Číselné algoritmy

Odmocňování v konečných tělesech

12. 4. 2021

Paralelní inverze modulo N

Pokud počítáme na více křivkách současně, lze uplatnit tento algoritmus

Vstup: N, $a_1, a_2, \ldots, a_k \in \mathbb{Z}_N$

Výstup: a_i soudělné s N, nebo $b_1, b_2, \ldots, b_k \in \mathbb{Z}_N$ splňující $a_i b_i \equiv 1 \pmod{N}$

1. $c_0 := 1$
2. **for** $i = 1$ to k **do** $c_i := c_{i-1} a_i \bmod N$
3. Urči $\alpha, \beta \in \mathbb{Z}$ tak, že $\alpha c_k + \beta N = \mathrm{NSD}(c_k, N) =: d$
4. **if** $d > 1$ **then** najdi a_i soudělné s N a konec
5. **for** $i = k$ downto 1 **do**

   $b_i := \alpha c_{i-1} \bmod N$

   $\alpha := \alpha a_i \bmod N$

return $b_1, b_2, \ldots, b_k$

ECM, shrnutí

Na vstupu je N, $\mathrm{NSD}(N, 6) = 1$, dělitelné alespoň dvěma různými prvočísly.
Označme $p \in \mathbb{P}$ nejmenší prvočíslo dělící N.
Inicializace ECM: volíme a, b, x, y tak, aby
$\mathrm{NSD}(4a^3 + 27b^2, N) = 1$ a $y^2 \equiv x^3 + ax + b \pmod{N}$.
Označme
$E_{a,b}(\mathbb{Z}_N) = \{[x, y] \mid x, y \in \mathbb{Z}_N, y^2 \equiv x^3 + ax + b \pmod{p}\} \cup \{0\}$.
Pro některé body této množiny je definován součet (viz další slajd).
ECM se pokusí během výpočtu $e_B[x, y]$ najít body, které nepůjdou sečíst. Pokud pomocí těchto dvou bodů dokáže najít vlastního dělitele, máme výstup. V opačném případě končí s neúspěchem.

ECM, vzorečky

Máme $[x_1, y_1], [x_2, y_2] \in \mathbb{E}_{a,b}(\mathbb{Z}_N)$. Definujeme $[x_3, y_3] := [x_1, y_1] + [x_2, y_2]$ vztahem

$$x_3 := s^2 - x_1 - x_2 \bmod N, y_3 := s(x_1 - x_3) - y_1 \bmod N,$$

kde

1. pro $\mathrm{NSD}(x_1 - x_2, N) = 1$ definujeme $s := (y_1 - y_2)t \bmod N$, kde $t \in \mathbb{Z}_N$ splňuje $t(x_1 - x_2) \equiv 1 \pmod N$
2. pro $[x_1, y_1] = [x_2, y_2]$ a $\mathrm{NSD}(2y_1, N) = 1$ definujeme $s = (3x_1^2 + a)t \pmod N$, kde $t \in \mathbb{Z}_N$ splňuje $(2y_1)t \equiv 1 \pmod N$

Dává smysl dodefinovat ještě součty $0 + [x, y] = [x, y] + 0 := [x, y]$, $[x, 0] + [x, 0] = 0$ a $[x, y] + [x, -y] = 0$. Jednoduchá implementace ECM může skončit neúspěchem, pokud by našla dva body jejichž součtem je nevlastní bod.

Square and multiply

Důležité je aby snaha o výpočet

$e_B[x,y] = \overbrace{[x,y]+[x,y]+\cdots+[x,y]}^{e_B}$ běžela podle nějakého efektivního algoritmu. Podstatné je, aby počet provedených operací s body $E_{a,b}(\mathbb{Z}_N)$ byl řádově $O(\log(e_B))$.

Vstup: $m \in \mathbb{N}$, $P \in E_{a,b}(\mathbb{Z}_N)$

Výstup: mP, pokud jde spočíst

1. $R := 0$, $Q := P$
2. **while** $(m \neq 0)$ **do**:
   if $2 \nmid m$ **then** $R := R + Q$
   $Q := Q + Q$
   $m := m \operatorname{div} 2$
3. **return** R

Odmocňování úvod

Cílem je nalézt algoritmus, který v konečném tělese $\mathbb{F}$ pro dané $a \in \mathbb{F}$ najde kořeny rovnice $x^2 = a$.
Zaměříme se na tělesa prvočíselné velikosti.
Algoritmus Tonelli-Shanks lze upravit tak, aby počítal odmocniny v konečných tělesech kladné charakteristiky.

Kvadratická rezidua, opakování

Definice

Nechť p je liché prvočíslo, $a \in \mathbb{Z}_p$. Řekneme, že a je kvadratické reziduum *modulo p, pokud kongruence $x^2 \equiv a \pmod{p}$ má celočíselné řešení.*

Tvrzení

Nechť p je liché prvočíslo a $a \in \mathbb{Z}_p^*$. Pak rovnice $x^2 \equiv a \pmod{p}$ je řešitelná právě když $a^{\frac{p-1}{2}} \bmod p = 1$.

Důkaz tvrzení

Důkaz: Připomeňme, že grupa $\mathbb{Z}_p^*$ je (cyklická) grupa řádu $p-1$, proto $y^{p-1} \equiv 1 \pmod{p}$ pro každé $y \in \mathbb{Z}_p^*$. Je-li $a \in \mathbb{Z}_p^*$ kvadratické reziduum, pak nutně $a^{\frac{p-1}{2}} \mod p = 1$. Dále si všimneme, že zobrazení $y \mapsto y^2 \mod p$ je endomorfismus $\mathbb{Z}_p^*$ s jádrem $\{1, -1\}$, tedy počet reziduí v $\mathbb{Z}_p^*$ je přesně $\frac{p-1}{2}$. Celkově: Polynom $x^{\frac{p-1}{2}} - 1$ se rozkládá nad $\mathbb{Z}_p$ na součin lineárních činitelů a kořeny tohoto polynomu jsou právě kvadratická rezidua ze $\mathbb{Z}_p^*$.

$p = 4k + 3$

Ukažme si algoritmy pro odmocňování modulo prvočísla speciálních tvarů.
Začneme případem, kdy $p \equiv 3 \pmod 4$, tedy $p = 4k + 3$ pro nějaké $k \in \mathbb{N}_0$.
Chceme řešit $x^2 \equiv a \pmod p$ pro $a \in \mathbb{Z}_p^*$ a předpokládejme, že úloha má řešení.
To znamená, že $a^{\frac{p-1}{2}} \equiv 1 \pmod p$, tedy také $a^{\frac{p+1}{2}} \equiv a \pmod p$.
Protože $\frac{p+1}{2} = 2k + 2$ je sudé, dostaneme vzorec pro odmocninu

$$x = \pm a^{k+1} \bmod p,$$

kde $k = \frac{p-3}{4}$.

$p = 8k + 5$

O něco obtížnější je případ, kdy $p \equiv 5 \pmod 8$, tedy $p = 8k + 5$ pro nějaké $k \in \mathbb{N}_0$.
Opět předpokládáme, že máme $a \in \mathbb{Z}_p^*$ a kongruence $x^2 \equiv a \pmod p$ je řešitelná.
Podmínka řešitelnosti se tentokrát napíše jako $a^{4k+2} \equiv 1 \pmod p$.
Druhá mocnina prvku $a^{2k+1} \bmod p \in \mathbb{Z}_p^*$ v tělese $\mathbb{Z}_p$ je jedna.
Musí proto platit $a^{2k+1} \bmod p = \pm 1$.
Pokud platí $a^{2k+1} \bmod p = 1$, dostáváme opět kongruenci $a^{2k+2} \equiv a \pmod p$, která stejně jako v předchozím případě vede k řešení

$$x \equiv \pm a^{k+1} \bmod p$$

$p = 8k + 5$, dokončení

Uvažme situaci, kdy $a^{2k+1} \bmod p = -1$. Ta vede na kongruenci $a^{2k+2} \equiv -a \pmod{p}$. Potřebovali bychom tuto kongruenci přenásobit kongruencí tvaru $z^2 \equiv -1 \pmod{p}$, kde $z \in \mathbb{Z}$ známe. Takovou relaci poskytuje zákon kvadratické reciprocity pro výpočet Legendreova symbolu $(\frac{2}{p})$. Pro prvočísla tvaru $8k + 5$ máme vždy $(\frac{2}{p}) = -1$, což lze přepsat jako

$$2^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

Vynásobením výše uvedených kongruencí se dostaneme ke vztahu

$$2^{4k+2} a^{2k+2} \equiv 1 \pmod{p}$$

Tento vztah nás dovede k řešení

$$x = \pm 2^{2k+1} a^{k+1} \bmod p$$

Tonelli-Shanks, úvod

Předpokládejme, že $2 \neq p \in \mathbb{P}$.
Necht' je $p - 1 = 2^e q$, kde $e \in \mathbb{N}$ a $q \in \mathbb{N}$ je liché.
Podle čínské věty o zbytcích máme izomorfismus

$$\mathbb{Z}_p^* \simeq (\mathbb{Z}_{2^e}, +) \times (\mathbb{Z}_q, +)$$

V grupě vlevo se reálně počítá, grupa vpravo by mohla být trochu názornější pro pochopení principu algoritmu.

Několik pozorování

- Pokud máme prvek $x \in \mathbb{Z}_p^*$ odpovídající dvojici $(i, j) \in \mathbb{Z}_{2^e} \times \mathbb{Z}_q$, pak x^2 odpovídá dvojici $(2i \bmod 2^e, 2j \bmod q)$. Odtud snadno nahlédneme, že kvadratická rezidua ze $\mathbb{Z}_p^*$ odpovídají přesně dvojicím (α, β), kde $\alpha \in \mathbb{Z}_{2^e}$ je sudé.
- Pokud prvek $a \in \mathbb{Z}_p^*$ odpovídá dvojici (i, j), pak prvek a^q odpovídá dvojici $(qi \bmod 2^e, 0)$. Řád prvku a^q bude potom řád $qi \bmod 2^e$ v $\mathbb{Z}_{2^e}$. Tedy řád $a^q \in \mathbb{Z}_p^*$ je vždy nezáporná mocnina dvou.
- Předpokládejme, že máme prvek $z \in \mathbb{Z}_p^*$, který odpovídá dvojici $(i, 0)$. Potom řád z je 2^e právě když i je liché právě když $z^{2^{e-1}} \equiv -1 \pmod p$.

Tonelli-Shanks, základní princip

Předpokládejme, že kromě zadaného $a \in \mathbb{Z}_p^*$ máme k dispozici také prvek $z \in \mathbb{Z}_p^*$, $o(z) = 2^e$. Podle předchozího pozorování pak bude $a^q = z^k$ pro nějaké $0 \leq k < 2^e$. Pokud a je kvadratické reziduum, musí být k sudé. Potom v grupě $\mathbb{Z}_p^*$ platí

$$a = a^{q+1} z^{-k} = (a^{\frac{q+1}{2}} z^{\frac{-k}{2}})^2.$$

Řešením je proto $x = \pm a^{\frac{q+1}{2}} z^{\frac{-k}{2}} \mod p$.
Zbývá vyřešit následující problémy:

1. Jak najdeme prvek $z \in \mathbb{Z}_p^*$ řádu 2^e?
2. Jak ze znalosti z, a, q a rovnosti $z^k = a^q$ dostaneme k?

Volba prvku z

- Zvolíme $z_0 \in \mathbb{Z}_p^*$ náhodně
- Spočteme $(z_0^q)^{2^{e-1}} \mod p$. Pokud vyjde 1, volíme nové z_0
- v opačném případě je $z_0^q \mod p$ prvek $\mathbb{Z}_p^*$ řádu 2^e

Protože $(z_0^q)^{2^{e-1}} = z_0^{\frac{p-1}{2}}$ provádíme test, jestli je zvolené z_0 kvadratické reziduum modulo p. Pravděpodobnost úspěšné volby z_0 je proto $\frac{1}{2}$.

Výpočet k

Potřebujeme ze znalosti z, a, q a rovnosti $z^k = a^q$ zjistit k. Přitom víme, že $a^q \in \langle z \rangle$, tedy v principu řešíme problém diskrétního logaritmu v grupě $\langle z \rangle$. Tato grupa má 2^e prvků, pomocí Pohlig-Hellmanovy redukce lze výpočet provést pomocí e výpočtů v grupě řádu 2.

Výpočet k, pokr.

Podívejme se na situaci v $\mathbb{Z}_{2^e}$: Prvek řádu 2^m vypadá nějak takto

$$c = 2^{e-m} + \sum_{i=1}^{m-1} a_i 2^{e-m+i}\,, a_i \in \{0,1\}$$

Pokud k prvku c přičteme 2^{e-m}, dostaneme prvek řádu $< 2^m$. Tedy řád $c \in \mathbb{Z}_{2^e}$ určuje nejnižší bit ve dvojkové reprezentaci c. Při řešení rovnice $z^k = c$, $o(c) = 2^m$ lze proto postupovat takto: Celou rovnici přenásobíme $z^{2^{e-m}}$, dostaneme $z^k z^{2^{e-m}} = c z^{2^{e-m}} =: c_1$, $2^{m_1} := o(c_1) < 2^m$. Dalším přenásobením pak dostaneme $z^k z^{2^{e-m}} z^{2^{e-m_1}} = c_1 z^{2^{e-m_1}} =: c_2$, kde řád c_2 je menší jak řád c_1. Takto pokračujeme, dokud nedostaneme na pravé straně prvek řádu 1. Tam skončíme s tím, že jsme odhalili $-k \bmod 2^e$.

Algoritmus Tonelli - Shanks

Vstup: Liché prvočíslo p, $a \in \mathbb{Z}_p^*$.

Výstup: $x \in \mathbb{Z}_p^*$, $x^2 \equiv a \pmod{p}$ pokud existuje, jinak hláška, že neexistuje.

Invarianty: po každé iteraci platí
$ab \equiv x^2 \pmod{p}, o(y) = 2^r, b \in \langle y \rangle$.

1. Vol $z_0 \in \mathbb{Z}_p^*$ náhodně. Pokud $z_0^{\frac{p-1}{2}} \bmod p \neq 1$ polož $z \leftarrow z_0^q \bmod p$, jinak vol z_0 znova.
2. $y \leftarrow z$, $r \leftarrow e$, $b \leftarrow a^q \bmod p$, $x \leftarrow a^{\frac{q+1}{2}} \bmod p$
3. Najdi nejmenší $m \in \mathbb{N}_0$, pro které bude $b^{2^m} \bmod p = 1$. Pokud $m = 0$, vypiš x a skonči. Pokud $m = r$, skonči s tím, že úloha nemá řešení.
4. $t \leftarrow y^{2^{r-m-1}} \bmod p$, $y \leftarrow t^2 \bmod p$, $r \leftarrow m$, $x \leftarrow xt \bmod p$, $b \leftarrow by \bmod p$. Jdi na krok **3.**

Poznámky ke složitosti

Krok 1.: Pravděpodobnost úspěchu $\frac{1}{2}$, složitost jedné iterace $O(\log^3(p))$.
Krok 2.: Složitost $O(\log^3(p))$.
Krok 3.: Implementujeme např. takto

Vstup: $b \in \langle z \rangle$

Výstup: nejmenší m pro které $b^{2^m} \bmod p = 1$

$m := 0$, $u := b$

while $(b \neq 1)$ **do**

$u := u^2 \bmod p$
$m := m + 1$

return m

Máme nejvýše $e \leq \log(p-1)$ iterací každá v čase $O(\log^2(p))$.
Krok 4.: Umocnění v čase $O(\log^3(p))$ zbytek v čase $O(\log^2(p))$.
Počet opakování kroků 3. a 4. je omezen číslem $e \leq \log(p-1)$.
Tedy odhad složitosti algoritmu je $O(\log^4(p))$.

Konec šesté přednášky

Děkuji za pozornost.