13. cvičení: Subexponenciální algoritmus pro faktorizaci a kvadratické síto (SEF a QSF)

Př: Faktorizujte $n = 143$ algoritmem SEF, volte parametr hladkosti $y = 5$.

pozn: $n = 143 \neq p^e$, ani není dělitelné prvočísly $2, 3, 5 \leq y$

1. fáze: prvočísla $\leq y$ jsou $2, 3, 5$, jsou tedy $k = 3$
hledáme $k+1 = 4$ y-hladké čtverce v $\mathbb{Z}_n^*$

v $\mathbb{Z}_{143}^*$ $i = 1$ $41^2 = 108 = 2^2 \cdot 3^3$ $\rightarrow \bar{v}_1 = (2, 3, 0)$

$i = 2$ $21^2 = 12 = 2^2 \cdot 3^1$ $\rightarrow \bar{v}_2 = (2, 1, 0)$

$i = 3$ $25^2 = 53$ - prvoč. ko

$17^2 = 3 = 3^1$ $\rightarrow \bar{v}_3 = (0, 1, 0)$

$i = 4$ $85^2 = 75 = 3^1 \cdot 5^2$ $\rightarrow \bar{v}_4 = (0, 1, 2)$

2. fáze: $c_1 \cdot (2,3,0) + c_2 (2,1,0) + c_3 (0,1,0) + c_4 (0,1,2) = (0,0,0)$

hledáme nebriv. řeš. nad $\mathbb{Z}_2$

nad $\mathbb{Z}_2$: $c_1 (0,1,0) + c_2 (0,1,0) + c_3 (0,1,0) + c_4 (0,1,0) = (0,0,0)$

např: $c_1 = c_2 = 1$, $c_3 = c_4 = 0$

to dává nad $\mathbb{Z}$: $1 \cdot (2,3,0) + 1 \cdot (2,1,0) = (4,4,0)$

kompletace $R_1^1 \cdot R_2^1 \cdot R_3^0 \cdot R_4^0$

v $\mathbb{Z}_{143}^*$ $(41 \cdot 21)^2 = 2^4 \cdot 3^4 \cdot 5^0 = (2^2 \cdot 3^2)^2$

$3^2 = 36^2$

$1 = (3^{-1} \cdot 36)^2 = (48 \cdot 36)^2 = 12^2$

Našli jsme nebriv. $\bar{v}$ v $\mathbb{Z}_{143}^*$, $c = 12$.

Faktor pro $n = 143$ je $\gcd(c-1, n) = \gcd(11, 143) = 11$,

faktorizace $143 = 11 \cdot 13$.

Př: Faktorizujte $n = 221$ pomocí SEF, volte $y = 10$.

Prvočísla $\leq y$ jsou $2, 3, 5, 7$, jsou tedy $k = 4$. Přitom žádné nedělí 221.

1. fáze: hledáme $k+1 = 5$ y-hladkých čtverců v $\mathbb{Z}_n^*$

v $\mathbb{Z}_{221}$: $i = 1$ $105^2 = 196 = 2^2 \cdot 7^2$ $\rightarrow \bar{v}_1 = (2, 0, 0, 2)$

BINGO! $\bar{v}_1$ má sudé souřadnice, dále hledat nemusíme

2. fáze: nad $\mathbb{Z}_2$ $1 \cdot (2,0,0,2) = (0,0,0)$

kompletace R_1^1 v $\mathbb{Z}_{221}$: $105^2 = (2\cdot 7)^2 = 14^2$

protože $105 \neq \pm 14$, tak jsme našli netriv. $\sqrt{1}$ v $\mathbb{Z}_{221}$

$c = 14^{-1} \cdot 105 = 79 \cdot 105 = 118$

faktor pro n je $\gcd(117, 221) = 13$

Eukleid: $221 = 117 + 104$

$117 = 104 + \boxed{13}$

$104 = 8 \cdot 13 + 0$

faktorizace: $221 = 13 \cdot 17$.

PŘ: Vyzkoušejte si pro $n = 221$ síťovací proceduru, volte parametr hladkosti $y = 10$ a parametr síta $z = 10$.

Položíme $m = \lfloor \sqrt{n} \rfloor = \lfloor \sqrt{221} \rfloor = 14$

$F(x) = (x + 14)^2 - 221$

Do síta (pole) V délky $z = 10$ spočteme hodnoty $F(x)$, $1 \leq x \leq 10$.

$F(1) = 15^2 - 221 = 4$, $F(2) = 16^2 - 221 = 35$ atd, počítáme v $\mathbb{Z}$.

	1	2	3	4	5	6	7	8	9	10
V	4	35	68	103	140	179	220	263	/	/

! 263 už není zb. mod 221

Algoritmus QSF by fungoval i tak, ale raději zmenšíme param. síta na $z = 7$.

Prvočíslem $p \leq y$ dělíme jen ty $V[s]$, které jím dělitelné jsou.

$p \mid F(s)$ iff $F(s) = 0$ v $\mathbb{Z}_p$ iff s je kořen pol. $F(x)$ mod $\mathbb{Z}_p$

mod $\mathbb{Z}_2$: $F(x) = (x+0)^2 - 1 = 0$

$x^2 = 1$

$x = \pm 1 = 1$

$2 \mid F(1 + 2\ell)$ pro $\ell \in \mathbb{N}$

změna pole

	1	2	3	4	5	6	7
V	4		17		35		55

a také si v jiném poli pamatujeme seznamy faktorů

	1	2	3	4	5	6	7
FAKTORY	2^2		2^2		2^2		2^2

mod $\mathbb{Z}_3$: $F(x) = (x+2)^2 - 2 = 0$

$(x+2)^2 = 2$

nexistuje kořen

$3 \nmid F(x)$

Eulerovo kritérium: $2^{\frac{3-1}{2}} = 2^1 = -1$ v $\mathbb{Z}_3$

tedy 2 není čtverec

nad $\mathbb{Z}_5$: $F(x) = (x-1)^2 - 1 = 0$

$(x-1)^2 = 1 = (\pm 1)^2$

$x = 1 \pm 1 = \begin{matrix} 0 \\ 2 \end{matrix}$

$5 \mid F(5\ell)$, $5 \mid F(2+5\ell)$ pro $\ell \in \mathbb{N}$

další síťování pole

	1	2	3	4	5	6	7
V	1	7	17	103	7	179	11
FAKTORY	2^2	5	2^2	$2^2 \cdot 5$		$2^2 \cdot 5$	

nad $\mathbb{Z}_7$: $F(x) = (x+0)^2 - 4 = 0$

$x^2 = 4 = (\pm 2)^2$

$x = \begin{matrix} 2 \\ 5 \end{matrix}$

$7 \mid F(2+7\ell)$, $7 \mid F(5+7\ell)$ pro $\ell \in \mathbb{N}$

poslední síťování

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

Našli jsme 3 $y=10$ - hladké čtverce tvaru $(x+14)^2$ v $\mathbb{Z}_{221}$:

$(1+14)^2 = \cancel{15^2} = 4 = 2^2$

$(2+14)^2 = 35 = 3 \cdot 7$

$(5+14)^2 = 140 = 2^2 \cdot 5 \cdot 7$

a to je málo, potřebujeme jich $k+1 = 5$, neboť jsou $k=4$ prvočís. $\leq y = 10$.

(Pozn: zde náhodou $15^2 = 2^2$ umožní najít netriv. π, $c = 2^{-1} \cdot 15 = 118$)

PŘ: Hledání kořenů kvadrat. polynomů nad $\mathbb{Z}_p$; $p > 2$.

V $\mathbb{Z}_{19}$ nalezněte kořeny, pokud existují:

a) $P(x) = x^2 + 6x + 7 = 0$

$(x+3)^2 - 2 = 0$

$(x+3)^2 = 2$

kořeny neexistují v $\mathbb{Z}_{19}$

Euler. kritérium

$2^{\frac{p-1}{2}} = 2^9 = -1$ v $\mathbb{Z}_{19}$

tudíž $2 \neq c^2$ není čtverec

b) $P(x) = x^2 + 2x + 15 = 0$

$(x+1)^2 = -14 = 5$

$(x+1)^2 = (\pm 9)^2$

kořeny: $x_{1,2} = -1 \pm 9 = \begin{cases} 8 \\ -10 = 9 \end{cases}$

· Euler. krit. $5^9 = 1$ v $\mathbb{Z}_{19}$, tedy $5 = c^2$ je čtverec

· Zde lze snadno spočítat $c = \sqrt{5}$

z Euler. krit. $5^{10} = 5$ v $\mathbb{Z}_{19}$

tedy $\sqrt{5} = \pm 5^5 = \pm 9$

c) $P(x) = x^2 + 9x + 14 = 0$

$x^2 - 10x + 14 = (x-5)^2 - 11 = 0$

$(x-5)^2 = 11 = (\pm 7)^2$

kořeny $x_{1,2} = 5 \pm 7 = \begin{cases} 12 \\ -2 = 17 \end{cases}$

Euler. krit. $11^9 = 1$ v $\mathbb{Z}_{19}$

odtud $11 = 11^{10} = (11^5)^2 = 7^2$

d) obecný vzorec

v $\mathbb{Z}_p$: $ax^2 + bx + c = 0$ pro $x_{1,2} = \dfrac{-b \pm \sqrt{b^2 - 4ac}}{2a}$ iff $D = b^2 - 4ac$ je čtverec v $\mathbb{Z}_p$

důkaz: $\left(x + \frac{b}{2a}\right)^2 = \dfrac{b^2 - 4ac}{4a^2}$

pro $p \neq 2$ lze doplnit na čtverec

zlomky budou násobením inver. prvky $(2a)^{-1}$ exist v $\mathbb{Z}_p$ pro $a \neq 0$, $p \neq 2$

pokud bude $D = b^2 - 4ac$ čtverec v $\mathbb{Z}_p$, tak půjde najít $\sqrt{D}$

a bude fungovat známý vzorec na výpočet kořenů x_1, x_2

V opačném případě kořeny neexistují

Domácí úkol:

1) Faktorizujte $n = 493$ algoritmem SEF, volte param. hladkosti $y = 8$.

[$493 = 13 \cdot 29$]

2) Pro $n = 493$ proveďte sítovací proceduru, volte param. hladkosti $y = 11$ a parametr síta $z = 8$.

[propadne jen $(1+22)^2 = 2^2 \cdot 3^2$

$(3+22)^2 = 2^2 \cdot 3 \cdot 11$]

3) Prohlédněte si př. 150 ze sbírky od Josefa Hekrdly, kde je faktorizace většího čísla, konkrétně $n = 1\,711\,343$.