Crible Quadratique

L'algorithme de factorisation par crible quadratique a été proposée par Springer, C. Pomerance en 1984 dans sa série de livres Lecture Notes in Computer Science. C'est aujourd'hui le second algorithme le plus rapide pour factoriser les très grands nombres (derrière le crible général des corps des nombres) et le plus rapide pour factoriser les nombres qui ont moins de 100 chiffres.

L'algorithme est le suivant :

- On sélectionne une borne B qui correspond à la limite supérieure des premiers qu'on utilisera pour factoriser n.
- On calcule m polynômes de forme $X = Q(x) = x^2 - n$ avec $x = \sqrt{n} + k$, $k \in [1; m]$.
- On calcule ensuite quels X sont B-friables.
- On utilise ensuite ces X pour factoriser n en puissances de premiers inférieurs à B.

Base de friabilité

La base de friabilité $\mathcal{B}$ est l'ensemble contenant l'ensemble des premiers inférieurs à B.

Nombres B-friables

Un nombre B-friable est un nombre composé d'entier : x est B-friable si, pour P l'ensemble des premiers inférieurs à B,

$$x = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_n^{k_n}, k_i \in \mathbb{N}, p_i \in \mathcal{B}$$

Calcul des polynômes

On calcule m polynômes de forme $X = Q(x) = x^2 - n$ avec $x = \sqrt{n} + k, k \in [1; m]$.

L'idée est de calculer des polynômes avec x à peine plus grand que $\sqrt{n}$ car on a :

$$x^2 - n = k^2 + 2k\lfloor\sqrt{n}\rfloor + \lfloor n\rfloor^2 - n$$

Si k est négligeable devant $\lfloor\sqrt{n}\rfloor$, alors le terme dominant est $2k\lfloor\sqrt{n}\rfloor \approx 2k\sqrt{n}$, et plus ce terme est petit par rapport à n, plus il a de chance d'être friable.

Une fois qu'on a nos m polynômes $X_1, X_2, \ldots, X_m$, on regarde lesquels sont B-friables et on se basera sur eux pour la factorisation.

Factorisation

On a k polynômes X B-friables de la forme $X = Q(x) = x^2 - n$ avec $x = \sqrt{n} + k$, $k \in [1; m]$.

Pour factoriser, on va, pour chaque polynôme X, chercher le plus petit diviseur commun entre X et n. Comme X est friable, soit le pgcd est égal à 1 et on passe au X suivant, soit il est égal à une puissance d'un premier inférieur à B.
Dans ce cas, on peut calculer la puissance de ce premier et diviser n par le pgcd. On passe ensuite au polynôme suivant jusqu'à ce que n soit égal à 1 ou à un nombre premier, auquel cas on a fini de factoriser n et on a obtenu tous les facteurs premiers et leurs puissances.

Complexité

La complexité du crible quadratique est de l'ordre de $O(e^{\sqrt{logNloglogN}})$.

Sources :

Crible Quadratique :

Chapitre 14 - Factorisation

https://link.springer.com/chapter/10.1007/3-540-39757-4_17

http://www.ams.org/notices/199612/pomerance.pdf