\right)^{\frac{1}{11}} \cdot 2 = -1$$

$$2^{x+3} = -1 \Rightarrow x+3 = 71 \Rightarrow x = 38$$

