DEF.: $a, b \in \mathbb{Z}$. Čísla a, b nazvu NESOUDĚLNÁ, jestliže $(a,b)=1$.

TEDY 1 je nesoudělná s čímkoli!

1. CVIKO:
- soustava kongruencí
- a^c
- $\varphi(n)$
- $[a]_m^{-1}$
- řád a mod m

3 24-19:55

2. CVIČENÍ:
- Rozhodněte, zda $(G, \cdot)$ je ...
- 21 - uvedte příklad
- tabulka
- podgrupa: - generování

3. CVIČENÍ
- př. 42
  inverze vs. inverzní permutace
- n-té odmocniny z 1.

3 24-20:03

(1) $14^{14^{14}}$ (př. 16.2)

14^{14} určete poslední dvě cifry $\rightarrow$ zbytek po dělení 100

EV: $a^{\varphi(m)} = 1 \pmod m$, $(a,m)=1$

$\varphi(100) = \varphi(4 \cdot 25) = \varphi(2^2 \cdot 5^2) = 2 \cdot (2-1) 5 (5-1) = 40$

$14^{14^{14}} \pmod{100} \neq (14^{14})^{14}$, $= 14^{14 \cdot 14}$

$\varphi(100)$

$14^{14} \pmod{40}$

$\varphi(40) = \varphi(5 \cdot 2^3) = 4 \cdot 4 = 16$

$14^{14^{14}} = 2^{14^{14}} \cdot 7^{14^{14}} \pmod{100}$

3 24-20:08

$14^{14^{14}} \pmod{100}$

$2^{14^{14}} \cdot 7^{14^{14}} = ? \pmod{25}$ (1)

$2^{14^{14}} \cdot 7^{14^{14}} = ? \pmod 4$

(1) $2^{14^{14}} \pmod{25}$

EV: $14^{14} \pmod{20}$, $\varphi(25) = 4 \cdot 5 = 20$

$2^{14} \cdot 7^{14} \pmod{20}$

$\downarrow$ $\begin{cases} 2^{14} \cdot 7^{14} \pmod 4 \\ 2^{14} \cdot 7^{14} \pmod 5 \end{cases}$

3 24-20:17

$7^{9^9} \pmod{100}$

$(7, 100) = 1 \Rightarrow$ EV $\varphi(100) = 40$

$7^{\varphi(100)} = 1 \pmod{100}$

$\Rightarrow 9^9 \bmod (\varphi(100))$, $\varphi(100) = 4$, $(9, 40) = 1$

$\Rightarrow 9^{\varphi(40)} \equiv 1 \pmod{40}$, $\varphi(40) = 16$

$9^{16} \equiv 1 \pmod{40}$

$\Rightarrow 9^9 \equiv (9^3)^3 \equiv (81 \cdot 9)^3 \equiv (1 \cdot 9)^3 \equiv 9^3 = 1 \cdot 9 = 9 \pmod{40}$

$9^9 \bmod 40 \equiv 9$

$7^9 \equiv ? \pmod{100}$

$(7^3)^3 \equiv (49 \cdot 7)^3 \equiv (343)^3 \equiv (43)^3 \equiv 07 \pmod{100}$

3 24-20:24

GRUPY

$e_G \cdot a = a \cdot e_G = a$ neutr.

$\rightarrow$ konstanta!

$a \cdot a^{-1} = a^{-1} \cdot a = e_G$ inverze.

TABULKA:

komutativita $\Rightarrow$ symetrická tabulka

$\cdot$	a	b	c
a	a	b	c
b	b	a	c
c	c	c	b

b je neutr.

ZNÁMÉ: $a \cdot a = b$, $ab = a$, ac, ba, ca

CHCI: bb 1), bc, cb, cc

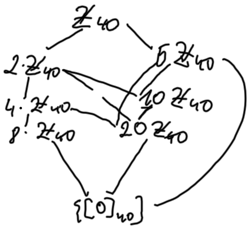
1) $bb = (a \cdot a) b = a \cdot (a \cdot b) = a \cdot a = b$

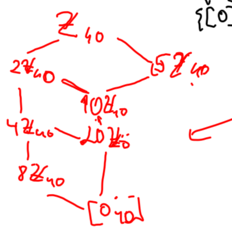
3 24-20:34

PODGRUPY $\mathbb{Z}_{40}$ SVAZ

$40 = 5 \cdot 2^3$

dělitelé: 1, 2, 4, 5, 8, 10, 20, 40





PLATÍ

3 24-20:42

POČET INVERZÍ

1) napíšu perm. do tabulky

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

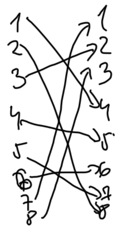
$3+6+1+1+2+3+2+0 =$

$\Rightarrow 17$ inverzí

INVERZNÍ PERMUTACE

$\sigma = ((1457)(283))^{-1} =$

$= (1754)(238)$



počet inverzí = počet průsečíků

3 24-20:53

42.8. určit π: $\sigma \circ \pi = \rho \quad / \sigma^{-1} \circ$

σ, ρ známé, π neznámá

$\underbrace{\sigma^{-1} \circ \sigma}_{id} \circ \pi = \sigma^{-1} \circ \rho$

$\pi = \sigma^{-1} \circ \rho$

3 24-21:00

$(G, \cdot)$ a M ... množina $= \{a_1, \dots, a_n\}$

$\langle M \rangle = \{a_1^{m_1} \cdot \ldots \cdot a_n^{m_n} \,/\,$ různé mocniny$\}$

PŘ 52.1.

$(M) = \{36, 42\}$ v $(\mathbb{Z}, +)$

$\langle M \rangle = \{36 \cdot k + 42 \cdot l \mid k, l \in \mathbb{Z}\} = 6\mathbb{Z}$

nsd$(36, 42) = 6$

Pozn $\mathbb{Z}_{12}^{\times} = \{$invertibilní$\}$

$= \{[1]_{12}, [5]_{12}, [7]_{12}, [11]_{12}\}$

3 24-21:03

39.4

$H = \left\{ \begin{pmatrix} 0 & a \\ a & b \end{pmatrix} \middle| \, a, b \in \mathbb{Q} \right\}$

$A, B \in H$

$A \cdot B^{-1} \in H$

$1_G \overset{?}{\in} H \rightarrow \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \notin H$

není podgrupa

3 24-21:12

39.6

$H = \left\{ \begin{pmatrix} 1 & a \\ a & 1 \end{pmatrix} \middle| \, a \in \mathbb{Q} \right\}$

$A = \begin{pmatrix} 1 & a \\ a & 1 \end{pmatrix} \quad B = \begin{pmatrix} 1 & b \\ b & 1 \end{pmatrix} \quad a, b \in \mathbb{Q}$

$B^{-1} = \begin{pmatrix} 1 & -b \\ -b & 1 \end{pmatrix} \cdot \frac{1}{1-b^2}$

$A \cdot B^{-1} = \begin{pmatrix} 1 & a \\ a & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & -b \\ -b & 1 \end{pmatrix} \cdot \frac{1}{1-b^2} =$

$= \begin{pmatrix} 1-ab & -b+a \\ -b+a & -ab+1 \end{pmatrix} \cdot \frac{1}{1-b^2} =$

$= \begin{pmatrix} \frac{1-ab}{1-b^2} & \frac{-b+a}{1-b^2} \\ \frac{-b+a}{1-b^2} & \frac{-ab+1}{1-b^2} \end{pmatrix} \notin H$

3 24-21:15