4 body

1. Pomocou Euklidovho algoritmu v maticovom tvare nájdite multiplikatívny inverzný prvok ku 31 v $\mathbb{Z}_{36}$.

Riešenie:

$$(36,31) = (31,5)\begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix} = (5,1)\begin{pmatrix}6 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix} = (1,0)\begin{pmatrix}5 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}6 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix} =$$

$$= (1,0)\begin{pmatrix}31 & 5\\ 6 & 1\end{pmatrix}\begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix} = (1,0)\begin{pmatrix}36 & 31\\ 7 & 6\end{pmatrix}$$

$$\begin{pmatrix}36 & 31\\ 7 & 6\end{pmatrix}^{-1} = \begin{pmatrix}-6 & 31\\ 7 & -36\end{pmatrix} \quad \Longrightarrow \quad (-6).36 + 7.31 = 1$$

To znamená, že v $\mathbb{Z}_{36}$ je $31^{-1} = 7$.

Na prednáške bol ukázaný iný spôsob úpravy uvedených matíc

$$(36,31) = (1,0)\begin{pmatrix}5 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}6 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix} \;\Rightarrow\; (1,0) = (36,31)\begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix}^{-1}\begin{pmatrix}6 & 1\\ 1 & 0\end{pmatrix}^{-1}\begin{pmatrix}5 & 1\\ 1 & 0\end{pmatrix}^{-1}$$

Inverzné matice $\begin{pmatrix}n & 1\\ 1 & 0\end{pmatrix}^{-1}$ sa totiž pomocou determinantov počítajú veľmi jednoducho, keďže $\begin{vmatrix}n & 1\\ 1 & 0\end{vmatrix} = -1$. Platí

$$\begin{pmatrix}n & 1\\ 1 & 0\end{pmatrix}^{-1} = \begin{pmatrix}0 & 1\\ 1 & -n\end{pmatrix}.$$

Oba spôsoby sú rovnako výpočtovo náročné. V prvom prípade najskôr násobíme matice a potom hľadáme inverznú maticu k súčinu. Tá sa tiež, ľahko, nájde pomocou determinantov. V druhom prípade najskôr nájdeme inverzné matice a potom musíme spraviť ich súčin.

Bodovanie

- Za správne použitie Euklidovho algoritmu v maticovom tvare sú **2 body**.
- Za správne vypočítanie inverznej matice $\begin{pmatrix}-6 & 31\\ 70 & -36\end{pmatrix}$ je **1 bod**.
- Za správne zapísanie riešenia, v $\mathbb{Z}_{36}$ je $31^{-1} = 7$, je **1 bod**.

3 body ♢

2. Majme množinu $\mathbb{M} = \{0, 1, \ldots, 26\}$ a pre $a, b \in \mathbb{M}$ funkciu $\alpha(x) : \mathbb{M} \to \mathbb{M}$ definovanú predpisom

$$\alpha(x) = ax + b \pmod{27}.$$

Akú podmienku musí spĺňat číslo $a \in \mathbb{M}$, aby bola funkcia $\alpha(x)$ permutáciou na množine $\mathbb{M}$? Koľko takých $a \in \mathbb{M}$ existuje? Vaše tvrdenia zdôvodnite.

Riešenie: nutná a postačujúca podmienka pre číslo $a \in \mathbb{M}$ je

$$\mathbf{gcd}\,(\boldsymbol{a}, \mathbf{27}) = \mathbf{1}\,.$$

To znamená, že číslo a musí byť nesúdeliteľné s číslom 27. Vtedy totiž existuje $a^{-1} \in \mathbb{M}$ a rovnica

$$ax + b = c$$

bude mať práve jedno riešenie pre každé číslo $c \in \mathbb{M}$, t. j. funkcia $\alpha(x) = ax + b$ je permutáciou na množine $\mathbb{M}$.

Počet čísel nesúdeliteľných s číslom 27 sa vypočíta pomocou Eulerovej funkcie

$$\varphi(27) = \varphi\left(3^3\right) = 3^3 - 3^2 = 18.$$

Existuje 18 rôznych čísel $a \in \mathbb{M}$, pre ktoré je funkcia $\alpha(x) = ax + b$ permutáciou na množine $\mathbb{M}$.

Bodovanie ★

- Za uvedenie podmienky pre číslo a je **1 bod**.
- Za správne zdôvodnenie uvedenej podmienky je **1 bod**.
- Za správne vypočítanie a zdôvodnenie počtu rôznych čísel a, pre ktoré je daná funkcia permutáciou na množine $\mathbb{M}$, je **1 bod**.

3 body ♡

3. Nech p, q sú také prvočísla, že $2 < p < q$ a α, β sú také prirodzené čísla, že $\alpha \cdot \beta$ je párne číslo. Vypočítajte hodnotu Jacobiho symbolu $J\left(\frac{p^\alpha}{q^\beta}\right)$.

Riešenie: pre výpočet Jacobiho symbolu platia (okrem iného) tieto dve pravidlá

$$J\left(\frac{ab}{n}\right) = J\left(\frac{a}{n}\right) J\left(\frac{b}{n}\right) \qquad \text{a} \qquad J\left(\frac{c}{mn}\right) = J\left(\frac{c}{m}\right) J\left(\frac{c}{n}\right)$$

Ich aplikáciou potom môžeme písať

$$J\left(\frac{p^\alpha}{q^\beta}\right) = J\left(\frac{p}{q^\beta}\right)^\alpha = J\left(\frac{p}{q}\right)^{\alpha\beta}$$

Podľa zadania sú p, q nepárne prvočísla, takže pre ne platí $\gcd(p, q) = 1$, čo znamená, že $J\left(\frac{p}{q}\right) \neq 0$. Ďalej podľa zadania vieme, že $\alpha \cdot \beta$ je párne číslo, a preto musí platiť

$$J\left(\frac{p^\alpha}{q^\beta}\right) = 1\,.$$

Bodovanie ★

- Za „vytiahnutie“ exponentov α a β z daného Jacobiho symbolu je **1 bod**.
- Za zdôvodnenie toho, že platí $J\left(\frac{p}{q}\right) \in \{-1, 1\}$ je **1 bod**.
- Za aplikáciu párnosti $\alpha \cdot \beta$ a výpočet daného Jacobiho symbolu je **1 bod**.

12 bodov ♠

4. Nájdite všetky riešenia kongruencie

$$x^2 \equiv 5 \pmod{4741}$$

na množine $\mathbb{Z}_{4741}$. Číslo 4741 je súčinom dvoch prvočísel.
Veľké mocniny musia byť počítané pomocou *squaring algoritmu.*
Multiplikatívne inverzné prvky môžete počítať ľubovoľným spôsobom.

Riešenie: si rozdelíme do niekoľkých krokov.

1. Najskôr si musíme rozložiť číslo 4741 na súčin prvočísel. Je zrejmé, že čísla 2, 3 a 5 toto číslo nedelia. Vyskúšaním rýchlo zistíme, že ani 7 nie je jeho deliteľom, avšak číslo 11 je deliteľom čísla 4741. Rozklad je $4741 = 11.431$.
   Poznámka: ak niekto pozná kritérium deliteľnosti jedenástimi

   > *Jedenástkou sú deliteľné čísla, ktorých rozdiel súčtov párnych a nepárnych cifier je deliteľný jedenástkou.*

   tak má rozklad hneď, aj bez skúšania.

2. Takže musíme riešiť sústavu kvadratických kongruencií

$$x^2 \equiv 5 \pmod{11} \qquad \text{a} \qquad x^2 \equiv 5 \pmod{431}$$

   Riešenie prvej z nich dostaneme rýchlo aj tabuľkou (vyskúšaním možností). Na nájdenie riešenia stačí skúsiť čísla $\{2, 3, 4\}$. Riešenia prvej kongruencie sú

$$x^2 \equiv 5 \pmod{11} = \begin{cases} 4 \\ 7 \quad (= -4 \pmod{11}) \end{cases}$$

3. Druhá kongruencia bola zvolená tak, aby sa jej riešenie pomocou tabuľky (skúšaním) nedalo stihnúť. Treba si ale všimnúť, že číslo 431 je Gaussovo prvočíslo, čiže $431 \equiv 3 \pmod 4$. Pre Gaussove prvočísla p vieme na základe Eulerovho kritéria „odmocninu“ čísla a priamo vypočítať podľa vzorca

$$\sqrt{a} = \pm a^{\frac{p+1}{4}} \pmod{p} \quad \text{čiže v našom prípade} \quad \sqrt{5} = \pm 5^{\frac{431+1}{4}} \pmod{431}$$

   Pomocou *squaring algoritmu* budeme počítať mocninu $5^{108} \pmod{431}$. Pseudokód squaring algoritmu je

Squaring algoritmus

VSTUP: x, d, n, kde binárny zápis čísla d je $b_{w-1}b_{w-2}\dots b_1b_0$ a $b_i \in \{0,1\}$
VÝSTUP: $R \equiv x^d \pmod n$

```
s = 1;
for i = w − 1, ..., 0 do
    s := s^2 (mod n);
    if b_i = 1 then
        s := s.x (mod n);
    end
end
R = s
```

Exponent 108 si zapíšeme binárne $108_{10} = 1101100_2$ a realizácia squaring algoritmu je uvedená v nasledujúcej tabuľke

i	6	5	4	3	2	1	0
b_i	1	1	0	1	1	0	0
s	5	125	109	358	354	326	250

Takže dostali sme $5^{108} \pmod{431} = 250$ a $-250 \equiv 181 \pmod{431}$, takže riešenia druhej kongruencie sú

$$x^2 \equiv 5 \pmod{431} = \begin{cases} 181 \\ 250 \end{cases}$$

4. Keď máme všetky 4 riešenia oboch kvadratických kongruencií, tak si zostavíme sústavy lineárnych kongruencií

$$\begin{aligned} x &\equiv a_1 \pmod{11} \\ x &\equiv a_2 \pmod{431} \end{aligned}$$

ktoré budeme riešiť pomocou *Čínskej zvyškovej vety.*
Čísla a_1 a a_2 vyberáme ako všetky možné usporiadané dvojice $(a_1, a_2) \in \mathbb{K}_1 \times \mathbb{K}_2$, kde $\mathbb{K}_1 = \{4, 7\}$ a $\mathbb{K}_2 = \{181, 250\}$. Máme teda 4 možnosti. Z nich stačí vypočítať len 2, pretože ak nájdeme jedno riešenie x_i, tak potom aj $-x_i \pmod{4741}$ je riešením pôvodnej kongruencie.

5. Ak riešenie budeme realizovať pomocou vzorca z vety o Čínskej zvyškovej vete (ČZV), tak si musíme uvedomiť, že hodnoty M_1, M_2 a y_1, y_2 sú pre všetky sústavy rovnaké. Sústavy sa líšia len hodnotami a_1 a a_2. Preto si stačí hodnoty M_1, M_2, y_1, y_2 vypočítať len raz, vypočítať ich súčiny a potom len dosadiť hodnoty a_1 a a_2 do výsledného vzorca. Tieto hodnoty sú

$M_1 = 431$	$y_1 = 431^{-1} = 2^{-1} = 6$	v $\mathbb{Z}_{11}$	$M_1.y_1 = 2586$
$M_2 = 11$	$y_2 = 11^{-1} = 196$	v $\mathbb{Z}_{431}$	$M_2.y_2 = 2156$

6. Hodnotu 11^{-1} v $\mathbb{Z}_{431}$ vypočítame pomocou rozšíreného Euklidovho algoritmu. Postup je uvedený v tabuľke

a	b	q	s	t
431	11	39	-5	196
11	2	5	1	-5
2	1	2	0	1
1	0		1	0

7. Vzorec na nájdenie (jediného) riešenia lineárnych kongruencií pomocou ČZV bude

$$x_i = (2586a_1 + 2156a_2) \pmod{4741}$$

Pomocou ČZV budeme riešiť sústavu lineárnych kongruencií (napríklad) pre tieto dve usporiadané dvojice $(a_1, a_2) \in \{(4, 181), (4, 250)\}$. Riešenia sú

- $\underline{(a_1, a_2) = (4, 181)}$

$$x_1 = 2336 \implies x_2 = -2336 \pmod{4741} = 2405$$

- $\underline{(a_1, a_2) = (4, 250)}$

$$x_3 = 4129 \implies x_4 = -4129 \pmod{4741} = 612$$

Všetky 4 riešenia pôvodnej kongruencie, usporiadané podľa veľkosti, sú $\{612, 2336, 2405, 4129\}$.

Bodovanie

1. Za rozklad čísla 4741 je **1 bod**.
2. Za zápis sústavy kvadratických kongruencií a nájdenie odmocniny čísla 5 v $\mathbb{Z}_{11}$ je **1 bod**.
3. Za výpočet odmocniny čísla 5 v $\mathbb{Z}_{431}$ sú **3 body**.
4. Za zostavenie všetkých štyroch sústav lineárnych kongruencií sú **2 body**.
5. Za výpočet hodnôt M_1, M_2, y_1, y_2 z ČZV sú **2 body**.
6. Za výpočet 11^{-1} v $\mathbb{Z}_{431}$ sú **2 body**.
7. Za výpočet všetkých štyroch riešení dosadením do vzorca je **1 bod**.

Ak bude mať študent správne 1. bod a celý ďalší postup riešenia, avšak bude mať nesprávne výsledky v dôsledku nejakej numerickej chyby, tak dostane celkovo 9 bodov.

3 body ♣

5. Vypočítajte hodnotu $J\left(\frac{1040}{2367}\right)$ bez rozkladu čísla 2367 na súčin mocnín prvočísel.

Riešenie:

$$J\left(\frac{1040}{2367}\right) = J\left(\frac{2^4}{2367}\right) J\left(\frac{65}{2367}\right) = \underbrace{\left(J\left(\frac{2}{2367}\right)\right)^4}_{=1} J\left(\frac{2367}{65}\right) \underbrace{(-1)^{\frac{64.2366}{4}}}_{=1} =$$

$$= J\left(\frac{27}{65}\right) = J\left(\frac{65}{27}\right) \underbrace{(-1)^{\frac{26.64}{4}}}_{=1} = J\left(\frac{11}{27}\right) = J\left(\frac{27}{11}\right) \underbrace{(-1)^{\frac{10.26}{4}}}_{=-1} =$$

$$= -J\left(\frac{5}{11}\right) = -J\left(\frac{11}{5}\right) \underbrace{(-1)^{\frac{4.10}{4}}}_{=1} = -J\left(\frac{1}{5}\right) = -1$$

Pri úpravách sa použili len pravidlá

- ▷ $J\left(\frac{m}{n}\right) = J\left(\frac{n}{m}\right)(-1)^{\frac{(m-1)(n-1)}{4}}$
- ▷ ak $a \equiv b \pmod{n}$, tak $J\left(\frac{a}{n}\right) = J\left(\frac{b}{n}\right)$
- ▷ $J\left(\frac{1}{n}\right) = 1$

Bodovanie ★

- Za správnu aplikáciu pravidiel pri výpočte Jacobiho symbolu, čiže správny postup pri jeho výpočte, sú **2 body**.
- Za správny výsledok je **1 bod**. To znamená, že ak je postup správny, ale pri výpočte sa vyskytla numerická chyba, tak sa strhne 1 bod.