# MÉTHODES DE FACTORISATION PAR CRIBLE

Ce texte est une introduction aux algorithmes de factorisation par crible.

## 1. La méthode de Fermat

Fermat a remarqué que pour trouver un facteur non-trivial d'un entier $n$ il suffit de l'écrire comme différence de deux carrés. En effet si $n = x^2 - y^2$ alors $n = (x - y)(x + y)$.

Par exemple pour factoriser $n = 152415789666102728852508 1$ on ajoute à $n$ les carrés successifs 1, 4, 9, ...et on regarde si la somme obtenue est un carré.

```
gp > n=152415789666102728852508 1
%1 = 152415789666102728852508 1
gp > for(k=1,20,if(issquare(n+k^2),print([k,sqrt(n+k^2)])))
[12, 1234567898765.000000000000000]
```

Donc $n = -12^2 + 1234567898765^2 = 1234567898753 * 1234567898777$.

Cette méthode ne fonctionne que si l'un des deux carrés est petit. Dans ce cas, on peut penser que l'autre carré est très proche de $\sqrt{n}$. On peut donc aussi bien calculer l'entier $r$ immédiatement supérieur à $\sqrt{n}$ et voir si $r^2 - n$ est aussi un carré.

```
 gp > round(sqrt(n))^2-n
%2 = 144
```

Si l'on parvient à écrire un multiple de $n$ comme différence de deux carrés, on peut encore espérer trouver un facteur non trivial de $n$. En effet, si $x^2 = y^2 \bmod n$ on peut espérer que le pgcd de $n$ et $x - y$ est non-trivial. On peut donc appliquer les calculs précédents aux premiers multiples de $n$. Cette méthode ne réussit que pour des $n$ particuliers, mais elle est efficace pour de petits $n$.

Dans le cas général, pour trouver des solutions non triviales à la congruence

$$x^2 - y^2 = 0 \bmod n$$

on ne sait pas faire mieux que de chercher des congruences entre nombres friables à un carré près, c'est-à-dire des congruences de la forme

$$\prod_i p_i = x^2 \bmod n$$

où $x$ est un entier quelconque et les $p_i$ sont des nombres premiers plus petits qu'une borne $B$ donnée. Une fois collectées de nombreuses relations telles que celle ci-dessus, on peut, par élimination linéaire, obtenir une congruence entre deux carrés. Dans les deux sections suivantes nous présentons deux algorithmes de ce type.

## 2. Le crible linéaire de Dixon

On choisit un résidu $x$ modulo $n$ au hasard et on calcule $y$, le reste de la division euclidienne de $x^2$ par $n$. On a donc $x^2 = y \bmod n$. On espère que $y$ est $B$-friable. Si tel est le cas, on obtient une congruence entre un carré et un nombre $B$-friable. On collecte suffisamment de telles relations et on termine selon le principe général exposé ci-dessus.

Par exemple supposons que l'on veuille factoriser $n = 7081$. On choisit $B = 3$. Les nombres $B$-friables sont les entiers de la forme $\pm 2^a 3^b$.

Après quelques tâtonnements on trouve

$$\begin{aligned} 4486^2 &= -2.3 \bmod n, \\ 1857^2 &= 2 \bmod n, \\ 2645^2 &= -3 \bmod n. \end{aligned}$$

On associe à ces trois congruences la matrice $3\times 3$ à coefficients dans $\mathbb{F}_2$ suivante

| | $-1$ | 2 | 3 |
|---|---|---|---|
| 4486 | 1 | 1 | 1 |
| 1857 | 0 | 1 | 0 |
| 2645 | 1 | 0 | 1 |

On vérifie que la ligne $[1, 1, 1] \in \mathbb{F}_2^3$ est annulée par la matrice. On en déduit la congruence entre les deux carrés

$$(4486.1857.2645)^2 = (-2.3)^2 \bmod n.$$

Le pgcd de $n$ et $4486.1857.2645 + 6$ est 73. On a donc trouvé un facteur non-trivial.

## 3. Le crible quadratique

Cet algorithme est dû à Carl Pomerance. Nous nous contentons de l'illustrer sur un exemple. Soit

$$n = 21311 = 101.211$$

le nombre à factoriser. On choisit un entier $m$ proche de la racine carrée de $n$

$$m = \lfloor n^{1/2} \rceil = 146.$$

On forme des congruences modulo $n$ en observant que pour tout entier $a$,

$$(m + a)^2 \equiv (m^2 - n) + a^2 + 2am \pmod n = 5 + a^2 + 292a \pmod{21311},$$

où l'on note que $m^2 - n$ est de l'ordre de $\sqrt{n}$.

On se donne une borne $B = 13$ et l'on cherche de petits entiers $a$ tels que $5 + a^2 + 292a$ soit $B$-friable. Par exemple pour $a$ compris entre $-60$ et 60 on trouve

| $a$ | $5 + 292a + a^2$ |
|---|---|
| $-27$ | $-2.5^2.11.13$ |
| $-5$ | $-2.5.11.13$ |
| $-1$ | $-2.11.13$ |
| 0 | 5 |
| 60 | $5^3.13^2$ |

On porte dans une matrice la parité des valuations :

| | $-1$ | 2 | 5 | 11 | 13 |
|---|---|---|---|---|---|
| $-27$ | 1 | 1 | 0 | 1 | 1 |
| $-5$ | 1 | 1 | 1 | 1 | 1 |
| $-1$ | 1 | 1 | 0 | 1 | 1 |
| 0 | 0 | 0 | 1 | 0 | 0 |
| 60 | 0 | 0 | 1 | 0 | 0 |

On forme des carrés à partir des lignes annulées par cette matrice. L'ensemble de ces lignes est un espace vectoriel dont une base est donnée par les trois lignes de la matrice suivante

| $-27$ | $-5$ | $-1$ | 0 | 60 |
|---|---|---|---|---|
| 1 | 0 | 1 | 0 | 0 |
| 1 | 1 | 0 | 1 | 0 |
| 1 | 1 | 0 | 0 | 1 |

La première ligne du tableau donne la congruence

$$(2.5.11.13)^2 \equiv (146 - 27)^2.(146 - 1)^2 \pmod{21311}.$$

On calcule alors le plus grand diviseur commun de $2.5.11.13 - (146 - 27).(146 - 1) = -15825$ et de 21311. On trouve le facteur non trivial $p = 211$ de $n = 21311$ et son cofacteur 101. Un test de primalité prouve aisément que $p$ et $q$ sont premiers.

En quoi cet algorithme est il meilleur que celui de Dixon ? La seule différence réside dans la manière de trouver des relations de congruences. Dans le crible de Dixon, le résidu de $x^2$ modulo $n$ est un entier aléatoire entre 1 et $n-1$. On espère que cet entier est friable. Dans le crible quadratique le nombre supposé friable est de l'ordre de $\sqrt{n}$. La probabilité de succès est donc bien plus grande.

## 4. Le crible algébrique, présentation générale

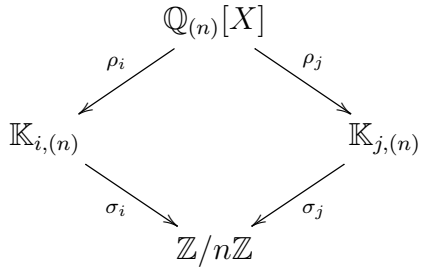
Le crible algébrique est un algorithme inventé par Pollard et Lenstra. Les frontières de cet algorithme ne sont pas nettes. De nombreuses variantes existent pour chacune des étapes qui le constituent. Nous donnons une présentation aussi générale que possible de cet algorithme. Nous donnons un exemple dans la section suivante.

On appelle toujours $n$ l'entier à factoriser et $m$ un entier auxiliaire qu'il conviendra de préciser plus tard.

Pour tout corps de nombres $\mathbb{K}$ on note $\mathcal{O}_{\mathbb{K}}$ son anneau des entiers et $\mathbb{K}_{(n)}$ l'anneau local en $n$ c'est-à-dire l'ensemble des éléments de $\mathbb{K}$ dont le dénominateur est premier à $n$.

Soient $f_i(X)$ pour $1 \leq i \leq I$ des polynômes irréductibles unitaires à coefficients entiers et de discriminants premiers à $n$. On suppose aussi que $f_i(m) = n$. Cette dernière condition se traduit algébriquement par l'égalité de tous les idéaux $(X - m, f_i(X))$ et de $(X - m, n)$ dans $\mathbb{Q}_{(n)}[X]$.

Appelons $\mathbb{K}_i = \mathbb{Q}[X]/f_i(X)$ le corps de nombres associé à $f_i$. L'égalité entre idéaux ci-dessus implique la commutativité du diagramme suivant pour tout couple $(i, j)$ d'entiers compris entre 1 et $I$.




Les flèches $\rho_i$ sont des quotients par les polynômes $f_i$ et les $\sigma_i$ sont des substitutions de $X$ par $m$.

Voici comment le crible algébrique utilise le diagramme ci-dessus. Observons d'abord que les trois étages du diagramme sont de natures arithmétiques très différentes.

Dans $\mathbb{Q}[X]$, la plupart des éléments sont irréductibles et très peu sont inversibles. Dans $\mathbb{Z}/n\mathbb{Z}$ c'est l'inverse. Il y a une majorité d'éléments inversibles et très peu d'éléments irréductibles puisqu'ils correspondent aux facteurs de $n$. Les corps $\mathbb{K}_i$ sont les seuls êtres intermédiaires que l'on puisse intercaler entre les deux précédents.

Prenons maintenant un élément $A(X)$ de $\mathbb{Z}[X]$. Pour tout $i$, on dit que

$$\rho_i(A) = A(X) \bmod f_i(X)$$

est friable s'il se factorise dans le groupe multiplicatif $\mathbb{K}_i^*$ en

$$A(X) \bmod f_i(X) = \prod_k \mathfrak{p}_{i,k}^{e_{i,k}}$$

où les $\mathfrak{p}_{i,k}$ sont une base de friabilité, c'est-à-dire un système de générateurs d'un sous-groupe de $\mathbb{K}_i^*$ que l'on note $\mathbb{K}_{i,s}$. On choisit en général le groupe formé des éléments dont la norme est un rationnel $B$-friable, c'est-à-dire divisible uniquement par des nombres premiers plus petits que $B$. Si $\mathcal{O}_{\mathbb{K}_i}$ est principal, les $\mathfrak{p}_{i,k}$ peuvent être des générateurs de petits idéaux premiers et des unités fondamentales. On a alors,

$$\sigma_i(\rho_i(A(X))) = A(m) \pmod n = \prod_k \sigma_i(\mathfrak{p}_{i,k})^{e_{i,k}}$$

Si $\rho_i(A)$ et $\rho_j(A)$ sont friables on obtient une congruence modulo $n$

$$A(m) \pmod n = \prod_k \sigma_i(\mathfrak{p}_{i,k})^{e_{i,k}} = \prod_k \sigma_j(\mathfrak{p}_{j,k})^{e_{j,k}},$$

soit encore

$$\prod_k \sigma_i(\mathfrak{p}_{i,k})^{e_{i,k}} \prod_k \sigma_j(\mathfrak{p}_{j,k})^{-e_{j,k}} = 1 \pmod n.$$

On se fixe une base de friabilité dans chacun des corps $\mathbb{K}_i$. Si pour un polynôme $A$ donné et deux entiers $i \neq j$, $\rho_i(A(X))$ et $\rho_j(A(X))$ sont friables on obtient une congruence utile comme ci-dessus. Lorsque le nombre de ces congruences excède le cardinal de la réunion de toutes les bases de friabilité, on obtient une congruence entre 2 carrés modulo $n$ et donc une chance de factoriser $n$ pour chaque relation excédentaire.

En général, les $\mathcal{O}_{\mathbb{K}_i}$ ne sont pas factoriels, aussi on adopte un point de vue dual. On sait que $\mathbb{K}_{i,s}$ est un groupe de type fini engendré par à peu près $\pi(B)$ générateurs. Ces générateurs ne sont pas canoniques et on ne sait pas les calculer. En revanche on sait que le groupe des éléments friables modulo les carrés $\mathbb{K}_{i,s}/(\mathbb{K}_{i,s})^2$ est un groupe commutatif d'exposant deux et de type fini, donc un espace vectoriel sur $\mathbb{Z}/2\mathbb{Z}$ de dimension voisine de $\pi(B)$. On associe à chaque idéal la valuation associée ou plutôt le résidu modulo deux de cette valuation. On obtient ainsi un certain nombre de formes linéaires de $\mathbb{K}_{i,s}/(\mathbb{K}_{i,s})^2$ à valeurs dans $\mathbb{Z}/2\mathbb{Z}$. On ajoute à ces formes quelques caractères construits à partir de résidus quadratiques. Ces derniers, en nombre suffisant, servent à tuer l'obstruction provenant du groupe de classe et du groupe des unités. On suppose que la collection des valuations et des caractères engendre le dual de $\mathbb{K}_{i,s}/(\mathbb{K}_{i,s})^2$. Autrement dit, si toutes ces valuations et caractères s'annulent en un nombre $a \in \mathbb{K}_{i,s}$, alors ce nombre est un carré.

Une relation élémentaire est alors définie par un polynôme $A(X)$ et deux entiers $i$ et $j$ tels que $\rho_i(X)$ et $\rho_j(X)$ soient friables chacun dans son corps. Une combinaison de relations est caractérisée par deux $I$-uplets $(G_i)_{1\leq i\leq I}$ et $(D_i)_{1\leq i\leq I}$

où chaque $G_i \in \mathbb{K}_i$ est le produit de tous les membres de gauche des relations élémentaires du type $(i, *)$ et $D_j \in \mathbb{K}_j$ est le produit de tous les membres de droite des relations élémentaires du type $(*, j)$. En tenant compte des valeurs prises par les valuations et les caractères, on obtient des combinaisons telles que tous les $G_i/D_i = C_i$ soient des carrés dans $\mathbb{K}_i$. Chacune de ces relations donne une congruence entre carrés modulo $n$. Pour cela, il reste à calculer les racines carrées $R_i$ telles que $R_i^2 = C_i$. C'est un problème en soi que nous n'aborderons pas ici. La relation s'écrit

$$(\prod_i \sigma_i(R_i))^2 = 1 \pmod{n}.$$

**Remarque** : En général, on choisit une unique polynôme $f$ tel que $f(m) = n$ et on définit le corps de nombre $\mathbb{K} = \mathbb{Q}[X]/f$ et les quatre morphismes $\sigma_{alg} : \mathbb{K}_{(n)} \to \mathbb{Z}/n\mathbb{Z}$, $\sigma_{rat} : \mathbb{Q}_{(n)} :\to \mathbb{Z}/n\mathbb{Z}$, $\rho_{rat} : \mathbb{Q}_{(n)}[X] \to \mathbb{Q}_{(n)}$, et $\rho_{alg} : \mathbb{Q}_{(n)}[X] \to \mathbb{K}_{(n)}$ par $\sigma_{rat}(n) = 0$, $\sigma_{alg}(X \bmod f) = m$, $\rho_{rat}(X) = m$, $\rho_{alg}(X) = X \bmod f$. Ces applications forment un diagramme commutatif,

$$\sigma_{alg}\rho_{alg} = \sigma_{rat}\rho_{rat}.$$

## 5. Un exemple de crible algébrique général

Soit toujours

$$n = 21311 = 101.211$$

le nombre à factoriser. Posons

$$m = \lfloor n^{1/2} \rceil = 146$$

et écrivons $n$ en base $m$

$$n = 146^2 - 5 = f(n)$$

avec

$$f(X) = X^2 - 5.$$

Le polynôme $f(X)$ étant irréductible, on définit le corps de nombres

$$\mathbb{K} = \mathbb{Q}[X]/f(X)$$

qui est un corps quadratique réel. Donc $d = 2$. On se donne une borne de friabilité $B = 20$ et on dit un nombre premier petit s'il est inférieur à $B$. On note $\mathcal{O}$ l'anneau $\mathbb{Z}[X]/f(X)$.

Venons en maintenant à la détermination de la base de friabilité. Elle se compose d'une base algébrique et d'une base rationnelle. La base rationnelle comprend $-1$, c'est à dire le signe et les nombres premiers inférieurs à $B = 20$ soit

$$\mathcal{B}_{rat} = \{-1, 2, 3, 5, 7, 11, 13, 17, 19\}.$$

Pour construire la base algébrique on factorise les nombres premiers $p$ entre 2 et 19 dans l'anneau $\mathcal{O}$. On ne s'intéresse qu'aux facteurs de degré résiduel 1. Pour les trouver, on cherche les racines de $f(X)$ modulo $p$. À chaque racine $c$ on associe l'idéal premier $(p, X - c)$ de $\mathcal{O}$, que l'on note aussi $p_c$. Plutôt que ces idéaux, ce sont les valuations associées qui nous seront utiles. Nous considérons ces valuations modulo 2.

On ajoute deux caractères à la base ainsi obtenue. Dans notre cas nous choisirons les deux caractères à l'infini c'est à dire les deux fonctions $\chi_1$ et $\chi_2$ définies par

$$\chi_1(a + bX) = signe(a + b\sqrt{5}),$$

et

$$\chi_2(a + bX) = signe(a - b\sqrt{5}).$$

On trouve donc la base

$$\mathcal{B}_{alg} = \{\chi_1, \chi_2, 2_1, 5_0, 11_7, 11_4, 19_9, 19_{10}\}.$$

À tout élément $a + bX$ de $\mathcal{O}$ on associe sa norme

$$\mathcal{N}(a + bX) = \mathcal{N}(a, b) = f(-a/b)b^d.$$

Soit $p \geq 3$ un nombre premier. Pour $a$ et $b$ premiers entre eux, on sait que $a + bX$ a un facteur commun avec $p$ si et seulement si $\mathcal{N}(a, b)$ est divisible par $p$. Il existe alors un unique idéal premier $p_c$ tel que $a + bc \equiv 0 \pmod{p}$ et, pour $p$ impair, la multiplicité de $p_c$ dans $a + bX$ est la multiplicité de $p$ dans $\mathcal{N}(a, b)$.

Il reste maintenant à fixer une borne $C_a$ et une borne $C_b$ et à chercher des paires $(a, b)$ telles que $-C_a \leq a \leq C_a$, $1 \leq b \leq C_b$, $a$ et $b$ sans facteur commun, et $(a + bm).\mathcal{N}(a, b)$ friable. Si $b = 0$ et si $a$ est un nombre premier $p \in \{2, 5, 11\}$, on obtient des relations dites gratuites. Ces relations correspondent aux trois dernières lignes de la matrice ci-dessous.

Ici nous prendrons

$$C_a = 40 \text{ et } C_b = 20.$$

Grâce à un crible on trouve 14 paires $(a, b)$ plus 3 relations gratuites soit 17 relations pour 17 inconnues dans la base. Comme dans le cas du crible quadratique, nous plaçons dans une matrice les résidus modulo 2 des valuations et les logarithmes des caractères avec $\log(1) = 0$ et $\log(-1) = 1$. Les lignes de la matrice correspondent aux relations et ses colonnes aux inconnues.

| $-1$ | 2 | 3 | 5 | 7 | 11 | 13 | $2_1$ | $5_0$ | $11_7$ | $11_4$ | $19_9$ | $19_{10}$ | $\chi_1$ | $\chi_2$ | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | $(-3,1)$ |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | $(-2,1)$ |
| 0 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | $(-2,5)$ |
| 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | $(1,1)$ |
| 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | $(4,1)$ |
| 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | $(5,2)$ |
| 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | $(10,3)$ |
| 0 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | $(38,17)$ |
| 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | $(-14,9)$ |
| 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | $(10,1)$ |
| 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | $(15,8)$ |
| 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | $(21,4)$ |
| 0 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | $(22,13)$ |
| 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | $(29,1)$ |
| 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | $(2,0)$ |
| 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | $(5,0)$ |
| 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | $(11,0)$ |

Nous appelons $\mathcal{S}$ la matrice ci-dessus et nous calculons maintenant le noyau de la transposée de $\mathcal{S}$. Autrement dit nous cherchons une base de l'espace des lignes annulées par la matrice. Ici la méthode de Gauss est recommandée. Pour de plus grandes matrices il vaut mieux exploiter le caractère lacunaire de $\mathcal{S}$.

Nous choisissons un vecteur $v_1$, dans ce noyaux de dimension 5.

$$v_1 = [0,0,1,0,0,0,1,1,1,0,1,1,0,0,0,0,0].$$

Ce vecteur correspond au polynôme

$$P_1 = (-2+5X)(10+3X)(38+17X)(-14+9X)(15+8X)(21+4X).$$

On lui associe l'entier rationnel

$$\rho_{rat}(P_1) = (-2+5m)(10+3m)(38+17m)(-14+9m)(15+8m)(21+4m),$$

et l'entier algébrique

$$\rho_{alg}(P_1) = (-2+5X)(10+3X)(38+17X)(-14+9X)(15+8X)(21+4X) \bmod f(X).$$

Chacun de ces deux entiers est friable et c'est même un carré. Il reste à calculer les racines carrées. Du coté rationnel, il suffit de décomposer chacun des termes du produit. Ce travail a déjà été fait au moment de construire $\mathcal{S}$. On obtient

$$\rho_{rat}(P_1) = 2^{14}.3^2.5^4.7^4.11^2.13^4 = (2^7.3.5^2.7^2.11.13^2)^2.$$

Du coté algébrique, on ne connaît pas la décomposition des facteurs et d'ailleurs, elle n'est pas forcément unique puisque l'anneau $\mathcal{O}$ n'est pas intégralement clos. On doit donc calculer une racine de $\rho_{alg}(P_1)$ par une méthode *ad hoc*. Nous n'abordons pas ce problème ici. On trouve

$$\rho_{alg}(P_1) = (4180 + 1881X)^2 \pmod{f(X)}.$$

On a donc

$$\sigma_{rat}(\rho_{rat}(P_1)) = (2^7.3.5^2.7^2.11.13^2)^2 \bmod n = 19337^2 \bmod n,$$

et

$$\sigma_{alg}(\rho_{alg}(P_1)) = (4180 + 1881m)^2 \bmod n = 1763^2 \bmod n.$$

Or on sait que

$$\sigma_{rat}(\rho_{rat}(P_1)) = \sigma_{alg}(\rho_{alg}(P_1)),$$

donc

$$19337^2 = 1763^2 \bmod 21311.$$

On calcule alors

$$gcd(19337 - 1763, 21311) = 101,$$

ce qui donne un facteur non trivial de $n$.

## 6. Éléments pour l'analyse des cribles

Cette section et la suivante sont consacrées à l'analyse de la complexité de divers algorithmes de crible. Nous donnons des éléments synthétiques pour l'analyse rapide de tous ces algorithmes.

On définit tout d'abord la quantité suivante pour $x, \nu, \lambda \in \mathbb{R}$ avec $x > e$, $\lambda \neq 0$, et $0 \leq \nu \leq 1$

$$L_x[\nu, \lambda] = exp(\lambda(\log x)^\nu(\log\log x)^{1-\nu}).$$

Comme on utilisera ces fonctions pour des estimations asymptotiques, on convient d'écrire $L_x[\nu, \lambda]$ pour $L_x[\nu, \lambda+o(1)]$ et $L_x[\nu]$ pour $L_x[\nu, \lambda]$ et $\lambda \neq 0$. Noter que $L_x[\nu]$ est défini à une exponentiation près (positive ou négative). L'échelle des $L_x[\nu, \lambda]$ est assez grossière puisque on identifie deux quantités dont les logarithmes sont équivalents. L'échelle des $L_x[\nu]$ est encore plus grossière. On note aussi que

$$L_x[\nu_1]L_x[\nu_2] = L_x[max(\nu_1, \nu_2)],$$

si $\nu_1 \neq \nu_2$ et

$$L_x[\nu, \lambda_1]L_x[\nu, \lambda_2] = L_x[\nu, \lambda_1 + \lambda_2]$$

si $\lambda_1 + \lambda_2 \neq 0$. Ces fonctions forment une progression entre le polynomial et l'exponentiel. On sait par ailleurs que

**Théorème 1.** *Si $0 < w < \nu \leq 1$, $\lambda > 0$, et $\mu > 0$, alors la probabilité qu'un nombre de taille $L_x[\nu, \lambda]$ soit $L_x[w, \mu]$-friable est*

$$L_x[\nu - w, -\lambda(\nu - w)/\mu + o(1)].$$

Supposons maintenant que nous ayons à analyser l'algorithme de crible linéaire de Dixon.

Soit donc $n$ un entier. On se donne une borne de friabilité $B = L_n[w]$ et l'on se trouve avec des entiers $y = x^2 \bmod n$ entre 1 et $n$ donc de taille $C = L_n[1]$. On continue jusqu'à avoir trouvé $\pi(B)$ tels entiers $B$-friables.

La probabilité pour qu'un entier de taille $L_n[1]$ soit $B$-friable est

$$P = L_n[1 - w]$$

et le temps de calcul est

$$T = P^{-1}B = L_n[1 - w]L_n[w] = L_n[max(1 - w, w)].$$

On voit que $T$ est minimum pour $1-w = w = 1/2$ ce qui indique une complexité

$$T = L_n[\frac{1}{2}].$$

Pour affiner l'analyse, on suppose maintenant que $B$ est de l'ordre de $L_n[1/2, b]$. En outre $y$ est de taille

$$L_n[1, 1],$$

et il est $B$-friable avec probabilité

$$P = L_n[\frac{1}{2}, -\frac{1}{2}.\frac{1}{b}].$$

Le temps total de la recherche des $y$ $B$-friables est alors

$$T_1 = \frac{B}{P}$$

puisqu'on veut $\pi(B)$ valeurs $B$-friables de $y$ et qu'une valeur aléatoire est $B$-friable avec une probabilité $P$.

L'inversion d'une matrice creuse de taille $\pi(B)$ se fait en temps $\pi(B)^2$ par des méthodes *ad hoc*. Ici nous avons donc

$$T_2 = B^2.$$

Nous devons choisir le paramètres $B = L_n[1/2, b]$ afin de minimiser $T_1 + T_2$ soit

$$T_1 + T_2 = L_n[\frac{1}{2}, max(b + \frac{1}{2b}, 2b)].$$

On minimise pour $b > 0$ la fonction affine par morceau

$$b \mapsto max(b + \frac{1}{2b}, 2b)$$

avec $b = 1/\sqrt{2}$.

**Théorème 2.** *Le crible linéaire de Dixon est optimal pour*

$$B = L_n[\frac{1}{2}, \frac{1}{\sqrt{2}}],$$

*et il s'exécute en temps*

$$T = L_n[\frac{1}{2}, \sqrt{2}].$$

## 7. Analyse du crible quadratique

Dans cette section nous analysons le crible quadratique.

On suppose toujours que $B$ est de l'ordre de $L_n[1/2, b]$. On voit que cette fois, les entiers $(m^2 - n) + a^2 + 2am$ sont de taille

$$L_n[1, 1/2].$$

Ils sont donc $B$-friables avec probabilité

$$P = L_n[\frac{1}{2}, -\frac{1}{2}.\frac{1}{2b}].$$

Le temps de recherche des entiers $a$ convenables est

$$T_1 = \frac{B}{P} = L_n[\frac{1}{2}, b + \frac{1}{4b}].$$

Le temps d'inversion de la matrice est

$$T_2 = \pi(B)^2 = L_n[\frac{1}{2}, 2b].$$

On minimise $T_1 + T_2$ en minimisant $max(b + \frac{1}{4b}, 2b)$ pour $b > 0$ ce qui donne $b = 1/2$. On a donc le

**Théorème 3.** *Le crible quadratique est optimal pour*

$$B = L_n[\frac{1}{2}, \frac{1}{2}],$$

*et il s'exécute en temps*

$$T = L_n[\frac{1}{2}, 1].$$

On note un gain *exponentiel* de $\sqrt{2}$ par rapport à l'algorithme de Dixon. Ce gain est dû à la plus petite taille des entiers supposés $B$-friables. Au lieu d'avoir des entiers de taille $n$, on a des entiers de taille $n^{1/2}$.