2. cvičení: Umocňování v $\mathbb{Z}_n$

Př: Najděte zbytek po dělení 13 z čísla $c = 5^{290}$.

Malá Fermatova věta: Je-li p prvočíslo, $a \neq k \cdot p$, pak $a^{p-1} \equiv 1 \pmod p$.

Zde $13 = p$ prvočís., $a = 5 \neq k \cdot 13$, tedy $5^{12} \equiv 1 \pmod{13}$.

$$c = 5^{290} = 5^{12 \cdot 24 + 2} = (5^{12})^{24} \cdot 5^2 \equiv 1^{24} \cdot 5^2 \equiv 25 \equiv 12 \pmod{13}$$

Př: Spočtěte $c = 31^{57}$ v $\mathbb{Z}_{14}$.

Euler-Fermatova věta: Je-li $\gcd(a,n) = 1$, pak $a^{\varphi(n)} = 1$ v $\mathbb{Z}_n$.

Zde ~~gcdt~~ nejdříve zmenšíme základ modulo $n = 14$

$$c = 31^{57} = \underbrace{31 \cdot \ldots \cdot 31}_{57 \text{ krát}} = \underbrace{3 \cdot \ldots \cdot 3}_{57 \text{ krát}} = 3^{57} \text{ v } \mathbb{Z}_{14}$$

$\gcd(3,14) = 1$ → lze použít E.-F. větu, $\varphi(14) = \varphi(2 \cdot 7) = 1 \cdot 6 = 6$

$3^6 = 1$ v $\mathbb{Z}_{14}$, tj. exponent zmenšíme modulo 6

$$c = 3^{57} = (3^6)^9 \cdot 3^3 = 3^3 = 27 = -1 = 13 \text{ v } \mathbb{Z}_{14}$$

Př: Spočtěte $c = 137^{131}$ v $\mathbb{Z}_{26}$

$$c = 137^{131} = 7^{131} = 7^{k \cdot 12 + 11} = 7^{11} \text{ v } \mathbb{Z}_{26}$$

$\gcd(7,26) = 1$ → lze E.-F., $\varphi(26) = \varphi(2 \cdot 13) = 12$

tj. $7^{12} = 1$ v $\mathbb{Z}_{26}$

Dopočteme algoritmem opak. čtverců

a^b v $\mathbb{Z}_n$: 7^{11} v $\mathbb{Z}_{26}$

$b = 11 = 8 + 2 + 1 = (1011)_2$ binární zápis

↳ X S SX SX, kde X = times $a = 7$ v $\mathbb{Z}_{26}$

S = square v $\mathbb{Z}_{26}$

v $\mathbb{Z}_{26}$		spočtená mocnina: 7°
↓	1	
X	7	7^1
S	$49 = -3$	7^2
S	9	7^4
X	$63 = 11$	7^5
S	$121 = -9$	7^{10}
X	$-63 = -11 = 15$	7^{11}

$$c = 7^{11} = 15 \text{ v } \mathbb{Z}_{26}$$

Př: Spočtěte 4^{21} v $\mathbb{Z}_{14}$

$\gcd(4,14)=2 \longrightarrow$ nelze E.-F.

použijeme opak. čtverce

$b = 21 = 16+4+1 = (1\,0\,1\,0\,1)_2$
$\quad X\,S\,S\,X\,S\,S\,X$, kde X = times $a=4$, S = square

v $\mathbb{Z}_{14}$ $\quad 1 \xrightarrow{X} 4 \xrightarrow{S} 16=2 \xrightarrow{S} 4 \xrightarrow{X} 16=2 \xrightarrow{S} 4 \xrightarrow{S} 16=2 \xrightarrow{X} 8$

Tedy $4^{21}=8$ v $\mathbb{Z}_{14}$.

Př: Spočtěte 3^{-1} a 7^{-1} v $\mathbb{Z}_{54}$.

a^{-1} exist. v $\mathbb{Z}_n$ iff $\gcd(a,n)=1$

$\gcd(3,54)=3 \longrightarrow 3^{-1}$ neex. v $\mathbb{Z}_{54}$

$\gcd(7,54)=1 \longrightarrow 7^{-1}$ exist. v $\mathbb{Z}_{54}$

$\searrow$ lze použ. E.-F. větu: $7^{\varphi(54)}=1$ v $\mathbb{Z}_{54}$

tudíž $7^{\varphi(54)-1}=7^{-1}$

$\varphi(54)=\varphi(2\cdot 3^3)=1\cdot(27-9)=18$

v $\mathbb{Z}_{54}$ $\quad 7^{-1}=7^{17}$ $\quad$ opak. čtverce

$17 = 16+1 = (1\,0\,0\,0\,1)$
$\quad X\,S\,S\,S\,S\,X$

$1 \xrightarrow{X} 7 \xrightarrow{S} 49=-5 \xrightarrow{S} 25 \xrightarrow{S} 625=31 \xrightarrow{S} 961=-11 \rightarrow$
$\xrightarrow{X} -77=31$

tedy $7^{-1}=7^{17}=31$ v $\mathbb{Z}_{54}$

Spočteme 7^{-1} v $\mathbb{Z}_{54}$ ještě jednou rozšíř. Euklid. alg.

$7x = 1$ v $\mathbb{Z}_{54}$, tj. $7x+54y=1$ v $\mathbb{Z}$

$$\left(\begin{array}{cc|c} 1 & 0 & 7 \\ 0 & 1 & 54 \end{array}\right) \sim \left(\begin{array}{cc|c} 1 & 0 & 7 \\ -8 & 1 & -2 \end{array}\right)_{R_2-8R_1} \sim \left(\begin{array}{cc|c} -23 & 3 & 1 \\ \cdot & \cdot & 0 \end{array}\right)^{R_1+3R_2}$$

Tedy: $-23\cdot 7+3\cdot 54=1$ v $\mathbb{Z}$

$7^{-1}=-23=31$ v $\mathbb{Z}_{54}$

Pozn: Výpočet a^{-1} v $\mathbb{Z}_n$ - časová složitost
- opak. čtverce $O(\mathrm{len}(n)^3)$
- rozšíř. Euklid $O(\mathrm{len}(n)^2)$

Grupy $\mathbb{Z}_n^*$ - řády prvků, podgrupy, řešení rovnic $x^k = 1$ v $\mathbb{Z}_n$

Př: Uvažujme grupu $(\mathbb{Z}_{25}^*, \cdot)$

a) Řád grupy a její prvky : $|\mathbb{Z}_{25}^*| = \varphi(25) = 25 - 5 = 20$

$\mathbb{Z}_{25}^* = \{a \in \mathbb{Z}_{25}, 5 + a\}$

b) Určete řád prvku $b = 6$ a použijte ho k výpočtu 6^{57} v $\mathbb{Z}_{25}$.

- možné řády $r \mid 20$, $20 = 2^2 \cdot 5$, tj $r \in \{1, 2, 4, 5, 10, 20\}$

v $\mathbb{Z}_{25}$ $6^2 = 11$, $6^4 = 121 = (-4)$, $6^5 = -24 = 1$ poprvé $\rightarrow r(6) = 5$

pak $6^{57} = 6^{5 \cdot 11 + 2} = 6^2 = 11$

c) Nalezněte generátor grupy $\mathbb{Z}_{25}^*$, pokud existuje

- hledáme prvek a řádu 20

volíme $a \in \mathbb{Z}_{25}^*$ (náhodně) a zkoušíme, zda $a^r \neq 1$ pro řádné $r < 20$, $r \mid 20$.

Zkusíme $a = 2$: $2^2 = 4$, $2^4 = 16 = -9$, $2^5 = 32 = 7$, $2^{10} = 49 = -1$

tudíž $2^{20} = 1$ poprvé, 2 je generátor

pozn: když $a^{10} \neq 1$, tak ani $a^5 \neq 1$, $a^2 \neq 1$,

anebo stačí ověřit, že $a^r \neq 1$ pro max. dělitele 20,

d) Kolik prvků v $\mathbb{Z}_{25}^*$ by posloužilo jako generátor? Jaká je pravděpodobnost, že při náhodné volbě $a \in \mathbb{Z}_{25}^*$ trefíme generátor?

- $\mathbb{Z}_{25}^* = \langle 2 \rangle$, každý prvek je tvaru 2^k, $0 \leq k < 20$.

$$r(2^k) = \frac{r(2)}{\gcd(k, r(2))} = \frac{20}{\gcd(k, 20)} \overset{\text{chci}}{=} 20,$$

tudíž $\gcd(k, 20) = 1$, takových k je $\varphi(20) = 8$

- je 8 možností, jak zvolit generátor,

pravděpodobnost trefy $P = \frac{8}{20} = \frac{2}{5} = 0{,}4$

- další generátory jsou 2^k, k nesoud s 20, např $2^3 = 8$, $2^7 = 7$...

e) Nalezněte vš. prvky řádu 5 v $\mathbb{Z}_{25}^*$

- tvaru $b = 2^k$, kde chceme $r(2^k) = \frac{20}{\gcd(k, 20)} = 5$

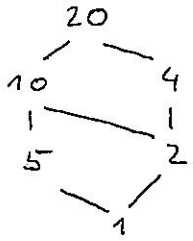
tedy $\gcd(k, 20) = 4$, $k \in \{4, 8, 12, 16\}$

$b_1 = 2^4 = 16$, $b_2 = 2^8 = 6$, $b_3 = 2^{12} = 21$, $b_4 = 2^{16} = 11$

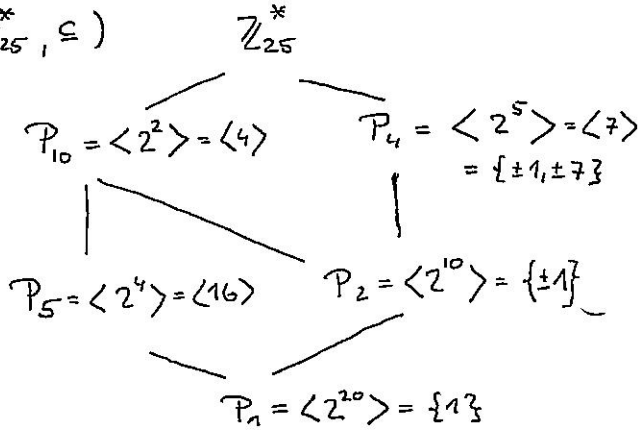
f) Nalezněte vš. podgrupy v $\mathbb{Z}_{25}^*$

- $\mathbb{Z}_{25}^*$ je cyklická grupa řádu $\varphi(25)=20$ s generátorem $a=2$, má tedy pro každou možnou velikost $r \mid 20$ právě jednu r-prvkovou podgrupu $P_r = \langle 2^{\frac{20}{r}} \rangle$ s generátorem $b = 2^{\frac{20}{r}}$ řádu r.
- svaz podgrup v $\mathbb{Z}_{25}^*$ je izomorfní se svazem podgrup v $(\mathbb{Z}_{20}, +)$, anebo se svazem dělitelů čísla 20

$(D_{20}, |)$



(Podgrupy v $\mathbb{Z}_{25}^*$, $\subseteq$)



g) Řešte $x^5 = 1$ v $\mathbb{Z}_{25}^*$

- Protože je $\mathbb{Z}_{25}^*$ cyklická a $5 \mid |\mathbb{Z}_{25}^*|$, jsou vš. řešení v 5-prvkové podgrupě:

$x \in P_5 = \langle 2^4 \rangle = \{\underbrace{16, 16^2 = 6, 16^3 = 21, 16^4 = 11}_{\text{prvky řádu 5}}, \underbrace{16^5 = 1}_{\text{prvek řádu 1}}\}$

h) Řešte $x^8 = 1$ v $\mathbb{Z}_{25}^*$

- Každé řešení $x = a$ splňuje $a^8 = 1$, tj. $r(a) \mid 8$, a také $a \in \mathbb{Z}_{25}^*$, tj. $r(a) \mid |\mathbb{Z}_{25}^*| = 20$.
  Tedy $r(a) \mid \gcd(8, 20) = 4$, $a^4 = 1$.
- Rovnice se redukuje na $x^4 = 1$, kterou řeší $x \in P_4 = \langle 2^5 \rangle = \{\pm 1, \pm 7\}$.

ch) Řešte $x^5 = x$ v $\mathbb{Z}_{25}$.

- v $\mathbb{Z}_{25}^*$ bez nuláků: $x^4 = 1$ a $x \in \{\pm 1, \pm 7\}$
- v $\mathbb{Z}_{25} \setminus \mathbb{Z}_{25}^*$: $x = 0$ je řešení
  $x = 5k$, $1 \le k \le 4$, není řešení: $(5k)^5 = 25 \cdot 5^3 k^5 = 0 \neq 5k$

Tedy $x \in \{0, \pm 1, \pm 7\}$.

Př: Rozhodněte, zda je grupa cyklická. Pokud ano, najděte generátor

a) $\mathbb{Z}_{17}^*$ ∘ $17 = p$ prvočíslo → grupa je cyklická

∘ $|\mathbb{Z}_{17}^*| = \varphi(17) = 16$, $\mathbb{Z}_{17}^* = \mathbb{Z}_{17} \setminus \{0\}$

možné řády $r \mid 16$, $r \in \{1, 2, 4, 8, 16\}$

$a \in \mathbb{Z}_{17}^*$ je generátor iff $a^8 \neq 1$.

zvolíme $a = 2$ $2^4 = -1$, $2^8 = 1$ - není generátor

$a = 3$ $3^4 = 81 = -4$, $3^8 = -1 \neq 1$ - je generátor

$\mathbb{Z}_{17}^* = \langle 3 \rangle$

• řešte $x^2 = 1$ v $\mathbb{Z}_{17}^*$

- protože $\mathbb{Z}_{17}^*$ je cyklická, bude právě $\gcd(2, |\mathbb{Z}_{17}^*|) = 2$ řešení

A ta snadno uhodneme $x = \pm 1$.

• řešte $x^{12} = 1$ v $\mathbb{Z}_{17}^*$

- dílčí cykličnosti grupy bude právě $\gcd(12, |\mathbb{Z}_{17}^*|) = 4$ řešení,

tj. rovnice se redukuje na $x^4 = 1$

Vš. řešení jsou ve 4-prvkové podgrupě

$x \in P_4 = \langle 3^{\frac{16}{4}} \rangle = \langle -4 \rangle = \{\pm 4, \pm 1\}$

Pozn: Našli jsme vš. kořeny polynomu $x^4 - 1$ v tělese $\mathbb{Z}_{17}$.

b) $\mathbb{Z}_{15}^*$ ∘ $|\mathbb{Z}_{15}^*| = \varphi(15) = \varphi(3 \cdot 5) = 2 \cdot 4 = 8$

$\mathbb{Z}_{15}^* = \{a \in \mathbb{Z}_{15},\ 3 \nmid a \text{ ani } 5 \nmid a\} = \{\pm 1, \pm 2, \pm 4, \pm 7\}$

• možné řády $r \mid 8$, $r \in \{1, 2, 4, 8\}$

hledáme generátor, tj. $a^4 \neq 1$

$(\pm 1)^2 = 1$, $(\pm 2)^4 = 16 = 1$, $(\pm 4)^2 = 1$

$(\pm 7)^2 = 49 = 4 \rightarrow (\pm 7)^4 = 16 = 1$

Žádný prvek nemá řád 8, grupa $\mathbb{Z}_{15}^*$ není cyklická.

• řešte $x^2 = 1$

Hrubou silou jsme našli 4 řešení $x \in \{\pm 1, \pm 4\}$,

tedy kvadrát $x^2 - 1$ má 4 kořeny v $\mathbb{Z}_{15}$, což je okruh, nikoli těleso.