Algorithmes pour l'arithmétique II
Cours 7

Julien Lavauzelle

Université Paris 8

Master 2 ACC – Algorithmes pour l'arithmétique

17/11/2022

La semaine dernière

Questions ?

Plan

Périodicité des suites récurrentes finies

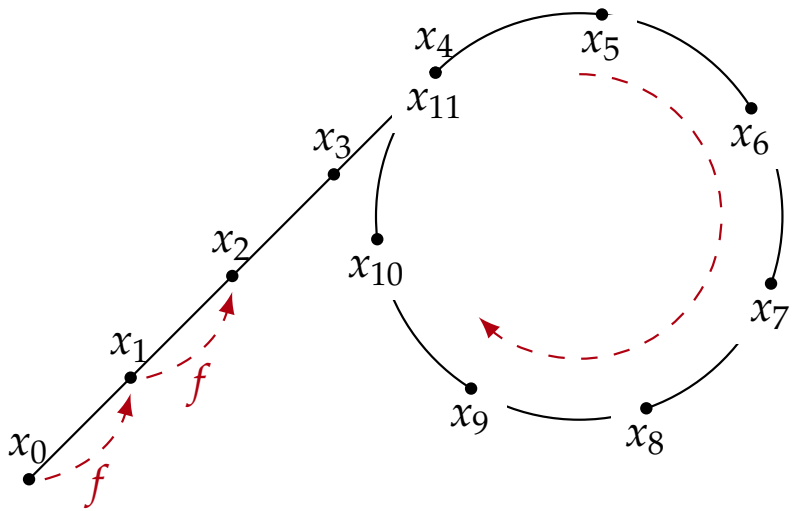
Contexte. Soit E un ensemble fini de cardinal M, et f une fonction $E \to E$. Étant donné $x_0 \in E$, on définit une suite récurrente $(x_t)_{t\geq 0}$ par

$$x_{t+1} = f(x_t)\,.$$

Alors on sait que $(x_t)_{t\geq 0}$ est ultimement périodique :

$$\exists T \geq 0, \exists \tau \geq 1, \forall t \geq T,\ x_{t+\tau} = x_t\,.$$

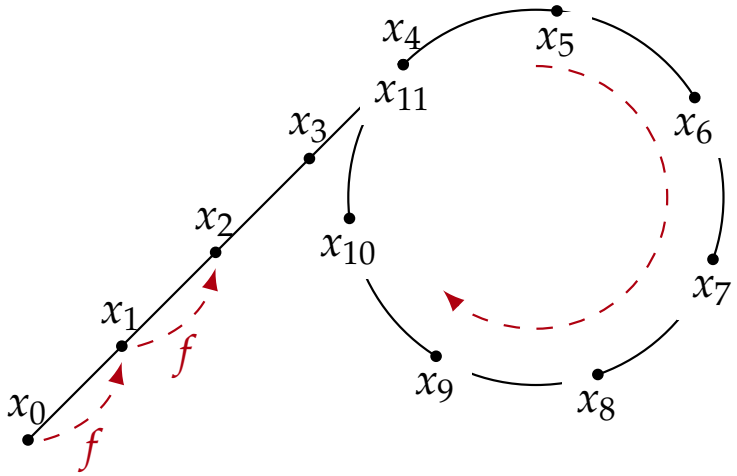
Déf. Le plus petit τ est appelé la **période**. Le plus petit T est appelé la **prépériode**.



Sur l'exemple, on a

- une période de 7,
- et une prépériode de 11.

Périodicité des suites récurrentes finies



Question. Si f et x_0 sont aléatoires, quelle est la taille typique de T ?

On a $T > m$, si et seulement si les $\{x_t\}_{t \le m}$ sont distincts.
Si f donne une suite aléatoire, on a donc d'après le **paradoxe des anniversaires** :

$$\begin{aligned}\mathbb{P}(T > m) &= \mathbb{P}(x_1 \neq x_0) \times \mathbb{P}(x_2 \notin \{x_1, x_0\}) \times \cdots \times \mathbb{P}(x_m \notin \{x_{m-1}, \ldots, x_0\}) \\ &= \left(1 - \frac{1}{M}\right)\left(1 - \frac{2}{M}\right) \ldots \left(1 - \frac{m}{M}\right) \simeq e^{-m^2/2M} \quad \text{pour } m \ll M\,.\end{aligned}$$

Conséquence. Avec grande probabilité, la suite $(x_t)_{t \ge 0}$ a une prépériode de taille $O(\sqrt{M})$.

Application à la factorisation

Soit $N \in \mathbb{Z}$ à factoriser, et p son plus petit facteur premier, inconnu.

Idée : On prend $E = \mathbb{Z}/N\mathbb{Z}$, et on choisit $x_0 \in \mathbb{Z}/NZ$ aléatoire et $f \in \mathbb{Z}/N\mathbb{Z}[X]$ au comportement itéré aléatoire (heuristique). Alors,

- la suite $(x_t \mod p)_{t\geq 0}$ a une prépériode de taille $O(\sqrt{p})$,
- sans connaître p, on peut détecter une collision pour $x_t \mod p$ en calculant $\mathrm{pgcd}(x_j - x_i, N)$.

En **pratique**, des fonctions du type $f(z) = z^2 + a$, avec $a \neq 0$ (ex : $a = 1$), ont un comportement suffisamment aléatoire pour que l'analyse probabiliste tienne.

Avantage : très efficace à calculer.

Question. Comment détecter la collision $\mathrm{pgcd}(x_j - x_i, N)$?

Méthode naïve :

- pour chaque nouvel x_j calculé, on teste la collision potentielle avec les x_i calculés antérieurement ;
- complexité quadratique en j en temps, linéaire en espace.

Remarque : si $\mathrm{pgcd}(x_j - x_i, N) = N$ sans avoir obtenu de facteur propre auparavant, il faut changer x_0.

$\Longrightarrow$ Il existe un meilleur algorithme, dû à Floyd.

Algorithme de Floyd (années 1960)

Lemme. Soit $(x_t)_{t\geq 0}$ une suite de prépériode T et de période τ. Alors, il existe $i \leq T-1$ tel que $x_{2i} = x_i$.

Preuve. La différence entre les indices $2i$ et i vaut i. Au moins l'un des $i \leq T-1$ est divisible par la période τ, ce qui assure que $x_{2i} = x_i$.

Exemple. $N = 11 \times 13 = 143$, donc $\sqrt{N} \lesssim 12$ et $\sqrt{p} = \sqrt{11} \lesssim 4$.

avec $x_0 = 133$

i	x_i	$y_i = x_{2i}$
0	133	133
1	101	49
2	49	127
3	114	127
4	127	127
5	114	127
6	127	127
7	114	127
8	127	127

période = 2
prépériode = 4

avec $x_0 = 34$

i	x_i	$y_i = x_{2i}$
0	34	34
1	13	27
2	27	83
3	15	105
4	83	83
5	26	105
6	105	83
7	15	105
8	83	83

période = 4
prépériode = 4

Algorithme ρ de Pollard

ALGORITHME ρ DE POLLARD POUR LA FACTORISATION (1975)

Entrée : un entier N composé
Sortie : un facteur d de N
Donnée externe : une fonction $f : \mathbb{Z}/N\mathbb{Z} \to \mathbb{Z}/\mathbb{Z}$, typiquement $f(z) = z^2 + 1 \mod N$

1. Tirer a uniformément dans $\{0, \ldots, N-1\}$
2. Initialiser $x \leftarrow f(a)$ et $y \leftarrow f(f(a))$
3. Calculer $d = \text{pgcd}(y - x, N)$
4. **Tant que** $d = 1$:
   - Calculer $x \leftarrow f(x)$
   - Calculer $y \leftarrow f(f(y))$
   - Calculer $d = \text{pgcd}(y - x, N)$
5. Si $d = N$, revenir à l'étape 1.
6. Sinon, retourner d.

Complexité.

- Le nombre d'itérations de la boucle 4. est $O(\sqrt{p})$ avec grande probabilité, où p est le plus petit facteur premier de N.
- On a $\text{pgcd}(y - x, N) = N$ avec faible probabilité : cela correspond à avoir une collision dans $\mathbb{Z}/N\mathbb{Z}$ avant d'en avoir dans des $\mathbb{Z}/p_i\mathbb{Z}$.

$\Longrightarrow$ complexité en $O(\sqrt{p}\log^2 N)$ opérations dans $\mathbb{Z}/N\mathbb{Z}$.

Pollard ρ : exemple

Exemple. Pollard ρ avec $N = 4307$

avec $x_0 = 2747$

x_i	$y_i = x_{2i}$	$\text{pgcd}(x_i - y_i, N)$
146	4089	1
4089	370	1
148	3451	1
370	2027	1
3384	370	1
3451	3451	4307

Pas de chance...

avec $x_0 = 2748$

x_i	$y_i = x_{2i}$	$\text{pgcd}(x_i - y_i, N)$
1334	766	1
766	2188	1
1005	1267	1
2188	620	1
2268	3502	1
1267	2435	73

C'est bon : $N = 73 \times 59$

Pour $N = 4307$, il y a 516 « mauvais » x_0 : proportion $\simeq 0.12$.

Fait. La proportion de « mauvais » x_0 diminue heuristiquement :

- Pour $N = 253$, il y a 98 « mauvais » x_0 : proportion $\simeq 0.38$.
- Pour $N = 1511057$, il y a 4378 « mauvais » x_0 : proportion $\simeq 0.0029$...

Plan

Nombres friables

Définition. Soit $B \geq 2$. Un entier $N \geq 2$ est B-friable (*B-smooth*) si tous ses diviseurs premiers sont plus petits que B.

Nombres friables

Définition. Soit $B \geq 2$. Un entier $N \geq 2$ est B-friable (*B-smooth*) si tous ses diviseurs premiers sont plus petits que B.

Définition. Soit $B \geq 2$. Un entier $N \geq 2$ est B-superfriable (*B-powersmooth*) si tous les p^e (avec p premier) qui divisent N satisfont $p^e \leq B$.

Nombres friables

Définition. Soit $B \geq 2$. Un entier $N \geq 2$ est B-friable (*B-smooth*) si tous ses diviseurs premiers sont plus petits que B.

Définition. Soit $B \geq 2$. Un entier $N \geq 2$ est B-superfriable (*B-powersmooth*) si tous les p^e (avec p premier) qui divisent N satisfont $p^e \leq B$.

Exemple. $N = 720 = 2^4 \times 3^2 \times 5$

- 720 est 5-friable,
- 720 n'est pas 5-superfriable, car $3^2 > 5$,
- 720 est 16-superfriable.

Nombres friables

Définition. Soit $B \geq 2$. Un entier $N \geq 2$ est B-friable (*B-smooth*) si tous ses diviseurs premiers sont plus petits que B.

Définition. Soit $B \geq 2$. Un entier $N \geq 2$ est B-superfriable (*B-powersmooth*) si tous les p^e (avec p premier) qui divisent N satisfont $p^e \leq B$.

Exemple. $N = 720 = 2^4 \times 3^2 \times 5$

- 720 est 5-friable,
- 720 n'est pas 5-superfriable, car $3^2 > 5$,
- 720 est 16-superfriable.

Théorème. Soit $C_{N,B}$ le nombre d'entiers B-friables entre 1 et N. On a asymptotiquement

$$\frac{C_{N,B}}{N} \sim u^{-u+o(1)} \quad \text{où } u = \frac{\log_2 N}{\log_2 B}$$

Nombres friables

Définition. Soit $B \geq 2$. Un entier $N \geq 2$ est B-friable (*B-smooth*) si tous ses diviseurs premiers sont plus petits que B.

Définition. Soit $B \geq 2$. Un entier $N \geq 2$ est B-superfriable (*B-powersmooth*) si tous les p^e (avec p premier) qui divisent N satisfont $p^e \leq B$.

Exemple. $N = 720 = 2^4 \times 3^2 \times 5$

- 720 est 5-friable,
- 720 n'est pas 5-superfriable, car $3^2 > 5$,
- 720 est 16-superfriable.

Théorème. Soit $C_{N,B}$ le nombre d'entiers B-friables entre 1 et N. On a asymptotiquement

$$\frac{C_{N,B}}{N} \sim u^{-u+o(1)} \quad \text{où } u = \frac{\log_2 N}{\log_2 B}$$

La probabilité que N soit N^ε-friable est donc $\varepsilon^{-\varepsilon}$.

- si $B = O(\sqrt{N})$, alors N est B-friable avec probabilité $1/4$.
- si $B = N^{0.1}$, alors N est B-friable avec probabilité 10^{-10}...

Les origines

Théorème (petit théorème de Fermat). Soit p premier. Pour tout a non-multiple de p, on a

$$a^{p-1} \equiv 1 \mod p\,.$$

Les origines

Théorème (petit théorème de Fermat). Soit p premier. Pour tout a non-multiple de p, on a

$$a^{p-1} \equiv 1 \mod p\,.$$

Conséquence. Si M est un multiple de $p-1$, on a également $p \mid a^M - 1$.

Les origines

Théorème (petit théorème de Fermat). Soit p premier. Pour tout a non-multiple de p, on a

$$a^{p-1} \equiv 1 \mod p\,.$$

Conséquence. Si M est un multiple de $p-1$, on a également $p \mid a^M - 1$.

Idée : on choisit M un nombre B-superfriable, avec B assez petit. Typiquement :

$$M = \text{ppcm}\{2, \ldots, B\} = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$

où les p_i sont premiers et e_i maximal tel que $p_i^{e_i} \leq B$.

Les origines

Théorème (petit théorème de Fermat). Soit p premier. Pour tout a non-multiple de p, on a

$$a^{p-1} \equiv 1 \mod p\,.$$

Conséquence. Si M est un multiple de $p-1$, on a également $p \mid a^M - 1$.

Idée : on choisit M un nombre B-superfriable, avec B assez petit. Typiquement :

$$M = \text{ppcm}\{2,\ldots,B\} = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$

où les p_i sont premiers et e_i maximal tel que $p_i^{e_i} \leq B$.
Puis, on espère obtenir un facteur propre de N en calculant $\text{pgcd}(a^M - 1, N)$ où a est tiré aléatoirement dans $\{2,\ldots,N-1\}$.

Méthode $p-1$ de Pollard

Méthode $p-1$ de Pollard pour la factorisation

Entrée : un entier N à factoriser, un entier $B \geq 2$
Sortie : un facteur propre de N
Hypothèse : il existe un facteur premier p de N tel que $p-1$ est B-superfriable

1. Calculer $M \leftarrow \text{ppcm}\{2, \ldots, B\}$.
2. Tirer aléatoirement $a \in \{2, \ldots, N-1\}$.
3. Calculer $d = \text{pgcd}(a, N)$.
4. **Si** $d \neq 1$, alors **retourner** d.
5. **Sinon :**
   - Calculer $c \leftarrow a^M - 1 \mod N$.
   - Calculer $d' \leftarrow \text{pgcd}(c, N)$.
   - **Si** $d' = N$, revenir à l'étape 2.
   - **Sinon, retourner** d'.

Méthode $p-1$ de Pollard

MÉTHODE $p-1$ DE POLLARD POUR LA FACTORISATION

Entrée : un entier N à factoriser, un entier $B \geq 2$
Sortie : un facteur propre de N
Hypothèse : il existe un facteur premier p de N tel que $p-1$ est B-superfriable

1. Calculer $M \leftarrow \text{ppcm}\{2, \ldots, B\}$.
2. Tirer aléatoirement $a \in \{2, \ldots, N-1\}$.
3. Calculer $d = \text{pgcd}(a, N)$.
4. **Si** $d \neq 1$, alors **retourner** d.
5. **Sinon :**
   - Calculer $c \leftarrow a^M - 1 \mod N$.
   - Calculer $d' \leftarrow \text{pgcd}(c, N)$.
   - **Si** $d' = N$, revenir à l'étape 2.
   - **Sinon, retourner** d'.

Remarque. Au lieu de calculer directement $\text{pgcd}(a^M - 1, N)$, on peut également calculer des pgcd « intermédiaires », de la forme $\text{pgcd}(a^{M_i} - 1, N)$ où M_i est un facteur de M qu'on calcule lors de l'étape 1.
$\Longrightarrow$ intéressant surtout pour de petites valeurs de N.

Pollard $p-1$: complexité

1. Calculer $M \leftarrow \text{ppcm}\{2,\ldots,B\}$.
2. Tirer aléatoirement $a \in \{1,\ldots,N-1\}$.
3. Calculer $d = \text{pgcd}(a,N)$.
4. **Si** $d \neq 1$, alors **retourner** d.
5. **Sinon :**
   - Calculer $c \leftarrow a^M - 1 \mod N$.
   - Calculer $d' \leftarrow \text{pgcd}(c,N)$.
   - **Si** $d' = N$, revenir à l'étape 3.
   - **Sinon, retourner** d'.

Pollard $p-1$: complexité

1. Calculer $M \leftarrow \text{ppcm}\{2,\ldots,B\}$.
2. Tirer aléatoirement $a \in \{1,\ldots,N-1\}$.
3. Calculer $d = \text{pgcd}(a,N)$.
4. **Si** $d \neq 1$, alors **retourner** d.
5. **Sinon :**
   - Calculer $c \leftarrow a^M - 1 \mod N$.
   - Calculer $d' \leftarrow \text{pgcd}(c,N)$.
   - **Si** $d' = N$, revenir à l'étape 3.
   - **Sinon, retourner** d'.

Complexité. L'étape coûteuse est le calcul de $a^M - 1 \mod N$, qui se fait en $O(B)$ opérations, comme $M = O(2^B)$.

$\Longrightarrow$ complexité totale $O(B \log B \log^2 N)$

Pollard $p-1$: complexité

1. Calculer $M \leftarrow \text{ppcm}\{2,\ldots,B\}$.
2. Tirer aléatoirement $a \in \{1,\ldots,N-1\}$.
3. Calculer $d = \text{pgcd}(a,N)$.
4. **Si** $d \neq 1$, alors **retourner** d.
5. **Sinon :**
   - Calculer $c \leftarrow a^M - 1 \mod N$.
   - Calculer $d' \leftarrow \text{pgcd}(c,N)$.
   - **Si** $d' = N$, revenir à l'étape 3.
   - **Sinon, retourner** d'.

Complexité. L'étape coûteuse est le calcul de $a^M - 1 \mod N$, qui se fait en $O(B)$ opérations, comme $M = O(2^B)$.

$\Longrightarrow$ complexité totale $O(B \log B \log^2 N)$

Remarques. Il se peut que $d' = N$ (fréquent lorsque N est petit).

- Cela peut se produire si a a un petit ordre modulo N (on tire a à nouveau).
- Si cela se produit systématiquement, cela signifie souvent que **tous** les facteurs premiers p de N tels que $p-1$ est B-superfriable.
- Il existe d'autres cas d'échec pathologiques, rares dès lors que N grandit.

Pollard $p-1$: exemple

Pour $N = 108\,147\,037$

Pollard $p-1$: exemple

Pour $N = 108\,147\,037$

- N est assez petit : on exécute donc la variante avec les pgcd intermédiaires.

Pollard $p-1$: exemple

Pour $N = 108\,147\,037$

- N est assez petit : on exécute donc la variante avec les pgcd intermédiaires.
- Pour l'exemple, on choisit $B = 14$ (on pourrait aller plus loin).

Pollard $p-1$: exemple

Pour $N = 108\,147\,037$

- N est assez petit : on exécute donc la variante avec les pgcd intermédiaires.
- Pour l'exemple, on choisit $B = 14$ (on pourrait aller plus loin).
- Donc $M = Q_1 \times \cdots \times Q_\ell = 2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13$.

Pollard $p-1$: exemple

Pour $N = 108\,147\,037$

- N est assez petit : on exécute donc la variante avec les pgcd intermédiaires.
- Pour l'exemple, on choisit $B = 14$ (on pourrait aller plus loin).
- Donc $M = Q_1 \times \cdots \times Q_\ell = 2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13$.
- On note $M_i = Q_1 \times \cdots \times Q_i$ (calcul intermédiaire).

Pollard $p-1$: exemple

Pour $N = 108\,147\,037$

- N est assez petit : on exécute donc la variante avec les pgcd intermédiaires.
- Pour l'exemple, on choisit $B = 14$ (on pourrait aller plus loin).
- Donc $M = Q_1 \times \cdots \times Q_\ell = 2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13$.
- On note $M_i = Q_1 \times \cdots \times Q_i$ (calcul intermédiaire).

Exemple avec $a = 2$

Q_i	$a^{M_i} - 1 \mod N$	$\mathrm{pgcd}(a^{M_i} - 1, N)$
8	255	1
9	77888826	1
5	14060764	1
7	66102662	1
11	53395803	1
13	92398868	36037

On a le facteur $p = 36037$, et
$p - 1 = 2^2 \cdot 3^2 \cdot 7 \cdot 11 \cdot 13$.

Pollard $p-1$: exemple

Pour $N = 108\,147\,037$

- N est assez petit : on exécute donc la variante avec les pgcd intermédiaires.
- Pour l'exemple, on choisit $B = 14$ (on pourrait aller plus loin).
- Donc $M = Q_1 \times \cdots \times Q_\ell = 2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13$.
- On note $M_i = Q_1 \times \cdots \times Q_i$ (calcul intermédiaire).

Exemple avec $a = 2$

Q_i	$a^{M_i} - 1 \mod N$	$\mathrm{pgcd}(a^{M_i} - 1, N)$
8	255	1
9	77888826	1
5	14060764	1
7	66102662	1
11	53395803	1
13	92398868	36037

On a le facteur $p = 36037$, et
$p - 1 = 2^2 \cdot 3^2 \cdot 7 \cdot 11 \cdot 13$.

Exemple avec $a = 20$ (choisi pour l'exemple)

Q_i	$a^{M_i} - 1 \mod N$	$\mathrm{pgcd}(a^{M_i} - 1, N)$
8	77299267	1
9	45988448	1
5	97367445	3001
7	$\times$	$\times$
11	$\times$	$\times$
13	$\times$	$\times$

On a le facteur $p = 3001$... chanceusement

Vers une extension de la méthode $p-1$

Intuition. Pour la méthode $p-1$ on a utilisé implicitement le morphisme surjectif

$$\begin{array}{ccc} (\mathbb{Z}/N\mathbb{Z})^\times & \longrightarrow & (\mathbb{Z}/p\mathbb{Z})^\times \\ a & \longmapsto & a \mod p \end{array}$$

Puis, on a cherché à obtenir l'élément neutre de $(\mathbb{Z}/p\mathbb{Z})^\times$:

$$p-1 \text{ divise } M \quad \Longleftrightarrow \quad (a \mod p)^M = 1,$$

ce que l'on peut tester en calculant $\text{pgcd}(a^M - 1, N)$.

Vers une extension de la méthode $p-1$

Intuition. Pour la méthode $p-1$ on a utilisé implicitement le morphisme surjectif

$$\begin{array}{ccc} (\mathbb{Z}/N\mathbb{Z})^\times & \longrightarrow & (\mathbb{Z}/p\mathbb{Z})^\times \\ a & \longmapsto & a \mod p \end{array}$$

Puis, on a cherché à obtenir l'élément neutre de $(\mathbb{Z}/p\mathbb{Z})^\times$:

$$p-1 \text{ divise } M \quad \Longleftrightarrow \quad (a \mod p)^M = 1,$$

ce que l'on peut tester en calculant $\text{pgcd}(a^M - 1, N)$.

Idée. Cherchons un groupe d'un ordre différent. Pour cela, on peut même partir de plusieurs éléments de $\mathbb{Z}/N\mathbb{Z}$.

Vers une extension de la méthode $p-1$

Intuition. Pour la méthode $p-1$ on a utilisé implicitement le morphisme surjectif

$$\begin{array}{ccc} (\mathbb{Z}/N\mathbb{Z})^\times & \longrightarrow & (\mathbb{Z}/p\mathbb{Z})^\times \\ a & \longmapsto & a \mod p \end{array}$$

Puis, on a cherché à obtenir l'élément neutre de $(\mathbb{Z}/p\mathbb{Z})^\times$:

$$p-1 \text{ divise } M \quad \Longleftrightarrow \quad (a \mod p)^M = 1,$$

ce que l'on peut tester en calculant $\text{pgcd}(a^M - 1, N)$.

Idée. Cherchons un groupe d'un ordre différent. Pour cela, on peut même partir de plusieurs éléments de $\mathbb{Z}/N\mathbb{Z}$.

Par exemple, on se fixe $D \in \mathbb{Z}$ et on considère

$$\mathcal{A} = \{(x,y) \in (\mathbb{Z}/N\mathbb{Z})^2 \mid x^2 - Dy^2 = 1\} \subseteq (\mathbb{Z}/N\mathbb{Z})^2$$

Alors on peut considérer $\mathcal{A}_p := \mathcal{A} \mod p$:

$$\begin{array}{ccc} \mathcal{A} & \longrightarrow & \mathcal{A}_p \\ (x,y) & \longmapsto & (x \mod p,\ y \mod p) \end{array}$$

Vers une extension de la méthode $p-1$

Intuition. Pour la méthode $p-1$ on a utilisé implicitement le morphisme surjectif

$$\begin{array}{ccc} (\mathbb{Z}/N\mathbb{Z})^\times & \longrightarrow & (\mathbb{Z}/p\mathbb{Z})^\times \\ a & \longmapsto & a \mod p \end{array}$$

Puis, on a cherché à obtenir l'élément neutre de $(\mathbb{Z}/p\mathbb{Z})^\times$:

$$p-1 \text{ divise } M \quad \Longleftrightarrow \quad (a \mod p)^M = 1,$$

ce que l'on peut tester en calculant $\text{pgcd}(a^M - 1, N)$.

Idée. Cherchons un groupe d'un ordre différent. Pour cela, on peut même partir de plusieurs éléments de $\mathbb{Z}/N\mathbb{Z}$.

Par exemple, on se fixe $D \in \mathbb{Z}$ et on considère

$$\mathcal{A} = \{(x,y) \in (\mathbb{Z}/N\mathbb{Z})^2 \mid x^2 - Dy^2 = 1\} \subseteq (\mathbb{Z}/N\mathbb{Z})^2$$

Alors on peut considérer $\mathcal{A}_p := \mathcal{A} \mod p$:

$$\begin{array}{ccc} \mathcal{A} & \longrightarrow & \mathcal{A}_p \\ (x,y) & \longmapsto & (x \mod p,\ y \mod p) \end{array}$$

Question. Que dire de la structure algébrique de $\mathcal{A}_p$?

Méthode $p+1$ de Williams

$$\begin{array}{ccc} \mathcal{A} & \longrightarrow & \mathcal{A}_p \\ (x,y) & \longmapsto & (x \mod p,\ y \mod p) \end{array}$$

Propriété. Si $D \in \mathbb{Z}$ n'est pas un carré modulo p, alors $\mathbb{F}_{p^2}$ s'écrit $\mathbb{F}_p(\sqrt{D})$, et la projection $\mathcal{A}_p := (\mathcal{A} \bmod p)$ est isomorphe à $\mathcal{U}_p = \{u \in \mathbb{F}_{p^2} \mid u^{p+1} = 1\}$ qui est un groupe d'ordre $p+1$.

Méthode $p+1$ de Williams

$$\begin{array}{ccc} \mathcal{A} & \longrightarrow & \mathcal{A}_p \\ (x,y) & \longmapsto & (x \mod p,\ y \mod p) \end{array}$$

Propriété. Si $D \in \mathbb{Z}$ n'est pas un carré modulo p, alors $\mathbb{F}_{p^2}$ s'écrit $\mathbb{F}_p(\sqrt{D})$, et la projection $\mathcal{A}_p := (\mathcal{A} \bmod p)$ est isomorphe à $\mathcal{U}_p = \{u \in \mathbb{F}_{p^2} \mid u^{p+1} = 1\}$ qui est un groupe d'ordre $p+1$.

Éléments de preuve. Si $(x,y) \in \mathcal{A}_p$, alors

$$u = x + y\sqrt{D} \in \mathbb{F}_{p^2} \longleftrightarrow (x,y) \in \mathcal{A}_p$$

et

$$u^{p+1} = u^p u =$$

Méthode $p+1$ de Williams

$$\begin{array}{ccc} \mathcal{A} & \longrightarrow & \mathcal{A}_p \\ (x,y) & \longmapsto & (x \mod p,\ y \mod p) \end{array}$$

Propriété. Si $D \in \mathbb{Z}$ n'est pas un carré modulo p, alors $\mathbb{F}_{p^2}$ s'écrit $\mathbb{F}_p(\sqrt{D})$, et la projection $\mathcal{A}_p := (\mathcal{A} \bmod p)$ est isomorphe à $\mathcal{U}_p = \{u \in \mathbb{F}_{p^2} \mid u^{p+1} = 1\}$ qui est un groupe d'ordre $p+1$.

Éléments de preuve. Si $(x,y) \in \mathcal{A}_p$, alors

$$u = x + y\sqrt{D} \in \mathbb{F}_{p^2} \longleftrightarrow (x,y) \in \mathcal{A}_p$$

et

$$u^{p+1} = u^p u = (x + y\sqrt{D}^p)(x + y\sqrt{D}) =$$

Méthode $p+1$ de Williams

$$\begin{array}{ccc} \mathcal{A} & \longrightarrow & \mathcal{A}_p \\ (x,y) & \longmapsto & (x \mod p,\ y \mod p) \end{array}$$

Propriété. Si $D \in \mathbb{Z}$ n'est pas un carré modulo p, alors $\mathbb{F}_{p^2}$ s'écrit $\mathbb{F}_p(\sqrt{D})$, et la projection $\mathcal{A}_p := (\mathcal{A} \bmod p)$ est isomorphe à $\mathcal{U}_p = \{u \in \mathbb{F}_{p^2} \mid u^{p+1} = 1\}$ qui est un groupe d'ordre $p+1$.

Éléments de preuve. Si $(x,y) \in \mathcal{A}_p$, alors

$$u = x + y\sqrt{D} \in \mathbb{F}_{p^2} \longleftrightarrow (x,y) \in \mathcal{A}_p$$

et

$$u^{p+1} = u^p u = (x + y\sqrt{D}^p)(x + y\sqrt{D}) = (x + y(-\sqrt{D}))(x + y\sqrt{D}) =$$

Méthode $p+1$ de Williams

$$\begin{array}{ccc} \mathcal{A} & \longrightarrow & \mathcal{A}_p \\ (x,y) & \longmapsto & (x \mod p,\ y \mod p) \end{array}$$

Propriété. Si $D \in \mathbb{Z}$ n'est pas un carré modulo p, alors $\mathbb{F}_{p^2}$ s'écrit $\mathbb{F}_p(\sqrt{D})$, et la projection $\mathcal{A}_p := (\mathcal{A} \bmod p)$ est isomorphe à $\mathcal{U}_p = \{u \in \mathbb{F}_{p^2} \mid u^{p+1} = 1\}$ qui est un groupe d'ordre $p+1$.

Éléments de preuve. Si $(x,y) \in \mathcal{A}_p$, alors

$$u = x + y\sqrt{D} \in \mathbb{F}_{p^2} \longleftrightarrow (x,y) \in \mathcal{A}_p$$

et

$$u^{p+1} = u^p u = (x + y\sqrt{D}^p)(x + y\sqrt{D}) = (x + y(-\sqrt{D}))(x + y\sqrt{D}) = x^2 - y^2 D = 1\,.$$

Méthode $p+1$ de Williams

$$\begin{array}{ccc} \mathcal{A} & \longrightarrow & \mathcal{A}_p \\ (x,y) & \longmapsto & (x \mod p,\ y \mod p) \end{array}$$

Propriété. Si $D \in \mathbb{Z}$ n'est pas un carré modulo p, alors $\mathbb{F}_{p^2}$ s'écrit $\mathbb{F}_p(\sqrt{D})$, et la projection $\mathcal{A}_p := (\mathcal{A} \bmod p)$ est isomorphe à $\mathcal{U}_p = \{u \in \mathbb{F}_{p^2} \mid u^{p+1} = 1\}$ qui est un groupe d'ordre $p+1$.

Éléments de preuve. Si $(x,y) \in \mathcal{A}_p$, alors

$$u = x + y\sqrt{D} \in \mathbb{F}_{p^2} \longleftrightarrow (x,y) \in \mathcal{A}_p$$

et

$$u^{p+1} = u^p u = (x + y\sqrt{D}^p)(x + y\sqrt{D}) = (x + y(-\sqrt{D}))(x + y\sqrt{D}) = x^2 - y^2 D = 1\,.$$

Par ailleurs $u = 1$ est l'unique élément de $\mathcal{U}_p$ tel que $x = 1$.

Méthode $p+1$ de Williams

$$\begin{array}{ccc} \mathcal{A} & \longrightarrow & \mathcal{A}_p \\ (x,y) & \longmapsto & (x \mod p,\ y \mod p) \end{array}$$

Propriété. Si $D \in \mathbb{Z}$ n'est pas un carré modulo p, alors $\mathbb{F}_{p^2}$ s'écrit $\mathbb{F}_p(\sqrt{D})$, et la projection $\mathcal{A}_p := (\mathcal{A} \bmod p)$ est isomorphe à $\mathcal{U}_p = \{u \in \mathbb{F}_{p^2} \mid u^{p+1} = 1\}$ qui est un groupe d'ordre $p+1$.

Éléments de preuve. Si $(x,y) \in \mathcal{A}_p$, alors

$$u = x + y\sqrt{D} \in \mathbb{F}_{p^2} \longleftrightarrow (x,y) \in \mathcal{A}_p$$

et

$$u^{p+1} = u^p u = (x + y\sqrt{D}^p)(x + y\sqrt{D}) = (x + y(-\sqrt{D}))(x + y\sqrt{D}) = x^2 - y^2 D = 1\,.$$

Par ailleurs $u = 1$ est l'unique élément de $\mathcal{U}_p$ tel que $x = 1$.

Par analogie avec la méthode $p-1$, on va donc calculer $u^M = x_M + y_M\sqrt{D}$ et espérer que $\mathrm{pgcd}(x_M - 1, N)$ donne un facteur propre de N.

Méthode $p+1$ de Williams

$$\begin{array}{ccc} \mathcal{A} & \longrightarrow & \mathcal{A}_p \\ (x,y) & \longmapsto & (x \mod p,\ y \mod p) \end{array}$$

Propriété. Si $D \in \mathbb{Z}$ n'est pas un carré modulo p, alors $\mathbb{F}_{p^2}$ s'écrit $\mathbb{F}_p(\sqrt{D})$, et la projection $\mathcal{A}_p := (\mathcal{A} \bmod p)$ est isomorphe à $\mathcal{U}_p = \{u \in \mathbb{F}_{p^2} \mid u^{p+1} = 1\}$ qui est un groupe d'ordre $p+1$.

Éléments de preuve. Si $(x,y) \in \mathcal{A}_p$, alors

$$u = x + y\sqrt{D} \in \mathbb{F}_{p^2} \longleftrightarrow (x,y) \in \mathcal{A}_p$$

et

$$u^{p+1} = u^p u = (x + y\sqrt{D}^p)(x + y\sqrt{D}) = (x + y(-\sqrt{D}))(x + y\sqrt{D}) = x^2 - y^2 D = 1\,.$$

Par ailleurs $u = 1$ est l'unique élément de $\mathcal{U}_p$ tel que $x = 1$.

Par analogie avec la méthode $p-1$, on va donc calculer $u^M = x_M + y_M\sqrt{D}$ et espérer que $\gcd(x_M - 1, N)$ donne un facteur propre de N.

Problème : comment calculer x_M sans connaissance de p ?

Méthode $p+1$ de Williams

Problème : comment calculer x_M sans connaissance de p ?

Méthode $p+1$ de Williams

Problème : comment calculer x_M sans connaissance de p ?

On cherche exprimer x_{2n} et x_{2n+1} en fonction de précédents x_i (*idée : exponentiation binaire*).

Si (x_n, y_n) est défini par $u^n = x_n + y_n\sqrt{D}$, alors :

Méthode $p+1$ de Williams

Problème : comment calculer x_M sans connaissance de p ?

On cherche exprimer x_{2n} et x_{2n+1} en fonction de précédents x_i (*idée : exponentiation binaire*).

Si (x_n, y_n) est défini par $u^n = x_n + y_n\sqrt{D}$, alors :

- On a $u^{2n} = (x_n + y_n\sqrt{D})^2 =$

Méthode $p+1$ de Williams

Problème : comment calculer x_M sans connaissance de p ?

On cherche exprimer x_{2n} et x_{2n+1} en fonction de précédents x_i (*idée : exponentiation binaire*).

Si (x_n, y_n) est défini par $u^n = x_n + y_n\sqrt{D}$, alors :

- On a $u^{2n} = (x_n + y_n\sqrt{D})^2 = (x_n^2 + Dy_n^2) + 2x_n y_n\sqrt{D} =$

Méthode $p+1$ de Williams

Problème : comment calculer x_M sans connaissance de p ?

On cherche exprimer x_{2n} et x_{2n+1} en fonction de précédents x_i (*idée : exponentiation binaire*).

Si (x_n, y_n) est défini par $u^n = x_n + y_n\sqrt{D}$, alors :

- On a $u^{2n} = (x_n + y_n\sqrt{D})^2 = (x_n^2 + Dy_n^2) + 2x_n y_n\sqrt{D} = (-1 + 2x_n^2) + 2x_n y_n\sqrt{D}$.

Méthode $p+1$ de Williams

Problème : comment calculer x_M sans connaissance de p ?

On cherche exprimer x_{2n} et x_{2n+1} en fonction de précédents x_i (*idée : exponentiation binaire*).

Si (x_n, y_n) est défini par $u^n = x_n + y_n\sqrt{D}$, alors :

- On a $u^{2n} = (x_n + y_n\sqrt{D})^2 = (x_n^2 + Dy_n^2) + 2x_n y_n\sqrt{D} = (-1 + 2x_n^2) + 2x_n y_n\sqrt{D}$.
  Donc, $x_{2n} = -1 + 2x_n^2$ et $y_{2n} = 2x_n y_n$.

Méthode $p+1$ de Williams

Problème : comment calculer x_M sans connaissance de p ?

On cherche exprimer x_{2n} et x_{2n+1} en fonction de précédents x_i (*idée : exponentiation binaire*).

Si (x_n, y_n) est défini par $u^n = x_n + y_n\sqrt{D}$, alors :

- On a $u^{2n} = (x_n + y_n\sqrt{D})^2 = (x_n^2 + Dy_n^2) + 2x_n y_n\sqrt{D} = (-1 + 2x_n^2) + 2x_n y_n\sqrt{D}$.
  Donc, $x_{2n} = -1 + 2x_n^2$ et $y_{2n} = 2x_n y_n$.
- D'une part, $u^{2n+1} = u^{2n}u$ donne $x_{2n+1} = x_{2n}x_1 + y_{2n}y_1 D = (1 + 2x_n^2)x_1 + 2x_n y_n y_1 D$.

Méthode $p+1$ de Williams

Problème : comment calculer x_M sans connaissance de p ?

On cherche exprimer x_{2n} et x_{2n+1} en fonction de précédents x_i (*idée : exponentiation binaire*).

Si (x_n, y_n) est défini par $u^n = x_n + y_n\sqrt{D}$, alors :

- On a $u^{2n} = (x_n + y_n\sqrt{D})^2 = (x_n^2 + Dy_n^2) + 2x_n y_n\sqrt{D} = (-1 + 2x_n^2) + 2x_n y_n\sqrt{D}$.
  Donc, $x_{2n} = -1 + 2x_n^2$ et $y_{2n} = 2x_n y_n$.
- D'une part, $u^{2n+1} = u^{2n}u$ donne $x_{2n+1} = x_{2n}x_1 + y_{2n}y_1 D = (1 + 2x_n^2)x_1 + 2x_n y_n y_1 D$.
- D'autre part, $u^{n+1} = u^n u$ donne $x_{n+1} = x_n x_1 + D y_n y_1$.

Méthode $p+1$ de Williams

Problème : comment calculer x_M sans connaissance de p ?

On cherche exprimer x_{2n} et x_{2n+1} en fonction de précédents x_i (*idée : exponentiation binaire*).

Si (x_n, y_n) est défini par $u^n = x_n + y_n\sqrt{D}$, alors :

- On a $u^{2n} = (x_n + y_n\sqrt{D})^2 = (x_n^2 + Dy_n^2) + 2x_n y_n\sqrt{D} = (-1 + 2x_n^2) + 2x_n y_n\sqrt{D}$.
  Donc, $x_{2n} = -1 + 2x_n^2$ et $y_{2n} = 2x_n y_n$.
- D'une part, $u^{2n+1} = u^{2n}u$ donne $x_{2n+1} = x_{2n}x_1 + y_{2n}y_1 D = (1 + 2x_n^2)x_1 + 2x_n y_n y_1 D$.
- D'autre part, $u^{n+1} = u^n u$ donne $x_{n+1} = x_n x_1 + D y_n y_1$.
- Donc, $x_{2n+1} = (-1 + 2x_n^2)x_1 + 2x_n(x_{n+1} - x_n x_1) = 2x_n x_{n+1} - x_1$.

Méthode $p+1$ de Williams

Problème : comment calculer x_M sans connaissance de p ?

On cherche exprimer x_{2n} et x_{2n+1} en fonction de précédents x_i (*idée : exponentiation binaire*).

Si (x_n, y_n) est défini par $u^n = x_n + y_n\sqrt{D}$, alors :

- On a $u^{2n} = (x_n + y_n\sqrt{D})^2 = (x_n^2 + Dy_n^2) + 2x_n y_n\sqrt{D} = (-1 + 2x_n^2) + 2x_n y_n\sqrt{D}$.
  Donc, $x_{2n} = -1 + 2x_n^2$ et $y_{2n} = 2x_n y_n$.
- D'une part, $u^{2n+1} = u^{2n}u$ donne $x_{2n+1} = x_{2n}x_1 + y_{2n}y_1 D = (1 + 2x_n^2)x_1 + 2x_n y_n y_1 D$.
- D'autre part, $u^{n+1} = u^n u$ donne $x_{n+1} = x_n x_1 + D y_n y_1$.
- Donc, $x_{2n+1} = (-1 + 2x_n^2)x_1 + 2x_n(x_{n+1} - x_n x_1) = 2x_n x_{n+1} - x_1$.
- Enfin, $x_{2n+2} = -1 + 2x_{n+1}^2$.

Méthode $p+1$ de Williams

Problème : comment calculer x_M sans connaissance de p ?

On cherche exprimer x_{2n} et x_{2n+1} en fonction de précédents x_i (*idée : exponentiation binaire*).

Si (x_n, y_n) est défini par $u^n = x_n + y_n\sqrt{D}$, alors :

- On a $u^{2n} = (x_n + y_n\sqrt{D})^2 = (x_n^2 + Dy_n^2) + 2x_n y_n\sqrt{D} = (-1 + 2x_n^2) + 2x_n y_n\sqrt{D}$.
  Donc, $x_{2n} = -1 + 2x_n^2$ et $y_{2n} = 2x_n y_n$.
- D'une part, $u^{2n+1} = u^{2n}u$ donne $x_{2n+1} = x_{2n}x_1 + y_{2n}y_1 D = (1 + 2x_n^2)x_1 + 2x_n y_n y_1 D$.
- D'autre part, $u^{n+1} = u^n u$ donne $x_{n+1} = x_n x_1 + D y_n y_1$.
- Donc, $x_{2n+1} = (-1 + 2x_n^2)x_1 + 2x_n(x_{n+1} - x_n x_1) = 2x_n x_{n+1} - x_1$.
- Enfin, $x_{2n+2} = -1 + 2x_{n+1}^2$.

Donc, la connaissance de (x_n, x_{n+1}) permet de déduire $(x_{2n}, x_{2n+1}, x_{2n+2})$.

Méthode $p+1$ de Williams

Problème : comment calculer x_M sans connaissance de p ?

On cherche exprimer x_{2n} et x_{2n+1} en fonction de précédents x_i (*idée : exponentiation binaire*).

Si (x_n, y_n) est défini par $u^n = x_n + y_n\sqrt{D}$, alors :

- On a $u^{2n} = (x_n + y_n\sqrt{D})^2 = (x_n^2 + Dy_n^2) + 2x_n y_n\sqrt{D} = (-1 + 2x_n^2) + 2x_n y_n\sqrt{D}$.
  Donc, $x_{2n} = -1 + 2x_n^2$ et $y_{2n} = 2x_n y_n$.
- D'une part, $u^{2n+1} = u^{2n}u$ donne $x_{2n+1} = x_{2n}x_1 + y_{2n}y_1 D = (1 + 2x_n^2)x_1 + 2x_n y_n y_1 D$.
- D'autre part, $u^{n+1} = u^n u$ donne $x_{n+1} = x_n x_1 + D y_n y_1$.
- Donc, $x_{2n+1} = (-1 + 2x_n^2)x_1 + 2x_n(x_{n+1} - x_n x_1) = 2x_n x_{n+1} - x_1$.
- Enfin, $x_{2n+2} = -1 + 2x_{n+1}^2$.

Donc, la connaissance de (x_n, x_{n+1}) permet de déduire $(x_{2n}, x_{2n+1}, x_{2n+2})$.

Conséquence : on peut adapter l'exponentiation binaire pour calculer les (x_n) !

Méthode $p+1$ de Williams

MÉTHODE $p+1$ DE WILLIAMS POUR LA FACTORISATION (1982)
VERSION PÉDAGOGIQUE

Entrée : un entier N à factoriser, un entier $B \geq 2$
Sortie : un facteur propre de N
Hypothèse : il existe un facteur premier p de N tel que $p+1$ est B-superfriable

1. Calculer $M \leftarrow \text{ppcm}\{2, \ldots, B\}$.
2. Tirer aléatoirement x_1 dans $\{1, \ldots, N-1\}$.
3. Calculer $d = \text{pgcd}(x_1, N)$.
4. **Si** $d \neq 1$, alors **retourner** d.
5. **Sinon :**
   - Calculer x_M via les relations décrites précédemment.
   - Calculer $d' \leftarrow \text{pgcd}(x_M - 1, N)$.
   - **Si** $d' = N$, revenir à l'étape 2.
   - **Sinon, retourner** d'.

Méthode $p+1$ de Williams

MÉTHODE $p+1$ DE WILLIAMS POUR LA FACTORISATION (1982)
VERSION PÉDAGOGIQUE

Entrée : un entier N à factoriser, un entier $B \geq 2$
Sortie : un facteur propre de N
Hypothèse : il existe un facteur premier p de N tel que $p+1$ est B-superfriable

1. Calculer $M \leftarrow \text{ppcm}\{2, \ldots, B\}$.
2. Tirer aléatoirement x_1 dans $\{1, \ldots, N-1\}$.
3. Calculer $d = \text{pgcd}(x_1, N)$.
4. **Si** $d \neq 1$, alors **retourner** d.
5. **Sinon :**
   - Calculer x_M via les relations décrites précédemment.
   - Calculer $d' \leftarrow \text{pgcd}(x_M - 1, N)$.
   - **Si** $d' = N$, revenir à l'étape 2.
   - **Sinon, retourner** d'.

Remarque.

- En initialisant un x_1 aléatoire, on détermine implicitement D. Avec bonne probabilité, D sera un non-résidu quadratique modulo p.
- En pratique, on calcule $v_n = 2x_n$ au lieu de x_n pour accélérer les calculs.

Méthode $p+1$ de Williams

MÉTHODE $p+1$ DE WILLIAMS POUR LA FACTORISATION (1982)
VERSION PÉDAGOGIQUE

Entrée : un entier N à factoriser, un entier $B \geq 2$
Sortie : un facteur propre de N
Hypothèse : il existe un facteur premier p de N tel que $p+1$ est B-superfriable

1. Calculer $M \leftarrow \text{ppcm}\{2, \ldots, B\}$.
2. Tirer aléatoirement x_1 dans $\{1, \ldots, N-1\}$.
3. Calculer $d = \text{pgcd}(x_1, N)$.
4. **Si** $d \neq 1$, alors **retourner** d.
5. **Sinon :**
   - Calculer x_M via les relations décrites précédemment.
   - Calculer $d' \leftarrow \text{pgcd}(x_M - 1, N)$.
   - **Si** $d' = N$, revenir à l'étape 2.
   - **Sinon, retourner** d'.

Remarque.

- En initialisant un x_1 aléatoire, on détermine implicitement D. Avec bonne probabilité, D sera un non-résidu quadratique modulo p.
- En pratique, on calcule $v_n = 2x_n$ au lieu de x_n pour accélérer les calculs.

A p+1 method of factoring. Williams, H. C.. Mathematics of Computation, 39 (159). **1982**.

Méthode ECM de Lenstra

Problème : les méthodes $p-1$ et $p+1$ ne fonctionnent que si ces derniers sont friables ou superfriables.

Méthode ECM de Lenstra

Problème : les méthodes $p-1$ et $p+1$ ne fonctionnent que si ces derniers sont friables ou superfriables.

Question. Des variantes (ou une généralisation) pour d'autres $p+\varepsilon$?

Méthode ECM de Lenstra

Problème : les méthodes $p-1$ et $p+1$ ne fonctionnent que si ces derniers sont friables ou superfriables.

Question. Des variantes (ou une généralisation) pour d'autres $p+\varepsilon$?

Prenons de la **hauteur** sur les idées précédentes $(p-1, p+1)$:

- On construit une structure $\mathcal{E}$ sur $\mathbb{Z}/N\mathbb{Z}$, telle que sa projection $\mathcal{E}_p$ sur $\mathbb{F}_p$ est un groupe.
- On sait calculer dans $\mathcal{E}_p$ via des opérations dans $\mathbb{Z}/N\mathbb{Z}$, sans connaissance de p.
- On sait identifier (avec bonne proba) l'élément neutre de $\mathcal{E}_p$.

Méthode ECM de Lenstra

Problème : les méthodes $p-1$ et $p+1$ ne fonctionnent que si ces derniers sont friables ou superfriables.

Question. Des variantes (ou une généralisation) pour d'autres $p+\varepsilon$?

Prenons de la **hauteur** sur les idées précédentes $(p-1, p+1)$:

- On construit une structure $\mathcal{E}$ sur $\mathbb{Z}/N\mathbb{Z}$, telle que sa projection $\mathcal{E}_p$ sur $\mathbb{F}_p$ est un groupe.
- On sait calculer dans $\mathcal{E}_p$ via des opérations dans $\mathbb{Z}/N\mathbb{Z}$, sans connaissance de p.
- On sait identifier (avec bonne proba) l'élément neutre de $\mathcal{E}_p$.

ECM (elliptic curve method) par Lenstra (1987) :

- $\mathcal{E}$ est une courbe elliptique, vue dans $\mathbb{Z}/N\mathbb{Z}$.
- L'ordre de $\mathcal{E}_p$ est entre $(p+1-2\sqrt{p})$ et $(p+1+2\sqrt{p})$: c'est la borne de Hasse.
- On peut choisir le point initial P **et** la courbe $\mathcal{E}$ au hasard. Puis on calcule le point $M \cdot P = (x_M : y_M : z_M)$, où $M \in \mathbb{N}$ correspond à la borne de friabilité B.
- On travaille en coordonnées projectives : le neutre est $(x : y : z) = (0 : 1 : 0)$, donc on cherche quand $\mathrm{pgcd}(z, N) \neq 1$.

Méthode ECM de Lenstra

Problème : les méthodes $p-1$ et $p+1$ ne fonctionnent que si ces derniers sont friables ou superfriables.

Question. Des variantes (ou une généralisation) pour d'autres $p+\varepsilon$?

Prenons de la **hauteur** sur les idées précédentes $(p-1, p+1)$:

- On construit une structure $\mathcal{E}$ sur $\mathbb{Z}/N\mathbb{Z}$, telle que sa projection $\mathcal{E}_p$ sur $\mathbb{F}_p$ est un groupe.
- On sait calculer dans $\mathcal{E}_p$ via des opérations dans $\mathbb{Z}/N\mathbb{Z}$, sans connaissance de p.
- On sait identifier (avec bonne proba) l'élément neutre de $\mathcal{E}_p$.

ECM (elliptic curve method) par Lenstra (1987) :

- $\mathcal{E}$ est une courbe elliptique, vue dans $\mathbb{Z}/N\mathbb{Z}$.
- L'ordre de $\mathcal{E}_p$ est entre $(p+1-2\sqrt{p})$ et $(p+1+2\sqrt{p})$: c'est la borne de Hasse.
- On peut choisir le point initial P **et** la courbe $\mathcal{E}$ au hasard. Puis on calcule le point $M \cdot P = (x_M : y_M : z_M)$, où $M \in \mathbb{N}$ correspond à la borne de friabilité B.
- On travaille en coordonnées projectives : le neutre est $(x : y : z) = (0 : 1 : 0)$, donc on cherche quand $\mathrm{pgcd}(z, N) \neq 1$.

Factoring integers with elliptic curves. Lenstra Jr., H. W.. Annals of Mathematics. 126 (3). **1987**.

Résumé

algorithme	**complexité**	**commentaires**
divisions successives	$O(p \log^2 N)$	élimine les très petits facteurs
Fermat	$O(\frac{(\sqrt{N}-p)^2}{2p} \log^2 N)$	élimine les facteurs proches de $\sqrt{N}$
Pollard ρ	$O(\sqrt{p} \log^2 N)$	élimine des facteurs petits
Pollard $p-1$ et $p+1$	$O(B \log B \log^2 N)$	élimine des facteurs proches de nombres B-superfriables
ECM	$O(2^{\sqrt{2 \log p \log\log p}})$ (sous-exp)	méthode utilisée en pratique pour éliminer les facteurs moyens (<60 chiffres)

Résumé

algorithme	**complexité**	**commentaires**
divisions successives	$O(p \log^2 N)$	élimine les très petits facteurs
Fermat	$O(\frac{(\sqrt{N}-p)^2}{2p} \log^2 N)$	élimine les facteurs proches de $\sqrt{N}$
Pollard ρ	$O(\sqrt{p} \log^2 N)$	élimine des facteurs petits
Pollard $p-1$ et $p+1$	$O(B \log B \log^2 N)$	élimine des facteurs proches de nombres B-superfriables
ECM	$O(2^{\sqrt{2 \log p \log\log p}})$ (sous-exp)	méthode utilisée en pratique pour éliminer les facteurs moyens (<60 chiffres)

Implications en cryptographie. Dans le chiffrement RSA, où $N = pq$, il faut éviter :

1. que p ou q soient petits,
2. que p et q soient très proches,
3. que $p + \varepsilon$ et $q + \varepsilon$ soient friables.

En pratique, la troisième consition est vérifiée avec très grande probabilité lorsque p et q sont de très grands premiers (plusieurs centaines de chiffres).

Autres références

A Course in Computational Algebraic Number Theory. H. Cohen. GTM38, Springer-Verlag. **1993**.

Prime Numbers and Computer Methods for Factorization. H. Riesel. Progress in Mathematics, Birkhaüser. **1985**.

Prime Numbers, a Computational Perspective. R. Crandall, C. Pomerance. Springer. **2001**.

Plan

Motivation

Dans cette section, on va voir l'algorithme de **crible quadratique** qui permet de factoriser n'importe quel entier N en temps

$$O\Big(\exp(\sqrt{\log N \log\log N})\Big)$$

Son extension, l'algorithme de **crible algébrique** (ou crible par corps de nombres généralisé) (*general number field sieve*, NFS) atteint une complexité encore meilleure :

$$O\Big(\exp((\tfrac{64}{9}\log N)^{1/3}(\log\log N)^{2/3})\Big)\,.$$

Complexité

Objectif : représenter des grandeurs sous-exponentielles $n^\alpha \ll f(n) \ll 2^{\beta n}$.

Complexité

Objectif : représenter des grandeurs sous-exponentielles $n^\alpha \ll f(n) \ll 2^{\beta n}$.

Définition. Notation L :

$$L_n[a,b] := \exp\left(b\, n^a\, (\log n)^{1-a}\right).$$

On prendra souvent exp et log en base 2.

Complexité

Objectif : représenter des grandeurs sous-exponentielles $n^\alpha \ll f(n) \ll 2^{\beta n}$.

Définition. Notation L :

$$L_n[a,b] := \exp\left(b\, n^a\, (\log n)^{1-a}\right).$$

On prendra souvent exp et log en base 2.

Exemples :

- Les fonctions exponentielles $2^{\beta n}$ sont des $L_n[1,\beta]$.
- Les fonctions polynomiales n^α sont des $L_n[0,\alpha]$.

Complexité

Objectif : représenter des grandeurs sous-exponentielles $n^\alpha \ll f(n) \ll 2^{\beta n}$.

Définition. Notation L :

$$L_n[a,b] := \exp\left(b\, n^a\, (\log n)^{1-a}\right).$$

On prendra souvent exp et log en base 2.

Exemples :

- Les fonctions exponentielles $2^{\beta n}$ sont des $L_n[1,\beta]$.
- Les fonctions polynomiales n^α sont des $L_n[0,\alpha]$.

On va utiliser cette notation pour les algorithmes de factorisation. On s'intéresse donc à leur complexité en fonction de $\log_2 N$ ou de $\log_2 p$. Ainsi :

- La complexité de la méthode ρ est en $O(\sqrt{p})$

Complexité

Objectif : représenter des grandeurs sous-exponentielles $n^\alpha \ll f(n) \ll 2^{\beta n}$.

Définition. Notation L :

$$L_n[a,b] := \exp\left(b\, n^a\, (\log n)^{1-a}\right).$$

On prendra souvent exp et log en base 2.

Exemples :

- Les fonctions exponentielles $2^{\beta n}$ sont des $L_n[1,\beta]$.
- Les fonctions polynomiales n^α sont des $L_n[0,\alpha]$.

On va utiliser cette notation pour les algorithmes de factorisation. On s'intéresse donc à leur complexité en fonction de $\log_2 N$ ou de $\log_2 p$. Ainsi :

- La complexité de la méthode ρ est en $O(\sqrt{p}) = O(L_{\log p}[1, \frac{1}{2}])$.

Objectif : représenter des grandeurs sous-exponentielles $n^\alpha \ll f(n) \ll 2^{\beta n}$.

Définition. Notation L :

$$L_n[a,b] := \exp\left(b\, n^a\, (\log n)^{1-a}\right).$$

On prendra souvent exp et log en base 2.

Exemples :

- Les fonctions exponentielles $2^{\beta n}$ sont des $L_n[1,\beta]$.
- Les fonctions polynomiales n^α sont des $L_n[0,\alpha]$.

On va utiliser cette notation pour les algorithmes de factorisation. On s'intéresse donc à leur complexité en fonction de $\log_2 N$ ou de $\log_2 p$. Ainsi :

- La complexité de la méthode ρ est en $O(\sqrt{p}) = O(L_{\log p}[1, \frac{1}{2}])$.
- La complexité de ECM est en $O(\exp(\sqrt{2 \log p \log\log p}))$

Complexité

Objectif : représenter des grandeurs sous-exponentielles $n^\alpha \ll f(n) \ll 2^{\beta n}$.

Définition. Notation L :

$$L_n[a,b] := \exp\left(b\, n^a\, (\log n)^{1-a}\right).$$

On prendra souvent exp et log en base 2.

Exemples :

- Les fonctions exponentielles $2^{\beta n}$ sont des $L_n[1,\beta]$.
- Les fonctions polynomiales n^α sont des $L_n[0,\alpha]$.

On va utiliser cette notation pour les algorithmes de factorisation. On s'intéresse donc à leur complexité en fonction de $\log_2 N$ ou de $\log_2 p$. Ainsi :

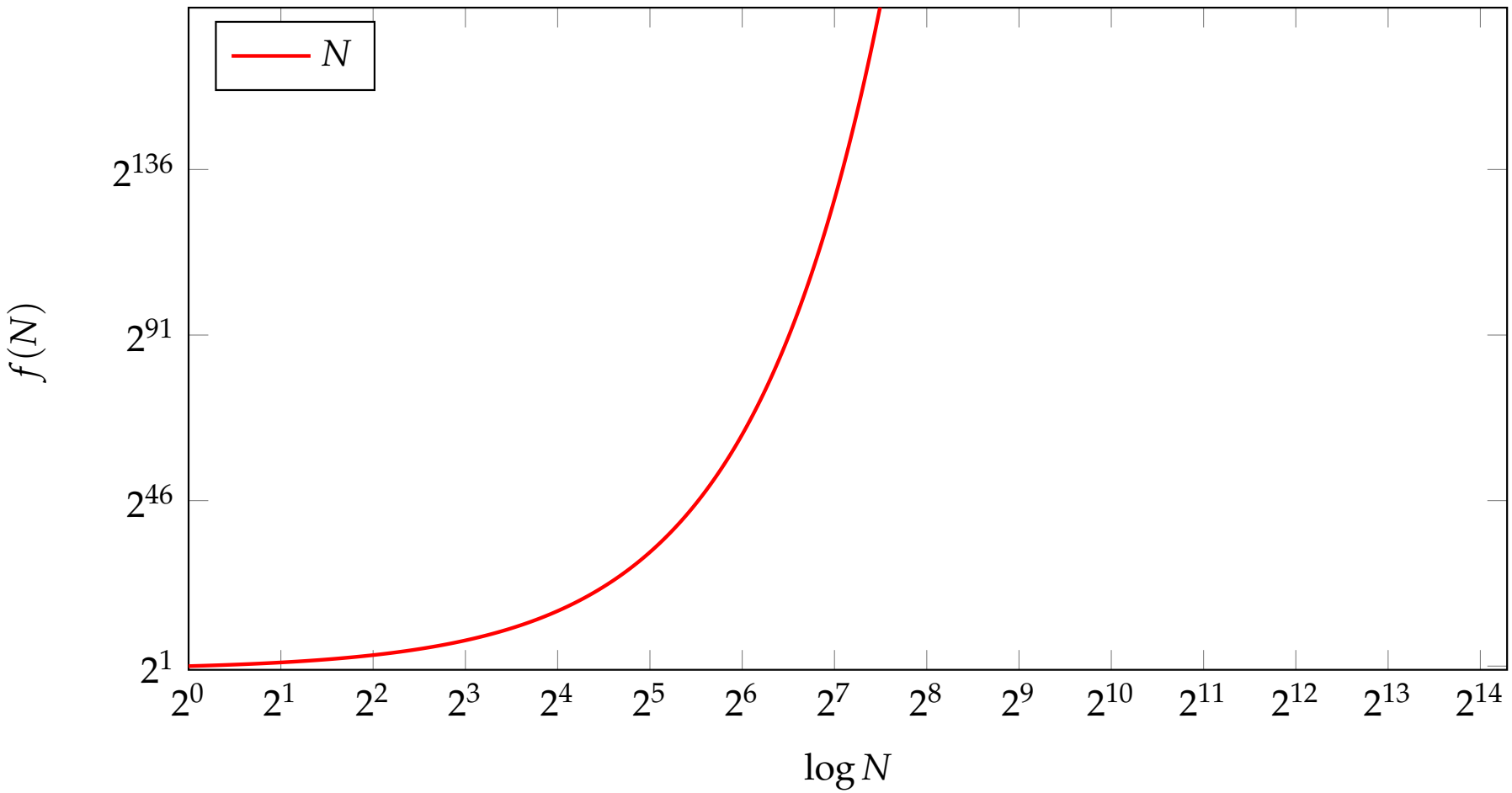
- La complexité de la méthode ρ est en $O(\sqrt{p}) = O(L_{\log p}[1, \frac{1}{2}])$.
- La complexité de ECM est en $O(\exp(\sqrt{2 \log p \log\log p})) = O(L_{\log p}[\frac{1}{2}, \sqrt{2}])$.

Complexité

Quelques **exemples** de comportement de fonctions (échelle « log log »).

Rappel :

- 2^{80} : très, très difficile à calculer, pour $\simeq 2^{30}$ op./s sur un processeur
- 2^{128} : supposé inatteignable

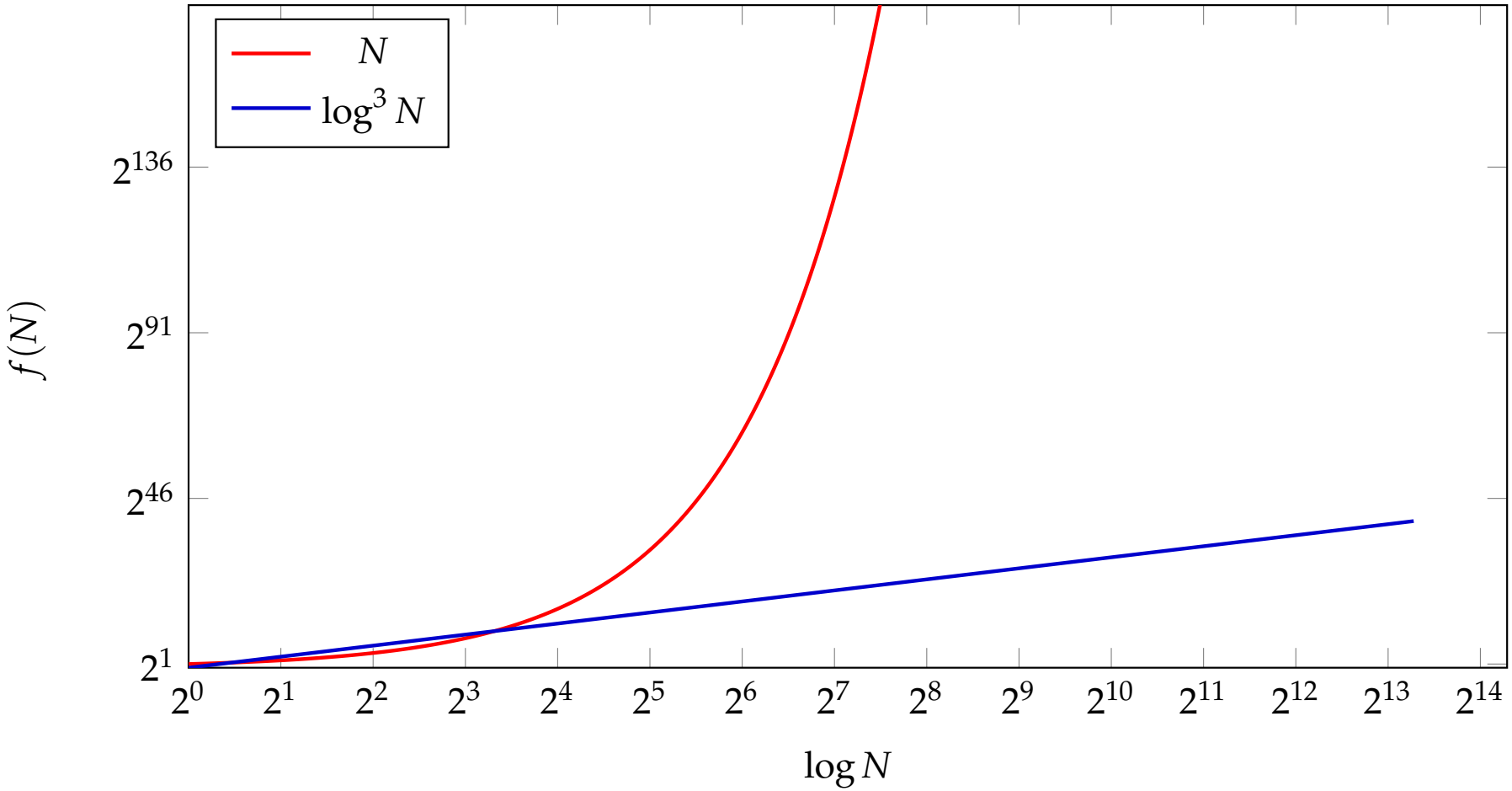


Complexité

Quelques **exemples** de comportement de fonctions (échelle « log log »).

Rappel :

- 2^{80} : très, très difficile à calculer, pour $\simeq 2^{30}$ op./s sur un processeur
- 2^{128} : supposé inatteignable

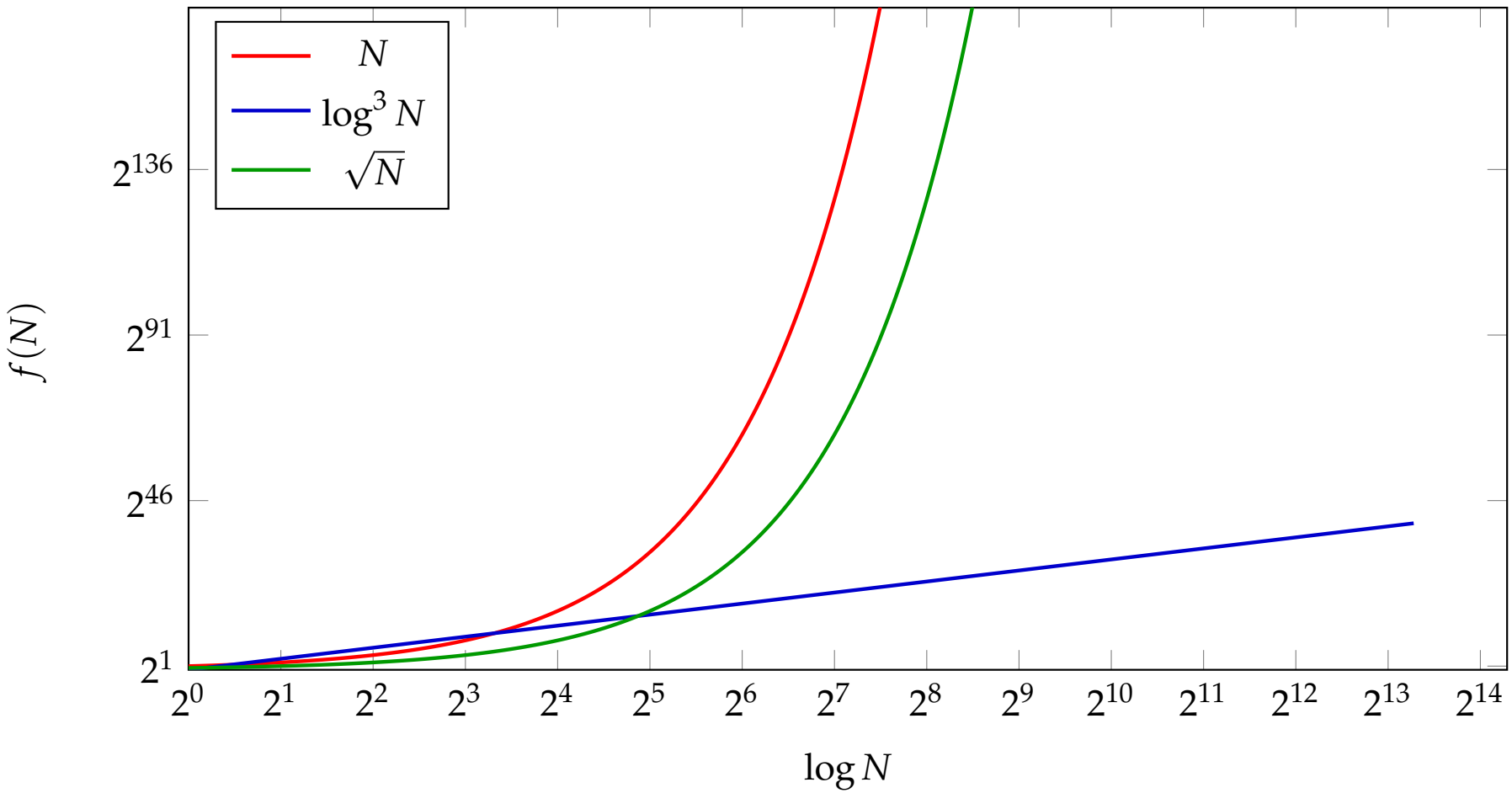


Complexité

Quelques **exemples** de comportement de fonctions (échelle « log log »).

Rappel :

- 2^{80} : très, très difficile à calculer, pour $\simeq 2^{30}$ op./s sur un processeur
- 2^{128} : supposé inatteignable

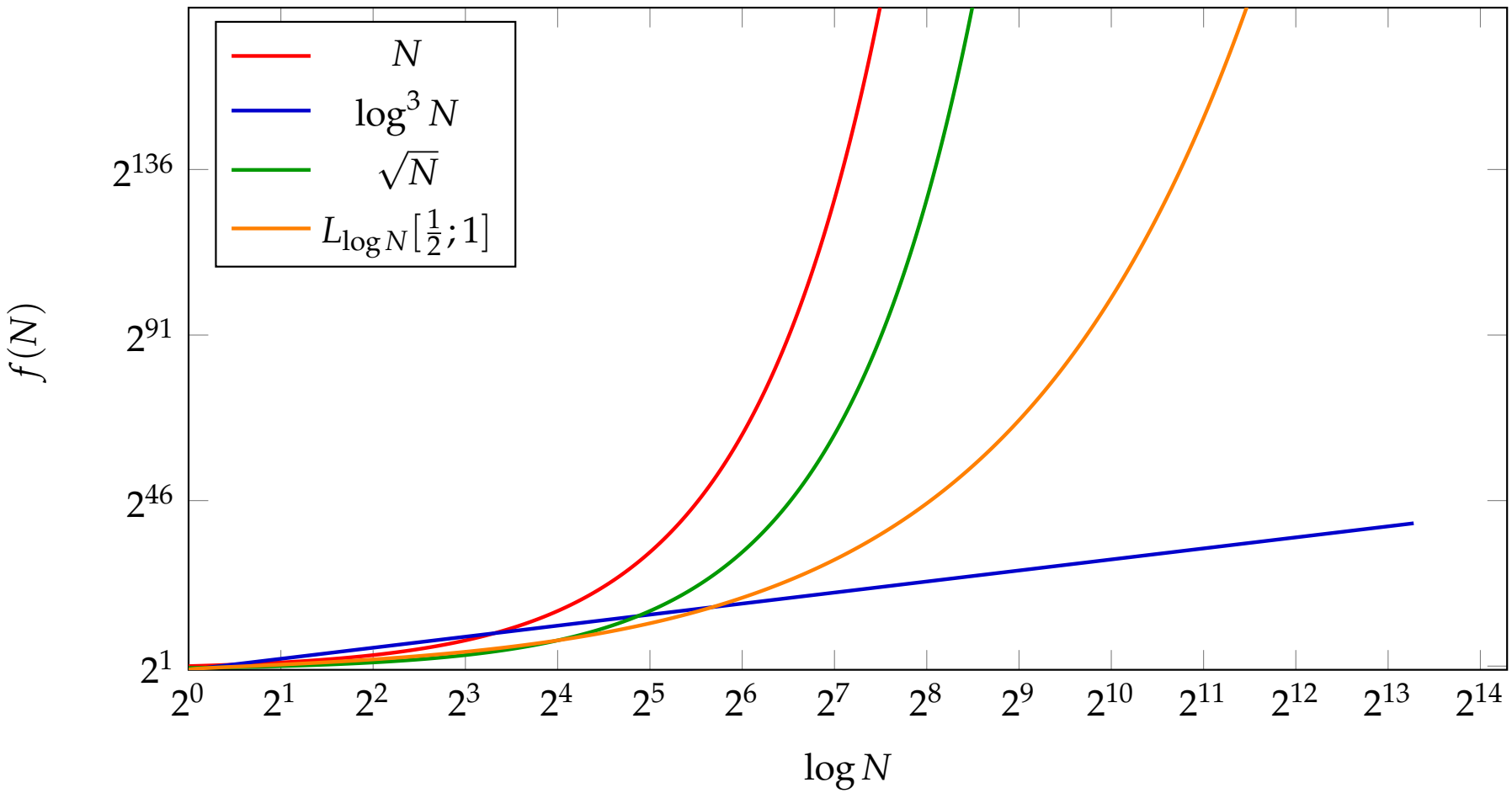


Complexité

Quelques **exemples** de comportement de fonctions (échelle « log log »).

Rappel :

- 2^{80} : très, très difficile à calculer, pour $\simeq 2^{30}$ op./s sur un processeur
- 2^{128} : supposé inatteignable

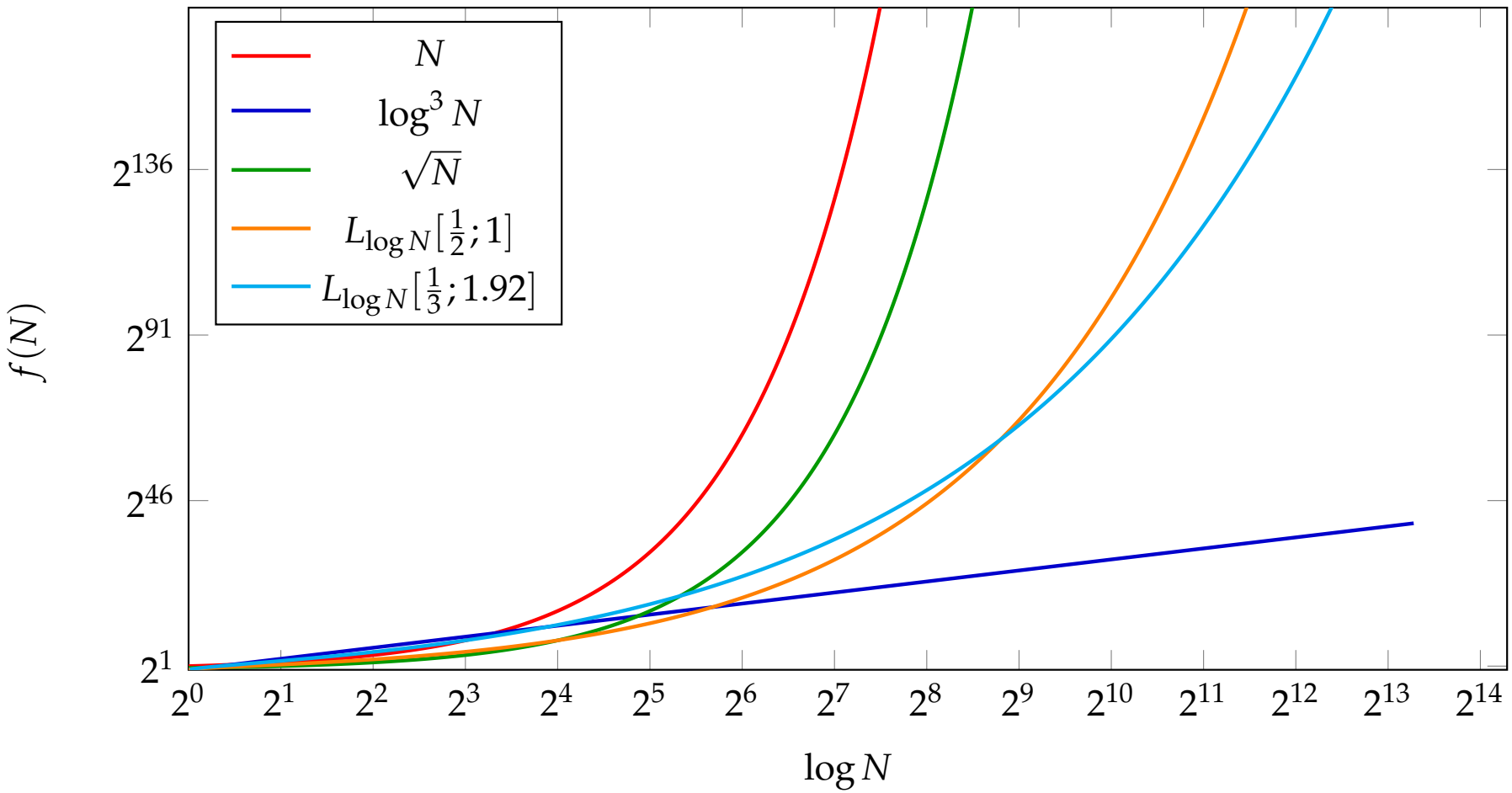


Complexité

Quelques **exemples** de comportement de fonctions (échelle « log log »).

Rappel :

- 2^{80} : très, très difficile à calculer, pour $\simeq 2^{30}$ op./s sur un processeur
- 2^{128} : supposé inatteignable



Crible quadratique : origines

Méthode de Fermat : si on arrive à écrire $N = a^2 - b^2$, alors $N = (a-b)(a+b)$ donne une factorisation de N.

Crible quadratique : origines

Méthode de Fermat : si on arrive à écrire $N = a^2 - b^2$, alors $N = (a-b)(a+b)$ donne une factorisation de N.

Raffinement de l'idée (Kraitchik, puis Dixon) :

Crible quadratique : origines

Méthode de Fermat : si on arrive à écrire $N = a^2 - b^2$, alors $N = (a-b)(a+b)$ donne une factorisation de N.

Raffinement de l'idée (Kraitchik, puis Dixon) :

> **Idée :** Si on obtient « seulement » $N \mid a^2 - b^2 = (a-b)(a+b)$, alors on peut espérer que $\text{pgcd}(a-b, N)$ ou $\text{pgcd}(a+b, N)$ donne un facteur propre de N.

Crible quadratique : origines

Méthode de Fermat : si on arrive à écrire $N = a^2 - b^2$, alors $N = (a-b)(a+b)$ donne une factorisation de N.

Raffinement de l'idée (Kraitchik, puis Dixon) :

> **Idée :** Si on obtient « seulement » $N \mid a^2 - b^2 = (a-b)(a+b)$, alors on peut espérer que $\mathrm{pgcd}(a-b, N)$ ou $\mathrm{pgcd}(a+b, N)$ donne un facteur propre de N.

Exemple. $N = 91$. On a $4^2 = 16$ et $17^2 = 289 \equiv 16 \bmod 91$.

Crible quadratique : origines

Méthode de Fermat : si on arrive à écrire $N = a^2 - b^2$, alors $N = (a-b)(a+b)$ donne une factorisation de N.

Raffinement de l'idée (Kraitchik, puis Dixon) :

> **Idée :** Si on obtient « seulement » $N \mid a^2 - b^2 = (a-b)(a+b)$, alors on peut espérer que $\text{pgcd}(a-b, N)$ ou $\text{pgcd}(a+b, N)$ donne un facteur propre de N.

Exemple. $N = 91$. On a $4^2 = 16$ et $17^2 = 289 \equiv 16 \bmod 91$. Puis, $\text{pgcd}(4+17, N) = 7$.

Crible quadratique : origines

Méthode de Fermat : si on arrive à écrire $N = a^2 - b^2$, alors $N = (a-b)(a+b)$ donne une factorisation de N.

Raffinement de l'idée (Kraitchik, puis Dixon) :

> **Idée :** Si on obtient « seulement » $N \mid a^2 - b^2 = (a-b)(a+b)$, alors on peut espérer que $\text{pgcd}(a-b, N)$ ou $\text{pgcd}(a+b, N)$ donne un facteur propre de N.

Exemple. $N = 91$. On a $4^2 = 16$ et $17^2 = 289 \equiv 16 \bmod 91$. Puis, $\text{pgcd}(4+17, N) = 7$. Ici, on a également $\text{pgcd}(17-4, N) = 13$.

Crible quadratique : origines

Méthode de Fermat : si on arrive à écrire $N = a^2 - b^2$, alors $N = (a-b)(a+b)$ donne une factorisation de N.

Raffinement de l'idée (Kraitchik, puis Dixon) :

> **Idée :** Si on obtient « seulement » $N \mid a^2 - b^2 = (a-b)(a+b)$, alors on peut espérer que $\text{pgcd}(a-b, N)$ ou $\text{pgcd}(a+b, N)$ donne un facteur propre de N.

Exemple. $N = 91$. On a $4^2 = 16$ et $17^2 = 289 \equiv 16 \mod 91$. Puis, $\text{pgcd}(4+17, N) = 7$. Ici, on a également $\text{pgcd}(17-4, N) = 13$.

Remarque. On obtient un facteur propre lorsque les a et b trouvés vérifient $a \not\equiv \pm b \mod N$.

Crible quadratique : origines

Méthode de Fermat : si on arrive à écrire $N = a^2 - b^2$, alors $N = (a-b)(a+b)$ donne une factorisation de N.

Raffinement de l'idée (Kraitchik, puis Dixon) :

> **Idée :** Si on obtient « seulement » $N \mid a^2 - b^2 = (a-b)(a+b)$, alors on peut espérer que $\text{pgcd}(a-b, N)$ ou $\text{pgcd}(a+b, N)$ donne un facteur propre de N.

Exemple. $N = 91$. On a $4^2 = 16$ et $17^2 = 289 \equiv 16 \bmod 91$. Puis, $\text{pgcd}(4+17, N) = 7$. Ici, on a également $\text{pgcd}(17-4, N) = 13$.

Remarque. On obtient un facteur propre lorsque les a et b trouvés vérifient $a \not\equiv \pm b \bmod N$.

Est-ce fréquent ?

Crible quadratique : origines

Méthode de Fermat : si on arrive à écrire $N = a^2 - b^2$, alors $N = (a-b)(a+b)$ donne une factorisation de N.

Raffinement de l'idée (Kraitchik, puis Dixon) :

Idée : Si on obtient « seulement » $N \mid a^2 - b^2 = (a-b)(a+b)$, alors on peut espérer que $\text{pgcd}(a-b, N)$ ou $\text{pgcd}(a+b, N)$ donne un facteur propre de N.

Exemple. $N = 91$. On a $4^2 = 16$ et $17^2 = 289 \equiv 16 \mod 91$. Puis, $\text{pgcd}(4+17, N) = 7$. Ici, on a également $\text{pgcd}(17-4, N) = 13$.

Remarque. On obtient un facteur propre lorsque les a et b trouvés vérifient $a \not\equiv \pm b \mod N$.

Est-ce fréquent ?

Lemme. Si N admet t diviseurs premiers distincts, alors l'équation $x^2 \equiv 1 \mod N$ admet 2^t solutions.

Crible quadratique : origines

Méthode de Fermat : si on arrive à écrire $N = a^2 - b^2$, alors $N = (a-b)(a+b)$ donne une factorisation de N.

Raffinement de l'idée (Kraitchik, puis Dixon) :

> **Idée :** Si on obtient « seulement » $N \mid a^2 - b^2 = (a-b)(a+b)$, alors on peut espérer que $\text{pgcd}(a-b, N)$ ou $\text{pgcd}(a+b, N)$ donne un facteur propre de N.

Exemple. $N = 91$. On a $4^2 = 16$ et $17^2 = 289 \equiv 16 \mod 91$. Puis, $\text{pgcd}(4+17, N) = 7$. Ici, on a également $\text{pgcd}(17-4, N) = 13$.

Remarque. On obtient un facteur propre lorsque les a et b trouvés vérifient $a \not\equiv \pm b \mod N$.

Est-ce fréquent ?

> **Lemme.** Si N admet t diviseurs premiers distincts, alors l'équation $x^2 \equiv 1 \mod N$ admet 2^t solutions.

Conséquence. Si N est composé ($t \geq 2$) et si $a^2 \equiv b^2 \mod N$ ont été trouvés « aléatoirement », alors il y a plus d'une chance sur deux pour que $a \not\equiv \pm b \mod N$.

Crible quadratique : origines

Méthode de Fermat : si on arrive à écrire $N = a^2 - b^2$, alors $N = (a-b)(a+b)$ donne une factorisation de N.

Raffinement de l'idée (Kraitchik, puis Dixon) :

Idée : Si on obtient « seulement » $N \mid a^2 - b^2 = (a-b)(a+b)$, alors on peut espérer que $\text{pgcd}(a-b, N)$ ou $\text{pgcd}(a+b, N)$ donne un facteur propre de N.

Exemple. $N = 91$. On a $4^2 = 16$ et $17^2 = 289 \equiv 16 \mod 91$. Puis, $\text{pgcd}(4+17, N) = 7$. Ici, on a également $\text{pgcd}(17-4, N) = 13$.

Remarque. On obtient un facteur propre lorsque les a et b trouvés vérifient $a \not\equiv \pm b \mod N$.

Est-ce fréquent ?

Lemme. Si N admet t diviseurs premiers distincts, alors l'équation $x^2 \equiv 1 \mod N$ admet 2^t solutions.

Conséquence. Si N est composé ($t \geq 2$) et si $a^2 \equiv b^2 \mod N$ ont été trouvés « aléatoirement », alors il y a plus d'une chance sur deux pour que $a \not\equiv \pm b \mod N$.

Question. Comment trouver a, b tels que $a^2 \equiv b^2 \mod N$?

Comment trouver $a^2 \equiv b^2 \mod N$?

Idée. Étant donnée une borne de lissité $B \geq 2$:

Comment trouver $a^2 \equiv b^2 \mod N$?

Idée. Étant donnée une borne de lissité $B \geq 2$:

1. on crée une base de facteurs premiers $\mathcal{P} = \{p_1, \ldots, p_s\}$, tous inférieurs à B

Comment trouver $a^2 \equiv b^2 \mod N$?

Idée. Étant donnée une borne de lissité $B \geq 2$:

1. on crée une base de facteurs premiers $\mathcal{P} = \{p_1, \ldots, p_s\}$, tous inférieurs à B
2. on collecte une quantité importante d'éléments **qui se décomposent sur** $\mathcal{P}$, et qui s'écrivent sous la forme

$$Q(x) := (x + \lceil \sqrt{N} \rceil)^2 - N$$

Comment trouver $a^2 \equiv b^2 \mod N$?

Idée. Étant donnée une borne de lissité $B \geq 2$:

1. on crée une base de facteurs premiers $\mathcal{P} = \{p_1, \ldots, p_s\}$, tous inférieurs à B
2. on collecte une quantité importante d'éléments **qui se décomposent sur** $\mathcal{P}$, et qui s'écrivent sous la forme
$$Q(x) := (x + \lceil \sqrt{N} \rceil)^2 - N$$
3. on essaie de **combiner** certains $Q(x_i)$ pour obtenir un carré modulo N :
$$Q(x_1) \cdots Q(x_k) \equiv b^2 \mod N$$

Comment trouver $a^2 \equiv b^2 \mod N$?

Idée. Étant donnée une borne de lissité $B \geq 2$:

1. on crée une base de facteurs premiers $\mathcal{P} = \{p_1, \ldots, p_s\}$, tous inférieurs à B
2. on collecte une quantité importante d'éléments **qui se décomposent sur** $\mathcal{P}$, et qui s'écrivent sous la forme
$$Q(x) := (x + \lceil \sqrt{N} \rceil)^2 - N$$
3. on essaie de **combiner** certains $Q(x_i)$ pour obtenir un carré modulo N :
$$Q(x_1) \cdots Q(x_k) \equiv b^2 \mod N$$

Alors, on aura obtenu $a^2 \equiv b^2 \mod N$ où $a := (x_1 + \lceil \sqrt{N} \rceil) \cdots (x_k + \lceil \sqrt{N} \rceil)$.

Comment trouver $a^2 \equiv b^2 \mod N$?

Idée. Étant donnée une borne de lissité $B \geq 2$:

1. on crée une base de facteurs premiers $\mathcal{P} = \{p_1, \ldots, p_s\}$, tous inférieurs à B
2. on collecte une quantité importante d'éléments **qui se décomposent sur** $\mathcal{P}$, et qui s'écrivent sous la forme
$$Q(x) := (x + \lceil \sqrt{N} \rceil)^2 - N$$
3. on essaie de **combiner** certains $Q(x_i)$ pour obtenir un carré modulo N :
$$Q(x_1) \cdots Q(x_k) \equiv b^2 \mod N$$

Alors, on aura obtenu $a^2 \equiv b^2 \mod N$ où $a := (x_1 + \lceil \sqrt{N} \rceil) \cdots (x_k + \lceil \sqrt{N} \rceil)$.

Exemple : $N = 1649$ donne $\lceil \sqrt{N} \rceil = 41$.

Comment trouver $a^2 \equiv b^2 \mod N$?

Idée. Étant donnée une borne de lissité $B \geq 2$:

1. on crée une base de facteurs premiers $\mathcal{P} = \{p_1, \ldots, p_s\}$, tous inférieurs à B
2. on collecte une quantité importante d'éléments **qui se décomposent sur** $\mathcal{P}$, et qui s'écrivent sous la forme
$$Q(x) := (x + \lceil \sqrt{N} \rceil)^2 - N$$
3. on essaie de **combiner** certains $Q(x_i)$ pour obtenir un carré modulo N :
$$Q(x_1) \cdots Q(x_k) \equiv b^2 \mod N$$

Alors, on aura obtenu $a^2 \equiv b^2 \mod N$ où $a := (x_1 + \lceil \sqrt{N} \rceil) \cdots (x_k + \lceil \sqrt{N} \rceil)$.

Exemple : $N = 1649$ donne $\lceil \sqrt{N} \rceil = 41$. On choisit la borne $B = 6$. Puis, modulo N, on obtient

$$\begin{cases} (x=0) & 41^2 = 1681 & \equiv 32 & \equiv 2^5 & \mod N & \text{(ok)} \\ (x=1) & 42^2 = 1764 & \equiv 115 & \equiv 5 \times 23 & \mod N & \\ (x=2) & 43^2 = 1849 & \equiv 200 & \equiv 2^3 \times 5^2 & \mod N & \text{(ok)} \end{cases}$$

Comment trouver $a^2 \equiv b^2 \mod N$?

Idée. Étant donnée une borne de lissité $B \geq 2$:

1. on crée une base de facteurs premiers $\mathcal{P} = \{p_1, \ldots, p_s\}$, tous inférieurs à B
2. on collecte une quantité importante d'éléments **qui se décomposent sur** $\mathcal{P}$, et qui s'écrivent sous la forme
$$Q(x) := (x + \lceil \sqrt{N} \rceil)^2 - N$$
3. on essaie de **combiner** certains $Q(x_i)$ pour obtenir un carré modulo N :
$$Q(x_1) \cdots Q(x_k) \equiv b^2 \mod N$$

Alors, on aura obtenu $a^2 \equiv b^2 \mod N$ où $a := (x_1 + \lceil \sqrt{N} \rceil) \cdots (x_k + \lceil \sqrt{N} \rceil)$.

Exemple : $N = 1649$ donne $\lceil \sqrt{N} \rceil = 41$. On choisit la borne $B = 6$. Puis, modulo N, on obtient

$$\begin{cases} (x=0) & 41^2 = 1681 & \equiv 32 & \equiv 2^5 & \mod N & \text{(ok)} \\ (x=1) & 42^2 = 1764 & \equiv 115 & \equiv 5 \times 23 & \mod N & \\ (x=2) & 43^2 = 1849 & \equiv 200 & \equiv 2^3 \times 5^2 & \mod N & \text{(ok)} \end{cases}$$

Ainsi, on note que
$$41^2 \times 43^2 \equiv 2^8 \times 5^2 \equiv (2^4 \times 5)^2 \mod N\,.$$

Comment trouver $a^2 \equiv b^2 \mod N$?

Idée. Étant donnée une borne de lissité $B \geq 2$:

1. on crée une base de facteurs premiers $\mathcal{P} = \{p_1, \ldots, p_s\}$, tous inférieurs à B
2. on collecte une quantité importante d'éléments **qui se décomposent sur** $\mathcal{P}$, et qui s'écrivent sous la forme
$$Q(x) := (x + \lceil \sqrt{N} \rceil)^2 - N$$
3. on essaie de **combiner** certains $Q(x_i)$ pour obtenir un carré modulo N :
$$Q(x_1) \cdots Q(x_k) \equiv b^2 \mod N$$

Alors, on aura obtenu $a^2 \equiv b^2 \mod N$ où $a := (x_1 + \lceil \sqrt{N} \rceil) \cdots (x_k + \lceil \sqrt{N} \rceil)$.

Exemple : $N = 1649$ donne $\lceil \sqrt{N} \rceil = 41$. On choisit la borne $B = 6$. Puis, modulo N, on obtient

$$\begin{cases} (x=0) & 41^2 = 1681 & \equiv 32 & \equiv 2^5 & \mod N & \text{(ok)} \\ (x=1) & 42^2 = 1764 & \equiv 115 & \equiv 5 \times 23 & \mod N & \\ (x=2) & 43^2 = 1849 & \equiv 200 & \equiv 2^3 \times 5^2 & \mod N & \text{(ok)} \end{cases}$$

Ainsi, on note que
$$41^2 \times 43^2 \equiv 2^8 \times 5^2 \equiv (2^4 \times 5)^2 \mod N\,.$$

Il résulte que $1763^2 \equiv 80^2 \mod N$, on a bien $114 \equiv 1763 \not\equiv \pm 80 \mod N$. Puis, on obtient $\text{pgcd}(114 - 80, 1649) = 17$ un facteur propre de $N = 1469$.

Comment trouver $a^2 \equiv b^2 \mod N$?

Idée. Étant donnée une borne de lissité $B \geq 2$:

1. on crée une base de facteurs premiers $\mathcal{P} = \{p_1, \ldots, p_s\}$, tous inférieurs à B
2. on collecte une quantité importante d'éléments **qui se décomposent sur** $\mathcal{P}$, et qui s'écrivent sous la forme
$$Q(x) := (x + \lceil \sqrt{N} \rceil)^2 - N$$
3. on essaie de **combiner** certains $Q(x_i)$ pour obtenir un carré modulo N :
$$Q(x_1) \cdots Q(x_k) \equiv b^2 \mod N$$

Alors, on aura obtenu $a^2 \equiv b^2 \mod N$ où $a := (x_1 + \lceil \sqrt{N} \rceil) \cdots (x_k + \lceil \sqrt{N} \rceil)$.

Exemple : $N = 1649$ donne $\lceil \sqrt{N} \rceil = 41$. On choisit la borne $B = 6$. Puis, modulo N, on obtient

$$\begin{cases} (x=0) & 41^2 = 1681 & \equiv 32 & \equiv 2^5 & \mod N & \text{(ok)} \\ (x=1) & 42^2 = 1764 & \equiv 115 & \equiv 5 \times 23 & \mod N & \\ (x=2) & 43^2 = 1849 & \equiv 200 & \equiv 2^3 \times 5^2 & \mod N & \text{(ok)} \end{cases}$$

Ainsi, on note que
$$41^2 \times 43^2 \equiv 2^8 \times 5^2 \equiv (2^4 \times 5)^2 \mod N\,.$$

Il résulte que $1763^2 \equiv 80^2 \mod N$, on a bien $114 \equiv 1763 \not\equiv \pm 80 \mod N$. Puis, on obtient $\text{pgcd}(114 - 80, 1649) = 17$ un facteur propre de $N = 1469$.

Remarque. Avec l'algorithme de Fermat, on aurait dû aller jusqu'à 57^2 pour factoriser.

Comment trouver $a^2 \equiv b^2 \mod N$?

Idée. Étant donnée une borne de lissité $B \geq 2$:

1. on crée une base de facteurs premiers $\mathcal{P} = \{p_1, \ldots, p_s\}$, tous inférieurs à B
2. on collecte une quantité importante d'éléments qui se décomposent sur $\mathcal{P}$, et de la forme
$$Q(x) := (x + \lceil \sqrt{N} \rceil)^2 - N$$
3. on essaie de combiner certains $Q(x_i)$ pour que
$$Q(x_1) \cdots Q(x_k) \equiv b^2 \mod N$$

Alors, on aura obtenu $a^2 \equiv b^2 \mod N$ où $a := (x_1 + \lceil \sqrt{N} \rceil) \cdots (x_k + \lceil \sqrt{N} \rceil)$.

Trois questions :

Comment trouver $a^2 \equiv b^2 \mod N$?

Idée. Étant donnée une borne de lissité $B \geq 2$:

1. on crée une base de facteurs premiers $\mathcal{P} = \{p_1, \ldots, p_s\}$, tous inférieurs à B
2. on collecte une quantité importante d'éléments qui se décomposent sur $\mathcal{P}$, et de la forme
$$Q(x) := (x + \lceil \sqrt{N} \rceil)^2 - N$$
3. on essaie de combiner certains $Q(x_i)$ pour que
$$Q(x_1) \cdots Q(x_k) \equiv b^2 \mod N$$

Alors, on aura obtenu $a^2 \equiv b^2 \mod N$ où $a := (x_1 + \lceil \sqrt{N} \rceil) \cdots (x_k + \lceil \sqrt{N} \rceil)$.

Trois questions :

1. quelle base de facteurs premiers $\mathcal{P}$ choisir ?

Comment trouver $a^2 \equiv b^2 \mod N$?

Idée. Étant donnée une borne de lissité $B \geq 2$:

1. on crée une base de facteurs premiers $\mathcal{P} = \{p_1, \ldots, p_s\}$, tous inférieurs à B
2. on collecte une quantité importante d'éléments qui se décomposent sur $\mathcal{P}$, et de la forme
$$Q(x) := (x + \lceil \sqrt{N} \rceil)^2 - N$$
3. on essaie de combiner certains $Q(x_i)$ pour que
$$Q(x_1) \cdots Q(x_k) \equiv b^2 \mod N$$

Alors, on aura obtenu $a^2 \equiv b^2 \mod N$ où $a := (x_1 + \lceil \sqrt{N} \rceil) \cdots (x_k + \lceil \sqrt{N} \rceil)$.

Trois questions :

1. quelle base de facteurs premiers $\mathcal{P}$ choisir ?
2. comment obtient-on ces éléments B-friables de la forme $Q(x)$?
   $\rightarrow$ technique de crible (ici, quadratique)

Comment trouver $a^2 \equiv b^2 \mod N$?

Idée. Étant donnée une borne de lissité $B \geq 2$:

1. on crée une base de facteurs premiers $\mathcal{P} = \{p_1, \ldots, p_s\}$, tous inférieurs à B
2. on collecte une quantité importante d'éléments qui se décomposent sur $\mathcal{P}$, et de la forme
$$Q(x) := (x + \lceil \sqrt{N} \rceil)^2 - N$$
3. on essaie de combiner certains $Q(x_i)$ pour que
$$Q(x_1) \cdots Q(x_k) \equiv b^2 \mod N$$

Alors, on aura obtenu $a^2 \equiv b^2 \mod N$ où $a := (x_1 + \lceil \sqrt{N} \rceil) \cdots (x_k + \lceil \sqrt{N} \rceil)$.

Trois questions :

1. quelle base de facteurs premiers $\mathcal{P}$ choisir ?
2. comment obtient-on ces éléments B-friables de la forme $Q(x)$?
   $\rightarrow$ technique de crible (ici, quadratique)
3. comment savoir quels $Q(x_i)$ multiplier pour obtenir un carré modulo N ?
   $\rightarrow$ algèbre linéaire dans $\mathbb{F}_2$

Étape I : base de facteurs

Première étape : construction de la **base de facteurs**.

Étape I : base de facteurs

Première étape : construction de la **base de facteurs**.

Si $x < \sqrt{N}/3$, alors on a

$$Q(x) = (x + \lceil \sqrt{N} \rceil)^2 - N \simeq x^2 + 2\sqrt{N}x < N.$$

Étape I : base de facteurs

Première étape : construction de la **base de facteurs**.

Si $x < \sqrt{N}/3$, alors on a

$$Q(x) = (x + \lceil \sqrt{N} \rceil)^2 - N \simeq x^2 + 2\sqrt{N}x < N.$$

Donc $(Q(x) \bmod N)$ vaut $Q(x)$, et pour tout premier $p \geq 2$, on a

$$p \mid Q(x) \implies N \text{ est un carré modulo } p$$

Étape I : base de facteurs

Première étape : construction de la **base de facteurs**.

Si $x < \sqrt{N}/3$, alors on a

$$Q(x) = (x + \lceil \sqrt{N} \rceil)^2 - N \simeq x^2 + 2\sqrt{N}x < N.$$

Donc $(Q(x) \bmod N)$ vaut $Q(x)$, et pour tout premier $p \geq 2$, on a

$$p \mid Q(x) \implies N \text{ est un carré modulo } p$$

Pour constituer la base de facteurs, on peut donc considérer **uniquement** les premiers p tel que $\left(\frac{N}{p}\right) = 1$ et $p \leq B$.

Étape I : base de facteurs

Première étape : construction de la **base de facteurs**.

Si $x < \sqrt{N}/3$, alors on a

$$Q(x) = (x + \lceil \sqrt{N} \rceil)^2 - N \simeq x^2 + 2\sqrt{N}x < N.$$

Donc $(Q(x) \bmod N)$ vaut $Q(x)$, et pour tout premier $p \geq 2$, on a

$$p \mid Q(x) \implies N \text{ est un carré modulo } p$$

Pour constituer la base de facteurs, on peut donc considérer **uniquement** les premiers p tel que $\left(\frac{N}{p}\right) = 1$ et $p \leq B$.

Exemple : $N = 369713 = 457 \times 809$. On choisit ici $B = 21$. On a alors

p	2	3	5	7	11	13	17	19
$\left(\frac{N}{p}\right)$	1	-1	-1	1	1	-1	-1	1

Étape I : base de facteurs

Première étape : construction de la **base de facteurs**.

Si $x < \sqrt{N}/3$, alors on a

$$Q(x) = (x + \lceil \sqrt{N} \rceil)^2 - N \simeq x^2 + 2\sqrt{N}x < N.$$

Donc $(Q(x) \bmod N)$ vaut $Q(x)$, et pour tout premier $p \geq 2$, on a

$$p \mid Q(x) \implies N \text{ est un carré modulo } p$$

Pour constituer la base de facteurs, on peut donc considérer **uniquement** les premiers p tel que $\left(\frac{N}{p}\right) = 1$ et $p \leq B$.

Exemple : $N = 369713 = 457 \times 809$. On choisit ici $B = 21$. On a alors

p	2	3	5	7	11	13	17	19
$\left(\frac{N}{p}\right)$	1	-1	-1	1	1	-1	-1	1

La base de facteurs est donc $\{2, 7, 11, 19\}$.

Étape III : algèbre linéaire

Troisième étape : l'**algèbre linéaire**.

Étape III : algèbre linéaire

Troisième étape : l'**algèbre linéaire**.

Soit $\mathcal{P} = \{p_1, \ldots, p_s\}$ la base de facteurs construite précédemment.

Étape III : algèbre linéaire

Troisième étape : l'**algèbre linéaire**.

Soit $\mathcal{P} = \{p_1, \ldots, p_s\}$ la base de facteurs construite précédemment.

Supposons que l'on ait collecté t éléments $Q(x_1), \ldots, Q(x_t)$ tels que les $Q(x_i) \mod N$ se décomposent dans $\mathcal{P}$ (étape II).

Étape III : algèbre linéaire

Troisième étape : l'**algèbre linéaire**.

Soit $\mathcal{P} = \{p_1, \ldots, p_s\}$ la base de facteurs construite précédemment.

Supposons que l'on ait collecté t éléments $Q(x_1), \ldots, Q(x_t)$ tels que les $Q(x_i) \bmod N$ se décomposent dans $\mathcal{P}$ (étape II). On peut alors écrire $Q(x_i) \bmod N$ sous la forme

$$p_1^{e_1^{(i)}} \times p_2^{e_2^{(i)}} \times \cdots \times p_s^{e_s^{(i)}}$$

et on note $\boldsymbol{e}(x_i) = (e_1^{(i)}, \ldots, e_s^{(i)})$.

Étape III : algèbre linéaire

Troisième étape : l'**algèbre linéaire**.

Soit $\mathcal{P} = \{p_1, \ldots, p_s\}$ la base de facteurs construite précédemment.

Supposons que l'on ait collecté t éléments $Q(x_1), \ldots, Q(x_t)$ tels que les $Q(x_i) \mod N$ se décomposent dans $\mathcal{P}$ (étape II). On peut alors écrire $Q(x_i) \mod N$ sous la forme

$$p_1^{e_1^{(i)}} \times p_2^{e_2^{(i)}} \times \cdots \times p_s^{e_s^{(i)}}$$

et on note $\boldsymbol{e}(x_i) = (e_1^{(i)}, \ldots, e_s^{(i)})$.

Alors, on a $Q(x_{i_1})Q(x_{i_2}) \ldots Q(x_{i_k}) \equiv p_1^{e_1} \cdots p_s^{e_s} \mod N$ où

$$(e_1, \ldots, e_s) \;=\; \boldsymbol{e}(x_{i_1}) + \boldsymbol{e}(x_{i_2}) + \cdots + \boldsymbol{e}(x_{i_k})\,.$$

Étape III : algèbre linéaire

Troisième étape : l'**algèbre linéaire**.

Soit $\mathcal{P} = \{p_1, \ldots, p_s\}$ la base de facteurs construite précédemment.

Supposons que l'on ait collecté t éléments $Q(x_1), \ldots, Q(x_t)$ tels que les $Q(x_i) \mod N$ se décomposent dans $\mathcal{P}$ (étape II). On peut alors écrire $Q(x_i) \mod N$ sous la forme

$$p_1^{e_1^{(i)}} \times p_2^{e_2^{(i)}} \times \cdots \times p_s^{e_s^{(i)}}$$

et on note $\boldsymbol{e}(x_i) = (e_1^{(i)}, \ldots, e_s^{(i)})$.

Alors, on a $Q(x_{i_1})Q(x_{i_2}) \ldots Q(x_{i_k}) \equiv p_1^{e_1} \cdots p_s^{e_s} \mod N$ où

$$(e_1, \ldots, e_s) \;=\; \boldsymbol{e}(x_{i_1}) + \boldsymbol{e}(x_{i_2}) + \cdots + \boldsymbol{e}(x_{i_k})\,.$$

Lemme. L'élément $Q(x_1) \ldots Q(x_k)$ est un carré modulo N si et seulement si

$$\sum_{i=1}^{k} \boldsymbol{e}(x_i) = \boldsymbol{0} \mod 2\,.$$

Étape III : algèbre linéaire

Lemme. L'élément $Q(x_1)\dots Q(x_k)$ est un carré modulo N si et seulement si

$$\sum_{i=1}^{k} \boldsymbol{e}(x_i) = \mathbf{0} \mod 2\,.$$

Étape III : algèbre linéaire

Lemme. L'élément $Q(x_1)\dots Q(x_k)$ est un carré modulo N si et seulement si

$$\sum_{i=1}^{k} \boldsymbol{e}(x_i) = \mathbf{0} \mod 2\,.$$

On va alors construire une matrice $\boldsymbol{M}$ entière de taille $(t \times s)$ telle la i-ème ligne de $\boldsymbol{M}$ est le vecteur ligne $\boldsymbol{e}(x_i)$:

$$\boldsymbol{M} = \begin{bmatrix} e_1^{(1)} & e_2^{(1)} & \dots & e_s^{(1)} \\ e_1^{(2)} & \dots & \dots & e_s^{(2)} \\ \vdots & & & \\ & & & \\ e_1^{(t)} & \dots & \dots & e_s^{(t)} \end{bmatrix} \in \mathbb{N}^{t\times s}$$

Étape III : algèbre linéaire

Lemme. L'élément $Q(x_1)\dots Q(x_k)$ est un carré modulo N si et seulement si

$$\sum_{i=1}^{k} \boldsymbol{e}(x_i) = \mathbf{0} \mod 2\,.$$

On va alors construire une matrice $\boldsymbol{M}$ entière de taille $(t \times s)$ telle la i-ème ligne de $\boldsymbol{M}$ est le vecteur ligne $\boldsymbol{e}(x_i)$:

$$\boldsymbol{M} = \begin{bmatrix} e_1^{(1)} & e_2^{(1)} & \dots & e_s^{(1)} \\ e_1^{(2)} & \dots & \dots & e_s^{(2)} \\ \vdots & & & \\ & & & \\ e_1^{(t)} & \dots & \dots & e_s^{(t)} \end{bmatrix} \in \mathbb{N}^{t\times s}$$

Pour obtenir un carré modulo N de la forme $Q(x_1)\dots Q(x_k)$, il suffit donc de chercher un élément du noyau à gauche de la matrice $(\boldsymbol{M} \mod 2)$, car

$$\boldsymbol{u} = (u_1, \dots, u_t) \in \mathbb{F}_2^t \text{ vérifie } \boldsymbol{uM} = \mathbf{0} \quad \Longrightarrow \quad \sum u_i \boldsymbol{e}(x_i) = \mathbf{0}\,.$$

Étape III : algèbre linéaire

Lemme. L'élément $Q(x_1)\dots Q(x_k)$ est un carré modulo N si et seulement si

$$\sum_{i=1}^{k} \boldsymbol{e}(x_i) = \mathbf{0} \mod 2\,.$$

On va alors construire une matrice $\boldsymbol{M}$ entière de taille $(t \times s)$ telle la i-ème ligne de $\boldsymbol{M}$ est le vecteur ligne $\boldsymbol{e}(x_i)$:

$$\boldsymbol{M} = \begin{bmatrix} e_1^{(1)} & e_2^{(1)} & \dots & e_s^{(1)} \\ e_1^{(2)} & \dots & \dots & e_s^{(2)} \\ \vdots & & & \\ & & & \\ e_1^{(t)} & \dots & \dots & e_s^{(t)} \end{bmatrix} \in \mathbb{N}^{t\times s}$$

Pour obtenir un carré modulo N de la forme $Q(x_1)\dots Q(x_k)$, il suffit donc de chercher un élément du noyau à gauche de la matrice $(\boldsymbol{M} \bmod 2)$, car

$$\boldsymbol{u} = (u_1, \dots, u_t) \in \mathbb{F}_2^t \text{ vérifie } \boldsymbol{uM} = \mathbf{0} \quad \Longrightarrow \quad \sum u_i \boldsymbol{e}(x_i) = \mathbf{0}\,.$$

Remarque. Pour que la matrice $(\boldsymbol{M} \bmod 2)$ ait un noyau (à gauche) non-nul, il est suffisant que le nombre de lignes non-nulles de $(\boldsymbol{M} \bmod 2)$ soit plus grand que le nombre de ses colonnes. En pratique, on souhaite donc que t soit sensiblement plus grand que s.

Étape III : exemple

Pour $N = 369713$ et $\mathcal{P} = \{2, 7, 11, 19\}$, supposons que l'on ait obtenu les éléments suivants :

x_i	6	8	24	106	120
$Q(x_i)$	8512	10976	30976	141512	161728
	$2^6 \times 7 \times 19$	$2^5 \times 7^3$	$2^8 \times 11$	$2^3 \times 7^2 \times 19^2$	$2^6 \times 7 \times 19^2$

Étape III : exemple

Pour $N = 369713$ et $\mathcal{P} = \{2, 7, 11, 19\}$, supposons que l'on ait obtenu les éléments suivants :

x_i	6	8	24	106	120
$Q(x_i)$	8512	10976	30976	141512	161728
	$2^6 \times 7 \times 19$	$2^5 \times 7^3$	$2^8 \times 11$	$2^3 \times 7^2 \times 19^2$	$2^6 \times 7 \times 19^2$

La matrice $\boldsymbol{M}$ est alors :

$$\boldsymbol{M} = \begin{bmatrix} 6 & 1 & 0 & 1 \\ 5 & 3 & 0 & 0 \\ 8 & 0 & 2 & 0 \\ 3 & 2 & 0 & 2 \\ 6 & 1 & 0 & 2 \end{bmatrix}$$

Étape III : exemple

Pour $N = 369713$ et $\mathcal{P} = \{2, 7, 11, 19\}$, supposons que l'on ait obtenu les éléments suivants :

x_i	6	8	24	106	120
$Q(x_i)$	8512	10976	30976	141512	161728
	$2^6 \times 7 \times 19$	$2^5 \times 7^3$	$2^8 \times 11$	$2^3 \times 7^2 \times 19^2$	$2^6 \times 7 \times 19^2$

La matrice $\boldsymbol{M}$ est alors :

$$\boldsymbol{M} = \begin{bmatrix} 6 & 1 & 0 & 1 \\ 5 & 3 & 0 & 0 \\ 8 & 0 & 2 & 0 \\ 3 & 2 & 0 & 2 \\ 6 & 1 & 0 & 2 \end{bmatrix}$$

Modulo 2, on obtient :

$$(\boldsymbol{M} \mod 2) = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$

Étape III : exemple

Pour $N = 369713$ et $\mathcal{P} = \{2, 7, 11, 19\}$, supposons que l'on ait obtenu les éléments suivants :

x_i	6	8	24	106	120
$Q(x_i)$	8512	10976	30976	141512	161728
	$2^6 \times 7 \times 19$	$2^5 \times 7^3$	$2^8 \times 11$	$2^3 \times 7^2 \times 19^2$	$2^6 \times 7 \times 19^2$

La matrice $\boldsymbol{M}$ est alors :

$$\boldsymbol{M} = \begin{bmatrix} 6 & 1 & 0 & 1 \\ 5 & 3 & 0 & 0 \\ 8 & 0 & 2 & 0 \\ 3 & 2 & 0 & 2 \\ 6 & 1 & 0 & 2 \end{bmatrix}$$

Modulo 2, on obtient :

$$(\boldsymbol{M} \mod 2) = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$

Puis, on trouve un élément $\boldsymbol{u}$ tel que $\boldsymbol{uM} = \boldsymbol{0}$, par exemple

$$\boldsymbol{u} = (0, 1, 1, 1, 1) \text{ ou encore } \boldsymbol{u} = (0, 0, 1, 0, 0)$$

Étape III : exemple

x_i	6	8	24	106	120
$Q(x_i)$	8512	10976	30976	141512	161728

$$\boldsymbol{M} = \begin{bmatrix} 6 & 1 & 0 & 1 \\ 5 & 3 & 0 & 0 \\ 8 & 0 & 2 & 0 \\ 3 & 2 & 0 & 2 \\ 6 & 1 & 0 & 2 \end{bmatrix} \qquad (\boldsymbol{M} \mod 2) = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \qquad \boldsymbol{u} = (0,1,1,1,1)$$

Étape III : exemple

x_i	6	8	24	106	120
$Q(x_i)$	8512	10976	30976	141512	161728

$$\boldsymbol{M} = \begin{bmatrix} 6 & 1 & 0 & 1 \\ 5 & 3 & 0 & 0 \\ 8 & 0 & 2 & 0 \\ 3 & 2 & 0 & 2 \\ 6 & 1 & 0 & 2 \end{bmatrix} \qquad (\boldsymbol{M} \mod 2) = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \qquad \boldsymbol{u} = (0,1,1,1,1)$$

On calcule $\boldsymbol{u} \cdot \boldsymbol{M} = (22,6,2,4)$, donc on va construire

Étape III : exemple

x_i	6	8	24	106	120
$Q(x_i)$	8512	10976	30976	141512	161728

$$\boldsymbol{M} = \begin{bmatrix} 6 & 1 & 0 & 1 \\ 5 & 3 & 0 & 0 \\ 8 & 0 & 2 & 0 \\ 3 & 2 & 0 & 2 \\ 6 & 1 & 0 & 2 \end{bmatrix} \qquad (\boldsymbol{M} \mod 2) = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \qquad \boldsymbol{u} = (0,1,1,1,1)$$

On calcule $\boldsymbol{u} \cdot \boldsymbol{M} = (22,6,2,4)$, donc on va construire

1. b une racine carrée de $Q(x_2)Q(x_3)Q(x_4)Q(x_5) = p_1^{22}\, p_2^6\, p_3^2\, p_4^4$, c'est-à-dire

$$b = p_1^{11}\, p_2^3\, p_3\, p_4^2 \equiv 369672 \mod N$$

Étape III : exemple

x_i	6	8	24	106	120
$Q(x_i)$	8512	10976	30976	141512	161728

$$\boldsymbol{M} = \begin{bmatrix} 6 & 1 & 0 & 1 \\ 5 & 3 & 0 & 0 \\ 8 & 0 & 2 & 0 \\ 3 & 2 & 0 & 2 \\ 6 & 1 & 0 & 2 \end{bmatrix} \qquad (\boldsymbol{M} \mod 2) = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \qquad \boldsymbol{u} = (0,1,1,1,1)$$

On calcule $\boldsymbol{u} \cdot \boldsymbol{M} = (22,6,2,4)$, donc on va construire

1. b une racine carrée de $Q(x_2)Q(x_3)Q(x_4)Q(x_5) = p_1^{22}\, p_2^6\, p_3^2\, p_4^4$, c'est-à-dire

$$b = p_1^{11}\, p_2^3\, p_3\, p_4^2 \equiv 369672 \mod N$$

2. a le produit des $x_i + \lceil \sqrt{N} \rceil$ correspondant, donc

$$a = (x_2 + \lceil \sqrt{N} \rceil)(x_3 + \lceil \sqrt{N} \rceil)(x_4 + \lceil \sqrt{N} \rceil)(x_5 + \lceil \sqrt{N} \rceil) \equiv 102784 \mod N$$

Étape III : exemple

x_i	6	8	24	106	120
$Q(x_i)$	8512	10976	30976	141512	161728

$$\boldsymbol{M} = \begin{bmatrix} 6 & 1 & 0 & 1 \\ 5 & 3 & 0 & 0 \\ 8 & 0 & 2 & 0 \\ 3 & 2 & 0 & 2 \\ 6 & 1 & 0 & 2 \end{bmatrix} \qquad (\boldsymbol{M} \mod 2) = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \qquad \boldsymbol{u} = (0,1,1,1,1)$$

On calcule $\boldsymbol{u} \cdot \boldsymbol{M} = (22,6,2,4)$, donc on va construire

1. b une racine carrée de $Q(x_2)Q(x_3)Q(x_4)Q(x_5) = p_1^{22}\, p_2^6\, p_3^2\, p_4^4$, c'est-à-dire

$$b = p_1^{11}\, p_2^3\, p_3\, p_4^2 \equiv 369672 \mod N$$

2. a le produit des $x_i + \lceil \sqrt{N} \rceil$ correspondant, donc

$$a = (x_2 + \lceil \sqrt{N} \rceil)(x_3 + \lceil \sqrt{N} \rceil)(x_4 + \lceil \sqrt{N} \rceil)(x_5 + \lceil \sqrt{N} \rceil) \equiv 102784 \mod N$$

Puis on a (finalement) :

$$\mathrm{pgcd}(a-b, N) = 457 \quad \text{et} \quad \mathrm{pgcd}(a+b, N) = 809\,.$$

Étape II : effritement (méthode naïve)

Deuxième étape : **effritement**, ou phase de collection

But : pour $t \geq s$, trouver t éléments de la forme $Q(x)$ qui se décomposent dans la base de facteurs $\mathcal{P} = \{p_1, \ldots, p_s\}$

Étape II : effritement (méthode naïve)

Deuxième étape : **effritement**, ou phase de collection

But : pour $t \geq s$, trouver t éléments de la forme $Q(x)$ qui se décomposent dans la base de facteurs $\mathcal{P} = \{p_1, \ldots, p_s\}$

Une première idée est de chercher ces éléments de manière itérative (x croissant de 1 en 1).

Étape II : effritement (méthode naïve)

Deuxième étape : **effritement**, ou phase de collection

But : pour $t \geq s$, trouver t éléments de la forme $Q(x)$ qui se décomposent dans la base de facteurs $\mathcal{P} = \{p_1, \ldots, p_s\}$

Une première idée est de chercher ces éléments de manière itérative (x croissant de 1 en 1).

COLLECTION D'ÉLEMENTS FRIABLES (MÉTHODE NAÏVE)

1. $i \leftarrow 0, \quad x = 0, \quad r = \lceil \sqrt{N} \rceil, \quad q = r^2 - N$
2. `liste_elements` $= []$
3. $\boldsymbol{M} = []$
4. **Tant que** $i < t$:
   - 4.1 **Si** q se décompose sur $\mathcal{P}$ comme $q = p_1^{e_1} \ldots p_s^{e_s}$
     - Ajouter le vecteur $(e_1, \ldots, e_s)$ comme dernière ligne de $\boldsymbol{M}$
     - Ajouter (x, q) à `liste_elements`
     - $i \leftarrow i + 1$
   - 4.2 $q \leftarrow q + 2(x + r) + 1$
   - 4.3 $x \leftarrow x + 1$
5. **Retourner** $\boldsymbol{M}$ et `liste_elements`

Exemple

$N = 369713$ et $\mathcal{P} = \{2, 7, 11, 19\}$.

x	$Q(x)$	$(e_1, \ldots, e_4)$	reste
0	1168	$[4,0,0,0]$	73
1	2387	$[0,1,1,0]$	31
2	3608	$[3,0,1,0]$	41
3	4831	$[0,0,0,0]$	4831
4	6056	$[3,0,0,0]$	757
5	7283	$[0,0,0,0]$	7283
6	**8512**	$[6,1,0,1]$	**1**
7	9743	$[0,0,0,0]$	9743
8	**10976**	$[5,3,0,0]$	**1**
9	12211	$[0,0,0,0]$	12211
⋮	⋮	⋮	⋮
23	29711	$[0,0,1,0]$	2701
24	**30976**	$[8,0,2,0]$	**1**
25	32243	$[0,0,0,1]$	1697
⋮	⋮	⋮	⋮
106	**141512**	$[3,2,0,2]$	**1**
⋮	⋮	⋮	⋮
120	**161728**	$[6,1,0,2]$	**1**

Exemple

$N = 369713$ et $\mathcal{P} = \{2, 7, 11, 19\}$.

x	$Q(x)$	$(e_1, \ldots, e_4)$	reste
0	1168	$[4,0,0,0]$	73
1	2387	$[0,1,1,0]$	31
2	3608	$[3,0,1,0]$	41
3	4831	$[0,0,0,0]$	4831
4	6056	$[3,0,0,0]$	757
5	7283	$[0,0,0,0]$	7283
6	**8512**	$[\mathbf{6,1,0,1}]$	**1**
7	9743	$[0,0,0,0]$	9743
8	**10976**	$[\mathbf{5,3,0,0}]$	**1**
9	12211	$[0,0,0,0]$	12211
⋮	⋮	⋮	⋮
23	29711	$[0,0,1,0]$	2701
24	**30976**	$[\mathbf{8,0,2,0}]$	**1**
25	32243	$[0,0,0,1]$	1697
⋮	⋮	⋮	⋮
106	**141512**	$[\mathbf{3,2,0,2}]$	**1**
⋮	⋮	⋮	⋮
120	**161728**	$[\mathbf{6,1,0,2}]$	**1**

On obtient la liste

$$\{(6, 8512), (8, 10976), (24, 30976), (106, 141512), (120, 161728)\}$$

Exemple

$N = 369713$ et $\mathcal{P} = \{2, 7, 11, 19\}$.

x	$Q(x)$	$(e_1, \ldots, e_4)$	reste
0	1168	$[4,0,0,0]$	73
1	2387	$[0,1,1,0]$	31
2	3608	$[3,0,1,0]$	41
3	4831	$[0,0,0,0]$	4831
4	6056	$[3,0,0,0]$	757
5	7283	$[0,0,0,0]$	7283
6	**8512**	$[6,1,0,1]$	**1**
7	9743	$[0,0,0,0]$	9743
8	**10976**	$[5,3,0,0]$	**1**
9	12211	$[0,0,0,0]$	12211
⋮	⋮	⋮	⋮
23	29711	$[0,0,1,0]$	2701
24	**30976**	$[8,0,2,0]$	**1**
25	32243	$[0,0,0,1]$	1697
⋮	⋮	⋮	⋮
106	**141512**	$[3,2,0,2]$	**1**
⋮	⋮	⋮	⋮
120	**161728**	$[6,1,0,2]$	**1**

On obtient la liste

$$\{(6, 8512), (8, 10976), (24, 30976), (106, 141512), (120, 161728)\}$$

Cela donne la matrice

$$\boldsymbol{M} = \begin{bmatrix} 6 & 1 & 0 & 1 \\ 5 & 3 & 0 & 0 \\ 8 & 0 & 2 & 0 \\ 3 & 2 & 0 & 2 \\ 6 & 1 & 0 & 2 \end{bmatrix}$$

Exemple

$N = 369713$ et $\mathcal{P} = \{2, 7, 11, 19\}$.

x	$Q(x)$	$(e_1, \ldots, e_4)$	reste
0	1168	$[4,0,0,0]$	73
1	2387	$[0,1,1,0]$	31
2	3608	$[3,0,1,0]$	41
3	4831	$[0,0,0,0]$	4831
4	6056	$[3,0,0,0]$	757
5	7283	$[0,0,0,0]$	7283
6	**8512**	$[6,1,0,1]$	**1**
7	9743	$[0,0,0,0]$	9743
8	**10976**	$[5,3,0,0]$	**1**
9	12211	$[0,0,0,0]$	12211
⋮	⋮	⋮	⋮
23	29711	$[0,0,1,0]$	2701
24	**30976**	$[8,0,2,0]$	**1**
25	32243	$[0,0,0,1]$	1697
⋮	⋮	⋮	⋮
106	**141512**	$[3,2,0,2]$	**1**
⋮	⋮	⋮	⋮
120	**161728**	$[6,1,0,2]$	**1**

On obtient la liste

$$\{(6, 8512), (8, 10976), (24, 30976), (106, 141512), (120, 161728)\}$$

Cela donne la matrice

$$\boldsymbol{M} = \begin{bmatrix} 6 & 1 & 0 & 1 \\ 5 & 3 & 0 & 0 \\ 8 & 0 & 2 & 0 \\ 3 & 2 & 0 & 2 \\ 6 & 1 & 0 & 2 \end{bmatrix}$$

Problème. Pour chaque ligne calculée, on fait beaucoup de tests de divisibilité qui échouent. Autrement dit, il y a **beaucoup** de zéros dans les $(e_1, \ldots, e_s)$ calculés.

Étape II : effritement (méthode de criblage)

Idée : pour être plus efficace, on va collecter ces éléments par une méthode de **crible**.

Étape II : effritement (méthode de criblage)

Idée : pour être plus efficace, on va collecter ces éléments par une méthode de **crible**.

Remarque. La notion de crible a déjà été vue pour établir une liste de nombres premiers : c'est le **crible d'Eratostène**.

Étape II : effritement (méthode de criblage)

Idée : pour être plus efficace, on va collecter ces éléments par une méthode de **crible**.

Remarque. La notion de crible a déjà été vue pour établir une liste de nombres premiers : c'est le **crible d'Eratostène**.

Pour $A \geq s$ un entier dépendant de B qu'on déterminera plus tard :

MÉTHODE DE CRIBLE QUADRATIQUE (VERSION PÉDAGOGIQUE)

1. On initialise un tableau $T = [Q(0), Q(1), \ldots, Q(A)]$
2. Pour chaque premier $p \in \mathcal{P}$:
   - 2.1 $e = 1$
   - 2.2 Tant que $p^e \leq A$:
     - On cherche tous les $0 \leq y < p^e$ tels que p^e divise $T[y]$
     - On divise par p tous les $T[x]$ où x est de la forme $y + kp^e$ (criblage)
     - On incrémente $e \leftarrow e + 1$
3. **Retourner** tous les $(x, Q(x))$ tels que $T[x] = 1$.

Étape II : effritement (méthode de criblage)

Idée : pour être plus efficace, on va collecter ces éléments par une méthode de **crible**.

Remarque. La notion de crible a déjà été vue pour établir une liste de nombres premiers : c'est le **crible d'Eratostène**.

Pour $A \geq s$ un entier dépendant de B qu'on déterminera plus tard :

MÉTHODE DE CRIBLE QUADRATIQUE (VERSION PÉDAGOGIQUE)

1. On initialise un tableau $T = [Q(0), Q(1), \ldots, Q(A)]$
2. Pour chaque premier $p \in \mathcal{P}$:
   - 2.1 $e = 1$
   - 2.2 Tant que $p^e \leq A$:
     - On cherche tous les $0 \leq y < p^e$ tels que p^e divise $T[y]$
     - On divise par p tous les $T[x]$ où x est de la forme $y + kp^e$ (criblage)
     - On incrémente $e \leftarrow e + 1$
3. **Retourner** tous les $(x, Q(x))$ tels que $T[x] = 1$.

Remarques :

- la recherche de solution de $Q(y) \equiv N \mod p$ est essentiellement une recherche de racine carrée ($\rightarrow$ Tonelli-Shanks, ou Cipolla)
- on peut déduire très efficacement les solutions modulo p^e des solutions modulo p^{e-1} (relèvement de Hensel).

Exemple de crible

Pour $N = 73217 = 211 \times 347$ (nouveau N) avec la base de facteurs $\mathcal{P} = \{2, 7, 11, 13\}$.

Exemple de crible

Pour $N = 73217 = 211 \times 347$ (nouveau N) avec la base de facteurs $\mathcal{P} = \{2, 7, 11, 13\}$.

Les étapes successives de l'algorithme sont :

p	e	solutions	T_0	T_1	T_2	T_3	T_4	T_5	T_6	T_7	T_8	T_9	T_{10}	T_{11}	T_{12}	T_{13}	T_{14}	T_{15}

Exemple de crible

Pour $N = 73217 = 211 \times 347$ (nouveau N) avec la base de facteurs $\mathcal{P} = \{2, 7, 11, 13\}$.

Les étapes successives de l'algorithme sont :

p	e	solutions	T_0	T_1	T_2	T_3	T_4	T_5	T_6	T_7	T_8	T_9	T_{10}	T_{11}	T_{12}	T_{13}	T_{14}	T_{15}
			224	767	1312	1859	2408	2959	3512	4067	4624	5183	5744	6307	6872	7439	8008	8579

Exemple de crible

Pour $N = 73217 = 211 \times 347$ (nouveau N) avec la base de facteurs $\mathcal{P} = \{2, 7, 11, 13\}$.

Les étapes successives de l'algorithme sont :

p	e	solutions	T_0	T_1	T_2	T_3	T_4	T_5	T_6	T_7	T_8	T_9	T_{10}	T_{11}	T_{12}	T_{13}	T_{14}	T_{15}
			224	767	1312	1859	2408	2959	3512	4067	4624	5183	5744	6307	6872	7439	8008	8579
2	1	[0]	112	767	656	1859	1204	2959	1756	4067	2312	5183	2872	6307	3436	7439	4004	8579

Exemple de crible

Pour $N = 73217 = 211 \times 347$ (nouveau N) avec la base de facteurs $\mathcal{P} = \{2, 7, 11, 13\}$.

Les étapes successives de l'algorithme sont :

p	e	solutions	T_0	T_1	T_2	T_3	T_4	T_5	T_6	T_7	T_8	T_9	T_{10}	T_{11}	T_{12}	T_{13}	T_{14}	T_{15}
			224	767	1312	1859	2408	2959	3512	4067	4624	5183	5744	6307	6872	7439	8008	8579
2	1	[0]	112	767	656	1859	1204	2959	1756	4067	2312	5183	2872	6307	3436	7439	4004	8579
	2	[2, 0]	56	767	328	1859	602	2959	878	4067	1156	5183	1436	6307	1718	7439	2002	8579

Exemple de crible

Pour $N = 73217 = 211 \times 347$ (nouveau N) avec la base de facteurs $\mathcal{P} = \{2, 7, 11, 13\}$.

Les étapes successives de l'algorithme sont :

p	e	solutions	T_0	T_1	T_2	T_3	T_4	T_5	T_6	T_7	T_8	T_9	T_{10}	T_{11}	T_{12}	T_{13}	T_{14}	T_{15}
			224	767	1312	1859	2408	2959	3512	4067	4624	5183	5744	6307	6872	7439	8008	8579
2	1	$[0]$	112	767	656	1859	1204	2959	1756	4067	2312	5183	2872	6307	3436	7439	4004	8579
	2	$[2, 0]$	56	767	328	1859	602	2959	878	4067	1156	5183	1436	6307	1718	7439	2002	8579
	3	$[2, 4, 6, 0]$	28	767	164	1859	301	2959	439	4067	578	5183	718	6307	859	7439	1001	8579

Exemple de crible

Pour $N = 73217 = 211 \times 347$ (nouveau N) avec la base de facteurs $\mathcal{P} = \{2, 7, 11, 13\}$.

Les étapes successives de l'algorithme sont :

p	e	solutions	T_0	T_1	T_2	T_3	T_4	T_5	T_6	T_7	T_8	T_9	T_{10}	T_{11}	T_{12}	T_{13}	T_{14}	T_{15}
			224	767	1312	1859	2408	2959	3512	4067	4624	5183	5744	6307	6872	7439	8008	8579
2	1	$[0]$	112	767	656	1859	1204	2959	1756	4067	2312	5183	2872	6307	3436	7439	4004	8579
	2	$[2, 0]$	56	767	328	1859	602	2959	878	4067	1156	5183	1436	6307	1718	7439	2002	8579
	3	$[2, 4, 6, 0]$	28	767	164	1859	301	2959	439	4067	578	5183	718	6307	859	7439	1001	8579
	4	$[2, 8, 10, 0]$	14	767	82	1859	301	2959	439	4067	289	5183	359	6307	859	7439	1001	8579

Exemple de crible

Pour $N = 73217 = 211 \times 347$ (nouveau N) avec la base de facteurs $\mathcal{P} = \{2, 7, 11, 13\}$.

Les étapes successives de l'algorithme sont :

p	e	solutions	T_0	T_1	T_2	T_3	T_4	T_5	T_6	T_7	T_8	T_9	T_{10}	T_{11}	T_{12}	T_{13}	T_{14}	T_{15}
			224	767	1312	1859	2408	2959	3512	4067	4624	5183	5744	6307	6872	7439	8008	8579
2	1	$[0]$	112	767	656	1859	1204	2959	1756	4067	2312	5183	2872	6307	3436	7439	4004	8579
	2	$[2, 0]$	56	767	328	1859	602	2959	878	4067	1156	5183	1436	6307	1718	7439	2002	8579
	3	$[2, 4, 6, 0]$	28	767	164	1859	301	2959	439	4067	578	5183	718	6307	859	7439	1001	8579
	4	$[2, 8, 10, 0]$	14	767	82	1859	301	2959	439	4067	289	5183	359	6307	859	7439	1001	8579
	5	$[0, 2]$	7	767	41	1859	301	2959	439	4067	289	5183	359	6307	859	7439	1001	8579

Exemple de crible

Pour $N = 73217 = 211 \times 347$ (nouveau N) avec la base de facteurs $\mathcal{P} = \{2, 7, 11, 13\}$.

Les étapes successives de l'algorithme sont :

p	e	solutions	T_0	T_1	T_2	T_3	T_4	T_5	T_6	T_7	T_8	T_9	T_{10}	T_{11}	T_{12}	T_{13}	T_{14}	T_{15}
			224	767	1312	1859	2408	2959	3512	4067	4624	5183	5744	6307	6872	7439	8008	8579
2	1	$[0]$	112	767	656	1859	1204	2959	1756	4067	2312	5183	2872	6307	3436	7439	4004	8579
	2	$[2, 0]$	56	767	328	1859	602	2959	878	4067	1156	5183	1436	6307	1718	7439	2002	8579
	3	$[2, 4, 6, 0]$	28	767	164	1859	301	2959	439	4067	578	5183	718	6307	859	7439	1001	8579
	4	$[2, 8, 10, 0]$	14	767	82	1859	301	2959	439	4067	289	5183	359	6307	859	7439	1001	8579
	5	$[0, 2]$	7	767	41	1859	301	2959	439	4067	289	5183	359	6307	859	7439	1001	8579
7	1	$[4, 0]$	1	767	41	1859	43	2959	439	581	289	5183	359	901	859	7439	143	8579

Exemple de crible

Pour $N = 73217 = 211 \times 347$ (nouveau N) avec la base de facteurs $\mathcal{P} = \{2, 7, 11, 13\}$.

Les étapes successives de l'algorithme sont :

p	e	solutions	T_0	T_1	T_2	T_3	T_4	T_5	T_6	T_7	T_8	T_9	T_{10}	T_{11}	T_{12}	T_{13}	T_{14}	T_{15}
			224	767	1312	1859	2408	2959	3512	4067	4624	5183	5744	6307	6872	7439	8008	8579
2	1	$[0]$	112	767	656	1859	1204	2959	1756	4067	2312	5183	2872	6307	3436	7439	4004	8579
	2	$[2, 0]$	56	767	328	1859	602	2959	878	4067	1156	5183	1436	6307	1718	7439	2002	8579
	3	$[2, 4, 6, 0]$	28	767	164	1859	301	2959	439	4067	578	5183	718	6307	859	7439	1001	8579
	4	$[2, 8, 10, 0]$	14	767	82	1859	301	2959	439	4067	289	5183	359	6307	859	7439	1001	8579
	5	$[0, 2]$	7	767	41	1859	301	2959	439	4067	289	5183	359	6307	859	7439	1001	8579
7	1	$[4, 0]$	1	767	41	1859	43	2959	439	581	289	5183	359	901	859	7439	143	8579
	2	$[7]$	1	767	41	1859	43	2959	439	83	289	5183	359	901	859	7439	143	8579

Exemple de crible

Pour $N = 73217 = 211 \times 347$ (nouveau N) avec la base de facteurs $\mathcal{P} = \{2, 7, 11, 13\}$.

Les étapes successives de l'algorithme sont :

p	e	solutions	T_0	T_1	T_2	T_3	T_4	T_5	T_6	T_7	T_8	T_9	T_{10}	T_{11}	T_{12}	T_{13}	T_{14}	T_{15}
			224	767	1312	1859	2408	2959	3512	4067	4624	5183	5744	6307	6872	7439	8008	8579
2	1	$[0]$	112	767	656	1859	1204	2959	1756	4067	2312	5183	2872	6307	3436	7439	4004	8579
	2	$[2, 0]$	56	767	328	1859	602	2959	878	4067	1156	5183	1436	6307	1718	7439	2002	8579
	3	$[2, 4, 6, 0]$	28	767	164	1859	301	2959	439	4067	578	5183	718	6307	859	7439	1001	8579
	4	$[2, 8, 10, 0]$	14	767	82	1859	301	2959	439	4067	289	5183	359	6307	859	7439	1001	8579
	5	$[0, 2]$	7	767	41	1859	301	2959	439	4067	289	5183	359	6307	859	7439	1001	8579
7	1	$[4, 0]$	1	767	41	1859	43	2959	439	581	289	5183	359	901	859	7439	143	8579
	2	$[7]$	1	767	41	1859	43	2959	439	83	289	5183	359	901	859	7439	143	8579
11	1	$[5, 3]$	1	767	41	169	43	269	439	83	289	5183	359	901	859	7439	13	8579

Exemple de crible

Pour $N = 73217 = 211 \times 347$ (nouveau N) avec la base de facteurs $\mathcal{P} = \{2, 7, 11, 13\}$.

Les étapes successives de l'algorithme sont :

p	e	solutions	T_0	T_1	T_2	T_3	T_4	T_5	T_6	T_7	T_8	T_9	T_{10}	T_{11}	T_{12}	T_{13}	T_{14}	T_{15}
			224	767	1312	1859	2408	2959	3512	4067	4624	5183	5744	6307	6872	7439	8008	8579
2	1	$[0]$	112	767	656	1859	1204	2959	1756	4067	2312	5183	2872	6307	3436	7439	4004	8579
	2	$[2, 0]$	56	767	328	1859	602	2959	878	4067	1156	5183	1436	6307	1718	7439	2002	8579
	3	$[2, 4, 6, 0]$	28	767	164	1859	301	2959	439	4067	578	5183	718	6307	859	7439	1001	8579
	4	$[2, 8, 10, 0]$	14	767	82	1859	301	2959	439	4067	289	5183	359	6307	859	7439	1001	8579
	5	$[0, 2]$	7	767	41	1859	301	2959	439	4067	289	5183	359	6307	859	7439	1001	8579
7	1	$[4, 0]$	1	767	41	1859	43	2959	439	581	289	5183	359	901	859	7439	143	8579
	2	$[7]$	1	767	41	1859	43	2959	439	83	289	5183	359	901	859	7439	143	8579
11	1	$[5, 3]$	1	767	41	169	43	269	439	83	289	5183	359	901	859	7439	13	8579
13	1	$[3, 1]$	1	59	41	13	43	269	439	83	289	5183	359	901	859	7439	1	8579

Exemple de crible

Pour $N = 73217 = 211 \times 347$ (nouveau N) avec la base de facteurs $\mathcal{P} = \{2, 7, 11, 13\}$.

Les étapes successives de l'algorithme sont :

p	e	solutions	T_0	T_1	T_2	T_3	T_4	T_5	T_6	T_7	T_8	T_9	T_{10}	T_{11}	T_{12}	T_{13}	T_{14}	T_{15}
			224	767	1312	1859	2408	2959	3512	4067	4624	5183	5744	6307	6872	7439	8008	8579
2	1	[0]	112	767	656	1859	1204	2959	1756	4067	2312	5183	2872	6307	3436	7439	4004	8579
	2	[2, 0]	56	767	328	1859	602	2959	878	4067	1156	5183	1436	6307	1718	7439	2002	8579
	3	[2, 4, 6, 0]	28	767	164	1859	301	2959	439	4067	578	5183	718	6307	859	7439	1001	8579
	4	[2, 8, 10, 0]	14	767	82	1859	301	2959	439	4067	289	5183	359	6307	859	7439	1001	8579
	5	[0, 2]	7	767	41	1859	301	2959	439	4067	289	5183	359	6307	859	7439	1001	8579
7	1	[4, 0]	1	767	41	1859	43	2959	439	581	289	5183	359	901	859	7439	143	8579
	2	[7]	1	767	41	1859	43	2959	439	83	289	5183	359	901	859	7439	143	8579
11	1	[5, 3]	1	767	41	169	43	269	439	83	289	5183	359	901	859	7439	13	8579
13	1	[3, 1]	1	59	41	13	43	269	439	83	289	5183	359	901	859	7439	1	8579
	2	[3]	1	59	41	1	43	269	439	83	289	5183	359	901	859	7439	1	8579

Exemple de crible

Pour $N = 73217 = 211 \times 347$ (nouveau N) avec la base de facteurs $\mathcal{P} = \{2, 7, 11, 13\}$.

Les étapes successives de l'algorithme sont :

p	e	solutions	T_0	T_1	T_2	T_3	T_4	T_5	T_6	T_7	T_8	T_9	T_{10}	T_{11}	T_{12}	T_{13}	T_{14}	T_{15}
			224	767	1312	1859	2408	2959	3512	4067	4624	5183	5744	6307	6872	7439	8008	8579
2	1	[0]	112	767	656	1859	1204	2959	1756	4067	2312	5183	2872	6307	3436	7439	4004	8579
	2	[2, 0]	56	767	328	1859	602	2959	878	4067	1156	5183	1436	6307	1718	7439	2002	8579
	3	[2, 4, 6, 0]	28	767	164	1859	301	2959	439	4067	578	5183	718	6307	859	7439	1001	8579
	4	[2, 8, 10, 0]	14	767	82	1859	301	2959	439	4067	289	5183	359	6307	859	7439	1001	8579
	5	[0, 2]	7	767	41	1859	301	2959	439	4067	289	5183	359	6307	859	7439	1001	8579
7	1	[4, 0]	1	767	41	1859	43	2959	439	581	289	5183	359	901	859	7439	143	8579
	2	[7]	1	767	41	1859	43	2959	439	83	289	5183	359	901	859	7439	143	8579
11	1	[5, 3]	1	767	41	169	43	269	439	83	289	5183	359	901	859	7439	13	8579
13	1	[3, 1]	1	59	41	13	43	269	439	83	289	5183	359	901	859	7439	1	8579
	2	[3]	1	59	41	1	43	269	439	83	289	5183	359	901	859	7439	1	8579

Et on obtient la liste $\{(0, 224), (3, 1859), (14, 8008)\}$

Exemple de crible

Pour $N = 73217 = 211 \times 347$ (nouveau N) avec la base de facteurs $\mathcal{P} = \{2, 7, 11, 13\}$.

Les étapes successives de l'algorithme sont :

p	e	solutions	T_0	T_1	T_2	T_3	T_4	T_5	T_6	T_7	T_8	T_9	T_{10}	T_{11}	T_{12}	T_{13}	T_{14}	T_{15}
			224	767	1312	1859	2408	2959	3512	4067	4624	5183	5744	6307	6872	7439	8008	8579
2	1	[0]	112	767	656	1859	1204	2959	1756	4067	2312	5183	2872	6307	3436	7439	4004	8579
	2	[2, 0]	56	767	328	1859	602	2959	878	4067	1156	5183	1436	6307	1718	7439	2002	8579
	3	[2, 4, 6, 0]	28	767	164	1859	301	2959	439	4067	578	5183	718	6307	859	7439	1001	8579
	4	[2, 8, 10, 0]	14	767	82	1859	301	2959	439	4067	289	5183	359	6307	859	7439	1001	8579
	5	[0, 2]	7	767	41	1859	301	2959	439	4067	289	5183	359	6307	859	7439	1001	8579
7	1	[4, 0]	1	767	41	1859	43	2959	439	581	289	5183	359	901	859	7439	143	8579
	2	[7]	1	767	41	1859	43	2959	439	83	289	5183	359	901	859	7439	143	8579
11	1	[5, 3]	1	767	41	169	43	269	439	83	289	5183	359	901	859	7439	13	8579
13	1	[3, 1]	1	59	41	13	43	269	439	83	289	5183	359	901	859	7439	1	8579
	2	[3]	1	59	41	1	43	269	439	83	289	5183	359	901	859	7439	1	8579

Et on obtient la liste $\{(0, 224), (3, 1859), (14, 8008)\}$

La matrice associée est

$$\boldsymbol{M} = \begin{bmatrix} 5 & 1 & 0 & 0 \\ 0 & 0 & 1 & 2 \\ 3 & 1 & 1 & 1 \end{bmatrix}$$

Améliorations

Observation 1. Les termes du tableau peuvent être initialement grands, et leur division par des premiers est légèrement coûteuse en pratique.

Améliorations

Observation 1. Les termes du tableau peuvent être initialement grands, et leur division par des premiers est légèrement coûteuse en pratique. Pour éviter cela, on peut

- remplacer les valeurs exactes $Q(x)$ par $T[x] = \lfloor \log Q(x) \rfloor$
- soustraire $\lfloor \log p \rfloor$ (précalculé) à $T[x]$ au lieu de diviser $T[x]$ par p
- en fin d'algorithme, plutôt que de tester si $T[x] = 1$, on vérifie si $|T[x]| \leq \log B^2$

Améliorations

Observation 1. Les termes du tableau peuvent être initialement grands, et leur division par des premiers est légèrement coûteuse en pratique. Pour éviter cela, on peut

- remplacer les valeurs exactes $Q(x)$ par $T[x] = \lfloor \log Q(x) \rfloor$
- soustraire $\lfloor \log p \rfloor$ (précalculé) à $T[x]$ au lieu de diviser $T[x]$ par p
- en fin d'algorithme, plutôt que de tester si $T[x] = 1$, on vérifie si $|T[x]| \leq \log B^2$

Observation 2. Si A est grand, il devient peu probable que $Q(x)$ soit B-friable lorsque x s'approche de A.

Améliorations

Observation 1. Les termes du tableau peuvent être initialement grands, et leur division par des premiers est légèrement coûteuse en pratique. Pour éviter cela, on peut

- remplacer les valeurs exactes $Q(x)$ par $T[x] = \lfloor \log Q(x) \rfloor$
- soustraire $\lfloor \log p \rfloor$ (précalculé) à $T[x]$ au lieu de diviser $T[x]$ par p
- en fin d'algorithme, plutôt que de tester si $T[x] = 1$, on vérifie si $|T[x]| \leq \log B^2$

Observation 2. Si A est grand, il devient peu probable que $Q(x)$ soit B-friable lorsque x s'approche de A.

Idée : on remplace $Q(x)$ par des $Q_{u,v}(x) = Q(ux + v)$ où u et v sont choisis de telle sorte que $Q_{u,v}(x)$ donne des nombres « petits » modulo N, lorsque $x \in [0, A]$.

C'est la variante dite « à **polynômes multiples** » ;

- cela permet de réduire sensiblement la taille de A,
- on peut choisir avantageusement u et v pour produire beaucoup de relations.

Résumé de l'algorithme

FACTORISATION PAR CRIBLE QUADRATIQUE (PÉDAGOGIQUE)

Entrée : N un entier à factoriser
Sortie : un facteur propre de N

1. **Initialisation** : calculer $B \simeq 2^{0.5\sqrt{\log N \log\log N}}$ (on verra pourquoi)
2. Calculer la **base de facteurs** $\mathcal{P} = \{p_1, \ldots, p_s\}$ tels que $p_j \leq B$ et $\left(\frac{N}{p_j}\right) = 1$.
3. **Effritement** :
   - 3.1 Calculer la matrice $\boldsymbol{M}$ et les éléments $\{(x, Q(x))\}$ associés par criblage.
   - 3.2 Si $\boldsymbol{M}$ a un noyau à gauche nul, revenir à 2. avec $B \leftarrow 2B$.
4. **Algèbre linéaire** :
   - 4.1 Calculer une solution aléatoire $\boldsymbol{u}$ de $\boldsymbol{u} \cdot (\boldsymbol{M} \bmod 2) = \boldsymbol{0}$
   - 4.2 Calculer $a = \prod_{j \in J}(x_j + \lceil\sqrt{N}\rceil)$ et $b = \prod_{j \in J} Q(x_j)$ où $J = \{j, u_j \neq 0\}$.
5. **Si** $\{\mathrm{pgcd}(a-b, N), \mathrm{pgcd}(a+b, N)\}$ ne contient pas de facteur propre de N, revenir à l'étape 4.1.
6. **Sinon,** retourner les facteurs propres obtenus.

Qu'en est-il de la **complexité** de l'algorithme ?

Complexité du crible quadratique

D'abord, **quelques résultats de théorie des nombres.**

Complexité du crible quadratique

D'abord, **quelques résultats de théorie des nombres.**

Soit M un entier ≥ 2.

Théorème de Tchebychev. Le nombre $\pi(M)$ de nombres premiers compris entre 2 et M vérifie

$$\alpha \frac{M}{\log M} \leq \pi(M) \leq \beta \frac{M}{\log M} .$$

Complexité du crible quadratique

D'abord, **quelques résultats de théorie des nombres.**

Soit M un entier ≥ 2.

Théorème de Tchebychev. Le nombre $\pi(M)$ de nombres premiers compris entre 2 et M vérifie

$$\alpha \frac{M}{\log M} \leq \pi(M) \leq \beta \frac{M}{\log M}\,.$$

Remarque. Les théorèmes de Hadamard et de de la Vallée-Poussin assurent $\pi(M) \sim \frac{M}{\ln M}$.

Complexité du crible quadratique

D'abord, **quelques résultats de théorie des nombres.**

Soit M un entier ≥ 2.

Théorème de Tchebychev. Le nombre $\pi(M)$ de nombres premiers compris entre 2 et M vérifie

$$\alpha \frac{M}{\log M} \leq \pi(M) \leq \beta \frac{M}{\log M}\,.$$

Remarque. Les théorèmes de Hadamard et de de la Vallée-Poussin assurent $\pi(M) \sim \frac{M}{\ln M}$.

On définit la **fonction de de Bruijn** $\psi(M, B)$ comme le nombre d'entiers $\leq M$ qui sont B-friables.

Complexité du crible quadratique

D'abord, **quelques résultats de théorie des nombres.**

Soit M un entier ≥ 2.

Théorème de Tchebychev. Le nombre $\pi(M)$ de nombres premiers compris entre 2 et M vérifie

$$\alpha \frac{M}{\log M} \leq \pi(M) \leq \beta \frac{M}{\log M}\,.$$

Remarque. Les théorèmes de Hadamard et de de la Vallée-Poussin assurent $\pi(M) \sim \frac{M}{\ln M}$.

On définit la **fonction de de Bruijn** $\psi(M,B)$ comme le nombre d'entiers $\leq M$ qui sont B-friables.

Proposition. Si $\log M \ll B \ll M$, alors $\psi(M,B)$ vérifie

$$\frac{\psi(M,B)}{M} \sim \left(\frac{\log M}{\log B}\right)^{-(\log M)/(\log B)}.$$

Complexité du crible quadratique

Étape 1 : base de facteurs

- Il y a $\pi(B)$ premiers pour lequels on doit tester la résiduosité quadratique de N
  $\rightarrow$ complexité en $O(B \log B \log N)$
  $\rightarrow$ on a donc $s \simeq \pi(B)/2$ premiers dans $\mathcal{P}$

Complexité du crible quadratique

Étape 1 : base de facteurs

- Il y a $\pi(B)$ premiers pour lequels on doit tester la résiduosité quadratique de N
  $\rightarrow$ complexité en $O(B \log B \log N)$
  $\rightarrow$ on a donc $s \simeq \pi(B)/2$ premiers dans $\mathcal{P}$

Étape 2 : effritement par crible. Soit M la taille maximale d'un entier $Q(x)$ à traiter.

- Alors, il faudra traiter $s \cdot \frac{M}{\psi(M,B)}$ entiers en moyenne

Complexité du crible quadratique

Étape 1 : base de facteurs

- Il y a $\pi(B)$ premiers pour lequels on doit tester la résiduosité quadratique de N
  $\rightarrow$ complexité en $O(B \log B \log N)$
  $\rightarrow$ on a donc $s \simeq \pi(B)/2$ premiers dans $\mathcal{P}$

Étape 2 : effritement par crible. Soit M la taille maximale d'un entier $Q(x)$ à traiter.

- Alors, il faudra traiter $s \cdot \frac{M}{\psi(M,B)}$ entiers en moyenne
- On peut montrer que pour chaque entier du tableau, on fait $O(\log \log B)$ opérations

Complexité du crible quadratique

Étape 1 : base de facteurs

- Il y a $\pi(B)$ premiers pour lequels on doit tester la résiduosité quadratique de N
  $\rightarrow$ complexité en $O(B \log B \log N)$
  $\rightarrow$ on a donc $s \simeq \pi(B)/2$ premiers dans $\mathcal{P}$

Étape 2 : effritement par crible. Soit M la taille maximale d'un entier $Q(x)$ à traiter.

- Alors, il faudra traiter $s \cdot \frac{M}{\psi(M,B)}$ entiers en moyenne
- On peut montrer que pour chaque entier du tableau, on fait $O(\log\log B)$ opérations
- La complexité est donc $C_2 = O(s \log\log B \cdot \frac{M}{\psi(M,B)}) = O(B \frac{\log\log B}{\log B} u^u)$ où $u = \frac{\log M}{\log B}$

Complexité du crible quadratique

Étape 1 : base de facteurs

- Il y a $\pi(B)$ premiers pour lequels on doit tester la résiduosité quadratique de N
  $\rightarrow$ complexité en $O(B \log B \log N)$
  $\rightarrow$ on a donc $s \simeq \pi(B)/2$ premiers dans $\mathcal{P}$

Étape 2 : effritement par crible. Soit M la taille maximale d'un entier $Q(x)$ à traiter.

- Alors, il faudra traiter $s \cdot \frac{M}{\psi(M,B)}$ entiers en moyenne
- On peut montrer que pour chaque entier du tableau, on fait $O(\log\log B)$ opérations
- La complexité est donc $C_2 = O(s \log\log B \cdot \frac{M}{\psi(M,B)}) = O(B \frac{\log\log B}{\log B} u^u)$ où $u = \frac{\log M}{\log B}$
- Si $M \simeq \sqrt{N}$ et $\log B \geq \sqrt{\log N}$, alors on obtient :

$$\log C_2 \simeq \log B + \frac{\log N \log\log N}{4 \log B}$$

Complexité du crible quadratique

Étape 1 : base de facteurs

- Il y a $\pi(B)$ premiers pour lequels on doit tester la résiduosité quadratique de N
  $\rightarrow$ complexité en $O(B \log B \log N)$
  $\rightarrow$ on a donc $s \simeq \pi(B)/2$ premiers dans $\mathcal{P}$

Étape 2 : effritement par crible. Soit M la taille maximale d'un entier $Q(x)$ à traiter.

- Alors, il faudra traiter $s \cdot \frac{M}{\psi(M,B)}$ entiers en moyenne
- On peut montrer que pour chaque entier du tableau, on fait $O(\log\log B)$ opérations
- La complexité est donc $C_2 = O(s \log\log B \cdot \frac{M}{\psi(M,B)}) = O(B \frac{\log\log B}{\log B} u^u)$ où $u = \frac{\log M}{\log B}$
- Si $M \simeq \sqrt{N}$ et $\log B \geq \sqrt{\log N}$, alors on obtient :

$$\log C_2 \simeq \log B + \frac{\log N \log\log N}{4 \log B}$$

Cette dernière quantité se maximise pour $\log B \simeq \frac{1}{2}\sqrt{\log N \log\log N}$, donc $B \in L_{\log N}[\frac{1}{2}, \frac{1}{2}]$, et donne

$$C_2 = \exp(\sqrt{\log N \log\log N}) = L_{\log N}[\tfrac{1}{2}, 1]\,.$$

Complexité du crible quadratique

Étape 3 : algèbre linéaire.

- On résout un système linéaire **creux** de taille $t \times s$ sur $\mathbb{F}_2$ où $t \simeq s \in O(\frac{B}{\log B})$

Complexité du crible quadratique

Étape 3 : algèbre linéaire.

- On résout un système linéaire **creux** de taille $t \times s$ sur $\mathbb{F}_2$ où $t \simeq s \in O(\frac{B}{\log B})$
  $\rightarrow$ Par l'algorithme de Wiedemann (par exemple), on a une complexité en

$$O(ts) = O(B^2 / \log^2 B) = O(\exp(\sqrt{\log N \log\log N})) = O(L_{\log N}[\tfrac{1}{2}, 1])$$

Complexité du crible quadratique

Étape 3 : algèbre linéaire.

- On résout un système linéaire **creux** de taille $t \times s$ sur $\mathbb{F}_2$ où $t \simeq s \in O(\frac{B}{\log B})$
  $\rightarrow$ Par l'algorithme de Wiedemann (par exemple), on a une complexité en

$$O(ts) = O(B^2 / \log^2 B) = O(\exp(\sqrt{\log N \log\log N})) = O(L_{\log N}[\tfrac{1}{2}, 1])$$

- Calculs terminaux (produits, pgcd) en $O(B \log^2 N)$

Complexité du crible quadratique

Étape 3 : algèbre linéaire.

- On résout un système linéaire **creux** de taille $t \times s$ sur $\mathbb{F}_2$ où $t \simeq s \in O(\frac{B}{\log B})$
  $\rightarrow$ Par l'algorithme de Wiedemann (par exemple), on a une complexité en

$$O(ts) = O(B^2 / \log^2 B) = O(\exp(\sqrt{\log N \log\log N})) = O(L_{\log N}[\tfrac{1}{2}, 1])$$

- Calculs terminaux (produits, pgcd) en $O(B \log^2 N)$

Conclusion. L'algorithme de crible quadratique permet de factoriser un entier N en temps

$$O(\exp(\sqrt{\log N \log\log N}))\,.$$

Crible algébrique

Le **crible algébrique** généralise l'idée du crible quadratique. L'idée est de chercher des $a^2 \equiv b^2 \mod N$ en cherchant des carrés dans des **anneaux d'entiers**.

Crible algébrique

Le **crible algébrique** généralise l'idée du crible quadratique. L'idée est de chercher des $a^2 \equiv b^2 \mod N$ en cherchant des carrés dans des **anneaux d'entiers**.

Idée. Soit $f(X) \in \mathbb{Z}[X]$ unitaire et irréductible, et $m \in \mathbb{Z}$ qui satisfait $f(m) \equiv 0 \mod N$. En posant $\alpha = \overline{X} \in \mathbb{Z}[X]/(f)$, on a $\mathbb{Z}[X]/(f) = \mathbb{Z}[\alpha]$.

Crible algébrique

Le **crible algébrique** généralise l'idée du crible quadratique. L'idée est de chercher des $a^2 \equiv b^2 \mod N$ en cherchant des carrés dans des **anneaux d'entiers**.

Idée. Soit $f(X) \in \mathbb{Z}[X]$ unitaire et irréductible, et $m \in \mathbb{Z}$ qui satisfait $f(m) \equiv 0 \mod N$. En posant $\alpha = \overline{X} \in \mathbb{Z}[X]/(f)$, on a $\mathbb{Z}[X]/(f) = \mathbb{Z}[\alpha]$.

On considère ensuite le morphisme d'anneaux

$$\begin{array}{rccc} \phi & : \mathbb{Z}[\alpha] & \to & \mathbb{Z}/N\mathbb{Z} \\ & P(\alpha) & \mapsto & \overline{P}(m) \mod N \end{array}$$

Alors on cherche $P \in \mathbb{Z}[X]$ tel que $P(\alpha)$ est un carré $z^2 \in \mathbb{Z}[\alpha]$ et $\overline{P}(m)$ est un carré $b^2 \in \mathbb{Z}/N\mathbb{Z}$. Si $a = \phi(z)$, alors $a^2 \equiv b^2 \mod N$.

Ensuite, pour trouver les éléments P, on va cribler les **normes** d'éléments $u + v\alpha \in \mathbb{Z}[\alpha]$ (analogues des petits p_i pour le crible quadratique).

Crible algébrique

Le **crible algébrique** généralise l'idée du crible quadratique. L'idée est de chercher des $a^2 \equiv b^2 \mod N$ en cherchant des carrés dans des **anneaux d'entiers**.

Idée. Soit $f(X) \in \mathbb{Z}[X]$ unitaire et irréductible, et $m \in \mathbb{Z}$ qui satisfait $f(m) \equiv 0 \mod N$. En posant $\alpha = \overline{X} \in \mathbb{Z}[X]/(f)$, on a $\mathbb{Z}[X]/(f) = \mathbb{Z}[\alpha]$.

On considère ensuite le morphisme d'anneaux

$$\begin{array}{rccc} \phi & : \mathbb{Z}[\alpha] & \to & \mathbb{Z}/N\mathbb{Z} \\ & P(\alpha) & \mapsto & \overline{P}(m) \mod N \end{array}$$

Alors on cherche $P \in \mathbb{Z}[X]$ tel que $P(\alpha)$ est un carré $z^2 \in \mathbb{Z}[\alpha]$ et $\overline{P}(m)$ est un carré $b^2 \in \mathbb{Z}/N\mathbb{Z}$. Si $a = \phi(z)$, alors $a^2 \equiv b^2 \mod N$.

Ensuite, pour trouver les éléments P, on va cribler les **normes** d'éléments $u + v\alpha \in \mathbb{Z}[\alpha]$ (analogues des petits p_i pour le crible quadratique).

La phase d'algèbre linéaire est sensiblement identique à cele du crible quadratique

Crible algébrique

Le **crible algébrique** généralise l'idée du crible quadratique. L'idée est de chercher des $a^2 \equiv b^2 \mod N$ en cherchant des carrés dans des **anneaux d'entiers**.

Idée. Soit $f(X) \in \mathbb{Z}[X]$ unitaire et irréductible, et $m \in \mathbb{Z}$ qui satisfait $f(m) \equiv 0 \mod N$. En posant $\alpha = \overline{X} \in \mathbb{Z}[X]/(f)$, on a $\mathbb{Z}[X]/(f) = \mathbb{Z}[\alpha]$.

On considère ensuite le morphisme d'anneaux

$$\begin{array}{rccc} \phi & : \mathbb{Z}[\alpha] & \to & \mathbb{Z}/N\mathbb{Z} \\ & P(\alpha) & \mapsto & \overline{P}(m) \mod N \end{array}$$

Alors on cherche $P \in \mathbb{Z}[X]$ tel que $P(\alpha)$ est un carré $z^2 \in \mathbb{Z}[\alpha]$ et $\overline{P}(m)$ est un carré $b^2 \in \mathbb{Z}/N\mathbb{Z}$. Si $a = \phi(z)$, alors $a^2 \equiv b^2 \mod N$.

Ensuite, pour trouver les éléments P, on va cribler les **normes** d'éléments $u + v\alpha \in \mathbb{Z}[\alpha]$ (analogues des petits p_i pour le crible quadratique).

La phase d'algèbre linéaire est sensiblement identique à cele du crible quadratique

Au final, on obtient une **complexité** du crible algébrique en

$$O\Big(\exp((\tfrac{64}{9}\log N)^{1/3}(\log\log N)^{2/3})\Big).$$

Crible algébrique

Le **crible algébrique** généralise l'idée du crible quadratique. L'idée est de chercher des $a^2 \equiv b^2 \mod N$ en cherchant des carrés dans des **anneaux d'entiers**.

Idée. Soit $f(X) \in \mathbb{Z}[X]$ unitaire et irréductible, et $m \in \mathbb{Z}$ qui satisfait $f(m) \equiv 0 \mod N$. En posant $\alpha = \overline{X} \in \mathbb{Z}[X]/(f)$, on a $\mathbb{Z}[X]/(f) = \mathbb{Z}[\alpha]$.

On considère ensuite le morphisme d'anneaux

$$\begin{array}{rccc} \phi & : \mathbb{Z}[\alpha] & \to & \mathbb{Z}/N\mathbb{Z} \\ & P(\alpha) & \mapsto & \overline{P}(m) \mod N \end{array}$$

Alors on cherche $P \in \mathbb{Z}[X]$ tel que $P(\alpha)$ est un carré $z^2 \in \mathbb{Z}[\alpha]$ et $\overline{P}(m)$ est un carré $b^2 \in \mathbb{Z}/N\mathbb{Z}$. Si $a = \phi(z)$, alors $a^2 \equiv b^2 \mod N$.

Ensuite, pour trouver les éléments P, on va cribler les **normes** d'éléments $u + v\alpha \in \mathbb{Z}[\alpha]$ (analogues des petits p_i pour le crible quadratique).

La phase d'algèbre linéaire est sensiblement identique à cele du crible quadratique

Au final, on obtient une **complexité** du crible algébrique en

$$O\Big(\exp((\tfrac{64}{9}\log N)^{1/3}(\log\log N)^{2/3})\Big).$$

A Tale of Two Sieves. C. Pomerance. Notices of the AMS. **1996**. . `[lien]`.

Prime Numbers, a Computational Perspective. R. Crandall, C. Pomerance. Springer. **2001**.

En pratique

Pour extraire des facteurs de taille $\leq$ 60-70 chiffres (« moyens »), on utilise la **méthode ECM**. Le record de factorisation d'ECM a produit un facteur de 83 chiffres.

Pour des facteurs de taille plus importante, on utilise le **crible algébrique**.

En pratique

Pour extraire des facteurs de taille $\leq$ 60-70 chiffres (« moyens »), on utilise la **méthode ECM**. Le record de factorisation d'ECM a produit un facteur de 83 chiffres.

Pour des facteurs de taille plus importante, on utilise le **crible algébrique**.

Le **record** de factorisation de modules RSA est RSA-250, effectuée en février 2020 :

$$
\begin{aligned}
&21403246502407449612644230728393335630086147151447550177977549208814180234471401366433455190958046796109928518724709145876873962619215573630474547705208051190564931066876915900197594056934574522305893259766974716817380693648946998715784949759374979 37\\
=\ &64135289477071580278790190170577389084825014742943447208116859632024532344630238623598752668347708737661925585694639798853367\\
\times\ &33372027594978156556226010605355114227940760344767554666784520987023841729210037080257448673296881877565718986258036932062711
\end{aligned}
$$

En pratique

Pour extraire des facteurs de taille $\leq$ 60-70 chiffres (« moyens »), on utilise la **méthode ECM**. Le record de factorisation d'ECM a produit un facteur de 83 chiffres.

Pour des facteurs de taille plus importante, on utilise le **crible algébrique**.

Le **record** de factorisation de modules RSA est RSA-250, effectuée en février 2020 :

$$
\begin{aligned}
&21403246502407449612644230728393335630086147151447550177977549208814180234471401366433455190958046796109928518724709145876873962619215573630474547705208051190564931066876915900197594056934574522305893259766974716817380693648946998715784949759374979 37\\
&= 64135289477071580278790190170577389084825014742943447208116859632024532344630238623598752668347708737661925585694639798853367\\
&\times 33372027594978156556226010605355114227940760344767554666784520987023841729210037080257448673296881877565718986258036932062711
\end{aligned}
$$

Temps de factorisation : équivalent 2700 années (oui !) de calcul sur 1 coeur.

Source :

`https://lists.gforge.inria.fr/pipermail/cado-nfs-discuss/2020-February/001166.html`

En pratique

Une **implémentation** proche de l'état de l'art de la recherche : CADO-NFS

- majoritairement codé en `C`, `C++`, plus de l'assembleur pour accélérer certains calculs
- licence LGPL (libre), développé principalement en France (notamment une équipe Inria à Nancy)
- permet de factoriser sur un processeur standard (Intel(R) Xeon(R) CPU E5-2650 @2.00GHz) : (source : site web cado-nfs)

RSA-120	RSA-130	RSA-140	RSA-155
1,9 heure	7,5 heures	23 heures	5,3 jours

- utilisé pour la factorisation record

En pratique

Une **implémentation** proche de l'état de l'art de la recherche : CADO-NFS

- majoritairement codé en `C`, `C++`, plus de l'assembleur pour accélérer certains calculs
- licence LGPL (libre), développé principalement en France (notamment une équipe Inria à Nancy)
- permet de factoriser sur un processeur standard (Intel(R) Xeon(R) CPU E5-2650 @2.00GHz) : (source : site web cado-nfs)

RSA-120	RSA-130	RSA-140	RSA-155
1,9 heure	7,5 heures	23 heures	5,3 jours

- utilisé pour la factorisation record

CADO-NFS, An Implementation of the Number Field Sieve Algorithm. The CADO-NFS Development Team. . **2017**. `http://cado-nfs.gforge.inria.fr`

Fin du cours

Questions ?