

Číselné algoritmy

CFRAC

10. 5. 2021

CFRAC - úvod

- ▶ Idea využití řetězových zlomků pro faktorizační algoritmy je poměrně stará (např. Lehmer - Powers 1931)
- ▶ Počítačová implementace algoritmu - Brillhart-Morrison 1975, faktorizace čísla $F_7 = 2^{2^7} + 1$
- ▶ Z našeho pohledu jde o příklad algoritmu založeného na Dixonově faktorizaci

Řetězový rozvoj $\sqrt{N}$ shrnutí

Mějme $N \in \mathbb{N}$, $\sqrt{N} \notin \mathbb{Q}$.

Položme $\alpha_0 = \sqrt{N}$, $a_0 = \lfloor \alpha_0 \rfloor$, $\alpha_1 = (\alpha_0 - a_0)^{-1}$, $a_1 = \lfloor \alpha_1 \rfloor, \dots$,
 $\alpha_i = (\alpha_{i-1} - a_{i-1})^{-1}$, $a_i = \lfloor \alpha_i \rfloor, \dots$

Pak $\sqrt{N} = \alpha_0 = [a_0; a_1, a_2, \dots]$.

Čísla α_i , lze vyjádřit ve tvaru $\alpha_i = \frac{R_i + \sqrt{N}}{S_i}$, kde $R_i \in \mathbb{Z}$ a $S_i \in \mathbb{N}$,
přičemž R_i, S_i lze počítat rekurzivně

$$R_0 = 0, S_0 = 1, R_{i+1} = a_i S_i - R_i, S_{i+1} = \frac{N - R_{i+1}^2}{S_i}, a_i = \lfloor \frac{R_i + \lfloor \sqrt{N} \rfloor}{S_i} \rfloor$$

Jsou-li dále $p_{-2}, p_{-1}, p_0, p_1, \dots$ $q_{-2}, q_{-1}, q_0, q_1, \dots$ posloupnosti
dané vztahy

$$p_{-2} = 0, p_{-1} = 1, p_i = a_i p_{i-1} + p_{i-2}$$

$$q_{-2} = 1, q_{-1} = 0, q_i = a_i q_{i-1} + q_{i-2}$$

$$\text{je } [a_0; a_1, \dots, a_n] = \frac{p_n}{q_n}$$

Generátor relací pro CFRAC

Pro každé $n \in \mathbb{N}$ je $p_{n-1}^2 \equiv (-1)^n S_n \pmod{N}$.

CFRAC tedy využívá relace tvaru $(p_{n-1}^2 \pmod{N}, (-1)^n S_n)$

V principu tedy můžeme napsat základní verzi algoritmu CFRAC.

Podívejme se ale nejprve na drobná vylepšení algoritmu pro počítání řetězového rozvoje $\sqrt{N}$.

Výpočet a_n , R_{n+1}

Označme $g := \lfloor \sqrt{N} \rfloor$. Známe-li R_n, S_n , získáme a_n pomocí celočíselného dělení. Pro další postup se bude hodit i zbytek po dělení, který označíme r_n . Tedy

$$R_n + g = a_n S_n + r_n, r_n \in \{0, 1, \dots, S_n - 1\}$$

Dále je $R_{n+1} = a_n S_n - R_n$, proto

$$R_{n+1} + g = a_n S_n + g - R_n = (R_n + g - r_n) + g - R_n = 2g - r_n$$

$$R_{n+1} + g = 2g - r_n$$

Výpočet S_{n+1}

Lemma

Při zavedeném značení pro $n \geq 1$ platí

$$S_{n+1} = S_{n-1} + a_n(r_n - r_{n-1})$$

Proof.

Máme $S_{n+1} = \frac{N - R_{n+1}^2}{S_n}$, $R_{n+1} = a_n S_n - R_n$.

Proto

$$N - R_{n+1}^2 = N - a_n^2 S_n^2 + 2a_n R_n S_n - R_n^2 = S_n S_{n-1} + S_n a_n (2R_n - a_n S_n).$$

$$S_{n+1} = S_{n-1} + a_n (2R_n - a_n S_n) = S_{n-1} + a_n (R_n + R_n - a_n S_n) =$$

$$S_{n-1} + a_n (g - r_{n-1} + r_n - g) = S_{n-1} + a_n (r_n - r_{n-1}),$$

jak se mělo dokázat. □

CFRAC - popis základní verze algoritmu

Vstup: $N \in \mathbb{N}$ složené, $\sqrt{N} \notin \mathbb{Q}$.

Výstup: vlastní dělitel N , nebo neúspěch

1. Zvolíme faktorizační bázi B
2. $S_0 := 1, p_{-1} := 0, r_0 := 0, g := \lfloor \sqrt{N} \rfloor$
3. $S_1 := N - g^2, R'_0 := g, a_0 := g, R'_1 := 2g, n := 1$
4. **while** (nemáme dost hladkých relací) **do**
 - $a_n := R'_n \operatorname{div} S_n, r_n := R'_n \bmod S_n$
 - $p_n := a_n p_{n-1} + p_{n-2} \bmod N$
 - $R'_{n+1} := 2g - r_n$
 - $S_{n+1} := S_{n-1} + a_n(r_n - r_{n-1})$
 - Je-li S_n součin prvků z B přidej $(p_{n-1}, (-1)^n S_n)$ do seznamu hladkých relací.
 - $n := n + 1$

CFRAC - dokončení popisu základní verze algoritmu

5. Přejdi do lineární fáze algoritmu. Z nalezených hladkých relací $(x_1, y_1), \dots, (x_k, y_k)$ urči množinu $I \subseteq \{1, \dots, k\}$, pro kterou bude $\prod_{i \in I} y_i = y^2$ pro nějaké $y \in \mathbb{Z}$. Polož $x := \prod_{i \in I} x_i$. Pak $x^2 \equiv y^2 \pmod{N}$.
6. $d := \text{NSD}(x \pm y, N)$.
7. **if** $d \in \{1, N\}$ **then return** neúspěch **else return** d

Poznámka k volbě B

Protože $(-1)^n S_n < 0$ pro každé liché n , je $-1 \in B$.

Dále předpokládáme, že prvočísla v B jsou mnohem menší než nejmenší prvočíselný dělitel N . Speciálně žádné prvočísllo z B nedělí N .

Obecně do faktorizační báze má smysl dávat prvočísla, která dělí pravé strany uvažovaných relací. Předpokládejme, že pro nějaké $n \in \mathbb{N}$ a $p \in \mathbb{P}$ je $p \mid S_n$. Podívejme se na vztah

$$p_{n-1}^2 - Nq_{n-1}^2 = (-1)^n S_n$$

Připomeňme, $\text{NSD}(p_{n-1}, q_{n-1}) = 1$. Pokud $p \mid S_n$, nebude $p \mid q_{n-1}$. Pokud navíc předpokládáme, že $p \nmid N$, nebude pro $p \mid S_n$ ani $p \mid p_{n-1}$. Z kongruence

$$p_{n-1}^2 \equiv Nq_{n-1}^2 \pmod{p}$$

pak dostaneme $\left(\frac{N}{p}\right) = 1$.

Prvočísllo p proto dáme do faktorizační báze pouze pokud splňuje $\left(\frac{N}{p}\right) = 1$. .

Experimenty z článku Brillharta a Morrisona

Ve své práci Brillhart a Morrison navrhují následující volby B .

- ▶ pro $N \leq 10^{20}$, $|B \cap \mathbb{P}| = 60$
- ▶ pro N mající 24 nebo 25 cifer $|B \cap \mathbb{P}| = 200$
- ▶ pro N mající 37 nebo 38 cifer $|B \cap \mathbb{P}| = 600$

Tyto hodnoty jsou navrženy pro verzi CFRACu, která zpracovává parciální relace.

Důležité tvrzení:

Tvrzení

Při zavedeném značení: Proměnné R'_n, S_n, a_n, r_n nabývají v průběhu algoritmu pouze hodnot v intervalu $\{0, 1, 2, \dots, \lfloor 2\sqrt{N} \rfloor\}$

Proof.

Připomeňme, že $S_n > 0$ pro každé $n \in \mathbb{N}_0$. Pak

$$N - R_{n+1}^2 = S_n S_{n+1} > 0$$

implikuje $|R_n| \leq \lfloor \sqrt{N} \rfloor$ pro $n \geq 1$ (ale pro $R_0 = 0$ nerovnost platí také). Takže $R'_n \in \{0, 1, \dots, 2\lfloor \sqrt{N} \rfloor\}$.

Dále si všimneme, že a_n, S_n, r_n jsou vždy nezáporná. Ze vzorečku pro dělení se zbytkem

$$R'_n = a_n S_n + r_n$$

máme $a_n, S_n, r_n \leq 2\lfloor \sqrt{N} \rfloor$.

Proč je toto tvrzení důležité

Pro algoritmy vycházející z Dixonovy faktorizace je důležité, aby se mezi generovanými relacemi co nejčastěji vyskytovaly hladké (případně parciální) relace.

To lze samozřejmě ovlivnit volbou faktorizační báze B . Na druhou stranu ale potřebujeme nasbírat alespoň $|B| + 1$ hladkých relací.

Je proto vhodné, aby absolutní hodnoty čísel na pravých stranách generovaných relací byly malé.

Pravé strany relací CFRACu jsou v intervalu $\{-2\lfloor\sqrt{N}\rfloor, \dots, 2\lfloor\sqrt{N}\rfloor\}$, kde $2\sqrt{N} \ll N$.

Pro srovnání generátor, který vrací relace $(x, x^2 \bmod N)$ pro náhodně volená x může za určitých okolností vrátit i relaci $(x, N - 1)$.

Periodicita řetězového rozvoje a Pellova rovnice (*)

Pellovou rovnicí se rozumí Diofantická rovnice

$$x^2 - Ny^2 = 1$$

Chceme najít netriviální celočíselné řešení této rovnice.

Lze ukázat, že pro $N \geq 5$ a $x, y \in \mathbb{N}$ splňující $x^2 - Ny^2 = \pm 1$ je $\frac{x}{y}$ konvergent řetězového rozvoje $\sqrt{N}$.

Na cvičení jsme si ukázali, že existují $a_0, a_1, \dots, a_n \in \mathbb{N}$ tak, že

$$\sqrt{N} = [a_0; \overline{a_1, a_2, \dots, a_n, 2a_0}]$$

Jak najít řešení Pellovy rovnice (*)

Věta

Necht' $\sqrt{N} = [a_0; \overline{a_1, a_2, \dots, a_n, 2a_0}] = [a_0; a_1, a_2, \dots]$. Označme $p_{-2}, p_{-1}, p_0, \dots, q_{-2}, q_{-1}, q_0, \dots$ posloupnosti definované vztahy

$$p_{-2} = 0, p_{-1} = 1, p_i = a_i p_{i-1} + p_{i-2}, i \in \mathbb{N}_0$$

$$q_{-2} = 1, q_{-1} = 0, q_i = a_i q_{i-1} + q_{i-2}, i \in \mathbb{N}_0$$

Necht' $k = m(n+1) - 1$, kde $m \in \mathbb{N}$. Pak

$$p_k^2 - Nq_k^2 = (-1)^{k+1}.$$

Důkaz je podobný důkazu věty $p_{n-1}^2 - Nq_{n-1}^2 = (-1)^n S_n$

Poznámka: Lze ukázat, že při použití nejkratší periody ($m = 1$) dostaneme netriviální řešení rovnice $x^2 - Ny^2 = \pm 1$, kde $x, y \in \mathbb{N}$ jsou nejmenší možná.

Příklad na závěr (*)

Pro $N = 13$ je $\sqrt{13} = [3; \overline{1, 1, 1, 1, 6}]$ (nejkratší perioda má délku 5)
Následující tabulka zachycuje prvních pár konvergentů rozvoje $\sqrt{13}$

ℓ	-1	0	1	2	3	4	5	6	7	8	9
a_ℓ	—	3	1	1	1	1	6	1	1	1	1
p_ℓ	1	3	4	7	11	18	119	137	256	393	649
q_ℓ	0	1	1	2	3	5	33	38	71	109	180

Pak pro $m = 1$, $m(n+1) - 1 = 4$ máme $18^2 - 13 * 5^2 = -1$
pro $m = 2$, $m(n+1) = 9$ máme $649^2 - 13 * 180^2 = 1$

To je pro dnešek vše

Děkuji za pozornost.