Matematická kryptografie – cvičení

1. července 2019

Rovnice v $\mathbb{Z}$ a $\mathbb{Z}_\eta$.

Věta 1. *Nechť $a, b \in \mathbb{Z}$, Nechť EE – algoritmus („Extended Euklid“ – Gaussova eliminace v okruhu $\mathbb{Z}$) z počáteční matice skončí s maticí podle diagramu:*

$$\begin{bmatrix} a & 1 & 0 \\ b & 0 & 1 \end{bmatrix} \xrightarrow{EE} \begin{bmatrix} d & S & T \\ 0 & U & V \end{bmatrix},$$

pak platí:

1. $d = \gcd(a, b)$,
2. $\gcd(a, b) = (S + \lambda U)a + (T + \lambda V)b$, $\lambda \in \mathbb{Z}$, (*Bezoutova rovnost*),
3. $\operatorname{lcm}(a, b) = |Ua| = |Vb| = |UV|\, d$,
4. $\gcd(a, b) \cdot \operatorname{lcm}(a, b) = |ab|$.

Nechť dále $c \in \mathbb{Z}$, pak diofantická rovnice

$$ax + by = c$$

má řešení právě když

$$\gcd(a, b) \mid c,$$

jestliže $\gcd(a, b) \mid c$, pak pro řešení diofantické rovnice platí

$$[x, y] = \frac{c}{d}[S, T] + \lambda[U, V] = \frac{c}{d}[S, T] + \frac{\lambda'}{d}[-b, a],\ \lambda, \lambda' \in \mathbb{Z}.$$

Poznámka 2. Gaussova eliminace v okruhu $\mathbb{K} \in \{\mathbb{Z}, \mathbb{Z}_n\}$ je transformace matice dále uvedenými operacemi:

1. Přičtení $\lambda-$násobku i-tého řádku k j-tému řádku, kde $i \neq j$, $\lambda \in \mathbb{K}$, zápis (λ, i, j).

2. Násobení i-tého řádku invertibilním prvkem $\lambda \in \mathbb{K}^*$, zápis (λ, i).

3. Prohození i-tého a j-tého řádku, zápis (i/j),
operace (i/j) je ekvivalentní posloupnosti operací z předchozích bodů: $(1, j, i)$, $(-1, i, j)$, $(1, j, i)$, $(-1, j)$.

Příklad 3. Stanovte všechna celočíselná řešení rovnice $3x + 5y = 8$.
Ekvivalentní zápis:

$$\begin{bmatrix} x & y \end{bmatrix} \cdot \begin{bmatrix} 3 & 1 & 0 \\ 5 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 8 & x & y \end{bmatrix}$$

Gaussova eliminace v okruhu $(\mathbb{Z}, +, 0, \cdot, 1)$.

$$\begin{bmatrix} 3 & 1 & 0 \\ 5 & 0 & 1 \end{bmatrix}_{(-2,1,2)} \sim \begin{bmatrix} 3 & 1 & 0 \\ -1 & -2 & 1 \end{bmatrix}_{(3,2,1)} \sim \begin{bmatrix} 0 & -5 & 3 \\ -1 & -2 & 1 \end{bmatrix}_{(-1,2)} \sim \begin{bmatrix} 0 & -5 & 3 \\ 1 & 2 & -1 \end{bmatrix}.$$

Rovnice v nové bázi:

$$\begin{bmatrix} x' & y' \end{bmatrix} \cdot \begin{bmatrix} 0 & -5 & 3 \\ 1 & 2 & -1 \end{bmatrix} = \begin{bmatrix} 8 & x & y \end{bmatrix},$$

tedy platí $x' \cdot 0 + y' \cdot 1 = 8$, $\begin{bmatrix} x & y \end{bmatrix} = x' \cdot \begin{bmatrix} -5 & 3 \end{bmatrix} + y' \begin{bmatrix} 2 & -1 \end{bmatrix}$, odtud zřejmě $x' \in \mathbb{Z}$ libovolné, $y' = 8$, tj.

$$\begin{bmatrix} x & y \end{bmatrix} = \begin{bmatrix} 16 & -8 \end{bmatrix} + \lambda \begin{bmatrix} -5 & 3 \end{bmatrix}, \ \lambda \in \mathbb{Z},$$

tj. platí

$$x = 16 - \lambda 5, \ y = -8 + \lambda 3, \ \lambda \in \mathbb{Z}.$$

Existuje nekonečně mnoho řešení uvedené rovnice.

Příklad 4. Stanovte všechna celočíselná řešení rovnice $13x + 15y = 1$.
Ekvivalentní zápis:

$$\begin{bmatrix} x & y \end{bmatrix} \cdot \begin{bmatrix} 13 & 1 & 0 \\ 15 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & x & y \end{bmatrix}$$

Gaussova eliminace v okruhu $(\mathbb{Z}, +, 0, \cdot, 1)$.

$$\begin{bmatrix} 13 & 1 & 0 \\ 15 & 0 & 1 \end{bmatrix}_{(-1,1,2)} \sim \begin{bmatrix} 13 & 1 & 0 \\ 2 & -1 & 1 \end{bmatrix}_{(-6,2,1)} \sim \begin{bmatrix} 1 & 7 & -6 \\ 2 & -1 & 1 \end{bmatrix}_{(-2,1,2)} \sim \begin{bmatrix} 1 & 7 & -6 \\ 0 & -15 & 13 \end{bmatrix}.$$

Rovnice v nové bázi:

$$\begin{bmatrix} x' & y' \end{bmatrix} \cdot \begin{bmatrix} 1 & 7 & -6 \\ 0 & -15 & 13 \end{bmatrix} = \begin{bmatrix} 1 & x & y \end{bmatrix},$$

tedy platí $x' \cdot 1 + y' \cdot 0 = 1$, $\begin{bmatrix} x & y \end{bmatrix} = x' \cdot \begin{bmatrix} 7 & -6 \end{bmatrix} + y' \begin{bmatrix} -15 & 13 \end{bmatrix}$, odtud zřejmě $x' = 1$, $y' \in \mathbb{Z}$ libovolné, tj.

$$\begin{bmatrix} x & y \end{bmatrix} = \begin{bmatrix} 7 & -6 \end{bmatrix} + \lambda \begin{bmatrix} 15 & -13 \end{bmatrix}, \ \lambda \in \mathbb{Z},$$

tj. platí

$$x = 7 + \lambda 15, \ y = -6 - \lambda 13, \ \lambda \in \mathbb{Z}.$$

Existuje nekonečně mnoho řešení uvedené rovnice.

Příklad 5. Stanovte všechna celočíselná řešení rovnice $9x + 6y = 42$.
Ekvivalentní zápis:

$$\begin{bmatrix} x & y \end{bmatrix} \cdot \begin{bmatrix} 9 & 1 & 0 \\ 6 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 42 & x & y \end{bmatrix}$$

Gaussova eliminace v okruhu $(\mathbb{Z}, +, 0, \cdot, 1)$.

$$\begin{bmatrix} 9 & 1 & 0 \\ 6 & 0 & 1 \end{bmatrix}_{(-1,2,1)} \sim \begin{bmatrix} 3 & 1 & -1 \\ 6 & 0 & 1 \end{bmatrix}_{(-2,1,2)} \sim \begin{bmatrix} 3 & 1 & -1 \\ 0 & -2 & 3 \end{bmatrix}.$$

Rovnice v nové bázi:

$$\begin{bmatrix} x' & y' \end{bmatrix} \cdot \begin{bmatrix} 3 & 1 & -1 \\ 0 & -2 & 3 \end{bmatrix} = \begin{bmatrix} 42 & x & y \end{bmatrix},$$

tedy platí $x' \cdot 3 + y' \cdot 0 = 42$, $\begin{bmatrix} x & y \end{bmatrix} = x' \cdot \begin{bmatrix} 1 & -1 \end{bmatrix} + y' \begin{bmatrix} -2 & 3 \end{bmatrix}$, odtud zřejmě $x' = 14$, $y' \in \mathbb{Z}$ libovolné, tj.

$$\begin{bmatrix} x & y \end{bmatrix} = \begin{bmatrix} 14 & -14 \end{bmatrix} + \lambda \begin{bmatrix} 2 & -3 \end{bmatrix}, \ \lambda \in \mathbb{Z},$$

tj. platí

$$x = 14 + \lambda 2, \ y = -14 - \lambda 3, \ \lambda \in \mathbb{Z}.$$

Existuje nekonečně mnoho řešení uvedené rovnice.

Příklad 6. Stanovte všechna celočíselná řešení rovnice $6x + 21y = 8$.
Ekvivalentní zápis:

$$\begin{bmatrix} x & y \end{bmatrix} \cdot \begin{bmatrix} 6 & 1 & 0 \\ 21 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 8 & x & y \end{bmatrix}$$

Gaussova eliminace v okruhu $(\mathbb{Z}, +, 0, \cdot, 1)$.

$$\begin{bmatrix} 6 & 1 & 0 \\ 21 & 0 & 1 \end{bmatrix}_{(-3,1,2)} \sim \begin{bmatrix} 6 & 1 & 0 \\ 3 & -3 & 1 \end{bmatrix}_{(-2,2,1)} \sim \begin{bmatrix} 0 & 7 & -2 \\ 3 & -3 & 1 \end{bmatrix}_{(1/2)} \sim \begin{bmatrix} 3 & -3 & 1 \\ 0 & 7 & -2 \end{bmatrix}.$$

Rovnice v nové bázi:

$$\begin{bmatrix} x' & y' \end{bmatrix} \cdot \begin{bmatrix} 3 & -3 & 1 \\ 0 & 7 & -2 \end{bmatrix} = \begin{bmatrix} 8 & x & y \end{bmatrix},$$

tedy platí $x' \cdot 3 + y' \cdot 0 = 8$. Tato rovnice však v okruhu $\mathbb{Z}$ nemá řešení, protože $3 \nmid 8$.
Uvedená rovnice nemá řešení.

Příklad 7. Stanovte všechna celočíselná řešení soustavy rovnic

$$\begin{aligned} 3x + 2y + 5z &= 4, \\ 2x + 4y + z &= 2. \end{aligned}$$

Ekvivalentní zápis:

$$\begin{bmatrix} x & y & z \end{bmatrix} \cdot \begin{bmatrix} 3 & 2 & 1 & 0 & 0 \\ 2 & 4 & 0 & 1 & 0 \\ 5 & 1 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 4 & 2 & x & y & z \end{bmatrix}.$$

Gaussova eliminace v okruhu $(\mathbb{Z}, +, 0, \cdot, 1)$.

$$\begin{bmatrix} 3 & 2 & 1 & 0 & 0 \\ 2 & 4 & 0 & 1 & 0 \\ 5 & 1 & 0 & 0 & 1 \end{bmatrix}_{\frac{(-1,2,1)}{(-2,2,3)}} \sim \begin{bmatrix} 1 & -2 & 1 & -1 & 0 \\ 2 & 4 & 0 & 1 & 0 \\ 1 & -7 & 0 & -2 & 1 \end{bmatrix}_{\frac{(-2,1,2)}{(-1,1,3)}} \sim \begin{bmatrix} 1 & -2 & 1 & -1 & 0 \\ 0 & 8 & -2 & 3 & 0 \\ 0 & -5 & -1 & -1 & 1 \end{bmatrix}_{(2,3,2)} \sim$$

$$\begin{bmatrix} 1 & -2 & 1 & -1 & 0 \\ 0 & -2 & -4 & 1 & 2 \\ 0 & -5 & -1 & -1 & 1 \end{bmatrix}_{\frac{(-1,2,1)}{(-2,2,3)}} \sim \begin{bmatrix} 1 & 0 & 5 & -2 & -2 \\ 0 & -2 & -4 & 1 & 2 \\ 0 & -1 & 7 & -3 & -3 \end{bmatrix}_{(-2,3,2)} \sim \begin{bmatrix} 1 & 0 & 5 & -2 & -2 \\ 0 & 0 & -18 & 7 & 8 \\ 0 & -1 & 7 & -3 & -3 \end{bmatrix}_{\frac{(-1,2)}{(-1,3)}} \sim$$

$$\begin{bmatrix} 1 & 0 & 5 & -2 & -2 \\ 0 & 0 & 18 & -7 & -8 \\ 0 & 1 & -7 & 3 & 3 \end{bmatrix}.$$

Rovnice v nové bázi:

$$\begin{bmatrix} x' & y' & z' \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 5 & -2 & -2 \\ 0 & 0 & 18 & -7 & -8 \\ 0 & 1 & -7 & 3 & 3 \end{bmatrix} = \begin{bmatrix} 4 & 2 & x & y & z \end{bmatrix},$$

tedy platí $x' \cdot 1 = 4,\ z' \cdot 1 = 2,\ y' \in \mathbb{Z}$ libovolné. Odtud plyne

$$\begin{bmatrix} x & y & z \end{bmatrix} = 4 \begin{bmatrix} 5 & -2 & -2 \end{bmatrix} + 2 \begin{bmatrix} -7 & 3 & 3 \end{bmatrix} + y' \begin{bmatrix} 18 & -7 & -8 \end{bmatrix},\ y' \in \mathbb{Z}.$$

Existuje nekonečně mnoho řešení uvedené rovnice.

Příklad 8. Stanovte $\gcd(a, b)$ a koeficienty v Bezoutově rovnici $\gcd(a, b) = Sa + Tb$ pro dále uvedené dvojice čísel $a, b \in \mathbb{Z}$.

1. $(a, b) = (221, 119),\ \gcd(a, b) = 17 = -a + 2b = (-1 + \lambda 7)a + (2 - \lambda 13)b,\ \lambda \in \mathbb{Z}.$
   $\begin{bmatrix} 221 & 1 & 0 \\ 119 & 0 & 1 \end{bmatrix} \sim \begin{bmatrix} 119 & 0 & 1 \\ 102 & 1 & -1 \end{bmatrix} \sim \begin{bmatrix} 102 & 1 & -1 \\ 17 & -1 & 2 \end{bmatrix} \sim \begin{bmatrix} 17 & -1 & 2 \\ 0 & 7 & -13 \end{bmatrix},$
2. $(a, b) = (-299, 247),\ \gcd(a, b) = 13 = -5a - 6b = (-5 + \lambda 19)a + (-6 + \lambda 23)b,\ \lambda \in \mathbb{Z}.,$
   $\begin{bmatrix} -299 & 1 & 0 \\ 247 & 0 & 1 \end{bmatrix} \sim \begin{bmatrix} 195 & 1 & 2 \\ 247 & 0 & 1 \end{bmatrix} \sim \begin{bmatrix} 195 & 1 & 2 \\ 52 & -1 & -1 \end{bmatrix} \sim \begin{bmatrix} 39 & 4 & 5 \\ 52 & -1 & -1 \end{bmatrix} \sim \begin{bmatrix} 39 & 4 & 5 \\ 13 & -5 & -6 \end{bmatrix} \sim$
   $\begin{bmatrix} 0 & 19 & 23 \\ 13 & -5 & -6 \end{bmatrix}.$

Příklad 9. (Použití Bezoutovy rovnosti)
Nechť $a, b, c \in \mathbb{Z}$, dokažte, že platí:

$$a|bc \wedge \gcd(a,b) = 1 \Rightarrow a|c.$$

Důkaz. Jestliže $\gcd(a,b) = 1$, potom podle Bezoutovy rovnosti existují čísla $a', b' \in \mathbb{Z}$ taková, že

$$1 = a'a + b'b.$$

Pak platí: $c = (a'a + b'b)c = a'ac + b'bc$. Zřejmě $a|(a'ac + b'bc)$, tj. $a|c$. □

Příklad 10. (Použití Bezoutovy rovnosti)
Nechť $p \in \mathbb{P}$, $a, b \in \mathbb{Z}$, dokažte, že platí:

$$p|ab \Rightarrow p|a \vee p|b.$$

Důkaz. Využijme ekvivalence

$$p|ab \Rightarrow p|a \vee p|b \nRightarrow p|ab \wedge p \nmid a \Rightarrow p|b \nRightarrow p|ab \wedge \gcd(a,p) = 1 \Rightarrow p|b.$$

Stejně jako v příkladu 9 z rovnosti $\gcd(a,p) = 1$ podle Bezoutovy rovnosti existují čísla $a', p' \in \mathbb{Z}$ taková, že

$$1 = a'a + p'p.$$

Pak platí: $b = (a'a + p'p)b = a'ab + p'pb$. Zřejmě $p|(a'ab + p'pb)$, tj. $p|b$. □

Příklad 11. Nechť $a, a', b, b' \in \mathbb{Z}$, pak platí

$$0 \neq \gcd(a,b) = aa' + bb' \Rightarrow \gcd(a',b') = 1,$$
$$1 = aa' + bb' \Rightarrow (\forall x \in \{a, a'\})(\forall y \in \{b, b'\})(\gcd(x,y) = 1).$$

Důkaz.

- Jestliže $d = \gcd(a,b)$, potom $a = \alpha d$, $b = \beta d$ pro nějaké $\alpha, \beta \in \mathbb{Z}$. Odtud zřejmě $d = \alpha da' + \beta db'$. Ze zákona krácení máme $1 = \alpha a' + \beta b'$. Odtud nutně $\gcd(a',b') \mid 1$, tj. $\gcd(a',b') = 1$.
- Jestliže $1 = aa' + bb'$, $x \in \{a, a'\}$, $y \in \{b, b'\}$, pak zřejmě $\gcd(x,y) \mid 1$, tj. $\gcd(x,y) = 1$.

□

Příklad 12. (Použití Bezoutovy rovnosti)
Nechť $a, b, c \in \mathbb{Z}$, dokažte, že platí:

$$\gcd(a,c) = 1 \wedge \gcd(b,c) = 1 \Rightarrow \gcd(ab,c) = 1.$$

Důkaz. Podle Bezoutovy rovnosti existují čísla a', b', c', c'', taková, že

$$1 = a'a + c_1 c,\ 1 = b'b + c_2 c.$$

Pak $1 = (a'a + c_1 c) \cdot (b'b + c_2 c) = a'b'ab + c(a'ac_2 + b'bc_1 + c_1 c_2 c)$. Odtud podle Příkladu 11 dostáváme ihned $\gcd(ab, c) = 1$. □

Poznámka 13. Předchozí příklad lze zobecnit následovně: Nechť $n \in \mathbb{N}^+$, $a_1, ..., a_n, c \in \mathbb{Z}$. Pak platí:

$$\gcd(a_1, c) = 1 \wedge ... \wedge \gcd(a_n, c) = 1 \Rightarrow \gcd(a_1 \cdot ... \cdot a_n, c) = 1.$$

Příklad 14. Ukažte, že platí: Nechť $a, b, c \in \mathbb{Z}$, potom

$$a|c \wedge b|c \wedge \gcd(a, b) = 1 \Rightarrow ab|c.$$

Důkaz. Jestliže $a|c$, $b|c$, pak podle definice lcm platí $\operatorname{lcm}(a, b)|c$. Podle věty 1 platí $\operatorname{lcm}(a, b) \cdot \gcd(a, b) = |ab|$, odtud $|ab|\,|c$, tj. $ab|c$. □

Příklad 15. Ukažte, že platí: Nechť $a, b, c \in \mathbb{Z}$, potom

$$\gcd(ca, cb) = |c| \gcd(a, b) \tag{1}$$

Důkaz. Označme $d := \gcd(a, b)$, $d' := \gcd(ca, cb)$. Odtud $d|a \wedge d|b$, tedy $cd|ca \wedge cd|cb$. Z definice gcd odtud nutně $\underline{cd|d'}$. Bezoutova rovnost pro d dává $d = aa' + bb'$, odtud $cd = caa' + cbb'$, odtud dále $\underline{d'|cd}$. Z podtržených výrazů plyne $d' = |c|\, d$, cbd. □

Příklad 16. Nechť $a, b, \alpha, \beta \in \mathbb{Z}$. Pak platí

$$a\alpha = b\beta \wedge \gcd(\alpha, \beta) = 1 \Rightarrow |a\alpha| = |b\beta| = \operatorname{lcm}(a, b).$$

Důkaz. Označme $\ell := a\alpha = b\beta$,
(1) zřejmě $a|\ell$ & $b|\ell$.
(2) nechť dále $a|t$ & $b|t$, potom $t = aa' = bb'$ pro nějaké $a', b' \in \mathbb{Z}$. Odtud dále plyne:

$$a'\ell = a'a\alpha = t\alpha,\ \text{tj. } \ell|t\alpha,$$
$$b'\ell = b'b\beta = t\beta,\ \text{tj. } \ell|t\beta.$$

Odtud dále ℓ dělí libovolnou lineární (celočíselnou) kombinaci $t\alpha, t\beta$, tj. $\ell|(t\alpha\alpha' + t\beta\beta')$. Protože $\gcd(\alpha, \beta) = 1$, existují takové koeficienty α', β', pro které platí $\alpha\alpha' + \beta\beta' = 1$, odtud $\ell|t$.
Z dokázaných bodů (1), (2) plyne $|\ell| = \operatorname{lcm}(a, b)$. □

Příklad 17. Ukažte, že pro každé $p \in \mathbb{P}^+$ a pro každé $k \in \mathbb{N}$ platí

$$0 < k < p \Rightarrow p \,|\, \binom{p}{k},$$

kde $\binom{p}{k} = \frac{p!}{k!(p-k)!}$.

Důkaz. Zřejmě $p! = \binom{p}{k} \cdot k! \cdot (p-k)!$. Protože $p|p!$, pak $p|\binom{p}{k} \cdot k! \cdot (p-k)!$. Dále zřejmě pro každé $\ell \in \mathbb{Z}$ platí implikace

$$0 < \ell < p \Rightarrow \gcd(\ell, p) = 1,$$

odtud podle Příkladu 12 a následné Poznámky plyne $\gcd(k!, p) = 1$, $\gcd((p-k)!, p) = 1$. Odtud podle Příkladu (9) $p|\binom{p}{k} \cdot k! \cdot (p-k)! \Rightarrow p|\binom{p}{k} \cdot (p-k)! \Rightarrow p|\binom{p}{k}$. □

Příklad 18. Ukažte, že pro $a, b, c \in \mathbb{Z}$ platí

$$\gcd(\gcd(a,b),c) = \gcd(\gcd(a,c),b) = \gcd(\gcd(b,c),a) = \gcd(a,b,c).$$

Připomeňme definici $\gcd(a_1, ..., a_n)$ kde $n \in \mathbb{N}^+$, $a_1, ..., a_n, t \in \mathbb{Z}$. Toto číslo je definováno vztahy:

$$(\forall i \in \{1, ..., n\})(\gcd(a_1, ..., a_n)|a_i), \tag{2}$$
$$(\forall i \in \{1, ..., n\})(t|a_i) \Rightarrow t|\gcd(a_1, ..., a_n).$$

Důkaz. Nechť $d_1 := \gcd(\gcd(a,b),c)$, pak zřejmě $d_1|\gcd(a,b) \wedge d_1|c$, protože $\gcd(a,b)|a$, $\gcd(a,b)|b$, potom $d_1|a$, $d_1|b$, $d_1|c$. Odtud podle (2) $d_1|\gcd(a,b,c)$. Obráceně, z vlastnosti $\gcd(a,b,c)|a$, $\gcd(a,b,c)|b$ plyne $\gcd(a,b,c)|\gcd(a,b)$. Dále $\gcd(a,b,c)|c$, tj $\gcd(a,b,c)|\gcd(\gcd(a,b),c)$, tj. $\gcd(a,b,c)|d_1$. Platí tedy $d_1|\gcd(a,b,c) \wedge \gcd(a,b,c)|d_1$, odtud rovnost $d_1 = \gcd(a,b,c)$.
Obdobně v ostatních případech $d_2 := \gcd(\gcd(a,c),b)$, $d_3 := \gcd(\gcd(b,c),a)$. □

Příklad 19. Ukažte, že pro $a, b, n, n' \in \mathbb{Z}$ platí:

$$a \equiv b \bmod n \wedge n'|n \Rightarrow a \equiv b \bmod n', \tag{3}$$
$$\gcd(n_1, n_2) = 1 \Rightarrow (a \equiv b \bmod n_1 \wedge a \equiv b \bmod n_2 \Leftrightarrow a \equiv b \bmod n_1 n_2), \tag{4}$$
$$a \equiv b \bmod n_1 n_2 \Rightarrow a \equiv b \bmod n_1 \wedge a \equiv b \bmod n_2 \tag{5}$$
$$a \equiv b \bmod n \Rightarrow \gcd(a,n) = \gcd(b,n). \tag{6}$$

Důkaz.

(3) $n|a-b$, $n'|n$, odtud $n'|a-b$, tj. $a \equiv b \bmod n'$

(4) Nechť $a \equiv b \bmod n_1 \wedge a \equiv b \bmod n_2$, tj. $n_1|a-b$, $n_2|a-b$. Protože $\gcd(n_1, n_2) = 1$, podle Příkladu 14 $n_1 n_2|a-b$, tj. $a \equiv b \bmod n_1 n_2$.

(5) Důsledek (3)

(6) Protože $a \equiv b \bmod n$, pak existuje $\lambda \in \mathbb{Z}$ takové, že $a = b + \lambda n$. Pak platí

$$\gcd(a,n) = \gcd(a - \lambda n, n) = \gcd(b,n).$$

□

Příklad 20. Nechť $(K, +, 0, \cdot, 1) \in$ Okr. (K je okruh). Prvek $a \in K$ se nazývá „dělitel nuly okruhu K“, $a \in div_0(K)$, právě když platí

$$a \in div_0(K) \Leftrightarrow a \in K \setminus \{0\} \wedge (\exists b \in K \setminus \{0\})(a \cdot b = 0).$$

Ukažte, že pro prvek a platí zákony krácení právě když je nenulový a není dělitel 0, tj. pro každé $a, x, y \in K$ platí:

$$a \notin div_0(K) \wedge a \neq 0 \Leftrightarrow (\forall x, y \in K)(ax = ay \Rightarrow x = y),$$
$$a \notin div_0(K) \wedge a \neq 0 \Leftrightarrow (\forall x, y \in K)(xa = ya \Rightarrow x = y).$$

Zřejmě stačí ukázat:

$$a \notin div_0(K) \wedge a \neq 0 \Leftrightarrow (\forall b \in K)(ab = 0 \Rightarrow b = 0),$$
$$a \notin div_0(K) \wedge a \neq 0 \Leftrightarrow (\forall b \in K)(ba = 0 \Rightarrow b = 0).$$

Důkaz. (krácení zleva)
[$\Rightarrow$] : Sporem, nechť $a \notin div_0(K)$, $a \neq 0$ a

$$\neg(\forall b \in K)(ab = 0 \Rightarrow b = 0) \models\!\!\models (\exists b \in K)(ab = 0 \wedge b \neq 0).$$

Pak ovšem $a \in div_0(K)$, což znamená spor.
[$\Leftarrow$] : Sporem, nechť

$$(a \in div_0(K) \vee a = 0) \wedge (\forall b \in K)(ab = 0 \Rightarrow b = 0).$$

Protože $1 \in K$, platí podle předpokladu $a \cdot 1 = 0 \Rightarrow 1 = 0$. Odtud nutně $a \neq 0$. Dále jestliže $a \in div_0(K)$, potom existuje b takové, že $ab = 0 \wedge b \neq 0$. Podle předpokladu však $ab = 0 \Rightarrow b = 0$, což vede ke sporu.
Obdobně se dokáže pro krácení zprava □

Lineární rovnice v $\mathbb{Z}_n$

Věta 21. *Nechť $a, b, x \in \mathbb{Z}$, $n \in \mathbb{N}$, $n \geq 2$.*

1. Rovnice v $\mathbb{Z}_n$
$$[a]_n[x]_n = [b]_n \tag{7}$$
má řešení právě když $\gcd(a, n) \mid b$.

2. Jestliže $\gcd(a, n) \mid b$, potom rovnice (7) má právě $d := \gcd(a, n)$ různých řešení, pro které platí
$$[x]_n = [\frac{1}{d}(bS + \lambda n)]_n,\ \lambda \in \{0, 1, \ldots, d-1\}.$$
Koeficient S je libovolný koeficient v Bezoutově rovnosti $\gcd(a, n) = Sa + Tn$.

Věta 22. *Nechť $a, b, x, y \in \mathbb{Z}$, $n \in \mathbb{N}$, $n \geq 2$. $[x]_n$ je řešením rovnice*

$$[a]_n[x]_n = [b]_n$$

v $\mathbb{Z}_n$ právě když x, y je řešením diofantické rovnice

$$ax + my = b$$

v $\mathbb{Z}$.

Příklad 23. Řešte rovnici $6x = 7$ v $\mathbb{Z}_{13}$. Kolik existuje řešení?
Podle věty 22 hledejme všechna řešení diofantické rovnice $6x + 13y = 7$ v $\mathbb{Z}$.

$$\begin{bmatrix} 6 & 1 & 0 \\ 13 & 0 & 1 \end{bmatrix} \sim \begin{bmatrix} 6 & 1 & 0 \\ 1 & -2 & 1 \end{bmatrix} \sim \begin{bmatrix} 0 & 13 & -6 \\ 1 & -2 & 1 \end{bmatrix}$$

Odtud dostaneme

$$\begin{bmatrix} x' & y' \end{bmatrix} \cdot \begin{bmatrix} 0 & 13 & -6 \\ 1 & -2 & 1 \end{bmatrix} = \begin{bmatrix} 7 & x & y \end{bmatrix},$$

tj. $y' = 7$, $x = -2y' + 13x'$, $x' \in \mathbb{Z}$, tj. $x = -14 + 13\lambda$, $\lambda \in \mathbb{Z}$. Odtud podle věty 22

$$[-14 + 13\lambda]_{13} = [-1]_{13} = [12]_{13}$$

je jediné řešení v $\mathbb{Z}_{13}$ zadané rovnice.

Příklad 24. Řešte rovnici $6x = 8$ v $\mathbb{Z}_{14}$. Kolik existuje řešení?
Podle věty 22 hledejme všechna řešení diofantické rovnice $6x + 14y = 8$ v $\mathbb{Z}$.

$$\begin{bmatrix} 6 & 1 & 0 \\ 14 & 0 & 1 \end{bmatrix} \sim \begin{bmatrix} 6 & 1 & 0 \\ 2 & -2 & 1 \end{bmatrix} \sim \begin{bmatrix} 0 & 7 & -3 \\ 2 & -2 & 1 \end{bmatrix}$$

Odtud dostaneme

$$\begin{bmatrix} x' & y' \end{bmatrix} \cdot \begin{bmatrix} 0 & 7 & -3 \\ 2 & -2 & 1 \end{bmatrix} = \begin{bmatrix} 8 & x & y \end{bmatrix},$$

tj. $2y' = 8$, $x = -2y' + 7x'$, $x' \in \mathbb{Z}$, tj. $x = -8 + 7\lambda$, $\lambda \in \mathbb{Z}$. Odtud podle věty 22

$$\{[-8 + 7\lambda]_{14}\} = \{[-1]_{14}, [6]_{14}\}$$

jsou právě dvě různá řešení v $\mathbb{Z}_{14}$ zadané rovnice.

Příklad 25. Řešte rovnici $6x = 14$ v $\mathbb{Z}_{12}$. Kolik existuje řešení?
Podle věty 22 hledejme všechna řešení diofantické rovnice $6x + 12y = 14$ v $\mathbb{Z}$.

$$\begin{bmatrix} 6 & 1 & 0 \\ 12 & 0 & 1 \end{bmatrix} \sim \begin{bmatrix} 6 & 1 & 0 \\ 0 & -2 & 1 \end{bmatrix}$$

Odtud dostaneme

$$\begin{bmatrix} x' & y' \end{bmatrix} \cdot \begin{bmatrix} 6 & 1 & 0 \\ 0 & -2 & 1 \end{bmatrix} = \begin{bmatrix} 14 & x & y \end{bmatrix},$$

tj. $6x' = 14$. Tato rovnice nemá v $\mathbb{Z}$ řešení, nemá proto řešení podle věty 22 ani zadaná rovnice v $\mathbb{Z}_{12}$.

Příklad 26. Řešte rovnici $4x + 6y = 8$ v $\mathbb{Z}_{12}$. Kolik existuje řešení?
Hledejme všechna řešení zadané rovnice Gaussovou eliminací v okruhu $\mathbb{Z}_{12}$.
Ekvivalentní zápis:

$$\begin{bmatrix} x & y \end{bmatrix} \cdot \begin{bmatrix} 4 & 1 & 0 \\ 6 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 8 & x & y \end{bmatrix},$$

Gaussova eliminace v $\mathbb{Z}_{12}$:

$$\begin{bmatrix} 4 & 1 & 0 \\ 6 & 0 & 1 \end{bmatrix}_{(-1,1,2)} \sim \begin{bmatrix} 4 & 1 & 0 \\ 2 & -1 & 1 \end{bmatrix}_{(-2,2,1)} \sim \begin{bmatrix} 0 & 3 & -2 \\ 2 & -1 & 1 \end{bmatrix}.$$

Ekvivalentní soustava v $\mathbb{Z}_{12}$:

$$\begin{bmatrix} x' & y' \end{bmatrix} \cdot \begin{bmatrix} 0 & 3 & -2 \\ 2 & -1 & 1 \end{bmatrix} = \begin{bmatrix} 8 & x & y \end{bmatrix} \tag{8}$$

tj. $2y' = 8,\ x' \in \mathbb{Z}_{12}$

Rovnici $2y' = 8$ řešíme v $\mathbb{Z}_{12}$, rovnice má zřejmě dvě různá řešení

$$y' = 4 + \lambda 6,\ \lambda \in \{0, 1\}.$$

pro dvojici řešení $[x, y]$ dostaneme z (8)

$$\begin{aligned} [x, y] &= x'[3, -2] + (4 + \lambda 6)[-1, 1],\ x' \in \{0, 1, ..., 11\} \\ [x, y] &= [-4, 4] + x'[3, -2] + \lambda[-6, 6], \qquad \lambda \in \{0, 1\} \end{aligned}$$

Změna báze lineárního obalu:

$$\begin{bmatrix} 3 & -2 \\ -6 & 6 \end{bmatrix} \sim \begin{bmatrix} 3 & -2 \\ 0 & 2 \end{bmatrix} \sim \begin{bmatrix} 3 & 0 \\ 0 & 2 \end{bmatrix},$$

pro množinu všech řešení v $\mathbb{Z}_{12}$ tedy platí:

$$[x, y] = [-4, 4] + \mu[3, 0] + \lambda[0, 2],\ \mu \in \{0, 1, 2, 3\},\ \lambda \in \{0, 1, ..., 5\}.$$

Existuje celkem 24 různých řešení zadané rovnice.

Mocniny v $\mathbb{Z}_n$

Definice 27. Nechť $(M, \odot, 1) \in \mathrm{Mon}, m \in \mathbb{N}, x \in M$. Mocniny x^m jsou definovány rekurzivně vztahy:

$$x^0 := 1,\ x^{m+1} := x \odot x^m.$$

Jestliže $(M, \odot, 1, \sim) \in \mathrm{Grp}$, pak definujeme mocninu pro záporný exponent vztahem

$$x^{-m} := (\tilde{x})^m.$$

Nechť $m, n \in \mathbb{Z},\ x, y \in M$. Pak platí (pokud jsou mocniny definovány):
$(x^m)^n = (x^n)^m = x^{m \cdot n}$,
$x^{m+n} = x^m \odot x^n$,
$x \odot y = y \odot x \Rightarrow (x \odot y)^m = x^m \odot y^m$.

Pro výpočet mocnin prvků $x \in \mathbb{Z}_n$ v $\mathbb{Z}_n$ jsou užitečná zobrazení $\mathbb{Z}_n \xrightarrow{X,S} \mathbb{Z}_n$ definovaná v postfixovém zápisu vztahy

$$(t)X = t \odot x,\ (t)S = t \odot t.$$

Příklad 28. Algoritmem „opakovaných čtverců“ vypočtěte následující mocniny:

1. 7^{113} v $\mathbb{Z}_{111}$.
   Protože $111 = 3 \cdot 37$, je $\gcd(7, 111) = 1$, lze užít Eulerovu–Fermatovu větu k redukci exponentu, $113 \bmod \varphi(111) = 113 \bmod 2 \cdot 36 = 41$.
   $41 = 101001_2$, algoritmus opakovaných čtverců $1XSSXSSSX$ dává posloupnost

   $$7, 49, 70, 46, 7, 49, 70, 46,$$

   tedy

   $$7^{113} = 46.$$

2. 391^{368}v $\mathbb{Z}_{345}$. Protože $\gcd(391, 345) = 23$, nelze redukovat exponent pomocí Eulerovy–Fermatovy věty. Lze ovšem vždy redukovat základ, $391 \bmod 345 = 46$.
   $368 = 101110000_2$, algoritmus opakovaných čtverců $1XSSXSXSXSSSS$
   dává posloupnost $46, 161, 115, 207, 230, 23, 138, 92, 253, 276, 322, 69,$ tedy

   $$391^{368} = 69.$$

Čínská věta o zbytcích - izomorfismy $\mathbb{Z}_n \to \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$

Věta 29. *Nechť $k \in \mathbb{N}^+,\ x, a_1, ..., a_k \in \mathbb{Z},\ n_1, ..., n_k \in \mathbb{N}^+,\ i \neq j \Rightarrow \gcd(n_i, n_j) = 1$, potom všechna řešení v $\mathbb{Z}$ soustavy rovnic:*

$$\begin{aligned} x &= a_1 \, mod \, n_1 \\ &\vdots \\ x &= a_k \, mod \, n_k \end{aligned}$$

jsou dána vztahem

$$x = \sum_{i=1}^{k} N_i \widetilde{N}_i a_i + \lambda N,\ \lambda \in \mathbb{Z},$$

kde $N = n_1 \cdot \ldots \cdot n_k,\ N_i n_i = N,\ [N_i]_{n_i}[\widetilde{N}_i]_{n_i} = 1\ v\ \mathbb{Z}_{n_i}$.

Funkce

$$\mathbb{Z}_n \underset{g}{\overset{f}{\rightleftarrows}} \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$$

definované $\forall x, y_1, ..., y_k \in \mathbb{Z}$ *vztahy*

$$\begin{aligned} f([x]_n) &= ([x]_{n_1}, \cdots, [x]_{n_k}) \\ g([y_1]_{n_1}, \cdots, [y_k]_{n_k}) &= [\sum_{i=1}^{k} N_i \widetilde{N}_i y_i]_n \end{aligned}$$

jsou navzájem inverzní izomorfismy okruhů $\mathbb{Z}_n$, $\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$.

Příklad 30. Stanovte všechna řešení $x \in \mathbb{Z}$ soustavy rovnic:

$$\begin{aligned} x &= 1 \bmod 11, \\ x &= 2 \bmod 12, \\ x &= 3 \bmod 13. \end{aligned}$$

Moduly 11, 12, 13, jsou navzájem nesoudělné, lze užít čínskou větu o zbytcích.

$$\begin{array}{llll} x = 1 \bmod 11, & 12 \cdot 13 \cdot \widetilde{N}_1 = 1 \bmod 11, & 1 \cdot 2 \cdot \widetilde{N}_1 = 1 \bmod 11, & \widetilde{N}_1 = 6, \\ x = 2 \bmod 12, & 11 \cdot 13 \cdot \widetilde{N}_2 = 1 \bmod 12, & -1 \cdot 1 \cdot \widetilde{N}_2 = 1 \bmod 12, & \widetilde{N}_2 = -1, \\ x = 3 \bmod 13, & 11 \cdot 12 \cdot \widetilde{N}_3 = 1 \bmod 13, & -2 \cdot (-1) \cdot \widetilde{N}_3 = 1 \bmod 13, & \widetilde{N}_3 = 7. \end{array}$$

Podle zmíněné věty

$$\begin{aligned} x &= 12 \cdot 13 \cdot 6 \cdot 1 + 11 \cdot 13 \cdot (-1) \cdot 2 + 11 \cdot 12 \cdot 7 \cdot 3 + \lambda \cdot 11 \cdot 12 \cdot 13, \\ x &= 1706 + \lambda 1716 = -10 + \lambda 1716,\ \lambda \in \mathbb{Z} \end{aligned}$$

Příklad 31. Stanovte všechna řešení $x \in \mathbb{Z}$ soustavy rovnic:

$$\begin{aligned} x &= 2 \bmod 3, \\ x &= 3 \bmod 7, \\ x &= 2 \bmod 13. \end{aligned}$$

Moduly 3, 7, 13, jsou navzájem nesoudělné, lze užít čínskou větu o zbytcích.

$$\begin{array}{llll} x = 2 \bmod 3, & 7 \cdot 13 \cdot \widetilde{N}_1 = 1 \bmod 3, & 1 \cdot 1 \cdot \widetilde{N}_1 = 1 \bmod 3, & \widetilde{N}_1 = 1, \\ x = 3 \bmod 7, & 3 \cdot 13 \cdot \widetilde{N}_2 = 1 \bmod 7, & 3 \cdot (-1) \cdot \widetilde{N}_2 = 1 \bmod 7, & \widetilde{N}_2 = 2, \\ x = 2 \bmod 13, & 3 \cdot 7 \cdot \widetilde{N}_3 = 1 \bmod 13, & 8 \cdot \widetilde{N}_3 = 1 \bmod 13, & \widetilde{N}_3 = 5. \end{array}$$

Podle zmíněné věty

$$\begin{aligned} x &= 7 \cdot 13 \cdot 1 \cdot 2 + 3 \cdot 13 \cdot 2 \cdot 3 + 3 \cdot 7 \cdot 5 \cdot 2 + \lambda \cdot 3 \cdot 7 \cdot 13, \\ x &= 626 + \lambda 273 = 80 + \lambda 273,\ \lambda \in \mathbb{Z} \end{aligned}$$

Příklad 32. Vypočtěte mocninu 111^{123456} v $\mathbb{Z}_n$, kde $n = 65231$.
protože $\gcd(111, n) = 37 \neq 1$, nelze redukovat exponent pomocí Eulerovy-Fermatovy věty. Dále $n = 37 \cdot 41 \cdot 43$, kde čísla v rozkladu jsou navzájem nesoudělná. Pro výpočet mocniny proto použijeme izomorfismů

$$\mathbb{Z}_n \underset{g}{\overset{f}{\rightleftarrows}} \mathbb{Z}_{37} \times \mathbb{Z}_{41} \times \mathbb{Z}_{43},$$

kde $f([x]_n) = ([x]_{37}, [x]_{41}, [x]_{43})$, $g([y_1]_{37}, [y_2]_{41}, [y_3]_{43}) = [N_1\widetilde{N}_1 y_1 + N_2\widetilde{N}_2 y_2 + N_3\widetilde{N}_3 y_3]_n$, kde

$$\begin{array}{llll} 41 \cdot 43 \cdot \widetilde{N}_1 = 1 \bmod 37, & 4 \cdot 6 \cdot \widetilde{N}_1 = 1 \bmod 37, & \text{EE algoritmus } \rightarrow, & \widetilde{N}_1 = 17, \\ 37 \cdot 43 \cdot \widetilde{N}_2 = 1 \bmod 41, & -4 \cdot 2 \cdot \widetilde{N}_2 = 1 \bmod 41, & \text{EE algoritmus } \rightarrow, & \widetilde{N}_2 = 5, \\ 37 \cdot 41 \cdot \widetilde{N}_3 = 1 \bmod 43, & 12 \cdot \widetilde{N}_3 = 1 \bmod 43, & \text{EE algoritmus } \rightarrow, & \widetilde{N}_3 = 18. \end{array}$$

Tedy platí

$$g([y_1]_{37}, [y_2]_{41}, [y_3]_{43}) = [29971y_1 + 7955y_2 + 27306y_3]_n.$$

Dále platí $f(111^{123456}) = f(111)^{123456} = (0, 29, 25)^{123456}$.

- $0^{123456} = 0$ v $\mathbb{Z}_{37}$,
- 29^{123456}, lze užít E–F větu k redukci exponentu, $123456 \bmod \varphi(41) = 16 = 10000_2$
  $29^{16} = 1XSSSS = 29, 21, 31, 18, \mathbf{37}$.
- 25^{123456}, lze užít E–F větu k redukci exponentu, $123456 \bmod \varphi(43) = 18 = 10010_2$
  $25^{18} = 1XSSSXS = 25, 23, 13, 40, 11, \mathbf{35}$.

Platí $111^{123456} = g([0]_{37}, [37]_{41}, [35]_{43}) = [29971 \cdot 0 + 7955 \cdot 37 + 27306 \cdot 35]_n = [10656]_{65231}$.

Protokol RSA

1) Návrh klíčů

Navrhněte klíče RSA pro přenos zpráv $0 \leq z < n$, $n \in \mathbb{N}^+$.

1. volba $p, q \in \mathbb{P}$, $p < q$, $n < pq$,
2. volba $e, d \in \mathbb{N}^+$, $ed = 1 \bmod \varphi(n)$,
3. (n, e) – veřejný klíč, (n, d) – soukromý klíč.

4. Šifrování $E : \{0, ..., n-1\} \to \{0, ..., n-1\}$, $E(x) := (x^e)_n$,
   dešifrování $D : \{0, ..., n-1\} \to \{0, ..., n-1\}$, $D(x) := (x^d)_n$.

5. Platí $E \circ D = D \circ E = id_{\{0,...,n-1\}}$.

Příklad 33. Navrhněte RSA klíče pro přenos zpráv z, $0 \leq z \leq 500$

Vybrané trojice $[p, q, pq]$ pro které $n < pq$, $p, q \in \mathbb{P}$, $p < q$,
$[3, 167, 501], [5, 101, 505], [11, 47, 517], [13, 41, 533], [19, 29, 551]$.

vybrané exponenty (e, d) pro vybranou trojici $[p, q, pq]$
$[3, 167, 501] \to (e, d) \in$ {[3, 111], [5, 133], [7, 95], [9, 37], [11, 151], [13, 281], [15, 155], [17, 293], [19, 35], [21, 253], [23, 231], [25, 93], [27, 123], [29, 229], [31, 75], [33, 161], [39, 315], [41, 81], [43, 139], [45, 273], [47, 219], [49, 61], [51, 319], [53, 213], [55, 163], [57, 233], [59, 287], [63, 195], [65, 189], [67, 223], [69, 77], [71, 159], [73, 141], [79, 311], [85, 125], [87, 187], [89, 97], [91, 135], [99, 275], [101, 309], [103, 303]}

$[5, 101, 505] \to (e, d) \in$ {[3, 267], [7, 343], [9, 89], [11, 291], [13, 277], [17, 353], [19, 379], [21, 381], [23, 87], [27, 163], [29, 69], [31, 271], [33, 97], [37, 173], [39, 359], [41, 361], [43, 307], [47, 383], [49, 49], [51, 251], [53, 317], [57, 393], [59, 339], [61, 341], [63, 127], [67, 203], [71, 231], [73, 137], [77, 213], [79, 319], [81, 321], [83, 347], [91, 211], [93, 357], [99, 299], [101, 301], [103, 167], [107, 243], [109, 389], [111, 191], [113, 177], [117, 253], [119, 279], [121, 281], [123, 387]}

$[11, 47, 517] \to (e, d) \in$ {[3, 307], [7, 263], [9, 409], [11, 251], [13, 177], [17, 433], [19, 339], [21, 241], [27, 443], [29, 349], [31, 371], [33, 237], [37, 373], [39, 59], [41, 101], [43, 107], [47, 323], [49, 169], [51, 451], [53, 217], [57, 113], [61, 181], [63, 387], [67, 103], [71, 311], [73, 397], [77, 233], [79, 99], [81, 301], [83, 327], [87, 423], [89, 429], [91, 91], [93, 277], [97, 313], [109, 249], [111, 431], [117, 173], [119, 259], [121, 441], [123, 187], [127, 163], [129, 189], [131, 151]}

$[13, 41, 533] \to (e, d) \in$ {[7, 343], [11, 131], [13, 37], [17, 113], [19, 379], [23, 167], [29, 149], [31, 31], [41, 281], [43, 67], [47, 143], [49, 49], [53, 317], [59, 179], [61, 181], [71, 311], [73, 217], [77, 293], [79, 79], [83, 347], [89, 329], [91, 211], [97, 193], [101, 461], [103, 247], [107, 323], [109, 229], [119, 359], [121, 361], [127, 223], [133, 397], [137, 473], [139, 259], [151, 391], [157, 373], [161, 161], [163, 427], [169, 409], [173, 197], [187, 403], [191, 191]}

$[19, 29, 551] \to (e, d) \in$ {[5, 101], [11, 275], [13, 349], [17, 89], [19, 451], [23, 263], [25, 121], [29, 365], [31, 439], [37, 109], [41, 209], [43, 211], [47, 311], [53, 485], [55, 55], [59, 299], [61, 157], [65, 473], [67, 331], [71, 71], [73, 145], [79, 319], [83, 419], [85, 421], [95, 191], [97, 265], [103, 367], [107, 179], [113, 281], [115, 355], [125, 125], [127, 127], [131, 227], [137, 401], [139, 475], [143, 215], [149, 389], [151, 247], [155, 491], [163, 235], [167, 335], [169, 337], [173, 437]}.

Příklad 34. Která z dvojice čísel:

$$(539, 11), (527, 87), (1001, 7), (559, 559),$$

může či nemůže sloužit jako šifrovací klíč protokolu RSA?

- $(539, 11)$ nemůže, $539 = 7^2 \cdot 11$, není „square free“.
- $(527, 87)$ nemůže, $87 \notin \mathbb{Z}^*_{\varphi(527)}$, $\varphi(527) = 16 \cdot 30$, $\gcd(87, 16 \cdot 30) = 3$.
- $(1001, 7)$ lze použít, **ale** $1001 = 7 \cdot 11 \cdot 13$, snažší dekompozice hrubou silou, jestliže $n = p_1 \cdot ... \cdot p_k$, $p_1 < ... < p_k$, potom $p_1 < \sqrt[k]{n}$.
- $(559, 559)$ lze použít jen teoreticky, splňuje podmínky $559 = 13 \cdot 43$, $559 \in \mathbb{Z}^*_{\varphi(559)}$, kde $559^{-1} = 559$ v $\mathbb{Z}^*_{\varphi(559)}$, tj, tímtéž klíčem je možné šifrovat i dešifrovat.
  V intervalu $p < q \leq 27499$, $p, q \in \mathbb{P}$ byly nalezeny jen dvojice

  $$(p, q) \in \{(3, 5), (5, 7), (5, 13), (7, 13), (13, 29), (13, 43), (29, 71), (71, 181)\},$$

  pro které platí, že (n, n), $n = pq$, je zároveň šifrovací i dešifrovací klíč protokolu RSA.

Hypotéza. *Lze vyslovit hypotézu, že dvojic prvočísel, pro které (n, n) je šifrovací i dešifrovací klíč, více neexistuje.*

Poznámka. (n, n), kde $n = pq$, $p < q$, je zároveň šifrovací i dešifrovací klíč protokolu RSA jestliže $p^2 + q^2 = 2 \bmod (p - 1)(q - 1)$.

2) RSA provoz

Příklad 35. Nechť Alice má soukromý a veřejný RSA klíč $(n_A, d_A) = (589, 47)$, $(n_A, e_A) = (589, 23)$, Bob má soukromý a veřejný šifrovací klíč $(n_B, d_B) = (323, 67)$, $(n_B, e_B) = (323, 43)$. Alice chce Bobovi poslat zprávu $z = 200$ šifrovaně. Vypočtěte šifrovanou zprávu, kterou Alice pošle Bobovi. Jaké výpočty provede Bob, chce-li zprávu dešifrovat?
Řešení: Alice vypočte:

$$c_B = (z^{e_B})_{n_B} = (200^{43})_{323}.$$

V okruhu $\mathbb{Z}_{323}$ počítejme mocninu 200^{43}. Protože $43 = 101011_2$, bude $200^{43} = 1XSSXSSXSX$, dostaneme posloupnost $200, 271, 120, 98, 237, 290, 183, 220, \mathbf{72}$, tedy Alice pošle Bobovi zprávu $c_B = 72$.

Bob zprávu dešifruje výpočtem $z = (c_B^{d_B})_{n_B} = (72^{67})_{323}$. V okruhu $\mathbb{Z}_{323}$ Bob vypočítá mocninu 72^{67}. Protože $72 = 1000011_2$, bude $72^{67} = 1XSSSSSXSX$, dostaneme posloupnost $72, 16, 256, 290, 120, 188, 293, 254, \mathbf{200}$. Bob získá zprávu $z = 200$.

Příklad 36. Nechť Alice má soukromý a veřejný RSA klíč $(n_A, d_A) = (1073, 125)$, $(n_A, e_A) = (1073, 629)$, Bob má soukromý a veřejný šifrovací klíč $(n_B, d_B) = (1147, 47)$, $(n_B, e_B) = (1147, 23)$. Bob chce Alici poslat zprávu $z = 333$ šifrovaně. Vypočtěte šifrovanou zprávu, kterou Bob pošle Alici. Jaké výpočty provede Alice, chce-li zprávu dešifrovat?
Řešení: Bob vypočte:

$$c_A = (z^{e_A})_{n_A} = (333^{629})_{1073}.$$

V okruhu $\mathbb{Z}_{1073}$ počítejme mocninu 333^{629}. Protože $629 = 1001110101_2$, bude $333^{629} = 1XSSSXSXSXSSXSSX$, dostaneme posloupnost $333, 370, 629, 777, 148, 444, 851, 999, 37, 296, 703, 185, 9$
tedy Bob pošle Alici zprávu $c_A = 814$.

Alice zprávu dešifruje výpočtem $z = (c_A^{d_A})_{n_B} = (814^{125})_{1073}$. V okruhu $\mathbb{Z}_{1073}$ Alice vypočítá mocninu 814^{125}. Protože $125 = 1111101_2$, bude $814^{125}. = 1XSXSXSXSXSSX$, dostaneme posloupnost $814, 555, 37, 296, 592, 666, 259, 555, 37, 296, 703, \mathbf{333}$. Alice získá zprávu $z = 333$.

3) Faktorizace – hrubá síla atd.

Tvrzení 37. (Rozklad modulu n hrubou silou) Nechť je dán modul n protokolu RSA, tj. existují prvočísla $p, q \in \mathbb{P}$, $p < q$ taková, že $n = pq$. Protože $0 < p < q \Rightarrow p^2 < pq = n$, máme horní odhad menšího z prvočísel

$$p < \sqrt{n}.$$

Hrubou silou se zde rozumí vyzkoušení všech prvočísel $p \in \mathbb{P}$ z intervalu $2 \leq p < \sqrt{n}$. Situaci lze mírně vylepšit využitím následujícího faktu:

$$p \in \mathbb{P},\ p \geq 5 \Rightarrow p \in (5 + 6\mathbb{N}) \cup (1 + 6\mathbb{N}),$$

tj. každé prvočíslo počínaje 5 dostanu z 5 střídavým přičítáním čísel 2 a 4, viz diagram

$$5 \xrightarrow{+2} 7 \xrightarrow{+4} 11 \xrightarrow{+2} 13 \xrightarrow{+4} 17 \xrightarrow{+2} 19 \xrightarrow{+4} 23 \xrightarrow{+2} ...$$

Příklad 38. Účastník protokolu RSA s veřejným klíčem $(n, e) = (1121, 95)$ obdržel šifrovanou zprávu $c = 701$. Zprávu c dešifrujte hrubou silou.

Řešení: Hrubou silou provedeme faktorizaci modulu $n = 1121$. Protože $\sqrt{1121} \doteq 33.48$, jako dělitelé n přicházejí v úvahu následující prvočísla:

$$\{3, 5, 7, 11, 13, 17, \mathbf{19}, 23, 29, 31\},$$

kde 19 je hledaný dělitel n. Platí $1121 = 19 \cdot 59$. Odtud $\varphi(n) = 18 \cdot 58 = 1044$ a můžeme vypočítat utajovaný dešifrovací exponent nešťastného účastníka z rovnice $95d = 1 \bmod 1044$. Pomocí EE–algoritmu dostaneme

$$\begin{bmatrix} 95 & 1 & 0 \\ 1044 & 0 & 1 \end{bmatrix} \sim \begin{bmatrix} 95 & 1 & 0 \\ 94 & -10 & 1 \end{bmatrix} \sim \begin{bmatrix} 1 & 11 & -1 \\ 94 & -10 & 1 \end{bmatrix} \sim \begin{bmatrix} 1 & 11 & -1 \\ 0 & -1044 & 95 \end{bmatrix}$$

odtud máme $d = 11$. Pro dešifrovanou zprávu platí $z = (701^{11})_{1121}$, protože $11 = 1011_2$, platí $z = 1XSSXSX$, dostaneme posloupnost:

$$701, 403, 985, 1070, 359, \mathbf{555},$$

tj. hledaná zpráva je $z = 555$.

Příklad 39. Je znám veřejný RSA klíč $(1207, 9)$. Zjistěte odpovídající dešifrovací klíč $(1207, d)$ rozkladem modulu $n = 1207$ hrubou silou.
Řešení: Hrubou silou provedeme faktorizaci modulu $n = 1207$. Protože $\sqrt{1207} \doteq 34.74$, jako dělitelé n přicházejí v úvahu následující prvočísla:

$$\{3, 5, 7, 11, 13, \mathbf{17}, 19, 23, 29, 31\},$$

kde 17 je hledaný dělitel n. Platí $1207 = 17 \cdot 71$. Odtud $\varphi(n) = 16 \cdot 70 = 1120$ a můžeme vypočítat utajovaný dešifrovací exponent nešťastného účastníka z rovnice $9d = 1 \bmod 1120$. Pomocí EE–algoritmu dostaneme

$$\begin{bmatrix} 9 & 1 & 0 \\ 1120 & 0 & 1 \end{bmatrix} \sim \begin{bmatrix} 9 & 1 & 0 \\ 4 & -124 & 1 \end{bmatrix} \sim \begin{bmatrix} 1 & 249 & -2 \\ 4 & -124 & 1 \end{bmatrix} \sim \begin{bmatrix} 1 & 249 & -2 \\ 0 & -1120 & 9 \end{bmatrix}$$

Odtud $(1207, 249)$ je hledaný dešifrovací klíč.

Příklad 40. Správci šifrovacích klíčů protokolu RSA se sdíleným modulem se klíče pomíchali. Je třeba klíče spárovat do dvojic šifrovací, dešifrovací klíč (n, e), (n, d), jsou-li dány dvojice

$$(6683, 121),\ (6683, 77),\ (6683, 2447),$$
$$(6683, 143),\ (6683, 3481),\ (6683, 2693).$$

Řešení: Jestliže dvojice $(n, e)\,, (n, d)$ tvoří pár šifrovací dešifrovací klíč protokolu RSA, potom nutně $ed = 1 \bmod \varphi(n)$. Abychom mohli stanovit hodnotu $\varphi(n)$ Eulerovy funkce, provedeme rozklad modulu n hrubou silou. Protože $\sqrt{6683} \doteq 81.75$, jako dělitelé n přicházejí v úvahu následující prvočísla:

$$\{3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, \mathbf{41}, 43, 47, 53, 59, 61, 67, 71, 73, 79\},$$

kde 41 je hledaný dělitel n. Platí $6683 = 41 \cdot 163$. Odtud $\varphi(n) = 40 \cdot 162 = 6480$. Nyní můžeme testovat rovnici $ed = 1 \bmod \varphi(n)$.
$121 \cdot 77 \bmod 6480 = 2837$, $121 \cdot 2447 \bmod 6480 = 4487$, $121 \cdot 143 \bmod 6480 = 4343$, $121 \cdot 3481 \bmod 6480 = 1$, máme tedy pár $\{(\mathbf{6683}, \mathbf{121}), (\mathbf{6683}, \mathbf{3481})\}$.
Dále $77 \cdot 2447 \bmod 6480 = 499$, $77 \cdot 143 \bmod 6480 = 4531$, $77 \cdot 2693 \bmod 6480 = 1$, máme tedy druhý pár $\{(\mathbf{6683}, \mathbf{77}), (\mathbf{6683}, \mathbf{2693})\}$.
Ověřme poslední pár $2447 \cdot 143 \bmod 6480 = 1$, tedy $\{(\mathbf{6683}, \mathbf{143}), (\mathbf{6683}, \mathbf{2447})\}$.

Tvrzení 41. Jestliže účastník protokolu RSA krom svého modulu n zveřejní i hodnotu Eulerovy funkce $\varphi(n)$, lze modul n snadno faktorizovat dále uvedeným postupem. Platí totiž:

$$f(x) \coloneqq (x - p)(x - q) = x^2 - (p + q)x + pq,$$

kde $\varphi(n) = (p - 1)(q - 1) = n - (p + q) + 1$, tj. pro polynom f platí:

$$f(x) = x^2 - (n + 1 - \varphi(n))x + n,$$

kde kořeny polynomu jsou hledaná prvočísla. Platí tedy

$$\frac{1}{2}(n+1-\varphi(n)) \pm \sqrt{\left(\frac{1}{2}(n+1-\varphi(n))\right)^2 - n} \in \{p,q\}.$$

Příklad 42. Faktorizujte modul $n = 76151$ klíče protokolu RSA, je-li známa hodnota $\varphi(n) = 75600$. Platí:

$$\begin{aligned} \frac{1}{2}(n+1-\varphi(n)) &= \frac{1}{2}(76151+1-75600) = 276 \\ 276 &\pm \sqrt{276^2 - 76151} = 276 \pm 5 \in \{271, 281\}. \end{aligned}$$

Kontrola $271 \cdot 281 = 76151$, $271, 281 \in \mathbb{P}$.

Příklad 43. Faktorizujte modul $n = 86701$ klíče protokolu RSA, je-li známa hodnota $\varphi(n) = 86112$.
$86112 = 277 \cdot 313$.

Příklad 44. Faktorizujte modul $n = 54841$ klíče protokolu RSA, je-li známa hodnota $\varphi(n) = 54352$.
$54841 = 173 \cdot 317$.

Tvrzení 45. Dekompozice n modulu RSA jsou-li známy oba klíče (n, e), (n, d). Metoda vyhledává dělitele 0 v okruhu $\mathbb{Z}_n$. Metoda je základem útoku při sdíleném modulu typu „insider“. V okruhu $\mathbb{Z}_n$, kde $n = pq,\ p, q \in \mathbb{P},\ p < q$, platí

$$(\forall z \in \mathbb{Z}_n)(\forall k \in \mathbb{N})(z^{1+k\varphi(n)} = z). \tag{9}$$

Protože $ed = 1 \bmod \varphi(n)$, je $ed - 1 = k\varphi(n)$ pro nějaké $k \in \mathbb{N}$. Jsou-li p, q lichá prvočísla, je $\varphi(n)$ a tudíž i $ed - 1$ dělitelno alespoň 4. Lze tedy sestrojit rekurzivně posloupnosti t_k, y_k následovně:

1. definujme $t_0 \coloneqq ed - 1$, $t_{k+1} \coloneqq \frac{1}{2}t_k$ pro všechna $k \in \mathbb{N}$, pro která t_k je sudé. Nechť t_m je liché.

2. zvolme $z \in \mathbb{Z}_n$,

3. v okruhu $\mathbb{Z}_n$ vypočtěme posloupnost $y_m \coloneqq z^{t_m}, y_{m-1} \coloneqq y_m^2, y_{m-2} \coloneqq y_{m-1}^2, ..., y_0 \coloneqq y_1^2$.

4. Jestliže $z \in \mathbb{Z}_n^*$, pak podle (9) existuje $k \in \{0, 1, ..., m\}$ takové, že $y_k^2 = 1$ odtud $(y_k - 1)(y_k + 1) = 0$ v $\mathbb{Z}_n$. Jestliže $y_k - 1 \neq 0$ v $\mathbb{Z}_n$ a $y_k + 1 \neq 0$ v $\mathbb{Z}_n$, jsou tímto nalezeny dělitelé 0 v $\mathbb{Z}_n$, platí proto $\gcd(y_k - 1, n)$, $\gcd(y_k + 1, n) \in \{p, q\}$.

5. Jestliže $z \in \mathbb{Z}_n \setminus \mathbb{Z}_n^*$, potom $\gcd(z, n) \in \{p, q\}$.

6. Jestliže v kroku 4. $y_k - 1 = 0$ v $\mathbb{Z}_n$ nebo $y_k + 1 = 0$ v $\mathbb{Z}_n$, je třeba v kroku 2. zvolit jiné z.

Příklad 46. Proveďte dekompozici modulu n protokolu RSA vyhledáním dělitelů 0 v okruhu $\mathbb{Z}_n$, jsou-li známy oba klíče $(n, e) = (32639, 397)$, $(n, d) = (32639, 325)$.

1. $t_0 = ed - 1 = 397 \cdot 325 - 1 = 129024$. Pro posloupnost t_k platí:
   $t = \{129024, 64512, 32256, 16128, 8064, 4032, 2016, 1008, 504, 252, 126, 63\}$, tedy $t_{11} = 63$.

2. Nechť $z = 2$,

3. $y_{11} \coloneqq 2^{63}$, $63 = 111111_2$, tj. $2^{63} = 1XSXSXSXSXSX$ v $\mathbb{Z}_{32639}$. Dostaneme posloupnost
   $2, 4, 8, 64, 128, 16384, 129, 16641, 643, 21781, 10923$, tj $y_{11} = 10923$. Dále $y_{10} = y_{11}^2 = 16384$, $y_9 = y_{10}^2 = 12320$, $y_8 = y_9^2 = 11050$, $y_7 = y_8^2 = 1$, tedy $11049 \cdot 11051 = 0$ v $\mathbb{Z}_{32639}$. Dále vypočteme $\gcd(1149, 32639)$ E–algoritmem:

$$\begin{bmatrix} 32639 \\ 11049 \end{bmatrix} \sim \begin{bmatrix} 10541 \\ 11049 \end{bmatrix} \sim \begin{bmatrix} 10541 \\ 508 \end{bmatrix} \sim \begin{bmatrix} 381 \\ 508 \end{bmatrix} \sim \begin{bmatrix} 381 \\ 127 \end{bmatrix} \sim \begin{bmatrix} 0 \\ 127 \end{bmatrix}$$

   Odtud $\mathbf{32639 = 127 \cdot 257}$.

Příklad 47. Proveďte dekompozici modulu n protokolu RSA vyhledáním dělitelů 0 v okruhu $\mathbb{Z}_n$, jsou-li známy oba klíče $(n, e) = (4369, 17)$, $(n, d) = (4369, 241)$.

1. $t_0 = ed - 1 = 17 \cdot 241 - 1 = 4096$. Pro posloupnost t_k platí:
   $t = \{4096, 2048, 1024, 512, 256, 128, 64, 32, 16, 8, 4, 2, 1\}$, tedy $t_{12} = 1$.

2. Nechť $z = 2$,

3. $y_{12} \coloneqq 2^1 = 2$, Dále $y_{11} = y_{12}^2 = 4$, $y_{10} = y_{11}^2 = 16$, $y_9 = y_{10}^2 = 256$, $y_8 = y_9^2 = 1$, tedy $255 \cdot 257 = 0$ v $\mathbb{Z}_{4369}$. Dále vypočteme $\gcd(255, 4369)$ E–algoritmem:

$$\begin{bmatrix} 255 \\ 4369 \end{bmatrix} \sim \begin{bmatrix} 255 \\ 34 \end{bmatrix} \sim \begin{bmatrix} 17 \\ 34 \end{bmatrix} \sim \begin{bmatrix} 17 \\ 0 \end{bmatrix}$$

   Odtud $\mathbf{4369 = 17 \cdot 257}$.

Příklad 48. (Stejné jako příklad 47, v kroku 2. jiná volba z.) Proveďte dekompozici modulu n protokolu RSA vyhledáním dělitelů 0 v okruhu $\mathbb{Z}_n$, jsou-li známy oba klíče $(n, e) = (4369, 17)$, $(n, d) = (4369, 241)$.

1. $t_0 = ed - 1 = 17 \cdot 241 - 1 = 4096$. Pro posloupnost t_k platí:
   $t = \{4096, 2048, 1024, 512, 256, 128, 64, 32, 16, 8, 4, 2, 1\}$, tedy $t_{12} = 1$.

2. Nechť $z = 17$,

3. $y_{12} \coloneqq 17^1 = 17$, Dále $y_{11} = y_{12}^2 = 289$, $y_{10} = y_{11}^2 = 510$, $y_9 = y_{10}^2 = 2329$, $y_8 = y_9^2 = 2312$, $y_7 = y_8^2 = 2057$, $y_6 = y_7^2 = 2057$. Tedy $y_7 = y_6 = ... = y_0 = 2057$, zřejmě $z = 17$ není invertibilní prvek v $\mathbb{Z}_{4369}$. Pak ovšem $\gcd(17, 4369) \in \{p, q\}$, E–algoritmus dává ihned:
   $$\begin{bmatrix} 17 \\ 4369 \end{bmatrix} \sim \begin{bmatrix} 17 \\ 0 \end{bmatrix}$$
   Odtud $\mathbf{4369 = 17 \cdot 257}$.

Příklad 49. Proveďte dekompozici modulu n protokolu RSA vyhledáním dělitelů 0 v okruhu $\mathbb{Z}_n$, jsou-li známy oba klíče $(n, e) = (345281, 559)$, $(n, d) = (345281, 1231)$.

1. $t_0 = ed - 1 = 559 \cdot 1231 - 1 = 688128 = 2^{15} \cdot 21$, tj. platí $t_{15} = 21$.

2. Nechť $z = 2$,

3. $y_{15} \coloneqq 2^{21} = 2097152 = 25466$, Dále $y_{14} = y_{15}^2 = 79438$, $y_{13} = y_{14}^2 = 40288$, $y_{12} = y_{13}^2 = 302244$, $y_{11} = y_{12}^2 = 96085$, $y_{10} = y_{11}^2 = 203847$, $y_9 = y_{10}^2 = 66902$, $y_8 = y_9^2 = 1$. Tedy $66901 \cdot 66903 = 0$ v $\mathbb{Z}_{345281}$. Dále vypočteme $\gcd(66901, 345281)$ E–algoritmem:
   $$\begin{bmatrix} 66901 \\ 345281 \end{bmatrix} \sim \begin{bmatrix} 66901 \\ 10776 \end{bmatrix} \sim \begin{bmatrix} 2245 \\ 10776 \end{bmatrix} \sim \begin{bmatrix} 2245 \\ 1796 \end{bmatrix} \sim \begin{bmatrix} 449 \\ 1796 \end{bmatrix} \sim \begin{bmatrix} 449 \\ 0 \end{bmatrix}$$
   Odtud $\mathbf{345281 = 449 \cdot 769}$.

Elementární útoky na protokol RSA

Příklad 50. Útok na protokol RSA účastníků se sdíleným modulem typu „insider“.
Jste jedním z účastníků protokolu RSA s veřejným a soukromým klíčem $(n_1, e_1) = (5917, 41)$, $(n_1, d_1) = (5917, 281)$, ostatní účastníci protokolu mají veřejné klíče $(n_2, e_2) = (5917, 661)$, $(n_3, e_3) = (5917, 347)$. Vypočtěte soukromé klíče pro ostatní účastníky využitím procedury v *Tvrzení* 45.

1. $t_0 = e_1 d_1 - 1 = 41 \cdot 281 - 1 = 11520$. Pro posloupnost t_k platí:
   $t = \{11520, 5760, 2880, 1440, 720, 360, 180, 90, 45\}$, tedy $t_8 = 45$.

2. Nechť $z = 2$,

3. $y_8 \coloneqq 2^{45}$, $45 = 101101_2$, tj. $2^{45} = 1XSSXSXSSX$ v $\mathbb{Z}_{5917}$. Dostaneme posloupnost $2, 4, 16, 32, 1024, 2048, 5068, 4844, 3771$, tj $y_8 = 3771$. Dále $y_7 = y_8^2 = 1890$, $y_6 = y_7^2 = 4149$, $y_5 = y_6^2 = 1648$, $y_4 = y_5^2 = 1$. Odtud $1647 \cdot 1649 = 0$ v $\mathbb{Z}_{5917}$. Pak ovšem $\gcd(1647, 5917) \in \{p, q\}$, E–algoritmus dává:

$$\begin{bmatrix}1647\\5917\end{bmatrix} \sim \begin{bmatrix}1647\\976\end{bmatrix} \sim \begin{bmatrix}671\\976\end{bmatrix} \sim \begin{bmatrix}671\\305\end{bmatrix} \sim \begin{bmatrix}305\\61\end{bmatrix} \sim \begin{bmatrix}0\\61\end{bmatrix}$$

Odtud $\mathbf{5917 = 61 \cdot 97}$. Dále odtud plyne $\varphi(5917) = 60 \cdot 96 = 5760$.
Výpočtem inverzí pro $e_2 = 661$, $e_3 = 347$ v okruhu $\mathbb{Z}_{5760}$ dostane soukromé exponenty d_2, d_3.

$$\begin{bmatrix}661 & 1 & 0\\5760 & 0 & 1\end{bmatrix} \sim \begin{bmatrix}661 & 1 & 0\\472 & -8 & 1\end{bmatrix} \sim \begin{bmatrix}189 & 9 & -1\\472 & -8 & 1\end{bmatrix} \sim \begin{bmatrix}189 & 9 & -1\\94 & -26 & 3\end{bmatrix} \sim$$
$$\sim \begin{bmatrix}29 & 89 & -10\\94 & -26 & 3\end{bmatrix} \sim \begin{bmatrix}1 & 61 & -7\\94 & -26 & 3\end{bmatrix} \sim \begin{bmatrix}1 & 61 & -7\\0 & -5760 & 661\end{bmatrix}.$$

Tedy $d_2 = 61$ v $\mathbb{Z}_{5760}$.

$$\begin{bmatrix}347 & 1 & 0\\5760 & 0 & 1\end{bmatrix} \sim \begin{bmatrix}347 & 1 & 0\\208 & -16 & 1\end{bmatrix} \sim \begin{bmatrix}139 & 17 & -1\\208 & -16 & 1\end{bmatrix} \sim \begin{bmatrix}139 & 17 & -1\\69 & -33 & 2\end{bmatrix} \sim$$
$$\sim \begin{bmatrix}1 & 83 & -5\\69 & -33 & 2\end{bmatrix} \sim \begin{bmatrix}1 & 83 & -5\\0 & -5760 & 347\end{bmatrix}.$$

Tedy $d_3 = 83$ v $\mathbb{Z}_{5760}$.

Tvrzení 51. Útok na protokol RSA při sdíleném modulu typu „outsider“
Jedna a tatáž zpráva z je poslána více účastníkům protokolu RSA se sdíleným modulem, s veřejnými klíči (n, e_i), $i \in \{1, 2, ..., k\}$. Účastníci tedy obdrží šifrované zprávy $c_i = (z^{e_i})_n$. Bez ztráty obecnosti lze předpokládat $c_i \neq 0$ v $\mathbb{Z}_n$.
Tyto zprávy zachytí útočnice Eve, která není součástí skupiny účastníků, odtud „outsider“. Útočnice Eve sestaví Bezoutovu rovnost

$$d \coloneqq \gcd(e_1, ..., e_k) = t_1 e_1 + ... + t_k e_k.$$

Dále platí v $\mathbb{Z}_n$

$$z^d = z^{t_1 e_1 + ... + t_k e_k} = c_1^{t_1} \cdot ... \cdot c_k^{t_k}.$$

Jestliže některý z koeficientů t v Bezoutově rovnosti je záporný, potom $c^t = (\tilde{c})^{-t}$, kde $\tilde{c}$ je inverzní prvek k c v multiplikativní grupě $\mathbb{Z}_n^*$. Jestliže $c \notin \mathbb{Z}_n^*$, pak inverze $\tilde{c}$ neexistuje, v tom případě má útočnice Eve štěstí, protože nalezla dekompozici modulu n, v tomto případě totiž $\gcd(c, n) \in \{p, q\}$.
Jestliže $d > 1$, Eve je dále nucena řešit problém diskrétní odmocniny v $\mathbb{Z}_n$, což se může stát významnou komplikací, viz dále uvedená sekce „Řešení rovnic v grupách a okruzích $\mathbb{Z}_n$“.

Příklad 52. Účastníkům protokolu se sdíleným modulem $n = 34571$ s veřejnými klíči $(n, 37)$, $(n, 23)$ je zaslána šifrovaně tatáž zpráva z. Účastník s klíčem $(n, 37)$, obdrží zprávu $c_1 = 26027$, účastník s klíčem $(n, 23)$, obdrží zprávu $c_2 = 5265$. Obě zprávy jsou zachyceny „outsiderem" Eve. Jak bude Eve dešifrovat zprávu útokem typu „outsider"?
Řešení:

1. Eve sestaví Bezoutovu rovnost $\gcd(37, 23) = x \cdot 37 + y \cdot 23$, koeficienty x, y najde EE – algoritmem:

$$\begin{bmatrix} 37 & 1 & 0 \\ 23 & 0 & 1 \end{bmatrix} \sim \begin{bmatrix} 14 & 1 & -1 \\ 23 & 0 & 1 \end{bmatrix} \sim \begin{bmatrix} 14 & 1 & -1 \\ 9 & -1 & 2 \end{bmatrix} \sim \begin{bmatrix} 1 & 5 & -8 \\ 4 & -3 & 5 \end{bmatrix} \sim \begin{bmatrix} 1 & 5 & -8 \\ 0 & -23 & 37 \end{bmatrix},$$

   tedy

$$1 = 5 \cdot 37 + (-8) \cdot 23.$$

2. Odtud dále platí

$$z = z^{5 \cdot 37 + (-8) \cdot 23} = c_1^5 \cdot c_2^{-8}.$$

   Vypočteme nejprve $c_2^{-8} = 5265^{-8} = (5265^{-1})^8$. Počítejme inverzi 5265^{-1} EE – algoritmem:

$$\begin{bmatrix} 5265 & 1 & 0 \\ 34571 & 0 & 1 \end{bmatrix} \sim \begin{bmatrix} 5265 & 1 & 0 \\ 2981 & -6 & 1 \end{bmatrix} \sim \begin{bmatrix} 2284 & 7 & -1 \\ 2981 & -6 & 1 \end{bmatrix} \sim \begin{bmatrix} 2284 & 7 & -1 \\ 697 & -13 & 2 \end{bmatrix} \sim$$
$$\begin{bmatrix} 1 & 5 & -8 \\ 0 & -23 & 37 \end{bmatrix} \sim \begin{bmatrix} 193 & 46 & -7 \\ 697 & -13 & 2 \end{bmatrix} \sim \begin{bmatrix} 193 & 46 & -7 \\ 118 & -151 & 23 \end{bmatrix} \sim \begin{bmatrix} 75 & 197 & -30 \\ 118 & -151 & 23 \end{bmatrix} \sim$$
$$\begin{bmatrix} 75 & 197 & -30 \\ 43 & -348 & 53 \end{bmatrix} \sim \begin{bmatrix} 32 & 545 & -83 \\ 43 & -348 & 53 \end{bmatrix} \sim \begin{bmatrix} 32 & 545 & -83 \\ 11 & -893 & 136 \end{bmatrix} \sim \begin{bmatrix} 10 & 2331 & -355 \\ 11 & -893 & 136 \end{bmatrix} \sim$$
$$\sim \begin{bmatrix} 10 & 2331 & -355 \\ 1 & -3224 & 491 \end{bmatrix} \sim \begin{bmatrix} 0 & 34571 & 491 \\ 1 & -3224 & 491 \end{bmatrix}$$

   takže $5265^{-1} = -3224$. Máme tedy

$$z = 26027^5 \cdot (-3224)^8.$$

   - $26027^5 = 1XSSX$, protože $5 = 101_2$, dostaneme posloupnost

$$26027, 20555, 15834, 25198,$$

     tj. $26027^5 = 25198$.
   - $(-3224)^8 = 3224^8 = 1XSSS$, protože $8 = 1000_2$, dostaneme posloupnost

$$3224, 22876, 10149, 15192,$$

     tj. $3224^8 = 15192$.

3. Pro zprávu z platí

$$z = 25198 \cdot 15192 = 3333.$$

Příklad 53. Účastníkům protokolu se sdíleným modulem $n = 3811$ s veřejnými klíči $(n, 5)$, $(n, 7)$ je zaslána šifrovaně tatáž zpráva z. Účastník s klíčem $(n, 5)$, obdrží zprávu $c_1 = 1147$, účastník s klíčem $(n, 7)$, obdrží zprávu $c_2 = 999$. Obě zprávy jsou zachyceny „outsiderem" Eve. Jak bude Eve dešifrovat zprávu útokem typu „outsider"?

Řešení:

1. Eve sestaví Bezoutovu rovnost $\gcd(5, 7) = x \cdot 37 + y \cdot 23$, koeficienty x, y najde EE – algoritmem:

$$\begin{bmatrix} 5 & 1 & 0 \\ 7 & 0 & 1 \end{bmatrix} \sim \begin{bmatrix} 5 & 1 & 0 \\ 2 & -1 & 1 \end{bmatrix} \sim \begin{bmatrix} 1 & 3 & -2 \\ 2 & -1 & 1 \end{bmatrix} \sim \begin{bmatrix} 1 & 3 & -2 \\ 0 & -7 & 5 \end{bmatrix},$$

   tedy

$$1 = 3 \cdot 5 + (-2) \cdot 7.$$

2. Odtud dále platí

$$z = z^{3 \cdot 5 + (-2) \cdot 7} = c_1^3 \cdot c_2^{-2}.$$

   Vypočteme nejprve $c_2^{-2} = 999^{-2} = (999^{-1})^2$. Počítejme inverzi 999^{-1} v $\mathbb{Z}_{3811}$ EE – algoritmem:

$$\begin{bmatrix} 999 & 1 & 0 \\ 3811 & 0 & 1 \end{bmatrix} \sim \begin{bmatrix} 999 & 1 & 0 \\ 814 & -3 & 1 \end{bmatrix} \sim \begin{bmatrix} 185 & 4 & -1 \\ 814 & -3 & 1 \end{bmatrix} \sim \begin{bmatrix} 185 & 4 & -1 \\ 74 & -19 & 5 \end{bmatrix} \sim \begin{bmatrix} 37 & 42 & -11 \\ 74 & -19 & 5 \end{bmatrix} \sim$$
$$\sim \begin{bmatrix} 37 & 42 & -11 \\ 0 & -103 & 27 \end{bmatrix}$$

   .

   EE – algoritmus ukázal, že 999 není v $\mathbb{Z}_{3811}$ invertibilním prvkem, takže je násobkem jednoho z prvočísel rozkladu modulu n, tj. $\gcd(c_2, n) \in \{p, q\}$, kde $n = pq$. Podle předchozího výpočtu máme rozklad $n = 3811 = 37 \cdot 103$. Můžeme vypočítat soukromé dešifrovací exponenty kteréhokoliv z účastníků protokolu. Například pro druhého z účastníků dostaneme z rovnice $7d = 1 \bmod \varphi(37 \cdot 103) = 3672$. Platí

$$\begin{bmatrix} 7 & 1 & 0 \\ 3672 & 0 & 1 \end{bmatrix} \sim \begin{bmatrix} 7 & 1 & 0 \\ 4 & -524 & 1 \end{bmatrix} \sim \begin{bmatrix} 4 & -524 & 1 \\ 3 & 525 & -1 \end{bmatrix} \sim \begin{bmatrix} 1 & -1049 & 2 \\ 3 & 525 & -1 \end{bmatrix} \sim \begin{bmatrix} 1 & -1049 & 2 \\ 0 & 3672 & -7 \end{bmatrix}.$$
$$\sim \begin{bmatrix} 1 & 2623 & -5 \\ 0 & 3672 & -7 \end{bmatrix}.$$

   Zprávu z dostaneme výpočtem $z = 999^{2623}$ v $\mathbb{Z}_{3811}$. Protože $2623 = 101000111111_2$, algoritmem $1XSSXSSSSXSXSXSXSXSX$ dostaneme hledanou zprávu:

$$999, 3330, 2701, 111, 888, 3478, 370, 3515, 1554, 2553, 888,$$
$$3478, 2701, 1147, 2553, 999, 3330, 2701, \mathbf{111}$$

3. Pro zprávu z platí $z = 111$.

Tvrzení 54. (útok při malém veřejném sdíleném exponentu)

Nechť jedna a tatáž zpráva z je posílána více účastníkům protokolu RSA s veřejnými klíči $(n_1, e), ..., (n_k, e)$ se sdíleným šifrovacím exponentem, tj. nechť $z \xrightarrow{(n_i,e)} c_i$. Potom hodnota $x = z^e$ je řešením soustavy

$$\begin{aligned} x &= c_1 \bmod n_1, \\ &\vdots \\ x &= c_k \bmod n_k. \end{aligned}$$

Soustava má řešení $x = x_0 + \lambda \mathrm{lcm}(n_1, ..., n_k)$, $\lambda \in \mathbb{Z}$, kde $0 \leq x_0 < \mathrm{lcm}(n_1, ..., n_k)$. Protože zpráva je dešifrovatelná pro každého účastníka, nutně platí $(\forall i \in \{1, ..., k\})(z < n_i)$, odtud $z < \min(n_1, ..., n_k)$. Útok bude proveditelný, bude-li platit $\min(n_1, ..., n_k)^e \leq \mathrm{lcm}(n_1, ..., n_k)$. Tato nerovnost omezuje velikost sdíleného exponentu e. Je-li splněna, potom $z^e = x_0$, odtud potom $z = \sqrt[e]{x_0}$.
Jestliže $\mathrm{lcm}(n_1, ..., n_k) = n_1 \cdot ... \cdot n_k$, potom uvedená nerovnost bude splněna pro $e \leq k$, odtud „malý sdílený exponent“.

Příklad 55. (útok při malém sdíleném veřejném exponentu)

Nechť účastníkům RSA protokolu se sdíleným malým veřejným exponentem s veřejnými klíči

$$(205, 3),\ (319, 3),\ (391, 3),$$

je zaslána jedna a tatáž zpráva z. Účastníci obdrží po řadě šifrované zprávy 82, 140, 98, tj.

$$82 \to (205, 3),\ 140 \to (319, 3),\ 98 \to (391, 3).$$

Útočnice Eve zprávy zachytí a rozhodne se dešifrovat zprávu z. Protože moduly 205, 319, 391 jsou navzájem nesoudělné a je splněna podmínka $e \leq 3$, má k dispozici dostatek zpráv k provedení útoku. Nejprve s využitím CRT vyřeší soustavu

$$\begin{aligned} x &= 82 \bmod 205, \\ x &= 140 \bmod 319, \\ x &= 98 \bmod 391. \end{aligned}$$

Eve dostane řešení

$$x = N_1 \widetilde{N}_1 82 + N_2 \widetilde{N}_2 140 + N_3 \widetilde{N}_3 98 + \lambda N,\ \lambda \in \mathbb{Z},$$

kde $N_1 = 124729$, $N_2 = 80155$, $N_3 = 65395$. Pro inverze platí

$$\begin{aligned} \begin{bmatrix} 124729 & 1 & 0 \\ 205 & 0 & 1 \end{bmatrix} &\sim \begin{bmatrix} 89 & 1 & -608 \\ 205 & 0 & 1 \end{bmatrix} \sim \begin{bmatrix} 89 & 1 & -608 \\ 27 & -2 & 1217 \end{bmatrix} \sim \begin{bmatrix} 8 & 7 & -4259 \\ 27 & -2 & 1217 \end{bmatrix} \sim \\ &\sim \begin{bmatrix} 8 & 7 & -4259 \\ 3 & -23 & 13994 \end{bmatrix} \sim \begin{bmatrix} 2 & 53 & -32247 \\ 3 & -23 & 13994 \end{bmatrix} \sim \begin{bmatrix} 2 & 53 & -32247 \\ 1 & -76 & 46241 \end{bmatrix} \sim \\ &\sim \begin{bmatrix} 0 & 205 & -124729 \\ 1 & -76 & 46241 \end{bmatrix}, \text{ tedy } \widetilde{N}_1 = -76 \end{aligned}$$

$$\begin{bmatrix} 80155 & 1 & 0 \\ 319 & 0 & 1 \end{bmatrix} \sim \begin{bmatrix} 86 & 1 & -251 \\ 319 & 0 & 1 \end{bmatrix} \sim \begin{bmatrix} 86 & 1 & -251 \\ 61 & -3 & 754 \end{bmatrix} \sim \begin{bmatrix} 25 & 4 & -1005 \\ 61 & -3 & 754 \end{bmatrix} \sim$$
$$\sim \begin{bmatrix} 25 & 4 & -1005 \\ 11 & -11 & 2764 \end{bmatrix} \sim \begin{bmatrix} 3 & 26 & -6533 \\ 11 & -11 & 2764 \end{bmatrix} \sim \begin{bmatrix} 3 & 26 & -6533 \\ 2 & -89 & 22363 \end{bmatrix} \sim$$
$$\sim \begin{bmatrix} 1 & 115 & -28896 \\ 2 & -89 & 22363 \end{bmatrix}, \text{ tedy } \widetilde{N}_2 = 115$$

$$\begin{bmatrix} 65395 & 1 & 0 \\ 391 & 0 & 1 \end{bmatrix} \sim \begin{bmatrix} 98 & 1 & -167 \\ 391 & 0 & 1 \end{bmatrix} \sim \begin{bmatrix} 98 & 1 & -167 \\ 97 & -3 & 502 \end{bmatrix} \sim \begin{bmatrix} 1 & 4 & -669 \\ 97 & -3 & 502 \end{bmatrix}, \text{ tedy } \widetilde{N}_3 = 4.$$

Řešením soustavy jsou čísla

$$\begin{aligned} x &= 124729 \cdot (-76) \cdot 82 + 80155 \cdot 115 \cdot 140 + 65395 \cdot 4 \cdot 98 + \lambda 205 \cdot 319 \cdot 391 =, \\ &= -777311128 + 1290495500 + 25634840 + \lambda 25569445 = \\ &= 538819212 + \lambda 25569445 = 1860867 + \lambda 25569445 \end{aligned}$$

Odtud plyne $z^3 = 1860867$, tj. $z = \sqrt[3]{1860867} = 123$. Všem účastníkům byla zaslána zpráva 123.

Tvrzení 56. Pro každé racionální číslo $\frac{a}{b}$, $a, b \in \mathbb{Z}$, $b \neq 0$, existuje tzv. řetězový zlomek:

$$\frac{a}{b} = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \ddots + \cfrac{1}{q_{n-1} + \cfrac{1}{q_n}}}}}$$

Koeficienty $q_0, ..., q_n$ lze vypočítat Euklidovým algoritmem podle schématu:

$$\begin{gathered} a_0 \coloneqq a, \quad a_1 \coloneqq b, \\ a_0 = q_0 a_1 + a_2,\ 0 \leq a_2 < |a_1|, \\ a_1 = q_1 a_2 + a_3,\ 0 \leq a_3 < |a_2|, \\ \vdots \\ a_k = q_k a_{k+1} + a_{k+2},\ 0 \leq a_{k+2} < |a_{k+1}|, \\ \vdots \\ a_n = q_n a_{n+1} + 0. \end{gathered}$$

Řetězový zlomek je jednoznačně určen posloupností koeficientů q_k, zapisujeme $\frac{a}{b} = [q_0, q_1, ..., q_n]$. Hodnota zlomku $(\frac{a}{b})_k = [q_0, q_1, ..., q_k]$ pro $0 \leq k \leq n$ se nazývá k–tá konvergenta, zřejmě $(\frac{a}{b})_0 = q_0$, $(\frac{a}{b})_1 = q_0 + \frac{1}{q_1}, .., (\frac{a}{b})_n = \frac{a}{b}$. Konvergenty jsou racionální aproximace daného čísla $\frac{a}{b}$, které „konvergují“ k tomuto číslu

Řetězový zlomek lze konstruovat pro každé reálné číslo $x \in \mathbb{R}$. Pak platí

- Je-li číslo x racionální, pak jeho řetězový zlomek je konečný.
- Je-li číslo x iracionální, pak jeho řetězový zlomek je nekonečný.
- Je-li číslo x iracionální, a je-li kořenem kvadratického polynomu s racionálními koeficienty, pak jeho řetězový zlomek je nekonečný a obsahuje periodu.

Příklad 57. Stanovte řetězový zlomek čísla $\frac{73}{15}$ a všechny jeho konvergenty. Platí

$$\begin{aligned} 73 &= 4 \cdot 15 + 13, \\ 15 &= 1 \cdot 13 + 2, \\ 13 &= 6 \cdot 2 + 1, \\ 2 &= 2 \cdot 1 + 0. \end{aligned}$$

Odtud $\frac{73}{15} = [4, 1, 6, 2]$, pro konvergenty platí $[(\frac{73}{15})_0, (\frac{73}{15})_1, (\frac{73}{15})_2, (\frac{73}{15})_3] = [4, 5, \frac{34}{7}, \frac{73}{15}]$.

Tvrzení 58. (Wiener's attack na RSA protokol) Nechť (n, e), (n, d) jsou klíče RSA protokolu, nechť (n, e) je veřejný. Jestliže jsou splněny podmínky

$$n = pq,\ p, q \in \mathbb{P},\ p < q < 2p,\ d < \frac{1}{3}\sqrt[4]{n},$$

pak je úspěšný dále popsaný útok.

Exponenty e d protokolu RSA splňují známou rovnici

$$ed = k\varphi(n) + 1$$

pro nějaké $k \in \mathbb{N}^+$. Vydělením rovnice součinem nd a odečtením $\frac{k}{d}$ dostaneme po úpravě rovnici

$$\frac{e}{n} - \frac{k}{d} = (\frac{e}{n} - \frac{1}{nd})(1 - \frac{n}{\varphi(n)}) + \frac{1}{nd}.$$

Čísla $1 - \frac{n}{\varphi(n)}$ a $\frac{1}{nd}$ jsou obecně malá, číslo $\frac{e}{n}$ obecně malé být nemusí. Wiener ve svém článku ukazuje, že jsou-li splněny výše uvedené podmínky, pak platí

$$\left|\frac{e}{n} - \frac{k}{d}\right| \leq \frac{1}{nd} \leq \frac{1}{2d^2}.$$

Podle známého matematického poznatku z poslední nerovnosti vyplývá, že zlomek $\frac{k}{d}$ se objeví mezi konvergentami rozvoje čísla $\frac{e}{n}$ v řetězový zlomek. Pro hodnotu Eulerovy funkce z toho plyne

$$\varphi(n) \in \{\frac{ed-1}{k} \mid \frac{k}{d} \text{ je konvergenta } \frac{e}{n}\},$$

tato vlastnost dovoluje vybrat vyhovující konvergenty.

Příklad 59. Nechť $(n, e) = (1277561, 927491)$ je veřejný RSA klíč. Provedeme Wienerův útok. Prověřit podmínky Wienerova teorému předem nelze. Dále uvedené výpočty byly provedeny algebraickým systémem Maple.

Pro koeficienty řetězového zlomku dostaneme:

$$\frac{927491}{1277561} \to [0, 1, 2, 1, 1, 1, 5, 1, 3, 1, 1, 1, 5, 1, 5, 1, 1, 1, 2, 1, 2],$$

odpovídající konvergenty

$$[0, 1, \frac{2}{3}, \frac{3}{4}, \frac{5}{7}, \frac{8}{11}, \frac{45}{62}, \frac{53}{73}, \frac{204}{281}, \frac{461}{635}, \frac{718}{989}, \frac{4051}{5580}, ...],$$

pro hodnoty $\{\frac{ed-1}{k} \mid \frac{k}{d}$ je konvergenta $\frac{e}{n}\}$ dostaneme:

$$[\text{udefined}, 927490, 1391236, \frac{3709963}{3}, \frac{6492436}{5}, 1275300, \text{ dále jen zlomky ...}].$$

Zbývá prověřit pouze tři kandidáty na hodnotu Eulerovy funkce $\varphi(n)$. Testem bude pokus dekomponovat n s využitím hodnoty $\varphi(n)$.

$\varphi(n) = 927490$, $a := \frac{1}{2}(n+1-\varphi(n)) = 175036$, $\sqrt{a^2 - n} = \sqrt{30636323735} = 175032.351 \notin \mathbb{N}$ **nevyhoví**.

$\varphi(n) = 1391236$, nesplňuje podmínku $\varphi(n) < n$ **nevyhoví**.

$\varphi(n) = 1275300$, $a := \frac{1}{2}(n + 1 - \varphi(n)) = 1131$, $\sqrt{a^2 - n} = \sqrt{1600} = 40$, $a \pm 40 \in \{1091, 1171\}$, **dekompozice n je nalezena**, hledaná konvergenta je 6. v pořadí, tj. $\frac{8}{11}$, odtud ihned plyne dešifrovací exponent $d = 11$. Podmínky Wienerova teorému mohou být dodatečně ověřeny a jsou splněny.

Příklad 60. Nechť $(n, e) = (55751, 22109)$ je veřejný RSA klíč. Provedeme Wienerův útok. Prověřit podmínky Wienerova teorému předem nelze. Dále uvedené výpočty byly provedeny algebraickým systémem Maple.

Pro koeficienty řetězového zlomku dostaneme:

$$\frac{22109}{55751} \to [0, 2, 1, 1, 11, 19, 1, 1, 7, 1, 2],$$

odpovídající konvergenty

$$[0, \frac{1}{2}, \frac{1}{3}, \frac{2}{5}, \frac{439}{1107}, \frac{462}{1165}, \frac{901}{2272}, ...],$$

pro hodnoty $\{\frac{ed-1}{k} \mid \frac{k}{d}$ je konvergenta $\frac{e}{n}\}$ dostaneme:

$$[\text{udefined}, 44217, 66326, 55272, \frac{1282321}{23}, \frac{2447462}{901}, \text{ dále jen zlomky ...}].$$

Zbývá prověřit pouze tři kandidáty na hodnotu Eulerovy funkce $\varphi(n)$. Testem bude pokus dekomponovat n s využitím hodnoty $\varphi(n)$.

$\varphi(n) = 44217$, $\varphi(n)$ není sudé číslo, konvergenta **nevyhoví**.

$\varphi(n) = 66326$, nesplňuje podmínku $\varphi(n) < n$ **nevyhoví**.

$\varphi(n) = 55272$, $a := \frac{1}{2}(n + 1 - \varphi(n)) = 240$, $\sqrt{a^2 - n} = \sqrt{1849} = 43$, $a \pm 43 \in \{283, 197\}$, **dekompozice n je nalezena**, hledaná konvergenta je 4. v pořadí, tj. $\frac{2}{5}$, odtud ihned plyne dešifrovací exponent $d = 5$. Podmínky Wienerova teorému mohou být dodatečně ověřeny a jsou splněny.

Příklad 61. Nechť $(n, e) = (1277561, 5569)$ je veřejný RSA klíč. Provedeme Wienerův útok. Prověřit podmínky Wienerova teorému předem nelze. Dále uvedené výpočty byly provedeny algebraickým systémem Maple.

Pro koeficienty řetězového zlomku dostaneme:

$$\frac{5569}{1277561} \to [0, 229, 2, 20, 1, 2, 1, 32],$$

odpovídající konvergenty

$$[0, \frac{1}{229}, \frac{2}{459}, \frac{5}{1147}, \frac{32}{7341}, \frac{69}{15829}, \frac{653}{149802}, \frac{722}{315433}, ...],$$

pro hodnoty $\{\frac{ed-1}{k} \mid \frac{k}{d}$ je konvergenta $\frac{e}{n}\}$ dostaneme:

$$[\text{udefined}, 1275300, 1278085, \frac{6387642}{5}, \frac{10220507}{8}, \frac{29383900}{23}, \text{ dále jen zlomky ...}].$$

Zbývá prověřit pouze dva kandidáty na hodnotu Eulerovy funkce $\varphi(n)$. Testem bude pokus dekomponovat n s využitím hodnoty $\varphi(n)$.

$\varphi(n) = 1275300$, $a := \frac{1}{2}(n + 1 - \varphi(n)) = 1131$, $\sqrt{a^2 - n} = \sqrt{1600} = 40$, $a \pm 40 \in \{1091, 1171\}$, **dekompozice n je nalezena**, hledaná konvergenta je 2. v pořadí, tj. $\frac{1}{229}$, odtud ihned plyne dešifrovací exponent $d = 229$. Podmínky Wienerova teorému mohou být dodatečně ověřeny a **nejsou splněny**.

Příklad 62. Nechť $(n, e) = (1277561, 49321)$ je veřejný RSA klíč. Provedeme Wienerův útok. Prověřit podmínky Wienerova teorému předem nelze. Dále uvedené výpočty byly provedeny algebraickým systémem Maple.

Pro koeficienty řetězového zlomku dostaneme:

$$\frac{49321}{1277561} \to [0, 25, 1, 9, 3, 3, 1, 20, 1, 7, 2],$$

odpovídající konvergenty

$$[0, \frac{1}{25}, \frac{1}{26}, \frac{10}{259}, \frac{31}{803}, \frac{103}{2668}, \frac{134}{3471}, \frac{2783}{72088}, ...],$$

pro hodnoty $\{\frac{ed-1}{k} \mid \frac{k}{d}$ je konvergenta $\frac{e}{n}\}$ dostaneme:

$$[\text{udefined}, 1233024, 1282345, \frac{6387069}{5}, \frac{39604762}{31}, \frac{131588427}{103}, \text{ dále jen zlomky ...}].$$

Zbývá prověřit pouze dva kandidáty na hodnotu Eulerovy funkce $\varphi(n)$. Testem bude pokus dekomponovat n s využitím hodnoty $\varphi(n)$.

$\varphi(n) = 1233024$, $a := \frac{1}{2}(n+1-\varphi(n)) = 22269$, $\sqrt{a^2-n} = \sqrt{494630800} = 22240.297 \notin \mathbb{N}$, **nevyhoví**.

$\varphi(n) = 1282345$, nesplňuje podmínku $\varphi(n) < n$, **nevyhoví**.

Wienerův útok je zde neúspěšný. Správným exponentem je $d = 181$, zlomek s tímto jmenovatelem není mezi konvergentami. Nalezneme-li rozklad n jiným způsobem, dostaneme $n = 1277561 = 1091 \cdot 1171$. Podmínky Wienerova teorému mohou být dodatečně ověřeny a **nejsou splněny**.

Grupy

Definice 63. Grupa, abelovská grupa, podgrupa, morfismy grup, mocniny prvků grupy, podgrupa generovaná podmnožinou, cyklická grupa, řád grupy, řád prvku v Grupě, (normální podgrupa), kongruence, faktorová grupa, direktní součin grup, ...

Věta 64. *Nechť $(G, \cdot, 1, \sim)$ je grupa, $g \in G$, $\langle g \rangle$ je konečná (cyklická) podgrupa G. Pak platí:*

1. $\langle g \rangle = \{1, g, ..., g^{r(g)-1}\}$, kde $r(g) = |\langle g \rangle|$ je řád grupy $\langle g \rangle$,
2. $r(g) = \min\{k \in \mathbb{N}^+ |\, g^k = 1\}$.

Věta 65. (*Lagrangeova*) *Nechť $H \subseteq| G$, G je konečná. Pak platí*

$$r(G) = r(H) \cdot [G : H].$$

Důkaz. Definujme relaci $\sim$ na G, $g_1 \sim g_2 \Leftrightarrow (\exists h_1, h_2 \in H)(g_1 h_1 = g_2 h_2)$. Můžeme si všimnout, že platí $g_1 \sim g_2 \Leftrightarrow g_1 H = g_2 H \Leftrightarrow (g_2)^{-1} \cdot g_1 \in H$. Protože $=$ je ekvivalence na podmnožinách G, relace $\sim$ je tudíž relací ekvivalence na G. Pro třídy ekvivalence platí $[g]_\sim = \{g' \mid g' \sim g\} = gH$. Systém $\{gH \mid g \in G\}$ je tedy rozklad množiny G. Pro každé $g \in G$ je funkce $f_g : H \to gH$ definovaná vztahem $f_g(x) = g \cdot x$ bijekce (tzv. levá translace), tj. pro každé $g \in G$ má třída gH stejný počet prvků jako H. Počet prvků grupy G je tedy násobkem počtu prvků podgrupy H, platí tedy $|G| = |H| \cdot k$, $k \in \mathbb{N}^+$, kde číslo k je tzv. index podgrupy H v grupě G, $[G : H] := |G| \,/\, |H|$. Odtud plyne tvrzení věty. □

Věta 66. *Nechť $(G, \cdot, 1, \sim)$ je grupa, $a, b \in G$, $r(a), r(b) \in \mathbb{N}^+$, $k \in \mathbb{Z}$. Pak platí:*

1. $a^k = 1 \Leftrightarrow r(a)|k$,
2. $r(a) = r(\tilde{a})$,
3. $a \cdot b = b \cdot a \wedge \gcd(r(a), r(b)) = 1 \Rightarrow r(ab) = r(a) \cdot r(b)$.

Důkaz. 1 " $\Leftarrow$ " Jestliže $k = \ell \cdot r(a)$, potom platí $a^k = a^{\ell r(a)} = (a^{r(a)})^\ell = 1^\ell = 1$.
" $\Rightarrow$ " Nechť $a^k = 1$. Protože $r(a) \in \mathbb{N}^+$, existují čísla $s, t \in \mathbb{Z}$ taková, že $k = s \cdot r(a) + t$, $0 \leq t < r(a)$. Odtud $1 = a^k = a^{s \cdot r(a)+t} = (a^{r(a)})^s \cdot a^t = 1^s \cdot a^t = a^t$. Kdyby $0 < t$, pak podle Věty 64 by nutně $r(a) \leq t$, což je v rozporu s $0 \leq t < r(a)$. Proto nutně $t = 0$, tj. $k = s \cdot r(a)$, tj $r(a)|k$.

2 Zřejmě platí $a^{r(a)} = 1$, $(\tilde{a})^{r(\tilde{a})} = 1$. Odtud $\left(a^{r(a)}\right)^\sim = \tilde{1}$ tj. $(\tilde{a})^{r(a)} = 1$, obdobně $\left((\tilde{a})^{r(\tilde{a})}\right)^\sim = \tilde{1}$, tj. $a^{r(\tilde{a})} = 1$. Podle bodu 1 $r(\tilde{a})|r(a)$, zároveň $r(a)|r(\tilde{a})$. Odtud plyne rovnost $r(a) = r(\tilde{a})$.

3 Zřejmě $(ab)^{r(a)\cdot r(b)} = (a^{r(a)})^{r(b)} \cdot (b^{r(b)})^{r(a)} = 1^{r(b)} \cdot 1^{r(a)} = 1$, tj. podle bodu 1 $r(ab)|r(a) \cdot r(b)$. Odtud plyne existence čísel r_a, r_b takových, že $r(ab) = r_a r_b$ a $r_a|r(a)$, $r_b|r(b)$, nechť $r(a) = r_a s_a$, $r(b) = r_b s_b$. Pak platí

$$1 = (ab)^{r(ab)} = a^{r_a r_b} b^{r_a r_b}. \tag{10}$$

Odtud plyne $1 = 1^{s_a} = a^{r_a s_a r_b} b^{r_a r_b s_a} = (a^{r(a)})^{r_b} b^{r(a) r_b} = b^{r(a) r_b}$, odtud podle bodu 1 $r(b)|r(a)r_b$, protože $r(a)$, $r(b)$ jsou nesoudělná čísla, podle Příkladu 9 nutně $r(b)|r_b$. Protože $r_b|r(b)$, platí $r(b) = r_b$.
obdobně dostaneme $1 = 1^{s_b} = a^{r_a r_b s_b} b^{r_a r_b s_b} = a^{r_a r(b)} b^{r_a r(b)} = a^{r_a r(b)}$, odtud podle bodu 1 $r(a)|r_a r(b)$, protože $r(a)$, $r(b)$ jsou nesoudělná čísla, podle Příkladu 9 nutně $r(a)|r_a$. Protože $r_a|r(a)$, platí $r(a) = r_a$. Platí tedy

$$r(ab) = r_a r_b = r(a) r(b).$$

□

Poznámka. Mohlo by se zdát, že vlastnost 3. ve Větě 66 má zobecnění $r(ab) = \operatorname{lcm}(a, b)$ bez předpokladu $\gcd(a, b) = 1$. Zdání klame, jak ukazuje příklad grupy $G = \mathbb{Z}_{13}^*$, kde pro prvky $12, 4 \in G$ platí: $r(12) = 2$, $r(4) = 6$, $r(12 \cdot 4) = r(9) = 3 \neq 6 = \operatorname{lcm}(2, 6) = \operatorname{lcm}(r(12), r(4))$.

Věta 67. (*Eulerova*) *Nechť G je konečná grupa. Pak platí:*

$$(\forall g \in G)(g^{|G|} = 1).$$

Důkaz. Nechť $g \in G$, potom $\langle g \rangle \subseteq| G$, podle Lagrangeovy věty $|\langle g \rangle| \cdot [G : \langle g \rangle] = |G|$. Odtud

$$g^{|G|} = g^{|\langle g \rangle| \cdot [G:\langle g \rangle]} = (g^{r(g)})^{[G:\langle g \rangle]} = 1.$$

□

Lemma 68. *Nechť $(G, \cdot, 1)$ je grupa, $g \in G$, $k \in \mathbb{N}^+$. Mějme dále uvedené výroky:*

1. $g^k = 1$,
2. $(\forall \ell \in \mathbb{Z})(g^\ell = 1 \Rightarrow k|\ell)$,
3. $k = r(g)$.

Pak platí: *1.* $\wedge$ *2.* $\Leftrightarrow$ *3.*

Důkaz.
[⇒] : Nechť platí *1.* ∧ *2.* Pak podle *1.* $r(g)|k$ a podle *2.* $k|r(g)$, tj. $k = r(g)$.
[⇐] : Nechť $k = r(g)$. Pak zřejmě platí *1.* a *2.* □

Věta 69. *Nechť $g \in G$, $m \in \mathbb{Z}$, $r(g) \in \mathbb{N}^+$, G je grupa. Pak platí:*

$$r(g^m) = \frac{r(g)}{\gcd(m, r(g))}.$$

Důkaz. Protože $r(g) \in \mathbb{N}^+$, je rovněž $\gcd(m, r(g)) \in \mathbb{N}^+$, položme $k \coloneqq \frac{r(g)}{\gcd(m,r(g))}$. Pak platí

$$(g^m)^k = g^{\frac{mr(g)}{\gcd(m,r(g))}} = g^{\operatorname{lcm}(m,r(g))} = (g^{r(g)})^{\frac{\operatorname{lcm}(m,r(g))}{r(g)}} = 1.$$

Platí tedy bod 1 Lemmatu 68 pro $g^m \in G$, $k \in \mathbb{N}^+$. Nechť dále $\ell \in \mathbb{Z}$ takové, že $(g^m)^\ell = 1$. Potom $r(g)|m\ell$, odtud $\frac{r(g)}{gcd(m,r(g))}|\frac{m\ell}{gcd(m,r(g))}$. Protože $\frac{r(g)}{gcd(m,r(g))}$, $\frac{m}{gcd(m,r(g))}$ jsou nesoudělná čísla, potom nutně $\frac{r(g)}{gcd(m,r(g))}|\ell$, tj $k|\ell$. Platí tedy $(\forall \ell \in \mathbb{Z})((g^m)^\ell = 1 \Rightarrow k|\ell)$, podle Lemmatu 68 to znamená, že $k = r(g^m)$, cbd. □

Věta 70. *Nechť $(G, \cdot, 1)$ je grupa. Pak platí*

1. *Každá cyklická grupa je komutativní.*
2. *Každá podgrupa cyklické grupy je cyklická. Jestliže $\{1\} \neq H \subseteq| G = \langle a \rangle$, potom $H = \langle a^d \rangle$, kde $d \coloneqq \min\{k \in \mathbb{N}^+ \mid a^k \in H\}$.*
3. *Nechť G je grupa $a \in G$, $r(a) \in \mathbb{N}^+$, $k \in \mathbb{Z}$. Potom*
$$r(a^k) = \frac{r(a)}{\gcd(r(a), k)}.$$
4. *Nechť G je konečná cyklická grupa. Pak platí*
$$A \subseteq| G,\ B \subseteq| G, |A| \,|\, |B| \Rightarrow A \subseteq| B,$$
$$A \subseteq| G,\ B \subseteq| G, |A| = |B| \Rightarrow A = B,$$
5. *Nechť G je konečná cyklická grupa. Pak platí:*
$$(\forall d \in \mathbb{N}, d \,|r(G))(\exists! H \subseteq| G)(r(H) = d),$$
$$(\forall d \in \mathbb{N}, d \,|r(G))(\exists! H \subseteq| G)(d \cdot r(H) = r(G)).$$
6. *Nechť G je konečná cyklická grupa, $a, b \in G$. Označme $\operatorname{gen}(H) \coloneqq \{a \in H \mid H = \langle a \rangle\}$ množinu všech generátorů grupy H (Jestliže H není cyklická, potom $\operatorname{gen}(H) = \emptyset$). Pak platí:*
   (a) $r(a) = r(b) \Leftrightarrow \langle a \rangle = \langle b \rangle$, *tj.*
   $$\operatorname{gen}(\langle a \rangle) = \{b \in G \mid r(b) = r(a)\}.$$

(b) Pro množinu všech generátorů grupy $\langle a\rangle$ a její mohutnost platí:

$$\begin{aligned} \mathrm{gen}(\langle a\rangle) &= \{a^k \mid 0 \le k < r(a) \wedge \gcd(k, r(a)) = 1\}, \\ |\mathrm{gen}(\langle a\rangle)| &= \varphi(r(a)). \end{aligned}$$

(c) Nechť $d \in \mathbb{N}^+$, pak platí:

$$\begin{aligned} d \nmid |G| &\Rightarrow \{a \in G \mid r(a) = d\} = \emptyset, \\ d \mid |G| &\Rightarrow |\{a \in G \mid r(a) = d\}| = \varphi(d) \end{aligned}$$

(d) Množina $\{\{b \in G \mid r(b) = m\} \mid m | r(G) \wedge m \in \mathbb{N}^+\}$ tvoří rozklad množiny G, dále pro každé $n \in \mathbb{N}^+$ platí

$$n = \sum_{k|n} \varphi(k).$$

7. *Jestliže je v grupě G prvek řádu $r(a) \in \mathbb{N}^+$, Pak je v grupě G alespoň $\varphi(r(a))$ prvků řádu $r(a)$.*

Příklad 71. V grupě $(\mathbb{Z}_{12}, +, 0)$ určete

1. řády prvků 2, 3, 8,
2. všechny generátory grupy,
3. všechny podgrupy a diagram svazu všech podgrup.

Řešení: *Řády prvků.* Řád prvku a v aditivní grupě je dán vztahem $r(a) = \min\{k \in \mathbb{N}^+ \mid k \times a = 0\}$. Protože platí

$$\begin{aligned} \{1, 2, 3, 4, 5, \mathbf{6}, ...\} \times 2 &= \{2, 4, 6, 8, 10, 12 = 0, ...\}, \\ \{1, 2, 3, \mathbf{4}, 5, 6, ...\} \times 3 &= \{3, 6, 9, 12 = 0, ...\}, \\ \{1, 2, \mathbf{3}, 4, 5, 6, ...\} \times 8 &= \{8, 16 = 6, 24 = 0, ...\}, \end{aligned}$$

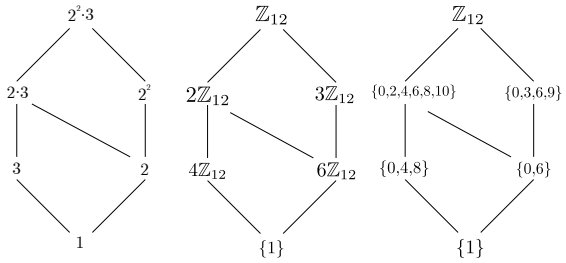
jsou řády prvků následující: $r(2) = 6$, $r(3) = 4$, $r(8) = 3$.

Generátory: Protože každý prvek grupy $\mathbb{Z}_{12}$ je násobkem prvku 1, je prvek 1 jedním z generátorů aditivní grupy $\mathbb{Z}_{12}$. Řád každého generátoru musí být roven řádu grupy a každý prvek jehož řád je roven řádu grupy je generátor grupy. Podle Věty 69 $r(m \times 1) = r(1) = 12$ právě když $\gcd(m, 12) = 1$, tj pro $m \in \{1, 5, 7, 11\}$. Generátory aditivní grupy jsou tedy prvky $\{1, 5, 7, 11\}$.

Svaz podgrup. Protože svaz dělitelů $(\mathrm{div}(12), |\,)$ je izomorfní se svazem podgrup

$$(Sub(\mathbb{Z}_{12}), \subseteq |\,)$$

aditivní grupy $\mathbb{Z}_{12}$, kde izomorfismem je funkce $f(k) = \frac{12}{k}\mathbb{Z}_{12}$, dostáváme:



Obrázek 1: svaz podgrup $(\mathbb{Z}_{12}, +, 0)$

Příklad 72. Vyšetřete grupu $\mathbb{Z}_8^*$.

1. *Počet prvků a možné řády podgrup.* Platí $|\mathbb{Z}_8^*| = \varphi(8) = 2^3 - 2^2 = 4$.
   $x \in \mathbb{Z}_8^* \leftrightarrow x \in \mathbb{Z}_8 \wedge \gcd(x, 8) = 1$, tj.

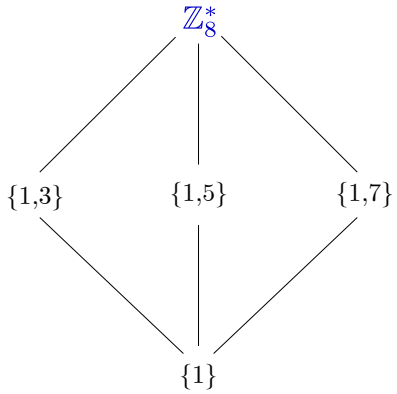
   $$\mathbb{Z}_8^* = \{1, 3, 5, 7\}.$$

   $H \subseteq | \, \mathbb{Z}_8^* \rightarrow |H| \mid |\mathbb{Z}_8^*|$, tj. $|H| \in \{1, 2, 4\}$.

2. *Řády prvků, cyklické podgrupy.* Platí

   $$(\mathbb{Z}_8^*)^2 = \{1, 3, 5, 7\}^2 = \{1, 1, 1, 1\}.$$

   Odtud dostaneme cyklické podgrupy $\langle 1 \rangle = \{1\}$, $\langle 3 \rangle = \{1, 3\}$, $\langle 5 \rangle = \{1, 5\}$, $\langle 7 \rangle = \{1, 7\}$, pro jejich řády platí $r(1) = 1$, $r(3) = r(5) = r(7) = 2$. V grupě neexistuje prvek řádu 4, tj. $\mathbb{Z}_8^*$ není cyklická grupa. Svaz podgrup:$\mathbb{Z}_8^*$



Obrázek 2: svaz $\mathbb{Z}_8^*$

Příklad 73. Vyšetřete grupu $\mathbb{Z}_{12}^*$.

1. *Počet prvků a možné řády podgrup.* Platí $|\mathbb{Z}_{12}^*| = \varphi(3 \cdot 4) = (3 - 1)(2^2 - 2) = 4$.
   $x \in \mathbb{Z}_{12}^* \leftrightarrow x \in \mathbb{Z}_{12} \wedge \gcd(x, 12) = 1$, tj.

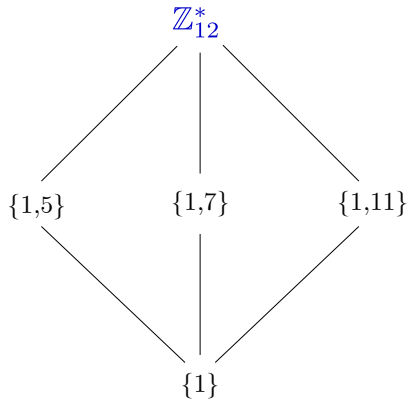
   $$\mathbb{Z}_{12}^* = \{1, 5, 7, 11\}.$$

   $H \subseteq | \, \mathbb{Z}_{12}^* \rightarrow |H| \mid |\mathbb{Z}_{12}^*|$, tj. $|H| \in \{1, 2, 4\}$.

2. *Řády prvků, cyklické podgrupy.* Platí

$$(\mathbb{Z}_{12}^*)^2 = \{1,5,7,11\}^2 = \{1,1,1,1\}.$$

Odtud dostaneme cyklické podgrupy $\langle 1\rangle = \{1\}$, $\langle 5\rangle = \{1,5\}$, $\langle 7\rangle = \{1,7\}$, $\langle 11\rangle = \{1,11\}$, pro jejich řády platí $r(1) = 1$, $r(5) = r(7) = r(11) = 2$. V grupě neexistuje prvek řádu 4, tj. $\mathbb{Z}_{12}^*$ není cyklická grupa. Svaz podgrup:$\mathbb{Z}_{12}^*$



Obrázek 3: svaz $\mathbb{Z}_{12}^*$

3. Uvažujme funkce $f : \mathbb{Z}_8^* \to \mathbb{Z}_{12}^*$ dané relacemi $\begin{pmatrix}1&3&5&7\\1&5&7&11\end{pmatrix}$, $\begin{pmatrix}1&3&5&7\\1&7&5&11\end{pmatrix}$, $\begin{pmatrix}1&3&5&7\\1&7&11&5\end{pmatrix}$, $\begin{pmatrix}1&3&5&7\\1&11&7&5\end{pmatrix}$, atd, jsou izomorfismy $f : \mathbb{Z}_8^* \to \mathbb{Z}_{12}^*$.

Příklad 74. Analyzujte grupu $(\mathbb{Z}_{18}^*, \cdot, 1)$.

1. Protože nosná množina je typu $\mathbb{Z}_{2p^e}^*$, kde $p \in \mathbb{P}$, $p \geq 3$, $e \in \mathbb{N}$, grupa $\mathbb{Z}_{18}^*$ je cyklická.

2. Řád grupy (počet prvků) $|\mathbb{Z}_{18}^*| = \varphi(18) = \varphi(2 \cdot 3^2) = (2-1)\cdot(3^2-3) = 6$. Možné řády podgrup jsou $\{1,2,3,6\}$.

3. U cyklické grupy je svaz podgrup izomorfní se svazem dělitelů řádu grupy, tj

$$(\mathrm{Sub}(\mathbb{Z}_{18}^*), \subseteq | \,) \cong (\mathrm{div}(|\mathbb{Z}_{18}^*|), \,|\,),$$

tedy ke každému děliteli čísla $|\mathbb{Z}_{18}^*|$ existuje právě jedna cyklická podgrupa grupy $\mathbb{Z}_{18}^*$. Jiné podgrupy cyklická grupa nemá.

4. Řády prvků – cyklické podgrupy.

$$\begin{aligned}\mathbb{Z}_{18}^* &= \{\mathbf{1},5,7,11,13,17\},\\ (\mathbb{Z}_{18}^*)^2 &= \{1,7,13,13,7,\mathbf{1}\},\\ (\mathbb{Z}_{18}^*)^3 &= \{1,17,\mathbf{1},17,\mathbf{1},17\}.\end{aligned}$$

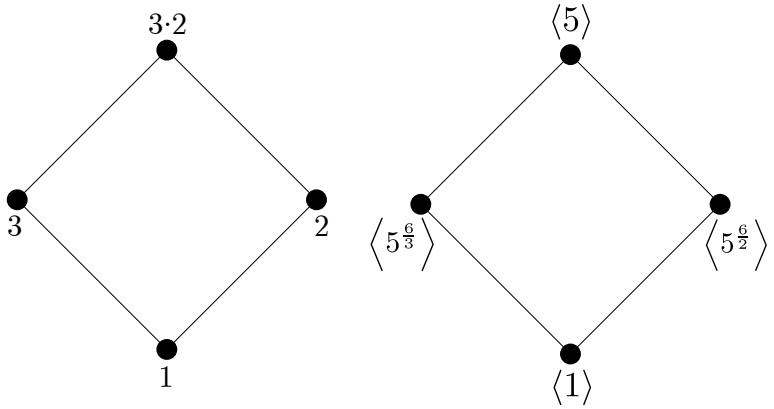
Z uvedených výpočtů vyplývá:
$r(1) = 1$, $\langle 1 \rangle = \{1\}$,
$r(17) = 2$, $\langle 17 \rangle = \{1, 17\}$,
$r(7) = r(13) = 3$, $\langle 7 \rangle = \langle 13 \rangle = \{1, 7, 13\}$,
$r(5) = r(11) = \mathbb{Z}_{18}^* = \{1, 5, 7, 11, 13, 17\}$

5. Svaz podgrup $(\mathrm{Sub}(\mathbb{Z}_{18}^*), \subseteq | \,)$ a dělitelů čísla $|\mathbb{Z}_{18}^*|$, $(\mathrm{div}(\mathbb{Z}_{18}^*), | \,)$. Izomorfizmem svazů

$$f : (\mathrm{div}(\mathbb{Z}_{18}^*), | \,) \to (\mathrm{Sub}(\mathbb{Z}_{18}^*), \subseteq | \,)$$

je například funkce $f(d) = \left\langle 5^{\frac{6}{d}} \right\rangle$.

$$f : (\mathrm{div}(|\mathbb{Z}_{18}^*|, | \,) \to (\mathrm{Sub}(\mathbb{Z}_{18}^*), \subseteq | \,), \quad f(d) = \left\langle 5^{\frac{6}{d}} \right\rangle$$



Obrázek 4: Svaz podgrup $\mathbb{Z}_{18}^* \;\cong\;$ dělitelů $|\mathbb{Z}_{18}^*|$.

Příklad 75. Nechť $(\mathbb{Z}_{25}^*, \cdot, 1)$ je multiplikativní grupa „modulo 25“. Grupa je tvaru $\mathbb{Z}_{p^e}^*$, kde $p \in \mathbb{P}$, $p \geq 3$, tedy je to grupa cyklická. Dále určete:

1. *Velikost grupy*: tj. její řád: $|\mathbb{Z}_{25}^*| = \varphi(5^2) = 5^2 - 5 = 20$.

2. *Prvky grupy*: $\mathbb{Z}_{25}^* = \{[x]_{25} \,|\, x \in \mathbb{N},\, \gcd(x, 25) = 1\}$, tj.

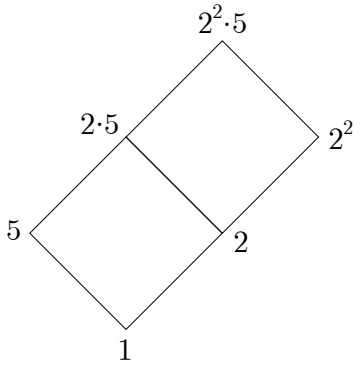
$$\mathbb{Z}_{25}^* = \{1, 2, 3, 4, 6, 7, 8, 9, 11, 12, 13, 14, 16, 17, 18, 19, 21, 22, 23, 24\}.$$

3. *Řád prvku* 6 *a vypočtěte* 6^{57} v $\mathbb{Z}_{25}^*$. Protože $|\mathbb{Z}_{25}^*| = 20$, možné řády jsou $\{1, 2, 4, 5, 10, 20\}$.

$$\begin{aligned} 6^2 &= 36 = 11, \\ 6^4 &= 11^2 = 21, \\ 6^5 &= 6 \cdot 21 = 1. \end{aligned}$$

Protože $6^1 \neq 1$, $6^5 = 1$, je $r(6) = 5$. Odtud plyne $6^{57} = 6^{(57)_5} = 6^2 = 11$.

4. *Generátor grupy* $\mathbb{Z}_{25}^*$. Pro svaz dělitelů čísla 20 platí:



Obrázek 5: svaz dělitelů čísla 20

Odtud zřejmě prvek $a \in \mathbb{Z}_{25}^*$, pro který $a^{10} \neq 1$ a $a^4 \neq 1$ je nutně prvek řádu 20, tj. generátor. Počítáme podle schématu

$$a \overset{()^2}{\longmapsto} a^2 \begin{cases} \overset{()^2}{\longmapsto} & a^4 \neq 1 \\ \overset{()^5}{\longmapsto} & a^{10} \neq 1 \end{cases}$$

Jestliže $a = 2$, dostaneme

$$2 \overset{()^2}{\longmapsto} 4 \begin{cases} \overset{()^2}{\longmapsto} & 16 \neq 1 \\ \overset{()^5}{\longmapsto} & 24 \neq 1 \end{cases}$$

tedy 2 je generátor.

5. *Najděte všechny prvky řádu* 5. Jsou to generátory jediné podgrupy řádu 5, počet jejích generátorů je $\varphi(5) = 4$. Protože jsme nalezli generátor grupy $\mathbb{Z}_{25}^*$, $\mathbb{Z}_{25}^* = \langle 2 \rangle$, hledejme všechny exponenty $k \in \mathbb{N}$, $0 \leq k < |\mathbb{Z}_{25}^*|$ takové, že $r(2^k) = \frac{r(2)}{\gcd(r(2),k)} = 5$, odtud $\gcd(20, k) = \frac{20}{5} = 4$, odtud $k = 4\ell$ a platí $\gcd(5, \ell) = 1$, tj. $\ell \in \{1, 2, 3, 4\}$, tj. $2^k = (2^4)^\ell = 16^\ell$. Všechny prvky řádu 5 jsou

$$\{16, 16^2, 16^3, 16^4\} = \{16, 6, 21, 11\}.$$

6. *Najděte všechna řešení rovnice* $x^5 = 1$ v $\mathbb{Z}_{25}^*$. Řešením jsou všechny prvky grupy $\mathbb{Z}_{25}^*$ jejichž řád je dělitelem čísla 5, tj. jsou to prvky řádu 5 již dříve nalezené, $\{16, 6, 21, 11\}$ a prvek 1. Řešením je tedy podgrupa $\langle 16 \rangle$.

Příklad 76. Vyšetřete grupu $\mathbb{Z}_{15}^*$.

1. *Počet prvků, možné řády podgrup.* Počet prvků $|\mathbb{Z}_{15}^*| = \varphi(15) = (3-1)(5-1) = 8$. Možné řády podgrup, $H \subseteq | \mathbb{Z}_{15}^* \to |H| \mid |\mathbb{Z}_{15}^*|, tj. |H| \in \{1, 2, 4, 8\}$.

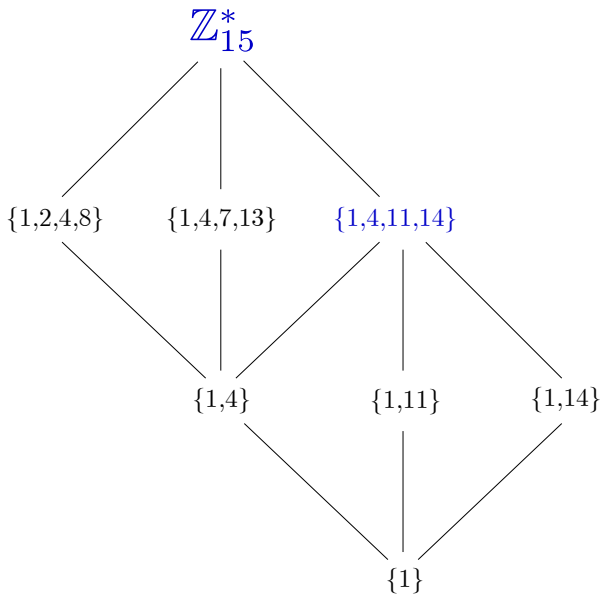
2. *Řády prvků, cyklické podgrupy.*

$$\begin{array}{rcl} \mathbb{Z}_{15}^* & = & \{\mathbf{1} \quad 2 \quad 4 \quad 7 \quad 8 \quad 11 \quad 13 \quad 14\} \\ (\mathbb{Z}_{15}^*)^2 & = & \{1 \quad 4 \quad \mathbf{1} \quad 4 \quad 4 \quad \mathbf{1} \quad 4 \quad \mathbf{1}\} \\ (\mathbb{Z}_{15}^*)^4 & = & \{1 \quad \mathbf{1} \quad 1 \quad \mathbf{1} \quad \mathbf{1} \quad 1 \quad \mathbf{1} \quad 1\} \end{array}$$

Odtud plyne: Cyklická grupa řádu 1: $\langle 1\rangle = \{1\}$,
cyklické grupy řádu 2: $\langle 4\rangle = \{1,4\}$, $\langle 11\rangle = \{1,11\}$, $\langle 14\rangle = \{1,14\}$. Již z tohoto výsledku je zřejmé, že grupa $\mathbb{Z}_{15}^*$ není cyklická, v konečné cyklické grupě totiž nemohou existovat dvě různé podgrupy téhož řádu.
cyklické grupy řádu 4: $\langle 2\rangle = \langle 8\rangle = \{1,2,4,8\}$, $\langle 7\rangle = \langle 13\rangle = \{1,4,7,13\}$.

3. *Necyklické podgrupy.* $\langle 4\rangle \vee \langle 11\rangle = \langle 4\rangle \vee \langle 14\rangle = \langle 11\rangle \vee \langle 14\rangle = \{1,4,11,14\}$
Zřejmě exponent grupy $\exp(\mathbb{Z}_{15}^*) = 4$, protože $\exp(\mathbb{Z}_{15}^*) < |\mathbb{Z}_{15}^*|$, grupa $\mathbb{Z}_{15}^*$ není cyklická.

4. Svaz podgrup $(\mathrm{Sub}(\mathbb{Z}_{15}^*), \subseteq|\,)$: Modře jsou vyznačeny necyklické podgrupy.



Obrázek 6: svaz podgrup $\mathbb{Z}_{15}^*$

Příklad 77. Vyšetřete grupu $\mathbb{Z}_{36}^*$.

1. *Počet prvků, možné řády podgrup.* Počet prvků $|\mathbb{Z}_{36}^*| = \varphi(2^2 3^2) = (2^2-2)(3^2-3) = 12$.
Možné řády podgrup $H \subseteq| \mathbb{Z}_{36}^* \to |H| \mid |\mathbb{Z}_{36}^*|$, *tj.* $|H| \in \{1,2,3,4,6,12\}$.

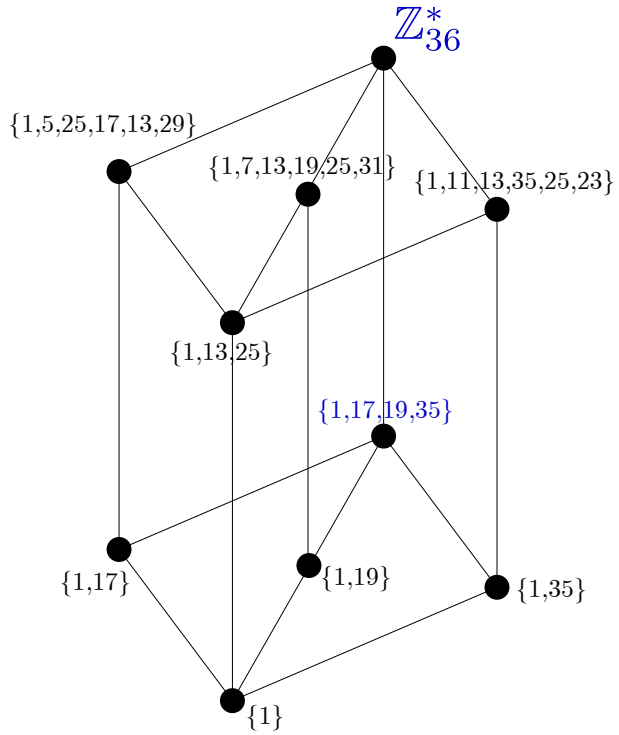
2. *Řády prvků, cyklické podgrupy.*

$$\begin{array}{rcl} \mathbb{Z}_{36}^* = & \{\mathbf{1} & 5 \quad 7 \quad 11 \quad 13 \quad 17 \quad 19 \quad 23 \quad 25 \quad 29 \quad 31 \quad 35\} \\ (\mathbb{Z}_{36}^*)^2 = & \{1 & 25 \quad 13 \quad 13 \quad 25 \quad \mathbf{1} \quad \mathbf{1} \quad 25 \quad 13 \quad 13 \quad 25 \quad \mathbf{1}\} \\ (\mathbb{Z}_{36}^*)^3 = & \{1 & 17 \quad 19 \quad 35 \quad \mathbf{1} \quad 17 \quad 19 \quad 35 \quad \mathbf{1} \quad 17 \quad 19 \quad 35\} \\ (\mathbb{Z}_{36}^*)^4 = & \{1 & 13 \quad 25 \quad 25 \quad 13 \quad 1 \quad 1 \quad 13 \quad 25 \quad 25 \quad 13 \quad 1\} \\ (\mathbb{Z}_{36}^*)^6 = & \{1 & \mathbf{1} \quad \mathbf{1} \quad \mathbf{1} \quad 1 \quad 1 \quad 1 \quad \mathbf{1} \quad 1 \quad \mathbf{1} \quad \mathbf{1} \quad 1\} \end{array}$$

Odtud plyne: Cyklická grupa řádu 1: $\langle 1\rangle = \{1\}$,
cyklické grupy řádu 2: $\langle 17\rangle = \{1, 17\}$, $\langle 19\rangle = \{1, 19\}$, $\langle 35\rangle = \{1, 35\}$,
cyklická grupa řádu 3: $\langle 13\rangle = \langle 25\rangle = \{1, 13, 25\}$,
cyklické grupy řádu 6: $\langle 5\rangle = \{1, 5, 25, 17, 13, 29\}$, $\langle 7\rangle = \{1, 7, 13, 19, 25, 31\}$, $\langle 11\rangle = \{1, 11, 13, 35, 25, 23\}$.
Poznámka: V grupě $\mathbb{Z}_{36}^*$ se tedy nevyskytuje prvek řádu 4, ačkoliv je číslo 4 dělitelem řádu grupy $\mathbb{Z}_{36}^*$. I z toho je patrno, že grupa $\mathbb{Z}_{36}^*$ není cyklická. Stejně tak v konečné cyklické grupě se nemohou vyskytovat dvě různé cyklické podgrupy téhož řádu, zde například $\langle 17\rangle = \{1, 17\} \neq \{1, 19\} = \langle 19\rangle$.

3. *Necyklické grupy.* Necyklická grupa řádu 4: $\langle 17\rangle \vee \langle 19\rangle = \langle 17\rangle \vee \langle 35\rangle = \langle 19\rangle \vee \langle 35\rangle = \{1, 17, 19, 35\}$
Zřejmě $\exp(\mathbb{Z}_{36}^*) = 6$, protože $\exp(\mathbb{Z}_{36}^*) < |\mathbb{Z}_{36}^*|$, grupa $\mathbb{Z}_{36}^*$ není cyklická.

4. *Svaz podgrup* $(\mathrm{Sub}(\mathbb{Z}_{36}^*), \subseteq|\,)$. Modře vyznačeny necyklické podgrupy:



Obrázek 7: svaz podgrup $\mathbb{Z}_{36}^*$

Příklad 78. Vyšetřete grupu $\mathbb{Z}_{27}^*$.

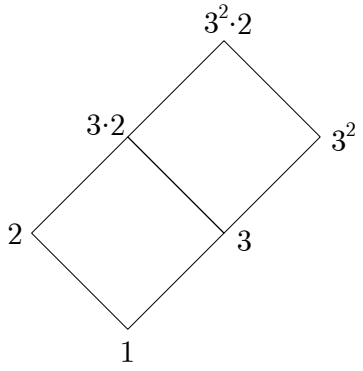
1. *Počet prvků, možné řády podgrup.* Počet prvků $|\mathbb{Z}_{27}^*| = \varphi(3^3) = (3^3 - 3^2) = 18 = 2 \cdot 3^2$. Možné řády podgrup $H \subseteq| \mathbb{Z}_{27}^* \to |H| \mid |\mathbb{Z}_{36}^*|$, *tj.* $|H| \in \{1, 2, 3, 6, 9, 18\}$.

2. *Řády prvků, cyklické podgrupy.* Protože $\mathbb{Z}_{27}^*$ je grupa typu $\mathbb{Z}_{p^e}^*$ kde $p \in \mathbb{P}$, $p \geq 3$, $e \in \mathbb{N}^+$, je to grupa cyklická a všechny její podgrupy jsou cyklické. Svaz jejích podgrup

je izomorfní se svazem všech dělitelů řádu grupy $|\mathbb{Z}_{27}^*|$, jestliže $\mathbb{Z}_{27}^* = \langle g \rangle$, pak pro izomorfismus platí

$$\begin{aligned} (\mathrm{div}(18), \,|\,) &\longrightarrow (\mathrm{Sub}(\mathbb{Z}_{27}^*), \subseteq|\,), \\ d &\longmapsto (\langle g^{\frac{18}{d}} \rangle, \cdot, 1). \end{aligned}$$

3. *Svaz dělitelů* $(\mathrm{div}(18), \,|\,)$.



Obrázek 8: svaz dělitelů čísla 18

4. *Generátory grupy* $\mathbb{Z}_{27}^*$. Podle svazu dělitelů je zřejmé, že každý prvek $g \in \mathbb{Z}_{27}^*$ je generátor $\mathbb{Z}_{27}^*$ právě když $g^{3\cdot 2} \neq 1$ a $g^{3^2} \neq 1$. Při hledání generátoru můžeme postupovat podle schématu:

$$a \overset{()^3}{\longmapsto} a^3 \begin{cases} \overset{()^2}{\longmapsto} & a^6 \neq 1 \\ \overset{()^3}{\longmapsto} & a^9 \neq 1 \end{cases}.$$

Pro prvek $2 \in \mathbb{Z}_{27}^*$ dostaneme

$$2 \overset{()^3}{\longmapsto} 8 \begin{cases} \overset{()^2}{\longmapsto} & 10 \neq 1 \\ \overset{()^3}{\longmapsto} & 26 \neq 1 \end{cases}.$$

Prvek 2 je tedy generátor $\mathbb{Z}_{27}^*$, tj. platí $\mathbb{Z}_{27}^* = \langle 2 \rangle$.
V konečné cyklické grupě $G = \langle g \rangle$ je počet prvků řádu $d \,|\, \big|G\big|$ dán hodnotou $\varphi(d)$, počet generátorů grupy G je tedy $\varphi(\big|G\big|)$, dále platí $\mathrm{gen}(G) = \{g^k \,|\, 0 \leq k < \big|G\big| \wedge \gcd(k, \big|G\big|) = 1\}$.
Odtud plyne

$$\mathrm{gen}(\mathbb{Z}_{27}^*) = 2^{\{1,5,7,11,13,17\}} = \{2, 5, 20, 23, 11, 14\}.$$

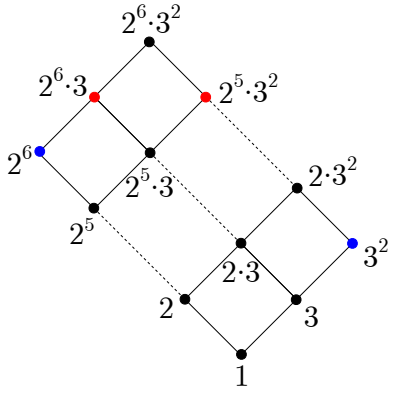
5. *Všechny podgrupy grupy* $\mathbb{Z}_{27}^*$. S využitím izomorfismu

$$d \longmapsto (\langle 2^{\frac{18}{d}} \rangle, \cdot, 1) \,:\, (\mathrm{div}(18), \,|\,) \to (\mathrm{Sub}(\mathbb{Z}_{27}^*), \subseteq|\,)$$

dostaneme: Cyklická podgrupa řádu 1: $\langle 2^{\frac{18}{1}} \rangle = \langle 1 \rangle = \{1\}$,
cyklická podgrupa řádu 2: $\langle 2^{\frac{18}{2}} \rangle = \langle 26 \rangle = \{1, 26\}$,

cyklická podgrupa řádu 3: $\langle 2^{\frac{18}{3}} \rangle = \langle 10 \rangle = \{1, 10, 19\}$,
cyklická podgrupa řádu 6: $\langle 2^{\frac{18}{6}} \rangle = \langle 8 \rangle = \{1, 8, 10, 26, 19, 17\}$,
cyklická podgrupa řádu 9: $\langle 2^{\frac{18}{9}} \rangle = \langle 4 \rangle = \{1, 4, 16, 10, 13, 25, 19, 22, 7\}$,
cyklická podgrupa řádu 18: $\langle 2^{\frac{18}{18}} \rangle = \langle 2 \rangle = \{1, 2, 4, 5, 7, 8, 10, 11, 13, 14, 16, 17, 19, 20, 22, 23, 25, 26\}$.

Příklad 79. Najděte generátor cyklické grupy $\mathbb{Z}^*_{577}$.
Grupa $\mathbb{Z}^*_{577}$ je opravdu cyklická, protože 577 je prvočíslo. Pro řád grupy platí $|\mathbb{Z}^*_{577}| = 576 = 2^6 \cdot 3^2$. Na následujícím obrázku svazu dělitelů řádu grupy $\mathbb{Z}^*_{577}$ jsou barevně vyznačené klíčové exponenty, které hrají úlohu v dále uvedeném algoritmu.



Obrázek 9: Svaz dělitelů $|\mathbb{Z}^*_{577}| = 2^6 \cdot 3^2$.

1. Náhodnou volbou $a \in \mathbb{Z}^*_{577}$ hledejme prvek γ pro který platí

$$\gamma = a^{2^6} \ \wedge \ \gamma^3 = a^{2^6 3} \neq 1.$$

   Nalezený prvek, který splňuje uvedené podmínky, označme γ_1, (prvek si zapamatujeme).

2. Náhodnou volbou $a \in \mathbb{Z}^*_{577}$ hledejme prvek γ pro který platí

$$\gamma = a^{3^2} \ \wedge \ \gamma^{2^5} = a^{2^5 3^2} \neq 1.$$

   Nalezený prvek, který splňuje uvedené podmínky, označme γ_2, (prvek si zapamatujeme).

3. Generátorem grupy $|\mathbb{Z}^*_{577}|$ je prvek $\gamma_1 \cdot \gamma_2$. Tato skutečnost plyne z následujících faktů. Protože $\gamma_1^{3^2} = a^{2^6 \cdot 3^2} = a^{\varphi(n)} = 1$ podle Eulerovy Fermatovy věty, odtud $r(\gamma_1) \,|\, 3^2$. Zároveň $\gamma_1^3 \neq 1$, tj. $r(\gamma_1) \nmid 3$, odtud nutně $r(\gamma_1) = 3^2$.
   Obdobně $\gamma_2^{2^6} = a^{2^6 \cdot 3^2} = a^{\varphi(n)} = 1$ podle Eulerovy Fermatovy věty, tj. $r(\gamma_2) \,|\, 2^6$. Zároveň $\gamma_2^{2^5} \neq 1$, $r(\gamma_2) \nmid 2^5$, odtud nutně $r(\gamma_2) = 2^6$. Řády prvků jsou nesoudělná čísla, proto podle Věty 66 platí $r(\gamma_1\gamma_2) = r(\gamma_1) \cdot r(\gamma_2) = 3^2 \cdot 2^6 = |\mathbb{Z}^*_{577}|$, tj. $\gamma_1\gamma_2$ je generátor grupy $\mathbb{Z}^*_{577}$.

Realizace uvedených kroků.

1. Mocniny počítáme v $\mathbb{Z}^*_{577}$ metodou „opakovaných čtverců“, $\gamma = a^{2^6} = 1aSSSSSS$, $\gamma^3 = 1\gamma S\gamma$, dostaneme tabulku

volba a	$\gamma = 1aSSSSSS$	$\gamma^3 = 1\gamma S\gamma$	poznámka
2	435	363	vyhovuje

Tabulka 1:

2. Mocniny počítáme v $\mathbb{Z}^*_{577}$ metodou „opakovaných čtverců“, $\gamma = a^{3^2} = 1aSSSa$, $\gamma^{2^5} = 1\gamma SSSSS$, dostaneme tabulku

volba a	$\gamma = 1aSSSa$	$\gamma^{2^5} = 1\gamma SSSSS$	poznámka
2	512	1	nevyhovuje
3	65	1	nevyhovuje
5	557	576	vyhovuje

Tabulka 2:

3. Generátorem grupy $|\mathbb{Z}^*_{577}|$ je prvek $\gamma_1 \cdot \gamma_2 = 435 \cdot 557 = 532$.

Příklad 80. Stanovte generátor cyklické grupy $\mathbb{Z}^*_{1009}$. Grupa $\mathbb{Z}^*_{1009}$ je opravdu cyklická, protože 1009 je prvočíslo. Pro řád grupy platí $|\mathbb{Z}^*_{1009}| = 1008 = 2^4 \cdot 3^2 \cdot 7$.

1. Náhodnou volbou $a \in \mathbb{Z}^*_{1009}$ hledejme prvek γ pro který platí

$$\gamma = a^{2^4 \cdot 3^2} \ \wedge \ \gamma \neq 1.$$

   Nalezený prvek, který splňuje uvedené podmínky, označme γ_1, (prvek si zapamatujeme).

2. Náhodnou volbou $a \in \mathbb{Z}^*_{1009}$ hledejme prvek γ pro který platí

$$\gamma = a^{2^4 \cdot 7} \ \wedge \ \gamma^3 \neq 1.$$

   Nalezený prvek, který splňuje uvedené podmínky, označme γ_2, (prvek si zapamatujeme).

3. Náhodnou volbou $a \in \mathbb{Z}^*_{1009}$ hledejme prvek γ pro který platí

$$\gamma = a^{3^2 \cdot 7} \ \wedge \ \gamma^{2^3} \neq 1.$$

   Nalezený prvek, který splňuje uvedené podmínky, označme γ_3, (prvek si zapamatujeme).

4. Generátorem grupy $|\mathbb{Z}^*_{1009}|$ je prvek $\gamma_1 \cdot \gamma_2 \cdot \gamma_3$

Realizace uvedených kroků:

1. Mocniny počítáme v $\mathbb{Z}^*_{1009}$ metodou „opakovaných čtverců“, $\gamma = a^{24\cdot 3^2} = 1aSSSaSSSS$, $\gamma^1 = \gamma$, dostaneme tabulku

volba a	$\gamma = 1aSSSaSSSS$	$\gamma = \gamma$	poznámka
2	105	105	vyhovuje

Tabulka 3:

2. Mocniny počítáme v $\mathbb{Z}^*_{1009}$ metodou „opakovaných čtverců“, $\gamma = a^{24\cdot 7} = 1aSaSaSSSS$, $\gamma^3 = 1\gamma S\gamma$, dostaneme tabulku

volba a	$\gamma = 1aSaSaSSSS$	$\gamma^3 = 1\gamma S\gamma$	poznámka
2	759	374	vyhovuje

Tabulka 4:

3. Mocniny počítáme v $\mathbb{Z}^*_{1009}$ metodou „opakovaných čtverců“, $\gamma = a^{3^2\cdot 7} = 1aSaSaSaSaSa$, $\gamma^{2^3} = 1\gamma SSS$, dostaneme tabulku

volba a	$\gamma = 1aSaSaSaSaSa$	$\gamma^{2^3} = 1\gamma SSS$	poznámka
2	192	1	nevyhovuje
3	192	1	nevyhovuje
5	192	1	nevyhovuje
7	469	1	nevyhovuje
11	179	1008	vyhovuje

Tabulka 5:

4. Generátorem grupy $\mathbb{Z}^*_{1009}$ je $105 \cdot 759 \cdot 179 = 163$

Příklad 81. V grupě $\mathbb{Z}^*_{1225}$ najděte všechny cyklické podgrupy největšího řádu.
Protože $1225 = 5^2 \cdot 7^2$ grupa $\mathbb{Z}^*_{1225}$ není cyklická. Využijme izomorfismu $g : \mathbb{Z}^*_{5^2} \times \mathbb{Z}^*_{7^2} \to \mathbb{Z}^*_{1225}$, $g(u,v) = (7^2Su + 5^2Tv)_{1225}$, kde konstanty S, T, odečteme z matice Eukleidova algoritmu po jeho skončení, tj.

$$\begin{bmatrix} 49 & 1 & 0 \\ 25 & 0 & 1 \end{bmatrix} \to \begin{bmatrix} 1 & -1 & 2 \\ 0 & 25 & -49 \end{bmatrix},$$

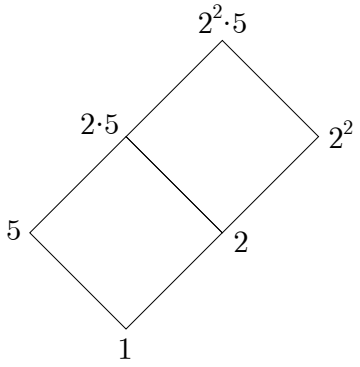
tj. $S = -1$, $T = 2$, tj.

$$g(u,v) \quad = \quad (7^2(-1)u + 5^2 2v)_{1225} = (-49u + 50v)_{1225}.$$

Dále využijeme následujících faktů. Konečné grupy $G_1, ..., G_k$ jsou cyklické právě když je cyklická grupa $G_1 \times ... \times G_k$ a platí pro $i, j \in \{1, ..., k\}$:

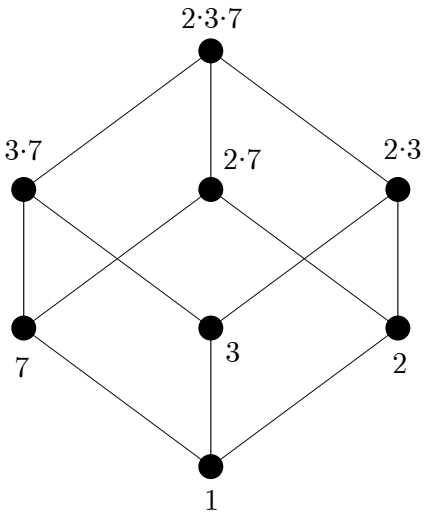
$$\begin{aligned} \langle (a_1, ..., a_k) \rangle = G_1 \times ... \times G_k \quad &\Leftrightarrow \quad G_i = \langle a_i \rangle \wedge i \neq j \Rightarrow \gcd(r(a_i), r(a_j)) = 1, \\ r((a_1, ..., a_k)) \quad &= \quad r(a_1) \cdot ... \cdot r(a_k). \end{aligned}$$

Je třeba nalézt v cyklických grupách $\mathbb{Z}_{5^2}^*$, $\mathbb{Z}_{7^2}^*$, prvky $a \in \mathbb{Z}_{5^2}^*$, $b \in \mathbb{Z}_{7^2}^*$, s nesoudělnými řády, jejichž součin je maximální. Protože $r(a) \in \mathrm{div}(20) = \{1, 2, 4, 5, 10, 20\}$, $r(b) \in \mathrm{div}(42) = \{1, 2, 3, 6, 14, 21, 42\}$. Maximální součin dvou nesoudělných čísel je zřejmě $20 \cdot 21 = 420$. Další takové prvky již neexistují. V grupě $\mathbb{Z}_{5^2}^*$ hledejme prvek řádu 20, tj. její generátor a v grupě $\mathbb{Z}_{7^2}^*$ hledejme prvek řádu 21.
Generátor grupy $\mathbb{Z}_{5^2}^*$. protože svaz dělitelů šísla 20 je dán diagramem:



Obrázek 10: Svaz dělitelů čísla 20

hledáme prvek $a \in \mathbb{Z}_{5^2}^*$ takový, že $a^4 \neq 1$, $a^{2 \cdot 5} \neq 1$. Například pro $a = 2$ máme $a^4 = 16 \neq 1$, $a^{10} = 1024 = 24 \neq 1$, tedy $r(2) = 20$.
Hledejme generátor grupy $\mathbb{Z}_{7^2}^*$. Jestliže $\langle c \rangle = \mathbb{Z}_{7^2}^*$, potom hledaný prvek řádu 21 bude $b = c^2$. Protože svaz dělitelů čsla 42 je dán diagramem:



Obrázek 11: Svaz dělitelů čísla 42

Zřejmě prvek $c \in \mathbb{Z}_{7^2}^*$ je generátorem grupy právě když $c^{3 \cdot 7} \neq 1$, $c^{2 \cdot 7} \neq 1$, $c^{2 \cdot 3} \neq 1$.

c	$c^{21} = 1CSSCSSC$	$c^{14} = 1CSCSCS$	$c^6 = 1CSCS$	poznámka
2	$2^{21} = 1$	$2^{14} = 18 \neq 1$	$2^6 = 15 \neq 1$	nevyhovuje
3	$3^{21} = 30 \neq 1$	$3^{14} = 30 \neq 1$	$3^6 = 43 \neq 1$	vyhovuje

Tabulka 6: Hledání generátoru grupy $\mathbb{Z}^*_{7^2}$

Platí tedy $\langle 3 \rangle = \mathbb{Z}^*_{7^2}$, odtud prvek řádu 21 je $b = 3^{\frac{42}{21}} = 3^2 = 9$.
Generátorem největší cyklické podgrupy grupy $\mathbb{Z}^*_{1225}$ je grupa generovaná prvkem $g(2,9) = (-49 \cdot 2 + 50 \cdot 9)_{1225} = 352$. Tedy

$$\langle 352 \rangle \subseteq| \, \mathbb{Z}^*_{1225}.$$

Jiná taková podgrupa maximálního řádu 420 již neexistuje, číslo 420 je součinem jediné nesoudělné dvojice čísel $(r(a), r(b)) = (20, 21) \in \{1, 2, 4, 5, 10, 20\} \times \{1, 2, 3, 6, 14, 21, 42\}$, přičemž $\langle a \rangle \subseteq| \, \mathbb{Z}^*_{5^2}$, $\langle b \rangle \subseteq| \, \mathbb{Z}^*_{7^2}$, jsou jediné podgrupy uvedených řádů.

Poznámka. Na řádku pro $c = 2$ Tabulky „Hledání generátoru grupy $\mathbb{Z}^*_{7^2}$“ byl nalezen hledaný prvek řádu 21. Jestliže $2^{14} \neq 1$, pak nutně $2^7 \neq 1$, jestliže $2^6 \neq 1$, pak nutně $2^3 \neq 1$, zároveň $2^{21} = 1$, odtud nutně $r(2) = 21$. Odtud můžeme vypočítat další generátor hledané grupy, $g(2,2) = (-49 \cdot 2 + 50 \cdot 2)_{1225} = 2$, máme tedy $\langle 2 \rangle = \langle 352 \rangle$.

Řešení rovnic v grupách a okruzích $\mathbb{Z}_n$.

Příklad 82. *Řešte rovnici $x^{35} = 1$ v grupě $\mathbb{Z}^*_{5^3}$.*

1. *Redukce exponentu.* V konečné grupě $(G, \cdot, 1)$ platí pro $k \in \mathbb{Z}$

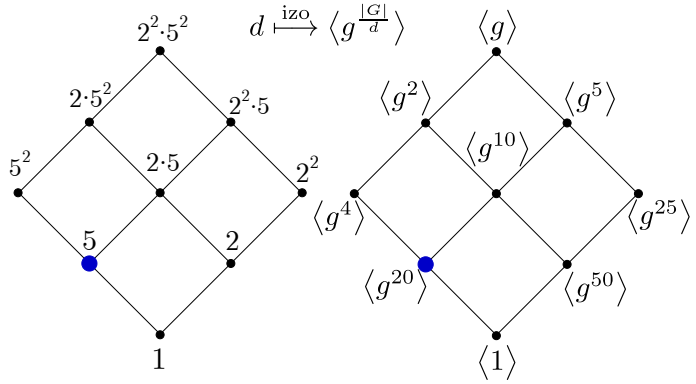
$$d = \gcd(k, |G|) \Rightarrow \{x \in G \,|\, x^k = 1\} = \{x \in G \,|\, x^d = 1\}.$$

   Odtud v $\mathbb{Z}^*_{5^3}$ platí: $\left|\mathbb{Z}^*_{5^3}\right| = 5^3 - 5^2 = 100 = 2^2 \cdot 5^2$, $\gcd(35, 100) = 5 \gcd(7, 20) = 5$, tedy

$$x^{35} = 1 \Leftrightarrow x^5 = 1.$$

2. Grupa $\mathbb{Z}^*_{5^3}$ je cyklická, řešením rovnice je cyklická podgrupa řádu 5. Počet prvků řádu 5, tj. generátorů hledané podgrupy, je $\varphi(5) = 4$, pravděpodobnost, že náhodně vybraný prvek je řádu 5, je malá, $\frac{4}{100}$. Najdeme proto raději generátor grupy $\mathbb{Z}^*_{5^3}$, kterých je daleko více, $\varphi(100) = \varphi(2^2 5^2) = 2 \cdot 20 = 40$.

3. Svaz dělitelů čísla 100 a izomorfní svaz cyklických podgrup. Řád a hledaná podgrupa grupy $\mathbb{Z}^*_{5^3} = \langle g \rangle$ vyznačeny modře.



Obrázek 12: svaz dělitelů $\left|\mathbb{Z}^*_{5^3}\right|$ – podgrup $\mathbb{Z}^*_{5^3}$

4. Generátor grupy $\mathbb{Z}^*_{5^3}$. Podle schématu

$$g \overset{()^5}{\longmapsto} g^5 \overset{()^2}{\longmapsto} g^{10} \begin{cases} \overset{()^2}{\longmapsto} & g^{20} \neq 1 \\ \overset{()^5}{\longmapsto} & g^{50} \neq 1 \end{cases}.$$

   Pro prvek $2 \in \mathbb{Z}^*_{5^3}$ dostaneme

$$2 \overset{()^5}{\longmapsto} 32 \overset{()^2}{\longmapsto} 24 \begin{cases} \overset{()^2}{\longmapsto} & 76 \neq 1 \\ \overset{()^5}{\longmapsto} & 124 \neq 1 \end{cases}.$$

   Prvek 2 je tedy generátor grupy $\mathbb{Z}^*_{5^3}$, generátor grupy řešení rovnice je tedy $2^{20} = 76$. Pro množinu řešení rovnice platí

$$76^{\{0,1,2,3,4\}} = \{1, 76, 26, 101, 51\}.$$

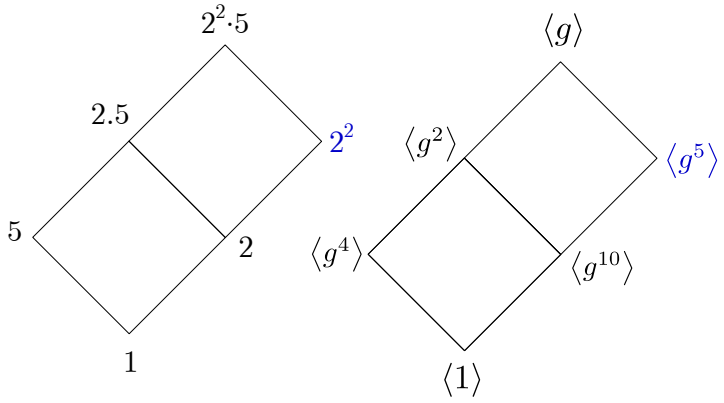
Příklad 83. Řešte rovnici $x^8 = 1$ v $\mathbb{Z}^*_{5^2}$.

1. Redukce exponentu. Protože $\left|\mathbb{Z}^*_{5^2}\right| = \varphi(5^2) = 5^2 - 5 = 20$, $\gcd(8, 20) = 4$, platí v $\mathbb{Z}^*_{5^2}$

$$x^8 = 1 \Leftrightarrow x^4 = 1.$$

2. Grupa $\mathbb{Z}^*_{5^2}$ je cyklická, řešení rovnice $x^4 = 1$ v cyklické grupě je cyklická podgrupa řádu 4. V grupě $\mathbb{Z}^*_{5^2}$ jsou pouze $2 = \varphi(4)$ prvky řádu 4 a $8 = \varphi(20)$ prvků řádu 20, hledáme proto generátor grupy $\mathbb{Z}^*_{5^2}$.

3. Svaz dělitelů čísla 20 a podgrup grupy $\mathbb{Z}^*_{5^2}$. Modře vyznačena hledaná grupa a její řád.



Obrázek 13: svaz dělitelů 20 – podgrup $\mathbb{Z}^*_{5^2}$

4. Generátory $\mathbb{Z}^*_{5^2}$. Prvek $g \in \mathbb{Z}^*_{5^2}$ je generátor $\mathbb{Z}^*_{5^2}$ právě když $g^4 \neq 1$ a $g^{10} \neq 1$. Počítejme podle schematu

$$g \overset{()^2}{\longmapsto} g^2 \begin{cases} \overset{()^2}{\longmapsto} & g^4 \neq 1 \\ \overset{()^5}{\longmapsto} & g^{10} \neq 1 \end{cases}.$$

   Pro prvek 2 platí

$$2 \overset{()^2}{\longmapsto} 4 \begin{cases} \overset{()^2}{\longmapsto} & 16 \neq 1 \\ \overset{()^5}{\longmapsto} & 24 \neq 1 \end{cases}.$$

   Prvek 2 je tedy generátor $\mathbb{Z}^*_{5^2}$.

5. Generátor hledané podgrupy je prvek $2^5 = 32$. Řešením rovnice $x^4 = 1$ jsou prvky grupy $\langle 32 \rangle$ tj platí

$$x^4 = 1 \Leftrightarrow x \in 32^{\{0,1,2,3\}} = \{1, 7, 24, 18\} = \{\pm 1, \pm 7\}.$$

Příklad 84. Řešte rovnici $x^{12} = 1$ v $\mathbb{Z}^*_{15}$.

1. Redukce exponentu. Protože $\left|\mathbb{Z}^*_{15}\right| = \varphi(3 \cdot 5) = 2 \cdot 4 = 8$, $\gcd(12, 8) = 4 \gcd(3, 2) = 4$ lze redukovat exponent v $\mathbb{Z}^*_{15}$,

$$x^{12} = 1 \Leftrightarrow x^4 = 1.$$

2. Grupa $\mathbb{Z}^*_{15}$ není cyklická, lze využít izomorfizmu

$$\mathbb{Z}^*_{15} \underset{g}{\overset{f}{\rightleftarrows}} \mathbb{Z}^*_3 \times \mathbb{Z}^*_5$$

   kde $f(x) = ((x)_3, (x)_5)$, $g(s,t) = (5\tilde{5}s + 3\tilde{3}t)_{15}$ kde $5\tilde{5} + 3\tilde{3} = 1$ v $\mathbb{Z}$. Řešením uvedené diofantické rovnice dostaneme $5 \cdot (-1) + 3 \cdot 2 = 1$, odtud

$$g(s,t) = (-5s + 6t)_{15}.$$

3. Řešení rovnice $x^4 = 1$ v cyklické grupě $\mathbb{Z}_3^*$.
   Redukce exponentu. Protože $\left|\mathbb{Z}_3^*\right| = \varphi(3) = 2$, $\gcd(2,4) = 2$, tj. $x^4 = 1 \Leftrightarrow x^2 = 1$. Řešením je podgrupa řádu 2, tj. řešením je celá grupa $\mathbb{Z}_3^* = \{1,2\}$.

4. Řešení rovnice $x^4 = 1$ v cyklické grupě $\mathbb{Z}_5^*$.
   Redukce exponentu. Protože $\left|\mathbb{Z}_5^*\right| = \varphi(5) = 4$, $\gcd(4,4) = 4$, k redukci exponentu nedojde. Řešením je opět celá grupa $\mathbb{Z}_5^*$, tj. množina prvků $\{1,2,3,4\}$.

5. Využitím izomorfismu získáme řešení rovnice v původní grupě $\mathbb{Z}_{15}^*$, dostaneme:

$$x^{12} = 1 \Leftrightarrow x^4 = 1 \Leftrightarrow x \in (-5\{1,2\} + 6\{1,2,3,4\})_{15} = \{1,7,13,4,11,2,8,14\}.$$

   Řešením je zřejmě celá grupa $\mathbb{Z}_{15}^*$, je to důsledek izomorfismu g a faktu, že řešením rovnice jsou celé podgrupy $\mathbb{Z}_3^*$, $\mathbb{Z}_5^*$.

Příklad 85. Řešte rovnici $x^8 = 1$v $\mathbb{Z}_{21}^*$.

1. Redukce exponentu. Protože $\left|\mathbb{Z}_{21}^*\right| = \varphi(3 \cdot 7) = 2 \cdot 6 = 12$, $\gcd(8,12) = 4$, tj. $x^8 = 1 \Leftrightarrow x^4 = 1$.

2. Grupa $\mathbb{Z}_{21}^*$ není cyklická, lze využít izomorfizmu

$$\mathbb{Z}_{21}^* \underset{g}{\overset{f}{\rightleftarrows}} \mathbb{Z}_3^* \times \mathbb{Z}_7^*$$

   kde $f(x) = ((x)_3, (x)_7)$, $g(s,t) = (7\tilde{7}s + 3\tilde{3}t)_{21}$ kde $7\tilde{7} + 3\tilde{3} = 1$ v $\mathbb{Z}$. Řešením uvedené diofantické rovnice dostaneme $7 \cdot 1 + 3 \cdot (-2) = 1$, odtud

$$g(s,t) = (7s - 6t)_{21}.$$

3. Řešení rovnice $x^4 = 1$ v grupě $\mathbb{Z}_3^*$. Protože $\left|\mathbb{Z}_3^*\right| = 2$ a exponent 4 je násobkem řádu grupy $\mathbb{Z}_3^*$, je řešením rovnice celá grupa, tj. prvky $\{1,2\}$.

4. Řešení rovnice $x^4 = 1$ v grupě $\mathbb{Z}_7^*$. Protože $\left|\mathbb{Z}_7^*\right| = 6$ můžeme redukovat exponent, protože $\gcd(4,6) = 2$, platí v $\mathbb{Z}_7^*$ $x^4 = 1 \Leftrightarrow x^2 = 1$. Řešením rovnice je podgrupa řádu 2, tj zřejmě podgrupa $\{1,-1\} = \{1,6\}$.

5. Řešení rovnice $x^8 = 1 \Leftrightarrow x^4 = 1$ v grupě $\mathbb{Z}_{21}^*$ je množina

$$(7\{1,2\} - 6\{1,-1\})_{21} = \{1,13,8,20\} = \{\pm 1, \pm 8\}.$$

Příklad 86. Řešte rovnici $x^{15} = 1$ v $\mathbb{Z}_{518}^*$.

1. Platí $\mathbb{Z}_{518}^* = \mathbb{Z}_{2\cdot 7\cdot 37}^*$, tj. $\left|\mathbb{Z}_{518}^*\right| = 1 \cdot 6 \cdot 36 = 2^3 3^3$, $\gcd(3 \cdot 5, 2^3 3^3) = 3$, lze tedy redukovat exponent, tj. platí

$$x \in \mathbb{Z}_{518}^* \Rightarrow x^{15} = 1 \Leftrightarrow x^3 = 1.$$

2. Grupa $\mathbb{Z}_{518}^*$ není cyklická, využijeme izomorfismu $\mathbb{Z}_{518}^* \overset{f}{\underset{g}{\rightleftarrows}} \mathbb{Z}_{14}^* \times \mathbb{Z}_{37}^*$ kde grupy $\mathbb{Z}_{14}^*$, $\mathbb{Z}_{37}^*$ jsou cyklické, pro izomorfismus g platí $g(s,t) = (37 \cdot \widetilde{37}s + 14 \cdot \widetilde{14}t)_{518}$, kde konstanty $\widetilde{37}$, $\widetilde{14}$ jsou řešením diofantické rovnice $37 \cdot \widetilde{37} + 14 \cdot \widetilde{14} = 1$. Odtud plyne $\widetilde{37} = -3$, $\widetilde{14} = 8$, tj.

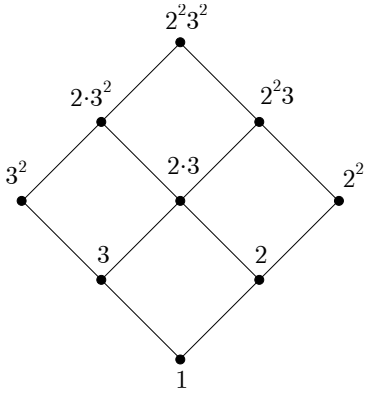
$$g(s,t) = (37 \cdot (-3)s + 14 \cdot 8t)_{518} = (-111s + 112t)_{518}.$$

3. Řešení rovnice $x^3 = 1$ v grupě $\mathbb{Z}_{14}^*$. Platí $\left|\mathbb{Z}_{14}^*\right| = 6$, tedy k redukci exponentu nedochází. K řešení rovnice najdeme generátor grupy $\mathbb{Z}_{14}^*$. Protože svaz podgrup je izomorfní se svazem dělitelů čísla 6, stačí najít prvek $g \in \mathbb{Z}_{14}^*$ pro který $g^2 \neq 1$ a $g^3 \neq 1$. Dostaneme:

$$\begin{array}{rcl} \mathbb{Z}_{14}^* & = & \{1 \quad 3 \quad 5 \quad 9 \quad 11 \quad 13\}, \\ (\mathbb{Z}_{14}^*)^2 & = & \{1 \quad 9 \quad 11 \quad 11 \quad 9 \quad 1\}, \\ (\mathbb{Z}_{14}^*)^3 & = & \{1 \quad \mathbf{13} \quad \mathbf{13} \quad 1 \quad 1 \quad 13\}. \end{array}$$

Našli jsme dva generátory grupy $\mathbb{Z}_{14}^*$, tj. platí $\mathbb{Z}_{14}^* = \langle 3 \rangle$. Řešením rovnice je cyklická grupa řádu 3 pro jejíž generátor platí $3^{\frac{6}{3}}$, tj. $x^3 = 1$ v grupě $\mathbb{Z}_{14}^*$ právě když $x \in \langle 3^2 \rangle = \{1, 9, 11\}$.

4. Řešení rovnice $x^3 = 1$ v grupě $\mathbb{Z}_{37}^*$. Platí $\left|\mathbb{Z}_{37}^*\right| = 36$, tedy k redukci exponentu nedochází. K řešení rovnice využijeme generátor grupy $\mathbb{Z}_{37}^*$. Pokud $\mathbb{Z}_{37}^* = \langle g \rangle$, pak pro grupu všech řešení rovnice $x^3 = 1$ v $\mathbb{Z}_{37}^*$ platí $x^3 = 1 \Leftrightarrow x \in \langle g^{\frac{36}{3}} \rangle = \langle g^{12} \rangle$. Pro svaz dělitelů čísla $36 = 2^2 3^2$ platí:



Obrázek 14: svaz dělitelů čísla 36

Každý prvek $g \in \mathbb{Z}_{37}^*$ pro který platí $g^{2 \cdot 3^2} \neq 1$, a $g^{2^2 \cdot 3} \neq 1$, je generátor grupy $\mathbb{Z}_{37}^*$. Pro výpočet použijeme schéma

$$g \overset{()^3}{\longmapsto} g^3 \overset{()^2}{\longmapsto} g^6 \begin{cases} \overset{()^3}{\longmapsto} & g^{18} \neq 1 \\ \overset{()^2}{\longmapsto} & g^{12} \neq 1 \end{cases}.$$

Pro prvek $2 \in \mathbb{Z}_{37}^*$ dostaneme

$$2 \overset{()^3}{\longmapsto} 8 \overset{()^2}{\longmapsto} 36 \begin{cases} \overset{()^3}{\longmapsto} & 36 \neq 1 \\ \overset{()^2}{\longmapsto} & 1 \neq 1 \end{cases}.$$

Prvek 2 tedy nevyhovuje, zvolme $3 \in \mathbb{Z}_{37}^*$ dostaneme

$$3 \overset{()^3}{\longmapsto} 27 \overset{()^2}{\longmapsto} 26 \begin{cases} \overset{()^3}{\longmapsto} & 1 \neq 1 \\ \overset{()^2}{\longmapsto} & 10 \neq 1 \end{cases}.$$

Prvek 3 tedy nevyhovuje, zvolme $5 \in \mathbb{Z}_{37}^*$ dostaneme

$$5 \overset{()^3}{\longmapsto} 14 \overset{()^2}{\longmapsto} 11 \begin{cases} \overset{()^3}{\longmapsto} & 36 \neq 1 \\ \overset{()^2}{\longmapsto} & 10 \neq 1 \end{cases}.$$

Prvek 5 je tedy generátor grupy, tj. $\mathbb{Z}_{37}^* = \langle 5 \rangle$. Pro podgrupu všech řešení v $\mathbb{Z}_{37}^*$ dostáváme

$$x^3 = 1 \Leftrightarrow x \in \langle 5^{12} \rangle = \langle 10 \rangle = \{1, 10, 26\}.$$

5. Pro řešení rovnice $x^{15} = 1$ v $\mathbb{Z}_{518}^*$ dostaneme pomocí izomorfismu vztah

$$x \in \mathbb{Z}_{518}^* \wedge x^{15} = 1 \Leftrightarrow x \in (-111\{1, 9, 11\} + 112\{1, 10, 26\})_{518} \Leftrightarrow$$
$$\Leftrightarrow x \in \{1, 491, 211, 149, 121, 359, 445, 417, 137\}.$$

Příklad 87. Nechť $(n, e) = (1537, 57)$ $[(n, d) = (1537, 281)]$ je šifrovací klíč protokolu RSA. Najděte všechny zprávy, které se šifrováním nezmění, tj. všechny prvky $x \in \mathbb{Z}_{1537}$ pro které platí v okruhu $\mathbb{Z}_{1537}$ $x^{57} = x$. Řešení se opírá o následující tvrzení:

Tvrzení. Nechť $p \in \mathbb{P}$, $k \in \mathbb{N}$, $k \geq 2$, $e \in \mathbb{N}^+$. Pak v okruhu $(\mathbb{Z}_{p^e}, +, 0, \cdot, 1)$ platí

$$\{x \in \mathbb{Z}_{p^e} \mid x^k = x\} = \{0\} \cup \{x \in \mathbb{Z}_{p^e}^* \mid x^{k-1} = 1\}.$$

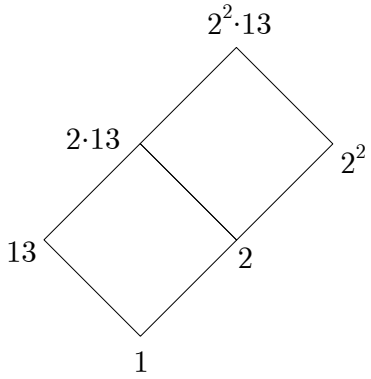
Protože $1537 = 29 \cdot 53$, využijeme izomorfismu $\mathbb{Z}_{1537} \overset{g}{\longleftarrow} \mathbb{Z}_{29} \times \mathbb{Z}_{53}$, kde pro g dostaneme

$$g(s, t) = (-318s + 319t)_{1537}.$$

1. Řešme rovnici $x^{56} = 1$ v $\mathbb{Z}_{29}^*$. Protože $\left|\mathbb{Z}_{29}^*\right| = 28$, $\gcd(28, 56) = 28$, tj. v $\mathbb{Z}_{29}^*$ platí $x^{56} = 1 \Leftrightarrow x^{28} = 1$. Řešení jsou tedy všechny prvky grupy $\mathbb{Z}_{29}^*$.

2. Řešme rovnici $x^{56} = 1$ v $\mathbb{Z}_{53}^*$. Protože $\left|\mathbb{Z}_{53}^*\right| = 52$, $\gcd(52, 56) = 4$, tj. v $\mathbb{Z}_{53}^*$ platí $x^{56} = 1 \Leftrightarrow x^4 = 1$. Řešením jsou tedy všechny prvky podgrupy řádu 4 v grupě $\mathbb{Z}_{53}^*$.

3. Svaz dělitelů čísla $52 = 2^2 \cdot 13$.



Obrázek 15: svaz dělitelů čísla 52

Pro vyhledání generátoru použijeme schéma

$$g \overset{()^2}{\longmapsto} g^2 \begin{cases} \overset{()^{13}}{\longmapsto} & g^{26} \neq 1 \\ \overset{()^2}{\longmapsto} & g^4 \neq 1 \end{cases}.$$

Pro prvek $2 \in \mathbb{Z}_{53}^*$ dostaneme

$$2 \overset{()^2}{\longmapsto} 4 \begin{cases} \overset{()^{13}}{\longmapsto} & 52 \neq 1 \\ \overset{()^2}{\longmapsto} & 16 \neq 1 \end{cases}.$$

Tedy 2 je generátor, $\mathbb{Z}_{53}^* = \langle 2 \rangle$. Pro generátor podgrupy řádu 4, která je řešením rovnice, dostaneme $\langle 2^{\frac{52}{4}} \rangle = \langle 2^{13} \rangle = \langle 30 \rangle = \{1, 30, 52, 23\}$. Platí tedy v $\mathbb{Z}_{53}^*$, $x^{56} = 1 \Leftrightarrow x^4 = 1 \Leftrightarrow x \in \{1, 30, 52, 23\}$.

4. Pomocí izomorfismu g dostaneme všechna řešení rovnice $x^{57} = x$ v okruhu $\mathbb{Z}_{1537}$, dostaneme

$$\begin{aligned} x^{57} = x &\Leftrightarrow x \in (319 \cdot (\{0\} \cup \mathbb{Z}_{29}^*) - 318 \cdot \{0, 1, 30, 52, 23\})_{1537} \\ &\Leftrightarrow x \in (319 \cdot \mathbb{Z}_{29} - 318 \cdot \{0, 1, 30, 52, 23\})_{1537} \end{aligned}$$

Máme tedy celkem $29 \cdot 5 = 145$ zpráv, které se zašifrováním uvedeným klíčem nezmění. Jsou to zprávy
{0, 1, 23, 30, 52, 53, 54, 76, 83, 105, 106, 107, 129, 136, 158, 159, 160, 182, 189, 211, 212, 213, 235, 242, 264, 265, 266, 288, 295, 317, 318, 319, 341, 348, 370, 371, 372, 394, 401, 423, 424, 425, 447, 454, 476, 477, 478, 500, 507, 529, 530, 531, 553, 560, 582, 583, 584, 606, 613, 635, 636, 637, 659, 666, 688, 689, 690, 712, 719, 741, 742, 743, 765, 772, 794, 795, 796, 818, 825, 847, 848, 849, 871, 878, 900, 901, 902, 924, 931, 953, 954, 955, 977, 984, 1006, 1007, 1008, 1030, 1037, 1059, 1060, 1061, 1083, 1090, 1112, 1113, 1114, 1136, 1143, 1165, 1166, 1167, 1189, 1196, 1218, 1219, 1220, 1242, 1249, 1271, 1272, 1273, 1295, 1302, 1324, 1325, 1326, 1348, 1355, 1377, 1378, 1379, 1401, 1408, 1430, 1431, 1432, 1454, 1461, 1483, 1484, 1485, 1507, 1514, 1536}.

Příklad 88. Stejný modul n jako v Příkladu 87, jiný šifrovací exponent e. Nechť $(n,e) = (1537, 59)$, $[(n,d) = (1537, 691)]$ je šifrovací klíč protokolu RSA. Najděte všechny zprávy, které se šifrováním nezmění, tj. všechny prvky $x \in \mathbb{Z}_{1537}$ pro které platí v okruhu $\mathbb{Z}_{1537}$ $x^{59} = x$. Využijeme opět Tvrzení z Příkladu 87.

Protože $1537 = 29 \cdot 53$, využijeme izomorfismu $\mathbb{Z}_{1537} \xleftarrow{g} \mathbb{Z}_{29} \times \mathbb{Z}_{53}$, kde pro g dostaneme

$$g(s,t) = (-318s + 319t)_{1537}.$$

1. Řešme rovnici $x^{58} = 1$ v $\mathbb{Z}_{29}^*$. Protože $\left|\mathbb{Z}_{29}^*\right| = 28$, $\gcd(28, 58) = 2$, tj. v $\mathbb{Z}_{29}^*$ platí $x^{58} = 1 \Leftrightarrow x^2 = 1$. Řešením jsou tedy všechny prvky cyklické podgrupy řádu 2 v grupě $\mathbb{Z}_{29}^*$, zřejmě $x^2 = 1 \Leftrightarrow x \in \{1, -1\} = \{1, 28\}$ v $\mathbb{Z}_{29}^*$.

2. Řešme rovnici $x^{58} = 1$ v $\mathbb{Z}_{53}^*$. Protože $\left|\mathbb{Z}_{53}^*\right| = 52$, $\gcd(52, 58) = 2$, tj. v $\mathbb{Z}_{53}^*$ platí $x^{58} = 1 \Leftrightarrow x^2 = 1$. Řešením jsou tedy všechny prvky podgrupy řádu 2 v grupě $\mathbb{Z}_{53}^*$, zřejmě $x^2 = 1 \Leftrightarrow x \in \{1, -1\} = \{1, 52\}$ v $\mathbb{Z}_{53}^*$.

3. Pomocí izomorfismu g dostaneme všechna řešení rovnice $x^{59} = x$ v okruhu $\mathbb{Z}_{1537}$, dostaneme
$$x^{59} = x \Leftrightarrow x \in (319 \cdot (\{0, 1, -1\}) - 318 \cdot \{0, 1, -1\})_{1537}.$$
Máme tedy celkem 9 zpráv, které se zašifrováním nezmění. Jsou to zprávy
$$\{0, 1, 318, 319, 637, 900, 1218, 1219, 1536\} = \{0, \pm 1, \pm 318, \pm 319, \pm 637\}.$$

Příklad 89. V grupě $\mathbb{Z}_{45}^*$ pomocí izomorfismu $\mathbb{Z}_{45}^* \cong \mathbb{Z}_5^* \times \mathbb{Z}_9^*$ řešte úlohy:

1. Stanovte řády prvků 17, 34 v grupě $\mathbb{Z}_{45}^*$.

2. Najděte všechny prvky řádu 6 v grupě $\mathbb{Z}_{45}^*$.

3. Určete všechny prvky maximálního řádu v grupě $\mathbb{Z}_{45}^*$, tj. prvky $\{x \in \mathbb{Z}_{45}^* \,|\, r(x) = r_m\}$, kde $r_m = \max\{r(x) \,|\, x \in \mathbb{Z}_{45}^*\}$.

Řešení: Nejprve sestavíme potřebné izomorfismy, nechť

$$\mathbb{Z}_{45}^* \underset{g}{\overset{f}{\rightleftarrows}} \mathbb{Z}_5^* \times \mathbb{Z}_9^*,$$

pak platí $f(x) = ((x)_5, (x)_9)$, $g(s,t) = (-9s + 10t)_{45}$, kde koeficienty $(\tilde{9}, \tilde{5}) = (-1, 2)$ izomorfismu $g(s,t) = (9\tilde{9}s + 5\tilde{5}t)_{45}$, jsou řešením diofantické rovnice $9\tilde{9} + 5\tilde{5} = 1$.
Dále využijeme faktu, že pro řády prvků $(a,b) \in \mathbb{Z}_5^* \times \mathbb{Z}_9^*$ platí $r((a,b)) = \mathrm{lcm}(r(a), r(b))$ a že řády prvků jsou děliteli řádů grup, tj platí

$$H \subseteq| \mathbb{Z}_5^* \Rightarrow r(H) \in \{1, 2, 4\},\ H \subseteq| \mathbb{Z}_9^* \Rightarrow r(H) \in \{1, 2, 3, 6\},$$

a že izomorfismy zachovávají řády prvků a grup.

1. • *Řád prvku* 17 v $\mathbb{Z}_{45}^*$.
Platí $f(17) = (2, 8) = (2, -1)$.
Řád prvku 2 v $\mathbb{Z}_5^*$, $2^{\{2,4\}} = \{4, 16\} = \{-1, 1\}$, tj. $r(2) = 4$,
řád prvku -1 v $\mathbb{Z}_9^*$, $(-1)^2 = 1$, tj. $r(-1) = 2$,
řád prvku 17 v $\mathbb{Z}_{45}^*$, $r(17) = \text{lcm}(4, 2) = 4$.

• *Řád prvku* 34 v $\mathbb{Z}_{45}^*$.
Platí $f(34) = (4, 7) = (-1, 7)$.
Řád prvku -1 v $\mathbb{Z}_5^*$, $(-1)^2 = 1$, tj. $r(-1) = 2$,
řád prvku 7 v $\mathbb{Z}_9^*$, $7^{\{2,3,6\}} = \{4, 1, 1\}$, tj. $r(7) = 3$,
řád prvku 34 v $\mathbb{Z}_{45}^*$, $r(34) = \text{lcm}(2, 3) = 6$.

2. *Všechny prvky řádu* 6.
Stanovme všechny dvojice $(r(a), r(b)) \in \{1, 2, 4\} \times \{1, 2, 3, 6\}$, pro které $\text{lcm}(r(a), r(b)) = 6$. Dostaneme:
$$(r(a), r(b)) \in \{(1, 6), (2, 3), (2, 6)\}.$$
Kombinace $(r(a), r(b)) = (1, 6)$,
v $\mathbb{Z}_5^*$ existuje jediný prvek řádu 1, je to prvek 1,
v $\mathbb{Z}_9^*$, existují $\varphi(6) = 2$ prvky řádu 6, jsou to generátory grupy $\mathbb{Z}_9^*$,
$$\begin{array}{rcl} \mathbb{Z}_9^* & = & \{\mathbf{1} \quad 2 \quad 4 \quad 5 \quad 7 \quad 8\}, \\ (\mathbb{Z}_9^*)^2 & = & \{1 \quad 4 \quad 7 \quad 7 \quad 4 \quad \mathbf{1}\}, \\ (\mathbb{Z}_9^*)^3 & = & \{1 \quad 8 \quad \mathbf{1} \quad 8 \quad \mathbf{1} \quad 8\}, \end{array}$$
Protože $2^2 \neq 1$ a $2^3 \neq 1$ potom nutně $r(2) = 6$,
protože $5^2 \neq 1$ a $5^3 \neq 1$ potom nutně $r(5) = 6$.
Prvky řádu 6 pro tuto kombinaci jsou: $\{(1, 2), (1, 5)\}$.

Kombinace $(r(a), r(b)) = (2, 3)$,
v $\mathbb{Z}_5^*$ existuje zřejmě jediný prvek řádu 2, je to prvek -1.
v $\mathbb{Z}_9^*$ existují $\varphi(3) = 2$ prvky řádu 3, podle předchozího výpočtu jsou to prvky 4, 7.
Prvky řádu 6 pro tuto kombinaci jsou $\{(-1, 4), (-1, 7)\}$.

Kombinace $(r(a), r(b)) = (2, 6)$,
podle předchozích výpočtů jsou to prvky $\{(-1, 2), (-1, 5)\}$.

Prvky řádu 6 v grupě $\mathbb{Z}_5^* \times \mathbb{Z}_9^*$ jsou $\{(1, 2), (1, 5), (-1, 4), (-1, 7), (-1, 2), (-1, 5)\}$, pomocí izomorfismu g dostaneme prvky řádu 6 v $\mathbb{Z}_{45}^*$. Platí
$$x \in \mathbb{Z}_{45}^* \Rightarrow r(x) = 6 \Leftrightarrow x \in \{11, 41, 4, 34, 29, 14\}.$$

3. *Všechny prvky v* $\mathbb{Z}_{45}^*$ *maximálního řádu.*
Ke každému děliteli d řádu konečné cyklické grupy existuje v této grupě prvek téhož řádu d. Maximální řád prvku v cyklické grupě $\mathbb{Z}_5^*$ je $\varphi(5) = 4$, maximální řád prvku v

grupě $\mathbb{Z}_9^*$ je $\varphi(9) = 6$, odtud maximální řád prvku v $\mathbb{Z}_{45}^*$ je $r_m = \text{lcm}(4, 6) = 12$.
Hledejme tedy všechny prvky řádu 12 v grupě $\mathbb{Z}_5^* \times \mathbb{Z}_9^*$, tj prvky $(a, b) \in \mathbb{Z}_5^* \times \mathbb{Z}_9^*$ pro které platí $(r(a), r(b)) \in \{1, 2, 4\} \times \{1, 2, 3, 6\}$ a $\text{lcm}(r(a), r(b)) = 12$. Této podmínce vyhovují kombinace

$$(r(a), r(b)) \in \{(4, 3), (4, 6)\}$$

Prvky řádu 4 *tj. generátory grupy* $\mathbb{Z}_5^*$.
Možné řády podgrup $\mathbb{Z}_5^*$ jsou $\{1, 2, 4\}$, prvek $g \in \mathbb{Z}_5^*$ pro který $g^2 \neq 1$ je generátor grupy $\mathbb{Z}_5^*$. Platí

$$\begin{array}{rcl} \mathbb{Z}_5^* & = & \{1 \quad 2 \quad 3 \quad 4\}, \\ (\mathbb{Z}_5^*)^2 & = & \{1 \quad 4 \quad 4 \quad 1\}, \end{array}$$

tedy v grupě $\mathbb{Z}_5^*$ platí $r(x) = 4 \Leftrightarrow x \in \{2, 3\}$.

Prvky řádu 6 *tj. generátory grupy* $\mathbb{Z}_9^*$.
Možné řády podgrup $\mathbb{Z}_9^*$ jsou děliteli $\left|\mathbb{Z}_9^*\right|$ tj. $\{1, 2, 3, 6\}$, prvek $g \in \mathbb{Z}_9^*$ pro který $g^2 \neq 1$ a $g^3 \neq 1$ je generátor grupy $\mathbb{Z}_9^*$. Platí

$$\begin{array}{rcl} \mathbb{Z}_9^* & = & \{1 \quad 2 \quad 4 \quad 5 \quad 7 \quad 8\}, \\ (\mathbb{Z}_9^*)^2 & = & \{1 \quad 4 \quad 7 \quad 7 \quad 4 \quad 1\}, \\ (\mathbb{Z}_9^*)^3 & = & \{1 \quad 8 \quad 1 \quad 8 \quad 1 \quad 8\}, \end{array}$$

uvedenou podmínku splňují dva prvky, tedy v grupě $\mathbb{Z}_9^*$ platí $r(x) = 6 \Leftrightarrow x \in \{2, 5\}$.

Prvky řádu 3 v grupě $\mathbb{Z}_9^*$.
Prvek $g \in \mathbb{Z}_9^*$, pro který platí $g^3 = 1$ a $g \neq 1$, je v $\mathbb{Z}_9^*$ prvek řádu 3, jak plyne ze svazu dělitelů čísla 9. Podle předchozího výpočtu uvedenou podmínku splňují prvky $g \in \{4, 7\}$.

Pro prvky maximálního řádu v grupě $\mathbb{Z}_{45}^*$ tedy platí

$$r(x) = 12 \Leftrightarrow x \in (-9\{2, 3\} + 10\{2, 5, 4, 7\})_{45} = \{2, 32, 22, 7, 38, 23, 13, 43\}.$$

Příklad 90. V grupě $\mathbb{Z}_{64}^*$ najděte všechna řešení rovnice $x^{12} = 1$.

Redukce exponentu. V konečné grupě $(G, \cdot, 1)$ platí ekvivalence $x^k = 1 \Leftrightarrow x^{\gcd(k, |G|)} = 1$. Protože $\mathbb{Z}_{64}^* = \mathbb{Z}_{2^6}^*$, $\left|\mathbb{Z}_{2^6}^*\right| = \varphi(2^6) = 2^5$, $\gcd(12, 2^5) = 4$, platí v $\mathbb{Z}_{64}^*$ $x^{12} = 1 \Leftrightarrow x^4 = 1$.

Grupa $\mathbb{Z}_{64}^*$ však není cyklická, využijme izomorfismu $(\mathbb{Z}_2, +, 0) \times (\mathbb{Z}_{2^4}, +, 0) \xrightarrow{f} \mathbb{Z}_{64}^*$, kde $f(k, \ell) = (-1)^k 5^\ell$. V grupě $(\mathbb{Z}_2, +, 0) \times (\mathbb{Z}_{2^4}, +, 0)$ má rovnice $x^4 = 1$ tvar $4 \times (k, \ell) = (0, 0)$, kde $x = f(k, \ell)$.

Řešení rovnice $4 \times k = 0$ v $(\mathbb{Z}_2, +, 0)$. Řešením je každý prvek aditivní grupy $\mathbb{Z}_2$, protože $4 = 0$ v $\mathbb{Z}_2$.

Řešení rovnice $4 \times \ell = 0$ v $(\mathbb{Z}_{2^4}, +, 0)$. $4 \times \ell = 0$ v $\mathbb{Z}_{2^4}$ právě když existuje $\lambda \in \mathbb{Z}$ takové, že $4{\cdot}\ell = 16{\cdot}\lambda$ v $\mathbb{Z}$, tj. $\ell = 4\lambda$. Řešením v $\mathbb{Z}_{2^4}$ jsou třídy $\ell \in \{4\lambda \mid \lambda \in \{0,1,2,3\}\} = \{0,4,8,12\}$.

Řešení rovnice $x^4 = 1$ v $\mathbb{Z}_{64}^*$. Řešení získáme využitím zmíněného izomorfismu, dostaneme:

$$x^4 = 1 \,\mathrm{v}\, \mathbb{Z}_{64}^* \Leftrightarrow x \in (-1)^{\{0,1\}} \cdot 5^{4\{0,1,2,3\}} = \pm 49^{\{0,1,2,3\}} = \{\pm 1, \pm 49, \pm 33, \pm 17\}.$$

Diskrétní logaritmus

Definice 91. Nechť $(G, \cdot, 1, \sim)$ je grupa, $a \in G$, $r(a) \in \mathbb{N}^+$, potom

$$(\mathbb{Z}_{r(a)}^{\oplus}, \oplus, 0, \ominus) \overset{k \mapsto a^k}{\longrightarrow} (\langle a \rangle, \cdot, 1, \sim)$$

je izomorfismus grup. Existuje tedy inverzní izomorfismus zvaný diskrétní logaritmus dlog_a, pro který platí:

$$(\mathbb{Z}_{r(a)}^{\oplus}, \oplus, 0, \ominus) \overset{\mathrm{dlog}_a}{\longleftarrow} (\langle a \rangle, \cdot, 1, \sim),$$
$$k \in \mathbb{Z}_{r(a)}^{\oplus} \Rightarrow \mathrm{dlog}_a(a^k) = k,$$
$$x \in \langle a \rangle \Rightarrow a^{\mathrm{dlog}_a(x)} = x,$$
$$x \in \langle a \rangle \Rightarrow \mathrm{dlog}_a(\tilde{x}) = \ominus \mathrm{dlog}_a(x),$$
$$\mathrm{dlog}_a(1) = 0.$$

Výpočet hodnoty $\mathrm{dlog}_a(x)$ pro $x \in \langle a \rangle$ se nazývá „Discrete Logarithm Problem“, stručně DLP.

Věta 92. *Nechť* $(G, \cdot, 1, \sim)$ *je grupa,* $a, b \in G$, $r(a) \in \mathbb{N}^+$, $(\mathbb{Z}_{r(a)}^{\oplus}, \oplus, 0, \odot, 1)$ *je standardní okruh celých čísel „modulo* $r(a)$*“, Pak platí:*

$$x, y \in \langle a \rangle \Rightarrow \mathrm{dlog}_a(x \cdot y) = \mathrm{dlog}_a(x) \oplus \mathrm{dlog}_a(y),$$
$$x \in \langle a \rangle, m \in \mathbb{Z} \Rightarrow \mathrm{dlog}_a(x^m) = m \times \mathrm{dlog}_a(x) = (m)_{r(a)} \odot \mathrm{dlog}_a(x),$$
$$x, y \in \langle a \rangle \Rightarrow x^{\mathrm{dlog}_a(y)} = y^{\mathrm{dlog}_a(x)},$$
$$x \in \langle a \rangle = \langle b \rangle \Rightarrow \mathrm{dlog}_a(x) = \mathrm{dlog}_a(b) \odot \mathrm{dlog}_b(x).$$

Věta 93. *Nechť* $(G, \cdot, 1, \sim)$ *je grupa,* $a \in G$, $r(a) = n_1 \cdot n_2 \cdot \ldots \cdot n_k \in \mathbb{N}^+$,
$i \neq j \Rightarrow \gcd(n_i, n_j) = 1$. *Pak dále uvedený diagram je komutativní diagram izomorfismů*

$$\begin{array}{ccc} \langle a \rangle & \overset{\mathrm{dlog}_a}{\longrightarrow} & \mathbb{Z}_{r(a)}^{\oplus} \\ \downarrow f & & \uparrow g \\ \left\langle a^{N_1} \right\rangle \times \cdots \times \left\langle a^{N_k} \right\rangle & \overset{\mathrm{dlog}_{a^{N_1}} \times \cdots \times \mathrm{dlog}_{a^{N_k}}}{\longrightarrow} & \mathbb{Z}_{n_1}^{\oplus} \times \cdots \times \mathbb{Z}_{n_k}^{\oplus} \end{array}$$

kde $N_i n_i = r(a)$, $f(x) = (x^{N_1}, \ldots, x^{N_k})$, $g(y_1, \ldots, y_k) = (\sum_{i=1}^{k} N_i \tilde{N}_i y_i)_{r(a)}$, *tj. platí*

$$\mathrm{dlog}_a(x) = (\sum_{i=1}^{k} N_i \tilde{N}_i \mathrm{dlog}_{a^{N_i}}(x))_{r(a)},$$

kde $N_i \tilde{N}_i = 1 \bmod n_i$, $i \in \{1, \ldots, k\}$.

Poznámka 94. Nechť $(G, \cdot, 1, \sim)$ je grupa, $a, b \in G$. Potom $\mathrm{dlog}_a(b)$ je definován právě když $b \in \langle a \rangle$. Jestliže G je konečná cyklická grupa a platí $b^{r(a)} = 1$, potom $\mathrm{dlog}_a(b)$ je definován. je to důsledek Věty 70, bodu 4.

Věta 95. *Nechť $m, n \in \mathbb{N}^+$, $a \in \mathbb{Z}_n$. Pak platí $a^m \in \mathbb{Z}_n^* \Leftrightarrow a \in \mathbb{Z}_n^*$.*

Příklad 96. (dlog_a – hrubá síla) Stanovte všechna celá čísla $x \in \mathbb{Z}$ pro která v $(\mathbb{Z}_7^*, \odot, 1)$ platí rovnice $5^x = 2$.

Řešení: Výpočet hrubou silou znamená výpočet mocnin $5^{\{0,1,2,3,4,5,6\}} = \langle 5 \rangle = \{1, 5, 4, 6, 2, 3, 1\}$, a vyhledání exponentu, pro který je splněna uvedená rovnice. Řešením je zřejmě exponent 4 v aditivní grupě $\mathbb{Z}_{r(5)}^{\oplus}$, kde $r(5) = 6$, jak jsme zároveň stanovili výpočtem mocnin prvku 5 v multiplikativní grupě grupě $\mathbb{Z}_7^*$.

Uvedeným postupem byl hrubou silou vypočítán diskrétní logaritmus $\mathrm{dlog}_5(2)$. Protože $5 \in \mathbb{Z}_7^*$, má smysl $\mathrm{dlog}_5 : \langle 5 \rangle \to \mathbb{Z}_{r(5)}^{\oplus}$, protože $2 \in \langle 5 \rangle$, řešení rovnice $5^x = 2$ existuje v $\mathbb{Z}_{r(5)}^{\oplus}$ a je jím hodnota $\mathrm{dlog}_5 2 = 4$. Pro řešení v $\mathbb{Z}$ platí $x = \mathrm{dlog}_5(2) + \lambda r(5)$, $\lambda \in \mathbb{Z}$, tj. $x = 4 + \lambda 6$, $\lambda \in \mathbb{Z}$.

Příklad 97. (Obtížnost řešení závisí na zvolené grupě) Stanovte $\mathrm{dlog}_{39} 416$ v aditivní grupě $\mathbb{Z}_{676}^{\oplus}$, tj.

$$\mathrm{dlog}_{39} : \langle 39 \rangle \to \mathbb{Z}_{r(26)}^{\oplus},$$

kde $\langle 39 \rangle \subseteq\mid \mathbb{Z}_{676}^{\oplus}$.
Řešení: V aditivní grupě pro diskrétní logaritmus platí $\mathrm{dlog}_a b \times a = b$, jestliže $b \in \langle a \rangle = \mathbb{Z} \times a$. Odtud $\mathrm{dlog}_{39} 416 \times 39 = 416$, v grupě $\mathbb{Z}_{676}^{\oplus}$ řešme rovnici $x \times 39 = 416$, ekvivalentně v $\mathbb{Z}$ $39x + 676y = 416$. V okruhu $\mathbb{Z}$ platí zákon krácení, rovnici lze krátit číslem 13, po zkrácení řešme diofantickou rovnici $3x + 52y = 32$. Řešením diofantické rovnice dostaneme: $[x, y] = 32[-17, 1] + \lambda[52, -3]$, odtud $x = -544 + \lambda 52 = 28 + \mu 52$, odtud $\mathrm{dlog}_{39} 416 = 28$ v grupě $\mathbb{Z}_{r(39)}^{\oplus}$, kde $r(39) = r(39 \times 1) = \frac{r(1)}{\gcd(39, r(1))} = \frac{676}{\gcd(39,676)} = 52$.

Příklad 98. (dlog_a – hrubá síla) V grupě $(\mathbb{Z}_{15}^*, \odot, 1)$ vypočtěte $\mathrm{dlog}_7 13$, dále stanovte všechna celá čísla $x \in \mathbb{Z}$ pro která v $(\mathbb{Z}_{15}^*, \odot, 1)$ platí rovnice $7^x = 13$.

Řešení: Protože $13, 7 \in \mathbb{Z}_{15}^*$, tvoří mocniny 7^x cyklickou podgrupu $\mathbb{Z}_{15}^*$, $\mathrm{dlog}_7 : \langle 7 \rangle \to \mathbb{Z}_{r(7)}^{\oplus}$, je tedy definován, proto bude v množině $\mathbb{Z}_{r(7)}^{\oplus}$ existovat nejvýše jedno řešení $x \in \mathbb{Z}_{r(7)}^{\oplus}$. Počítejme řád prvku 7 v $\mathbb{Z}_{15}^*$ a zároveň hledejme exponent x, dostaneme $7^{\{1,2,3,4\}} = \{7, 4, 13, 1\}$, platí tedy $x = \mathrm{dlog}_7 13 = 3$ a je to jediné řešení v $\mathbb{Z}_4^{\oplus}$. Pro řešení v $\mathbb{Z}$ platí $x = \mathrm{dlog}_7(13) + \lambda r(7)$, $\lambda \in \mathbb{Z}$, tj. $x = 3 + \lambda 4$, $\lambda \in \mathbb{Z}$.

Příklad 99. (dlog_a – využití izomorfismů) Stanovte $\mathrm{dlog}_{136}(5)$ v $\mathbb{Z}_{143}^*$ a najděte všechna celá čísla $x \in \mathbb{Z}$ pro která v $\mathbb{Z}_{143}^*$ platí $136^x = 5$, jestliže je znám rozklad $143 = 11 \cdot 13$.

Řešení: Protože $143 = 11 \cdot 13$, využijme izomorfismu $\mathbb{Z}_{143}^* \cong \mathbb{Z}_{11}^* \times \mathbb{Z}_{13}^*$. Jestliže existuje nějaké $x \in \mathbb{Z}$ pro které je splněna rovnice $136^x = 5$ v $\mathbb{Z}_{143}^*$, pak pro totéž $x \in \mathbb{Z}$ je splněna jak v $\mathbb{Z}_{11}^*$, tak v $\mathbb{Z}_{13}^*$. Hledejme tedy celá čísla $x \in \mathbb{Z}$, pro která je rovnice $136^x = 5$ splněna v

obou grupách $\mathbb{Z}_{11}^*$, $\mathbb{Z}_{13}^*$.

Řešení $136^x = 5$ *v* $\mathbb{Z}_{11}^*$ *(hrubá síla).* Protože $(136)_{11} = 4$, řešíme v $\mathbb{Z}_{11}^*$ rovnici $4^x = 5$, včetně stanovení řádu prvku 4. Platí $4^{\{1,2,3,4,5,\ldots,10\}} = \{4, 5, 9, 3, 1, \ldots\}$. Všechna celá čísla $x \in \mathbb{Z}$, která řeší rovnici $4^x = 5$, lze psát ve tvaru $x = 2 + \lambda 5$, $\lambda \in \mathbb{Z}$.

Řešení $136^x = 5$ *v* $\mathbb{Z}_{13}^*$ *(hrubá síla).* Protože $(136)_{13} = 6$, řešíme v $\mathbb{Z}_{13}^*$ rovnici $6^x = 5$, včetně stanovení řádu prvku 6. Platí $6^{\{1,2,3,4,5,6,7,8,9,10,11,12\}} = \{6, 10, 8, 9, 2, 12, 7, 3, 5, 4, 11, 1\}$. Všechna celá čísla $x \in \mathbb{Z}$, která řeší rovnici $6^x = 5$, lze psát ve tvaru $x = 9 + \mu 12$, $\mu \in \mathbb{Z}$.

Společné exponenty. Hledejme všechna řešení diofantické rovnice $2 + \lambda 5 = 9 + \mu 12$, tj. $\lambda 5 - \mu 12 = 7$. Platí

$$\begin{bmatrix} 5 & 1 & 0 \\ -12 & 0 & 1 \end{bmatrix} \sim \begin{bmatrix} 5 & 1 & 0 \\ 3 & 3 & 1 \end{bmatrix} \sim \begin{bmatrix} 3 & 3 & 1 \\ 2 & -2 & -1 \end{bmatrix} \sim \begin{bmatrix} 2 & -2 & -1 \\ 1 & 5 & 2 \end{bmatrix} \sim \begin{bmatrix} 1 & 5 & 2 \\ 0 & 12 & 5 \end{bmatrix},$$

platí tedy $[\lambda, \mu] = 7 \cdot [5, 2] + \alpha \cdot [12, 5]$, $\alpha \in \mathbb{Z}$, odtud např. $\lambda = 35 + 12\alpha$, a tedy

$$\begin{aligned} x &= 2 + 5\lambda = 2 + 5(35 + 12\alpha) = 177 + 60\alpha, \in \mathbb{Z}, \\ x &= 57 + 60\beta,\ \beta \in \mathbb{Z}. \end{aligned}$$

Protože $f(136) = (4, 6) \in \mathbb{Z}_{11}^* \times \mathbb{Z}_{13}^*$, kde $r(4) = 5$ v $\mathbb{Z}_{11}^*$, $r(6) = 12$ v $\mathbb{Z}_{13}^*$, odtud $r((4, 6)) = \mathrm{lcm}(r(4), r(6)) = 60$, odtud $\mathrm{dlog}_{136}(5) = 57$.

Příklad 100. (dlog_a – využití izomorfismů) Vypočtěte $\mathrm{dlog}_{2411}(674)$ v $\mathbb{Z}_{4199}^*$ pokud je definován, jestliže je znám rozklad $4199 = 13 \cdot 17 \cdot 19$.

Řešení: Protože $674, 2411 \in \mathbb{Z}_{4199}^*$, úloha bude mít řešení pokud $674 \in \langle 2411 \rangle \subseteq| \mathbb{Z}_{4199}^*$, potom $\mathrm{dlog}_{2411}(674) \in \mathbb{Z}_{r(2411)}^{\oplus}$ a platí $2411^{\mathrm{dlog}_{2411}(674)} = 674$ v $\mathbb{Z}_{4199}^*$. Řešení rovnice $2411^x = 674$ hledejme s využitím izomorfismu $\mathbb{Z}_{4199}^* \cong \mathbb{Z}_{13}^* \times \mathbb{Z}_{17}^* \times \mathbb{Z}_{19}^*$.

Řešení rovnice $2411^x = 674$ *v* $\mathbb{Z}_{13}^*$. V $\mathbb{Z}_{13}^*$ má rovnice tvar $6^x = 11$. Hrubá síla dává

$$6^{\{1,2,3,4,5,6,7,8,9,10,11,12\}} = \{6, 10, 8, 9, 2, 12, 7, 3, 5, 4, 11, 1\},$$

odtud plyne řešení $x = 11 + 12\alpha$, $\alpha \in \mathbb{Z}$.

Řešení rovnice $2411^x = 674$ *v* $\mathbb{Z}_{17}^*$. V $\mathbb{Z}_{17}^*$ má rovnice tvar $14^x = 11$. Hrubá síla dává

$$14^{\{1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16\}} = \{14, 9, 7, 13, 12, 15, 6, 16, 3, 8, 10, 4, 5, 2, 11, 1\},$$

odtud plyne řešení $x = 15 + 16\beta$, $\beta \in \mathbb{Z}$.

Řešení rovnice $2411^x = 674$ *v* $\mathbb{Z}_{19}^*$. V $\mathbb{Z}_{19}^*$ má rovnice tvar $17^x = 9$. Hrubá síla dává

$$17^{\{1,2,3,4,5,6,7,8,9\}} = \{17, 4, 11, 16, 6, 7, 5, 9, 1\},$$

odtud plyne řešení $x = 8 + 9\gamma$, $\gamma \in \mathbb{Z}$.

Hledaný exponent x je řešením soustavy kongruencí

$$\begin{aligned} x &= 11 \bmod 12, \\ x &= 15 \bmod 16, \\ x &= 8 \bmod 9. \end{aligned}$$

Poslední dvě rovnice můžeme řešit čínskou větou o zbytcích, dostaneme

$$\begin{aligned} x &= 9 \cdot \tilde{9} \cdot 15 + 16 \cdot \tilde{16} \cdot 8 + 144\lambda, \\ 1 &= 9 \cdot (-7) + 16 \cdot (4), \text{ tj. } \tilde{9} = -7,\ \tilde{16} = 4, \\ x &= -945 + 512 + 144\lambda = 143 + 144\beta. \end{aligned}$$

Dále řešíme soustavu $x = 11 + 12\alpha = 143 + 144\beta$, tj $12\alpha - 144\beta = 132$, $\alpha - 12\beta = 11$. Odtud zřejmě $\alpha = 11 + 12\beta$, $\beta \in \mathbb{Z}$ a tedy

$$x = 11 + 12\alpha = 11 + 12(11 + 12\beta) = 143 + 144\beta,\ \beta \in \mathbb{Z}.$$

Protože dlog_{2411} je izomorfismus $\langle 2411 \rangle \to \mathbb{Z}^{\oplus}_{r(2411)}$, z nalezeného řešení plyne $r(2411) = 144$ a $\mathrm{dlog}_{2411} = 143 = -1$.

Příklad 101. Vypočtěte $\mathrm{dlog}_{2411}(674)$ v $\mathbb{Z}^*_{4199}$ s využitím izomorfismu cyklické podgrupy $\langle 2411 \rangle \subseteq\!| \mathbb{Z}^*_{4199}$ a CRT-izomorfismu aditivní grupy $\mathbb{Z}^{\oplus}_{r(2411)}$.

Za tím účelem je potřeba zjistit řád grupy $\langle 2411 \rangle$. Jestliže je znám rozklad $4199 = 13 \cdot 17 \cdot 19$, k určení řádu grupy $\langle 2411 \rangle$ je možné užít izomorfismu $f : \mathbb{Z}^*_{4199} \to \mathbb{Z}^*_{13} \times \mathbb{Z}^*_{17} \times \mathbb{Z}^*_{19}$, $f(x) = ((x)_{13}, (x)_{17}, (x)_{19})$.

Řešení: Pro řád prvku $r(2411)$ s využitím izomorfismu $f(x) = ((x)_{13}, (x)_{17}, (x)_{19})$, platí $r(2411) = r(f(2411)) = r((6, 14, 17) = \mathrm{lcm}(r(6), r(14), r(17))$ kde $r(6)$ je řád prvku 6 v grupě $\mathbb{Z}^*_{13}$. Snadno se zjistí (hrubou silou) že $\langle 6 \rangle = \mathbb{Z}^*_{13}$, tj. $r(6) = 12$. Obdobně, $r(14)$ je řád prvku 14 v grupě $\mathbb{Z}^*_{17}$, opět se snadno zjistí, že $\langle 14 \rangle = \mathbb{Z}^*_{17}$, tj. $r(14) = 16$. Pro řád prvku 17 v grupě $\mathbb{Z}^*_{19}$ obdobně vyjde $r(17) = 9$. Odtud $r(6, 14, 17) = \mathrm{lcm}(r(6), r(14), r(17)) = \mathrm{lcm}(12, 16, 9) = \mathrm{lcm}(\mathrm{lcm}(12, 16), 9) = \mathrm{lcm}(4 \cdot \mathrm{lcm}(3, 4), 9) = \mathrm{lcm}(48, 9) = 3 \cdot \mathrm{lcm}(16, 3) = 9 \cdot 16$. Řád prvku 2411 v grupě $\mathbb{Z}^*_{4199}$ je tedy složené číslo $9 \cdot 16$, kde $\gcd(9, 16) = 1$, což umožňuje vzužít k redukci výpočtů dále uvedených izomorfismů z Věty 93.

Pro výpočet diskrétního logaritmu $\mathrm{dlog}_{2411}(674)$ využijeme dále izomorfismu

$$h : \langle 2411 \rangle \to \left\langle 2411^{16} \right\rangle \times \left\langle 2411^{9} \right\rangle,\ h(x) = (x^{16}, x^{9}),$$

a CRT-izomorfismu

$$g : \mathbb{Z}^{\oplus}_{9} \times \mathbb{Z}^{\oplus}_{16} \to \mathbb{Z}^{\oplus}_{9 \cdot 16},\ g(u, v) = (64u - 63v)_{144},$$

podle dále uvedeného diagramu.

$$\begin{array}{ccc} 674 \in \langle 2411 \rangle & \stackrel{\mathrm{dlog}_{2411}}{\longrightarrow} & \mathbb{Z}^{\oplus}_{9 \cdot 16} \\ \downarrow h & & \uparrow g \\ \langle 2411^{16} \rangle \times \langle 2411^{9} \rangle & \stackrel{\mathrm{dlog}_{2411^{16}} \times \mathrm{dlog}_{2411^{9}}}{\longrightarrow} & \mathbb{Z}^{\oplus}_{9} \times \mathbb{Z}^{\oplus}_{16} \\ \| & \| & \| \\ \langle 1582 \rangle \times \langle 343 \rangle & \mathrm{dlog}_{1582} \times \mathrm{dlog}_{343} & \mathbb{Z}^{\oplus}_{9} \times \mathbb{Z}^{\oplus}_{16} \end{array}.$$

Dostaneme metodou opakovaných čtverců v grupě $\mathbb{Z}_{4199}^*$ $h(674) = (674^{16}, 674^9) = (783, 3440)$.
Dále počítáme diskrétní logaritmy (hrubou silou) avšak v cyklických grupách menších řádů:
$\mathrm{dlog}_{1582}783$. Hledejme exponent $k \in \mathbb{Z}_9^{\oplus}$ takový, že $1582^k = 783$. Dostaneme

$$1582^{\{0,1,2,3,4,5,6,7,\mathbf{8}\}} = \{1, 1582, 120, 885, 1803, 1225, 2211, 35, \mathbf{783}\},$$

tj. $\mathrm{dlog}_{1582}783 = 8$.
$\mathrm{dlog}_{343}3440$. Hledejme exponent $k \in \mathbb{Z}_{16}^{\oplus}$ takový, že $343^k = 3440$. Dostaneme

$$343^{\{0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,\mathbf{15}\}} =$$
$$= \{1, 343, 77, 1217, 1730, 1331, 3041, 1711, 3212, 1578, 3782, 3934, 1483, 590, 818, \mathbf{3440}\},$$

tj. $\mathrm{dlog}_{343}3440 = 15$. Odtud dále dostaneme
$\mathrm{dlog}_{2411}674 = g(8, 15) = (64 \cdot 8 - 63 \cdot 15)_{144} = 143$.

Věta 102. *(Babystep – Giantstep algoritmus DLP) Nechť $(G, \cdot, 1)$ je grupa, $g, h \in G$, $r(g) \in \mathbb{N}^+$. Pak platí,* $\mathrm{dlog}_g h$ *existuje právě když množiny $\{g^k \,|\, k \in \{0, 1, ..., n-1\}\}$, $\{hg^{-n\ell} \,|\, \ell \in \{0, 1, ..., n-1\}\}$ mají neprázdný průnik, kde $n := \lceil \sqrt{r(g)} \rceil$ ($\lceil x \rceil$ celá část čísla x,* tzv „ceil“, $\lceil x \rceil \in \mathbb{Z}$, $\lceil x \rceil - 1 < x \leq \lceil x \rceil$). *Jestliže*

$$\{g^k \,|\, k \in \{0, 1, ..., n-1\}\} \cap \{hg^{-n\ell} \,|\, \ell \in \{0, 1, ..., n-1\}\} \neq \emptyset,$$

pak existují indexy $k, \ell \in \{0, 1, ..., n-1\}$ takové, že $g^k = hg^{-n\ell}$, odtud $\mathrm{dlog}_g h = (k + n\ell)_{r(g)}$.

Příklad 103. Metodou „Babystep – Giantstep“ vypočtěte $\mathrm{dlog}_{136}5$ v grupě $\mathbb{Z}_{143}^*$.
Řešení: Položme $n := \lceil \sqrt{\varphi(143)} \rceil = \lceil 10.95 \rceil = 11$. Řád prvku 136 nám není znám, pro výpočet n vezmeme proto řád grupy$\mathbb{Z}_{143}^*$, tedy hodnotu větší, $\varphi(143) = 120$.
Dále sestavíme posloupnost „babystep“

$$\{(136^k)_{143} \,|\, k \in \{0, 1, ..., 11\}\} = \{1, 136, \mathbf{49}, 86, 113, 67, 103, \mathbf{137}, 42, 135, 56, (37)\}$$

Dále vypočtěme EE–algoritmem 37^{-1} v grupě $\mathbb{Z}_{143}^*$. Dostaneme

$$\begin{bmatrix} 37 & 1 & 0 \\ 143 & 0 & 1 \end{bmatrix} \sim \begin{bmatrix} 37 & 1 & 0 \\ 32 & -3 & 1 \end{bmatrix} \sim \begin{bmatrix} 5 & 4 & -1 \\ 32 & -3 & 1 \end{bmatrix} \sim \begin{bmatrix} 5 & 4 & -1 \\ 2 & -27 & 7 \end{bmatrix} \sim \begin{bmatrix} 1 & 58 & -15 \\ 2 & -27 & 7 \end{bmatrix} \sim \begin{bmatrix} 1 & 58 & -15 \\ 0 & -143 & 37 \end{bmatrix},$$

tj. $37^{-1} = 58$, tj. $136^{-11} = 58$. Dále sestavíme posloupnost „giant step“

$$\{(5 \cdot 58^k)_{143} \,|\, k \in \{0, 1, ..., 10\}\} = \{5, 4, 89, 14, 97, \mathbf{49}, 125, 100, 80, 64, \mathbf{137}\}.$$

V posloupnostech máme dvě shody, ze kterých plyne v grupě $\mathbb{Z}_{143}^*$, $136^2 = 5 \cdot (136^{-11})^5$, odtud $136^{57} = 5$. Dále dostaneme $136^7 = 5 \cdot (136^{-11})^{10}$, tj. rovněž platí $136^{117} = 5$. Z uvedených rovnic plyne $136^{117-57} = 136^{60} = 1$ tj. řád prvku 136 je opravdu menší než $\varphi(143) = 120$. Platí tedy $\mathrm{dlog}_{136}5 = (57)_{r(136)}$.
Určeme řád prvku 136. Zřejmě $r(136) \,|\, 60$, kde $60 = 2^2 \cdot 3 \cdot 5$. Protože dolní sousedé ve svazu dělitelů čísla 60 jsou čísla 30, 20, 12 a zároveň platí $136^{30} = 12 \neq 1$, $136^{20} = 133 \neq 1$, $136^{12} = 27 \neq 1$, odtud nutně $r(136) = 60$, tj. $\mathrm{dlog}_{136}5 = (57)_{60} = 57$.

Příklad 104. Vypočtěte $\mathrm{dlog}_{202}100$ v grupě $\mathbb{Z}^*_{463}$ s využitím CRT-izomorfismu aditivní grupy $\mathbb{Z}^{\oplus}_{r(202)}$ a odpovídajících izomorfismů cyklické grupy $\langle 202\rangle$.

Řešení: Protože 463 je prvočíslo, grupa $\mathbb{Z}^*_{463}$ je cyklická. Pro řád grupy platí $|\mathbb{Z}^*_{463}| = 462 = 2\cdot 3\cdot 7\cdot 11$. Označme $(n_1,n_2,n_3,n_4) := (2,3,7,11)$, $N := n_1\cdot n_2\cdot n_3\cdot n_4 = 462$, $N_i n_i = N$, tj. $(N_1,N_2,N_3,N_4) = (231,154,66,42)$. Odtud $202^{\{231,154,66,42\}} = \{462,21,118,134\}$, tj. 202 je generátor grupy, tj. $\mathbb{Z}^*_{463} = \langle 202\rangle$, dále $\langle 202\rangle \overset{\mathrm{dlog}_{202}}{\longrightarrow} \mathbb{Z}^{\oplus}_{462}$ je izomorfismus grup k jehož výpočtu je podle Věty 93 možno užít rovnici

$$\mathrm{dlog}_{202}100 = (\sum_{i=1}^{4} N_i\tilde{N}_i \mathrm{dlog}_{202^{N_i}}(100^{N_i}))_N.$$

- Výpočet $\mathrm{dlog}_{202^{N_1}}(100^{N_1}) = \mathrm{dlog}_{202^{231}}(100^{231})$. Prvek $202^{231} = 462$, je generátor cyklické podgrupy řádu $n_1 = 2$, $100^{231} = 1$, odtud $\mathrm{dlog}_{202^{231}}(100^{231}) = \mathrm{dlog}_{462}(1) = 0$.
  Mocniny 202^{231}, 100^{231} jsme vypočetli metodou opakovaných čtverců,
  $231 = 11100111_2 \sim 1XSXSXSSSXSXSX$. 202^{231}, $uX = (u\cdot 202)_{463}$, $uS = (u^2)_{463}$, dostali jsme

  $$202^{231} \sim 202, 60, 82, 242, 269, 133, 95, 228, 219, 272, 310, 259, \mathbf{462}.$$

  100^{231}, $uX = (u\cdot 100)_{463}$, $uS = (u^2)_{463}$, dále

  $$100^{231} \sim 100, 277, 383, 381, 134, 362, 15, 225, 276, 244, 324, 338, \mathbf{1}.$$

- Výpočet $\mathrm{dlog}_{202^{N_2}}(100^{N_2}) = \mathrm{dlog}_{202^{154}}(100^{154})$. Prvek $202^{154} = 21$ je generátor cyklické podgrupy řádu $n_2 = 3$, $100^{154} = 1$, odtud $\mathrm{dlog}_{202^{154}}(100^{154}) = \mathrm{dlog}_{21}(1) = 0$.
  Mocniny 202^{154}, 100^{154} jsme vypočetli metodou opakovaných čtverců, $154 = 10011010_2 \sim 1XSSSXSXSSXS$.
  202^{154}, $uX = (u\cdot 202)_{463}$, $uS = (u^2)_{463}$, dostali jsme

  $$202^{154} \sim 202, 60, 359, 167, 398, 58, 141, 435, 321, 22, \mathbf{21}.$$

  100^{154}, $uX = (u\cdot 100)_{463}$, $uS = (u^2)_{463}$, dále

  $$100^{154} \sim 100, 277, 334, 436, 78, 65, 18, 324, 338, 1, \mathbf{1}.$$

- Výpočet $\mathrm{dlog}_{202^{N_3}}(100^{N_3}) = \mathrm{dlog}_{202^{66}}(100^{66})$. Prvek $202^{66} = 118$ je generátor cyklické podgrupy řádu $n_3 = 7$, $100^{66} = 230$, odtud $\mathrm{dlog}_{202^{66}}(100^{66}) = \mathrm{dlog}_{118}(230)$, vypočteme později.
  Mocniny 202^{66}, 100^{66} jsme vypočetli metodou opakovaných čtverců, $66 = 1000010_2 \sim 1XSSSSSXS$.
  202^{66}, $uX = (u\cdot 202)_{463}$, $uS = (u^2)_{463}$, dostaneme

  $$202^{66} \sim 202, 60, 359, 167, 109, 306, 233, \mathbf{118}.$$

  100^{66}, $uX = (u\cdot 100)_{463}$, $uS = (u^2)_{463}$, dostaneme

  $$100^{66} \sim 100, 277, 334, 436, 266, 380, 34, \mathbf{230}.$$

Výpočet $\mathrm{dlog}_{118}(230)$ metodou „babystep–giantstep“. Řád prvku 118 je znám, $r(118) = 7$, $n := \lceil\sqrt{7}\rceil = 3$, sestavme posloupnost „babystep“

$$\{(118^k)_{463} \,|\, k \in \{0,1,2,3\}\} = \{1, \mathbf{118}, 34, (308)\}.$$

Z „babystep“ máme vypočteno $118^3 = 308$, pak inverzi pomocí EE–algoritmu:

$$\begin{bmatrix}308 & 1 & 0\\ 463 & 0 & 1\end{bmatrix} \sim \begin{bmatrix}308 & 1 & 0\\ 155 & -1 & 1\end{bmatrix} \sim \begin{bmatrix}155 & -1 & 1\\ 153 & 2 & -1\end{bmatrix} \sim \begin{bmatrix}155 & -1 & 1\\ 2 & -3 & 2\end{bmatrix} \sim$$
$$\sim \begin{bmatrix}1 & 230 & -153\\ 2 & -3 & 2\end{bmatrix} \sim \begin{bmatrix}1 & 230 & -153\\ 0 & -463 & 308\end{bmatrix},$$

pro „giantstep“ tedy platí

$$\{(230 \cdot (118)^{-3k})_{463} \,|\, k \in \{0,1,2\}\} = \{(230 \cdot 230^k)_{463} \,|\, k \in \{0,1,2\}\} = \{230, \mathbf{118}, 286\}.$$

Z uvedených posloupností došlo ke shodě $118^1 = 230 \cdot (118)^{-3 \cdot 1}$, odtud plyne $118^4 = 230$, odtud tedy platí $\mathrm{dlog}_{118}(230) = 4$.

- Výpočet $\mathrm{dlog}_{202^{N_4}}(100^{N_4}) = \mathrm{dlog}_{202^{42}}(100^{42})$. Prvek $202^{42} = 134$ je generátor podgrupy řádu $n_4 = 11$, $100^{42} = 337$.

  Mocniny 202^{42}, 100^{42} byly vypočteny metodou opakovaných čtverců, $42 = 101010_2 \sim 1XSSXSSXS$.
  202^{42}, $uX = (u \cdot 202)_{463}$, $uS = (u^2)_{463}$, dostali jsme

  $$202^{42} \sim 202, 60, 359, 290, 297, 239, 126, 134.$$

  100^{42}, $uX = (u \cdot 100)_{463}$, $uS = (u^2)_{463}$, dále

  $$100^{42} \sim 100, 277, 334, 64, 392, 411, 356, 337.$$

  Výpočet $\mathrm{dlog}_{134}(337)$ metodou „babystep–giantstep“. Řád prvku 134 je znám, $r(134) = 11$, $n := \lceil\sqrt{11}\rceil = 4$, sestavme posloupnost „babystep“

  $$\{(134^k)_{463} \,|\, k \in \{0,1,2,3,4\}\} = \{1, 134, \mathbf{362}, 356, (15)\}.$$

  Z „babystep“ výpočtu dostáváme $134^4 = 15$,
  Vypočtěme nejdříve 15^{-1}, pomocí EE–algoritmu:

  $$\begin{bmatrix}15 & 1 & 0\\ 463 & 0 & 1\end{bmatrix} \sim \begin{bmatrix}15 & 1 & 0\\ 13 & -30 & 1\end{bmatrix} \sim \begin{bmatrix}2 & 31 & -1\\ 13 & -30 & 1\end{bmatrix} \sim \begin{bmatrix}2 & 31 & -1\\ 1 & -216 & 7\end{bmatrix} \sim \begin{bmatrix}1 & -216 & 7\\ 0 & 463 & -15\end{bmatrix}$$

  pro „giantstep“ tedy platí

  $$\{(337 \cdot (134)^{-4k})_{463} \,|\, k \in \{0,1,2,3\}\} = \{(337 \cdot (-216)^k)_{463} \,|\, k \in \{0,1,2,3\}\} = \{337, \mathbf{362}, 55, 158\}.$$

  Z uvedených posloupností došlo ke shodě $134^2 = 337 \cdot (134)^{-4 \cdot 1}$, odtud plyne $134^6 = 337$, odtud tedy platí $\mathrm{dlog}_{134}(337) = (6)_{11} = 6$.

Pro $\mathrm{dlog}_{202}100$ je podle vzorce potřeba dopočítat inverze

$$\begin{aligned}
231 \cdot \tilde{N}_1 = 1 \bmod 2 &\Rightarrow \tilde{N}_1 = 1,\\
154 \cdot \tilde{N}_2 = 1 \bmod 3 &\Rightarrow \tilde{N}_2 = 1 \bmod 3 \Rightarrow \tilde{N}_2 = 1,\\
66 \cdot \tilde{N}_3 = 1 \bmod 7 &\Rightarrow 3\tilde{N}_3 = 1 \bmod 7 \Rightarrow \tilde{N}_3 = 5,\\
42 \cdot \tilde{N}_4 = 1 \bmod 11 &\Rightarrow 9\tilde{N}_4 = 1 \bmod 11 \Rightarrow \tilde{N}_4 = 5,
\end{aligned}$$

tedy platí $\mathrm{dlog}_{202}100 = (231 \cdot 1 \cdot 0 + 154 \cdot 1 \cdot 0 + 66 \cdot 5 \cdot 4 + 42 \cdot 5 \cdot 6)_{462} = 270$.

Definice 105. (Diffieova–Hellmanova distribuce klíčů symetrického šifrování, metoda distribuce DH) Publikováno v r. 1976

1. Nechť grupa $(G, \cdot, 1)$, prvek $g \in G$, $r(g) \in \mathbb{N}^+$ jsou veřejně známy.
2. Alice zvolí tajné číslo $a \in \mathbb{N}^+$, $a < r(g)$, vypočte v grupě G $A \coloneqq g^a$, hodnotu A pošle Bobovi.
3. Bob zvolí tajné číslo $b \in \mathbb{N}^+$, $b < r(g)$, vypočte v grupě G $B \coloneqq g^b$, hodnotu B pošle Alici.
4. Alice vypočte klíč symetrického šifrovacího protokolu $K \coloneqq B^a = g^{ba}$.
5. Bob vypočte klíč symetrického šifrovacího protokolu $K \coloneqq A^b = g^{ab}$.

Definice 106. (Diffieův–Helmanův problém, DHP) Je dána grupa $(G, \cdot, 1)$, a jsou dány prvky $g, A, B \in G$ a existují celá čísla $a, b \in \mathbb{Z}$ taková, že $A = g^a$, $B = g^b$, čísla $a, b \in \mathbb{Z}$ nejsou známa. Má se stanovit g^{ab}.
Definujme relaci $\mathrm{dhp} \subseteq \langle g \rangle^3$ takovou, že

$$\mathrm{dhp} \coloneqq \{(g^a, g^b, g^{ab}) \,|\, a, b \in \mathbb{Z}\},$$

rozhodnout, zda trojice $(A, B, C) \in \langle g \rangle^3$ je prvkem dhp je ekvivalentní formulace DHP.

O řešení Diffieova–Helmanova problému má zájem ten, kdo poslouchá komunikační kanál při Diffieově–Hellmanově distribuci klíčů a zachytí hodnoty A, B a je mu známa grupa $(G, \cdot, 1)$ a prvek $g \in G$, konečného řádu $r(g) \in \mathbb{N}^+$. Vyřešením Diffieova–Helmanova problému tak útočník získá šifrovací klíč symetrického šifrovacího protokolu.

Definice 107. (Šifrovací protokol Elgamalův, El-Gamal) Navržen Taherem Elgamalem v roce 1985.
Jestliže Alice chce být příjemcem šifrovaných zpráv v protokolu El-Gamal, pak provede následující kroky:

1. Alice zvolí grupu $(G, \cdot, 1)$ a prvky $g \in G$, $a \in \mathbb{Z}$. Dále vypočte $A := g^a$ v grupě G.
2. Alice zveřejní grupu $(G, \cdot, 1)$ a prvky g, $A \in G$,

3. Alice utají číslo $a \in \mathbb{Z}$.

Jestliže Bob chce poslat šifrovaně protokolem El–Gamal zprávu Alici, provede následující kroky

1. Získá veřejně dostupné parametry, tj. grupu $(G, \cdot, 1)$ a prvky g, $A \in G$.
2. Zvolí $k \in \mathbb{Z}$ tzv. „jepičí“ klíč a zprávu $m \in G$, kterou chce poslat Alici. V grupě G vypočte dvě veličiny $(c_1, c_2) \coloneqq (g^k, mA^k)$.
3. Dvojici prvků (c_1, c_2), která je v tomto protokolu šifrovanou zprávou, pošle Alici.

Alice po obdržení dvojice (c_1, c_2) dešifruje zprávu výpočtem v grupě G v následujícím kroku:

1. $c_2(c_1^a)^{-1} = mA^k(g^{ka})^{-1} = m(g^{ak})(g^{ka})^{-1} = m$.

Příklad 108. Dva účastníci protokolu, **A**lice, **B**ob, se rozhodnou sestavit klíč symetrického šifrován metodou DH. Jak budou postupovat?

A&B Společně a veřejně se dohodnou na grupě, nechť $G = \mathbb{Z}_{127}^*$.

A&B Společně a veřejně vyberou prvek $g \in G$ co nejvyššího řádu (ztíží to výpočet dlog_g). Protože 127 je prvočíslo, G je cyklická grupa, A&B vyberou její generátor, např. $g \coloneqq 3$.

A Alice zvolí (náhodně) číslo a, $1 < a < r(g) = \mathbb{Z}_{127}^* = 126$, např. $a = 55$, vypočte $A \coloneqq g^a$, číslo A pošle Bobovi.
Výpočet $A \coloneqq g^a$ metodou opakovaných čtverců:

$$55 = 110111_2 \leftrightarrow XSXSSXSXSX,\ uX = (u \cdot 3)_{127},\ uS = (u \cdot u)_{127},$$
$$A = 3^{55} = 1XSXSSXSXSX \to 3, 9, 27, 94, 73, 92, 82, 119, 64, \mathbf{65},$$

tedy $A = 65$.

B Bob zvolí (náhodně) číslo b, $1 < b < r(g) = \mathbb{Z}_{127}^* = 126$, např. $b = 101$, vypočte $B \coloneqq g^b$, číslo B pošle Alici.
Výpočet $B \coloneqq g^b$ metodou opakovaných čtverců:

$$101 = 1100101_2 \leftrightarrow XSXSSSXSSX,\ uX = (u \cdot 3)_{127},\ uS = (u \cdot u)_{127},$$
$$B = 3^{101} = 1XSXSSSXSSX \to 3, 9, 27, 94, 73, 122, 112, 98, 79, \mathbf{110},$$

tedy $B = 110$.

A Alice po obdržení čísla $B = 110$ vypočte klíč $K \coloneqq B^a = 110^{55}$, metodou opakovaných čtverců, kde $uX = (u \cdot 110)_{127}$, $uS = (u \cdot u)_{127}$, dostane:

$$K = 110^{55} = 1XSXSSXSXSX \to 110, 35, 40, 76, 61, 106, 60, 123, 16, \mathbf{109}.$$

Alice tedy získala klíč symetrické šifry $K = 109$.

B Bob po obdržení čísla $A = 65$ vypočte klíč $K := A^b = 65^{101}$, metodou opakovaných čtverců, kde $uX = (u \cdot 65)_{127},\ uS = (u \cdot u)_{127}$, dostane:

$$K = 65^{101} = 1XSXSSSXSSX \to 65, 34, 51, 61, 38, 47, 7, 49, 115, \mathbf{109}.$$

Bob tedy získal klíč symetrické šifry $K = 109$.

Příklad 109. Dva účastníci protokolu, **A**lice, **B**ob, se rozhodnou sestavit klíč symetrického šifrován metodou DH. Jak budou postupovat?

A&B Společně a veřejně se dohodnou na grupě, nechť $G = \mathbb{Z}^*_{291}$.

A&B Společně a veřejně vyberou prvek $g \in G$ co nejvyššího řádu (ztíží to výpočet dlog_g). Protože $291 = 3 \cdot 97$, grupa G není cyklická. S využitím CRT izomorfismu $\mathbb{Z}^*_{291} \cong \mathbb{Z}^*_3 \times \mathbb{Z}^*_{97}$, A&B vyberou prvek maximálního řádu v $\mathbb{Z}^*_{291}$ tak, že v cyklických grupách $\mathbb{Z}^*_3$, $\mathbb{Z}^*_{97}$, vyberou jejich generátory, např. $g_1 := 2$, $g_2 := 5$. Potom pro řád prvku (g_1, g_2) platí $r((g_1, g_2)) = \mathrm{lcm}(r(g_1), r(g_2)) = \mathrm{lcm}(2, 96) = 96$. S využitím CRT izomorfismu dostaneme

$$g := (97 \cdot \tilde{97} \cdot 2 + 3 \cdot \tilde{3} \cdot 5)_{291} = (97 \cdot 2 - 96 \cdot 5)_{291} = 5$$

A Alice zvolí (náhodně) číslo a, $1 < a < r(g) = |\langle g \rangle| = 96$, např. $a = 50$, vypočte $A := g^a$, číslo A pošle Bobovi.
Výpočet $A := g^a = 5^{50}$ metodou opakovaných čtverců:

$$50 = 110010_2 \leftrightarrow XSXSSSXS,\ uX = (u \cdot 5)_{291},\ uS = (u \cdot u)_{291},$$
$$A = 5^{50} = 1XSXSSSXS \to 5, 25, 125, 202, 64, 22, 110, \mathbf{169},$$

tedy $A = 169$.

B Bob zvolí (náhodně) číslo b, $1 < b < r(g) = |\langle g \rangle| = 96$, např. $b = 73$, vypočte $B := g^b$, číslo B pošle Alici.
Výpočet $B := g^b = 5^{73}$ metodou opakovaných čtverců:

$$73 = 1001001_2 \leftrightarrow XSSSXSSSX,\ uX = (u \cdot 5)_{291},\ uS = (u \cdot u)_{291},$$
$$A = 5^{73} = 1XSSSXSSSX \to 5, 25, 43, 103, 224, 124, 244, 172, 278$$

tedy $B = 278$.

A Alice po obdržení čísla $B = 278$ vypočte klíč $K := B^a = 278^{50}$, metodou opakovaných čtverců, kde $uX = (u \cdot 278)_{291},\ uS = (u \cdot u)_{291}$, dostane:

$$K = 278^{50} = 1XSXSSSXS \to 278, 169, 131, 283, 64, 22, 5, \mathbf{25}.$$

Alice tedy získala klíč symetrické šifry $K = 25$.

B Bob po obdržení čísla $A = 169$ vypočte klíč $K := A^b = 169^{73}$, metodou opakovaných čtverců, kde $uX = (u \cdot 169)_{291},\ uS = (u \cdot u)_{291}$, dostane:

$$K = 169^{73} = 1XSSSXSSSX \to 169, 43, 103, 133, 70, 244, 172, 193, \mathbf{25}.$$

Bob tedy získal klíč symetrické šifry $K = 25$.

Příklad 110. Účastníci protokolu symetrické šifry se pro distribuci klíčů rozhodli použít Diffieovy–Hellmanovy metody distribuce klíčů, za tím účelem se dohodli na grupě $\mathbb{Z}_{11}^*$ a prvku $2 \in \mathbb{Z}_{11}^*$. Odposlechem komunikace byla zjištěna výměna parametrů 6 a 3. Jaký klíč k šifrování použili?

Řešení: Při Diffieově–Hellmanově metodě si účastníci vyměňují hodnoty $A = g^a$, $B = g^b$, přitom grupa $(G, \cdot, 1)$ a prvek $g \in G$ jsou známi. Klíčem je prvek $K = A^b = B^a = g^{ab}$. Ze zadání příkladu máme

$$6 = 2^a,\ 3 = 2^b,\ K = 2^{ab} = 6^b = 3^a.$$

Vypočtěme číslo b z rovnice $2^b = 3$ v $\mathbb{Z}_{11}^*$. Dostaneme hrubou silou $2^{\{1,2,3,4,5,6,7,8,9,10\}} = \{2, 4, 8, 5, 10, 9, 7, 3, 6, 1\}$, odtud plyne $b = 8$, $2^8 = 3$ v $\mathbb{Z}_{11}^*$, tudíž $K = 6^8 = 4$.

Příklad 111. Účastníci protokolu symetrické šifry se pro distribuci klíčů rozhodli použít Diffieovy–Hellmanovy metody distribuce klíčů, za tím účelem se dohodli na grupě $\mathbb{Z}_{1441}^*$ a prvku $2 \in \mathbb{Z}_{1441}^*$. Odposlechem komunikace byla zjištěna výměna parametrů 73 a 53. Jaký klíč k šifrování použili?

Řešení: Při Diffieově–Hellmanově metodě si účastníci vyměňují hodnoty $A = g^a$, $B = g^b$, přitom grupa $(G, \cdot, 1)$ a prvek $g \in G$ jsou známi. Klíčem je prvek $K = A^b = B^a = g^{ab}$. Ze zadání příkladu máme

$$73 = 2^a,\ 53 = 2^b,\ K = 2^{ab} = 73^b = 53^a.$$

Vypočtěme číslo b z rovnice $2^b = 53$ v $\mathbb{Z}_{1441}^*$. Je třeba vypočítat hodnotu diskrétního logaritmu

$$\langle 2 \rangle \xrightarrow{\mathrm{dlog}_2} \mathbb{Z}_{r(2)}^{\oplus}$$

v bodě 53.

Nejprve určeme řád prvku 2 v grupě $\mathbb{Z}_{1441}^*$. Protože $1441 = 11 \cdot 131$, využijeme CRT izomorfismu $\mathbb{Z}_{1441}^* \to \mathbb{Z}_{11}^* \times \mathbb{Z}_{131}^*$, $2 \mapsto (2, 2)$, k jeho určení.

• Určení řádu prvku 2 v grupě $\mathbb{Z}_{11}^*$. Vzhledem k malému řádu grupy $\mathbb{Z}_{11}^*$ použijme „hrubou sílu“, tj. $2^{\{1,2,3,4,5,6,7,8,9,10\}} = \{2, 4, 8, 5, 10, 9, 7, 3, 6, 1\}$, odtud plyne $r(2) = 10$ v $\mathbb{Z}_{11}^*$, tj. 2 je generátor grupy $\mathbb{Z}_{11}^*$.

• Určení řádu prvku 2 v grupě $\mathbb{Z}_{131}^*$. Protože 131 je prvočíslo, grupa $\mathbb{Z}_{131}^*$ je cyklická řádu $130 = 2 \cdot 5 \cdot 13$. Vypočtěme mocniny

$$2^{\{5 \cdot 13, 2 \cdot 13, 2 \cdot 5\}} = 2^{\{65, 26, 10\}} = \{130, 53, 107\},$$

tedy v každém dolním sousedu čísla 130 svazu dělitelů čísla 130 je mocnina čísla 2 různá od 1, řád prvku 2 je tedy nutně 130, tj 2 je generátor grupy $\mathbb{Z}_{131}^*$, tj. $r(2) = 130$ v grupě $\mathbb{Z}_{131}^*$. Vzhledem k CRT izomorfismu $(2, 2) \mapsto 2$ prvek 2 má v grupě $\mathbb{Z}_{1441}^*$ řád $r(2) = \mathrm{lcm}(10, 130) = 130$.

Dále vypočteme $\mathrm{dlog}_2(53)$ **s využitím CRT-izomorfismu na straně aditivní grupy** $\mathbb{Z}^{\oplus}_{r(2)}$.

Protože $r(2) = 130 = 2{\cdot}5{\cdot}13$, definujme $(n_1, n_2, n_3) \coloneqq (2, 5, 13)$, $N_i n_i = r(2)$, tj. $(N_1, N_2, N_3) = (65, 26, 10)$. Podle Věty 93 platí

$$\mathrm{dlog}_2(53) = (\sum_{i=1}^{4} N_i \tilde{N}_i \mathrm{dlog}_{2^{N_i}}(53^{N_i}))_N \tag{11}$$

Metodou opakovaných čtverců vypočteme 53^{65} v grupě $\mathbb{Z}^*_{1441}$. Dostaneme

$$53^{65} = 1XSSSSSSX \to 53, 1368, 1006, 454, 53, 1368, 1006, \mathbf{1},$$

kde $65 = 1000001_2$, $uX = (u{\cdot}53)_{1441}$, $uS = (u{\cdot}u)_{1441}$. Odtud $\mathrm{dlog}_{2^{65}}(53^{65}) = \mathrm{dlog}_{2^{65}}(1) = 0$. ◀

Výpočet $\mathrm{dlog}_{2^{26}}(53^{26}) \in \mathbb{Z}^{\oplus}_5$. Metodou opakovaných čtverců vypočteme 53^{26} v grupě $\mathbb{Z}^*_{1441}$. Dostaneme

$$53^{26} = 1XSXSSXS \to 53, 1368, 454, 53, 1368, 454, \mathbf{53},$$

kde $26 = 11010_2$, $uX = (u \cdot 53)_{1441}$, $uS = (u \cdot u)_{1441}$.
Metodou opakovaných čtverců vypočteme 2^{26} v grupě $\mathbb{Z}^*_{1441}$. Dostaneme

$$2^{26} = 1XSXSSXS \to 2, 4, 8, 64, 1214, 987, \mathbf{53}(!)$$

kde $26 = 11010_2$, $uX = (u \cdot 2)_{1441}$, $uS = (u \cdot u)_{1441}$. Odtud nutně $\mathrm{dlog}_{2^{26}}(53^{26}) = \mathrm{dlog}_{53}(53) = 1$. ◀
Při výpočtu mocniny 2^{26} bylo náhodou objeveno, že

$$\mathbf{dlog_2 53 = 26}.$$

Z cvičných důvodů však systematický výpočet dokončíme.

Výpočet $\mathrm{dlog}_{2^{10}}(53^{10}) \in \mathbb{Z}^{\oplus}_{13}$. Metodou opakovaných čtverců vypočteme 53^{10} v grupě $\mathbb{Z}^*_{1441}$. Dostaneme

$$53^{10} = 1XSSXS \to 53, 1368, 1006, 1, \mathbf{1},$$

kde $10 = 1010_2$, $uX = (u \cdot 53)_{1441}$, $uS = (u \cdot u)_{1441}$. Odtud nutně $\mathrm{dlog}_{2^{10}}(53^{10}) = \mathrm{dlog}_{2^{10}}(1) = 0$. ◀
Zbývá vypočítat vztah (11). Dostaneme

$$\mathrm{dlog}_2(53) = (26 \cdot \tilde{26} \cdot \mathrm{dlog}_{2^{26}}(53^{26}))_{130} = (26 \cdot \tilde{26})_{130},$$

kde $26 \cdot \tilde{26} = 1 \bmod 5$, tj. $\tilde{26} = 1 \bmod 5$, odtud $\mathrm{dlog}_2(53) = 26$.

Alternativní výpočet s využitím „Babystep–Giantstep“

Řád prvku 2 je znám, $r(2) = 130$, definujme $n := \lceil\sqrt{130}\rceil = 12$.
Babystep: $2^{\{0,1,2,3,4,5,6,7,8,9,10,11,12\}} = \{1, 2, \mathbf{4}, 8, 16, 32, 64, 128, 256, 512, 1024, 607, (1214)$,
inverze $1214^{-1} = 146$

$$\begin{bmatrix}1214 & 1 & 0\\ 1441 & 0 & 1\end{bmatrix} \sim \begin{bmatrix}1214 & 1 & 0\\ 227 & -1 & 1\end{bmatrix} \sim \begin{bmatrix}79 & 6 & -5\\ 227 & -1 & 1\end{bmatrix} \sim \begin{bmatrix}79 & 6 & -5\\ 69 & -13 & 1\end{bmatrix} \sim$$
$$\sim \begin{bmatrix}10 & 19 & -16\\ 69 & -13 & 1\end{bmatrix} \sim \begin{bmatrix}10 & 19 & -16\\ 9 & -127 & 107\end{bmatrix} \sim \begin{bmatrix}1 & 146 & -123\\ 9 & -127 & 107\end{bmatrix} \sim \begin{bmatrix}1 & 146 & -123\\ 0 & -1441 & 1214\end{bmatrix}$$

Giantstep:

$$\begin{aligned} 53 \cdot (2^{-12})^{\{0,1,\ldots\}} &= 53 \cdot 146^{\{0,1,2,3,4,5,6,7,8,9,10,11\}} = \\ &= 53 \cdot \{1, 146, 1142, 1017, 59, 1409, 1092, 922, 599, 994, 1024, 1081\} = \\ &= \{53, 533, \mathbf{4}, 584, 245, 1186, 236, 1313, 45, 806, 955, 1094\}. \end{aligned}$$

Odtud plyne $2^2 = 53 \cdot (2^{-12})^2$, tedy $2^{26} = 53$, tedy platí

$$\mathbf{dlog_2(53) = 26}.$$

Dále můžeme vypočítat $K = 73^{26}$, metodou opakovaných čtverců dostaneme:

$$73^{26} = 1XSXSSXS \to 73, 1006, 1388, 1368, 1006, 1388, \mathbf{1368},$$

kde $(x)X = (x \cdot 73)_{1441}$, $(x)S = (x \cdot x)_{1441}$, tedy šifrovací klíč byl $\boldsymbol{K}$= **1368**.

Příklad 112. Je dána cyklická grupa $\mathbb{Z}^*_{131} = \langle g\rangle$ s generátorem $g = 124$. Navrhněte šifrovací/dešifrovací klíč protokolu El–Gamal pro danou grupu a její generátor.

1. Zvolme číslo $a \in \mathbb{N}$ takové, že $1 < a < 130$, například $a = 111$, toto je soukromý klíč.
2. Veřejným klíčem bude číslo $A := g^a = 124^{111}$, vypočteme jej metodou opakovaných čtverců. Protože $111 = 1101111_2$, položme $uX = (u \cdot 124)_{131}$, $uS = (u \cdot u)_{131}$,

   $$1XSXSSXSXSXSX \sim 124, 49, 50, 11, 121, 70, 53, 22, 91, 18, 62, \mathbf{90}.$$

   Veřejným klíčem bude $A =$ **90**.

Příklad 113. Je dána cyklická grupa $\mathbb{Z}^*_{109} = \langle g\rangle$ s generátorem $g = 6$. Navrhněte šifrovací/dešifrovací klíč protokolu El–Gamal pro danou grupu a její generátor.

1. Zvolme číslo $a \in \mathbb{N}$ takové, že $1 < a < 108$, například $a = 100$, toto je soukromý klíč.
2. Veřejným klíčem bude číslo $A := g^a = 6^{100}$, vypočteme jej metodou opakovaných čtverců. Protože $100 = 1100100_2$, položme $uX = (u \cdot 6)_{109}$, $uS = (u \cdot u)_{109}$,

   $$1XSXSSSXSS \sim 6, 36, 107, 4, 16, 38, 10, 100, \mathbf{81}.$$

   Veřejným klíčem bude $A =$ **81**.

Příklad 114. Pošlete šifrovaně zprávu $m = 100$ účastníkovi s veřejným klíčem $A = 148$ protokolu El-Gamal daného cyklickou grupou $\mathbb{Z}_{227}^* = \langle g \rangle$ s generátorem $g = 206$.

Zvolme „jepičí“ klíč $k = 57$ a v grupě $\mathbb{Z}_{227}^*$ vypočteme $(c_1, c_2) = (g^k, m \cdot A^k) = (206^{57}, 100 \cdot 148^{57})$, metodou opakovaných čtverců pro $57 = 111001_2$, vypočteme:

$$206^{57} \;=\; 1XSXSXSSSX, \to 206, 214, 46, 73, 56, 185, 175, 207, \mathbf{193},$$

kde $uX = (u \cdot 206)_{227}$, $uS = (u \cdot u)_{227}$,

$$148^{57} = 1XSXSXSSSX \to 148, 112, 5, 25, 68, 84, 19, 134, \mathbf{83}$$

kde $uX = (u \cdot 148)_{227}$, $uS = (u \cdot u)_{227}$. Odtud plyne: $c_1 \coloneqq 193$, $c_2 \coloneqq 100 \cdot 83 = 128$
Odesílaná zašifrovaná zpráva je

$$(c_1, c_2) \coloneqq (193, 128).$$

Příklad 115. Účastník protokolu El–Gamal daného cyklickou grupou $\mathbb{Z}_{227}^* = \langle g \rangle$ s generátorem $g = 206$ obdržel šifrovanou zprávu $(c_1, c_2) \coloneqq (193, 128)$. Účastník má soukromý klíč $a = 123$.
Dešifrujte zprávu $(c_1, c_2) = (193, 128)$. Platí $m = c_2(c_1^a)^{-1} = 128 \cdot (193^{123})^{-1}$.
• Nejprve vypočteme metodou opakovaných čtverců mocninu

$$193^{123} = 1XSXSXSXSSXSX \to 193, 21, 194, 181, 202, 171, 88, 26, 222, 170, 71, \mathbf{83}$$

kde $uX = (u \cdot 193)_{227}$, $uS = (u \cdot u)_{227}$, tj. $193^{123} = 83$.
• Dále vypočtěme inverzi $\widetilde{83}$ v grupě $\mathbb{Z}_{227}^*$ EE–algoritmem:

$$\begin{bmatrix} 83 & 1 & 0 \\ 227 & 0 & 1 \end{bmatrix} \sim \begin{bmatrix} 83 & 1 & 0 \\ 61 & -2 & 1 \end{bmatrix} \sim \begin{bmatrix} 61 & -2 & 1 \\ 22 & 3 & -1 \end{bmatrix} \sim \begin{bmatrix} 22 & 3 & -1 \\ 17 & -8 & 3 \end{bmatrix} \sim$$
$$\sim \begin{bmatrix} 17 & -8 & 3 \\ 5 & 11 & -4 \end{bmatrix} \sim \begin{bmatrix} 5 & 11 & -4 \\ 2 & -41 & 15 \end{bmatrix} \sim \begin{bmatrix} 2 & -41 & 15 \\ 1 & 93 & -34 \end{bmatrix} \sim \begin{bmatrix} 1 & 93 & -34 \\ 0 & -227 & 83 \end{bmatrix}.$$

Odtud $\widetilde{83} = 93$, dále dostaneme $m = 128 \cdot 93 = 100$.

Příklad 116. Dešifrujte zprávu $(c_1, c_2) = (78, 156)$ protokolu El–Gamal určeného grupou $\mathbb{Z}_{181}^* = \langle 18 \rangle$ znáte-li veřejný i soukromý klíč protokolu $(A, a) = (151, 111)$.
Řešení: Dešifrování zprávy v protokolu El-Gamal je dáno vztahem $m = c_2 \cdot c_1^{-a}$.
Nejprve stanovme inverzi c_1^{-1} v grupě $\mathbb{Z}_{181}^*$ EE–algoritmem:

$$\begin{bmatrix} 78 & 1 & 0 \\ 181 & 0 & 1 \end{bmatrix} \sim \begin{bmatrix} 78 & 1 & 0 \\ 25 & -2 & 1 \end{bmatrix} \sim \begin{bmatrix} 3 & 7 & -3 \\ 25 & -2 & 1 \end{bmatrix} \sim \begin{bmatrix} 3 & 7 & -3 \\ 1 & -58 & 25 \end{bmatrix} \sim \begin{bmatrix} 0 & 181 & -78 \\ 1 & -58 & 25 \end{bmatrix}$$

dostáváme $c_1^{-1} = -58$, dále vypočteme $c_1^{-a} = (-58)^{111}$ metodou opakovaných čtverců, $111 = 1101111_2$, tj.:

$$(-58)^{111} = 1XSXSSXSXSXSX \to 123, 106, 6, 36, 29, 128, 94, 159, 122, 164, 108, \mathbf{71},$$

kde $uX = (u \cdot (-58))_{181}$, $uS = (u \cdot u)_{181}$, tedy pro zprávu m platí: $m = 156 \cdot 71 = 35$.

Příklad 117. V grupě $\mathbb{Z}_{587}^*$ najděte generátor cyklické podgrupy co nejvyššího prvočíselného řádu.

Řešení: Nejprve určeme řád grupy $\mathbb{Z}_{587}^*$, tj. hodnotu $\varphi(587)$. Protože číslo 587 není velké, zkusíme jej hrubou silou rozložit, vyzkoušíme 587 dělit prvočísly p z intervalu $3 \leq p \leq \lfloor\sqrt{587}\rfloor = 24$, zjistíme, že žádné není dělitelem 587, je tedy 587 prvočíslo. Pak $\varphi(587) = 586 = 2 \cdot 293$, pro možné řády prvků $a \in \mathbb{Z}_{587}^*$, grupy platí $r(a) \in \{1, 2, 293, 586\}$. Největší prvočíselný řád vlastní podgrupy tedy bude 293.
Dále je třeba najít prvek $g \in \mathbb{Z}_{587}^*$ řádu $r(g) = 293$.
Nechť $q \in \mathbb{P}$, $q \,|\, |G|$. K vyhledání generátoru cyklické podgrupy $\langle g \rangle \subseteq| G$, $r(g) = q$, lze použít následující algoritmus:

$c := 1$;
`for` a `in` G `while` $c = 1$ `do`
    $c := a^{\frac{|G|}{q}}$;
`end do;`
$g := c$;

Důkaz. Nechť $|G| = q_1^{e_1} \cdot ... \cdot q_r^{e_r}$, $a \in G$, $a^{\frac{|G|}{q_1}} \neq 1$. Odtud $r(a) \,|\, |G|$ a zároveň $r(a) \nmid \frac{|G|}{q_1}$, odtud nutně $r(a) = q_1^{e_1} \cdot m$, kde $m \,|\, q_2^{e_2} \cdot ... \cdot q_r^{e_r}$. Položme $g := a^{\frac{|G|}{q_1}}$, pak platí

$$r(g) = r(a^{\frac{|G|}{q_1}}) = \frac{q_1^{e_1} \cdot m}{\gcd(q_1^{e_1} \cdot m, q_1^{e_1-1} \cdot q_2^{e_2} ... \cdot q_r^{e_r})} = \frac{q_1^{e_1} \cdot m}{q_1^{e_1-1} m \cdot \gcd(q_1, \frac{q_2^{e_2} \cdot ... \cdot q_r^{e_r}}{m})} = q_1.$$

□

Zřejmě stačí najít prvek a, pro který $a^{\frac{586}{293}} = a^2 \neq 1$, potom platí $r(a^2) = 293$, tj. $g := a^2$ bude hledaný generátor.

Vypočtěme dále v $\mathbb{Z}_{587}^*$ $\{2, 3, 4, 5, ...\}^2 = \{4, 9, 16, 25, ...\}$, dostáváme tak řadu generátorů cyklické podgrupy prvočíselného řádu. Celkem jich takto můžeme najít $\varphi(293) = 292$.

Příklad 118. Najděte generátor největší cyklické podgrupy grupy $\mathbb{Z}_{107}^*$ prvočíselného řádu.
Řešení:
1) Řád podgrupy $\mathbb{Z}_{107}^*$ je dělitel $|\mathbb{Z}_{107}^*| = \varphi(107) = 106 = 2 \cdot 53$, tedy největší možný prvočíselný řád je 53. Protože $\mathbb{Z}_{107}^*$ je cyklická grupa, prvek $g \in \mathbb{Z}_{107}^*$ řádu 53 určitě existuje.
2) K vyhledání generátoru cyklické podgrupy $\langle g \rangle \subseteq| G$, $r(g) = q \in \mathbb{P}$ použijeme následující algoritmus:

$c := 1$;
`for` a `in` G `while` $c = 1$ `do`
    $c := a^{\frac{|G|}{q}}$;
`end do;`
$g := c$;

3) V tomto příkladu $G = \mathbb{Z}_{107}^*$, $q = 53$, $\frac{|G|}{q} = 2$, hledáme tedy prvek $a \in \mathbb{Z}_{107}^*$, pro který $a^2 \neq 1$. Hrubou silou nalezneme:

$$\{2, 3, 4, ...\}^2 = \{4, 9, 16, ...\},$$

dostáváme tak řadu generátorů hledané cyklické podgrupy, celkem jich takto můžeme získat $\varphi(q) = q - 1$, tj. celkem 52.

Příklad 119. Najděte generátor největší cyklické podgrupy grupy $\mathbb{Z}_{223}^*$ prvočíselného řádu.

Řešení:

1) Řád podgrupy $\mathbb{Z}_{223}^*$ je dělitel $|\mathbb{Z}_{223}^*| = \varphi(223) = 222 = 2 \cdot 3 \cdot 37$, tedy největší možný prvočíselný řád je 37. Protože 223 je prvočíslo, $\mathbb{Z}_{223}^*$ je cyklická grupa, prvek $g \in \mathbb{Z}_{223}^*$ řádu 37 určitě existuje.

2) K vyhledání generátoru cyklické podgrupy $\langle g \rangle \subseteq | G$, $r(g) = q \in \mathbb{P}$ použijeme následující algoritmus:

$c := 1$;
`for` a `in` G `while` $c = 1$ `do`
    $c := a^{\frac{|G|}{q}}$;
`end do;`
$gen := c$;

3) V tomto příkladu $G = \mathbb{Z}_{223}^*$, $q = 37$, $\frac{|G|}{q} = 2 \cdot 3 = 6$, hledáme tedy prvek $b \in \mathbb{Z}_{107}^*$, pro který $b^6 \neq 1$. Hrubou silou nalezneme:

$$\{2, 3, 4, 5, 6, ...\}^6 = \{64, 60, 82, 15, 49, ...\},$$

dostáváme tak řadu generátorů hledané cyklické podgrupy, celkem jich takto můžeme získat $\varphi(q) = q - 1$, tj. celkem 36.

Definice 120. Nechť G je grupa, $x, b \in \langle a \rangle \subseteq | G$, $r(a) \in \mathbb{N}^+$, $(\mathbb{Z}_{r(a)}, \oplus, 0, \odot, 1)$ je okruh celých čísel „modulo“ $r(a)$. Pak dvojice $(s, t) \in \mathbb{Z}_{r(a)} \times \mathbb{Z}_{r(a)}$ se nazývá reprezentace prvku x vzhledem ke generátoru a a prvku b, právě když

$$x = a^s b^t.$$

Reprezentace se nazývá netriviální, jestliže navíc $\gcd(t, r(a)) = 1$.

Věta 121.

1. *Nechť $(G, \cdot, 1)$ je grupa, $b \in \langle a \rangle \subseteq | G$, $r(a) \in \mathbb{N}^+$. Pak platí:*
   $(\forall x \in \langle a \rangle)(\forall t \in \mathbb{Z}_{r(a)})(\exists! s \in \mathbb{Z}_{r(a)})(x = a^s b^t)$, *tj. platí:*
   • *Každý prvek $x \in \langle a \rangle$ má reprezentaci vzhledem k danému generátoru a a prvku $b \in \langle a \rangle$.*
   • *Jestliže (s_1, t), (s_2, t), jsou reprezentace téhož prvku $x \in \langle a \rangle$ vzhledem ke generátoru a a prvku $b \in \langle a \rangle$, potom $s_1 = s_2$.*

2. $x \in \langle a \rangle, t \in \mathbb{Z}_{r(a)} \Rightarrow (\mathrm{dlog}_a x \ominus (t \odot \mathrm{dlog}_a b), t)$ *je reprezentace prvku* x *vzhledem ke generátoru* a *a prvku* $b \in \langle a \rangle$, *operace* $\ominus, \odot$ *jsou operace okruhu* $(\mathbb{Z}_{r(a)}, \oplus, 0, \odot, 1)$.

3. *Jestliže* $1 = a^s b^t$, *kde* $t \in \mathbb{Z}_{r(a)}$ *a* $\gcd(r(a), t) = 1$ (*tzv. netriviální reprezentace prvku* $1 \in G$), *potom* $\mathrm{dlog}_a b$ *je jediným řešením* $x \in \mathbb{Z}_{r(a)}$ *rovnice* $t \cdot x + s = 0 \bmod r(a)$.

Příklad 122. V grupě $\mathbb{Z}_{21}^*$ stanovte všechny reprezentace prvku 4 vzhledem ke generátoru 2 a prvku 8. Které reprezentace jsou netriviální?
Řešení:
1) Korektnost zadání. Zadání má smysl, pokud platí $4, 8 \in \langle 2 \rangle \subseteq | \mathbb{Z}_{21}^*$. Zřejmě $2 \in \langle 2 \rangle \subseteq | \mathbb{Z}_{21}^*$, odtud $4 = 2^2$, $8 = 2^3 \in \langle 2 \rangle$. Zadání úlohy je korektní.
2) Pro libovolnou volbu čísla $t \in \{0, .., r(2)\}$ stanovíme $s \in \{0, .., r(2)\}$ tak, aby $4 = 2^s \cdot 8^t$, podle Věty 121 lze všechny reprezentace získat ze vztahu $(\mathrm{dlog}_a x \ominus (t \odot \mathrm{dlog}_a b), t)$.
• Nejprve stanovme řád prvku 2 v $\mathbb{Z}_{21}^*$. Hrubá síla: $2^{\{1,2,3,4,5,6\}} = \{2, 4, 8, 16, 11, 1\}$, tj. $r(2) = 6$.
• Z uvedených výpočtů můžeme odečíst hodnoty diskrétního logaritmu dlog_2, dostaneme $\mathrm{dlog}_2(4) = 2$, $\mathrm{dlog}_2(8) = 3$.
• Všechny reprezentace dostaneme vyčíslením funkce $t \mapsto (\mathrm{dlog}_a x \ominus (t \odot \mathrm{dlog}_a b), t)$, tj.

$$t \mapsto (2 - t \cdot 3, t) : \{0, 1, ..., 5\} \to \{0, 1, ..., 5\} \times \{0, 1, ..., 5\},$$

kde příslušné operace jsou počítány v okruhu $\mathbb{Z}_{r(2)} = \mathbb{Z}_6$. Dostaneme:

$$(2, 0), (5, 1), (2, 2), (5, 3), (2, 4), (5, 5).$$

Z uvedené posloupnosti reprezentací vybereme netriviální, tj. takové, pro které $\gcd(t, r(a)) = 1$, tj. $\gcd(t, 6) = 1$, dostaneme:

$$(5, 1), (5, 5).$$

Příklad 123. V grupě $\mathbb{Z}_{100}^*$ stanovte všechny netriviální reprezentace prvku 1 vzhledem ke generátoru 3 a prvku 29.

Řešení: Ze zadání úlohy plyne $a = 3$, $b = 29$, $G = \mathbb{Z}_{100}^*$, hledá se dvojice $(s, t) \in \mathbb{Z}_{r(3)} \times \mathbb{Z}_{r(3)}$ taková, že $1 = 3^s 29^t$ v grupě G.
1) Korektnost zadání. Zadání má smysl, pokud platí $1, 29 \in \langle 3 \rangle \subseteq | \mathbb{Z}_{100}^*$. Zřejmě $1 \in \langle 3 \rangle \subseteq | \mathbb{Z}_{100}^*$ platí. Otázku $29 \in \langle 3 \rangle$? nechme nezodpovězenou, pokud nebude $29 \in \langle 3 \rangle$, úloha nebude mít pro každou volbu $t \in \mathbb{Z}_{r(3)}$ řešení.
2) Hledáme-li netriviální reprezentace, pak pro libovolnou volbu čísla $t \in \{0, .., r(3) - 1\}$ které je nesoudělné s $r(3)$, stanovíme $s \in \{0, .., r(3) - 1\}$ tak, aby $1 = 3^s \cdot 29^t$, podle Věty 121 lze všechny reprezentace získat ze vztahu $(\mathrm{dlog}_a x \ominus (t \odot \mathrm{dlog}_a b), t)$, kde $x = 1$.
• Nejprve stanovme řád prvku 3 v $\mathbb{Z}_{100}^*$. Možné řády jsou dělitelé $\varphi(100) = 40 = 2^3 \cdot 5$, tj. 2,4,5,8,10,20,40. Zároveň víme, že prvek řádu 40 v $\mathbb{Z}_{100}^*$ neexistuje, protože $\mathbb{Z}_{100}^*$ není cyklická grupa, $100 = 2^2 5^2$. Hrubá síla: $3^{\{2,4,5,8,10,20\}} = \{9, 81, 43, 41, 49, 1\}$. tj. $r(3) | 20 = 2^2 \cdot 5$. Zároveň $3^4 = 81 \neq 1$, $3^{10} = 49 \neq 1$, tj. $r(3) = 20$.
• Dále potřebujeme vypočítat hodnotu diskrétního logaritmu $\mathrm{dlog}_3 29$, počítejme v $\mathbb{Z}_{100}^*$ hrubou silou, $3^{\{1,2,3,4,5,6\}} = \{3, 9, 27, 81, 43, 29\}$, dostaneme $\mathrm{dlog}_3(29) = 6$, zároveň platí

$\mathrm{dlog}_3(1) = 0$.
• Všechny netriviální reprezentace dostaneme vyčíslením funkce $t \mapsto (\ominus(t \odot \mathrm{dlog}_a b), t)$, pro t nesoudělné s 20 a z množiny $\{0, ..., 19\}$ tj.

$$t \mapsto (-t \cdot 6, t) : \{1, 3, 7, 9, 11, 13, 17, 19\} \to \mathbb{Z}_{20} \times \mathbb{Z}_{20}$$

kde příslušné operace jsou počítány v okruhu $\mathbb{Z}_{r(3)} = \mathbb{Z}_{20}$. Dostaneme:

$$(14, 1), (2, 3), (18, 7), (6, 9), (14, 11), (2, 13), (18, 17), (6, 19).$$

Příklad 124. V grupě $G = \mathbb{Z}_{83}^*$ je známa dvojice čísel $(25, 26)$ jako reprezentace prvku $1 \in G$ vzhledem ke generátoru 30 a prvku $40 \in \langle 30 \rangle$, tj. $1 = 30^{25} \cdot 40^{26}$. Na základě těchto údajů vypočtěte $\mathrm{dlog}_{30} 40$.

Řešení: „Logaritmováním" uvedené rovnice ihned dostaneme:

$$0 = 25 \cdot \mathrm{dlog}_{30}(30) + 26 \cdot \mathrm{dlog}_{30}(40) = 25 + 26 \cdot \mathrm{dlog}_{30}(40), \tag{12}$$

kde operace v rovnici (12) jsou operace v okruhu $\mathbb{Z}_{r(30)}$.
• Stanovení řádu prvku 30 v grupě $\mathbb{Z}_{83}^*$. Protože $|\mathbb{Z}_{83}^*| = 82 = 2 \cdot 41$, potom $r(30) \in \{2, 41, 82\}$. Protože

$$30^{\{2,41\}} = \{70, 1\},$$

pro řád prvku 30 máme $r(30) = 41$. Odtud rovněž vyplývá, že uvedená reprezentace prvku 1 je netriviální.
• Místo rovnice (12) řešíme diofantickou rovnici

$$26x + 41y = -25,$$

tj

$$\begin{bmatrix} 26 & 1 & 0 \\ 41 & 0 & 1 \end{bmatrix} \sim \begin{bmatrix} 26 & 1 & 0 \\ 15 & -1 & 1 \end{bmatrix} \sim \begin{bmatrix} 11 & 2 & -1 \\ 15 & -1 & 1 \end{bmatrix} \sim \begin{bmatrix} 11 & 2 & -1 \\ 4 & -3 & 2 \end{bmatrix} \sim$$
$$\sim \begin{bmatrix} 3 & 8 & -5 \\ 4 & -3 & 2 \end{bmatrix} \sim \begin{bmatrix} 3 & 8 & -5 \\ 1 & -11 & 7 \end{bmatrix} \sim \begin{bmatrix} 0 & 41 & -26 \\ 1 & -11 & 7 \end{bmatrix},$$

tj.

$$[x', y'] \cdot \begin{bmatrix} 0 & 41 & -26 \\ 1 & -11 & 7 \end{bmatrix} = [-25, x, y],$$

odtud $x = 41x' - 25 \cdot (-11) = 29 + \lambda 41$, $\lambda \in \mathbb{Z}$. Odtud plyne řešení úlohy $\mathrm{dlog}_{30}(40) = 29$.

Příklad 125. V grupě $G = \mathbb{Z}_{90}^*$ je známa dvojice čísel $(6, 3)$ jako reprezentace prvku $1 \in G$ vzhledem ke generátoru 7 a prvku $19 \in \langle 7 \rangle$, tj. $1 = 7^6 \cdot 19^3$. Na základě těchto údajů vypočtěte $\mathrm{dlog}_7 19$.

Řešení: „Logaritmováním" uvedené rovnice ihned dostaneme:

$$0 = 6 \cdot \mathrm{dlog}_7(7) + 3 \cdot \mathrm{dlog}_7(19) = 6 + 3 \cdot \mathrm{dlog}_7(19), \tag{13}$$

kde operace v rovnici (13) jsou operace v okruhu $\mathbb{Z}_{r(7)}$.
• Stanovení řádu prvku 7 v grupě $\mathbb{Z}_{90}^*$. Protože $|\mathbb{Z}_{90}^*| = \varphi(2 \cdot 3^2 \cdot 5) = 24$, potom $r(7) \in \{2, 3, 4, 6, 8, 12, 24\}$. Protože

$$7^{\{2,3,4,6,8,12\}} = \{49, 73, 61, 19, 31, 1\},$$

pro řád prvku 7 máme $r(7) = 12$. Odtud rovněž vyplývá, že uvedená reprezentace prvku 1 **není** netriviální.
• Místo rovnice (13) řešíme diofantickou rovnici $3x + 12y = -6$, tj

$$\begin{bmatrix} 3 & 1 & 0 \\ 12 & 0 & 1 \end{bmatrix} \sim \begin{bmatrix} 3 & 1 & 0 \\ 0 & -4 & 1 \end{bmatrix}$$

tj.

$$[x', y'] \cdot \begin{bmatrix} 3 & 1 & 0 \\ 0 & -4 & 1 \end{bmatrix} = [-6, x, y],$$

odtud $x' = -2, y' \in \mathbb{Z}$, tj. $x = -2 - 4 \cdot y' = 2 + \lambda 4$, $\lambda \in \mathbb{Z}$. Odtud pro $\mathrm{dlog}_7(19)$ plyne $\mathrm{dlog}_7(19) \in \{2, 6, 10\}$. Protože reprezentace není netriviální, je třeba ověřit, který z prvků $\{2, 6, 10\}$ je hledaný logaritmus. Dostaneme

$$7^{\{2,6,10\}} = \{49, 19, 79\},$$

odtud plyne hledaná hodnota $\mathrm{dlog}_7(19) = 6$.

Příklad 126. V grupě $\mathbb{Z}_{90}^*$ lze ověřit, že platí: $1 = 7^6 \cdot 17^2$. Lze využít této rovnosti k výpočtu $\mathrm{dlog}_7(17)$? Pokud rovnosti užít nelze, skutečnost pečlivě zdůvodněte!

Řešení: Budeme-li předpokládat, že rovnice představuje v grupě $\mathbb{Z}_{90}^*$ reprezentaci prvku 1 vzhledem ke generátoru 7 a prvku 17, pak „logaritmováním“ rovnice dostaneme

$$0 = 6 \cdot \mathrm{dlog}_7(7) + 2 \cdot \mathrm{dlog}_7(17) = 6 + 2 \cdot \mathrm{dlog}_7(17). \tag{14}$$

Z příkladu 125 víme, že $r(7) = 12$, řešme proto diofantickou rovnici $2x+12y = -6$, dostaneme

$$\begin{bmatrix} 2 & 1 & 0 \\ 12 & 0 & 1 \end{bmatrix} \sim \begin{bmatrix} 2 & 1 & 0 \\ 0 & -6 & 1 \end{bmatrix}$$

odtud

$$[x', y'] \cdot \begin{bmatrix} 2 & 1 & 0 \\ 0 & -6 & 1 \end{bmatrix} = [-6, x, y],$$

tj. $x' = -3, y' \in \mathbb{Z}$, tj, $x = -3 - 6 \cdot y' = 3 + \lambda 6$, $\lambda \in \mathbb{Z}$. Pro $\mathrm{dlog}_7(19)$ odtud plyne $\mathrm{dlog}_7(19) \in \{3, 9\}$.
Zbývá výsledek ověřit, počítejme mocniny

$$7^{\{3,9\}} = \{73, 37\}.$$

Žádné z nalezených řešení nevyhovuje! Rovnice $1 = 7^6 \cdot 17^2$ tedy není reprezentací prvku 1 vzhledem ke generátoru 7 a prvku 17. Protože $\mathrm{dlog}_7 : \langle 7 \rangle \to \mathbb{Z}_{r(7)}^{\oplus}$, je nutné, aby $17 \in \langle 7 \rangle$, to však není splněno. Platí totiž

$$\langle 7 \rangle = 7^{\{0,1,2,3,4,5,6,7,8,9,10,11\}} = \{1, 7, 49, 73, 61, 67, 19, 43, 31, 37, 79, 13\},$$

tj $17 \notin \langle 7 \rangle$. Proto v rovnici 14 hodnota $\mathrm{dlog}_7(17)$ není definována.

Testy prvočíselnosti

Definice 127. (Fermatův test prvočíselnosti) Nechť $n \in \mathbb{N}$, $n \geq 3$, položme $\mathbb{Z}_n^+ := \mathbb{Z}_n \setminus \{0\} = \{1, 2, ..., n-1\}$, $K_n := \{a \in \mathbb{Z}_n^+ \mid a^{n-1} = 1 \bmod n\}$. Fermatův test prvočíselnosti je následující pravděpodobnostní algoritmus, který testuje zda číslo n je prvočíslo:

$m := 5$; #počet pokusů
$s := 1$; #nastavení příznaku „n je prvočíslo“
`for` i `from` 1 `to` m `do`

$a := \text{rand}(1..n-1)$; #náhodný výběr $a \in \mathbb{Z}_n^+$
`if` $a \notin K_n$ `then` $s :=$
0; `break end if` #nastavení příznaku „n je číslo složené“

`end do;`
`if` $s =$
1 `then print(`„n je prvočíslo“`) else print(`„n je číslo složené“`)end if;`

Jestliže test odpoví „n je číslo složené“, pak výrok „n je číslo složené“ je pravdivý.
Jestliže test odpoví „n je prvočíslo“, pak výrok „n je prvočíslo“ je pravdivý s pravděpodobností $\geq 1 - \frac{1}{2^m}$.

Prvek $a \in K_n$ je tzv. svědek prvočíselnosti čísla n. Jestliže však n je číslo složené, a je tzv „falešný svědek“.
Prvek $a \in \mathbb{Z}_n^+ \setminus K_n$ je tzv. svědek složenosti čísla n. Falešní svědci složenosti neexistují.

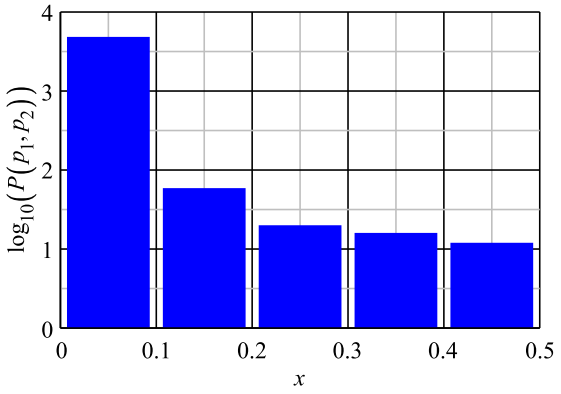
Existují složená čísla n (Carmichaelova), pro která platí $K_n = \mathbb{Z}_n^* \subsetneq \mathbb{Z}_n^+$. Jestliže n je Carmichaelovo číslo, potom test odpoví nepravdivě „n je prvočíslo“ s pravděpodobností pro některá Carmichaelova čísla velmi blízkou jedné.
Carmichaelových čísel je nekonečně mnoho, jsou však řídce rozmístěna. V množině $\{1, ..., 500\,000\}$ je jich pouze 32, jsou to čísla 561, 1105, 1729, 2465, 2821, 6601, 8911, 10585, 15841, 29341, 41041, 46657, 52633, 62745, 63973, 75361, 101101, 115921, 126217, 162401, 172081, 188461, 252601, 278545, 294409, 314821, 334153, 340561, 399001, 410041, 449065, 488881.

Poznámka 128. Nechť $\mathbb{Z}_n^+ := \mathbb{Z}_n \setminus \{0\}$, $n \geq 2$. Fermatův test prvočíselnosti využívá těchto poznatků:

$$K_n \subseteq \mathbb{Z}_n^*,$$
$$n \in \mathbb{P} \Rightarrow K_n = \mathbb{Z}_n^* = \mathbb{Z}_n^+,$$
$$n \in \text{Carmichael} \Rightarrow K_n = \mathbb{Z}_n^* \subsetneq \mathbb{Z}_n^+, \frac{1}{2} < \frac{|K_n|}{|\mathbb{Z}_n^+|} < 1 \text{ (experimentálně)}$$
$$n \notin \mathbb{P} \wedge n \notin \text{Carmichael} \Rightarrow |K_n| \leq \frac{1}{2} \left|\mathbb{Z}_n^+\right|.$$

Protože $\mathbb{Z}_n^+ \setminus K_n \supseteq \mathbb{Z}_n^+ \setminus \mathbb{Z}_n^* = div_0(\mathbb{Z}_n)$, může se stát, že svědek složenosti $a \in \mathbb{Z}_n^+ \setminus K_n$ bude i dělitel nuly okruhu $a \in \mathbb{Z}_n$, pak ovšem $d := \gcd(a, n) > 0$ je jedním z faktorů čísla n.

Jestliže pro rozklad čísla n na součin prvočísel platí $n = p_1^{e_1} \cdot ... \cdot p_k^{e_k}$, $i \neq j \Rightarrow p_i \neq p_j$, potom $|K_n| = \prod_{i=1}^{k} \gcd(n-1, p_i - 1)$.
Například, jestliže $n = p_1 p_2$, $p_1 \neq p_2$, potom $|K_{p_1 p_2}| = \gcd(p_1 - 1, p_2 - 1)^2$ a poměr $P(p_1, p_2) = \frac{|K_{p_1 p_2}|}{|\mathbb{Z}^+_{p_1 p_2}|} = \frac{\gcd(p_1-1, p_2-1)^2}{p_1 p_2 - 1}$ může nabývat volbou prvočísel p_1, p_2 rozličných hodnot v plném rozsahu intervalu $(0, \frac{1}{2})$, například platí: $P(503, 541) \doteq 1.470 \cdot 10^{-5}$, $P(59, 523) \doteq 0.110$, $P(271, 541) \doteq 0.497$.
Četnost výskytu „malých hodnot $P(p_1, p_2)$“ je však zřetelně větší, jak ukazují počítačové experimenty. Na dále uvedeném obrázku v **logaritmickém měřítku** jsou uvedeny četnosti výskytu hodnot $P(p_1, p_2)$ v rozsahu prvočísel $p_1, p_2 \leq 541$. Z obrázku je patrno, že hodnoty v intervalu $(0.0, 0.1)$ se vyskytují asi 385 krát častěji než hodnoty v intervalu $(0.4, 0.5)$.



Obrázek 16: četnosti výskytu hodnot $P(p_1, p_2)$

Příklad 129. Užijte Fermatův test na zjištění, zda $n := 533$ je či není prvočíslo.

1. Vyberme „svědka“, například $40 \in \mathbb{Z}_n$, počítejme hodnotu 40^{532} v $\mathbb{Z}_n$, metodou „opakovaných čtverců“

   $$532 = 1000010100_2 \to 40^{532} = 1XSSSSSXSSXSS,$$

   kde $uX = (u \cdot 40)_{533}$, $uS = (u \cdot u)_{533}$, dostaneme postupně

   $$40^{532} \to 40, 1, 1, 1, 1, 1, 40, 1, 1, 40, 1, \mathbf{1}$$

   Tento „svědek dosvědčuje“ prvočíselnost n s pravděpodobností větší než $\frac{1}{2}$.

2. Vyberme dalšího svědka, například $73 \in \mathbb{Z}_n$, počítejme hodnotu 73^{532} v $\mathbb{Z}_n$, metodou „opakovaných čtverců“

   $$532 = 1000010100_2 \to 73^{532} = 1XSSSSSXSSXSS,$$

   kde $uX = (u \cdot 73)_{533}$, $uS = (u \cdot u)_{533}$, dostaneme postupně

   $$73^{532} \to 73, 532, 1, 1, 1, 1, 73, 532, 1, 73, 532, \mathbf{1},$$

Tento svědek dosvědčuje prvočíselnost n nyní již s celkovou pravděpodobností větší než $1 - \frac{1}{4}$.

3. Vyberme dalšího svědka, například $5 \in \mathbb{Z}_n$, počítejme hodnotu 5^{532} v $\mathbb{Z}_n$, metodou „opakovaných čtverců“

$$532 = 1000010100_2 \to 5^{532} = 1XSSSSSXSSXSS,$$

kde $uX = (u \cdot 5)_{533}$, $uS = (u \cdot u)_{533}$, dostaneme postupně

$$5^{532} \to 5, 25, 92, 469, 365, 508, 408, 168, 508, 408, 168, \mathbf{508} \neq \mathbf{1}.$$

Tento svědek dosvědčuje složenost čísla n s jistotou. Svědkové z předchozích dvou kroků jsou tedy falešní.

Příklad 130. Užijte Fermatův test na zjištění, zda $n := 323$ je či není prvočíslo.

1. Vyberme „svědka“, například $18 \in \mathbb{Z}_n^+$, počítejme hodnotu 18^{322} v $\mathbb{Z}_n$, metodou „opakovaných čtverců“

$$322 = 101000010_2 \to 18^{322} = 1XSSXSSSSSXS,$$

kde $uX = (u \cdot 18)_{322}$, $uS = (u \cdot u)_{322}$, dostaneme postupně

$$18^{322} \to 18, 1, 1, 18, 1, 1, 1, 1, 1, 18, \mathbf{1}$$

Tento „svědek dosvědčuje“ prvočíselnost n s pravděpodobností větší než $\frac{1}{2}$.

2. Vyberme dalšího svědka, například $34 \in \mathbb{Z}_n^+$, počítejme hodnotu 34^{322} v $\mathbb{Z}_n$, metodou „opakovaných čtverců“

$$322 = 1000010100_2 \to 34^{322} = 1XSSXSSSSSXS,$$

kde $uX = (u \cdot 34)_{322}$, $uS = (u \cdot u)_{322}$, dostaneme postupně

$$34^{322} \to 34, 187, 85, 306, 289, 187, 85, 119, 272, 204, \mathbf{272} \neq \mathbf{1}.$$

Tento svědek dosvědčuje složenost čísla n s jistotou. Svědek prvočíselnosti z předchozího kroku je falešný.

Vyzkoušejme, zda 34 je dělitel nuly okruhu $\mathbb{Z}_n$. Zkusme vypočítat $\gcd(34, 323)$, EE–algoritmus dá $\gcd(34, 323) = 17$, odtud $323 = 17 \cdot 19$, máme navíc faktorizaci čísla n.

Příklad 131. Stanovte všechny falešné svědky Fermatova testu prvočíselnosti čísla $n = 323$ z Příkladu 130.

Řešení: Falešný svědek prvočíselnosti je prvek $a \in K_n$, kde n je číslo složené. Je třeba najít všechna řešení rovnice $x^{n-1} = 1$ v $\mathbb{Z}_n^+$. Protože $K_n \subseteq \mathbb{Z}_n^*$, rovnici $x^{n-1} = 1$ řešíme v grupě

$\mathbb{Z}_n^*$. V Příkladu 130 byla nalezena faktorizace $n = 17 \cdot 19$, můžeme využít CRT izomorfismu grup $\mathbb{Z}_{323}^* \leftrightarrows \mathbb{Z}_{17}^* \times \mathbb{Z}_{19}^*$.

Řešení rovnice $x^{322} = 1$ v $\mathbb{Z}_{17}^*$. Protože $|\mathbb{Z}_{17}^*| = 16$, můžeme redukovat exponent, $x^{322} = 1 \Leftrightarrow x^{\gcd(322,16)} = 1 \Leftrightarrow x^2 = 1$. V cyklické grupě má posledně zapsaná rovnice právě dvě řešení $x \in \{1, -1\}$.

Řešení rovnice $x^{322} = 1$ v $\mathbb{Z}_{19}^*$. Protože $|\mathbb{Z}_{19}^*| = 18$, můžeme redukovat exponent, $x^{322} = 1 \Leftrightarrow x^{\gcd(322,18)} = 1 \Leftrightarrow x^2 = 1$. V cyklické grupě má posledně zapsaná rovnice právě dvě řešení $x \in \{1, -1\}$.

S využitím CRT izomorfismu $g(u, v) = (19 \cdot \tilde{19}u + 17 \cdot \tilde{17}v)_{323}, = (-19 \cdot 8u + 17 \cdot 9v)_{323}$, Odtud plyne

$$K_{323} = (-19 \cdot 8 \cdot \{\pm 1\} + 17 \cdot 9 \cdot \{\pm 1\})_{323} = \{\pm 1, \pm 18\}.$$

Věta 132. *Nechť platí*

$$t = 1 + 2\mathbb{N},\ h \in \mathbb{N}^+,\ n = t \cdot 2^h + 1,$$
$$\beta_i : \mathbb{Z}_n \to \mathbb{Z}_n,\ \beta_i(\alpha) = \alpha^{t \cdot 2^i},\ i \in \{0, ..., h-1\},$$
$$K_n = \{\alpha \in \mathbb{Z}_n \,|\, \alpha^{n-1} = 1\ v \mathbb{Z}_n\},$$
$$M_n = \{\alpha \in \mathbb{Z}_n \,|\, \alpha^2 = 1 \Rightarrow \alpha \in \{1, -1\},\ v\mathbb{Z}_n\} =$$
$$= (\mathbb{Z}_n \setminus \{\alpha \in \mathbb{Z}_n \,|\, \alpha^2 = 1\}) \cup \{-1, 1\},$$
$$L_n = K_n \cap \bigcap_{i=0}^{h-1} \beta_i^*(M_n).$$

Následující procedura LnT testuje, zda $\alpha \in L_n$, platí $\alpha \in L_n \Leftrightarrow LnT(\alpha, n) = 1$.

```
LnT := proc(α, n)
h := 0; t := n − 1;
while t mod 2 = 0 do
    h := h + 1; t := t/2;
end do;
β := α^t mod n;
if β = 1 then return 1 end if;
for i from 0 to h − 1 do
    if β = n − 1 then return 1 end if;
    if β = 1 then return 0 end if;
    β := β^2;
end do;
return 0;
end proc;
```

Procedura LnT tvoří jádro Rabinova–Millerova testu prvočíselnosti.
Jestliže pro nějaké $\alpha \in \mathbb{Z}_n$ platí $LnT(\alpha, n) = 0$, pak $\alpha \notin L_n$ a výrok „n je číslo složené“ je pravdivý.
Jestliže pro posloupnost $\alpha_1, ..., \alpha_k \in \mathbb{Z}_n$ platí $LnT(\alpha_1, n) = ... = LnT(\alpha_k, n) = 1$, pak $\alpha_1, ..., \alpha_k \in L_n$ a výrok „n je prvočíslo“ je pravdivý s pravděpodobností větší než $1 - \frac{1}{4^k}$.

Příklad 133. Je dáno číslo $n = 25$. Pro toto číslo stanovte množiny M_n, K_n, $\beta_i^*(M_n)$ a L_n v Rabinově–Millerově testu prvočíselnosti. Stanovte všechny falešné svědky prvočíselnosti čísla n jak pro Fermatův test, tak pro Rabinův–Millerův test a porovnejte jejich počty. pro zvolené prvky $\alpha \in \mathbb{Z}_n^* \setminus L_n$ a $\alpha \in L_n$ sledujte chod procedury LnT. Protože $25 - 1 = 3 \cdot 2^3$, pro další výpočty položme $t \coloneqq 3$, $h \coloneqq 3$.

Množina M_n Nechť $n = 25$. Pro množinu M_n platí

$$M_n = \{\alpha \in \mathbb{Z}_n \,|\, \alpha^2 = 1 \Rightarrow \alpha \in \{1, -1\}\} = \{\alpha \in \mathbb{Z}_n \,|\, \alpha^2 \neq 1\} \cup \{1, -1\}.$$

Prvků v množině M_n pro které $\alpha^2 \neq 1$ bude jistě hodně, stanovme proto komplement

$$\mathbb{Z}_n \setminus \{\alpha \in \mathbb{Z}_n \,|\, \alpha^2 \neq 1\} = \{\alpha \in \mathbb{Z}_n \,|\, \alpha^2 = 1\},$$

tj. řešme rovnici $x^2 = 1$ v $\mathbb{Z}_{25}$. Protože řešením jsou pouze prvky v $\mathbb{Z}_{25}^*$ a $\mathbb{Z}_{25}^*$ je cyklická grupa, řešením bude cyklická podgrupa řádu 2, tedy zřejmě $x^2 = 1$ v $\mathbb{Z}_{25} \Leftrightarrow x \in \{-1, 1\}$. Odtud plyne

$$M_n = (\mathbb{Z}_n \setminus \{-1, 1\}) \cup \{-1, 1\} = \mathbb{Z}_n.$$

Množina K_n Množina $K_n = \{\alpha \in \mathbb{Z}_n \,|\, \alpha^{n-1} = 1\}$ je klíčová množina Fermatova testu prvočíselnosti. Její prvky získáme řešením rovnice $x^{24} = 1$ v $\mathbb{Z}_{25}$. Řešením jsou opět pouze prvky v $\mathbb{Z}_{25}^*$ a $\mathbb{Z}_{25}^*$ je cyklická grupa, řešením bude cyklická podgrupa řádu $\gcd(24, |\mathbb{Z}_{25}^*|) = \gcd(24, \varphi(25)) = \gcd(24, 20) = 4$. Pro nalezení podgrupy řádu 4 cyklické grupy $\mathbb{Z}_{25}^*$ najdeme její generátor. Stačí najít prvek $a \in \mathbb{Z}_{25}^*$ pro který $a^4 \neq 1$ a $a^{10} \neq 1$. Prvek $2 \in \mathbb{Z}_{25}^*$ této podmínce vyhovuje, máme tedy $a \in \mathbb{Z}_{25}^* = \langle 2 \rangle$. Podgrupa řádu 4 je dána vztahem $\left\langle 2^{\frac{20}{4}} \right\rangle = \langle 2^5 \rangle = \langle 7 \rangle = \{1, 7, 24, 18\} = \{\pm 1, \pm 7\}$. Platí tedy

$$K_n = \{1, 7, 24, 18\} = \{\pm 1, \pm 7\}.$$

Máme tedy pravděpodobnost Fermatova testu výroku „25 je prvočíslo“ po jednom pokusu $\frac{|K_n|}{|Z_n^+|} = \frac{4}{24} = \frac{1}{6}$. Protože 25 jistě prvočíslem není, máme celkem 4 falešné svědky prvočíselnosti.

Množina L_n Množina $L_n = K_n \cap \bigcap_{i=0}^{h-1} \beta_i^*(M_n)$ je klíčová množina Rabinova–Millerova testu prvočíselnosti. Protože $M_n = \mathbb{Z}_n$, platí $\beta_i^*(M_n) = \mathbb{Z}_n$, proto $L_n = K_n$, tedy i v případě Rabinova–Millerova testu prvočíselnosti máme stejný počet falešných svědků prvočíselnosti.

Chod *LnT*(4,25)

(0) Zvolme nejprve $\alpha = 4 \in \mathbb{Z}_{25}^* \setminus L_{25}$. Pro $\beta_0 = \alpha^t = 4^3 = 14$. Protože $\beta_0 \notin \{-1, 1\}$, vypočte se v cyklu pro $i = 0$ hodnota $\beta_1 = 14^2 = 21$.

(1) Protože opět $\beta_1 \notin \{-1, 1\}$, v cyklu pro $i = 1$ se vypočte hodnota $\beta_2 = 21^2 = 16$.

(2) Protože opět $\beta_2 \notin \{-1, 1\}$, v cyklu pro $i = 2$ se vypočte hodnota $\beta_3 = 16^2 = 6$, tato hodnota se zahodí.

(3) Jelikož $\beta_0, \beta_1 \notin \{-1, 1\}$, procedura opouští tělo cyklu a vrací hodnotu 0, což znamená $\alpha \notin L_n$.

Chod *LnT*(7,25)

(0) Zvolme $\alpha = 7 \in L_{25}$. Pro $\beta_0 = \alpha^t = 7^3 = 18$. Protože $\beta_0 \notin \{-1, 1\}$, vypočte se v cyklu pro $i = 0$ hodnota $\beta_1 = 18^2 = 24 = -1$.

(1) Protože $\beta_1 = -1$, v cyklu pro $i = 1$ se tato skutečnost vyhodnotí, procedura vrátí hodnotu 1, tj. $\alpha \in L_n$, procedura se zastaví.

Příklad 134. Je dáno číslo $n = 65$. Pro toto číslo stanovte množiny M_n, K_n, $\beta_i^*(M_n)$ a L_n v Rabinově–Millerově testu prvočíselnosti. Stanovte všechny falešné svědky prvočíselnosti čísla n jak pro Fermatův test, tak pro Rabinův–Millerův test a porovnejte jejich počty. Pro zvolené prvky $\alpha \in \mathbb{Z}_n^* \setminus L_n$ a $\alpha \in L_n$ sledujte chod procedury LnT. Protože $65 - 1 = 1 \cdot 2^6$, pro další výpočty položme $t \coloneqq 1$, $h \coloneqq 6$.

Množina M_n Nechť $n = 65$. Pro množinu M_n platí

$$M_n = \{\alpha \in \mathbb{Z}_n \,|\, \alpha^2 = 1 \Rightarrow \alpha \in \{1, -1\}\} = \{\alpha \in \mathbb{Z}_n \,|\, \alpha^2 \neq 1\} \cup \{1, -1\}.$$

Prvků v množině M_n pro které $\alpha^2 \neq 1$ bude jistě hodně, stanovme proto komplement

$$\mathbb{Z}_n \setminus \{\alpha \in \mathbb{Z}_n \,|\, \alpha^2 \neq 1\} = \{\alpha \in \mathbb{Z}_n \,|\, \alpha^2 = 1\},$$

tj. řešme rovnici $x^2 = 1$ v $\mathbb{Z}_{65}$. Protože řešením jsou pouze prvky v $\mathbb{Z}_{65}^*$ a $\mathbb{Z}_{65}^* = \mathbb{Z}_{5 \cdot 13}^*$, grupa není cyklická. Rovnici $x^2 = 1$ budeme řešit s využitím izomorfismu $\mathbb{Z}_{65}^* \leftrightarrows \mathbb{Z}_5^* \times \mathbb{Z}_{13}^*$.

Řešení rovnice $x^2 = 1$ v obou grupách $\mathbb{Z}_3^*$ a $\mathbb{Z}_{13}^*$ budou cyklické podgrupy řádu 2, tedy zřejmě v $x^2 = 1 \Leftrightarrow x \in \{-1, 1\}$. Odtud plyne pomocí zmíněného izomorfismu

$$\{\alpha \in \mathbb{Z}_n \,|\, \alpha^2 = 1\} = (13 \cdot \tilde{13} \cdot \{\pm 1\} + 5 \cdot \tilde{5} \cdot \{\pm 1\})_{65} = (26 \cdot \{\pm 1\} - 25 \cdot \{\pm 1\})_{65} = \{\pm 1, \pm 14\}.$$

Máme tedy

$$M_n = (\mathbb{Z}_n \cap \{\pm 1, \pm 14\}^c) \cup \{\pm 1\} = (\mathbb{Z}_n \cap \{\pm 14\}^c) \cup \{\pm 1\} = \mathbb{Z}_n \setminus \{\pm 14\}.$$

Množiny $\beta_i^*(M_n)$. Platí $\beta_i^*(M_n) = \beta_i^*(\mathbb{Z}_n \setminus \{\pm 14\}) = \mathbb{Z}_n \setminus \beta_i^*(\{\pm 14\})$. Stanovíme proto množiny $\beta_i^*(\{\pm 14\})$.

• Protože $\beta_0(\alpha) = \alpha$, je

$$\beta_0^*(\{\pm 14\}) = \{\pm 14\}.$$

• Protože $\beta_1(\alpha) = \alpha^2$, je $\alpha \in \beta_1^*(\{\pm 14\}) \Leftrightarrow \alpha^2 \in \{\pm 14\}$. Protože prvky ± 14 jsou invertibilními prvky okruhu $\mathbb{Z}_{65}$, budou řešením rovnic $\alpha^2 = 14$, $\alpha^2 = -14$ invertibilní prvky okruhu $\mathbb{Z}_{65}$. S využitím izomorfismu $\mathbb{Z}_{65}^* \cong \mathbb{Z}_5^* \times \mathbb{Z}_{13}^*$, hledejme řešení uvedených rovnic.

Rovnice $\alpha^2 = 14 = -1$, $\alpha^2 = -14 = 1$ v $\mathbb{Z}_5^*$. Protože $\mathbb{Z}_5^* = \{1, 2, 3, 4\}$, $(\mathbb{Z}_5^*)^2 = \{1, 4, 9, 16\} = \{1, -1, -1, 1\}$, máme odtud $\alpha^2 = -1 \Leftrightarrow \alpha \in \{2, 3\} = \{2, -2\}$, $\alpha^2 = 1 \Leftrightarrow \alpha \in \{1, 4\} = \{1, -1\}$

Rovnice $\alpha^2 = 14 = 1$, $\alpha^2 = -14 = -1$ v $\mathbb{Z}_{13}^*$. Protože $\mathbb{Z}_{13}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$, $(\mathbb{Z}_{13}^*)^2 = \{1, 4, 9, 3, 12, 10, 10, 12, 3, 9, 4, 1\} = \{1, 4, -4, 3, -1, -3, -3, -1, 3, -4, 4, 1\}$, máme odtud $\alpha^2 = -1 \Leftrightarrow \alpha \in \{5, -5\}$, $\alpha^2 = 1 \Leftrightarrow \alpha \in \{1, -1\}$. Pro řešení rovnice v $\mathbb{Z}_{65}$ dostaneme

$$\begin{aligned} \alpha^2 = 14 &\Leftrightarrow \alpha \in (13 \cdot \tilde{13} \cdot \{2, -2\} + 5 \cdot \tilde{5} \cdot \{1, -1\})_{65} = (26 \cdot \{2, -2\} - 25 \cdot \{1, -1\})_{65}, \\ &\Leftrightarrow \alpha \in \{\pm 12, \pm 27\}. \end{aligned}$$

dále

$$\begin{aligned} \alpha^2 = -14 &\Leftrightarrow \alpha \in (13 \cdot \tilde{13} \cdot \{1, -1\} + 5 \cdot \tilde{5} \cdot \{5, -5\})_{65} = (26 \cdot \{1, -1\} - 25 \cdot \{5, -5\})_{65} \\ &\Leftrightarrow \alpha \in \{\pm 21, \pm 31\}. \end{aligned}$$

Odtud plyne

$$\alpha^2 \in \{\pm 14\} \Leftrightarrow \alpha \in \{\pm 12, \pm 21, \pm 27, \pm 31\} = \sqrt{\{\pm 14\}},$$

• Protože $\beta_2(\alpha) = \alpha^4$, je $\alpha \in \beta_2^*(\{\pm 14\}) \Leftrightarrow \alpha^4 \in \{\pm 14\} \Leftrightarrow \alpha^2 \in \sqrt{\{\pm 14\}} \Leftrightarrow \alpha \in \sqrt{\{\pm 12, \pm 21, \pm 27, \pm 31\}}$.
Eulerovo kritérium: V grupě $\mathbb{Z}_{p^e}^*$ platí $x \in (\mathbb{Z}_{p^e}^*)^2 \Leftrightarrow x^{\frac{1}{2}\varphi(p^e)} = 1$, $x \notin (\mathbb{Z}_{p^e}^*)^2 \Leftrightarrow x^{\frac{1}{2}\varphi(p^e)} = -1$, pro $p \in \mathbb{P}, p \geq 3$, $e \in \mathbb{N}^+$. Podle tohoto kritéria otestujeme řešitelnost rovnic $\alpha^2 = x$, pro $x \in \{\pm 12, \pm 21, \pm 27, \pm 31\}$. Vzhledem k CRT izomorfismu $\mathbb{Z}_{65}^* \leftrightarrows \mathbb{Z}_5^* \times \mathbb{Z}_{13}^*$ platí $\alpha \in (\mathbb{Z}_{65}^*)^2 \Leftrightarrow (\alpha_1, \alpha_2) \in (\mathbb{Z}_5^*)^2 \times (\mathbb{Z}_{13}^*)^2$, kde $\alpha \leftrightarrows (\alpha_1, \alpha_2)$.

∘ Řešení v $\mathbb{Z}_5$. Protože $\{\pm 12, \pm 21, \pm 27, \pm 31\} \subseteq \mathbb{Z}_5^*$, pak všechna řešení rovnice $\alpha^2 = x$ pro $x \in \{\pm 12, \pm 21, \pm 27, \pm 31\}$ budou opět ležet v $\mathbb{Z}_5^*$. Protože $\frac{1}{2}\varphi(5) = 2$, dostaneme $\{\pm 12, \pm 21, \pm 27, \pm 31\}^2 = \{-1, 1, -1, 1\}$. Odtud plyne, že rovnice $\alpha^2 = x$ pro $x \in \{\pm 12, \pm 27\}$ nemá v $\mathbb{Z}_5^*$ řešení.

∘ Řešení v $\mathbb{Z}_{13}$. Protože $\{\pm 12, \pm 21, \pm 27, \pm 31\} \subseteq \mathbb{Z}_{13}^*$, pak všechna řešení rovnice $\alpha^2 = x$ pro $x \in \{\pm 12, \pm 21, \pm 27, \pm 31\}$ budou opět ležet v $\mathbb{Z}_{13}^*$. Protože $\frac{1}{2}\varphi(13) = 6$, dostaneme $\{\pm 12, \pm 21, \pm 27, \pm 31\}^6 = \{1, -1, 1, -1\}$. Odtud plyne, že rovnice $\alpha^2 = x$ pro $x \in \{\pm 21, \pm 31\}$ nemá v $\mathbb{Z}_{13}^*$ řešení.

Odtud plyne, že neexistuje prvek $\alpha \in \mathbb{Z}_{65}$ takový, že $\alpha^2 \in \{\pm 12, \pm 21, \pm 27, \pm 31\}$, tj. $\sqrt{\{\pm 12, \pm 21, \pm 27, \pm 31\}} = \sqrt[4]{\{\pm 14\}} = \emptyset$.

• Protože platí $\beta_i^*(T) = \beta_0^*(\sqrt[2^i]{T})$, plyne z předchozího výsledku pro $i \geq 0$

$$\beta_{2+i}^*(\{\pm 14\}) = \beta_0^*(\sqrt[2^{2+i}]{\{\pm 14\}}) = \beta_0^*(\sqrt[2^i]{\sqrt[2^2]{\{\pm 14\}}}) = \beta_0^*(\sqrt[2^i]{\emptyset}) = \emptyset.$$

Množiny $\beta_i^*(M_n)$. Protože $M_n = \mathbb{Z}_n \setminus \{\pm 14\}$, dostaneme

$$\begin{aligned}
\beta_i^*(M_n) &= \beta_i^*(\mathbb{Z}_n \setminus \{\pm 14\}) = \beta_i^*(\mathbb{Z}_n) \setminus \beta_i^*(\{\pm 14\}) = \mathbb{Z}_n \setminus \beta_0^*(\sqrt[2^i]{\{\pm 14\}}) = \mathbb{Z}_n \setminus \sqrt[2^i]{\{\pm 14\}} \\
\beta_0^*(M_n) &= \mathbb{Z}_n \setminus \sqrt[2^0]{\{\pm 14\}} = \mathbb{Z}_n \setminus \{\pm 14\}, \\
\beta_1^*(M_n) &= \mathbb{Z}_n \setminus \sqrt[2^1]{\{\pm 14\}} = \mathbb{Z}_n \setminus \{\pm 12, \pm 21, \pm 27, \pm 31\}, \\
\beta_i^*(M_n) &= \mathbb{Z}_n \setminus \sqrt[2^i]{\{\pm 14\}} = \mathbb{Z}_n \text{ pro } i \geq 2.
\end{aligned}$$

Množina K_n Klíčová množina Fermatova testu prvočíselnosti, $K_n = \{\alpha \in \mathbb{Z}_n \,|\, \alpha^{n-1} = 1 \text{ v } \mathbb{Z}_n\}$. Zřejmě $K_{65} \subseteq \mathbb{Z}_{65}^*$, s využitím izomorfismu $\mathbb{Z}_{65}^* \cong \mathbb{Z}_5^* \times \mathbb{Z}_{13}^*$, řešme rovnici $x^{64} = 1$ v $\mathbb{Z}_{65}^*$.

• $x^{64} = 1$ v $\mathbb{Z}_5^*$. Platí $x^{64} = 1 \Leftrightarrow x^4 = 1$, neboť $\gcd(64, |\mathbb{Z}_5^*|) = 4$, protože $|\mathbb{Z}_5^*| = 4$, řešením rovnice je tedy celá množina $\mathbb{Z}_5^*$.

• $x^{64} = 1$ v $\mathbb{Z}_{13}^*$. Platí $x^{64} = 1 \Leftrightarrow x^4 = 1$, neboť $\gcd(64, |\mathbb{Z}_{13}^*|) = 4$, kde $|\mathbb{Z}_{13}^*| = 12$. Stanovme nejprve generátor cyklické grupy $\mathbb{Z}_{13}^*$, hledejme prvek $\alpha \in \mathbb{Z}_{13}^*$ pro který platí $\alpha^4 \neq 1 \wedge \alpha^6 \neq 1$. Uvedeným podmínkám vyhovuje prvek 2, tj. $\langle 2 \rangle = \mathbb{Z}_{13}^*$. Řešením rovnice je tedy cyklická podgrupa $\left\langle 2^{\frac{12}{4}} \right\rangle = \langle 2^3 \rangle = \{1, 8, 12, 5\} = \{\pm 1, \pm 5\}$.

• $x^{64} = 1$ v $\mathbb{Z}_{65}^*$. CRT izomorfismus dává všechna řešení rovnice v $\mathbb{Z}_{65}^*$.

$$x^{64} = 1 \Leftrightarrow x \in (26 \cdot \{\pm 1, \pm 2\} - 25 \cdot \{\pm 1, \pm 5\})_{65} \Leftrightarrow x \in \{\pm 1, \pm 8, \pm 14, \pm 18, \pm 21, \pm 27, \pm 31\},$$
$$K_n = \{\pm 1, \pm 8, \pm 14, \pm 18, \pm 21, \pm 27, \pm 31\}.$$

Množina L_n Platí

$$\begin{aligned}
L_n &= K_n \cap \bigcap_{i=0}^{h-1} \beta_i^*(Z_n \setminus \{\pm 14\}) = K_n \cap \bigcap_{i=0}^{h-1} \beta_i^*(Z_n) \setminus \beta_i^*(\{\pm 14\}) = \\
&= K_n \cap \bigcap_{i=0}^{h-1} (Z_n \setminus \sqrt[2^i]{\{\pm 14\}}) = K_n \setminus \bigcup_{i=0}^{h-1} \sqrt[2^i]{\{\pm 14\}} = \\
&= K_n \setminus \{\pm 14, \pm 12, \pm 21, \pm 27, \pm 31\} = \\
&= \{\pm 1, \pm 8, \pm 18\} \cdots \text{falešní svědkové prvočíselnosti.}
\end{aligned}$$

Pro pravděpodobnost výroku „65 je prvočíslo“ v případě jednoho pokusu máme u Fermatova testu hodnotu $\frac{|K_{65}|}{|Z_{65}^+|} = \frac{14}{64} \doteq 0.219$, u Rabinova–Millerova testu vychází $\frac{|L_{65}|}{|Z_{65}^+|} = \frac{6}{64} \doteq 0.094$. U Fermatova testu máme více jak 2.3 krát vyšší pravděpodobnost chybné odpovědi.

Chod Ln(7,65)

(0) Zvolme $\alpha = 7 \in \mathbb{Z}_{65}^* \setminus L'_{65}$. Pro $\beta_0 = \alpha^1 = 7$. Protože $\beta_0 \notin \{-1, 1\}$, vypočte se v cyklu pro $i = 0$ hodnota $\beta_1 = 7^2 = 49$.

(1) Protože opět $\beta_1 \notin \{-1, 1\}$, v cyklu pro $i = 1$ se vypočte hodnota $\beta_2 = 49^2 = 61$.

(2) Protože opět $\beta_2 \notin \{-1, 1\}$, v cyklu pro $i = 2$ se vypočte hodnota $\beta_3 = 61^2 = 16$.

(3) Protože opět $\beta_3 \notin \{-1, 1\}$, v cyklu pro $i = 3$ se vypočte hodnota $\beta_4 = 16^2 = 61$.

(3) Protože opět $\beta_4 \notin \{-1, 1\}$, v cyklu pro $i =$ se vypočte hodnota $\beta_5 = 61^2 = 16$, tato hodnota se zahodí.

(3) Jelikož $\beta_0, \beta_1, \beta_3, \beta_4, \notin \{-1, 1\}$, procedura opouští tělo cyklu a vrací hodnotu 0, což znamená $\alpha \notin L_n$.

Chod *LnT*(8,25)

(0) Zvolme $\alpha = 8 \in L_{65}$. Pro $\beta_0 = \alpha^1 = 8$. Protože $\beta_0 \notin \{-1, 1\}$, vypočte se v cyklu pro $i = 0$ hodnota $\beta_1 = 8^2 = 64 = -1$.

(1) Protože $\beta_1 = -1$ v cyklu pro $i = 1$ se tato rovnost vyhodnotí a procedura vrátí hodnotu 1, což znamená, $\alpha = 8 \in L_{65}$.

Příklad 135. Je dáno číslo $n = 13$. Pro toto číslo stanovte množiny M_n, K_n, $\beta_i^*(M_n)$ a L_n v Rabinově–Millerově testu prvočíselnosti. Stanovte všechny falešné svědky prvočíselnosti čísla n jak pro Fermatův test, tak pro Rabinův–Millerův test a porovnejte jejich počty. Pro zvolené prvky $\alpha \in \mathbb{Z}_n^* \setminus L_n$ a $\alpha \in L_n$ sledujte chod procedury LnT. Protože $13 - 1 = 3 \cdot 2^2$, pro další výpočty položme $t := 3$, $h := 2$.

Množina *Mn* Nechť $n = 13$. Pro množinu M_n platí

$$M_n = \{\alpha \in \mathbb{Z}_n \,|\, \alpha^2 = 1 \Rightarrow \alpha \in \{1, -1\}\} = \{\alpha \in \mathbb{Z}_n \,|\, \alpha^2 \neq 1\} \cup \{1, -1\}.$$

Protože $n = 13$ je prvočíslo, řešením rovnice $\alpha^2 = 1$ v $\mathbb{Z}_{13}$ je cyklická podgrupa $\mathbb{Z}_{13}^*$ řádu 2, tedy nutně $\alpha^2 = 1 \Leftrightarrow \alpha \in \{1, -1\}$. Odtud plyne

$$M_n = (\mathbb{Z}_n \setminus \{1, -1\}) \cup \{1, -1\} = \mathbb{Z}_n.$$

Množiny $\beta_i^*(M_n)$. Platí $\beta_i^*(M_n) = \beta_i^*(\mathbb{Z}_n) = \mathbb{Z}_n$.

Množiny *K*$_n$ L_n. Množina $K_n = \{\alpha \in \mathbb{Z}_n \,|\, \alpha^{n-1} = 1\}$ je klíčová množina Fermatova testu prvočíselnosti. Protože $n = 13$ je prvočíslo, podle Eulerovy–Fermatovy věty $K_n = \mathbb{Z}_n^*$. Odtud rovněž dostáváme

$$L_n = K_n \cap \bigcap_{i=0}^{h-1} \beta_i^*(M_n) = \mathbb{Z}_n^* \bigcap_{i=0}^{h-1} \mathbb{Z}_n = \mathbb{Z}_n^*.$$

Chod *Ln*(5,13)

(0) Zvolme $\alpha = 5 \in L_{65}$. Pro $\beta_0 = 5^3 = 125 = 8$. Protože $\beta_0 \notin \{-1, 1\}$, vypočte se v cyklu pro $i = 0$ hodnota $\beta_1 = 8^2 = 12 = -1$.

(1) Protože $\beta_1 = -1$ v cyklu pro $i = 1$ se tato rovnost vyhodnotí a procedura vrátí hodnotu 1, což znamená, $\alpha = 5 \in L_{13}$.

Příklad 136. Je dáno číslo $n = 21$. Pro toto číslo stanovte množiny M_n, K_n, $\beta_i^*(M_n)$ a L_n v Rabinově–Millerově testu prvočíselnosti. Stanovte všechny falešné svědky prvočíselnosti čísla n jak pro Fermatův test, tak pro Rabinův–Millerův test a porovnejte jejich počty. Pro zvolené prvky $\alpha \in \mathbb{Z}_n^* \setminus L_n$ a $\alpha \in L_n$ sledujte chod procedury LnT. Protože $21 - 1 = 5 \cdot 2^2$, pro další výpočty položme $t \coloneqq 5$, $h \coloneqq 2$.

Množina M_n Nechť $n = 21$. Pro množinu M_n platí

$$M_n = \{\alpha \in \mathbb{Z}_n \,|\, \alpha^2 = 1 \Rightarrow \alpha \in \{1, -1\}\} = \{\alpha \in \mathbb{Z}_n \,|\, \alpha^2 \neq 1\} \cup \{1, -1\}.$$

Prvků v množině M_n pro které $\alpha^2 \neq 1$ bude jistě hodně, stanovme proto komplement

$$\mathbb{Z}_n \setminus \{\alpha \in \mathbb{Z}_n \,|\, \alpha^2 \neq 1\} = \{\alpha \in \mathbb{Z}_n \,|\, \alpha^2 = 1\},$$

tj. řešme rovnici $x^2 = 1$ v $\mathbb{Z}_{21}$. Protože řešením jsou pouze prvky v $\mathbb{Z}_{21}^*$ a $\mathbb{Z}_{21}^* = \mathbb{Z}_{3\cdot 7}^*$, grupa není cyklická. Rovnici $x^2 = 1$ budeme řešit s využitím izomorfismu $\mathbb{Z}_{21}^* \leftrightarrows \mathbb{Z}_3^* \times \mathbb{Z}_7^*$. Řešení rovnice $x^2 = 1$ v obou grupách $\mathbb{Z}_3^*$ a $\mathbb{Z}_7^*$ budou cyklické podgrupy řádu 2, tedy zřejmě v $x^2 = 1 \Leftrightarrow x \in \{-1, 1\}$. Odtud plyne pomocí zmíněného izomorfismu

$$\{\alpha \in \mathbb{Z}_n \,|\, \alpha^2 = 1\} = (7 \cdot \tilde{7} \cdot \{\pm 1\} + 3 \cdot \tilde{3} \cdot \{\pm 1\})_{65} = (7 \cdot \{\pm 1\} - 6 \cdot \{\pm 1\})_{65} = \{\pm 1, \pm 13\}.$$

Máme tedy

$$M_n = (\mathbb{Z}_n \cap \{\pm 1, \pm 13\}^c) \cup \{\pm 1\} = (\mathbb{Z}_n \cap \{\pm 13\}^c) \cup \{\pm 1\} = \mathbb{Z}_n \setminus \{\pm 13\} = \mathbb{Z}_n \setminus \{\pm 8\}.$$

Množiny $\beta_i^*(M_n)$. Platí $\beta_i^*(M_n) = \beta_i^*(\mathbb{Z}_n \setminus \{\pm 8\}) = \mathbb{Z}_n \setminus \beta_i^*(\{\pm 8\})$. Stanovíme proto množiny $\beta_i^*(\{\pm 8\})$.

• Nejprve $\beta_0^*(\{\pm 8\})$. Protože $\alpha \in \beta_0^*(\{\pm 8\}) \Leftrightarrow \alpha^5 \in \{\pm 8\}$. Protože ± 8 jsou invertibilní prvky v $\mathbb{Z}_{21}^*$, řešením budou invertibilní prvky v $\mathbb{Z}_{21}^*$. S využitím izomorfismu $\mathbb{Z}_{21}^* \rightleftarrows \mathbb{Z}_3^* \times \mathbb{Z}_7^*$, řešme rovnice $\alpha^5 = \pm 8$.

◦ Rovnice $\alpha^5 = 8$ v $\mathbb{Z}_3^*$. Protože $\mathbb{Z}_3^*$ je cyklická grupa a $\gcd(5, |\mathbb{Z}_3^*|) = 1$, je jediným řešením $\alpha = 8 = -1$.

◦ Rovnice $\alpha^5 = 8$ v $\mathbb{Z}_7^*$. Protože $\mathbb{Z}_7^*$ je cyklická grupa a $\gcd(5, |\mathbb{Z}_7^*|) = 1$, je jediným řešením $\alpha = 8 = 1$.

◦ Rovnice $\alpha^5 = -8$ v $\mathbb{Z}_3^*$. Obdobně předchozímu bodu, jediným řešením rovnice je $\alpha = -8 = 1$.

◦ Rovnice $\alpha^5 = -8$ v $\mathbb{Z}_7^*$. Obdobně předchozímu bodu, jediným řešením rovnice je $\alpha = -8 = -1$.

• Pro řešení rovnic v $\mathbb{Z}_{21}^*$ pomocí CRT izomorfismu máme:

$$\alpha^5 \in \{\pm 8\} \Leftrightarrow \alpha \in (7 \cdot \{\pm 1\} - 6 \cdot \{\mp 1\})_{21} = \{\pm 8\}$$

Máme tedy

$$\alpha^5 \in \{\pm 8\} \Leftrightarrow \alpha \in \{\pm 8\} \text{ v } \mathbb{Z}_7^*.$$

$$\beta_0^*(\{\pm 8\}) = \{\pm 8\}.$$

• Protože $\beta_1(\alpha) = \alpha^2$, je $\alpha \in \beta_1^*(\{\pm 8\}) \Leftrightarrow \alpha^2 \in \{\pm 8\}$. Protože prvky ± 8 jsou invertibilními prvky okruhu $\mathbb{Z}_{21}$, budou řešením rovnic $\alpha^2 = 8$, $\alpha^2 = -8$ invertibilní prvky okruhu $\mathbb{Z}_{21}$. S využitím izomorfismu $\mathbb{Z}_{21}^* \cong \mathbb{Z}_3^* \times \mathbb{Z}_7^*$, hledejme řešení uvedených rovnic. Podle Eulerova testu nejprve zjistěme řešitelnost rovnic $\alpha^2 = 8$, $\alpha^2 = -8$ v $\mathbb{Z}_3^*$ a $\mathbb{Z}_7^*$.
Rovnice $\alpha^2 = 8$. Platí $8^{\frac{1}{2}\varphi(3)} = -1$, $8^{\frac{1}{2}\varphi(7)} = 1$, rovnice $\alpha^2 = 8$ není v $\mathbb{Z}_{21}^*$ řešitelná.
Rovnice $\alpha^2 = -8$. Platí $(-8)^{\frac{1}{2}\varphi(3)} = -8 = 1$, $(-8)^{\frac{1}{2}\varphi(7)} = -1$, rovnice $\alpha^2 = -8$ není v $\mathbb{Z}_{21}^*$ řešitelná.
Odtud plyne

$$\beta_1^*(\{\pm 13\}) = \sqrt{\{\pm 13\}} = \emptyset$$

• Protože platí $\beta_i^*(T) = \beta_0^*(\sqrt[2^i]{T})$, plyne z předchozího výsledku pro $i \geq 0$

$$\beta_{1+i}^*(\{\pm 8\}) = \beta_0^*(\sqrt[2^{1+i}]{\{\pm 8\}}) = \beta_0^*(\sqrt[2^i]{\sqrt[2]{\{\pm 8\}}}) = \beta_0^*(\sqrt[2^i]{\emptyset}) = \emptyset.$$

Množiny $\beta_i^*(M_n)$. Protože $M_n = \mathbb{Z}_n \setminus \{\pm 8\}$, dostaneme

$$\begin{aligned}
\beta_i^*(M_n) &= \beta_i^*(\mathbb{Z}_n \setminus \{\pm 8\}) = \beta_i^*(\mathbb{Z}_n) \setminus \beta_i^*(\{\pm 8\}) = \mathbb{Z}_n \setminus \beta_0^*(\sqrt[2^i]{\{\pm 8\}}) = \mathbb{Z}_n \setminus \sqrt[2^i]{\{\pm 8\}} \\
\beta_0^*(M_n) &= \mathbb{Z}_n \setminus \sqrt[2^0]{\{\pm 1\}} = \mathbb{Z}_n \setminus \{\pm 8\}, \\
\beta_1^*(M_n) &= \mathbb{Z}_n \setminus \sqrt[2^1]{\{\pm 8\}} = \mathbb{Z}_n \setminus \emptyset = \mathbb{Z}_n.
\end{aligned}$$

Množina K_n Klíčová množina Fermatova testu prvočíselnosti, $K_n = \{\alpha \in \mathbb{Z}_n \,|\, \alpha^{n-1} = 1 \text{ v } \mathbb{Z}_n\}$. Zřejmě $K_{21} \subseteq \mathbb{Z}_{21}^*$, s využitím izomorfismu $\mathbb{Z}_{21}^* \cong \mathbb{Z}_3^* \times \mathbb{Z}_7^*$, řešme rovnici $x^{20} = 1$ v $\mathbb{Z}_{21}^*$.
• $x^{20} = 1$ v $\mathbb{Z}_3^*$. Platí $x^{64} = 1 \Leftrightarrow x^2 = 1$, neboť $\gcd(20, |\mathbb{Z}_3^*|) = 2$, protože $|\mathbb{Z}_3^*| = 2$, řešením rovnice je tedy celá množina $\mathbb{Z}_3^*$.
• $x^{20} = 1$ v $\mathbb{Z}_7^*$. Platí $x^{20} = 1 \Leftrightarrow x^2 = 1$, neboť $\gcd(20, |\mathbb{Z}_7^*|) = 2$, kde $|\mathbb{Z}_7^*| = 6$. Řešením rovnice je v $\mathbb{Z}_7^*$ cyklická podgrupa řádu 2, tj. množina $\{1, -1\}$. CRT izomorfismus dává všechna řešení rovnice v $\mathbb{Z}_{21}^*$.

$$x^{20} = 1 \Leftrightarrow x \in (7 \cdot \{\pm 1\} - 6 \cdot \{\pm 1\})_{21} \Leftrightarrow x \in \{\pm 1, \pm 8\},$$
$$K_n = \{\pm 1, \pm 8\}.$$

Množina L_n Platí

$$\begin{aligned}
L_n &= K_n \cap \bigcap_{i=0}^{h-1} \beta_i^*(Z_n \setminus \{\pm 8\}) = K_n \cap \bigcap_{i=0}^{h-1} \beta_i^*(Z_n) \setminus \beta_i^*(\{\pm 8\}) = \\
&= K_n \cap \bigcap_{i=0}^{h-1} (Z_n \setminus \sqrt[2^i]{\{\pm 8\}}) = K_n \setminus \bigcup_{i=0}^{h-1} \sqrt[2^i]{\{\pm 8\}} = \\
&= K_n \setminus \{\pm 8\} = \\
&= \{\pm 1\} \cdots \text{falešní svědkové prvočíselnosti.}
\end{aligned}$$

Pro pravděpodobnost výroku „21 je prvočíslo“ v případě jednoho pokusu máme u Fermatova testu hodnotu $\frac{|K_{21}|}{|Z_{21}^+|} = \frac{4}{20} \doteq 0.25$, u Rabinova–Millerova testu vychází

$\frac{|L_{21}|}{|Z_{21}^+|} = \frac{2}{20} \doteq 0.1$. U Fermatova testu máme 2.5 krát vyšší pravděpodobnost chybné odpovědi.

Chod *LnT*(-1,21)

(0) Zvolme $\alpha = -1 \in L_{21}$. Vypočte se $\beta_0 = \alpha^5 = -1 \neq 1$.
Protože $\beta_0 \neq 1$, procedura vstoupí do cyklu s indexem $i = 0$. Protože $\beta_0 = -1$, v cyklu se hodnota vyhodnotí, procedura vrátí hodnotu 1, což znamená $\alpha = -1 \in L_{21}$ a procedura se ukončí.

Chod *LnT*(2,21)

(0) Zvolme $\alpha = 2 \in \mathbb{Z}_{21} \setminus L_{21}$. Pro $\beta_0 = \alpha^5 = 11$. Protože $\beta_0 \notin \{-1, 1\}$, vypočte se v cyklu pro $i = 0$ hodnota $\beta_1 = 11^2 = 16$.
(1) Protože $\beta_1 \notin \{1, -1\}$ v cyklu pro $i = 1$ se vypočte $\beta_2 = 4$, hodnota se zahodí, maximální počet cyklů h je dovršen, cykl se ukončí a procedura vrátí hodnotu 0 což znamená, že $\alpha \notin L_{21}$.

GRUPY

Definice 137. Grupa G je (vnitřním) direktním součinem podgrup $G_i \subseteq| G$, $i \in \{1, ..., n\}$ právě když zobrazení $(a_1, ..., a_n) \mapsto a_1 \cdot ... \cdot a_n : G_1 \times \cdots \times G_n \to G$ je izomorfismus grup. Symbolický zápis:

$$G = G_1 \dot{\times} \cdots \dot{\times} G_n.$$

Lemma 138.
Jestliže podgrupy $G_i \subseteq| G$, $i = 1, .., n$ jsou komutativní, pak $G = G_1 \dot{\times} \cdots \dot{\times} G_n$, je komutativní.
Jestliže $A, B \subseteq| G \in \mathbf{Ab}$, $|G| = |A|\,|B| \in \mathbb{N}^+$, $A \cap B = \{1\}$, potom $G = A \dot{\times} B$.
Jestliže $A, B \subseteq| G \in \mathbf{Ab}$, $|G| \in \mathbb{N}^+$, $\gcd(|A|, |B|) = 1$, pak $A \cap B = \{1\}$, $G^{|A|} = B$, $G^{|B|} = A$.

Příklad 139. S využitím CRT izomorfismů stanovte podgrupy $A, B \subseteq| \mathbb{Z}_{15}^*$ direktního rozkladu grupy $\mathbb{Z}_{15}^* = A \dot{\times} B$ a pro prvky 2, 8 stanovte jejich rozklad $2 = u \cdot v$, $u \in A$, $v \in B$, $8 = u \cdot v$, $u \in A$, $v \in B$.

Řešení: Pomocí CRT izomorfismů platí $\mathbb{Z}_{15}^* \underset{g}{\overset{f}{\rightleftarrows}} \mathbb{Z}_3^* \times \mathbb{Z}_5^*$, kde $f(x) = ((x)_3, (y)_5)$, $g(u, v) = (-5u + 6v)_{15}$. Protože $A' := \{(u, 1) \,|\, u \in \mathbb{Z}_3^*\}$, $B' := \{(1, v) \,|\, v \in \mathbb{Z}_5^*\}$, jsou podgrupy grupy $\mathbb{Z}_3^* \times \mathbb{Z}_5^*$, pro které platí $A' \cap B' = \{(1, 1)\}$ a každý prvek (u, v) grupy $\mathbb{Z}_3^* \times \mathbb{Z}_5^*$ je součinem jediných dvou prvků z $A' \times B'$, totiž $(u, v) = (u, 1) \cdot (1, v)$, tj. $\mathbb{Z}_3^* \times \mathbb{Z}_5^* = A' \dot{\times} B'$. Odtud plyne $A = g(A')$, $B = g(B')$, tj. platí

$$\begin{aligned} A &= (-5 \cdot \{1, 2\} + 6 \cdot 1)_{15} = \{1, 11\}, \\ B &= (-5 \cdot 1 + 6 \cdot \{1, 2, 3, 4\})_{15} = \{1, 7, 13, 4\}. \end{aligned}$$

Využitím uvedených izomorfismů získáme hledané reprezentace prvků 2, 8.

$$\begin{aligned} 2 &= g \circ f(2) = g(2, 2) = g((2, 1) \cdot (1, 2)) = g(2, 1) \cdot g(1, 2) = 11 \cdot 7, \\ 8 &= g \circ f(8) = g(2, 3) = g((2, 1) \cdot (1, 3)) = g(2, 1) \cdot g(1, 3) = 11 \cdot 13. \end{aligned}$$

Ostatní reprezentace plynou z dále uvedené tabulky součinů:

1	7	13	4
11	2	8	14

Tabulka 7: Součiny direktních podgrup $A\dot{\times}B$

Poznámka. Námi nalezený rozklad grupy $\mathbb{Z}_{15}^*$ na vnitřní direktní součin podgrup není jediný, stejně jako CRT–izomorfismus není jediným izomorfismem grup $\mathbb{Z}_{15}^*$, $\mathbb{Z}_3^* \times \mathbb{Z}_5^*$. Například pro další rozklady platí $\mathbb{Z}_{15}^* = \langle 11\rangle \dot{\times} \langle 2\rangle = \langle 14\rangle \dot{\times} \langle 2\rangle$.

Příklad 140. Využitím CRT izomorfismů stanovte podgrupy $A, B \subseteq| \mathbb{Z}_{20}^*$ direktního rozkladu grupy $\mathbb{Z}_{20}^* = A\dot{\times}B$ a pro prvky 3, 19 stanovte jejich rozklad $3 = u \cdot v$, $u \in A$, $v \in B$, $19 = u \cdot v$, $u \in A$, $v \in B$.

Řešení: Pomocí CRT izomorfismů platí $\mathbb{Z}_{20}^* \overset{f}{\underset{g}{\rightleftarrows}} \mathbb{Z}_4^* \times \mathbb{Z}_5^*$, kde $f(x) = ((x)_4, (y)_5)$, $g(u,v) = (5u - 4v)_{20}$. Protože $A' := \{(u,1) \,|\, u \in \mathbb{Z}_4^*\}$, $B' := \{(1,v) \,|\, v \in \mathbb{Z}_5^*\}$, jsou podgrupy grupy $\mathbb{Z}_4^* \times \mathbb{Z}_5^*$, pro které platí $A' \cap B' = \{(1,1)\}$ a každý prvek (u,v) grupy $\mathbb{Z}_4^* \times \mathbb{Z}_5^*$ je součinem jediných dvou prvků z $A' \times B'$, totiž $(u,v) = (u,1) \cdot (1,v)$, tj. $\mathbb{Z}_4^* \times \mathbb{Z}_5^* = A'\dot{\times}B'$. Odtud plyne $A = g(A')$, $B = g(B')$, tj. platí

$$\begin{aligned} A &= (5 \cdot \{1,3\} - 4 \cdot 1)_{20} = \{1, 11\}, \\ B &= (5 \cdot 1 - 4 \cdot \{1,2,3,4\})_{20} = \{1, 17, 13, 9\}. \end{aligned}$$

Využitím uvedených izomorfismů získáme hledané reprezentace prvků 2, 8.

$$\begin{aligned} 3 &= g \circ f(3) = g(3,3) = g((3,1) \cdot (1,3)) = g(3,1) \cdot g(1,3) = 11 \cdot 13, \\ 19 &= g \circ f(19) = g(3,4) = g((3,1) \cdot (1,4)) = g(3,1) \cdot g(1,4) = 11 \cdot 9. \end{aligned}$$

Příklad 141. Najděte všechny direktní rozklady grupy $\mathbb{Z}_{31}^*$ tvaru $\mathbb{Z}_{31}^* = A\dot{\times}B$.

Řešení: Protože 31 je prvočíslo, grupa $\mathbb{Z}_{31}^*$ je cyklická, svaz dělitelů čísla $|\mathbb{Z}_{31}^*| = 30 = 2 \cdot 3 \cdot 5$ je izomorfní se svazem podgrup grupy $\mathbb{Z}_{31}^*$. Možné řády dvojic podgrup $A, B \subseteq| \mathbb{Z}_{31}^*$, které v součinu dávají $|\mathbb{Z}_{31}^*| = 30$, jsou následující:

$$30 = |A|\,|B| = 2 \cdot 15 = 3 \cdot 10 = 5 \cdot 6,$$

Řády podgrup v uvedených součinech jsou nesoudělná čísla, proto platí $A \cap B = \{1\}$. Stačí tedy najít odpovídající podgrupy uvedených řádů. Za tím účelem stanovme generátor grupy $\mathbb{Z}_{31}^*$.
Prvek $g \in \mathbb{Z}_{31}^*$ bude generátor grupy $\mathbb{Z}_{31}^*$ právě když $1 \notin \{g^6, g^{10}, g^{15}\}$. Platí:

$$\begin{aligned} g = 2 &\;\Rightarrow\; \{g^6, g^{10}, g^{15}\} = \{2, 1, 1\} \text{ podmínka nesplněna}, \\ g = 3 &\;\Rightarrow\; \{g^6, g^{10}, g^{15}\} = \{16, 25, 30\} \text{ podmínka splněna}, \end{aligned}$$

máme tedy $\mathbb{Z}_{31}^* = \langle 3 \rangle$. Pro podgrupy uvedených řádů platí

$$\begin{aligned} \left|\langle 3^{15} \rangle \times \langle 3^2 \rangle\right| &= |\langle 30 \rangle| \cdot |\langle 9 \rangle| = \quad 2 \cdot 15, \\ \left|\langle 3^{10} \rangle \times \langle 3^3 \rangle\right| &= |\langle 25 \rangle| \cdot |\langle 27 \rangle| = \quad 3 \cdot 10, \\ \left|\langle 3^6 \rangle \times \langle 3^5 \rangle\right| &= |\langle 16 \rangle| \cdot |\langle 26 \rangle| = \quad 5 \cdot 6. \end{aligned}$$

Pro hledané rozklady platí $\mathbb{Z}_{31}^* = \langle 30 \rangle \dot{\times} \langle 9 \rangle = \langle 25 \rangle \dot{\times} \langle 27 \rangle = \langle 16 \rangle \dot{\times} \langle 26 \rangle$. Řešením jsou i součiny zapsané v obráceném pořadí, tedy např. $\langle 9 \rangle \dot{\times} \langle 30 \rangle$ atd.

Věta 142. *Nechť $p, q \in \mathbb{P}$, $p - 1 = q^e \cdot m$, $e \in \mathbb{N}^+$, $q \nmid m$, $b \in \langle a \rangle \subseteq | \, \mathbb{Z}_p^* = \langle a \rangle \dot{\times} H$, $|\langle a \rangle| = q^e$, $|H| = m$. Nechť dále $k \in \mathbb{N}^+$, $p_1, ..., p_k$ jsou po dvou různá prvočísla a existují posloupnosti*

$$\begin{aligned} s, t : \{1, ..., k+1\} &\to \{0, 1, ..., q^e - 1\}, \\ h : \{1, ..., k+1\} &\to H, \\ e_1, ..., e_k : \{1, ..., k+1\} &\to \mathbb{N}, \end{aligned}$$

pro které platí

$$(a^{s_i} b^{t_i} h_i)_p = p_1^{e_{1i}} \cdot ... \cdot p_k^{e_{ki}}, \text{ pro } i \in \{1, .., k+1\}, \tag{15}$$

kde a, b, h_i na levé straně rovnosti (15) jsou libovolní reprezentanti odpovídajících zbytkových tříd $a, b, h_i \in \mathbb{Z}_p^*$.
Pak pro každý vektor $\boldsymbol{c} = (c_1, ..., c_{k+1}) \in \mathbb{Z}_{q^e}^{k+1}$, který je v prostoru $\mathbb{Z}_{q^e}^{k+1}$ řešením homogenní soustavy

$$\begin{bmatrix} e_{11} & \cdots & e_{1,k+1} \\ \vdots & & \vdots \\ e_{k1} & \cdots & e_{k,k+1} \end{bmatrix} \cdot \begin{bmatrix} c_1 \\ \vdots \\ c_{k+1} \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}, \tag{16}$$

platí

$$a^s b^t = 1,$$

kde $s = (s_1 c_1 + ... + s_{k+1} c_{k+1})_{q^e}$, $t = (t_1 c_1 + ... + t_{k+1} c_{k+1})_{q^e}$.

Příklad 143. Nechť $p = 509$, $q = 127$, $p - 1 = 4 \cdot q$, $p, q \in \mathbb{P}$. Dále je dáno $54 \in \langle 16 \rangle \subseteq | \, \mathbb{Z}_{509}^* = \langle 16 \rangle \dot{\times} H$, kde $|\langle 16 \rangle| = 127$, $H = \{1, 208, 301, 508\}$. Algoritmem SEDL stanovte netriviální reprezentaci prvku 1 vzhledem ke generátoru 16 a prvku 54 v grupě $\mathbb{Z}_{509}^*$ a na základě toho vypočtěte $\mathrm{dlog}_{16} 54$.

Řešení:
1. fáze algoritmu. Zvolme prvočísla $p_1, p_2, p_3, p_4 = 2, 3, 5, 7$. K náhodné volbě $s_i, t_i \in \{0, 1, ..., 126\}$, $h_i \in \{1, 208, 301, 508\}$ vypočteme (opakovaným dělením prvočísly p_1, p_2, p_3, p_4) exponenty $e_{1i}, ..., e_{4i} \in \mathbb{N}$ tak, aby platilo $(a^{s_i} b^{t_i} h_i)_p = p_1^{e_{1i}} p_2^{e_{2i}} p_3^{e_{3i}} p_4^{e_{4i}}$. Pokud taková čtveřice exponentů neexistuje, provedeme jinou volbu s_i, t_i, h_i. Tímto způsobem pro $i \in \{1, .., 5\}$ získáme údaje, viz příklad v následující tabulce, kde jsou pro kontrolu navíc uvedeny veličiny $x_i = (a^{s_i} b^{t_i} h_i)_p = p_1^{e_{1i}} p_2^{e_{2i}} p_3^{e_{3i}} p_4^{e_{4i}}$.

i	s	t	h	x	e_1	e_2	e_3	e_4	pokusy
1	117	23	508	189	0	3	0	1	3
2	8	52	301	10	1	0	1	0	4
3	93	51	508	144	4	2	0	0	4
4	8	104	301	288	5	2	0	0	7
5	8	113	1	294	1	1	0	2	4

Tabulka 8: Konkrétní realizace algoritmu SEDL

2. fáze algoritmu. V tělese $\mathbb{Z}_{127}$ řešíme homogenní soustavu rovnic pro neznámý vektor $\boldsymbol{c} = (c_1, ..., c_5) \in \mathbb{Z}_{127}^5$ s maticí soustavy tvořenou sloupcovými vektory $\boldsymbol{e}_i = (e_{1i}, e_{2i}, e_{3i}, e_{4i})$, $i \in \{1, ..., 5\}$. Dostaneme:

$$\begin{bmatrix} 0 & 1 & 4 & 5 & 1 \\ 3 & 0 & 2 & 2 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 2 \end{bmatrix} \begin{matrix} \\ \\ (-3,4,2) \\ (-1,3,1) \end{matrix} \sim \begin{bmatrix} 0 & 0 & 4 & 5 & 1 \\ 0 & 0 & 2 & 2 & -5 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 2 \end{bmatrix} \begin{matrix} \\ \\ (-2,2,1) \\ (1/4),(2/3) \\ (-2,4,3) \end{matrix} \sim \begin{bmatrix} 1 & 0 & 0 & 0 & 2 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & -27 \\ 0 & 0 & 0 & 1 & 11 \end{bmatrix}.$$

Pro získání reprezentace je třeba vybrat řešení nenulové (netriviální). Jestliže zvolíme $c_5 \in \mathbb{Z}_{127}$ libovolně, ostatní složky vektoru $\boldsymbol{c}$ jsou již jednoznačně určeny. Dostaneme: $c_1 = -2c_5$, $c_2 = 0$, $c_3 = 2^{-1} \cdot 27c_5 = 77c_5$, $c_4 = -11c_5$, tj.

$$\boldsymbol{c} = (-2, 0, 77, -11, 1)c_5 = (125, 0, 77, 116, 1)c_5.$$

Zvolme vektor $\boldsymbol{c} = (125, 0, 77, 116, 1)$.

3. fáze algoritmu. Podle Věty 142 vypočteme v $\mathbb{Z}_{127}$ „skalární součiny“, tj. hodnoty

$$\begin{aligned} s &= (117, 8, 93, 8, 8) \bullet (125, 0, 77, 116, 1) = 117 \cdot 125 + 8 \cdot 0 + 93 \cdot 77 + 8 \cdot 116 + 8 \cdot 1 = 116, \\ t &= (23, 52, 51, 104, 113) \bullet (125, 0, 77, 116, 1) = 23 \cdot 125 + 52 \cdot 0 + 51 \cdot 77 + 104 \cdot 116 + 113 \cdot 1 = 56, \end{aligned}$$

dále podle téže věty platí v grupě $\mathbb{Z}_{509}^*$

$$16^{116} \cdot 54^{56} = 1.$$

Protože $\gcd(56, 127) = 1$, jedná se o netriviální reprezentaci prvku 1 vzhledem ke generátoru 16 a prvku 54, která umožňuje vypočítat $\mathrm{dlog}_{16}54$ jako jediné řešení rovnice $116 + 56 \cdot \mathrm{dlog}_{16}54 = 0$ v $\mathbb{Z}_{127}$. Protože $-34 \cdot 56 = 1$ v $\mathbb{Z}_{127}$, dostaneme

$$\mathrm{dlog}_{16}54 = 34 \cdot 116 = 7.$$

Kontrolní výpočet, $16^7 = 54$ v grupě $\mathbb{Z}_{509}^*$.

Příklad 144. Nechť $p = 53$, $q = 13$, $p - 1 = 4 \cdot q$, $p, q \in \mathbb{P}$. Dále je dáno $10 \in \langle 15 \rangle \subseteq| \mathbb{Z}_{53}^* = \langle 2 \rangle = \langle 15 \rangle \dot{\times} H$, kde $|\langle 15 \rangle| = 13$, $H = \{1, 30, 52, 28\}$. Algoritmem SEDL stanovte netriviální reprezentaci prvku 1 vzhledem ke generátoru $a = 15$ a prvku $b = 10$ v grupě $\mathbb{Z}_{53}^*$ a na základě toho vypočtěte $\mathrm{dlog}_{15} 10$.

Řešení:
1. fáze algoritmu. Zvolme prvočísla $p_1, p_2, p_3 = 2, 3, 5$. K náhodné volbě $s_i, t_i \in \{0, 1, ..., 12\}$, $h_i \in \{1, 30, 52, 23\}$ vypočteme (opakovaným dělením prvočísly p_1, p_2, p_3) exponenty $e_{1i}, e_{2i}, e_{3i} \in \mathbb{N}$ tak, aby platilo $(a^{s_i} b^{t_i} h_i)_p = p_1^{e_{1i}} p_2^{e_{2i}} p_3^{e_{3i}}$. Pokud taková trojice exponentů neexistuje, provedeme jinou volbu s_i, t_i, h_i. Tímto způsobem pro $i \in \{1, .., 4\}$ získáme údaje, viz příklad v následující tabulce, kde jsou pro kontrolu navíc uvedeny veličiny $x_i = (a^{s_i} b^{t_i} h_i)_p = p_1^{e_{1i}} p_2^{e_{2i}} p_3^{e_{3i}}$.

i	s	t	h	x	e_1	e_2	e_3	pokusy
1	0	12	23	50	1	0	2	2
2	8	7	52	25	0	0	2	1
3	9	0	23	50	1	0	2	1
4	11	9	30	32	5	0	0	1

Tabulka 9: Konkrétní realizace algoritmu SEDL

2. fáze algoritmu. V tělese $\mathbb{Z}_{13}$ řešíme homogenní soustavu rovnic pro neznámý vektor $\boldsymbol{c} = (c_1, ..., c_4) \in \mathbb{Z}_{13}^4$ s maticí soustavy tvořenou sloupcovými vektory $\boldsymbol{e}_i = (e_{1i}, e_{2i}, e_{3i})$, $i \in \{1, ..., 4\}$. Dostaneme:

$$\begin{bmatrix} 1 & 0 & 1 & 5 \\ 0 & 0 & 0 & 0 \\ 2 & 2 & 2 & 0 \end{bmatrix}_{(-2,1,3)} \sim \begin{bmatrix} 1 & 0 & 1 & 5 \\ 0 & 2 & 0 & -10 \end{bmatrix}_{(-6,2,1)} \sim \begin{bmatrix} 1 & 0 & 1 & 5 \\ 0 & 1 & 0 & 8 \end{bmatrix}.$$

Pro získání reprezentace (nejenom netriviální) je třeba vybrat řešení nenulové (netriviální). Jestliže zvolíme $c_3, c_4, \in \mathbb{Z}_{13}$ libovolně, pro ostatní složky vektoru $\boldsymbol{c}$ dostaneme: $c_1 = -c_3 - 5c_4$, $c_2 = -8c_4$, tj. dostaneme

$$\boldsymbol{c} = c_3(-1, 0, 1, 0) - c_4(5, 8, 0, -1).$$

Zvolme vektor $\boldsymbol{c} = (-1, 0, 1, 0) = (12, 0, 1, 0)$.

3. fáze algoritmu. Podle Věty 142 vypočteme v $\mathbb{Z}_{13}$ hodnoty „skalárních součinů“

$$\begin{aligned} s &= (0, 8, 9, 11) \bullet (12, 0, 1, 0) = 9, \\ t &= (12, 7, 0, 9) \bullet (12, 0, 1, 0) = 12^2 = 1, \end{aligned}$$

dále podle téže věty platí v grupě $\mathbb{Z}_{13}^*$

$$15^9 \cdot 10^1 = 1.$$

Protože $\gcd(1,13)=1$, jedná se o netriviální reprezentaci prvku 1 vzhledem ke generátoru 15 a prvku 10, která umožňuje vypočítat $\mathrm{dlog}_{15}10$ jako jediné řešení rovnice $9+1\cdot \mathrm{dlog}_{15}10=0$ v $\mathbb{Z}_{13}$. Odtud dostaneme $\mathrm{dlog}_{15}10=-9=4$.

Kontrolní výpočet, $15^4=10$ v grupě $\mathbb{Z}_{53}^*$.

Příklad 145. Nechť $p=101$, $q=5$, $p-1=4\cdot q^2$, $p,q\in\mathbb{P}$. Dále je dáno $25\in\langle 16\rangle \subseteq| \mathbb{Z}_{101}^* = \langle 2\rangle = \langle 16\rangle \dot{\times} H$, kde $|\langle 16\rangle| = 5^2 = 25$, $H=\{1,10,100,91\}$. Algoritmem SEDL stanovte netriviální reprezentaci prvku 1 vzhledem ke generátoru $a=16$ a prvku $b=25$ v grupě $\mathbb{Z}_{25}^*$ a na základě toho vypočtěte $\mathrm{dlog}_{16}25$.

Řešení:
1. fáze algoritmu. Zvolme prvočísla $p_1,p_2,p_3,p_4 = 2,3,5,7$. K náhodné volbě $s_i,t_i\in\{0,1,...,24\}$, $h_i\in\{1,10,100,91\}$ vypočteme (opakovaným dělením prvočísly p_1,p_2,p_3,p_4) exponenty $e_{1i},e_{2i},e_{3i},e_{4i}\in\mathbb{N}$ tak, aby platilo $(a^{s_i}b^{t_i}h_i)_p = p_1^{e_{1i}}p_2^{e_{2i}}p_3^{e_{3i}}p_4^{e_{4i}}$. Pokud taková čtveřice exponentů neexistuje, provedeme jinou volbu s_i,t_i,h_i. Tímto způsobem pro $i\in\{1,..,5\}$ získáme údaje, viz příklad v následující tabulce, kde jsou pro kontrolu navíc uvedeny veličiny $x_i=(a^{s_i}b^{t_i}h_i)_p = p_1^{e_{1i}}p_2^{e_{2i}}p_3^{e_{3i}}p_4^{e_{4i}}$.

i	s	t	h	x	e_1	e_2	e_3	e_4	pokusy
1	20	11	91	90	1	2	1	0	1
2	5	9	1	24	3	1	0	0	2
3	0	13	91	18	1	2	0	0	1
4	23	4	91	42	1	1	0	1	6
5	14	24	91	8	3	0	0	0	1

Tabulka 10: Konkrétní realizace algoritmu SEDL

2. fáze algoritmu. V okruhu $\mathbb{Z}_{25}$ řešíme homogenní soustavu rovnic pro neznámý vektor $\boldsymbol{c}=(c_1,...,c_5)\in\mathbb{Z}_{25}^5$ s maticí soustavy tvořenou sloupcovými vektory $\boldsymbol{e}_i=(e_{1i},e_{2i},e_{3i},e_{4i})$, $i\in\{1,...,5\}$. Dostaneme:

$$\begin{bmatrix}1&3&1&1&3\\2&1&2&1&0\\1&0&0&0&0\\0&0&0&1&0\end{bmatrix}\begin{matrix}\\(-1,3,1)\\(-2,3,2)\\(-1,4,1)\\(-1,4,2)\end{matrix}\sim\begin{bmatrix}0&3&1&0&3\\0&1&2&0&0\\1&0&0&0&0\\0&0&0&1&0\end{bmatrix}\begin{matrix}\\(-3,2,1)\\(1/3)\end{matrix}\sim\begin{bmatrix}1&0&0&0&0\\0&1&2&0&0\\0&0&-5&0&3\\0&0&0&1&0\end{bmatrix}.$$

Gaussova eliminace zde končí, prvek -5 není v $\mathbb{Z}_{25}$ invertibilním prvkem. Výměnou 3. a 5.

sloupce a vynásobením 3. řádku inverzním prvkem 3^{-1} dostaneme soustavu

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 2 \\ 0 & 0 & 1 & 0 & 15 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} c_1 \\ c_2 \\ c_5 \\ c_4 \\ c_3 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix},$$

ze které je zřejmé, že všechna její řešení získáme libovolnou volbou $c_3 \in \mathbb{Z}_{25}$, ostatní složky vektoru $\boldsymbol{c}$ jsou v $\mathbb{Z}_{25}$ touto volbou jednoznačně určeny. Dostaneme

$$(c_1, c_2, c_3, c_4, c_5) = -c_3(0, 2, -1, 0, 15).$$

Vyberme nenulové řešení $\boldsymbol{c} = (0, 2, -1, 0, 15)$.

3. fáze algoritmu. Podle Věty 142 vypočteme v $\mathbb{Z}_{25}$ hodnoty „skalárních součinů“

$$\begin{aligned} s &= (20, 5, 0, 23, 14) \bullet (0, 2, -1, 0, 15) = 20, \\ t &= (11, 9, 13, 4, 24) \bullet (0, 2, -1, 0, 15) = 15, \end{aligned}$$

odtud podle téže věty platí v grupě $\mathbb{Z}_{101}^*$

$$16^{20} \cdot 25^{15} = 1.$$

Protože $\gcd(15, 25) = 5$, **ne**jedná se o netriviální reprezentaci prvku 1 vzhledem ke generátoru 16 a prvku 25, která umožňuje vypočítat $\mathrm{dlog}_{16}25$ pouze jako jedno z pěti řešení rovnice $20 + 15 \cdot \mathrm{dlog}_{16}25 = 0 \Leftrightarrow 15 \cdot \mathrm{dlog}_{16}25 = 5$ v $\mathbb{Z}_{25}$. Řešením diofantické rovnice $15x + 25y = 5$ v $\mathbb{Z}$ dostaneme

$$\begin{bmatrix} 15 & 1 & 0 \\ 25 & 0 & 1 \end{bmatrix} \sim \begin{bmatrix} 15 & 1 & 0 \\ 10 & -1 & 1 \end{bmatrix} \sim \begin{bmatrix} 5 & 2 & -1 \\ 10 & -1 & 1 \end{bmatrix} \sim \begin{bmatrix} 5 & 2 & -1 \\ 0 & -5 & 3 \end{bmatrix}.$$

Odtud dostaneme pro řešení x v $\mathbb{Z}_{25}$ prvky $\{2, 7, 12, 17, 22\}$. Dále v $\mathbb{Z}_{101}^*$ vypočteme

$$16^{\{2,7,\mathbf{12},17,22\}} = \{54, 80, \mathbf{25}, 52, 92\}$$

Tedy

$$\mathrm{dlog}_{16}25 = 12.$$

1. fáze algoritmu. Pokračování příkladu s týmž zadáním pro jinou konkrétní realizaci algoritmu:

i	s	t	h	x	e_1	e_2	e_3	e_4	pokusy
1	13	11	1	84	2	1	0	1	1
2	3	9	100	30	1	1	1	0	3
3	23	15	100	45	0	2	1	0	1
4	21	2	1	84	2	1	0	1	1
5	4	16	100	70	1	0	1	1	3

Tabulka 11: Jiná konkrétní realizace algoritmu SEDL

2. fáze algoritmu. V okruhu $\mathbb{Z}_{25}$ řešíme homogenní soustavu rovnic pro neznámý vektor $\boldsymbol{c} = (c_1, ..., c_5) \in \mathbb{Z}_{25}^5$ s maticí soustavy tvořenou sloupcovými vektory $\boldsymbol{e}_i = (e_{1i}, e_{2i}, e_{3i}, e_{4i})$, $i \in \{1, ..., 5\}$. Dostaneme:

$$\begin{bmatrix} 2 & 1 & 0 & 2 & 1 \\ 1 & 1 & 2 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 \end{bmatrix} \begin{matrix} \\ \\ (-2,4,1) \\ (-1,4,2) \end{matrix} \sim \begin{bmatrix} 0 & 1 & 0 & 0 & -1 \\ 0 & 1 & 2 & 0 & -1 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 \end{bmatrix} \begin{matrix} \\ \\ (-1,1,2) \\ (-1,1,3) \\ (-2,3,2) \end{matrix} \sim \begin{bmatrix} 0 & 1 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & -4 \\ 0 & 0 & 1 & 0 & 2 \\ 1 & 0 & 0 & 1 & 1 \end{bmatrix} \begin{matrix} \\ \\ (1/4) \\ (2/4) \end{matrix} \sim$$

$$\sim \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 & 2 \\ 0 & 0 & 0 & 0 & -4 \end{bmatrix} \begin{matrix} \\ (6,4) \\ (-2,4,3) \\ (1,4,2) \\ (-1,4,1) \end{matrix} \sim \begin{bmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

Gaussova eliminace zde končí, dostali jsme soustavu

$$\begin{bmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} c_1 \\ c_2 \\ c_3 \\ c_4 \\ c_5 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix},$$

ze které je zřejmé, že $c_1 = -c_4$, $c_2 = c_3 = c_5 = 0$, všechna její řešení získáme libovolnou volbou $c_4 \in \mathbb{Z}_{25}$, ostatní složky vektoru $\boldsymbol{c}$ jsou v $\mathbb{Z}_{25}$ touto volbou jednoznačně určeny. Dostaneme

$$(c_1, c_2, c_3, c_4, c_5) = c_4(-1, 0, 0, 1, 0).$$

Vyberme nenulové řešení $\boldsymbol{c} = (24, 0, 0, 1, 0)$.

3. fáze algoritmu. Podle Věty 142 vypočteme v $\mathbb{Z}_{25}$ hodnoty „skalárních součinů“

$$\begin{aligned} s &= (13, 3, 23, 21, 4) \bullet (24, 0, 0, 1, 0) = 8, \\ t &= (11, 9, 15, 2, 16) \bullet (24, 0, 0, 1, 0) = 16, \end{aligned}$$

odtud podle téže věty platí v grupě $\mathbb{Z}_{101}^*$

$$16^8 \cdot 25^{16} = 1.$$

Protože $\gcd(16, 25) = 1$, jedná se o netriviální reprezentaci prvku 1 vzhledem ke generátoru 16 a prvku 25, která umožňuje vypočítat $\mathrm{dlog}_{16}25$ jako jediné řešení rovnice $8 + 16 \cdot \mathrm{dlog}_{16}25 = 0 \Leftrightarrow 16 \cdot \mathrm{dlog}_{16}80 = -8$ v $\mathbb{Z}_{25}$. Vynásobením rovnice prvkem 16^{-1} v $\mathbb{Z}_{25}^*$ dostaneme $\mathrm{dlog}_{16}25 = 11 \cdot (-8) = 12$.

Příklad 146. Nechť $p = 401$, $q = 5$, $p - 1 = 16 \cdot q^2$, $p, q \in \mathbb{P}$. Dále je dáno $88 \in \langle 5 \rangle \subseteq |\mathbb{Z}_{401}^* = \langle 3 \rangle = \langle 5 \rangle \dot{\times} H$, kde $|\langle 5 \rangle| = 5^2 = 25$, $|H| = 16$. Algoritmem SEDL stanovte netriviální reprezentaci prvku 1 vzhledem ke generátoru $a = 5$ a prvku $b = 88$ v grupě $\mathbb{Z}_{401}^*$ a na základě toho vypočtěte $\mathrm{dlog}_5 88$.

Řešení:
1. fáze algoritmu. Zvolme prvočísla $p_1, p_2, p_3, p_4 = 2, 3, 5, 7$. K náhodné volbě $s_i, t_i \in \{0, 1, ..., 24\}$, $h_i \in H$ vypočteme (opakovaným dělením prvočísly p_1, p_2, p_3, p_4) exponenty $e_{1i}, e_{2i}, e_{3i}, e_{4i} \in \mathbb{N}$ tak, aby platilo $(a^{s_i} b^{t_i} h_i)_p = p_1^{e_{1i}} p_2^{e_{2i}} p_3^{e_{3i}} p_4^{e_{4i}}$. Pokud taková čtveřice exponentů neexistuje, provedeme jinou volbu s_i, t_i, h_i. Protože řád grupy H je malý, prvky grupy H si nejprve vypočteme. Zřejmě H je cyklická grupa (podgrupa cyklické grupy je cyklická) s generátorem $3^{25} = 268$, tj

$$H = \{1, 268, 45, 30, 20, 147, 98, 199, 400, 133, 356, 371, 381, 254, 303, 202\}$$

Tímto způsobem pro $i \in \{1, 2, 3, ...\}$ získáme údaje, viz příklad v následující tabulce, kde jsou pro kontrolu navíc uvedeny veličiny $x_i = (a^{s_i} b^{t_i} h_i)_p = p_1^{e_{1i}} p_2^{e_{2i}} p_3^{e_{3i}} p_4^{e_{4i}}$. Z experimentálních důvodů jsme vypočetly více řádků tabulky, než bylo nutné, stačilo by 5 řádků.

i	s	t	h	x	e_1	e_2	e_3	e_4	pokusy
1	14	7	254	60	2	1	1	0	9
2 **4**	2	16	1	5	0	0	1	0	8
3	9	9	268	48	4	1	0	0	2
4	1	7	45	9	0	2	0	0	1
5	3	11	356	343	0	0	0	3	3
6	8	11	356	2	1	0	0	0	2
7	24	22	199	105	0	1	1	1	2
8 **1**	16	5	45	160	5	0	1	0	4
9	16	22	20	4	2	0	0	0	1
10	24	20	202	336	4	1	0	1	1
11	8	3	30	30	1	1	1	0	1
12	10	10	98	98	1	0	0	2	7
13 **5**	23	15	400	350	1	0	2	1	5
14	4	1	45	28	2	0	0	1	4
15 **3**	6	1	303	35	0	0	1	1	3
16 **2**	20	2	20	81	0	4	0	0	7

Tabulka 12: Konkrétní realizace algoritmu SEDL

2. fáze algoritmu. **(zelený výběr).** V okruhu $\mathbb{Z}_{25}$ řešíme homogenní soustavu rovnic pro neznámý vektor $\boldsymbol{c} = (c_1, ..., c_5) \in \mathbb{Z}_{25}^5$ s maticí soustavy tvořenou sloupcovými vektory

$\boldsymbol{e}_i = (e_{1i}, e_{2i}, e_{3i}, e_{4i})$, $i \in \{1, ..., 5\}$. Dostaneme:

$$\begin{bmatrix} 2 & 0 & 4 & 0 & 0 \\ 1 & 0 & 1 & 2 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 3 \end{bmatrix} \begin{matrix} \\ (-2,2,1) \\ (-1,2,3) \\ \\ \end{matrix} \sim \begin{bmatrix} 0 & 0 & 2 & -4 & 0 \\ 1 & 0 & 1 & 2 & 0 \\ 0 & 1 & -1 & -2 & 0 \\ 0 & 0 & 0 & 0 & 3 \end{bmatrix} \begin{matrix} \\ \\ \\ (-12,1) \\ \end{matrix} \sim \begin{bmatrix} 0 & 0 & 1 & -2 & 0 \\ 1 & 0 & 1 & 2 & 0 \\ 0 & 1 & -1 & -2 & 0 \\ 0 & 0 & 0 & 0 & 3 \end{bmatrix} \begin{matrix} \\ \\ (-1,1,2) \\ (1,1,3) \\ (-8,4) \end{matrix} \sim$$

$$\sim \begin{bmatrix} 0 & 0 & 1 & -2 & 0 \\ 1 & 0 & 0 & 4 & 0 \\ 0 & 1 & 0 & -4 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{matrix} \\ \\ (1/2) \\ (2/3) \\ \end{matrix} \sim \begin{bmatrix} 1 & 0 & 0 & 4 & 0 \\ 0 & 1 & 0 & -4 & 0 \\ 0 & 0 & 1 & -2 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

Odtud plyne $c_1 = -4c_4$, $c_2 = 4c_4$, $c_3 = 2c_4$, $c_5 = 0$, tj $\boldsymbol{c} = c_4(-4, 4, 2, 1, 0)$, zvolme

$$\boldsymbol{c} = (-4, 4, 2, 1, 0).$$

3. fáze algoritmu. Podle Věty 142 vypočteme v $\mathbb{Z}_{25}$ hodnoty „skalárních součinů“

$$\begin{aligned} s &= (14, 2, 9, 1, 3) \bullet (-4, 4, 2, 1, 0) = -29 = 21, \\ t &= (7, 16, 9, 7, 11) \bullet (-4, 4, 2, 1, 0) = 61 = 11, \end{aligned}$$

odtud podle téže věty platí v grupě $\mathbb{Z}^*_{401}$

$$5^{21} \cdot 88^{11} = 1.$$

Protože $\gcd(11, 25) = 1$, jedná se o netriviální reprezentaci prvku 1 vzhledem ke generátoru 5 a prvku 88, která umožňuje vypočítat $\mathrm{dlog}_5 88$ jako jediné řešení rovnice $21 + 11 \cdot \mathrm{dlog}_5 88 = 0 \Leftrightarrow 11 \cdot \mathrm{dlog}_5 88 = 4$ v $\mathbb{Z}_{25}$. Vynásobením rovnice prvkem 11^{-1} v $\mathbb{Z}^*_{25}$ dostaneme

$$\mathrm{dlog}_5 88 = -9 \cdot 4 = 14.$$

2. fáze algoritmu. **(modrý výběr).** V okruhu $\mathbb{Z}_{25}$ řešíme homogenní soustavu rovnic pro neznámý vektor $\boldsymbol{c} = (c_1, ..., c_5) \in \mathbb{Z}^5_{25}$ s maticí soustavy tvořenou sloupcovými vektory $\boldsymbol{e}_i = (e_{1i}, e_{2i}, e_{3i}, e_{4i})$, $i \in \{1, ..., 5\}$. Dostaneme:

$$\begin{bmatrix} 5 & 0 & 0 & 0 & 1 \\ 0 & 4 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 2 \\ 0 & 0 & 1 & 0 & 1 \end{bmatrix} \begin{matrix} \\ (-5,3,1) \\ (-6,2) \\ \\ \end{matrix} \sim \begin{bmatrix} 0 & 0 & -5 & -5 & -9 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 2 \\ 0 & 0 & 1 & 0 & 1 \end{bmatrix} \begin{matrix} \\ \\ (-1,4,3) \\ (5,4,1) \\ \end{matrix} \sim \begin{bmatrix} 0 & 0 & 0 & -5 & -4 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{bmatrix} \begin{matrix} \\ (1/3) \\ (3/4) \\ (-1,4) \end{matrix} \sim$$

$$\sim \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 5 & 4 \end{bmatrix} \begin{matrix} \\ \\ \\ (6,4,3) \\ (6,4,1) \end{matrix} \sim \begin{bmatrix} 1 & 0 & 0 & 6 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 5 & 0 \\ 0 & 0 & 0 & 5 & 4 \end{bmatrix} \begin{matrix} \\ \\ \\ \\ (-6,4) \end{matrix} \sim \begin{bmatrix} 1 & 0 & 0 & 6 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 5 & 0 \\ 0 & 0 & 0 & -5 & 1 \end{bmatrix}.$$

Odtud plyne $c_1 = -6c_4, c_2 = 0,\ c_3 = -5c_4,\ c_5 = 5c_4$, tj $\boldsymbol{c} = c_4(-6, 0, -5, 1, 5)$, zvolme

$$\boldsymbol{c} = (-6, 0, -5, 1, 5).$$

3. fáze algoritmu. Podle Věty 142 vypočteme v $\mathbb{Z}_{25}$ hodnoty „skalárních součinů“

$$\begin{aligned} s &= (16, 20, 6, 2, 23) \bullet (-6, 0, -5, 1, 5) = -9 = 16, \\ t &= (5, 2, 9, 16, 15) \bullet (-6, 0, -5, 1, 5) = 56 = 6, \end{aligned}$$

odtud podle téže věty platí v grupě $\mathbb{Z}^*_{401}$

$$5^{16} \cdot 88^6 = 1.$$

Protože $\gcd(6, 25) = 1$, jedná se o netriviální reprezentaci prvku 1 vzhledem ke generátoru 5 a prvku 88, která umožňuje vypočítat $\mathrm{dlog}_5 88$ jako jediné řešení rovnice $16 + 6 \cdot \mathrm{dlog}_5 88 = 0$ v $\mathbb{Z}_{25}$. Vynásobením rovnice prvkem 6^{-1} v $\mathbb{Z}^*_{25}$ dostaneme

$$\mathrm{dlog}_5 88 = -4 \cdot (-16) = 14.$$

Faktorizace

Věta 147. *Nechť $k \in \mathbb{N}^+$, $p_1, ..., p_k$ jsou po dvou různá prvočísla, $n \in \mathbb{N}$, $n \geq 3$, a existují posloupnosti*

$$\begin{aligned} \alpha : \{1, ..., k+1\} &\to \mathbb{Z}^*_n, \\ e_1, ..., e_k : \{1, ..., k+1\} &\to \mathbb{N}, \end{aligned}$$

pro které platí

$$(\alpha_i^2)_n = p_1^{e_{1i}} \cdot ... \cdot p_k^{e_{ki}},\ pro\ i \in \{1, .., k+1\}. \tag{17}$$

Pak existuje v okruhu $\mathbb{Z}$ vektor $(\lambda_1, ..., \lambda_k) \in \mathbb{Z}^k$ a nenulový vektor $\mathbf{0} \neq (c_1, ..., c_{k+1}) \in \mathbb{Z}^{k+1}$, které v okruhu $\mathbb{Z}$ vyhovují soustavě

$$\begin{bmatrix} e_{11} & \cdots & e_{1,k+1} \\ \vdots & & \vdots \\ e_{k1} & \cdots & e_{k,k+1} \end{bmatrix} \cdot \begin{bmatrix} c_1 \\ \vdots \\ c_{k+1} \end{bmatrix} = 2 \cdot \begin{bmatrix} \lambda_1 \\ \vdots \\ \lambda_k \end{bmatrix}, \tag{18}$$

a v $\mathbb{Z}^*_n$ platí

$$\alpha^2 = \beta^2,$$

kde

$$\alpha = \alpha_1^{c_1} \cdot ... \cdot \alpha_{k+1}^{c_{k+1}},\ \beta = p_1^{\lambda_1} \cdot ... \cdot p_k^{\lambda_k}, \tag{19}$$

operace v rovnici (19) jsou operacemi v okruhu $\mathbb{Z}^*_n$.
Jestliže v okruhu $\mathbb{Z}_n$ navíc platí $\alpha - \beta \neq 0$ a $\alpha + \beta \neq 0$, potom $\gcd(\alpha - \beta, n)$, $\gcd(\alpha + \beta, n)$ jsou netriviální dělitelé čísla n.

Příklad 148. Proveďte faktorizaci čísla $n = 143$ metodou SEF („sub exponenciální faktorizace“, tj. s využitím poznatků Věty 147).

0. fáze: Vybereme prvočísla $p_1, p_2, p_3, p_4 := 2, 3, 5, 7$, tj. $k = 4$. Prvočísla musí být dostatečně malá, aby vyhledání exponentů jejich postupným dělením bylo rychlé, zároveň žádné z prvočísel nesmí být dělitel čísla n, protože hodnota levé strany rovnice (17) je nesoudělná s n, prvek α_i^2 je totiž prvkem $\mathbb{Z}_n^*$.

1. fáze: Pro index $i \in \{1, ..., k+1\} = \{1, 2, 3, 4, 5\}$ vybereme náhodně prvek $[\alpha_i]_n \in \mathbb{Z}_n^*$, vypočteme $(\alpha_i^2)_n$ a stanovíme jeho rozklad

$$(\alpha_i^2)_n = p_1^{e_{1i}} \cdot ... \cdot p_k^{e_{ki}},$$

tj. exponenty $e_{1i}, ..., e_{ki}$. Pokud takové exponenty neexistují, opakujeme náhodný výběr prvku $[\alpha_i]_n \in \mathbb{Z}_n^*$. V následující tabulce jsou uvedeny výsledky pro $n = 143$ získané v prostředí algebraického systému Maple.

i	α	$(\alpha^2)_n$	e_1	e_2	e_3	e_4	pokus č.
1	41	108	2	3	0	0	1
2	42	48	4	1	0	0	2
3	17	3	0	1	0	0	3
4	85	75	0	1	2	0	4
5	30	42	1	1	0	1	9

Tabulka 13: Konkrétní realizace SEF

2. fáze: Nalezneme vektory $(c_1, ..., c_5) \in \mathbb{Z}^5$, $(\lambda_1, ..., \lambda_4) \in \mathbb{Z}^4$, takové, že $(c_1, ..., c_5) \neq \mathbf{0}$, a platí

$$\begin{bmatrix} 2 & 4 & 0 & 0 & 1 \\ 3 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} c_1 \\ c_2 \\ c_3 \\ c_4 \\ c_5 \end{bmatrix} = 2 \cdot \begin{bmatrix} \lambda_1 \\ \lambda_2 \\ \lambda_3 \\ \lambda_4 \end{bmatrix}. \tag{20}$$

Hledané vektory nalezneme řešením soustavy (20) v tělese $\mathbb{Z}_2$, ve které je soustava (20) tvaru

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} c_1 \\ c_2 \\ c_3 \\ c_4 \\ c_5 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}.$$

Stačí vybrat nějaké nenulové řešení $\boldsymbol{c}$ v tělese $\mathbb{Z}_2$, například $\boldsymbol{c} = (c_1, c_2, c_3, c_4, c_5) = (1, 1, 1, 1, 0)$.

Odtud dostaneme řešení soustavy (20)

$$\begin{bmatrix} 2 & 4 & 0 & 0 & 1 \\ 3 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 0 \end{bmatrix} = 2 \cdot \begin{bmatrix} 3 \\ 3 \\ 1 \\ 0 \end{bmatrix},$$

tedy pro vektor $\boldsymbol{\lambda}$ platí $\boldsymbol{\lambda} = (3, 3, 1, 0)$.

3. fáze: Kompletace výsledků. Podle Věty 147 v okruhu $\mathbb{Z}_n$, $n = 143$, vypočteme

$$\begin{aligned} \alpha &= \prod_{i=1}^{k+1} \alpha_i^{c_i} = 41^1 \cdot 42^1 \cdot 17^1 \cdot 85^1 \cdot 30^0 = 90, \\ \beta &= \prod_{i=1}^{k} p_i^{\lambda_i} = 2^3 \cdot 3^3 \cdot 5^1 \cdot 7^0 = 79. \end{aligned}$$

Dále podle téže věty v okruhu $\mathbb{Z}_n$ platí

$$\alpha^2 = \beta^2 \leftrightarrow (\alpha - \beta)(\alpha + \beta) = 0,$$

odtud dostaneme $(90 - 79)(90 + 79) = 0 \leftrightarrow 11 \cdot 26 = 0$. Dostali jsme v okruhu $\mathbb{Z}_n$ dělitele nuly, proto nutně $\gcd(11, 143) = 11$, $\gcd(26, 143) = 13$, jsou (netriviální) dělitelé 143.

$$143 = 11 \cdot 13.$$

Příklad 149. Metodou SEF proveďte faktorizaci $n = 7007$.

0. fáze: Vybereme prvočísla $p_1, p_2, p_3 := 2, 3, 5$, tj. $k = 3$. Dělením se přesvědčíme, že vybraná prvočísla nejsou děliteli čísla $n = 7007$.
1. fáze: Pro index $i \in \{1, ..., k + 1\} = \{1, 2, 3, 4\}$ vybereme náhodně prvek $[\alpha_i]_n \in \mathbb{Z}_n^*$, vypočteme $(\alpha_i^2)_n$ a stanovíme jeho rozklad

$$(\alpha_i^2)_n = p_1^{e_{1i}} \cdot ... \cdot p_k^{e_{ki}},$$

tj. exponenty $e_{1i}, ..., e_{ki}$. Pokud takové exponenty neexistují, opakujeme náhodný výběr prvku $[\alpha_i]_n \in \mathbb{Z}_n^*$. V následující tabulce jsou uvedeny výsledky pro $n = 7007$ získané v prostředí algebraického systému Maple.

i	α	$(\alpha^2)_n$	e_1	e_2	e_3	pokus č.
1	1896	225	0	2	2	23
2	5787	2916	2	6	0	27
3	4107	1600	6	0	2	30
4	2745	2500	2	0	4	72

Tabulka 14: Konkrétní realizace SEF

2. fáze: Nalezneme vektory $(c_1, ..., c_4) \in \mathbb{Z}^4$, $(\lambda_1, ..., \lambda_3) \in \mathbb{Z}^3$, takové, že $(c_1, ..., c_4) \neq \mathbf{0}$, a platí

$$\begin{bmatrix} 0 & 2 & 6 & 2 \\ 2 & 6 & 0 & 0 \\ 2 & 0 & 2 & 4 \end{bmatrix} \cdot \begin{bmatrix} c_1 \\ c_2 \\ c_3 \\ c_4 \end{bmatrix} = 2 \cdot \begin{bmatrix} \lambda_1 \\ \lambda_2 \\ \lambda_3 \end{bmatrix}. \tag{21}$$

Hledané vektory nalezneme řešením soustavy (21) v tělese $\mathbb{Z}_2$, ve které je soustava (21) tvaru

$$\begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} c_1 \\ c_2 \\ c_3 \\ c_4 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}.$$

Stačí vybrat nějaké nenulové řešení $\boldsymbol{c}$ v tělese $\mathbb{Z}_2$, například $\boldsymbol{c} = (c_1, c_2, c_3, c_4) = (1, 0, 1, 0)$. Odtud dostaneme řešení soustavy (21)

$$\begin{bmatrix} 0 & 2 & 6 & 2 \\ 2 & 6 & 0 & 0 \\ 2 & 0 & 2 & 4 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \end{bmatrix} = 2 \cdot \begin{bmatrix} 3 \\ 1 \\ 2 \end{bmatrix},$$

tedy pro vektor $\boldsymbol{\lambda}$ platí $\boldsymbol{\lambda} = (3, 1, 2)$.

3. fáze: Kompletace výsledků. Podle Věty 147 v okruhu $\mathbb{Z}_n$, $n = 7007$, vypočteme

$$\begin{aligned} \alpha &= \prod_{i=1}^{k+1} \alpha_i^{c_i} = 1896^1 \cdot 5787^0 \cdot 4107^1 \cdot 2745^0 = 2095, \\ \beta &= \prod_{i=1}^{k} p_i^{\lambda_i} = 2^3 \cdot 3^1 \cdot 5^2 = 600. \end{aligned}$$

Odtud dále platí v okruhu $\mathbb{Z}_{7007}$

$$(\alpha - \beta)(\alpha + \beta) = 1495 \cdot 2695 = 0,$$

tj. $\gcd(1495, 7007) = 13$, $\gcd(2695, 7007) = 539$ jsou dělitelé čísla 7007.

Například podle Rabinova–Millerova testu není 539 prvočíslo, můžeme podobným způsobem pokračovat v jeho faktorizaci.

Příklad 150. Faktorizujte číslo $n = 1711343$ metodou SEF.

0. fáze: Vybereme prvočísla $p_1, p_2, p_3, p_4 := 2, 3, 5, 7$, tj. $k = 4$. Dělením se přesvědčíme, že vybraná prvočísla nejsou děliteli čísla $n = 1711343$.
1. fáze: Pro index $i \in \{1, ..., k+1\} = \{1, 2, 3, 4, 5\}$ vybereme náhodně prvek $[\alpha_i]_n \in \mathbb{Z}_n^*$, vypočteme $(\alpha_i^2)_n$ a stanovíme jeho rozklad

$$(\alpha_i^2)_n = p_1^{e_{1i}} \cdot ... \cdot p_k^{e_{ki}},$$

tj. exponenty $e_{1i}, ..., e_{ki}$. Pokud takové exponenty neexistují, opakujeme náhodný výběr prvku $[\alpha_i]_n \in \mathbb{Z}_n^*$. V následující tabulce jsou uvedeny výsledky pro $n = 1711343$ získané v prostředí algebraického systému Maple.

i	α	$(\alpha^2)_n$	e_1	e_2	e_3	e_4	pokus č.
1	1392457	279936	7	7	0	0	161
2	475698	1125000	3	2	6	0	387
3	1711215	16384	14	0	0	0	726
4	1474739	600	3	1	2	0	967
5	350	122500	2	0	4	2	1074

Tabulka 15: Konkrétní realizace SEF

2. fáze: Nalezneme vektory $(c_1, ..., c_5) \in \mathbb{Z}^5$, $(\lambda_1, ..., \lambda_4) \in \mathbb{Z}^4$, takové, že $(c_1, ..., c_5) \neq \mathbf{0}$, a platí

$$\begin{bmatrix} 7 & 3 & 14 & 3 & 2 \\ 7 & 2 & 0 & 1 & 0 \\ 0 & 6 & 0 & 2 & 4 \\ 0 & 0 & 0 & 0 & 2 \end{bmatrix} \cdot \begin{bmatrix} c_1 \\ c_2 \\ c_3 \\ c_4 \\ c_5 \end{bmatrix} = 2 \cdot \begin{bmatrix} \lambda_1 \\ \lambda_2 \\ \lambda_3 \\ \lambda_4 \end{bmatrix}. \tag{22}$$

Hledané vektory nalezneme řešením soustavy (22) v tělese $\mathbb{Z}_2$, ve kterém je soustava (22) tvaru

$$\begin{bmatrix} 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} c_1 \\ c_2 \\ c_3 \\ c_4 \\ c_5 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}.$$

Gaussova eliminace v tělese $\mathbb{Z}_2$ dává

$$\begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} c_1 \\ c_2 \\ c_3 \\ c_4 \\ c_5 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \tag{23}$$

odtud v $\mathbb{Z}_2$ $c_2 = 0$, $c_1 = c_4$. Stačí vybrat nějaké nenulové řešení $\boldsymbol{c}$ v tělese $\mathbb{Z}_2$, které splňuje uvedené podmínky, například $\boldsymbol{c} = (c_1, c_2, c_3, c_4, c_5) = (1, 0, 0, 1, 0)$. Odtud dostaneme řešení soustavy (22)

$$\begin{bmatrix} 7 & 3 & 14 & 3 & 2 \\ 7 & 2 & 0 & 1 & 0 \\ 0 & 6 & 0 & 2 & 4 \\ 0 & 0 & 0 & 0 & 2 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = 2 \cdot \begin{bmatrix} 5 \\ 4 \\ 1 \\ 0 \end{bmatrix}.$$

tedy pro vektor $\boldsymbol{\lambda}$ platí $\boldsymbol{\lambda} = (5, 4, 1, 0)$.

3. fáze: Kompletace výsledků. Podle Věty 147 v okruhu $\mathbb{Z}_n$, $n = 1711343$, vypočteme

$$\begin{aligned} \alpha &= \prod_{i=1}^{k+1} \alpha_i^{c_i} = 1392457^1 \cdot 475698^0 \cdot 1711215^0 \cdot 1474739^1 \cdot 350^0 = 12960, \\ \beta &= \prod_{i=1}^{k} p_i^{\lambda_i} = 2^5 \cdot 3^4 \cdot 5^1 \cdot 7^0 = 12960. \end{aligned}$$

Nalezli jsme řešení, které sice splňuje tvrzení Věty 147 $\alpha^2 = \beta^2$, avšak $\alpha - \beta = 0$, tedy $\alpha - \beta \notin \mathrm{div}_0(\mathbb{Z}_n)$, stejně tak se dá ukázat, že $\alpha + \beta \notin \mathrm{div}_0(\mathbb{Z}_n)$. Toto řešení nevede na faktor čísla n.
Dá se ukázat, že žádné řešení soustavy (23) nevede na hodnoty α, β, pro které by $\alpha - \beta, \alpha + \beta \in \mathrm{div}_0(\mathbb{Z}_n)$. Například:

2. fáze-a: Vyberme jiné řešení soustavy (23), nechť například $\boldsymbol{c} = (c_1, c_2, c_3, c_4, c_5) = (1, 0, 0, 1, 1)$. Odtud dostaneme řešení soustavy (22)

$$\begin{bmatrix} 7 & 3 & 14 & 3 & 2 \\ 7 & 2 & 0 & 1 & 0 \\ 0 & 6 & 0 & 2 & 4 \\ 0 & 0 & 0 & 0 & 2 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 1 \end{bmatrix} = 2 \cdot \begin{bmatrix} 6 \\ 4 \\ 3 \\ 1 \end{bmatrix}.$$

tedy pro vektor $\boldsymbol{\lambda}$ platí $\boldsymbol{\lambda} = (6, 4, 3, 1)$.

3. fázea: Kompletace výsledků. Podle Věty 147 v okruhu $\mathbb{Z}_n$, $n = 1711343$, vypočteme

$$\begin{aligned} \alpha &= \prod_{i=1}^{k+1} \alpha_i^{c_i} = 1392457^1 \cdot 475698^0 \cdot 1711215^0 \cdot 1474739^1 \cdot 350^1 = 1113314, \\ \beta &= \prod_{i=1}^{k} p_i^{\lambda_i} = 2^6 \cdot 3^4 \cdot 5^3 \cdot 7^1 = 1113314. \end{aligned}$$

Opět neúspěch. Je třeba spočítat jiné hodnoty v tabulce realizací algoritmu SEF.

Příklad 151. Faktorizujte číslo $n = 1711343$ metodou SEF. Stejné zadání jako v předchozím příkladu, jiná tabulka náhodných výběrů $[\alpha_i]_n \in \mathbb{Z}_n^*$.

0. fáze: Vybereme prvočísla $p_1, p_2, p_3, p_4 := 2, 3, 5, 7$, tj. $k = 4$. Dělením se přesvědčíme, že vybraná prvočísla nejsou děliteli čísla $n = 1711343$.
1. fáze: Pro index $i \in \{1, ..., k+1\} = \{1, 2, 3, 4, 5\}$ vybereme náhodně prvek $[\alpha_i]_n \in \mathbb{Z}_n^*$, vypočteme $(\alpha_i^2)_n$ a stanovíme jeho rozklad

$$(\alpha_i^2)_n = p_1^{e_{1i}} \cdot ... \cdot p_k^{e_{ki}},$$

tj. exponenty $e_{1i}, ..., e_{ki}$. Pokud takové exponenty neexistují, opakujeme náhodný výběr prvku $[\alpha_i]_n \in \mathbb{Z}_n^*$. V následující tabulce jsou uvedeny výsledky pro $n = 1711343$ získané v prostředí algebraického systému Maple.

i	α	$(\alpha^2)_n$	e_1	e_2	e_3	e_4	pokus č.
1	950049	27	0	3	0	0	147
2	1346916	1687500	2	3	6	0	737
3	1710447	802816	14	0	0	2	1176
4	128489	97200	4	5	2	0	1589
5	1309394	240000	7	1	4	0	1673
6	1082300	78732	2	9	0	0	2102
7	888298	460992	6	1	0	4	2386
8	1634237	129654	1	3	0	4	3132
9	405695	20000	5	0	4	0	3504
10	1058519	5000	3	0	4	0	4166

Tabulka 16: Konkrétní realizace SEF

2. fáze: Vyberme prvních 5 řádků tabulky. Nalezneme vektory $(c_1, ..., c_5) \in \mathbb{Z}^5$, $(\lambda_1, ..., \lambda_4) \in \mathbb{Z}^4$, takové, že $(c_1, ..., c_5) \neq \mathbf{0}$, a platí

$$\begin{bmatrix} 0 & 2 & 14 & 4 & 7 \\ 3 & 3 & 0 & 5 & 1 \\ 0 & 6 & 0 & 2 & 4 \\ 0 & 0 & 2 & 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} c_1 \\ c_2 \\ c_3 \\ c_4 \\ c_5 \end{bmatrix} = 2 \cdot \begin{bmatrix} \lambda_1 \\ \lambda_2 \\ \lambda_3 \\ \lambda_4 \end{bmatrix}. \tag{24}$$

Hledané vektory nalezneme řešením soustavy (24) v tělese $\mathbb{Z}_2$, ve kterém je soustava (24) tvaru

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} c_1 \\ c_2 \\ c_3 \\ c_4 \\ c_5 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}.$$

Gaussova eliminace v tělese $\mathbb{Z}_2$ dává

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} c_1 \\ c_2 \\ c_3 \\ c_4 \\ c_5 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \tag{25}$$

odtud v $\mathbb{Z}_2$ $c_5 = 0$, $c_1 + c_2 + c_4 = 0$. Stačí vybrat nějaké nenulové řešení $\boldsymbol{c}$ v tělese $\mathbb{Z}_2$, které vyhovuje uvedeným podmínkám, například $\boldsymbol{c} = (c_1, c_2, c_3, c_4, c_5) = (1, 0, 0, 1, 0)$. Odtud

dostaneme řešení soustavy (24)

$$\begin{bmatrix} 0 & 2 & 14 & 4 & 7 \\ 3 & 3 & 0 & 5 & 1 \\ 0 & 6 & 0 & 2 & 4 \\ 0 & 0 & 2 & 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = 2 \cdot \begin{bmatrix} 2 \\ 4 \\ 1 \\ 0 \end{bmatrix}.$$

tedy pro vektor $\boldsymbol{\lambda}$ platí $\boldsymbol{\lambda} = (2, 4, 1, 0)$.

3. fáze: Kompletace výsledků. Podle Věty 147 v okruhu $\mathbb{Z}_n$, $n = 1711343$, vypočteme

$$\begin{aligned} \alpha &= \prod_{i=1}^{k+1} \alpha_i^{c_i} = 950049^1 \cdot 1346916^0 \cdot 1710447^0 \cdot 128489^1 \cdot 1309394^0 = 749771, \\ \beta &= \prod_{i=1}^{k} p_i^{\lambda_i} = 2^2 \cdot 3^4 \cdot 5^1 \cdot 7^0 = 1620. \end{aligned}$$

Nalezli jsme řešení, které splňuje tvrzení Věty 147 $\alpha^2 = \beta^2$, zároveň $\alpha - \beta \neq 0$, $\alpha + \beta \neq 0$, tedy $\alpha - \beta$, $\alpha + \beta \in \mathrm{div}_0(\mathbb{Z}_n)$. Odtud plyne, že $\gcd(\alpha - \beta, n)$, $\gcd(\alpha + \beta, n)$, jsou netriviální dělitelé čísla n. Dostaneme

$$\begin{aligned} \gcd(\alpha - \beta, n) &= \gcd(748151, 1711343) = 599, \\ \gcd(\alpha + \beta, n) &= \gcd(751391, 1711343) = 2857. \end{aligned}$$

$599 \cdot 2857 = 1711343$. Rozklad byl nalezen.