Číselné algoritmy

Kořeny polynomů v $\mathbb{Z}_p[x]$, odmocňování v $\mathbb{Z}_N$

19. 4. 2021

Kvadratické rovnice nad $\mathbb{F}_p$

Lineární rovnice $ax + b = 0, a, b \in \mathbb{F}_p, a \neq 0$ vyřešíme rozšířeným Euklidovým algoritmem: $x = -\frac{b}{a}$.
Kořeny kvadratické rovnice $ax^2 + bx + c = 0, a, b, c \in \mathbb{F}_p, a \neq 0$ a $p \in \mathbb{P}$ liché lze hledat pomocí Tonelliho-Shanksova algoritmu.

$$x^2 + \frac{b}{a}x + \frac{c}{a} = (x + \frac{b}{2a})^2 - \frac{b^2}{4a^2} + \frac{c}{a} = 0\,.$$

$$x_{1,2} = -\frac{b}{2a} \pm \frac{\sqrt{b^2 - 4ac}}{2a}\,.$$

Pro $D = b^2 - 4ac$ řešíme kongruenci $x^2 \equiv D \pmod{p}$, která má v $\mathbb{Z}_p$ $0, 1$ nebo 2 řešení. Pomocí těchto řešení dostaneme $0, 1$ nebo 2 řešení kvadratické rovnice.

Algoritmus pro hledání kořenů $P \in \mathbb{F}_p[x]$

Vstup: Liché prvočíslo p, nenulový polynom $P(x) \in \mathbb{F}_p[x]$

Výstup: $K = \{r \in \mathbb{F}_p \mid P(r) = 0\}$

0. $K \leftarrow \emptyset$
1. $A(x) \leftarrow \mathrm{NSD}(x^p - x, P(x))$, pokud $A(0) = 0$, pak $K \leftarrow K \cup \{0\}$ a $A(x) \leftarrow A(x)/x$.
2. pokud $\deg(A) = 0$, konec; pokud $\deg(A) = 1, 2$ spočti kořeny metodou popsanou výše a přidej je do K, konec
3. zvol náhodně $a \in \mathbb{F}_p$ a spočti $B(x) \leftarrow \mathrm{NSD}((x+a)^{\frac{p-1}{2}} - 1, A(x))$; proces opakuj dokud je $\deg(B(x)) = 0$ nebo $\deg(B(x)) = \deg(A(x))$
4. zavolej rekurzivě algoritmus pro polynomy $B(x)$ a $A(x)/B(x)$, $K \leftarrow K \cup K_1 \cup K_2$, kde K_1 je množina kořenů $B(x)$ a K_2 je množina kořenů $A(x)/B(x)$.
5. return K

Komentář k algoritmu

Krok 1. Připomeňme, že $x^p - x = \prod_{c \in \mathbb{F}_p}(x - c)$, takže $\mathrm{NSD}(x^p - x, P(x)) = \prod_{c \in K}(x - c)$, kde K je hledaná množina všech kořenů polynomu $P(x)$.

Krok 3. Označme L množinu všech kořenů polynomu $A(x)$. Pro zvolené $a \in \mathbb{F}_p$ je $\mathrm{NSD}((x + a)^{\frac{p-1}{2}} - 1, A(x)) = \prod_{c \in L'}(x - c)$, kde $L' = \{c \in L \mid c + a \text{ je nenulové kvadratické reziduum modulo } p\}$.

Tento způsob rozkládání funguje jako heuristika, pomocí které se snažíme aby stupně $B(x)$ a $A(x)/B(x)$ byly zhruba stejně velké.

Heuristická úvaha k úspěšnosti volby a

Zamysleme se ještě nad pravděpodobností úspěchu v bodě 3. Necht' $k_1, \ldots, k_n$ jsou kořeny A. Označme p_i pravděpodobnost jevu X_i='$a + k_i$ je kvadratické reziduum', pro velká p je p_i zhruba $1/2$. Budeme předpokládat, že jevy X_i jsou nezávislé (intuitivně je tento předpoklad dost problematický).
S tímto dodatečným předpokladem pak máme pravděpodobnost selhání přibližně $\frac{1}{2^{n-1}}$.

Odmocňování v $\mathbb{Z}_{p^k}$, $p \in \mathbb{P}$ liché

Předpokládejme, že n je tvaru p^k, kde p je liché prvočíslo $k \in \mathbb{N}$.
Problém umíme vyřešit pro $k = 1$.
Necht' tedy $k \geq 2$, $a \in \mathbb{Z}_{p^k}$, $\mathrm{NSD}(a, p) = 1$.
Chceme najít x tak, aby $x^2 \equiv a \pmod{p^k}$.
Předpokládejme, že máme $x' \in \mathbb{Z}$, pro které je
$x'^2 \equiv a \pmod{p^{k-1}}$. Použijeme metodu, která nápadně připomíná Henselovo zdvihání.

Henselovo zdvihání

Budeme hledat řešení tvaru $x' + p^{k-1}z$, kde z zvolíme tak, aby to vyšlo. Platí

$$(x'+p^{k-1}z)^2 = x'^2+2p^{k-1}x'z+p^{2(k-1)}z^2 \equiv x'^2+2p^{k-1}x'z \pmod{p^k}$$

$$x'^2 + 2p^{k-1}x'z = a + (x'^2 - a) + 2p^{k-1}x'z$$

Z předpokladu je $x'^2 - a = p^{k-1}y$ pro nějaké $y \in \mathbb{Z}$. Potřebujeme zvolit z tak, aby p dělilo $y + 2x'z$, což lze, protože p je liché a x' musí být nesoudělné s p. Pak stačí položit $z = -y.(2x')^{-1}$, kde výraz počítáme v p-prvkovém tělese.

Algoritmus pro $x^2 \equiv a \pmod{p^k}$, p liché

Vstup: $p \in \mathbb{P}$ liché $k \in \mathbb{N}$, $a \in \mathbb{Z}^*_{p^k}$

Výstup: $x \in \mathbb{Z}_{p^k}, x^2 \equiv a \pmod{p^k}$, nebo 'nemá rešení'

1. Najdi $z_0 \in \mathbb{Z}_p$, $z_0^2 \equiv a \pmod{p}$. Pokud neexistuje, vypiš 'nemá řešení' a konec

2. $x := z_0$

3. **for** $i = 1$ to $k - 1$ **do**

Urči $t \in \mathbb{Z}_p$ tak, aby $2xt \equiv 1 \pmod{p}$

$y := (\frac{x^2 - a}{p^i}) \bmod p$

$z := -yt \bmod p$

$x := x + p^i z$

4. **return** x

Poznámka k algoritmu

Z předchozích úvah je jasné, že v $\mathbb{Z}_{p^k}$ má kongruence $x^2 \equiv a \pmod{p^k}$ řešení právě tehdy, když je řešitelná kongruence $x^2 \equiv a \pmod{p}$. Navíc v $\mathbb{Z}_{p^k}$ má kongruence $x^2 \equiv a \pmod{p^k}$ bud' 0 nebo 2 řešení.

Případ složeného modulu

Předpokládejme, že $n = p_1^{k_1} \cdots p_l^{k_l}$, kde $p_1, \ldots, p_l$ jsou různá prvočísla a $k_1, \ldots, k_l \in \mathbb{N}$. Podle čínské věty o zbytcích platí

$$b\colon i \mapsto (i \bmod p_1^{k_1}, \ldots, i \bmod p_l^{k_l})$$

je izomorfismus okruhů $\mathbb{Z}_n$ a $\mathbb{Z}_{p_1^{k_1}} \times \cdots \times \mathbb{Z}_{p_l^{k_l}}$.

Kongruenci $x^2 \equiv a \pmod{n}$ lze řešit takto: Pro $i = 1, \ldots, l$ spočteme $a_i := a \bmod p_i^{k_i}$. Vyřešíme kongruence $x_i^2 \equiv a_i \pmod{p_i^{k_i}}$. Pokud pro nějaké i úloha nemá řešení, pak nemá řešení ani původní úloha. V opačném případě najdeme $b^{-1}(x_1, \ldots, x_l)$.

Odmocňování a faktorizace

Z hlediska efektivity je samozřejmě problém v získání faktorizace n na součin prvočísel. Ukažme si, že pokud bychom uměli efektivně odmocnit a modulo n, pak bychom dokázali se srovnatelnou efektivitou rozbít RSA. Prvek $a \in \mathbb{Z}_n$ budeme nazývat kvadratické reziduum (modulo n), pokud má kongruence $x^2 \equiv a \pmod{n}$ řešení.

Tvrzení

Předpokládejme, že existuje deterministický algoritmus A, který pro vstup n, a, kde n je součin dvou různých lichých prvočísel a $a \in \mathbb{Z}_n$ je kvadratické reziduum modulo n, vrátí $A(a, n) \in \mathbb{Z}_n$ takové, že $A(a, n)^2 \equiv a \pmod{n}$. Pak existuje pravděpodobnostní algoritmus B, který pro $n = pq$, $p \neq q$ lichá prvočísla vrátí prvočíselného dělitele n, přičemž B má zhruba stejnou efektivitu jako A (nebudu formulovat přesněji, nepředpokládám ale, že by A mohl být řádově lepší než počítání Euklidova algoritmu pro $\mathrm{NSD}(d, n), d \in \mathbb{Z}_n$).

Důkaz tvrzení

Důkaz: Sestrojme algoritmus B, pak dokážeme, že má požadované vlastnosti.

Vstup: n, kde n je součin různých lichých prvočísel
Výstup: prvočíselný dělitel n, nebo neúspěch

1. $d \leftarrow$ náhodné číslo z $\{2, \ldots, n-1\}$
2. Spočti $\mathrm{NSD}(d, n)$, pokud je větší jak 1, vrat' $\mathrm{NSD}(d, n)$ a skonči
3. $a \leftarrow d^2$, $d' \leftarrow A(n, a)$
4. Pokud $d = \pm d' \bmod n$, skonči neúspěšně, v opačném případě vrat' $\mathrm{NSD}(d - d', n)$.

Prohlédneme si algoritmus B přes izomorfismus $b\colon \mathbb{Z}_n \to \mathbb{Z}_p \times \mathbb{Z}_q$. Necht' pro zvolené d je $b(d) = (i, j)$. Krok 2 ošetří případy kdy je $i = 0$ nebo $j = 0$, v dalším proto předpokládáme, že $i \neq 0$ a $j \neq 0$. Dále $b(a) = (i^2 \bmod p, j^2 \bmod q)$. Algoritmus A pak vrátí odmocninu a modulo n. Pak ale $b(d') = (\pm i \bmod p, \pm j \bmod p)$. Pokud je $d = d'$ nebo $d = -d' \bmod n$, končíme s neúspěchem. V opačném případě $b(d - d')$ má právě jednu souřadnici nulovou. Proto právě jedno z čísel p, q dělí $d - d'$.

dokončení důkazu

V algoritmu počítáme nejvýše 2 krát společného dělitele, jednou umocňujeme a jednou použijeme algoritmus A. Zbývá si rozmyslet, jak je to s pravděpodobností neúspěchu: Na množině $\mathbb{Z}_n^*$ zavedeme relaci $\sim$ tak, že $x \sim y$ právě pro $x^2 \equiv y^2 \mod n$. Relace $\sim$ rozdělí množinu $\mathbb{Z}_n^*$ na $(p-1)(q-1)/4$ bloků velikosti 4. Protože A je deterministický, jeho výstup je jednoznačně dán vstupem. Díky toho vidíme, že v každém bloku $\sim$ jsou právě dva prvky, pro které skončí algoritmus neúspěchem - pro blok $[x]_\sim$ jsou to prvky $A(n, x^2 \mod n)$ a $-A(n, x^2 \mod n)$. Pokud volíme $d \in \mathbb{Z}_n$ náhodně, je pravděpodobnost úspěchu za předpokladu $d \in \mathbb{Z}_n^*$ rovna 0.5, celková pravděpodobnost úspěchu bude ještě o něco větší.

Fermatova faktorizace

Mějme $N \in \mathbb{N}$ liché. Fermatova faktorizační metoda je založena na bijekci mezi množinami

$$A := \{(x, y) \mid x, y \in \mathbb{N}_0, N = x^2 - y^2\},$$

$$B := \{(p, q) \mid q \leq p \in \mathbb{N}, N = pq\}$$

Prvku $(x, y) \in A$ přiřadíme $(x + y, x - y) \in B$,
naopak prvku $(p, q) \in B$ přiřadíme prvek $(\frac{p+q}{2}, \frac{p-q}{2}) \in A$.
Fermatova faktorizační metoda se snaží číslo na vstupu vyjádřit jako rozdíl dvou čtverců.

Princip Fermatovy faktorizace

Vstup: $1 < N \in \mathbb{N}$ liché

Výstup: vlastní dělitel N nebo $N \in \mathbb{P}$

1. **for** $x = \lceil \sqrt{N} \rceil$ to $\frac{N+1}{2}$ **do**
   $y := \lfloor \sqrt{x^2 - N} \rfloor$
   if $N = x^2 - y^2$ **then break**
2. **if** $x < \frac{N+1}{2}$ **then return** $(x + y, x - y)$
3. **return** '$N \in \mathbb{P}$'

Pokud $N \notin \mathbb{P}$, je $N = pq$ pro $2 < q \leq p$. Pak

$$\frac{N+1}{2} = \frac{pq+1}{2} > \frac{p+p+1}{2} > \frac{p+q}{2}$$

V takovém případě cyklus v kroku 1. skončí dříve než x nabude hodnoty $\frac{N+1}{2}$

Složitost Fermatovy faktorizace

Složitostí se zabývat nebudeme, v nejhorším případě ($N = 3p$, $3 < p \in \mathbb{P}$) bude krok 1. končit při $x = \frac{p+3}{2} \approx \frac{N}{6}$. Ohad složitosti by pak vyšel hůř než zkusmé dělení.
Algoritmus je ale použitelný pro vstupy typu $N = pq$, kde $p, q \in \mathbb{P}$ a $|p - q|$ je malé.
Optimalizací algoritmu a kombinováním Fermatovy faktorizace a zkusmého dělení lze dosáhnout faktorizačního algoritmu se složitostí $O(N^{\frac{1}{4}}\mathrm{Poly}(\log(N))$.

Konec 7. přednášky

Děkuji za pozornost.