Číselné algoritmy

Kvadratické síto

17. 5. 2021

Kvadratické síto - úvod

- Autor C. Pomerance (1981)
- Lze chápat jako instanci Dixonovy faktorizace
- Způsob generování relací umožňuje hledat hladké relace pomocí prosívání
- V praxi stále nejlepší algoritmus pro faktorizaci čísel, které mají 80 - 100 cifer
- V roce 1994 faktorizován RSA-129, v současnosti nejdelší číslo faktorizované pomocí QS RSA-140.

Základní verze kvadratického síta

Pro $N \in \mathbb{N}$ na vstupu definujeme polynom
$Q(x) := (x + \lfloor\sqrt{N}\rfloor)^2 - N \in \mathbb{Z}[x]$.
Kromě faktorizační báze B je třeba volit také prosívací interval
$I = \{-M, \ldots, M\}$.
Zřejmě je pro každé $z \in \mathbb{Z}$

$$(z + \lfloor\sqrt{N}\rfloor)^2 \equiv Q(z) \pmod{N}.$$

Relace pro kvadratické síto jsou dvojice tvaru

$$(z + \lfloor\sqrt{N}\rfloor, Q(z)), z \in I.$$

Lze předpokládat, že $M \ll \sqrt{N}$, tedy pravé strany relací jsou řádově velké jako $\sqrt{N}$. Obecně se ale jedná o delší čísla, než se kterými pracuje algoritmus CFRAC.

Důležité pozorování

Pro každé $p \in \mathbb{P}$ a pro každé $k, z \in \mathbb{Z}$ platí

$$p \mid Q(z) \Rightarrow p \mid Q(z + kp)$$

Toto jednoduché pozorování umožňuje snadno spočíst množinu

$$\{z \in I \mid Q(z) \equiv 0 \pmod{p}\},$$

kde $p \in \mathbb{P}$.

- Určíme množinu $C_p := \{z \in \mathbb{Z}_p \mid Q(z) \equiv 0 \pmod{p}\}$. Pro malá prvočísla lze například hrubou silou, pro větší prvočísla máme například algoritmus Tonelli-Shanks. Vždy bude $|C_p| \leq 2$.
- $\{z \in I \mid Q(z) \equiv 0 \pmod{p}\} = \cup_{c \in C_p} \{c + kp \mid k \in \{\lceil -\frac{M+c}{p} \rceil, \ldots, \lfloor \frac{M-c}{p} \rfloor\}\}$

Prosívání a hrubá síla

Srovnejme tento postup s naivním přístupem, kdy pro každé $z \in I$ otestujeme, zda je $p \mid Q(z)$. Pokud bychom brali délku $|Q(z)|$ jako $\frac{1}{2}\log(N)$ bude odhad složitosti tohoto postupu asi $O(|I|\log(p)\log(N))$.
Naproti tomu prosívání potřebuje upravit koeficienty polynomu do $\mathbb{Z}_p$ a určit množinu C_p - dojdeme k odhadu $O(\log(N)\log(p) + \log^4(p))$.

Jednoduché prosívání v kvadratickém sítu

Vstup: N, I, B

Výstup: $I_0 := \{z \in I \mid Q(z) \text{ je součin prvků z } B\}$

for $z \in I$ **do** $Q[z] := Q(z)$

for $p \in B \cap \mathbb{P}$ **do**

$C := \{z \in \mathbb{Z}_p \mid Q(z) \equiv 0 \pmod{p}\}$

for $c \in C$ **do**

for $k \in \{\lceil -\frac{M+c}{p} \rceil\}, \ldots, \lfloor \frac{M-c}{p} \rfloor\}$ **do** uprav $Q[c + kp]$

return $I_0 := \{z \in I \mid |Q[z]| = 1\}$

uprav $Q[c + kp]$ znamená, že hodnotu v proměnné $Q[c + kp]$ podělíme nejvyšší možnou mocninou p.

$$Q[c + kp] := Q[c + kp]/p^{v_p(Q[c+kp])}$$

Prosívání vyšších mocnin

Možno je prosívat i vyšší mocniny prvočísel z faktorizační báze, například takto:

for $e = 1$ to $\lfloor \log_p(E) \rfloor$ **do**
  $C := \{z \in \mathbb{Z}_{p^e} \mid Q(z) \equiv 0 \pmod{p^e}\}$
  for $c \in C$ **do**
    for $k \in \{\lceil -\frac{M+c}{p^e} \rceil\}, \ldots, \lfloor \frac{M-c}{p^e} \rfloor\}$ **do**
    $Q[c + kp^e] := Q[c + kp^e]/p$

$E := \max\{|Q(z)| \mid z \in I\}$.
Pro lichá p můžeme množinu C v nové iteraci vždy přepočítat pomocí Henselova zdvihnutí.

Volby parametrů (*)

Pro představu uvádíme doporučované volby parametrů podle knihy J. Buchmann: Introduction to Cryptography

#cifer N	80	100	120
$\|B\|$	15 000	51 000	245 000
$\|I\|$	6 000 000	14 000 000	26 000 000

Pro praktické využití algoritmu je třeba prosívací fázi urychlit i za cenu, že na výstup nedostaneme všechny hladké relace. Zpravidla se počítá pouze přibližně, snahou je vytipovat relace, které by mohly být hladké. Z těchto vytipovaných relací pak určíme, které jsou opravdu hladké.

Prosívání v kvadratickém sítu, přibližné

Vstup: N, I, B

Výstup: $I_0 \subseteq \{z \in I \mid Q(z) \text{ je součin prvků z } B\}$

zvol práh T (typicky dle doporučení z literatury)

for $z \in I$ **do** $Q[z] := \#$ bitů reprezentujících $Q(z)$

for $p \in B \cap \mathbb{P}$ **do**

$C := \{z \in \mathbb{Z}_p \mid Q(z) \equiv 0 \pmod{p}\}$

for $c \in C$ **do**

for $k \in \{\lceil -\frac{M+c}{p} \rceil\}, \ldots, \lfloor \frac{M-c}{p} \rfloor\}$ **do** uprav $Q[c + kp]$

$K := \{z \in I \mid Q[z] \leq T\}$

return $I_0 := \{z \in K \mid Q[z] \text{ je součin prvků z } B\}$

V tomto případě uprav $Q[c + kp]$ znamená
$Q[c + kp] := Q[c + kp] - \#$ bitů reprezentujících p.

Hodnota T

Tato verze prosívání nahrazuje operaci dělení výpočetně jednodušší operací odečítání. Cena, kterou za urychlení platíme, je ztráta přesnosti.
Klíčová je proto volba prahu T. Příliš velká volba T povede na velkou množinu K, ze které bude stále obtížné určit hladké relace. Naopak příliš malá volba T pravděpodobně povede k tomu, že neodhalíme dostatečný počet hladkých relací.
Konkrétní příklady nastavení hodnoty T lze najít v textu E. Landquist: The Quadratic Sieve Factoring Algorithm (okaz je na webu).

Varianta s velkými prvočísly

Připomeňme, že relace (x, y) se nazývá *parciální*, pokud y je součin prvků B a jednoho prvočísla mimo faktorizační bázi. Prosívání lze upravit tak, aby hledalo kromě hladkých relací také parciální relace. Nechť $p_{\max}$ je nejvyšší prvočíslo v $B = \{-1, 2, 3, 5, \ldots, p_{\max}\}$. Zvolíme $q \in (p_{\max}, p_{\max}^2)$. Pokud po vydělení y prvočísly z B v nejvyšších možných mocninách a dostaneme výsledek y' splňující $|y'| \leq q$, pak je

- buď $y' = \pm 1$, pak (x, y) je hladká relace
- nebo $p_{\max} < |y'| \in \mathbb{P}$, pak (x, y) je parciální relace a $|y'|$ je 'velké prvočíslo' této relace

Jednoduché prosívání pro variantu kvadratického síta s velkými prvočísly

Vstup: N, I, B, q, $B = \{-1, 2, 3, \ldots, p_{\max}\}$, $q \in (p_{\max}, p_{\max}^2)$

Výstup: $I_0 := \{z \in I \mid (z + \lfloor\sqrt{N}\rfloor, Q(z))$ je hladká nebo parciální relace $\}$

for $z \in I$ **do** $Q[z] := Q(z)$

for $p \in B \cap \mathbb{P}$ **do**

$C := \{z \in \mathbb{Z}_p \mid Q(z) \equiv 0 \pmod{p}\}$

for $c \in C$ **do**

for $k \in \{\lceil -\frac{M+c}{p} \rceil\}, \ldots, \lfloor \frac{M-c}{p} \rfloor\}$ **do** uprav $Q[c + kp]$

return $I_0 := \{z \in I \mid |Q[z]| \leq q\}$

uprav $Q[c + kp]$ opět znamená vydělení hodnoty v proměnné nejvyšší možnou mocninou p.

Zpracování parciálních relací

Před spuštěním lineární fáze kvadratického síta je třeba zpracovat parciální relace.
Pro velké prvočíslo p označíme $R_p = \{(x, y) \mid (x, y)$ je nalezená parciální relace a $p \mid y\}$.
Prvky v množině R_p spárujeme a pomocí některých párů vytvoříme nové řádky pro lineární fázi.
Řekněme, že $R_p = \{(x_1, y_1), (x_2, y_2), (x_3, y_3)\}$. Vezmeme dvojici parciálních relací $(x_1, y_1), (x_2, y_2)$. Pak

$$x_1^2 x_2^2 \equiv y_1 y_2 \pmod{N}, y_1 y_2 = p^2 \prod_{b \in B} b^{e_b}$$

Do matice pak můžeme přidat nový řádek odpovídající dvojici $(x_1, y_1), (x_2, y_2)$. V tomto řádku bude ve sloupci indexovaném prvkem $b \in B$ hodnota $e_b \bmod 2$.
Podobně bychom vytvořili další řádek matice z dvojice relací $(x_1, y_1), (x_3, y_3)$.

Triviální lineární závislosti způsobené párováním

Teoreticky lze vytvořit řádek také z relací $(x_2, y_2), (x_3, y_3)$. Snadno se ale přesvědčíme, že ten by byl součtem předchozích dvou a lineární závislost těchto tří řádků by dala špatné řešení. Obecně chceme mít prostor špatných řešení co nejmenší, proto bychom přidali pouze dva řádky vytvořené parciálními relacemi z R_p.

MPQS

Doposud jsme pracovali s kvadratickým sítem, kde byly relace generovány jedním polynomem $Q(x)$.
P. Montgomery navrhl variantu kvadratického síta, které využije více polynomů. Tento návrh je umožňuje lepší paralelizaci kvadratického síta, dále je možno zkrátit prosívací interval. Nevýhodou je pak čas strávený inicializací polynomů, navíc pro každý polynom a každé prvočíslo z faktorizační báze hledáme kořeny polynomu modulo p.

Polynomy pro MPQS

Uvažujeme polynomy tvaru $ax^2 + 2bx + c$, kde $a \in \mathbb{N}$, $b, c \in \mathbb{Z}$, $b^2 - ac \in \mathbb{N}$, $N \mid b^2 - ac$.
Pak $aQ(x) = a^2x^2 + 2abx + ac = (ax + b)^2 - (b^2 - ac)$. Pokud I_Q je prosívací interval polynomu Q, dostáváme relace tvaru

$$(az + b, aQ(z)), z \in I_Q$$

Necht' $M \in \mathbb{N}$ je takové, že $I_Q = \{\lfloor -\frac{b}{a} \rfloor - M, \ldots, \lfloor -\frac{b}{a} \rfloor + M\}$.
Hodnoty a, b, c se snažíme nastavit tak, aby $\min_{z \in I_Q} aQ(z)$ a $\max_{z \in I_Q} aQ(z)$. měly zhruba stejnou absolutní hodnotu.
Protože je $\min_{z \in I_Q} aQ(z) \approx -(b^2 - ac)$,
$\max_{z \in I_Q} aQ(z) \approx (aM)^2 - (b^2 - ac)$, rovnost

$$(b^2 - ac) \approx (aM)^2 - (b^2 - ac)$$

vede k volbě $a \approx \frac{\sqrt{2(b^2 - ac)}}{M}$. Na takto voleném prosívacím intervalu je maximální hodnota $|Q(z)|$ asi $M\sqrt{\frac{b^2 - ac}{2}}$. Pokud a, b, c volíme tak, aby $N = b^2 - ac$, jsou hodnoty $|Q(z)|$ na I_Q srovnatelné s hodnotami plynomu $(x + \lfloor \sqrt{N} \rfloor)^2 - N$ na intervalu $\{-M, \ldots, M\}$.

Inicializace polynomu pro MPQS

- Pro dané M udávající délku prosívacího intervalu zvolíme $a \in \mathbb{P}$, $a \approx \frac{\sqrt{2N}}{M}$, $(\frac{N}{a}) = 1$
- určíme $b \in \mathbb{Z}_a$ tak, aby $b^2 \equiv N \pmod{a}$
- dopočteme $c = \frac{b^2 - N}{a}$
- prvočíslo a přidáme do faktorizační báze

MPQS pár poznámek

Jak bylo zmíněno, pro každý polynom Q a každé prvočíslo p z faktorizační báze potřebujeme najít $\{c \in \mathbb{Z}_p \mid Q(c) \equiv 0 \pmod{p}\}$.
Pokud máme vždy $b^2 - ac = N$, je výhodné spočíst nejprve odmocninu z N v $\mathbb{Z}_p$ a pomocí této odmocniny dopočíst kořeny jednotlivých polynomů.
Dále se využívá inicializace více polynomů se stejným vedoucím koeficientem. Postup upravíme tak, že a volíme ve tvaru $a = p_1 p_2 \dots p_t$, kde $2 < p_1 < p_2 < \cdots < p_t$ a $(\frac{N}{p_i}) = 1$ pro každé p_i.
Kongruence $b^2 \equiv N \pmod{a}$ má pak 2^t různých řešení v $\mathbb{Z}_a$, každé z nich lze použít pro inicializaci polynomu pro MPQS.

Konec

Děkuji za pozornost.