Sorbonne Université
Cryptologie, cryptographie algébrique
4M035 - 2021/22
Alain Kraus

# Chapitre III - Méthodes de factorisation

Le problème de la factorisation des grands entiers est a priori très difficile. L'efficacité de nombreux cryptosystèmes, comme RSA, est basé sur cette difficulté présumée. Le problème de décider si un entier est premier ou non, est en fait beaucoup plus simple que celui de trouver les diviseurs premiers d'un entier composé. Un entier ayant plusieurs milliers de chiffres décimaux qui est premier, faute parfois de prouver que tel est bien le cas, on peut néanmoins en avoir une certitude morale, avec une probabilité aussi proche de 1 que l'on veut. Par ailleurs, on peut souvent démontrer facilement qu'un grand entier est composé si tel est le cas. Pour autant, les méthodes utilisées ne fournissent en général aucune information sur ses diviseurs premiers. On va décrire certaines méthodes permettant parfois de les déterminer. Étant donné un entier naturel composé $n$, nous appellerons « factoriser $n$ » le fait de trouver un diviseur non trivial de $n$. De nos jours, en dépit des progrès algorithmiques et informatiques réalisés, on ne parvient pas à factoriser un entier qui est un produit de deux nombres premiers ayant chacun environ cent cinquante chiffres décimaux, sauf dans des cas très particuliers.

**Table des matières**



## 1. Méthode des divisions successives

Soit $n$ un entier composé. Afin de déterminer le plus petit diviseur premier $p$ de $n$, il suffit de diviser $n$ successivement par tous les nombres premiers $2, 3, 5, 7, 11, \cdots$, jusqu'à atteindre $p$. En notant $\pi(N)$ le nombre de nombres premiers plus petits qu'un entier $N$, il s'agit donc d'effectuer $\pi(p)$ divisions avant de déterminer $p$, soit d'après le théorème des

nombres premiers, environ $\frac{p}{\log p}$ divisions. Puisque $p$ est plus petit que $\sqrt{n}$, dans le pire des cas on devra alors effectuer approximativement $\frac{2\sqrt{n}}{\log n}$ opérations. Le temps nécessaire à ce calcul est évidemment prohibitif si $n$ est grand. Ce procédé est en fait inefficace par rapport aux autres méthodes de factorisation dont on dispose aujourd'hui, dès que $p$ est plus grand disons que $10^7$.

La méthode des divisions successives, qui est la plus simple, consiste à déterminer les diviseurs premiers de $n$ plus petits qu'une borne que l'on se fixe au départ, par exemple $10^6$. On a

$$\pi\big(10^6\big) = 78498.$$

Avec cette borne choisie, c'est donc le nombre des nombres premiers par lesquels on divise $n$ au départ. Bien que cette méthode ne permette pas de factoriser des entiers n'ayant que des grands facteurs premiers, elle est néanmoins incontournable. C'est la première méthode que l'on doit essayer afin de factoriser $n$, d'autant que « la plupart » des entiers possèdent au moins un petit diviseur premier. Heuristiquement, environ quatre-vingt-douze pour cent des entiers ont un diviseur premier plus petit que 1000. En effet, étant donnés un entier $m \geq 1$ et un nombre premier $\ell$, le reste de la division euclidienne de $m$ par $\ell$ est compris entre 0 et $\ell - 1$, d'où une chance sur $\ell$ pour qu'il soit nul, i.e. pour que $m$ soit divisible par $\ell$. La probabilité pour que $m$ ne soit pas divisible par $\ell$ est donc $1 - \frac{1}{\ell}$. Celle pour que $m$ ne soit pas divisible par un nombre premier plus petit que 1000 est donc

$$\prod_{\ell<1000} \Big(1 - \frac{1}{\ell}\Big),$$

qui vaut environ $0,081$, d'où la proportion annoncée.

**Exemples 3.1.**

1) On constate directement par cette méthode que $10^{10} + 19$ est premier.

2) Les entiers de la forme $10^{100} + a$ avec $1 \leq a \leq 100$ sont composés. Seuls ceux pour lesquels $a$ vaut $9, 37, 39, 61, 63$ ou 99 n'ont pas de diviseurs premiers plus petits que 1000.

3) Déterminons la factorisation complète de $n = 34624234323236231$ (choisi arbitrairement). Il est composé car $2^{n-1}$ n'est pas congru à 1 modulo $n$. On vérifie ensuite que 709 divise $n$. On a

$$n = 709 \times 48835309341659.$$

Par ailleurs, $\frac{n}{709}$ n'est pas premier et n'est pas divisible par un nombre premier plus petit que $10^6$. C'est un entier ayant quatorze chiffres décimaux. On peut dans ce cas pousser la recherche par divisions successives d'un diviseur premier plus petit par exemple que $2.10^6$. On obtient alors la décomposition de $n$ en facteurs premiers

$$n = 709 \times 1002863 \times 48695893.$$

4) Prenons $n = 2^{83} - 1$. Il a vingt-cinq chiffres décimaux. On a $3^{n-1} \not\equiv 1 \bmod. n$, donc $n$ est composé. On vérifie que l'on a

$$n = 167 \times 57912614113275649087721.$$

C'est la décomposition de $n$ en facteurs premiers. En effet, le critère de Pocklington permet de démontrer facilement que $m = \frac{n}{167}$ est premier. On vérifie par divisions successives que

$$m - 1 = 2^3 \times 5 \times 83 \times 383 \times 4049 \times 11248342573613.$$

L'entier $q = 11248342573613$ est premier, car il n'a pas de diviseurs premiers plus petits que sa racine carrée qui vaut environ 3353854,8. Par ailleurs, on a

$$3^{m-1} \equiv 1 \bmod. m \quad \text{et} \quad \operatorname{pgcd}\Big(3^{\frac{m-1}{q}} - 1, m\Big) = 1.$$

Cela entraîne que $m$ est premier, car on a $q \geq \sqrt{m}$.

## 2. Méthode $p-1$ de Pollard

Elle a été présentée par J. M. Pollard en 1974. Soit $n$ un entier composé. Cette méthode probabiliste permet de déterminer les diviseurs premiers $p$ de $n$, pour lesquels il n'intervient dans la décomposition de $p-1$ en facteurs premiers que des petits nombres premiers et affectés d'exposants pas trop grands.

### 1. Principe

Soit $p$ un diviseur premier de $n$ tel que les diviseurs premiers de $p-1$ soient inférieurs ou égaux à un certain entier $B$, avec des exposants pas trop grands de sorte que l'on ait

$$B! \equiv 0 \bmod. p - 1. \tag{1}$$

Choisissons un entier $a$ tel que $1 < a < n$. On peut supposer que $a$ est premier avec $n$, sinon on a déterminé un diviseur non trivial de $n$. Compte tenu du petit théorème de Fermat, on obtient alors

$$a^{B!} \equiv 1 \bmod. p.$$

Par suite, on a

$$\operatorname{pgcd}\big(a^{B!} - 1, n\big) \equiv 0 \bmod. p.$$

Si l'on a $\operatorname{pgcd}\big(a^{B!} - 1, n\big) \neq n$, ce qui est pratiquement presque toujours le cas, on obtient un facteur non trivial de $n$, qui est un multiple de $p$, ce qui permet souvent d'obtenir $p$.

Il convient de noter que dans l'application de cette méthode, on ne calcule pas l'entier $B!$. On calcule seulement l'entier

$$a^{B!} \bmod. n$$

en considérant la suite $(x_k)$ d'entiers modulo $n$ définie par

$$x_1 = a \text{ mod. } n \quad \text{et} \quad x_k = x_{k-1}^k \text{ mod. } n.$$

On a alors $x_B = a^{B!} \text{ mod. } n$. On peut aussi remplacer dans (1) l'entier $B!$ par le ppcm des entiers plus petits que $B$. En pratique, on prend souvent $B$ entre $10^3$ et $10^6$.

**2. Algorithme $p-1$ de Pollard**

1) On choisit un entier naturel $B$ disons plus petit que $10^7$.

2) On choisit un entier $a$ tel que $1 < a < n$ (par exemple $a = 2$ ou $a = 3$).

3) On calcule le pgcd de $a$ et $n$. Si l'on a $\text{pgcd}(a, n) \neq 1$, on obtient un diviseur non trivial de $n$ et l'algorithme est terminé.

4) Si l'on a $\text{pgcd}(a, n) = 1$, on calcule $a^{B!}$ modulo $n$, puis l'entier

$$d = \text{pgcd}\big(a^{B!} - 1, n\big).$$

Si l'on a $1 < d < n$, alors $d$ est un diviseur non trivial de $n$. Si $d = 1$, on reprend à la première étape avec un plus grand entier $B$. Si $d = n$, on retourne à la première étape avec un plus petit entier $B$ ou à la deuxième avec un autre entier $a$.

Si l'on parvient à déterminer un diviseur non trivial $d$ de $n$, afin d'essayer d'obtenir la factorisation complète de $n$, on peut recommencer l'algorithme avec l'entier $\frac{n}{d}$, en espérant qu'il possède aussi un diviseur premier $\ell$ tel que $\ell - 1$ n'ait que des petits facteurs premiers.

Cette méthode fournira en pratique un facteur premier $p$ de $n$, pas nécessairement le plus petit, sous réserve que les diviseurs premiers de $p-1$ ne soient pas trop grands. L'inconvénient de cette méthode est que si $p-1$, autrement dit si l'ordre du groupe $\mathbb{F}_p^*$, possède un grand diviseur premier, il convient de choisir au départ un très grand entier $B$, ce qui est généralement prohibitif pour le temps de calcul de $a^{B!} - 1$ modulo $n$. Comme on le verra dans le chapitre suivant, H. W. Lenstra en 1986 a eu l'idée de «remplacer $\mathbb{F}_p^*$» par le groupe des points rationnels d'une courbe elliptique sur $\mathbb{F}_p$, ce qui laisse beaucoup plus de chances de déterminer $p$, car on dispose au départ d'un grand nombre de groupes pour la mise en oeuvre de sa méthode, dite ECM. C'est l'analogue elliptique de la méthode $p-1$ de Pollard.

**Exemples 3.2.** Dans les exemples qui suivent, on vérifie au départ que les entiers $n$ considérés sont composés (avec le test de Fermat).

1) Prenons $n = 2^{67} - 1$. Il a vingt-et-un chiffres décimaux. Avec $B = 3000$, on trouve

$$3^{B!} - 1 \equiv 21443970396776172590 \text{ mod. } n.$$

(On ne peut pas prendre $a = 2$, car pour tout multiple $d$ de 67 on a $2^d \equiv 1$ mod. $n$.) On vérifie ensuite que l'on a

$$\mathrm{pgcd}\big(3^{B!} - 1, n\big) = 193707721.$$

On a en fait $193707720 = 2^3 \times 3^3 \times 5 \times 67 \times 2677$, ce qui explique a posteriori le choix de $B$. On obtient

$$2^{67} - 1 = 193707721 \times 761838257287,$$

qui est la décomposition de $n$ en facteurs premiers. Signalons qu'en 1903, Cole a annoncé cette factorisation lors d'un congrès de la société mathématique américaine. Il l'avait obtenue en calculant « à la main » tous les dimanches pendant trois ans.

2) Prenons $n = \frac{10^{59}-1}{9}$. Il a cinquante-neuf chiffres qui ne sont que des 1. Avec

$$B = 1000,$$

et $a = 2$, on trouve instantanément avec Pari, que 2559647034361 est un diviseur premier de $n$. On a

$$n = 2559647034361 \times p \quad \text{où} \quad p = 434087628565746021214453428992855982675574675 1.$$

L'entier $p$ est un nombre premier. Pour le démontrer, on peut utiliser la variante du théorème d'Agrawal, Kayal et Saxena, exposée dans le chapitre II (th. 2.7). Ce n'est pas le procédé le plus rapide, mais en tout cas un bon exercice sur machine. On vérifie par divisions successives que $r = 2 \times 5^3 \times 139 = 34750$ est un diviseur de $p - 1$, et il est plus grand que $\big(\frac{\log p}{\log 2}\big)^2$ qui vaut environ 22984. Par ailleurs, on a

$$7^{p-1} \equiv 1 \text{ mod. } p \quad \text{et} \quad \mathrm{pgcd}\Big(7^{\frac{p-1}{q}} - 1, p\Big) = 1$$

pour tous les diviseurs premiers $q$ de $r$. On vérifie ensuite que l'on a dans l'anneau $\mathbb{Z}[X]$

$$(X-1)^p \equiv X^p - 1 \equiv 7^{\frac{p-1}{r}} X - 1 \text{ mod. } (p, X^r - 7).$$

Le temps qu'il m'a fallu sur Pari pour calculer $(X-1)^p$ modulo $(p, X^r - 7)$ est de trente secondes environ. Puisque $p$ n'est pas la puissance non triviale d'un entier (on le vérifie directement), cela prouve que $p$ est premier.

3) Prenons $n = 2^{257} - 1$. Il a soixante-dix-huit chiffres décimaux. La méthode $p - 1$ de Pollard permet de trouver un facteur premier de $n$ (pas le plus petit) en choisissant

$$B = 15.10^5.$$

On vérifie que l'on a

$$\mathrm{pgcd}\big(3^{B!} - 1, n\big) = p \quad \text{où} \quad p = 1155685395246619182673033.$$

L'entier $p$ est premier, comme on le constate en utilisant l'égalité (divisions successives)

$$p-1 = 2^3 \times 3^2 \times 19^2 \times 47 \times 67 \times 257 \times 439 \times 119173 \times 1050151,$$

et par exemple le théorème 2.3, avec $a = 3$ et $F = 439 \times 119173 \times 1050151$. Le temps qu'il m'a fallu sur Pari pour obtenir $p$ est d'environ dix secondes. Par ailleurs, $\frac{n}{p}$ est un entier ayant cinquante-quatre chiffres décimaux, qui est composé. La méthode $p-1$ s'avère inefficace pour en trouver une factorisation. On verra que la méthode rho de Pollard permet facilement d'y parvenir.

4) Posons $n = 47969711156799309793644106104403$. Avec $B = 5.10^6$, on trouve que

$$\mathrm{pgcd}\big(2^{B!} - 1, n\big) = 7098676778697011,$$

d'où

$$n = 6757556746456673 \times 7098676778697011,$$

qui est un produit de deux nombres premiers.

## 3. Méthode rho de Pollard

C'est une méthode probabiliste inventée par Pollard en 1975. Soit $n$ un entier composé. Son efficacité pour factoriser $n$ dépend essentiellement de la taille du plus petit diviseur premier de $n$.

### 1. Principe

Il repose sur l'idée suivante. On choisit un polynôme $f(X)$ à coefficients dans $\mathbb{Z}$ et un entier naturel $x_0 < n$, par exemple $x_0 = 1$ ou 2, ou un autre entier choisi de façon aléatoire. On considère la suite d'entiers $(x_i)_{i\in\mathbb{N}}$ définie par les égalités,

$$x_{i+1} = f(x_i) \text{ modulo } n \quad \text{pour} \quad i = 0, 1, \cdots. \tag{2}$$

Autrement dit, $x_{i+1}$ est le reste de la division euclidienne de $f(x_i)$ par $n$. Les entiers $x_i$ sont donc compris entre 0 et $n-1$. On calcule les termes de cette suite dans l'espoir d'en trouver deux distincts, disons $x_i$ et $x_j$, qui soient congrus modulo un diviseur de $n$ autre que 1. On peut alors expliciter ce diviseur en calculant le pgcd de $|x_i - x_j|$ avec $n$.

**Exemple 3.3.** Illustrons cette idée avec un petit entier $n$, par exemple $n = 319$ (pour lequel cette méthode est évidemment inutile). Prenons $f(X) = X^2 + 1$ (ce n'est pas un hasard) et $x_0 = 1$. On vérifie que l'on a

$$x_1 = 2, \quad x_2 = 5, \quad x_3 = 26, \quad x_4 = 39, \quad x_5 = 246.$$

On obtient l'égalité $\text{pgcd}(x_5 - x_3, n) = 11$, d'où $n = 11 \times 29$.

Dans l'application de cette méthode, il importe de choisir $f(X)$ de sorte ses valeurs sur les entiers soient suffisamment aléatoires. Par exemple, un polynôme de degré 1 ne convient pas. Des expérimentations numériques poussées laissent penser que certains polynômes de degré 2, comme $X^2 + 1$, sont généralement bien adaptés. On verra que pour des entiers particuliers, comme les nombres de Mersenne ou de Fermat, il existe d'autres choix de polynômes pour lesquels la méthode est très efficace.

**2. Estimation du nombre d'itérations**

La question qui se pose est de connaître une estimation du nombre d'itérations auquel on doit s'attendre pour trouver un diviseur non trivial de $n$. On va voir qu'il est d'ordre $O\big(n^{\frac{1}{4}}\big)$. Considérons pour cela un entier naturel $r$ (moralement le plus petit diviseur premier de $n$, que l'on ne connaît pas) et estimons la moyenne, prise sur toutes les applications d'un ensemble $E$ de cardinal $r$ dans lui-même et tous les choix possibles de $x_0 \in E$, du plus petit entier $\ell$ pour lequel il existe $k < \ell$ tels que les éléments $x_k$ et $x_\ell$ obtenus par itérations soient égaux.

**Théorème 3.1.** *Soit $E$ un ensemble de cardinal $r$. Soit $\lambda > 0$ un nombre réel. Posons*

$$s = 1 + \big[\sqrt{2\lambda r}\,\big].$$

*Supposons $\lambda$ choisi de sorte que $s < r$. Pour toute application $f : E \to E$ et tout élément $x_0 \in E$, soit $(x_i)_{i\in\mathbb{N}}$ la suite d'éléments de $E$ définie par la relation $x_{i+1} = f(x_i)$. La proportion de couples $(f, x_0)$ pour lesquels*

$$x_0, x_1, \cdots, x_s \quad \textit{sont distincts deux à deux},$$

*où $f$ parcourt les applications de $E$ dans $E$ et où $x_0$ parcourt les éléments de $E$, est plus petite que $e^{-\lambda}$.*

Démonstration : Le nombre de couples $(f, x_0)$, où $f$ est une application de $E$ dans $E$ et $x_0$ un élément de $E$, est $r^{r+1}$. Vérifions que le nombre de couples $(f, x_0)$ pour lesquels $x_0, x_1, \cdots, x_s$ sont distincts deux à deux est

$$N = r^{r-s} \prod_{j=0}^{s} (r - j).$$

Il y a $r$ choix possibles pour $x_0$, $r - 1$ choix pour $f(x_0) = x_1$, $r - 2$ choix pour $f(x_1)$, et de même

$$r - (h + 1)$$

choix pour $f(x_h)$ pour tout $h$ tel que $0 \leq h \leq s-1$. Il reste $r-s$ éléments de $E$ dont il faut définir l'image par $f$. Puisque ces choix sont arbitraires, il y a donc $r^{r-s}$ choix d'images par $f$ des éléments de $E$ autres que $x_0, \cdots, x_{s-1}$, d'où l'assertion. La proportion cherchée étant

$$\frac{N}{r^{r+1}},$$

on obtient

$$\frac{N}{r^{r+1}} = r^{-s-1} \prod_{j=0}^{s} (r-j) = \prod_{j=1}^{s} \Big(1 - \frac{j}{r}\Big).$$

Par ailleurs, on a l'inégalité

$$\log(1-x) < -x \quad \text{pour tout } x \text{ tel que } 0 < x < 1.$$

On en déduit que l'on a

$$\log\left(\prod_{j=1}^{s}\Big(1-\frac{j}{r}\Big)\right) < -\sum_{j=1}^{s}\frac{j}{r} = -\frac{s(s+1)}{2r} < -\frac{s^2}{2r} < -\frac{\big(\sqrt{2\lambda r}\big)^2}{2r} = -\lambda,$$

(car pour tout $x > 0$, on a $(1+[x])^2 > x^2$), d'où $\frac{N}{r^{r+1}} < e^{-\lambda}$ et le résultat.

Avec les notations précédentes, prenons $\lambda = 2$, avec $r$ de sorte que $s = 1 + [2\sqrt{r}] < r$. La proportion de couples $(f, x_0)$ tels que les éléments $x_0, \cdots, x_s$ soient distincts deux à deux, est plus petite que $e^{-2} < 0,14$. On obtient l'énoncé suivant :

**Corollaire 3.1.** *Un couple $(f, x_0)$ étant choisi aléatoirement, il y a plus de « quatre-vingt-six pour cent de chances» pour que le plus petit entier $\ell$, tel qu'il existe $k < \ell$ avec $x_k = x_\ell$, soit plus petit que $1 + [2\sqrt{r}]$.*

**Conséquence.** Soit $p$ le plus petit diviseur premier de $n$. Considérons un couple $(f, x_0)$ où $f$ est un polynôme de $\mathbb{Z}[X]$ et $x_0$ un entier naturel plus petit que $n$. Soient $(x_i)_{i\in\mathbb{N}}$ la suite définie par la condition (2) et $y_i$ le reste de la division euclidienne de $x_i$ par $p$. Les $y_i$ ne sont pas connus car $p$ ne l'est pas. Cela étant, compte tenu du corollaire 3.1, utilisé avec $E = \big\{0, \cdots, p-1\big\}$ et le couple $(\widetilde{f}, y_0)$ où $\widetilde{f} : E \to E$ est l'application polynomiale associée à $f$, on peut espérer qu'il existe $i$ et $j$ tels que

$$x_i \neq x_j, \quad y_i = y_j \quad \text{avec} \quad \mathrm{Max}(i,j) = O\big(\sqrt{p}\big).$$

Puisque l'on a $p \leq \sqrt{n}$, il est donc vraisemblable de détecter $p$ en $O\big(n^{\frac{1}{4}}\big)$ itérations.

### 3. Calcul des pgcd

Afin de déterminer le plus petit diviseur premier de $n$, il convient a priori pour tout $i$, de calculer les entiers

$$\mathrm{pgcd}\big(|x_j - x_i|, n\big) \quad \text{pour tout } j < i.$$

En réalité, on ne calcule pas tous ces pgcd, ce qui serait trop coûteux. Un procédé pour contourner ce problème consiste à calculer un seul pgcd par entier $i$, à savoir le pgcd de $|x_{2i} - x_i|$ avec $n$. On va voir que l'on doit s'attendre à trouver un entier $i$ tel que

$$x_i \neq x_{2i} \quad \text{et} \quad \mathrm{pgcd}\big(|x_{2i} - x_i|, n\big) \neq 1$$

en $O\big(n^{\frac{1}{4}}\big)$ itérations. Établissons pour cela le résultat suivant.

**Proposition 3.1.** *Soient $E$ un ensemble fini et $f : E \to E$ une application. Soient $x_0$ un élément de $E$ et $(x_i)_{i\in\mathbb{N}}$ la suite définie par $x_{i+1} = f(x_i)$. Soit $\ell$ le plus petit indice tel que $x_\ell$ soit égal à l'un des $x_k$ avec $k < \ell$. Posons $t = \ell - k$.*

*1) Pour les indices $i$ tels que $0 \leq i < \ell$, les $x_i$ sont tous distincts et forment l'ensemble des valeurs de la suite.*

*2) Pour tout couple $(i, j)$ tel que $i \neq j$, on a l'équivalence*

$$x_i = x_j \iff k \leq \mathrm{Min}(i, j) \quad et \quad i \equiv j \text{ mod. } t.$$

Démonstration : Remarquons d'abord qu'il existe un unique couple d'entiers $(k, \ell)$ satisfaisant la condition de l'énoncé.

1) Le fait que les $x_i$ soient tous distincts pour $0 \leq i < \ell$ résulte de la définition de $\ell$. Vérifions que pour tout $m \geq \ell$, il existe un indice $r$ tel que l'on ait

$$k \leq r \leq \ell - 1 \quad \text{et} \quad x_m = x_r. \tag{3}$$

Cela est vrai si $m = \ell$ (avec $r = k$). Supposons $m \geq \ell$ et l'assertion satisfaite par $m$. Soit $r$ un entier vérifiant la condition (3). On a les égalités

$$x_{m+1} = f(x_m) = f(x_r) = x_{r+1}.$$

On a $k + 1 \leq r + 1 \leq \ell - 1$, ou bien $r + 1 = \ell$ auquel cas $x_{m+1} = x_k$. La condition (3) est donc satisfaite pour $m + 1$, d'où l'assertion.

2) Pour tout entier $i \geq k$, on a, en notant $f^0$ l'identité de $E$,

$$x_{i+t} = f^{i-k}(x_{t+k}) = f^{i-k}(x_\ell) = f^{i-k}(x_k) = x_i. \tag{4}$$

Soit $(i,j)$ un couple tel que $k \leq \mathrm{Min}(i,j)$ et $i \equiv j$ mod. $t$. D'après la condition (4), on a donc $x_i = x_j$.

Inversement, considérons un couple $(i,j)$ tel que $i < j$ et $x_i = x_j$. Il existe un plus petit entier $q \in \mathbb{N}$ tel que l'on ait

$$j - qt < \ell.$$

Vérifions que l'on a $k \leq j - qt$. Sinon, on aurait $j - qt < k$, d'où $j - qt + t < k + t = \ell$, puis $j - (q-1)t < \ell$. Par ailleurs, on a $j \geq \ell$ (par définition de $\ell$), d'où $q \geq 1$ et $q - 1$ est dans $\mathbb{N}$, ce qui contredit le caractère minimal de $q$. On a ainsi

$$k \leq j - qt < \ell. \tag{5}$$

D'après la condition (4), on a donc

$$x_{j-qt} = x_j.$$

On distingue alors deux cas.
Supposons $i < \ell$. La condition (5), l'égalité $x_i = x_{j-qt}$ et la première assertion impliquent alors

$$i = j - qt,$$

d'où $i \equiv j$ mod. $t$ et $k \leq i = \mathrm{Min}(i,j)$.
Supposons $\ell \leq i$. Il existe un plus petit entier $q' \in \mathbb{N}$ tel que $i - q't < \ell$. On a $q' \geq 1$, et l'on a comme ci-dessus, en utilisant le caractère minimal de $q'$,

$$k \leq i - q't < \ell. \tag{6}$$

D'après (4), on obtient

$$x_{i-q't} = x_i = x_j = x_{j-qt}.$$

D'après la première assertion, il en résulte que $i - q't = j - qt$, d'où $i \equiv j$ mod. $t$ et d'après (6), on a $k \leq i = \mathrm{Min}(i,j)$, d'où le résultat.

Reprenons les notations définies dans l'énoncé de la proposition précédente :

**Corollaire 3.2.** *Pour tout $i \geq 1$, on a l'équivalence*

$$x_i = x_{2i} \iff k \leq i \quad et \quad i \equiv 0 \text{ mod. } t.$$

**Remarque 3.1.** L'entier $t$ s'appelle la période de la suite $(x_i)_{i\in\mathbb{N}}$, et $k$ s'appelle l'indice d'entrée dans la période. On peut représenter l'ensemble des valeurs de la suite sous la forme de la lettre grec $\rho$. L'origine de «l'ovale» de cette lettre étant l'élément $x_k$ et

sa « longueur » étant la période $t$. C'est cette représentation qui justifie l'appellation « rho » de cette méthode de factorisation.

Notons $r$ le cardinal de $E$. Soient $f : E \to E$ une application et $x_0$ un élément de $E$. Soit $(x_i)_{i\in\mathbb{N}}$ la suite définie par $x_{i+1} = f(x_i)$. On a vu qu'il y a une grande probabilité pour que le plus petit entier $\ell$, pour lequel il existe $k < \ell$ avec $x_k = x_\ell$, soit plus petit que $2\sqrt{r}$ (cor. 3.1). Si tel est le cas, les entiers $k$ et $t$ sont en particulier plus petits que $2\sqrt{r}$. D'après le corollaire 3.2, il est donc probable que le plus petit entier $i \geq 1$ vérifiant $x_i = x_{2i}$ soit d'ordre $O\big(\sqrt{r}\big)$.

**Conséquence.** Soient $f$ un polynôme de $\mathbb{Z}[X]$, $x_0$ un entier et $(x_i)_{i\in\mathbb{N}}$ la suite définie par la condition (2). Soit $(y_i)_{i\in\mathbb{N}}$ la suite d'entiers telle que $y_i$ soit le reste de la division euclidienne de $x_i$ par le plus petit diviseur premier $p$ de $n$. Compte tenu de ce qui précède, avec $E = \big\{0, \cdots, p-1\big\}$, il y a donc de grandes chances pour que le plus petit $i \geq 1$ tel que $y_i = y_{2i}$ i.e. tel que $x_i \equiv x_{2i}$ mod. $p$, soit d'ordre $O\big(\sqrt{p}\big)$ autrement dit $O\big(n^{\frac{1}{4}}\big)$. Par ailleurs, on aura sans doute $x_i \neq x_{2i}$, car sinon la suite $(x_i)_{i\in\mathbb{N}}$ aurait une période anormalement courte. Cela justifie la stratégie annoncée pour le calcul des pgcd.

**Exemples 3.4.**

1) Prenons $n = \frac{4^{53}+1}{5}$. On a vu que $n$ est pseudo-premier fort. Il a trente-deux chiffres décimaux. Avec

$$x_0 = 2 \quad \text{et} \quad f = X^2 + 1,$$

on trouve en 2164 itérations que $p = 15358129$ est un diviseur premier de $n$. On constate en 36583 itérations que 586477649 est un diviseur premier de $\frac{n}{p}$. Ces calculs ont demandé moins d'une seconde sur Pari. On en déduit la décomposition en facteurs premiers de $n$,

$$n = 15358129 \times 586477649 \times 1801439824104653.$$

Le critère de Pocklington permet de prouver facilement que 1801439824104653 est premier.

2) Prenons $n = \frac{4^{73}+1}{5}$, qui a quarante-quatre chiffres décimaux. On vérifie que 293 et 9929 divisent $n$. Avec $x_0 = 2$ et $f = X^2 + 1$, on peut détecter en cinquante secondes environ sur Pari, après 20493668 itérations, que 649301712182209 est un diviseur premier de $n$. On obtient la décomposition complète de $n$ en facteurs premiers

$$n = 293 \times 9929 \times 649301712182209 \times 9444732965601851473921.$$

3) Supposons que $n$ soit un nombre de Mersenne, $n = 2^h - 1$ avec $h$ premier. Ses diviseurs premiers sont congrus à 1 modulo $2h$ (si $h \neq 2$). Soit $p$ le plus petit diviseur premier de $n$. L'ensemble des puissances $2h$-ièmes dans $\mathbb{F}_p^*$ est de cardinal $\frac{p-1}{2h}$. Posons

$$f = X^{2h} + 1.$$

Les valeurs modulo $p$ d'une suite d'itérés associée à $f$ appartiennent à un ensemble de cardinal $\frac{p-1}{2h}$. Avec ce choix de $f$, on peut ainsi espérer déterminer $p$ «environ $\sqrt{h}$ fois plus vite» qu'avec le polynôme $X^2+1$.

3.1) Prenons $n = 2^{101}-1$. Il est composé et a trente-et-un chiffres décimaux. Avec $x_0 = 3$ et $f = X^{202}+1$, on trouve en moins d'une seconde sur Pari, après 156779 itérations, que $p = 7432339208719$ divise $n$. On obtient ainsi l'égalité

$$n = pq \quad \text{avec} \quad q = 341117531003194129,$$

où $p$ et $q$ sont premiers. Avec le couple $(X^2+1, 3)$ on obtient ces résultats en deux fois plus de temps.

3.2) Prenons $n = 2^{257}-1$. On a vu dans les exemples 3.2 que $n$ est composé en le factorisant partiellement, sous la forme $p \times c_{54}$, où $p$ est un nombre premier de vingt-cinq chiffres et $c_{54}$ un nombre composé ayant cinquante-quatre chiffres. En utilisant la méthode rho, avec $x_0 = 3$ et $f = X^{514}+1$, on constate en cinq secondes environ sur Pari, après 455757 itérations, que 535006138814359 divise $c_{54}$. Il est premier. On obtient finalement la factorisation complète de $n$,

$$n = 535006138814359 \times 115568539524661918267303 3 \times p_{39},$$

où $p_{39}$ est un nombre premier de trente-neuf chiffres. Avec le couple $(X^2+1, 3)$ on obtient le plus petit diviseur premier de $n$ en trois minutes environ.

4) Supposons que $n$ soit un nombre de Fermat $F_h = 2^{2^h}+1$. Ses diviseurs premiers sont congrus à 1 modulo $2^{h+2}$ (si $h \geq 2$). Dans ce cas, de façon analogue aux nombres de Mersenne, en choisissant

$$f = X^{2^{h+2}}+1,$$

plutôt que $X^2+1$, on peut espérer gagner un facteur temps de $\sqrt{2^{h+1}}$ pour factoriser $n$.

4.1) Prenons $n = F_7 = 2^{128}+1$. Le test de Pepin permet de vérifier directement que $F_7$ est composé. Avec $x_0 = 3$ et $f = X^{512}+1$, après 9884772 itérations on obtient en cinquante secondes environ, 59649589127497217 comme diviseur premier de $F_7$. On en déduit la décomposition de $F_7$ en produit de deux nombres premiers,

$$F_7 = 59649589127497217 \times 5704689200685129054721.$$

4.2) Prenons $n = F_8 = 2^{256}+1$. Il est composé. Avec $x_0 = 3$ et $f = X^{1024}+1$, après 1028917 itérations on obtient en dix secondes, 1238926361552897 comme diviseur premier de $F_8$. On a en fait

$$F_8 = 1238926361552897 \times p_{63},$$

où $p_{63}$ est un nombre premier de soixante-trois chiffres. Cette factorisation a été obtenue par Brent et Pollard en 1981. C'est historiquement le succès le plus spectaculaire de la méthode rho.

## 4. Méthode de Fermat

Soit $n$ un entier impair composé. Elle est très efficace pour factoriser $n$ si $n$ s'écrit comme un produit de deux entiers proches l'un de l'autre. Elle repose sur le fait que trouver une factorisation de $n$ est équivalent à écrire $n$ comme une différence de deux carrés. On l'a déjà constaté dans la description des attaques possibles du système RSA. Plus précisément :

**Lemme 3.1.** *L'ensemble des couples $(a,b) \in \mathbb{N}^2$ tels que $n = ab$ avec $a \geq b$, et celui des couples $(r,s) \in \mathbb{N}^2$ tels que $n = r^2 - s^2$, sont en bijection.*

Démonstration : Soient $A$ l'ensemble des couples $(a,b) \in \mathbb{N}^2$ tels que $n = ab$ avec $a \geq b$, et $B$ l'ensemble des couples $(r,s) \in \mathbb{N}^2$ tels que $n = r^2 - s^2$. Les applications $f : A \to B$ et $g : B \to A$ définies par

$$f\big((a,b)\big) = \Big(\frac{a+b}{2}, \frac{a-b}{2}\Big) \quad \text{et} \quad g\big((r,s)\big) = (r+s, r-s),$$

sont réciproques l'une de l'autre. En effet, il suffit de remarquer que pour tout $(a,b) \in \mathbb{N}^2$, on a l'égalité

$$ab = \Big(\frac{a+b}{2}\Big)^2 - \Big(\frac{a-b}{2}\Big)^2,$$

et que si $n = r^2 - s^2$ où $(r,s) \in \mathbb{N}^2$, alors $n = (r+s)(r-s)$ et l'on a $r+s \geq r-s$.

Dans le cas où $n$ est le produit de deux entiers proches l'un de l'autre, il est facile d'écrire $n$ comme une différence de deux carrés, et donc de factoriser $n$. C'est l'idée de Fermat. Plus précisément, soit $\big[\sqrt{n}\big]$ la partie entière de $\sqrt{n}$. Supposons que l'on ait

$$n = ab \quad \text{où} \quad a \text{ et } b \text{ sont proches l'un de l'autre, avec } a \geq b.$$

Posons

$$r = \frac{a+b}{2} \quad \text{et} \quad s = \frac{a-b}{2}.$$

On a $n = r^2 - s^2$. L'entier $s$ est petit et $r$ est donc plus grand que $\sqrt{n}$ tout en lui étant proche. Par suite, il existe un petit entier naturel $u$ tel que

$$\big(\big[\sqrt{n}\big] + u\big)^2 - n \quad \text{soit un carré.}$$

Afin de déterminer un tel entier $u$, on examine successivement les entiers

$$\big[\sqrt{n}\big] + 1, \quad \big[\sqrt{n}\big] + 2, \cdots$$

et on teste pour chacun d'eux si son carré moins $n$ est un carré. Si l'on y parvient, on obtient $n$ comme une différence de deux carrés, ce qui fournit une factorisation de $n$.

**Exemples 3.5.**

1) Prenons

$$n = 3188572306041062120191724558058194008400870997412201337.$$

Il a cinquante-six chiffres décimaux. La méthode de Fermat permet facilement de factoriser $n$. On trouve

$$\left(\left[\sqrt{n}\right] + 1\right)^2 - n = 172^2,$$

d'où l'égalité

$$n = (r - 172)(r + 172) \quad \text{avec} \quad r = [\sqrt{n}] + 1.$$

On obtient ainsi $n = pq$, avec

$$p = 56467444656554648454848765 11 \quad \text{et} \quad q = 5646744465655464845484876167.$$

Les entiers $p$ et $q$ sont premiers et $p - q = 344$.

2) Avec $n = 2^{47} - 1$, on trouve que $u = 74013$ convient. On a en effet, l'égalité

$$\left(\left[\sqrt{n}\right] + 74013\right)^2 - n = 1327233^2.$$

On en déduit la factorisation

$$n = 10610063 \times 13264529,$$

d'où la décomposition complète de $n$,

$$n = 2351 \times 4513 \times 13264529.$$

3) Posons $n = 1099998619700431613$. On constate que l'on a

$$\left(\left[\sqrt{n}\right] + 1191153\right)^2 - n = 50000006^2,$$

d'où la factorisation

$$n = 999999337 \times 1099999349,$$

qui est un produit de deux nombres premiers.

## 5. L'approche de Kraitchik

Vers 1920 M. Kraitchik a raffiné la méthode de Fermat et son idée s'avère de nos jours très fructueuse. On l'a déjà rencontrée dans l'analyse du cryptosystème de Rabin : étant donné un entier impair composé $n$, si l'on dispose d'un procédé pour extraire les racines carrées modulo $n$, on sait factoriser $n$. Il s'agit de rechercher des entiers dont la différence de leurs carrés soit «seulement» un multiple de $n$, et pas $n$ a priori. Autrement dit, on cherche à expliciter des congruences entre des carrés modulo $n$. Supposons que l'on ait déterminé deux entiers $u$ et $v$ tels que

$$u^2 \equiv v^2 \text{ mod. } n \quad \text{avec} \quad u \not\equiv \pm v \text{ mod. } n. \tag{7}$$

Dans ce cas, on peut obtenir très simplement une factorisation de $n$, vu que $n$ divise $(u-v)(u+v)$ sans diviser $u-v$ ni $u+v$. Le calcul des entiers

$$\text{pgcd}(u-v,n) \quad \text{et} \quad \text{pgcd}(u+v,n),$$

fournit alors des diviseurs non triviaux de $n$.

**Remarque 3.2.** Supposons que $n$ ne soit pas une puissance d'un nombre premier. Alors, si $a$ et $b$ sont deux entiers premiers avec $n$ tels que $a^2 \equiv b^2$ mod. $n$, il y a plus d'une chance sur deux pour que l'on ait $a \not\equiv \pm b$ mod. $n$. En effet, $n$ a par hypothèse au moins deux facteurs premiers impairs. Par ailleurs, l'équation $x^2 = 1$ possède $2^t$ solutions modulo $n$, où $t$ est le nombre de diviseurs premiers de $n$. Elle a donc au moins quatre solutions, et deux au moins sont distinctes de $\pm 1$, d'où notre assertion.

Tout le problème est donc de trouver des entiers $u$ et $v$ vérifiant la condition (7). L'idée basique est de considérer le polynôme

$$Q(X) = X^2 - n \in \mathbb{Z}[X],$$

parfois appelé polynôme de Kraitchik, et de rechercher des entiers $x_i$ de sorte que le produit des $Q(x_i)$ soit un carré. Supposons que l'on ait déterminé de tels entiers $x_1, \cdots, x_k$. Posons

$$Q(x_1)\cdots Q(x_k) = v^2 \quad \text{où} \quad v \in \mathbb{N}. \tag{8}$$

En posant

$$u = x_1 \cdots x_k,$$

on obtient

$$u^2 \equiv (x_1^2 - n)\cdots(x_k^2 - n) = Q(x_1)\cdots Q(x_k) = v^2 \text{ mod. } n. \tag{9}$$

Comme on l'a remarqué ci-dessus, il y a une probabilité importante que l'on ait aussi $u \not\equiv \pm v$ mod. $n$, et le couple $(u, v)$ satisfait ainsi la condition (7). Toute la difficulté est précisément la détermination de tels entiers $x_i$. Illustrons cette idée sur un cas simple.

**Exemple 3.6.** Factorisons l'entier $n = 2041$. Posons $Q(X) = X^2 - 2041$. Le plus petit carré plus grand que $n$ est $46^2 = 2116$. Avec $x = 46, 47, 48, 49, 50, 51$, on obtient respectivement

$$Q(x) = 75, \quad 168, \quad 263, \quad 360, \quad 459, \quad 560.$$

Par ailleurs, on a

$$75 = 3 \times 5^2, \quad 168 = 2^3 \times 3 \times 7, \quad 360 = 2^3 \times 3^2 \times 5, \quad 560 = 2^4 \times 5 \times 7.$$

Le produit de ces entiers $2^{10} \times 3^4 \times 5^4 \times 7^2$ est un carré. Posons

$$u = 46 \times 47 \times 49 \times 51 \quad \text{et} \quad v = 2^5 \times 3^2 \times 5^2 \times 7.$$

D'après (9), on a $u^2 \equiv v^2$ mod. $n$, autrement dit

$$311^2 \equiv 1416^2 \text{ mod. } 2041,$$

d'où la factorisation $2041 = 13 \times 157$.

On se doute bien que ce n'est aussi toujours aussi facile. Le fait que l'on ait pu factoriser 2041 de cette façon semble relever du miracle. Comme on va le voir, c'est néanmoins le point de départ de méthodes modernes de factorisation.

## 6. Recherche de congruences de carrés

Soit $n$ un entier impair composé. On va décrire ici le principe de base visant à expliciter des congruences modulo $n$ entre carrés. Commençons par définir la notion d'entier friable.

**Définition 3.1.** *Soit $B$ un entier naturel. On dit qu'un entier est $B$-friable si tous ses diviseurs premiers sont inférieurs ou égaux à $B$.*

Conformément à l'approche de Kraitchik, afin de trouver des entiers $x_i$ tels que le produit des $Q(x_i)$ soit un carré, l'idée générale est la suivante. On se fixe au départ un entier $B$. Si l'on parvient à trouver suffisamment d'entiers $x_i \in \mathbb{N}$ tels que $Q(x_i)$ soit un entier naturel $B$-friable, alors en utilisant des algorithmes d'algèbre linéaire, on peut extraire une sous-famille non vide des $x_i$ pour laquelle le produit des $Q(x_i)$ correspondants soit un carré. En fait, il suffit d'en connaître $\pi(B) + 1$ en vertu du lemme crucial suivant.

**Lemme 3.2.** *Soient $k$ et $B$ des entiers naturels tels que $k \geq \pi(B)+1$. Soient $m_1, \cdots, m_k$ des entiers naturels $B$-friables. Il existe une sous-famille non vide des $m_i$ dont le produit est un carré.*

Démonstration : Par hypothèse, les diviseurs premiers de $m_i$ sont inférieurs ou égaux à $B$. Soit $p_j$ le $j$-ième nombre premier. Pour tout entier $i$ compris entre 1 et $k$, notons

$$m_i = \prod_{j=1}^{\pi(B)} p_j^{\alpha_{i,j}},$$

la décomposition de $m_i$ en produit de nombres premiers avec $\alpha_{i,j} \geq 0$. Posons

$$v(m_i) = \big(\alpha_{i,1}, \cdots, \alpha_{i,\pi(B)}\big).$$

Soit $M$ la matrice à coefficients dans $\mathbb{F}_2$, de taille $\big(k, \pi(B)\big)$, dont l'élément de la $i$-ème ligne et de la $j$-ième colonne est $\alpha_{i,j}$ modulo 2. Le rang de $M$ est au plus $\pi(B)$. Puisque l'on a $k \geq \pi(B)+1$, les vecteurs lignes de $M$ forment un système lié du $\mathbb{F}_2$-espace vectoriel $\mathbb{F}_2^{\pi(B)}$. Il existe donc $i_1, \cdots, i_t$ tels que les composantes du $\pi(B)$-uplet

$$v(m_{i_1}) + \cdots + v(m_{i_t})$$

soient toutes paires. Cela signifie que le produit $m_{i_1} \cdots m_{i_t}$ est un carré, d'où le résultat.

La démonstration de ce lemme fournit un procédé, issu de l'algèbre linéaire, pour expliciter une sous-famille non vide des $m_i$ dont le produit est un carré. Précisons cette démarche.

**Principe général.** Soit $B$ un entier naturel. Supposons que l'on dispose de $k$ entiers naturels $x_i$ tels que $Q(x_i)$ soit $B$-friable, avec

$$k \geq \pi(B)+1. \tag{10}$$

D'après le lemme 3.2, il existe une sous-famille des $Q(x_i)$ dont le produit est un carré. Voici comment on procède afin d'expliciter une telle sous-famille. Soit

$$Q(x_i) = \prod_{j=1}^{\pi(B)} p_j^{\alpha_{i,j}} \quad (1 \leq i \leq k),$$

la décomposition en facteurs premiers de $Q(x_i)$ avec $\alpha_{i,j} \geq 0$. Soit $M$ la matrice de taille $\big(k, \pi(B)\big)$ à coefficients dans $\mathbb{F}_2$, dont l'élément de la $i$-ème ligne et de la $j$-ième colonne est

$$\alpha_{i,j} \text{ mod. } 2.$$

Soit $\ell_i$ le $i$-ème vecteur ligne de $M$. D'après la condition (10), il existe un élément non nul

$$\big(\varepsilon_1, \cdots, \varepsilon_k\big) \in \mathbb{F}_2^k,$$

tel que l'on ait

$$\sum_{i=1}^{k} \varepsilon_i \ell_i = 0.$$

L'élément $\big(\varepsilon_1, \cdots, \varepsilon_k\big)$ appartient au noyau de la matrice transposée de $M$. Si $I$ est le sous-ensemble (non vide) de $\big\{1, \cdots, k\big\}$ formé des indices $i$ tels que $\varepsilon_i = 1$, on a

$$\sum_{i \in I} \ell_i = 0.$$

Il en résulte que l'entier

$$\prod_{i \in I} Q(x_i) \quad \text{est un carré,}$$

car c'est un produit de nombres premiers affectés d'exposants pairs. On a ainsi

$$u^2 \equiv v^2 \text{ mod. } n \quad \text{avec} \quad u = \prod_{i \in I} x_i \quad \text{et} \quad \prod_{i \in I} Q(x_i) = v^2.$$

En conclusion, si l'on connaît au moins $\pi(B) + 1$ entiers $x_i$ tels que $Q(x_i)$ soit $B$-friable, il suffit de déterminer une base du noyau de la matrice transposée de $M$ pour obtenir la condition souhaitée. On utilise pour cela des algorithmes standard d'algèbre linéaire. Compte tenu de la remarque 3.3, il est alors facile en pratique de trouver un élément de ce noyau pour lequel les entiers $u$ et $v$ obtenus vérifient la condition $u \not\equiv \pm v$ mod. $n$.

**Exemple 3.7.** Reprenons l'exemple 3.6, avec $n = 2041$. Choisissons $B = 7$. On a $\pi(B) = 4$ et il y a cinq entiers $x_i$ entre 46 et 53 tels que $Q(x_i)$ soit 7-friable. Ce sont $46, 47, 49, 51, 53$. On a respectivement $Q(x_i) = 75, 168, 360, 560, 768$. Avec les notations précédentes, on a

$$M = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

On constate ici directement que $\ell_1 + \ell_5 = 0$. Par suite, $Q(46) \times Q(53)$ est un carré, qui n'est autre que $2^8 \times 3^2 \times 5^2$. Cela conduit à la congruence

$$(46 \times 53)^2 \equiv (2^4 \times 3 \times 5)^2 \text{ mod. } 2041 \quad \text{i.e.} \quad 397^2 \equiv 240^2 \text{ mod. } 2041.$$

Par ailleurs, on a $\text{pgcd}(397 - 240, 2041) = 157$, d'où $n = 13 \times 157$.

**Exemple 3.8.** Prenons $n = 4333801$. Choisissons $B = 25$. On a $\pi(B) = 9$. Il y a dix entiers $x_i$ entre $\lceil\sqrt{n}\rceil + 1 = 2082$ et $\lceil\sqrt{n}\rceil + 10^3$ tels que $Q(x_i)$ soit $B$-friable. Il s'agit de

$$x_1 = 2086, \quad x_2 = 2099, \quad x_3 = 2131, \quad x_4 = 2147, \quad x_5 = 2221, \quad x_6 = 2247,$$

$$x_7 = 2351, \quad x_8 = 2477, \quad x_9 = 2776, \quad x_{10} = 2891.$$

Les entiers $Q(x_i)$ correspondants sont respectivement

$$17595, \quad 72000, \quad 207360, \quad 275808, \quad 599040, \quad 715208,$$

$$1193400, \quad 1801728, \quad 3372375, \quad 4024080.$$

La matrice $M$ qui leur est associée est de taille $(10, 9)$. On vérifie que

$$M = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Par ailleurs, $(0, 1, 0, 1, 1, 0, 1, 0, 0, 0)$ appartient au noyau de la matrice transposée de $M$. Autrement dit, on a

$$\ell_2 + \ell_4 + \ell_5 + \ell_7 = 0.$$

Cela signifie que $Q(x_2) \times Q(x_4) \times Q(x_5) \times Q(x_7)$ est un carré. C'est en fait

$$2^{24} \times 3^8 \times 5^6 \times 13^4 \times 17^2.$$

On en déduit la congruence

$$3827053^2 \equiv 4198908^2 \text{ mod. } n.$$

On a $\text{pgcd}\big(4198908 - 3827053, n\big) = 6761$, d'où $n = 641 \times 6761$.

**Remarque 3.3.** Dans la recherche d'entiers $x_i \in \mathbb{N}$ tels que $Q(x_i)$ soit $B$-friable, il suffit parfois avec de la chance, d'en déterminer nettement moins que $\pi(B) + 1$ pour conclure. Par exemple, posons $n = 7937773$. Prenons $B = 27$. On a $\pi(B) = 9$. Il y a trois entiers $x_i$ entre $\lceil\sqrt{n}\rceil + 1 = 2818$ et $\lceil\sqrt{n}\rceil + 10^5$ tels que $Q(x_i)$ soit 27-friable. Ce sont

$$2823, \quad 3973, \quad 22937.$$

On a

$$Q(2823) = 2^2 \times 7^3 \times 23, \quad Q(3973) = 2^2 \times 3^8 \times 13 \times 23,$$

$$Q(22937) = 2^2 \times 3^2 \times 7 \times 13^2 \times 23^3.$$

On voit aussitôt que $Q(2823) \times Q(22937)$ est un carré, d'où la congruence

$$1248967^2 \equiv 4043676^2 \text{ mod. } n.$$

Puisque l'on a $\text{pgcd}(4043676 - 1248967, n) = 3331$, on obtient $n = 2383 \times 3331$.

Dans la stratégie que l'on vient d'exposer, il se pose évidemment les problèmes suivants, pour lesquels on a donné jusqu'à présent aucune indication.

1) Comment choisir la constante $B$ de façon optimale en fonction de $n$ ?

2) Comment trouver efficacement environ $\pi(B)$ entiers $x$ tels que $Q(x)$ soit $B$-friable ?

Ces questions sont les points essentiels de la méthode du crible quadratique.

## 7. Le crible quadratique

La méthode du crible quadratique a été inventée par C. Pomerance en 1981. C'est aujourd'hui la méthode la plus couramment utilisée pour factoriser des entiers $n$ qui n'ont pas de diviseurs premiers significativement plus petits que $\sqrt{n}$. Elle ne dépend en fait que de la taille de $n$, i.e. de son nombre de chiffres décimaux, et non de propriétés arithmétiques particulières de ses diviseurs premiers. Avec cette méthode on parvient, avec des moyens informatiques adéquates, à factoriser tout entier ayant jusqu'à cent vingt chiffres décimaux.

Soit $n$ un entier impair composé. Afin de factoriser $n$, on recherche des congruences modulo $n$ entre carrés. Il s'agit donc de choisir une constante $B$ convenable et d'expliciter suffisamment d'entiers $x_i$ tels que $Q(x_i) = x_i^2 - n$ soit $B$-friable.

### 1. Principe du crible

On se donne au départ une constante $B$ et une borne $X$. Commençons par examiner le problème de détecter tous les entiers $B$-friables de l'intervalle $[1, X]$.

La première approche à laquelle on peut penser est d'utiliser la méthode des divisions successives. Autrement dit, on divise chaque entier de l'intervalle $[1, X]$ par tous les nombres premiers plus petits que $B$, en tenant compte des exposants éventuels. Les entiers $B$-friables sont exactement ceux pour lesquels les quotients obtenus après ces divisions valent 1. Ce procédé nécessite environ $\pi(B)$ divisions par entier, soit en tout $X\pi(B)$ divisions. L'ordre de grandeur de $\pi(B)$ étant $\frac{B}{\log B}$, cela est très coûteux si $B$ est grand.

Le principe du crible consiste plutôt, pour chaque nombre premier $p \leq B$, à repérer très facilement tous les entiers de $[1, X]$ divisibles par $p$ ou par une puissance de $p$. Ce procédé rappelle celui du crible d'Eratosthène qui permet de déterminer tous les nombres

premiers de $[1, X]$. Rappelons son principe. On écrit dans un tableau tous les entiers entre 2 et $X$. On commence par le nombre 2 et on barre avec «des pas de longueur 2» tous les multiples stricts de 2. Le premier entier non barré est ensuite 3, et on barre tous les multiples stricts de 3 avec «des pas de longueur 3». En effectuant ce processus pour tous les entiers plus petits que $\sqrt{X}$, les entiers qui n'ont pas été barrés sont tous les nombres premiers plus petits que $X$.
En ce qui concerne la recherche des entiers $B$-friables de $[1, X]$, on procède de façon analogue. On construit au départ un tableau contenant tous les entiers entre 1 et $X$. Pour chaque nombre premier $p \leq B$, on «parcourt» le tableau comme suit. En commençant avec l'entier $p$, et en effectuant successivement des pas de longueur $p$, on divise par $p$ tous les entiers possibles dans le tableau, qui ne sont autres que les multiples de $p$ plus petits que $X$. On obtient alors un nouveau tableau d'entiers entre 1 et $X$ qui diffère du précédent seulement «aux cases d'entiers» multiples de $p$. En commençant avec l'entier $p$, qui est maintenant à la case $p^2$, et en effectuant successivement des pas de longueur $p^2$, on divise de nouveau par $p$ tous les entiers possibles du nouveau tableau. On procède de même jusqu'à la plus grande puissance de $p$ inférieure à $X$, qui est $p^k$ avec $k \leq \left[\frac{\log X}{\log p}\right]$. Lorsque l'on a effectué ce processus pour tous les nombres premiers $p \leq B$, on obtient un tableau dans lequel les cases où se trouvent le chiffre 1 sont exactement celles du départ des entiers $B$-friables. On a ainsi localisé très facilement toutes les cases du tableau de départ dans lesquelles se trouvait un entier $B$-friable. Le temps d'exécution de ce crible est beaucoup plus rapide que celui de la méthode des divisions successives. Le nombre d'opérations à effectuer pour cribler un nombre premier $p \leq B$ est proportionnel à $\frac{X}{p}$. Par ailleurs, on peut démontrer que pour tout $B > 1$, on a

$$\log\log B < \sum_{p \leq B} \frac{1}{p} < \log\log B + C + \frac{1}{\log^2 B},$$

où $C = 0,261\cdots$ est une constante absolue. On doit donc effectuer pour le crible complet «environ» $X \log\log B$ opérations, ce qui beaucoup plus petit que $X\pi(B)$.

**Exemple 3.9.** Il faut vingt secondes sur Pari pour cribler tous les entiers plus petits que $10^7$ qui sont 3-friables. Il y en a cent quatre vingt neuf,

$$2, 3, 4, \cdots, 27648, \cdots, 442368, \cdots, 2359296, \cdots, 5971968 = 2^{13}.3^6, \cdots 9565938 = 2.3^{14}.$$

Cela étant, afin de factoriser $n$, ce qui nous importe est la recherche des entiers $B$-friables de la forme $Q(x)$, où $Q(X) = X^2 - n$, lorsque $x$ parcourt les entiers d'un intervalle

$$I = [\sqrt{n}, \sqrt{n} + A],$$

où $A$ est une certaine constante qui dépend de $n$ et $B$. Ce n'est pas aussi simple que la recherche des entiers $B$-friables de $I$, mais l'idée est la même. On utilise le lemme suivant.

**Lemme 3.3.** *Soit $p$ un nombre premier impair tel que $n$ soit un carré non nul modulo $p$. Soit $k$ un entier $\geq 1$.*

*1) Le polynôme $Q(X)$ a exactement deux racines modulo $p^k$.*

*2) Soit $a$ un entier tel que $Q(a) \equiv 0$ mod. $p^k$. Il existe un entier $b$ compris entre 1 et $p-1$ tel que $2ab \equiv 1$ mod. $p$. On a*

$$Q\big(a + (n - a^2)b\big) \equiv 0 \text{ mod. } p^{k+1}.$$

Démonstration : 1) La première assertion provient du fait que le groupe $\big(\mathbb{Z}/p^k\mathbb{Z}\big)^*$ est cyclique et de l'exercice 6 de la feuille de travaux dirigés de ce chapitre.
2) D'après l'hypothèse faite, $2a$ est inversible modulo $p$. Soit $b$ l'entier compris entre 1 et $p-1$ tel que $2ab \equiv 1$ mod. $p$. On obtient

$$Q\big(a + (n - a^2)b\big) = (a^2 - n)(1 - 2ab) + (n - a^2)^2 b^2 \equiv 0 \text{ mod. } p^{k+1},$$

d'où le lemme.

On commence par construire un tableau $T_0$, dans lequel se trouvent les $Q(x)$ où $x$ parcourt les entiers de $I$. Ils sont « rangés dans des cases » par ordre croissant, autrement dit, dans la $k$-ième case se trouve l'entier

$$([\sqrt{n}] + k)^2 - n.$$

Pour chaque nombre premier $p \leq B$ tel que $n$ soit un carré modulo $p$, l'idée est de localiser à intervalles réguliers les entiers $Q(x)$ qui sont divisibles par $p$ et par les puissances de $p$ éventuelles, en utilisant le lemme ci-dessus. Après avoir divisé par $p$ « suffisamment d'entiers convenables », on obtient à la fin un tableau dans lequel les cases où apparaît le chiffre 1 correspondent à celles des entiers $Q(x)$ qui sont $B$-friables.

Plus précisément, soit $p$ un nombre premier impair inférieur à $B$. On peut supposer que $p$ ne divise pas $n$, sinon on a trouvé un facteur non trivial de $n$. On est alors dans l'un des cas suivants.

1) Si $\left(\frac{n}{p}\right) = -1$ i.e. si $n$ n'est pas un carré modulo $p$, aucun des entiers $Q(x)$ n'est divisible par $p$, et dans ce cas il n'y a pas de crible à effectuer pour $p$.

2) Supposons $\left(\frac{n}{p}\right) = 1$. Puisque $p$ ne divise pas $n$, il existe deux plus petits entiers $a_1$ et $a_2$ distincts modulo $p$, vérifiant les conditions

$$a_i \geq \big[\sqrt{n}\big] + 1 \quad \text{et} \quad Q(a_i) \equiv 0 \text{ mod. } p.$$

On divise alors par $p$ l'entier $Q(a_1)$ et ceux qui se déduisent de $Q(a_1)$ successivement par des pas de longueur de $p$. Ce sont les entiers de la forme $Q(a_1 + jp)$ où $j = 0, 1, \cdots$. On effectue les mêmes opérations en ce qui concerne $Q(a_2)$. On obtient ainsi un nouveau tableau $T_1$ qui diffère de $T_0$ seulement aux entiers $Q(a_i + jp)$ qui sont remplacés par $\frac{Q(a_i+jp)}{p}$.

On repère ensuite dans $T_1$ les entiers divisibles par $p$, autrement dit les entiers de $T_0$ divisibles par $p^2$. Puisque $p$ est impair, le polynôme $Q(X)$ a exactement deux racines modulo $p^2$, que l'on connaît explicitement en fonction de $a_1$ et $a_2$ (lemme 6.3). Soient $b_1$ et $b_2$ les plus petits entiers distincts modulo $p^2$ tels que

$$b_i \geq \left[\sqrt{n}\right] + 1 \quad \text{et} \quad Q(b_i) \equiv 0 \text{ mod. } p^2.$$

Dans le tableau $T_1$, on divise alors $\frac{Q(b_1)}{p}$ par $p$, puis successivement les entiers de $T_1$ qui se déduisent de $\frac{Q(b_1)}{p}$ par des pas de longueur $p^2$. On fait de même en ce qui concerne $\frac{Q(b_2)}{p}$. On recommence ce processus jusqu'à la plus grande puissance de $p$ possible divisant un entier $Q(x)$ de $T_0$.

Supposons maintenant $p = 2$. Dans ce cas, le premier entier $Q(x)$ pair de $T_0$ est $\left([\sqrt{n}] + 1\right)^2 - n$ ou $\left([\sqrt{n}] + 2\right)^2 - n$, et l'on crible tous les $Q(x)$ pairs par des pas de longueur 2. Si l'on a $n \equiv 3$ mod. 4, il n'y a aucun $Q(x)$ divisible par 4 et le crible s'arrête. Si l'on a $n \equiv 5$ mod. 8, le polynôme $Q$ a deux racines modulo 4 et n'a pas de racine modulo 8. Si l'on a $n \equiv 1$ mod. 8, pour tout $t \geq 3$ le polynôme $Q$ a quatre racines modulo $2^t$. Dans les deux cas, le principe du criblage reste le même.

**2. Choix de la constante $B$**

Ce choix est difficile. Si $B$ est petit, il suffit d'un petit nombre d'entiers $x$ tels que $Q(x)$ soit $B$-friable pour conclure. Malheureusement, il est vraisemblable que l'on ne parviendra pas à expliciter un seul entier $x$ ayant cette propriété. Si $B$ est trop grand, il faudra obtenir un grand nombre de tels entiers $x$, ce qui risque d'être prohibitif. Il s'agit donc de trouver un compromis.

Étant donné un entier $B$, on est ainsi confronté au problème d'estimer la fréquence des entiers $Q(x)$ qui sont $B$-friables où $x$ est dans un intervalle d'origine $\sqrt{n}$, en fonction de $B$ et $n$. Pour cela, choisissons un intervalle $I$ de la forme

$$I = \left[n^{\frac{1}{2}}, n^{\frac{1}{2}} + n^{\varepsilon}\right] \quad \text{où} \quad 0 < \varepsilon < \frac{1}{2}.$$

Pour tout $x \in I$ on a

$$0 \leq Q(x) \leq 2n^{\frac{1}{2}+\varepsilon} + n^{2\varepsilon}.$$

On a $2n^{\frac{1}{2}+\varepsilon} + n^{2\varepsilon} = 2n^{\frac{1}{2}+\varepsilon}\big(1 + o(1)\big)$, où $o(1)$ est une fonction de $n$ tendant vers zéro quand $n$ tend vers l'infini. Ainsi, $Q(x)$ est « approximativement » plus petit que $2n^{\frac{1}{2}+\varepsilon}$. Admettons que la probabilité pour qu'un entier de la forme $Q(x)$ plus petit que $2n^{\frac{1}{2}+\varepsilon}$ soit $B$-friable, soit la même que celle pour qu'un entier choisi au hasard dans $\left[1, 2n^{\frac{1}{2}+\varepsilon}\right]$ le soit aussi. On est alors amené à optimiser $B$ pour trouver, aléatoirement, environ $\pi(B)$ entiers $B$-friables dans $\left[1, 2n^{\frac{1}{2}+\varepsilon}\right]$. Décrivons une heuristique qui laisse penser que l'on peut prendre pour $B$ une constante de l'ordre de

$$\exp\Big(\frac{1}{2}\sqrt{\log(n)\log\log(n)}\Big). \tag{11}$$

### 2.1. La fonction $\psi(X,Y)$

Pour tout nombre réel $Y > 0$, on dira qu'un entier est $Y$-friable s'il est $[Y]$-friable. Pour tous réels $X$ et $Y$ positifs, notons $\psi(X,Y)$ le nombre d'entiers $Y$-friables de l'intervalle $[1,X]$. La probabilité pour qu'un entier aléatoire de $[1,X]$ soit $Y$-friable est $\frac{\psi(X,Y)}{[X]}$, donc environ $\frac{\psi(X,Y)}{X}$. Commençons par estimer ce rapport si $Y = X^{\frac{1}{2}}$.

**Proposition 3.2.** *Lorsque $X$ tend vers l'infini, on a*

$$\lim \frac{\psi\big(X, X^{\frac{1}{2}}\big)}{X} = 1 - \log 2.$$

Démonstration : Pour chaque nombre premier $p \leq X$, il y a exactement $\big[\frac{X}{p}\big]$ entiers multiples de $p$ inférieurs à $X$. Par ailleurs, il n'y pas d'entiers plus petits que $X$ divisibles par deux nombres premiers distincts strictement plus grands que $X^{\frac{1}{2}}$. On a ainsi

$$\psi\big(X, X^{\frac{1}{2}}\big) = [X] - \sum_{X^{\frac{1}{2}} < p \leq X} \Big[\frac{X}{p}\Big].$$

En omettant les parties entières dans cette égalité, on commet une erreur d'au plus $\pi(X)$. Puisque l'on a

$$\pi(X) = O\Big(\frac{X}{\log X}\Big),$$

on obtient

$$\psi\big(X, X^{\frac{1}{2}}\big) = X\left(1 - \sum_{X^{\frac{1}{2}} < p \leq X} \frac{1}{p}\right) + O\Big(\frac{X}{\log X}\Big).$$

Comme on l'a déjà signalé, il existe une constante $C$ telle que l'on ait pour $t$ assez grand

$$\sum_{p \leq t} \frac{1}{p} = \log\log t + C + O\Big(\frac{1}{\log t}\Big).$$

En écrivant que l'on a

$$\sum_{X^{\frac{1}{2}} < p \leq X} \frac{1}{p} = \sum_{p \leq X} \frac{1}{p} - \sum_{p \leq X^{\frac{1}{2}}} \frac{1}{p},$$

on obtient quand $X$ tend vers l'infini

$$\sum_{X^{\frac{1}{2}} < p \leq X} \frac{1}{p} = \log\log X - \log\log X^{\frac{1}{2}} + O\Big(\frac{1}{\log X}\Big),$$

autrement dit,

$$\sum_{X^{\frac{1}{2}} < p \leq X} \frac{1}{p} = \log 2 + O\Big(\frac{1}{\log X}\Big).$$

Cela conduit à l'égalité

$$\psi\big(X, X^{\frac{1}{2}}\big) = (1 - \log 2)X + O\Big(\frac{X}{\log X}\Big),$$

d'où l'assertion.

**Remarque 3.4.** L'énoncé précédent signifie qu'environ trente pour cent des entiers n'ont pas de diviseurs premiers plus grands que leur racine carrée.

Plus généralement, Dickman en 1930 a établi que pour tout $u > 0$, il existe un nombre réel $\rho(u) > 0$ tel que l'on ait, quand $X$ tend vers l'infini,

$$\lim \frac{\psi\big(X, X^{\frac{1}{u}}\big)}{X} = \rho(u).$$

De plus, si $u$ est dans l'intervalle $[1, 2]$, on a $\rho(u) = 1 - \log u$. On ne connaît pas d'expression de $\rho(u)$ en termes de fonctions élémentaires dans le cas où $u > 2$. On peut en fait approcher numériquement la fonction $\rho$ et il apparaît qu'elle décroît rapidement vers 0 quand $u$ devient grand, approximativement comme la fonction $u^{-u}$. Cela a été précisé en 1983 par Canfield, Erdös et Pomerance.

### 2.2. Optimisation

Pour $X$ grand, afin de rechercher aléatoirement environ $\pi(B)$-entiers $B$-friables dans $[1, X]$, ce qui précède suggère de choisir $B$ de la forme

$$B = X^{\frac{1}{u}},$$

où $u$ est une fonction de $X$ à déterminer pour optimiser cette recherche. Voici comment procéder « très heuristiquement ». En choisissant aléatoirement des entiers entre 1 et $X$, on doit s'attendre à ce qu'au bout de

$$\frac{X}{\psi\big(X, X^{\frac{1}{u}}\big)}$$

choix, on détecte un entier $B$-friable. Puisqu'il nous en faut à peu près $\pi(B)$, cela conduit à

$$\frac{\pi(B)X}{\psi\big(X, X^{\frac{1}{u}}\big)}$$

choix d'entiers entre 1 et $X$. Parmi ces entiers, afin de détecter ceux qui sont $B$-friables avec le crible quadratique, il faut effectuer en moyenne $\log\log B$ opérations par entier. On est donc amené à minimiser l'expression

$$\frac{(\log\log B)\pi(B)X}{\psi\big(X, X^{\frac{1}{u}}\big)}.$$

Quand $B$ est grand, $\pi(B)$ est équivalent à $\frac{B}{\log B}$. Approximons grossièrement

$$\pi(B)\log\log B \quad \text{par } B \qquad \text{et} \quad \frac{X}{\psi\big(X, X^{\frac{1}{u}}\big)} \quad \text{par} \quad u^u.$$

On est alors amené à essayer de trouver $u$ de sorte que

$$X^{\frac{1}{u}}u^u \text{ soit minimal.} \tag{12}$$

Autrement dit, il s'agit de trouver $u$, comme fonction de $X$, de sorte que

$$\frac{\log X}{u} + u\log u \quad \text{soit minimal.}$$

La dérivée de cette fonction de $u$ est $1 + \log u - \frac{\log X}{u^2}$. Elle est nulle si l'on a

$$u^2(1+\log u) = \log X.$$

En prenant le logarithme des deux membres de cette égalité, on en déduit que

$$\log u \quad \text{est de l'ordre de} \quad \frac{1}{2}\log\log X.$$

Il en résulte qu'avec la fonction

$$u(X) = \left(\frac{2\log X}{\log\log X}\right)^{\frac{1}{2}},$$

on obtient une assez bonne approximation de la condition (12). Cela conduit à l'égalité

$$B = \exp\left(\frac{1}{\sqrt{2}}\big(\log X\log\log X\big)^{\frac{1}{2}}\right).$$

Cela signifie que lorsque $X$ est grand, cette valeur de $B$ semble être un compromis efficace pour détecter aléatoirement environ $\pi(B)$ entiers $B$-friables dans l'intervalle $[1, X]$.

Avec $X = 2n^{\frac{1}{2}+\varepsilon}$ où $0 < \varepsilon < \frac{1}{2}$, on obtient

$$B = \exp\Big(\frac{1}{2}\big(1+o(1)\big)\sqrt{\log(n)\log\log(n)}\Big),$$

$o(1)$ étant une fonction de $n$ tendant vers zéro quand $n$ tend vers l'infini. Cela explique heuristiquement l'estimation (11) pour $B$.

De plus, on obtient

$$X^{\frac{1}{u}}u^u = \exp\Big(\sqrt{2}\big(1+o(1)\big)\big(\log X\log\log X\big)^{\frac{1}{2}}\Big),$$

où $o(1)$ est une fonction de $X$ tendant vers zéro. Ainsi, $X^{\frac{1}{u}}u^u$ est de l'ordre de $B^2$ pour $X$ grand. Sommairement, cela signifie, qu'avec ce choix de $B$, le nombre d'étapes de calculs nécessaires pour déterminer $\pi(B)$ entiers $B$-friables, est asymptotiquement de l'ordre de

$$\exp\Big(\sqrt{\log(n)\log\log(n)}\Big).$$

**Exemples 3.10.** On factorise ci-dessous certains entiers $n$ par la méthode du crible. On a suivi l'heuristique précédente en ce qui concerne le choix de $B$. On a recherché les entiers $x_i$ tels que $Q(x_i)$ soient $B$-friables dans des intervalles de la forme $\big[\sqrt{n}+1, \sqrt{n}+A\big]$, en choisissant $A$ jusqu'à pouvoir conclure, et de sorte que son ordre de grandeur soit, a priori, bien adapté. Dans chacun des cas, il a suffit d'en détecter moins de $\pi(B)$, mais néanmoins un nombre significatif par rapport à $\pi(B)$. Précisons qu'il s'agit seulement ici d'illustrer numériquement la méthode du crible. Bien entendu, elle n'est pas nécessaire pour factoriser les entiers que l'on va considérer.

1) Posons $n = 39335476910299$. On prend

$$B = 179.$$

On a $\pi(B) = 41$ et $\big[\sqrt{n}\big] = 6271800$. Il y a trente-trois entiers $x_i$ entre $\big[\sqrt{n}\big] + 1$ et $\big[\sqrt{n}\big] + 3.10^5$ tels que $Q(x_i)$ soit $B$-friable. Il s'agit des entiers

$$x_1 = 6274946, \quad x_2 = 6277786, \quad 6277808, 6278707, 6280186, 6283157,$$

$$x_7 = 6283293, \quad x_8 = 6283753, \quad 6283977, 6287697, 6294428, 6295382,$$

$$6301670, 6303083, 6303232, 6318023, 6328666, 6333691,$$

$$6344493, 6352357, 6359493, 6392182, 6392213, 6392977,$$

$$6407082, 6419668, 6420749, 6423277, 6448368, 6470993,$$

$$6523322, 6555475, \ x_{33} = 6558557.$$

On est donc confronté ici au problème de trouver un élément du noyau d'une matrice à coefficients dans $\mathbb{F}_2$ de taille $(41, 33)$. On constate qu'avec

$$I = \Big\{1, 2, 4, 5, 8, 9, 14, 15, 18, 21, 26\Big\},$$

le produit des $Q(x_i)$ pour $i \in I$ est un carré. En posant

$$\prod_{i\in I} Q(x_i) = v^2 \quad \text{et} \quad \prod_{i\in I} x_i = u,$$

on a $u^2 \equiv v^2$ mod. $n$, ce qui entraîne la congruence

$$348465955513272 \equiv 95970596900142 \text{ mod. } n.$$

On a

$$\text{pgcd}\big(9597059690014 - 34846595551327, n\big) = 8251183,$$

d'où la factorisation,

$$n = 4767253 \times 8251183.$$

2) Posons $n = \frac{10^{17}-1}{9}$. Prenons

$$B = 321.$$

On a $\pi(B) = 66$. Il y a cinquante entiers $x_i$ entre $\lceil\sqrt{n}\rceil + 1 = 105409256$ et $\lceil\sqrt{n}\rceil + 2.10^5$ tels que $Q(x_i)$ soit $B$-friable,

$$x_1 = 105409384, \quad x_2 = 105409399, \quad \cdots, x_{50} = 105601519.$$

On obtient ici la congruence,

$$38544113223272102 \equiv 60507313258540652 \text{ mod. } n.$$

Par ailleurs, on a

$$\text{pgcd}\big(60507313258540652 - 38544113223272102, n\big) = 5363222357,$$

d'où la factorisation,

$$n = 2071723 \times 5363222357.$$

3) Reprenons l'exemple de Cole avec $n = 2^{67} - 1$. On prend

$$B = 792.$$

On a $\pi(B) = 138$. Il y a cent entiers $x_i$ entre $\lceil\sqrt{n}\rceil + 1$ et $\lceil\sqrt{n}\rceil + 2.10^6$ tels que $Q(x_i)$ soit $B$-friable,

$$x_1 = 12148002413, \quad \cdots x_{50} = 12148598437, \quad \cdots, x_{100} = 12149926938.$$

On en déduit la congruence

$$8843393584764750876^2 \equiv 3706011195060823215^2 \text{ mod. } n,$$

ce qui permet de retrouver le facteur premier 761838257287 de $n$.