Číselné algoritmy

Algoritmus ECM

22. 3. 2021

Pollardova $(p-1)$-metoda, shrnutí

- Potřebuje, aby vstup N byl dělitelný prvočíslem p, pro které je $(p-1)$ součin malých prvočísel
- Ve skutečnosti potřebujeme, aby řád grupy $\mathbb{Z}_p^*$ byl B-mocný
- Výpočet, který teoreticky probíhá v grupě $\mathbb{Z}_p^*$ je realizován v $\mathbb{Z}_N$

$(p+1)$-metoda, náčrt

Zkusme navrhnout faktorizační algortimus, který bude aplikovatelný na vstupy dělitelné prvočíslem p, pro které je $p+1$ B-mocné.
Pokusíme se využít strukturu konečného tělesa $\mathbb{F}_{p^2}$. O grupě $\mathbb{F}_{p^2}^*$ víme, že je cyklická řádu $p^2-1=(p+1)(p-1)$.
Grupa $\mathbb{F}_{p^2}^*$ obsahuje právě jednu podgrupu řádu $p-1$

$$H = \{g^{p+1} \mid g \in \mathbb{F}_{p^2}^*\}.$$

Jednoduché pozorování

Tvrzení

Necht' pro $p \in \mathbb{P}$ platí, že $(p+1)$ je B-mocné. Pak pro každé $g \in \mathbb{F}_{p^2}^*$ platí $g^{e_B} \in H$.

Připomenutí: $e_B = \prod_{p \in \mathbb{P}, p \leq B} p^{\lfloor \log_p(B) \rfloor}$ je největší B-mocné číslo.
Předpoklad říká, že $(p+1) \mid e_B$.
Důkaz: Poučku $g^{|G|} = 1_G$ pro každé $g \in G$, kde G je konečná grupa aplikujeme pro $G = \mathbb{F}_{p^2}^*/H$.
Máme $|G| = (p^2-1)/(p-1) = p+1$, a tedy $(gH)^{p+1} = H$ pro každé $gH \in \mathbb{F}_{p^2}^*/H$.
Tedy $g^{p+1} \in H$ pro každé $g \in \mathbb{F}_{p^2}^*$. Pak také $g^{e_B} \in H$.

Konstrukce tělesa $\mathbb{F}_{p^2}$

Těleso velikosti p^2 lze konstruovat jako $\mathbb{F}_p[x]/(x^2 - c)$, $x^2 - c$ je ireducibilní polynom (tedy $(\frac{c}{p}) = -1$).
Při konkrétních výpočtech realizujeme prvky tělesa jako polynomy tvaru $ax + b$, kde $a, b \in \mathbb{F}_p$.
V této konkrétní realizaci je velice snadné popsat grupu H.

$$H := \{ax + b \mid a = 0, b \in \mathbb{F}_p^*\}.$$

Tvrzení z předchozího slajdu tedy přepíšeme takto: Pro každé $0 \neq ax + b$, $a, b \in \mathbb{F}_p$ existuje $b' \in \mathbb{F}_p^*$ tak, aby

$$(ax + b)^{e_B} \bmod (x^2 - c) = b'.$$

$(p+1)$-hrubý popis algoritmu

- Na vstupu je N složené, dělitelné prvočíslem p, pro které je $p+1$ B-mocné
- Zvolíme $c \in \mathbb{Z}_N^*$ (doufáme, že $x^2 - c \in \mathbb{F}_p[x]$ je ireducibilní)
- zvolíme $a, b \in \{1, \ldots, N-1\}$. Pokud je náhodou $\mathrm{NSD}(a, N) > 1$ nebo $\mathrm{NSD}(b, N) > 1$, máme vlastní faktor N
- V okruhu $\mathbb{Z}_N[x]/(x^2 - c)$ spočteme $a'x + b' := (ax + b)^{e_B}$ (rychlým umocněním). De facto se jedná o výpočet $(a + bx)^{e_B} \bmod x^2 - c$, přičemž výpočty s koeficienty se provádí modulo N.
- Pokud bylo $p+1$ B-mocné bude $p \mid \mathrm{NSD}(a', N)$, zkusíme, zda $\mathrm{NSD}(a', N)$ není vlastní dělitel N.
- Podobně jako u $(p-1)$-metody je možné zvýšit pravděpodobnost úspěšného výstupu organizací výpočtu.

$(p+1)$-metoda dokončení

Analogicky bychom mohli navrhnout například (p^2+p+1)-metodu. Pokud ale zůstaneme pouze u multiplikativních grup konečného tělesa, budeme vždy potřebovat, aby vstup N byl dělitelný prvočíslem dost speciálních vlastností. Tento nedostatek odstraňuje metoda ECM.

ECM - úvod

- publikována v článku H. W. Lenstra, *Factoring integers with elliptic curves*, Ann. of Math. 126(1987), 649 - 673.
- Využívá strukturu grupy bodů eliptické křivky nad konečným tělesem
- V praxi velmi dobře použitelná metoda pro odhalování 'malých' prvočíslených dělitelů

Projektivní rovina, značení

Necht' $\mathbb{F}$ je těleso, projektivní rovinou nad $\mathbb{F}$ budeme rozumět množinu

$$\mathbb{P}_2(\mathbb{F}) := \{\langle v \rangle \mid 0 \neq v \in \mathbb{F}^3\}$$

Pro $0 \neq (w, x, y) \in \mathbb{F}^3$ se též značí $\langle v \rangle = (w : x : y)$.
Tedy pro $(w, x, y), (w', x', y') \in \mathbb{F}^3 \setminus \{0\}$ je
$(w : x : y) = (w' : x' : y')$ právě když pro nějaké $\lambda \in \mathbb{F}$ platí

$$(w, x, y) = (\lambda w', \lambda x', \lambda y')$$

Značení: Bod $(w : x : y) \in \mathbb{P}_2(\mathbb{F})$ budeme označovat jako *vlastní bod*, pokud $w \neq 0$. Vlastní body budeme zapisovat ve tvaru $[x, y] := (1 : x : y)$. Tedy pro $w \neq 0$ je

$$(w : x : y) = [\frac{x}{w}, \frac{y}{w}].$$

Ostatní body označujeme jako body *nevlastní*.

Projektivní rovinné křivky

Definice

Projektivní rovinná křivka *je množina bodů* $\mathbb{P}_2(\mathbb{F})$ *ve tvaru*

$$V(F) := \{(w : x : y) \in \mathbb{P}_2(\mathbb{F}) \mid F(w, x, y) = 0\},$$

kde $F \in \mathbb{F}[W, X, Y]$ *je nekonstantní homogenní polynom.*

Poznámka: Je-li F ireducibilní a $\mathbb{F}$ algebraicky uzavřené je F určen jednoznačně až na skalární násobek množinou $V(\mathbb{F})$. Obecněji $V(F)$ určuje ireducibilní dělitele F za předpokladu $\mathbb{F} = \overline{\mathbb{F}}$.

Eliptické křivky

Definice

Nechť $\mathbb{F}$ *je těleso,* $\mathrm{char}(\mathbb{F}) \neq 2, 3$. *Pro účely této přednášky budeme eliptickou křivkou nad* $\mathbb{F}_p$ *rozumět projektivní rovinnou křivku danou polynomem* $E_{a,b} = WY^2 - X^3 - aW^2X - bW^3 \in \mathbb{F}[W, X, Y]$, *kde* $a, b \in \mathbb{F}$ *splňují* $4a^3 + 27b^2 \neq 0$.

Poznámka: Při uvedeném označení je

$$V(E_{a,b}) = \{[x, y] \mid x, y \in \mathbb{F}, y^2 = x^3 + ax + b\} \cup \{(0 : 0 : 1)\}$$

Jediný nevlastní bod $V(E_{a,b})$ budeme označovat 0.

Grupa bodů eliptické křivky

Pro eliptickou křivku nad tělesem $\mathbb{F}$ definujeme na $V(E_{a,b})$ strukturu komutativní grupy následujícím způsobem:

- 0 je neutrální prvek grupy
- Operace opačného prvku je daná vztahy $-0 := 0$ a $-[x, y] := [x, -y]$
- $0 + 0 = 0$, $0 + [x, y] := [x, y]$, $[x, y] + 0 := [x, y]$.
- $[x, y] + [x, -y] := 0$
- $[x_1, y_1] + [x_2, y_2] = [x_3, y_3]$, kde $x_3 = s^2 - x_1 - x_2$ a $y_3 = s(x_1 - x_3) - y_1$, kde $s := \frac{y_1 - y_2}{x_1 - x_2}$, pokud $x_1 \neq x_2$ a $s = \frac{3x_1^2 + a}{2y_1}$, pokud $[x_1, y_1] = [x_2, y_2]$ a $y_1 \neq 0$.

Odvození vzorců provedeme později, prozatím poznamenejme, že vzorce lze odvodit z pravidla 'součet bodů v průniku projektivní přímky a $V(E_{a,b})$ je vždy nula'

Definice

Výše popsanou grupu budeme označovat $E_{a,b}(\mathbb{F})$.

Velikost $E_{a,b}(\mathbb{F})$

Věta

(Hasse) Nechť $3 < p \in \mathbb{P}$, $a, b \in \mathbb{F}_p$ *splňující* $4a^3 + 27b^2 \neq 0$. *Pak*

$$||E_{a,b}(\mathbb{F}_p)| - (p+1)| < 2\sqrt{p}$$

Věta

(Deuring) Nechť $3 < p \in \mathbb{P}$ *a*
$m \in ((p+1) - 2\sqrt{p}, (p+1) + 2\sqrt{p}) \cap \mathbb{N}$. *Pak existují* $a, b \in \mathbb{F}_p$ *splňující* $4a^3 + 27b^2 \neq 0$ *taková, že*

$$|E_{a,b}(\mathbb{F}_p)| = m$$

Princip metody ECM

Na vstupu je složené N, které není mocnina prvočísla, dále předpokládáme $\mathrm{NSD}(N, 6) = 1$. K dispozici máme $B \in \mathbb{N}$.
Označme $p \in \mathbb{P}$ (nejmenšího) prvočíselného dělitele N.
Předpokládejme, že se podařilo zvolit $a, b \in \mathbb{F}_p$ tak, že $|E_{a,b}(\mathbb{F}_p)|$ je B-mocné.
Pro každý bod $P \in E_{a,b}(\mathbb{F}_p)$ pak platí

$$e_B.P = \overbrace{P + P + \cdots + P}^{e_B} = 0$$

Počítání modulo N

Představme si následující výpočet: Protože neznáme $p \in \mathbb{P}$, budeme místo s prvky množiny $E_{a,b}(\mathbb{F}_p)$ počítat s prvky množiny

$$E'_{a,b}(\mathbb{F}_p) := \{[x, y] \mid x, y \in \mathbb{Z}_N \mid y^2 \equiv x^3 + ax + b \bmod p\} \cup \{0\}$$

Sčítání prvků v této množině se provádí podle stejných vzorců, které definují strukturu $E_{a,b}(\mathbb{F}_p)$, pouze místo modulo p počítáme modulo N.
Určitý problém by mohl nastat při výpočtu s podle vzorců $s = \frac{y_1 - y_2}{x_1 - x_2}$ nebo $s = \frac{3x_1^2 + a}{2y_1}$.
V prvním případě nebude součet definován, pokud $\mathrm{NSD}(x_1 - x_2, N) > 1$, ve druhém případě nebude součet definován, pokud $\mathrm{NSD}(2y_1, N) > 1$.
Metoda ECM hledá body $[x_1, y_1], [x_2, y_2] \in E'_{a,b}(\mathbb{F}_p)$ a v ideálním případě bude $\mathrm{NSD}(x_1 - x_2, N)$ nebo $\mathrm{NSD}(2y_1, N)$ vlastní dělitel N

ECM - hrubý popis algoritmu

Vstup: N dělitelné dvěma různými prvočísly, $2, 3 \nmid N$

Výstup: Vlastní dělitel N nebo neúspěch

k dispozici: B, posloupnost všech prvočísel $\leq B$

1. Zvol $a, b \in \mathbb{Z}_N$ náhodně, test $\mathrm{NSD}(4a^3 + 27b^2, N) = 1$

2. Urči bod $P = [x, y] \in E'_{a,b}(\mathbb{F}_p)$
$//y^2 \equiv x^3 + ax + b \pmod{N}$.

3. Spočti $P := e_B \cdot P$ // operace v $E'_{a,b}(\mathbb{F}_p)$

4. Pokud objevíme $[x_1, y_1], [x_2, y_2] \in E'_{a,b}(\mathbb{F}_p)$, které nejdou sečíst, spočteme $\mathrm{NSD}(x_1 - x_2, N)$ nebo $\mathrm{NSD}(2y_1, N)$ podle toho, jestli je $[x_1, y_1] \neq [x_2, y_2]$ nebo $[x_1, y_1] = [x_2, y_2]$.

5. Pokud v předchozím kroku dostaneme vlastního dělitele N, pošleme ho na výstup, jinak algoritmus končí s neúspěchem.

Volba bodu P

Poměrně nevinně vypadající krok **2.** je problematický. Mohli bychom například

- Zvolit $x \in \mathbb{Z}_N$ náhodně
- Spočíst $x' := x^3 + ax + b \bmod N$
- Pokusit se najít odmocninu v x' v okruhu $\mathbb{Z}_N$, tedy $y \in \mathbb{Z}_N$ splňující $y^2 \equiv x' \pmod N$.

Problém je v tom, že spočítat odmocninu v $\mathbb{Z}_N$ je bez znalosti faktorizace N obtížná úloha.
Možná řešení:

(a) Speciální volba a, b v kroku **1.**: Zvolíme $b = 1$, $a \in \mathbb{Z}_N$ náhodně. Pak položíme $P := [0, 1]$.

(b) Volba náhodného bodu na náhodné křivce: Volíme $x, y, a \in \mathbb{Z}_N$ náhodně. Položíme $b := (y^2 - x^3 - ax) \bmod N$ a otestujeme, jestli $\mathrm{NSD}(4a^3 + 27b^2, N) = 1$.

Proč dojde k faktorizaci

Předpokládejme, že se podařilo parametry a, b nastavit tak, aby $|E_{a,b}(\mathbb{F}_p)|$ bylo B-mocné pro nějaké $p \in \mathbb{P}$, $p \mid N$.
Bod $P = [x, y]$ reprezentuje bod
$\overline{P} = [x \bmod p, y \bmod p] \in E_{a,b}(\mathbb{F}_p)$. Bude proto platit $e_B \overline{P} = 0$.
V průběhu výpočtu kroku **3.** tedy musíme narazit na body P_1, P_2 takové, že v $E_{a,b}(\mathbb{F}_p)$ platí $\overline{P_1} + \overline{P_2} = 0$.
Nechť $q \in \mathbb{P}$ je dělitel N, $q \neq p$. Bod P reprezentuje také bod
$\widetilde{P} = [x \bmod q, y \bmod q] \in E_{a,b}(\mathbb{F}_q)$. Pokud pro nalezené body P_1, P_2 bude platit $\widetilde{P_1} + \widetilde{P_2} \neq 0$, nebude součet $P_1 + P_2$ definován a výpočet v kroku **3.** se zastaví.
Obecně očekáváme, že grupové struktury $E_{a,b}(\mathbb{F}_p)$ a $E_{a,b}(\mathbb{F}_q)$ jsou nezávislé do té míry, že problém při výpočtu $e_B \overline{P}$ nastane jindy než při výpočtu $e_B \widetilde{P}$. V takovém případě bude faktorizace pomocí ECM úspěšná.
V případě neúspěchu je možné zkusit výpočet na jiné křivce.

K volbě B

Je samozřejmě možné přistoupit k volbě B podobně jako u $(p-1)$-metody. ECM ale umožňuje i jiný přístup - heuristická analýza složitosti ECM vede k 'optimální volbě'

$$B \approx e^{\sqrt{\frac{1}{2}\ln(p)\ln\ln(p)}},$$

kde p je nejmenší prvočíselný dělitel vstupu.

Konec 4. přednášky

Děkuji za pozornost.