Théorie Algorithmique des Nombres

Méthodes sous-exponentielles

David Kohel

09/11/2020

Méthodes sous-exponentielles.

Quadratic sieve (crible quadratique)
– methode pour factorisation des entiers
– introduit par Carl Pomerance 1981

Généralisation : crible algébrique (General number field sieve).

Données d'entrée : n (composé)

Remarque : Facile à identifier des premiers parmi les entiers.
– algorithmes probabilistes efficaces pour reconnaître des premiers.

Complexité des méthodes sous-exponentielles

- Crible quadratique : $L_n(1/2, 1) = \exp\left((1+o(1))(\log n)^{1/2}(\log\log n)^{1/2}\right)$
- Crible algébrique :

$$L_n(1/3, \sqrt[3]{64/9}) = L_n(\lambda, c), \text{ où}$$

$$L_n(\lambda, c) = \exp\left((c+o(1))(\log n)^{\lambda}(\log\log n)^{1-\lambda}\right)$$

$$= \begin{cases} \exp\left((c+o(1))\log\log(n)\right) = (\log n)^{c+o(1)} & \text{si } \lambda = 0 \\ n^{c+o(1)} \text{ si } \lambda = 1. \end{cases}$$

Alors $L_\lambda(\lambda, c)$ est une fonction, en $\log x$, qui est : 1/ polynôme si $\lambda = 0$,
2/ exponentiel si $\lambda = 1$,
et dite sous-exponentielle si $0 < \lambda < 1$.
La valeur λ permet d'interpoler entre les classes de fonctions polynômes et exponentielle (avec la famille des fonctions $L_\lambda(\lambda, c)$).

N.B. $L_\lambda(\lambda, c) = L_\lambda(\lambda, 1)^c$, c.à.d. que c est l'exposant dans la classe pour λ fixé.

Crible quadratique.

Objectif. (i) Construire des tuples $(a_j, (e_{0j}, e_{1j}, \dots, e_{nj}))$ tel que relations

$$a_j^2 \equiv \prod_{i=0}^{n} p_i^{e_{ij}} \bmod n \quad \text{où} \quad p_i \in \{\underbrace{-1}_{p_0}, 2, 3, \dots, p_n\} = \mathcal{B}.$$

(ii) Puis ...

on veut trouver un produit

$$a^2 = \prod_{j\in J} a_j^2 \equiv \prod_{j\in J}\left(\prod_{i=0}^{n} p_i^{e_{ij}}\right)$$

$$= \prod_{i=0}^{n} p_i^{2d_i} = b^2, \text{ où } b = \prod_{i=0}^{n} p_i^{d_i}.$$

Ensuite, comme $a^2 \equiv b^2 \bmod n$, on factorise n par :

$$n = \text{pgcd}(a-b, n)\,\text{pgcd}(a+b, n).$$

[En supposant que $(a-b, a+b, n) = 1$.]

Astuce : Si on choisit $(e_0, e_1, \dots, e_n)$ au hazard, la probabilité de trouver :

$$a^2 \equiv \prod_{i=0}^{n} p_i^{e_i} \quad \text{(un carré)}$$

sera plus grand si $\prod_{i=0}^{n} p_i^{e_i} \bmod n$ est plus petit.

Ou inversement, si on choisit a et on cherche un factorisation $a^2 \bmod n$ dans la base $\mathcal{B} = \{-1, 2, 3, \dots, p_n\}$ on veut $a \sim \sqrt{kn}$. En effet...

Donc on choisit :

$a = x + \lfloor \sqrt{kn} \rfloor$, et alors

on a $$a^2 = x^2 + 2x\lfloor \sqrt{kn} \rfloor + \lfloor \sqrt{kn} \rfloor^2 \in \mathbb{N}$$
$$= z^2 + 2z\sqrt{kn} + kn \in \mathbb{R}$$

où $x + \lfloor \sqrt{kn} \rfloor = z + \sqrt{kn}$ avec $z \in \mathbb{R}$, tel que $x - z = \sqrt{kn} - \lfloor \sqrt{kn} \rfloor < 1$.

Par conséquent

$$a^2 = z^2 + 2z\sqrt{kn} + kn$$
$$\equiv z(z + 2\sqrt{kn}) \approx 2z\sqrt{kn}$$

si $x \in O(\sqrt{n})$. ↖ négligible

La taille de a croit bilinéairement en $x \approx z$ ($|x - z| < 1$) et en $\sqrt{k}$, fois $\sqrt{n}$. On veut x et k petit.

Crible Soit $f(x) = x^2 - kn$. Si $f(x) \equiv 0 \bmod p$ alors $f(a + lp) \equiv 0 \bmod p$.

Alors, si a_1, a_2 sont les deux racines

du polynôme $f(x) \bmod p \in \mathbb{F}_p[x]$, alors $f(a_i + lp)$, $l \in \mathbb{Z}$ est un système d'entiers congruent à $0 \bmod p$. Cette observation permet de chercher des entiers a qui satisfaient

$$f(a) = a^2 - kn \equiv 0 \bmod p_i$$

pour plusieurs p_i.

Algorithme (crible quadratique)

- Choisir un borne de friabilité B (smoothness bound) et poser

$$\mathcal{B} = \{-1\} \cup \{p_i \text{ premier} : p_j \leq B\}$$

- Déterminer $r = |\mathcal{B}| + \varepsilon$ relations: $a_j^2 \equiv \prod_{i=0}^{n} p_i^{e_{ij}}$ en utilisant un crible mod p_i
- Tabuler les relations dans un matrice:

$$\left\{\begin{bmatrix} e_{10} & e_{11} & \cdots & e_{1n} \\ e_{20} & & & \\ \vdots & & & \\ e_{r0} & & & e_{rn} \end{bmatrix}\right. = A \in \mathbb{M}_{r,n+1}(\mathbb{F}_2)$$

r relations $\geq n+1 = |\mathcal{B}| = \#$ de colonnes $= \#$ lignes

Soit $v = (b_1, \dots, b_r) \in \ker(A)$ à gauche : $v \cdot A = 0 \in \mathbb{F}_2^{n+1}$.
$\in \mathbb{F}_2^r$

- Si $v \cdot A = 0$ alors

$$\left(e_j = \sum_{i=1}^{r} b_i e_{ij}\right)_{0 \leq j \leq n} = (0, \dots, 0) \bmod 2,$$

alors il existe $(b_j \in \{0,1\} \subseteq \mathbb{Z})$,

$$d_j = \left(\sum_{i=1}^{r} b_i e_{ij}\right)/2 \in \mathbb{Z}.$$

Posons

$$a = \prod_{c_i \neq 0} a_i \quad \text{et} \quad b = \prod_{j=0}^{n} p_j^{d_j},$$

et il suit que $a^2 \equiv b^2 \bmod n$.

thm chinois

Remarque (crible).

Si a_1, a_2, a_3, a_4 sont les quatre racines de $f(x) \bmod p_j p_k$ (2 racines mod p_j × 2 racines mod p_k) alors si

$$f(a_i + l p_j^{e_j} p_k^{e_k}) \equiv f(a_i) \equiv 0 \bmod p_j^{e_j} p_k^{e_k},$$

on peut construire des a_i avec congruences $\bmod p_j^{e_j} p_k^{e_k}$ présorts. On peut également construire des relations permettant l'élimination mod 2 des exposants impairs.

Exemple. $n = 59291$

$\lfloor \sqrt{n} \rfloor = 243$ $\quad 243^2 \equiv -2^1 \cdot 11^1$

$\lfloor \sqrt{2n} \rfloor = 344$ $\quad 244^2 \equiv 5^1 \cdot 7^2$ $\quad \Big] (244 \cdot 487)^2 \equiv 5^2 \cdot 7^2$

$\lfloor \sqrt{3n} \rfloor = 421$ $\quad 487^2 \equiv 5$

$\lfloor \sqrt{4n} \rfloor = 486$ (487)

$243^2 = -2^1 \cdot 11^2$ $\quad \mathcal{B} = \{-1, 2, 5, 7, 11\}$

$244 = 5^1 \cdot 7^2$

$487 = 5^1$

$$A = \begin{matrix} -1 & 2 & 5 & 7 & 11 \end{matrix} \begin{bmatrix} 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 2 \\ 0 & 0 & 1 & 2 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix} \xrightarrow{\text{mod } 2} \begin{bmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix} \} \text{ lin. dép}$$

$v = (0,1,1)$ tel que $v \cdot A = (0\,0\,0\,0\,0)$.

Trois relations, dont deux utilisées; en générale on doit chercher plus de relations que le nombre de premiers dans la base de friabilité $\mathcal{B}$, pour assurer une dépendence.

Par conséquent, $(244 \cdot 487)^2 \equiv (5 \cdot 7)^2$,

alors $(n = 59291 = 211 \cdot 281)$:

$\text{pgcd}(244 \cdot 487 - 5 \cdot 7, n) = 211$,

$\text{pgcd}(244 \cdot 487 + 5 \cdot 7, n) = 281$.

Idée du calcul de complexité :

(i) Pour trouver de relations, dans la base de friabilité :
- On veut B aussi grand que possible.

(ii) Pour trouver un élément de $\ker(A)$, on veut la taille de la matrice assez petite :
- On veut B aussi petit que possible.

La complexité optimisant le calcul de relations et la réduction de la matrice A (pour déterminer son noyau $\ker(A)$), arrive à une solution avec

$$|B| = L_n(\lambda, c)$$

pour $\lambda = 1/2$. Complexité totale :

$$L_n(1/2, c').$$

Equilibre optimal entre (i) et (ii).