

$$\begin{aligned}
 \text{komplesace: } & 16^{26} \cdot 54^{87} \cdot 208 = 480 \cdot 351 \cdot 208 = 208 \\
 & 16^{26} \cdot 54^{87} = 1 \\
 & 16^{26} \cdot (16^x)^{87} = 16^0 \quad x = -26 \cdot 87^{-1} = -26 \cdot 73 = -1898 = 7 \in \mathbb{Z}_{127} \\
 & 26 + 87x = 0 \\
 & x = -26 \cdot 87^{-1} \quad 16^7 = 54 \vee \text{dlog}_{16}(54) = 7
 \end{aligned}$$

Přednáška Algoritmus kvadratického říta (QSF)

22.5.2019

- umožní uživatelům řídat čísla pro SEF

- zavádí parametr říta z

$$y, z = e^{\ln(n)^{\frac{1}{2} + \alpha(i)}} \doteq e^{\sqrt{\ln(n)}}$$

- když je n v 1. fázii SEF volili $a_i < \sqrt{n}$, tak $a_i^2 < n$, modulos jsme neváili a najdeme jen binomický \sqrt{n} . Poté chceme volit $a_i > \sqrt{n}$.

- budeme vybrat čísla z intervalu $(\sqrt{n}, \sqrt{n} + z)$

$$\text{Okračujeme } m = \lfloor \sqrt{n} \rfloor$$

$$F(x) = (m+x)^2 - n$$

Při $s \leq z < 1$, $z >$ platí díky předpokladu rovnosti:

$$1 \leq F(s) \leq z^2 + 2z\sqrt{n} = n^{\frac{1}{2}} + o(n)$$

$F(s)$ je obytek po vydělení čísla $(s+m)^2$ číslem n , tedy $F(s)$ je číverec. $\in \mathbb{Z}_n$.

- jak svolit z , abychom měli dostatek y -hladkých číverců?

G je pravidelnost, že číslo s intervalu (\sqrt{n}, n) je y -hladké

k nálezení y -hladkého číverce poslouhíme $1/y$ čísel, proto máslarne $z = \frac{k}{y}$

- uvoříme jich V délky Lz , s hodnotami: $V[s] = F(s)$

- párky budou postupně dělit prvočísky do s , ale jen ty, které dělítelné jsou

$p/F(s)$, právě když $F(s) = 0 \pmod{p}$, což je právě když s je kořenem $F(x) \pmod{p}$

kvadratický polynom $F(x) = (x+m)^2 - n$ může mít dva kořeny: s_1 a s_2 .

Prvočísem p jsou dělítelná právě ta $F(s)$. Zde $s = s_1 + l \cdot p$, kde $l \in \mathbb{N}$.

\Rightarrow budu dělit: $F(s_1), F(s_2), F(s_1 + p), F(s_2 + p), F(s_1 + 2p), \dots$

shuk o p

Nynější výsledek ovlivňuje časové složitosti QSF.

Přednáška Příklad: Faktorizujte $n=403$ s parametry $y=8, z=8$. Nudítejte algoritmus procedury

23.5.2019

$$m = \lfloor \sqrt{n} \rfloor = \lfloor \sqrt{403} \rfloor = 20$$

$$F(x) = (x+20)^2 - 403 \in \mathbb{Z}$$

i	1	2	3	4	5	6	7	8
V	38	81	126	173	222	273	326	381

$$F(1) = 21^2 - 403 = 38$$

$$F(2) = 22^2 - 403 = 81$$

pozn: n je poměrně malé a parametr z je moc velký, proto máme $F(8)$ výše a lehčí

n a nedostal se hned u \sqrt{n} , jak jsme čekali.

Jde o řízenou dělit prvočísky: $p=2$

Jak vypadá $F(x) \pmod{2}$?

$$(x+0)^2 - 1 = 0$$

$$x^2 = 1 \rightarrow s = \pm 1 = 1 \pmod{2}$$

$$2 | F(1+2k), \text{ kde } i \in \{1, 3, 5, 7\}$$

i	①	2	③	4	⑤	6	⑦	8
V	19	81	63	173	111	273	163	381
D	2	2	2	2	2	2	2	2

$$p=3: F(x) = (x+2)^2 - 1 = 0$$

$$(x+2)^2 = 1 \rightarrow s = -2 \pm 1 = \begin{cases} -1 = 2 \\ -3 = 0 \end{cases}$$

$$3 | F(3k+2)$$

$$3 | F(3k)$$

i	1	2	3	4	5	6	7	8
V	19	1	7	173	37	91	163	127
D	2	3	2,3	2,3	3	2	3	3

$$p=5: F(x) = (x+0)^2 - 3 \quad \text{Zkoušíme Eulerovo kritérium: } 3^{\frac{p-1}{2}} = 3^{\frac{4}{2}} = 9 = -1 \in \mathbb{Z}_5$$

$$\begin{array}{l} x^2 - 3 = 0 \\ x^2 = 3 \end{array} \quad \Rightarrow 3 \text{ je nečtvrtcec, proto } F(x) \text{ nikdy není čtělitelné } \forall x$$

$$p=7: \quad F(x) = (x + (-1))^2 - 4 = 0 \quad s = \pm 2 + 1 = \begin{cases} 3 \\ -1 = 6 \end{cases} \quad \begin{array}{l} 7/F(7k+3) \\ 7/F(7k+6) \end{array}$$

$$\text{Ansatz: } (x-1)^2 = 4$$

$$x-1 = \pm 2$$

i	1	2	3	4	5	6	7	8
V	19	1	1	173	37	13	163	127
D	2	3 ⁴	2·3 ² ·7	—	2·3	3·7	2	3

← y-hladká jsou lačná, která m mají 1

ažli jsme dvě y-fložka čísla, a to $F(2) = 81$ a $F(3) = 126$, a k nim přísluší vektory exponencií $v_1 = (0, 4, 0, 0)$ a $v_2 = (1, 2, 0, 1)$. Po faktorisaci ale těchto vektorů získáme 5. To by se normálně řešilo tak, že sestavíme tabulku o $z(8)$, doplníť ji se hodnoty V a skuru se němu dělit. Tady však bohužel nevíme, protože $F(9) > 403$, a tím rázem vše lyčkou reprezentovali se abyskem.

Jak na hledání kořenů v \mathbb{Z}_p ?

$$F(x) = (x+m)^2 - n = 0$$

$$(x+m)^2 = n$$

- je n'achèverais ?

- do overtime Eulerovým kritériem: musí být $n^{\frac{1}{2}} = 1 \approx Z_p$

- jak najit FN a Zp?

$$\text{- už víme, že } n^{\frac{p-2}{2}} = 1, \text{ vypočítejme ho na obou stranách: } h: \\ n^{\frac{p-1}{2}+1} = n \quad (n^{\frac{p-1}{2}+1} = n^{\frac{p-1}{2} + \frac{2}{2}} = n^{\frac{p-1+2}{2}} = n^{\frac{p+1}{2}})$$

- pokud je $\frac{p+1}{2}$ sude, pak $\pm \sqrt{\frac{p+1}{4}} = a$, tedy $a^2 = n$

- pokud je $\frac{p+1}{2}$ sude, pak $\exists h \in \mathbb{Z} : h^2 = a$, tedy $a = h^2$.
- pokud předchozí postup vše, tj. $\frac{p+1}{2}$ je liché, je na to slovíčko alg., který vyscháme

Příklad: \mathbb{Z}_{101}^* , má podgrupu $G = \langle 16 \rangle$ řádu 25, $b = 25$, $b \in G$. Vypočítejte dlog₁₆(25) Crišoník
 a \mathbb{Z}_8^* , avolej $y = 8$. $\varphi(101) = 100 = 2^2 \cdot 5^2$, $P = \{2, 3, 5, 7\}$ 23.5.2019

1. fáce: $a = 16$, $b = 25$, hledáme $a^{\pm} \cdot b^{\pm} \cdot h$, aby bylo y-hodnota $\pm 16^{\pm} 25^{\pm} \cdot h$
 $|H| = 4$, pokud jiný nejednoduchší prvek je H, abych vedená, jak H vypadá
 $a^{\pm} \cdot b^{\pm}$ mohlo být v H, abrem $3^{25} \times 2^{10} = 10 \Rightarrow H = \{ \pm 1, \pm 10 \}$

$$\begin{aligned} i=1: & \quad 16^{20} \cdot 25^{11} \cdot (-10) = 66 \times \\ & 16^5 \cdot 25^9 \cdot 1 = 97 \times \\ & 16^{14} \cdot 25^{14} \cdot (-1) = 21 = 3 \cdot 7 \quad \checkmark \\ & 16^7 \cdot 25^{13} \cdot 1 = 1 \end{aligned}$$

Holle je is Zio!

$$v_1 = (0, 1, 0, 1)$$

$$v_2 = (0, 1, 0, 0)$$

$$n_3 = (2, 0, 2, 0)$$

$$v_4 = \begin{pmatrix} 1, 3, 0, 0 \\ 0, 0 \end{pmatrix}$$

$$v_5 = (0, 0, 1, 1)$$

2. face: while je w \mathbb{Z}_{25} !

$$\text{Gauß: } \text{reduz. je nach } \mathbb{Z}_{25}. \quad -25$$

$$\left(\begin{array}{ccccc} 0 & 0 & 2 & 1 & 0 \end{array} \right) \sim R_4 \left(\begin{array}{ccccc} 1 & 0 & 0 & 0 & 1 \end{array} \right) \sim R_1 \quad | \quad 1$$

$$\left(\begin{array}{ccccc} 1 & 1 & 0 & 3 & 0 \end{array} \right) \sim R_2 - R_4 \left(\begin{array}{ccccc} 0 & 1 & 0 & 3 & -1 \end{array} \right) \sim R_2 \quad | \quad 0$$

$$\left(\begin{array}{ccccc} 0 & 0 & 2 & 0 & 1 \end{array} \right) \sim R_3 \left(\begin{array}{ccccc} 0 & 0 & 1 & 0 & 1 \end{array} \right) \sim 12R_3 \quad | \quad 0$$

$$\left(\begin{array}{ccccc} 1 & 0 & 0 & 0 & 1 \end{array} \right) \sim R_1 - R_3 \left(\begin{array}{ccccc} 0 & 0 & 0 & 1 & -1 \end{array} \right) \sim R_4 \quad | \quad 0$$

$$\left(\begin{array}{c|ccccc} 0 & 1 & R_1 & 1 & 0 & 0 & 0 & 1 \\ 0 & -1 & R_2 - 3R_4 & 0 & 1 & 0 & 0 & 2 \\ 0 & 13 & R_3 & 0 & 0 & 1 & 0 & 13 \\ 0 & -1 & R_4 & 0 & 0 & 0 & 1 & -1 \end{array} \right) \rightsquigarrow$$

$$S = \sum c_i \cdot s_i = -14 - 14 + 12 + 20 + 4 = 8$$

$\} \in \mathbb{Z}_{25}$

$$+ = 8, \quad - + = -14, \quad -34 + 24 + 11 + 4 = -9 = 10$$

$$p=5: F(x) = (x+0)^2 - 3 \quad \text{Ukážme Eulerovo kritérium: } 3^{\frac{p-1}{2}} = 3^{\frac{4}{2}} = 9 = -1 \text{ v } \mathbb{Z}_5$$

$$\sim \mathbb{Z}_5 \quad x^2 - 3 = 0 \quad \Rightarrow 3 \text{ je nečtvrtceč, proto } F(x) \text{ nikdy nemůže být dělitelné } p^2$$

$$x^2 = 3$$

$$p=7: F(x) = (x+(-1))^2 - 4 = 0 \quad s = \pm 2 + 1 = \begin{cases} 3 \\ -1 = 6 \end{cases} \quad \begin{matrix} 7/F(7k+3) \\ 7/F(7k+6) \end{matrix}$$

$$\sim \mathbb{Z}_7 \quad (x-1)^2 = 4 \quad x-1 = \pm 2$$

i	1	2	3	4	5	6	7	8
V	19	1	1	173	37	13	163	127
D	2	34	$2 \cdot 3^2 \cdot 7$	-	$2 \cdot 3$	$3 \cdot 7$	2	3

← y-hladká jsou dvojice, která může mít 1

Existují dvě y-hladká čísla, a to $F(2) = 81$ a $F(3) = 126$, a k nim patří reálné exponenci $\nu_1 = (0, 4, 0, 0)$ a $\nu_2 = (1, 2, 0, 1)$. Pro faktorisaci ale lze použít vektoru řešených 5. To by se normálně řešilo tak, že si vytvoříme tabulkou o $z(8)$, doposud tedy se hodnoty V a slouží k nim dělit. Tady však by už bylo něco složitější, protože $F(9) > 403$, a k tomu všem výpočty musíme provést rychleji.

Jak na hledání kořenů v \mathbb{Z}_p ?

$$F(x) = (x+m)^2 - n = 0$$

$$(x+m)^2 = n$$

- je n čtverec?

- když ano, pak využijeme Eulerovým kritériem: musí být $n^{\frac{p-1}{2}} = 1 \text{ v } \mathbb{Z}_p$

- jak najít T_n v \mathbb{Z}_p ?

- když ne, řešme $n^{\frac{p-1}{2}} = 1$, využívajeme to, že má dva obecné různé řešení:

$$n^{\frac{p+1}{2}} = n \quad (n^{\frac{p+1}{2}+1} = n^{\frac{p+1}{2} + \frac{p-1}{2}} = n^{\frac{p+2}{2}} = n^{\frac{p+1}{2}})$$

$$\frac{p+1}{2} = n$$

- pokud je $\frac{p+1}{2}$ sudé, pak $\pm n^{\frac{p+1}{2}} = a$, kde $a^2 = n$.

- pokud předešlou postup všechno, když $\frac{p+1}{2}$ je liché, je možno využít alg. který vyučujeme

Př: \mathbb{Z}_{101}^* má podgrupu $G = \langle 16 \rangle$ řádu 25, $b = 25$, $b \in G$. Vypočítejte dlog₁₆(25) Cvičení: 23.5.2019

1. fáze: $a = 16$, $b = 25$, hledáme $a^s \cdot b^t \cdot h$, aby bylo y-hladké, tj. $16^s 25^t \cdot h$ mělo řád 100, poté musí existovat nějaký prvek z H, aby ho mohlo dělit, jak H vypadá $a^{25} \text{ by mělo byt v H, skutečně } 3^{25} \text{ v } \mathbb{Z}_{101} = 10 \Rightarrow H = \{-1, \pm 10\}$

$$i=1: 16^{20} \cdot 25^1 \cdot (-10) = 66 \times$$

$$16^5 \cdot 25^9 \cdot 1 = 97 \times$$

$$16^4 \cdot 25^{14} \cdot (-1) = 21 = 3 \cdot 7 \quad \checkmark$$

$$i=2: 16^7 \cdot 25^{17} \cdot 10 = 3 \quad \checkmark$$

$$i=3: 16^1 \cdot 25^2 \cdot (-1) = 100 = 2^2 \cdot 5^2 \quad \checkmark$$

$$i=4: 16^{20} \cdot 25^1 \cdot 1 = 54 = 2 \cdot 3^3 \quad \checkmark$$

$$i=5: 16^4 \cdot 25^4 \cdot 10 = 35 = 5 \cdot 7 \quad \checkmark$$

tohle je v \mathbb{Z}_{101}

$$\nu_1 = (0, 1, 0, 1)$$

$$\nu_2 = (0, 1, 0, 0)$$

$$\nu_3 = (2, 0, 2, 0)$$

$$\nu_4 = (1, 3, 0, 0)$$

$$\nu_5 = (0, 0, 1, 1)$$

2. fáze: tohle je v \mathbb{Z}_{25} :

$$2^4 = 16 \text{ v } \mathbb{Z}_{25}$$

$$\left(\begin{array}{ccccc} 0 & 0 & 2 & 1 & 0 \end{array} \right) \sim R_4 \left(\begin{array}{ccccc} 1 & 0 & 0 & 0 & 1 \end{array} \right) \sim R_1 \left(\begin{array}{ccccc} 1 & 0 & 0 & 0 & 1 \end{array} \right) \sim R_1 \left(\begin{array}{ccccc} 1 & 0 & 0 & 0 & 1 \end{array} \right)$$

$$\sim R_2 - R_4 \left(\begin{array}{ccccc} 0 & 1 & 0 & 3 & -1 \end{array} \right) \sim R_2 \left(\begin{array}{ccccc} 0 & 1 & 0 & 3 & -1 \end{array} \right) \sim R_2 - 3R_4 \left(\begin{array}{ccccc} 0 & 0 & 1 & 0 & 13 \end{array} \right) \sim R_3 \left(\begin{array}{ccccc} 0 & 0 & 1 & 0 & 13 \end{array} \right)$$

$$\sim R_1 - R_3 \left(\begin{array}{ccccc} 0 & 0 & 0 & 1 & -1 \end{array} \right) \sim R_4 \left(\begin{array}{ccccc} 0 & 0 & 0 & 1 & -1 \end{array} \right) \sim R_4 \left(\begin{array}{ccccc} 0 & 0 & 0 & 1 & -1 \end{array} \right)$$

$$\sim R_2 \sim \mathbb{Z}_{25}$$

Na volim $c_5 = 1$, pak $c_4 = 1$, $c_3 = -13$, $c_2 = -2$, $c_1 = -1 \Rightarrow c = (-1, -2, 12, 1, 1)$

$$S = \sum c_i \cdot s_i = -14 - 14 + 12 + 20 + 4 = 8 \quad \} \text{ v } \mathbb{Z}_{25}$$

$$T = \sum c_i \cdot t_i = -14 - 34 + 24 + 11 + 4 = -9 = 16$$

$$h = \prod h_i c_i = (-1)^{-1} \cdot 10^{-2} \cdot (-1)^{12} \cdot 1^4 \cdot 10^1 = -1 \cdot 10^{-1} \cdot 1 \cdot 1 = -1 \cdot (-10) = 10 \text{ v } \mathbb{Z}_{101}$$

Kompletace: Máme reprezentaci $(s, t, h) = (8, 16, 10)$, tj. $16^8 \cdot 25^{10} = 68 \cdot 52 = 1 \pmod{101}$.

$$16^8 \cdot 25^{10} = 1$$

$$16^8 \cdot (16^x)^{10} = 16^8$$

$$8 + 16x = 0$$

$$x = -8 \cdot 16^{-1} \pmod{25}$$

$$\varphi(25) = 5 \cdot 4 = 20$$

$$16^{-1} = 16^{19} \pmod{25}$$

$$16^{-1} = 11$$

$$x = -8 \cdot 11 = -88 = 12$$

$$\text{dlog}_{16}(25) = 12 \quad \checkmark$$

Příklad: Dekonvoluta číslo 143 algoritmem SEF s parametry $y=5$.

$P = \{2, 3, 5\}$, zadání se nám nedělí 143. $k=3$

1. fáze: $a^2 = 2^{e_1} \cdot 3^{e_2} \cdot 5^{e_3}$

$$\begin{aligned} \text{v } \mathbb{Z}_{143}: \quad & i=1 \quad 41^2 = 108 = 2^2 \cdot 3^3, \quad v_1 = (2, 3, 0) \\ & i=2 \quad 21^2 = 12 = 2^2 \cdot 3, \quad v_2 = (2, 1, 0) \\ & i=3 \quad 17^2 = 3, \quad v_3 = (0, 1, 0) \\ & i=4 \quad 85^2 = 75 = 3 \cdot 5^2, \quad v_4 = (0, 1, 2) \end{aligned}$$

2. fáze: Chci mít soudobá čísla, proto pracuju v \mathbb{Z}_2

$$\begin{pmatrix} 2 & 2 & 0 & 0 \\ 3 & 1 & 1 & 1 \\ 0 & 0 & 0 & 2 \end{pmatrix} \text{ v } \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \quad \text{Zvolím } c_1 = c_2 = 1, \quad c_3 = c_4 = 0 \quad \text{nemůžu tyto mít, jsem v } \mathbb{Z}_2.$$

Kompletace: levé strany: $(41 \cdot 21 \cdot 17 \cdot 85)^2 = (41 \cdot 21)^2 = 3^2 \pmod{143}$
pravé strany: $2^2 \cdot 3^3 \cdot 2^2 \cdot 3 = 2^4 \cdot 3^4 = (2^2 \cdot 3^2)^2 = (4 \cdot 9)^2 = 36^2$

$$3^2 = 36^2 \\ 1 = (3^{-1} \cdot 36)^2 = (48 \cdot 36)^2 = 12^2 \quad \text{příklad } 12 \neq 1, \text{ to jsme chléli}$$

$$\text{gcd}(11, 143) = 11, \text{ máme faktor } 11, \text{ to je původní číslo. } 143 = 11 \cdot 13.$$

Příklad: Proveďte násobení procedurou QSF, $n=221$, $y=2=8$.

$$m=\lceil \sqrt{n} \rceil = 14 \quad F(x) = (x+14)^2 - 221$$

i	1	2	3	4	5	6	7	8
V	4	35	68	103	140	179	220	263

Toto je násobek, jde možné velké, pracujeme jen se 7. hodnotou.

$$p=2: \quad F(x) = (x+0)^2 - 1 \quad \rightarrow s = \pm 1 = 1 \pmod{2} \\ x^2 - 1 = 0 \quad 2/F(2k+1) \\ x^2 = 1 \quad i \in \{1, 3, 5, 7\}$$

i	1	2	3	4	5	6	7
V	1	35	17	103	35	179	55
D	2^2	2^2	2^2	2^2	2^2	2^2	2^2

$$p=3: \quad F(x) = (x+2)^2 + 1 \quad 2^{\frac{p-1}{2}} = 2^1 = 2 \neq 1 \quad \text{není k řádu} \\ (x+2)^2 = -1 = 2 \pmod{3} \quad \text{nic nebránilo dělitelnost 3 méně}$$

$$p=5: \quad F(x) = (x+4)^2 - 1 \quad \rightarrow x-1 = \pm 1 \Rightarrow s_1 = 0, s_2 = 2 \\ (x+4)^2 = 1 \quad 5/F(5k), 5/F(5k+2) \\ \text{racionální součin je } 1 \quad i \in \{0, 2, 5, 7\}$$

$$p=7: \quad F(x) = (x+0)^2 - 4 \quad \rightarrow x = \pm 2, s_1 = 2, s_2 = 5 \pmod{7} \\ x^2 = 4 \quad i \in \{2, 5\}$$

i	1	2	3	4	5	6	7
V	1	1	17	103	1	179	11
D	2^2	$5 \cdot 7$	2^2	x	$2^2 \cdot 5 \cdot 7$	-	$2^2 \cdot 5$

Máme 3 y-blödky čísla: 1, 35, 140.