Algorithmes de factorisation des entiers

http://www.math.univ-lyon1.fr/~roblot/ens.html

1. Références et Complexité
2. Enoncé du problème
3. Algorithmes préliminaires
   - Primalité et pseudo-primalité
   - Reconnaissance des puissances de premiers
4. Quelques résultats d'arithmétique
   - Nombre et taille des facteurs premiers
   - Nombres B-friables
5. Factorisation : algorithmes exponentiels
   - Divisions successives
   - Méthode de Fermat
   - Méthode de Gauss
   - Méthode $p-1$ de Pollard
   - Méthode ρ de Pollard
   - Méthode des factorielles
6. Factorisation : algorithmes sous-exponentiels
   - Crible quadratique de Pomerance
   - Méthode ECM de Lenstra
   - Crible du corps de nombres

Références

- H. Cohen, *A Course in Computational Algebraic Number Theory*, GTM **38**, Springer-Verlag, 1993
- H. Riesel, *Prime Numbers and Computer Methods for Factorization*, Progress in Mathematics, Birkhaüser, 1985
- R. Crandall, C. Pomerance, *Primer Numbers, A Computational Perspective*, Springer, 2001

Complexité

Complexité en $O(f(N))$. il existe $C > 0$ (constante) telle que le nombre d'opérations (dans un sens à préciser) est $\leq C\, f(N)$

Définition.

$$L(\alpha, \beta; N) := \exp\left(\beta(\log N)^{\alpha}(\log\log N)^{1-\alpha}\right)$$

Rappel. la taille de N est $\log N$

- Complexité exponentielle : $\alpha = 1$ et $L(1, \beta; N) = N^{\beta}$
- Complexité polynômiale : $\alpha = 0$ et $L(0, \beta; N) = (\log N)^{\beta}$
- Complexité sous-exponentielle : $0 < \alpha < 1$

Problème de la factorisation des entiers

Soit $N \geq 2$ un entier

Trouver les nombres premiers $p_1, \ldots, p_s$ et les entiers $e_1, \ldots e_s \geq 1$ tels que

$$N = p_1^{e_1} \cdots p_s^{e_s}$$

Par réduction, on se ramène aux trois problèmes suivants

1. Est-ce que N est un nombre premier ?
2. (Sinon, est-ce que N est une puissance d'un nombre premier ?)
3. Sinon, trouver d avec $2 \leq d < N$ et d diviseur de N

Cas le plus difficile. $N = pq$ avec p et q premiers de même taille

1. Références et Complexité
2. Enoncé du problème
3. Algorithmes préliminaires
   - Primalité et pseudo-primalité
   - Reconnaissance des puissances de premiers
4. Quelques résultats d'arithmétique
   - Nombre et taille des facteurs premiers
   - Nombres B-friables
5. Factorisation : algorithmes exponentiels
   - Divisions successives
   - Méthode de Fermat
   - Méthode de Gauss
   - Méthode $p-1$ de Pollard
   - Méthode ρ de Pollard
   - Méthode des factorielles
6. Factorisation : algorithmes sous-exponentiels
   - Crible quadratique de Pomerance
   - Méthode ECM de Lenstra
   - Crible du corps de nombres

Primalité et pseudo-primalité

Problème. N est-il un nombre premier ?

Deux problèmes différents.

Est-ce que N est presque sûrement premier ?
Est-ce que N est premier ?

Tests de primalités :

- APRCL (Adleman, Pomerance, Rumely, Cohen, Lenstra) : complexité démontrée $(\log N)^{c \log \log \log N}$ (*presque* polynômiale) ; utilise les sommes de Gauss et sommes de Jacobi
- ECPP (Atkin-Morain) : complexité polynômiale conjecturée $O((\log N)^5)$; utilise les courbes elliptiques et produit un certificat
- AKS (Agrawal, Kayal, Saxena) : complexité polynômiale démontrée $O((\log N)^6)$; utilise le résultat : p premier si et seulement si $(X+1)^p \equiv X^p + 1 \pmod{p}$

Forte pseudo-primalité

Théorème

Soit p un nombre premier, on écrit $p - 1 = 2^s\, t$ avec t impair. Alors, pour tout a premier avec p, on a :

$$a^t \equiv 1 \pmod{p} \text{ ou } a^{2^i t} \equiv -1 \pmod{p} \text{ pour un } i \text{ avec } 1 \leq i < s$$

Définition : N est fortement pseudo-premier en base a si $N(= p)$ et a vérifient les conclusions du théorème

Théorème

Supposons $N > 9$ impair et composite. Alors

$$|\{1 \leq a < N \text{ avec } N \text{ fortement pseudo-premier en base } a\}| \leq \frac{1}{4}\varphi(N)$$

Fait : si N est fortement pseudo-premier en base a pour (disons) 20 valeurs de a au hasard, on est *sûr* que N est premier

Reconnaissance des puissances de premiers

Problème : existe-t-il p premier et $k \geq 2$ tel que $N = p^k$?

Petit théorème de Fermat

Soit p un nombre premier. Alors, tout entier a vérifie

$$a^p \equiv a \pmod{p}$$

Méthode : On calcule $d = \mathrm{PGCD}(a^N - a, N)$ pour diverses valeurs de a

(1) Si $d = 1$, alors N n'est pas une puissance d'un nombre premier

(2) Si $d = N$, on recommence avec un autre a

(3) Si $1 < d < N$ et si $d = p$ est un nombre premier, on teste si N est une puissance de p, sinon on recommence avec d et N/d

Fait : Dans le cas 3, il est très rare de ne pas obtenir un nombre premier

1. Références et Complexité
2. Enoncé du problème
3. Algorithmes préliminaires
   - Primalité et pseudo-primalité
   - Reconnaissance des puissances de premiers
4. Quelques résultats d'arithmétique
   - Nombre et taille des facteurs premiers
   - Nombres B-friables
5. Factorisation : algorithmes exponentiels
   - Divisions successives
   - Méthode de Fermat
   - Méthode de Gauss
   - Méthode $p-1$ de Pollard
   - Méthode ρ de Pollard
   - Méthode des factorielles
6. Factorisation : algorithmes sous-exponentiels
   - Crible quadratique de Pomerance
   - Méthode ECM de Lenstra
   - Crible du corps de nombres

Nombre et taille des facteurs premiers

Théorème

$\omega(n) =$ nombre de facteurs premiers distincts de n

$$\sum_{n \leq x} \omega(n) = x \log\log x + O(x)$$

Preuve.

$$\sum_{n \leq x} \omega(n) = \sum_{n \leq x} \sum_{p \mid n} 1 = \sum_{p \leq x} \sum_{\substack{n \leq x \\ p \mid n}} 1 = \sum_{p \leq x} \left\lfloor \frac{x}{p} \right\rfloor = \sum_{p \leq x} \frac{x}{p} + O(\pi(x))$$

puis on utilise la formule $\sum_{p \leq x} 1/p = \log\log x + O(1)$ $\square$

Conséquence heuristique : le nombre de facteurs premiers distincts d'un entier au hasard entre 0 et x est $\log\log x$

Nombre et taille des facteurs premiers

Posons $N = p_1 p_2 \ldots p_s$ avec $p_1 \leq p_2 \leq \cdots \leq p_s$, donc $s \approx \log \log N$.

Fait. On a facilement $p_1 \leq N^{1/s}$

Quand est-il de la taille de p_s ? de p_{s-1} ?...

Raisonnement heuristique : N/p_s a $s-1$ facteurs premiers donc on a

$$\begin{aligned} s - 1 &\approx \log \log N/p_s = \log (\log N - \log p_s) \\ &= \log \log N - \log (1 - \log p_s / \log N) \approx s - \log (1 - \log p_s / \log N) \end{aligned}$$

D'où on tire $\log (1 - \log p_s / \log N) \approx -1 \Rightarrow p_s \approx N^{0{,}63}$

Puis, en appliquant ce raisonnement à N/p_s, $N/(p_s p_{s-1})$, ..., on trouve

$$p_{s-1} \approx N^{0{,}23}, \quad p_{s-2} \approx N^{0{,}09}, \ldots$$

Fait. On peut montrer $p_s \sim N^{0{,}624}$ et $p_{s-1} \sim N^{0{,}210}$

Nombres B-friables

Définition. x est B-friable si tous les diviseurs de premiers x sont $\leq B$

Remarque. Les entiers B-friables jouent un rôle important dans beaucoup de méthodes de factorisation

Fait. Les entiers B-friables sont plus nombreux que l'on pourrait penser. Ainsi 25% des entiers $\leq x$ sont $\sqrt{x}$-friables (pour x assez grand)

Théorème

On pose

$$\psi(x, B) = |\{1 \leq n \leq x \text{ avec } n \text{ } B\text{-friable}\}|$$

Pour $1 \leq B \leq x$, posons $v = \log x / \log B$, alors la proportion d'entiers B-friables $\leq x$ est

$$\frac{\psi(x, B)}{x} = v^{-v+o(1)}$$

Exemple. Prenons $B = \sqrt{x}$, donc $v = 2$ et $\psi(x, \sqrt{x})/x \approx 2^{-2} = 0.25$

On suppose pour la suite que $N \geq 2$ est un nombre composite

Le cas le plus difficile est $N = pq$ avec $p < q$ deux premiers de même taille

1. Références et Complexité
2. Enoncé du problème
3. Algorithmes préliminaires
   - Primalité et pseudo-primalité
   - Reconnaissance des puissances de premiers
4. Quelques résultats d'arithmétique
   - Nombre et taille des facteurs premiers
   - Nombres B-friables
5. Factorisation : algorithmes exponentiels
   - Divisions successives
   - Méthode de Fermat
   - Méthode de Gauss
   - Méthode $p-1$ de Pollard
   - Méthode ρ de Pollard
   - Méthode des factorielles
6. Factorisation : algorithmes sous-exponentiels
   - Crible quadratique de Pomerance
   - Méthode ECM de Lenstra
   - Crible du corps de nombres

Divisions successives

Méthode. On divise N par des valeurs successives jusqu'à tomber sur une division exacte.

Division par tous les entiers. il faut $O(\sqrt{N})$ divisions (taille maximale du plus petit premier divisant N)

Division par des premiers. il faut $O(\sqrt{N}/\log N)$ divisions mais il faut disposer d'une table des premiers ou les calculer au fur et à mesure : crible d'Eratosthène jusqu'à $\sqrt{N}$ coûte $O(\sqrt{N}\log\log N)$

Version intermédiaire : On teste 2, 3 et 5, puis ensuite uniquement les entiers inversibles modulo 30

$$\text{Gain : facteur} \quad \frac{30}{\varphi(30)} = 3,75$$

Méthode de Fermat

Idée. Trouver deux entiers a et b tels que

$$N = a^2 - b^2 = (a-b)(a+b)$$

Algorithme.

(1) Faire $a \leftarrow \lceil \sqrt{N} \rceil$

(2) Si $a^2 - N$ est un carré, renvoyer $(a, \sqrt{a^2 - N})$.

(3) Faire $a \leftarrow a + 1$ et retourner en 2

Améliorations.

- On stocke aussi $A = a^2$ et à l'étape 2 : $A \leftarrow A + 2a + 1$
- On teste si $a^2 - N$ est un carré si et seulement si $a^2 - N$ est un carré modulo M avec M bien choisi

Méthode de Fermat

Efficacité. Si $N = pq$ alors $a = (p+q)/2$ et $b = (p-q)/2$. On part de $\approx \sqrt{N}$ donc il faut

$$\approx \frac{p+q}{2} - \sqrt{N} = \frac{1}{2}\left(p + N/q\right) - \sqrt{N} = \frac{(\sqrt{N}-p)^2}{2p} \text{ itérations}$$

Cas extrême. Si $p < q < p + 4\sqrt{p} + 4$, on a directement le résultat !

Cas moyen. $q \approx N^{2/3}$ alors nombre d'itérations est $\approx \frac{1}{2}N^{2/3}$

Amélioration. On multiplie N par un facteur f de telle sorte que $fp \approx q$. Mais comment trouver f ? On peut essayer tous les $f = 1, 2, \ldots, N^{1/3}$, ou essayer des f ayant beaucoup de diviseurs. En combinant les deux, on peut obtenir une méthode en $O(N^{1/3})$ si le plus petit diviseur de N est $\geq N^{1/3}$.

Méthode de Fermat : Exemple

On factorise $N = 10\,235\,789$

s	$s^2 - N$	mod 16	$\sqrt{s^2 - N}$	s	$s^2 - N$	mod 16	$\sqrt{s^2 - N}$
3200	4211	3		3213	87580	12	
3201	10612	4	103.015	3214	94007	7	
3202	17015	7		3215	100436	4	316.916
3203	23420	12		3216	106867	3	
3204	29827	3		3217	113300	4	336.600
3205	36236	12		3218	119735	7	
3206	42647	7		3219	126172	12	
3207	49060	4	221.495	3220	132611	3	
3208	55475	3		3221	139052	12	
3209	61892	4	248.781	3222	145495	7	
3210	68311	7		3223	151940	4	389.795
3211	74732	12		3224	158387	3	
3212	81155	3		3225	164836	4	406.000

On obtient $N = (3225 - 406)(3225 + 406) = 2819 \cdot 3631$

Méthode de Gauss

Idée. Trouver des résidus quadratiques modulo N pour en déduire des informations sur les premiers divisant N

Définition. Soit q premier et a entier, on pose

$$\left(\frac{a}{q}\right) = \begin{cases} 0 & \text{si } q \mid a \\ 1 & \text{si } a \text{ est un carré inversible modulo } q \\ -1 & \text{si } a \text{ n'est pas un carré modulo } q \end{cases}$$

Pour $b = q_1^{e_1} \cdots q_t^{e_t}$, on pose $\left(\frac{a}{b}\right) = \left(\frac{a}{q_1}\right)^{e_1} \cdots \left(\frac{a}{q_t}\right)^{e_t}$

Loi de réciprocité quadratique

Soient a et b deux entiers impairs. Alors

$$\left(\frac{a}{b}\right) = (-1)^{\frac{(a-1)(b-1)}{4}} \left(\frac{b}{a}\right)$$

Méthode de Gauss

Exemple. Si 15 est un carré modulo N alors pour tout p divisant N, on a

$$1 = \left(\frac{15}{p}\right) = (-1)^{(p-1)/2}\left(\frac{p}{15}\right) = (-1)^{(p-1)/2}\left(\frac{p}{3}\right)\left(\frac{p}{5}\right)$$

$(-1)^{(p-1)/2}$	$\left(\frac{p}{3}\right)$	$\left(\frac{p}{5}\right)$	mod 4	mod 3	mod 5	mod 60
1	1	1	1	1	$1, 4$	$1, 49$
1	-1	-1	1	2	$2, 3$	$17, 53$
-1	-1	1	3	2	$1, 4$	$11, 59$
-1	1	-1	3	1	$2, 3$	$7, 43$

Donc $p \equiv 1, 7, 11, 17, 43, 49, 53$ ou $59 \pmod{60}$

Efficacité. k résidus quadratiques (indépendants) diminue de 2^{-k} les diviseurs (premiers) à considérer. Ainsi 20 résidus divisent par $1\,048\,576$ l'ensemble des diviseurs à tester.

Méthode de Gauss

Problème. Comment trouver les résidus ? Calculer $x^2 \mod N$ pour de multiples valeurs de $x \geq \lceil\sqrt{N}\rceil$ peut donner de grand résidu qu'il faut factoriser pour pouvoir obtenir les informations

Méthode. On considère des x proches de $\lceil\sqrt{kN}\rceil$ pour $k = 1, 2, \ldots$ et on garde seulement les $x^2 - kN$ qui sont friables

Difficulté. Implantation générale assez technique (possibilité d'obtenir les classes convenables en parcourant toutes les classes)

Variante. on combine plusieurs résidus pour obtenir des résidus quadratiques premiers.

Exemple : $x_1^2 - N = 2^2 \cdot 3 \cdot 5 \cdot 7$ et $x_2^2 - 2N = 5^3 \cdot 7$ donne que 3 est un résidu quadratique modulo N

Méthode de Gauss : Exemple

On factorise $N = 103\,861$ ($p < \sqrt{N} \approx 322,27$)

- $323^2 - N = 2^2 \cdot 3^2 \cdot 13$ donc $\left(\frac{p}{13}\right) = 1$ et $p \equiv 1,\ 3,\ 4,\ 9,\ 10,$ ou $12 \pmod{13}$
- $327^2 - N = 2^2 \cdot 13 \cdot 59$ donc 59 est un carré modulo p, $\left(\frac{p}{59}\right) = -1$ et $p \equiv 2,\ 6,\ 8,\ 10,\ 11,\ \dots,\ 54,\ 55,\ 56,$ ou $58 \pmod{59}$. Puis, on en déduit que $p \equiv 10,\ 14,\ 23,\ 30,\ 38,\ 40,\ \dots,\ 751,\ 755,\ 758,\ 763,\ 764,$ ou $766 \pmod{767}$
- $457^2 - 2\,N = 7^2 \cdot 23$ donc $\left(\frac{p}{23}\right) = -1$ et $p \equiv 5,\ 7,\ 10,\ 11,\ 14,\ 15,\ 17,\ 19,\ 20,\ 21,\ 22 \pmod{23}$. Finalement, en utilisant le fait que $p < 322$ et p premier, on obtient $p = 43,\ 61,\ 103,\ 113,\ 157,\ 191,$ 283 ou 313

Après essai, on trouve que 283 divise N et $N = 283 \cdot 367$

Méthode $p-1$ de Pollard

Idée. Supposons que $p-1$ divise M alors p divise $\mathrm{PGCD}(a^M-1, N)$

Spécificité. Ne dépend pas de la taille de p, mais de la taille des diviseurs primaires de $p-1$

Superfriable. $m = q_1^{e_1} \cdots q_t^{e_t}$ est B-superfriable si $q_i^{e_i} \leq B$ pour $i = 1, \ldots, t$

Fait. Posons $M(c) = \mathrm{PPCM}(1, \ldots, c)$. Si m est B-superfriable alors m divise $M(B)$.
On a les formules : $M(1) = 1$, puis pour $c \geq 2$

- $M(c) = qM(c-1)$ si $c = q^e$ (q premier)
- $M(c) = M(c-1)$ sinon

Calcul de PGCD. On a

$$\mathrm{PGCD}(a^M-1, N) = \mathrm{PGCD}((a^M \mod N)-1, N)$$

Méthode $p-1$ de Pollard

Algorithme.

(1) Faire $m \leftarrow 2$, $c \leftarrow 2$

(2) Tant que $c \leq B$, Faire
  Si $c = q^e$ alors
    $m \leftarrow m^q \mod N$
    $d \leftarrow \mathrm{PGCD}(m-1, N)$
    Si $d > 1$ alors renvoyer d et terminer
  $c \leftarrow c + 1$

(3) Renvoyer "Echec : pas de facteur p avec $p-1$ B-superfriable" et terminer

Remarque. l'algorithme peut échouer avec $d = N$, dans ce cas on recommence avec une autre valeur initiale pour m

Amélioration. Plutôt que d'itérer sur les $c \leq B$, on peut parcourir les premiers $q_1 < q_2 < \cdots \leq B$ et faire $m \leftarrow m^{q_i^{e_i}} \mod N$ avec $e_i \geq 1$ maximal tel que $q_i^{e_i} \leq B$

Méthode $p-1$ de Pollard

Complexité. On calcule $m \leftarrow m^a \mod N$ pour $a \leq B$ en temps $O(\log B \log^2 N)$ donc l'algorithme retourne p si $p-1$ est B-superfriable en temps probabiliste $O(B \log^2 N)$ (le cas $d = N$ pour m aléatoire a une probabilité $\leq 1/2$)

Amélioration (2nd stage). Souvent $p-1$ n'est pas B-superfriable, mais $p-1 = fQ$ avec f B-superfriable et Q premier $> B$ mais pas trop grand, disons $Q < B' \leq B \log B$. Alors, p divise $\mathrm{PGCD}(a^{Q\,M(B)} - 1, N)$

Supposons connu les (différences des) premiers $Q_1, \ldots, Q_r$ entre B et B', alors on peut calculer facilement

$$a^{Q_1\,M(B)} \mod N,$$
$$a^{Q_2\,M(B)} \mod N = a^{Q_1\,M(B)} \cdot a^{(Q_2-Q_1)M(B)} \mod N,$$
$$a^{Q_3\,M(B)} \mod N = a^{Q_2\,M(B)} \cdot a^{(Q_3-Q_2)M(B)} \mod N \cdots$$

par une simple multiplication modulaire si on pré-calcule les petites puissances de a modulo N

Méthode $p-1$ de Pollard : Exemple

On factorise $N = 136\,838\,612\,177$. On prend $a = 2$, $B = 100$ et on procède premier par premier.

- $2^6 \leq B$ puis $a^{2^6} \mod N = 122\,567\,948\,726$ et $\mathrm{PGCD}(a^{e_1} - 1, N) = 1$
- $3^4 \leq B$ puis $a^{e_1\, 3^4} \mod N = 25\,694\,491\,622$ et $\mathrm{PGCD}(a^{e_2} - 1, N) = 1$
- $5^2 \leq B$ puis $a^{e_2\, 5^2} \mod N = 3\,295\,688\,067$ et $\mathrm{PGCD}(a^{e_3} - 1, N) = 1$
- $7^2 \leq B$ puis $a^{e_3\, 7^2} \mod N = 108\,770\,095\,964$ et $\mathrm{PGCD}(a^{e_4} - 1, N) = 1$
- $11 \leq B$ puis $a^{e_4\, 11} \mod N = 84\,598\,852\,995$ et $\mathrm{PGCD}(a^{e_5} - 1, N) = 1$
- $13 \leq B$ puis $a^{e_5\, 13} \mod N = 26\,088\,272\,808$ et $\mathrm{PGCD}(a^{e_6} - 1, N) = 1$
- $17 \leq B$ puis $a^{e_6\, 17} \mod N = 57\,795\,217\,304$ et $\mathrm{PGCD}(a^{e_7} - 1, N) = 1$
- $19 \leq B$ puis $a^{e_7\, 19} \mod N = 131\,992\,584\,120$ et $\mathrm{PGCD}(a^{e_8} - 1, N) = 1$
- $23 \leq B$ puis $a^{e_8\, 23} \mod N = 89\,064\,599\,475$ et $\mathrm{PGCD}(a^{e_9} - 1, N) = 133\,723$

D'où la factorisation $N = 133\,723 \cdot 1\,023\,299$

Remarque. $133\,722 = 2 \cdot 3^2 \cdot 17 \cdot 19 \cdot 23$ et $1\,023\,298 = 2 \cdot 17 \cdot 30\,097$

Méthode ρ de Pollard : le paradoxe des anniversaires

Question. Combien faut-il de personnes pour en avoir (au moins) deux avec le même anniversaire ? et avec une probabilité $> 1/2$?

E ensemble de n éléments. On choisit des éléments $x_1, \dots, x_k$ dans E au hasard *avec répétition possible*

Quelle est la probabilité p_k qu'il existe au moins une coïncidence, c'est-à-dire i et j distincts tels que $x_i = x_j$?

La probabilité que tous les x_i soient distincts est donnée par la formule

$$1 - p_k = \frac{n(n-1)\cdots(n-(k-1))}{n^k} = \prod_{i=1}^{k-1}\left(1 - \frac{i}{n}\right) \approx \exp\left(\frac{-k(k-1)}{2n}\right)$$

On en déduit

Théorème

Si $k \geq 1,2\sqrt{n}$, alors on a $p_k > 1/2$

Réponse. pour $n = 365$, on trouve $\lceil 1,2\sqrt{n}\rceil = 23$

Méthode ρ de Pollard

Idée. Soient $x_1, \ldots, x_k$ nombres au hasard entre 0 et $N-1$. Si on prend k de l'ordre de $\sqrt{p}$ alors, par le paradoxe des anniversaires, il y a une probabilité $> 1/2$ qu'il existe $i \neq j$ tels que $x_i \equiv x_j \pmod{p}$ et donc

$$\mathrm{PGCD}(x_i - x_j, N) > 1$$

d'où une possible factorisation de N.

Problème. il faut stocker toutes les valeurs et tester toutes les paires !

Solution. On considère la suite définie par $x_0 = \lceil \sqrt{N} \rceil$, puis pour $i \geq 1$, par $x_i = x_{i-1}^2 + c \mod N$. La suite $(x_i)_{i \geq 0}$ se comporte de *manière expérimentale* (pour $c \neq 0$ ou -2) comme une suite aléatoire et est *ultimement périodique*
On utilise la méthode de Floyd pour déterminer une collision

Méthode ρ de Pollard : Méthode de Floyd

Soit (x_i) une suite ultimement périodique de pré-période $M \geq 0$ et de période $T \geq 1$.

Théorème

Pour $m := T\lceil M/T \rceil$, on a $x_m = x_{2m}$

Preuve. On a $m \geq T \cdot M/T = M$ et $2m = m + T\lceil M/T \rceil$, donc on a bien $x_{2m} = x_m$. $\square$

Remarque : On a $M/T \leq \lceil M/T \rceil < M/T + 1$, et donc $M \leq m < M + T$.

Méthode. On calcule simultanément x_i et x_{2i}

Méthode ρ de Pollard

Algorithme.

(1) Faire $a \leftarrow \lceil\sqrt{N}\rceil$, $b \leftarrow a$, $c \leftarrow 1$

(2) Faire $a \leftarrow a^2 + c \mod N$
Faire $b \leftarrow b^2 + c \mod N$
Faire $b \leftarrow b^2 + c \mod N$

(3) Calculer $d \leftarrow \mathrm{PGCD}(a - b, N)$
si $d = 1$ alors retourner en 2

(4) Renvoyer d et terminer

Remarque. L'algorithme peut renvoyer $d = N$, dans ce cas on peut recommencer avec une autre valeur pour c

Complexité. Temps probabiliste $O(\sqrt{p}\log^2 N) = O(N^{1/4}\log^2 N)$

Améliorations. Stocker les $a - b$ en faisant $Q \leftarrow Q \cdot (a - b) \mod N$ à la fin de l'étape 2, et à la place de l'étape 3, calculer le PGCD de Q et N à intervalles réguliers.
On peut aussi utiliser l'amélioration de Brent

Méthode ρ de Pollard : Amélioration de Brent

Idée. Au lieu de considérer $x_{2i} - x_i$, pour chaque $i = 2^k$, on considère $x_j - x_{2^k}$ pour $3 \cdot 2^{k-1} < j \leq 2^{k+1}$

Premiers calculs. On calcule x_1, x_2, on teste $x_2 - x_1$, puis x_3, x_4, teste $x_4 - x_2$, puis x_5, x_6, x_7, teste $x_7 - x_4$, puis x_8, teste $x_8 - x_4$, x_9, x_{10}, x_{11}, x_{12}, x_{13}, teste $x_{13} - x_8 \ldots$

Avantages.

- $j - 2^k$ parcourt $2^{k-1} + 1, \ldots, 2^k$ donc on trouve une collision pour $k = \lceil \max\{\log_2 M, \log_2 T\} \rceil$
- Une seule évaluation par boucle
- Pas besoin de recalculer les x_i deux fois pour i petit
- Une seule valeur de x_i stockée à tout moment

Résultat. On peut constater (et donner des arguments heuristiques) pour une amélioration de l'ordre de 25%

Méthode ρ de Pollard : Exemple

On cherche à factoriser $N = 127\,199$. On a $x_1 = \lceil \sqrt{N} \rceil = 357$ et $x_2 = x_1^2 + 1 \mod N = 251$.

m	x_m	x_{2m}	PGCD	m	x_m	x_{2m}	PGCD
1	357	251	1	11	125075	105564	1
2	251	7210	1	12	59412	28503	1
3	63002	97662	1	13	13495	103617	1
4	7210	114009	1	14	93257	97895	1
5	86909	54078	1	15	18022	99548	1
6	97662	59412	1	16	53438	42431	1
7	103628	93257	1	17	2295	44053	1
8	114009	53438	1	18	51867	115435	1
9	95068	51867	1	19	54039	28231	1
10	54078	106079	1	20	106079	123495	311

D'où la factorisation $N = 311 \cdot 409$

Coût de calcul : 58 calculs de $x \mapsto x^2 + 1 \mod N$ et 20 PGCD

Méthode ρ de Pollard : Exemple (amélioration de Brent)

On cherche à factoriser $N = 127\,199$. On calcule $\mathrm{PGCD}(x_j - x_{2^k}, N)$ pour $3 \cdot 2^{k-1} < j \leq 2^k$

k	j	x_{2^k}	x_j	PGCD	k	j	x_{2^k}	x_j	PGCD
0		357				11	95068	125075	
	2		251	1		12		59412	
1		251				13		13495	1
	3		63002			14		93257	1
	4		7210	1		15		18022	1
2		7210				16		53438	1
	5		86909		4		53438		
	6		97662		...	...	...	...	...
	7		103628	1	5		42431		
	8		114009	1	...	...	...	...	...
3		114009				50		98304	1
	9	95068				51		113989	1
	10		54078			52		114272	311

Coût de calcul : 51 calculs de $x \mapsto x^2 + 1 \mod N$ et 16 PGCD

Méthode des factorielles

Définition. On pose $F_N(k) = k! \mod N$

Quelques résultats.

- N est premier si et seulement si $F_N(N-1) = N-1$
- N est premier si et seulement si $\mathrm{PGCD}(F_N(\lfloor\sqrt{N}\rfloor), N) = 1$

Application à la factorisation

Soit $k \geq 1$, le plus petit entier tel que $\mathrm{PGCD}(F_N(k), N) > 1$. Alors k est le plus petit nombre premier divisant N.

Complexité. k peut être calculé en $O(\log N)$ évaluation de la fonction F_N par dichotomie

Problème. F_N coûte cher à calculer

Méthode des factorielles : version de Pollard–Strassen

Définition. Posons $\varphi_B(X) = X(X-1)\cdots(X-B+1)$, alors, pour tout $j \geq 1$

$$\varphi_B(jB) = \frac{(jB)!}{((j-1)B)!}$$

Conséquence. Le plus petit $j \geq 1$ tel que $\mathrm{PGCD}(\varphi_B(jB), N) > 1$ donne que le plus petit facteur premier de N est dans $](j-1)B, jB]$
Si le PGCD est dans l'intervalle, c'est le facteur premier. Sinon, on parcourt les éléments de l'intervalle pour trouver celui qui divise N.

Paramètre. Prenons $B = \lceil N^{1/4} \rceil$. Alors il existe j avec $1 \leq j \leq B$ tel que $\mathrm{PGCD}(\varphi_B(jB), N) > 1$.
Une fois trouvé j, il faut $O(N^{1/4} \log^2 N)$ opérations pour isoler le premier.

Calcul des $\varphi_B(jB)$. Evaluation modulo N d'un polynôme de degré B en B valeurs en temps $O(B \log^2 N)$

Complexité. Factorise en $O(N^{1/4} \log^2 N)$. C'est l'algorithme avec la meilleure complexité *déterministe* démontrée

Méthode des factorielles : Exemple

On factorise $N = 737\,419$. On a $B = \lceil N^{1/4} \rceil = 30$.

On a

$$\varphi_{30}(X) \mod N = X^{30} + 736984X^{29} + 90335X^{28} + 614948X^{27} + 334301X^{26}$$
$$+413052X^{25} + 219546X^{24} + 330711X^{23} + 713199X^{22} + 313429X^{21} + 138020X^{20}$$
$$+504805X^{19} + 381513X^{18} + 430795X^{17} + 99885X^{16} + 564428X^{15} + 265574X^{14}$$
$$+400913X^{13} + 84143X^{12} + 484992X^{11} + 241631X^{10} + 424763X^{9} + 384906X^{8}$$
$$+514873X^{7} + 4391X^{6} + 99109X^{5} + 321698X^{4} + 323840X^{3} + 552595X^{2} + 334486X$$

Puis, on a

- $\varphi_{30}(B) \mod N = 289286$ et PGCD$= 1$,
- $\varphi_{30}(2B) \mod N = 722233$ et PGCD$= 1$,
- $\varphi_{30}(3B) \mod N = 257088$ et PGCD$= 1, \dots,$
- $\varphi_{30}(27B) \mod N = 311652$ et PGCD$= 787 \in [26B, 27B[$

d'où la factorisation $N = 787 \cdot 937$

1. Références et Complexité
2. Enoncé du problème
3. Algorithmes préliminaires
   - Primalité et pseudo-primalité
   - Reconnaissance des puissances de premiers
4. Quelques résultats d'arithmétique
   - Nombre et taille des facteurs premiers
   - Nombres B-friables
5. Factorisation : algorithmes exponentiels
   - Divisions successives
   - Méthode de Fermat
   - Méthode de Gauss
   - Méthode $p-1$ de Pollard
   - Méthode ρ de Pollard
   - Méthode des factorielles
6. Factorisation : algorithmes sous-exponentiels
   - Crible quadratique de Pomerance
   - Méthode ECM de Lenstra
   - Crible du corps de nombres

Crible quadratique de Pomerance

Idée. Trouver a et b tels que $a^2 \equiv b^2 \pmod{N}$, il suit que $N \mid (a-b)(a+b)$ et avec un peu de chance $\mathrm{PGCD}(a-b, N)$ isole un facteur de N

Combinaisons de congurences. Pour trouver a et b, on considère des valeurs de a telle que $a^2 \mod N$ est B-friable et on les combine. Par exemple

$$\begin{aligned} a_1^2 \mod N &= q_1^3\, q_2^1\, q_3^1\, q_4^0 \\ a_2^2 \mod N &= q_1^2\, q_2^2\, q_3^0\, q_4^1 \\ a_3^2 \mod N &= q_1^1\, q_2^1\, q_3^1\, q_4^3 \end{aligned}$$

donne que $(a_1\, a_2\, a_3)^2 \equiv q_1^6\, q_2^4\, q_3^2\, q_4^4 \equiv (q_1^3\, q_2^2\, q_3\, q_4^2)^2 \pmod{N}$

Méthode.

1. Engendrer un grand nombre de a tels que $a^2 \mod N$ est B-friable
2. Combiner ces valeurs pour en déduire des congruences $a^2 \equiv b^2 \pmod{N}$

Crible quadratique : Combinaison des congruences

Notations. Posons $2 = p_1 < p_2 < \cdots < p_t \leq B$. Pour x B-friable, on a

$$x = p_1^{e_1} \cdots p_t^{e_t} \quad \text{avec} \quad e_i \geq 0$$

On associe à x le vecteur $\vec{e}(x) = (\bar{e}_1, \ldots \bar{e}_t) \in \mathbb{F}_2^t$

Lemme

Soit $x_1, \ldots, x_k$ des entiers B-friables. Alors $x_1 \cdots x_k$ est un carré si et seulement si $\vec{e}(x_1) + \cdots \vec{e}(x_k) = 0$

Conséquences.

1. Trouver un carré comme combinaison des congruences trouvées est un problème d'algèbre linéaire sur $\mathbb{F}_2$
2. Pour être sûr d'avoir une solution, il suffit d'avoir plus de congruences que de premiers $\leq B$
3. Par la méthode du pivot de Gauss, la détermination des combinaisons donnant des carrés est en $O(t^3) = O(B^3)$ opérations, voire $O(B^{2+\varepsilon})$ par la méthode de Lanczos

Crible quadratique : Criblage

Remarque. Posons $M = \lceil \sqrt{N} \rceil$ et prenons $\epsilon > 0$ (petit). Pour $M \leq x \leq M + M^{\epsilon}$, on a $x^2 \mod N = x^2 - N \approx M^{1+\epsilon}$

On pose $f(x) = (M + x)^2 - N$ et on cherche à trouver les valeurs de x avec $0 \leq x \leq T$ (T paramètre à déterminer) telles que $f(x)$ est B-friable

Restriction sur les premiers. Soit $p \leq B$ et supposons que $f(x)$ est B-friable. Alors p divise $f(x) = (M + x)^2 - N$ donc N est un carré modulo p. Ainsi, il suffit de considèrer *uniquement* les premiers $p \leq B$ tels que $\left(\frac{N}{p}\right) = 1$. On appelle l'ensemble de ces premiers la *base des facteurs*

Criblage. Soit p dans la base des facteurs. N possède (au plus) deux racines carrées $\pm r$ modulo p. Et $f(x)$ est divisible par p si et seulement si $x + M \equiv \pm r \pmod p$. De même, N possède 2 racines carrées modulo p^e si p est impair ou $p = 2$ et $e < 3$, sinon 4. Et les valeurs de x pour lesquelles p^e divise $f(x)$ sont celles telles que $x + M$ est congru à une de ces racines modulo p^e

Crible quadratique : Un exemple de criblage

On prend $N = 194\,111$. On a donc $M = \lceil\sqrt{N}\rceil = 441$. On choisit $B = 15$ et $T = 15$. La base des facteurs est $\{2, 5, 7, 11\}$, le polynôme est $f(x) = x^2 + 882x + 370$

- $p = 2$

0 est l'unique racine de f modulo 2 donc $2 \mid f(x) \iff x \equiv 0 \pmod 2$

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
2	1	2	1	2	1	2	1	2	1	2	1	2	1	2	1

f n'a pas de racines modulo 4 donc $4 \nmid f(x)$ pour tout x

- $p = 5$

0 et 3 sont racines de f modulo 5 donc $5 \mid f(x) \iff x \equiv 0, 3 \pmod 5$

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
10	1	2	5	2	5	2	1	10	1	10	1	2	5	2	5

3 et 15 sont racines de f modulo 5^2 donc $5^2 \mid f(x) \iff x \equiv 3, 15 \pmod{5^2}$

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
10	1	2	25	2	5	2	1	10	1	10	1	2	5	2	25

Crible quadratique : Un exemple de criblage

40 et 78 sont racines de f modulo 5^3 (en dehors de la table)

- $p = 7$

1 et 6 sont racines de f modulo 7 donc $7 \mid f(x) \iff x \equiv 1, 6 \pmod 7$

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
10	7	2	25	2	5	14	1	70	1	10	1	2	35	2	175

...

- $p = 11$

3 et 6 sont racines de f modulo 11 donc $11 \mid f(x) \iff x \equiv 3, 6 \pmod{11}$

...

124 et 325 sont racines de f modulo 11^3 donc $11^3 \mid f(x) \iff x \equiv 124, 325 \pmod{11^3}$

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
10	7	2	3025	2	5	154	1	70	1	10	1	2	12005	22	175

$f(x)$ est B-friable si et seulement si l'entrée correspondant à x vaut $f(x)$, ici on trouve que $f(3)$ et $f(13)$ sont B-friables

Crible quadratique : Calcul des racines de $f(x)$

Problème. Soit p premier avec tel que N est un carré modulo p.
Trouver les racines x_i de $f(x) = (M + x)^2 - N$ modulo p, p^2, ...
équivaut à trouver les racines carrées r_i de N modulo p^e, puis à poser
$x_i = r_i - M \mod p^e$

Racines carrées modulo 2^e

La racine carrée de N modulo 2 est 1 (on peut supposer N impair)
Puis, on a

- N est un carré modulo 4 si et seulement si $N \equiv 1 \pmod 4$. Dans ce cas les racines carrées sont ± 1
- N est un carré modulo 2^e avec $e \geq 3$ si et seulement si $N \equiv 1 \pmod 8$. Dans ce cas, N a quatre racines carrées modulo 2^e. Elles peuvent être construite par récurrence en partant d'une racine carrée r de N modulo 2^{e-1} par la procédure suivante
  1. Si $r^2 \not\equiv N \pmod{2^e}$, alors faire $r \leftarrow r + 2^{e-2}$
  2. Renvoyer $(r, -r, r + 2^{e-1}, -r + 2^{e-1})$ et terminer

Crible quadratique : Calcul des racines de $f(x)$

Racines carrées modulo p^e (p impair)

On utilise, par exemple, l'algorithme de Cipolla pour une racine carrée de N modulo p

(1) Soit $b \in \mathbb{F}_p$ au hasard. Si $b^2 - 4N$ est un carré modulo p, recommencer en 1

(2) Retourner $x^{(p+1)/2} \mod x^2 - bx + N$ et terminer

Pour tout $e \geq 2$, alors N a aussi exactement deux racines carrées modulo p^e. Elles peuvent être construite par récurrence à partir d'une racine carrée r de N modulo p^{e-1} par la procédure suivante

(1) Faire $s \leftarrow (N - r^2)/p^{e-1}$, puis $k \leftarrow 2^{-1}s \mod p$

(2) Renvoyer $\pm(r + kp^{e-1})$ et terminer

Coût. Dominé par l'algorithme de Cipolla en $O(\log^3 p) = O(\log^3 B)$

Crible quadratique : Algorithme de criblage

Notons $p_1, \ldots, p_K$ les nombres premiers de la base des facteurs avec $K \approx \frac{1}{2} B / \log B$. On suppose $T \geq B$.

(1) Pour $x = 0$ à T, poser $v[x] \leftarrow 1$

(2) Pour $i = 1$ à K, faire

  (a) Faire $p \leftarrow p_i$, $e \leftarrow 1$

  (b) Faire $\mathcal{R} \leftarrow \mathrm{racines\_de\_}f(N, p^e)$

  (c) Si tous les éléments de $\mathcal{R}$ sont $> T$, passer à la prochaine valeur en 2

  (d) Pour tout $x \in \mathcal{R}$, Faire

    Tant que $x \leq T$

      $v[x] \leftarrow v[x] \cdot p$

      $x \leftarrow x + p^e$

  (e) Faire $e \leftarrow e + 1$ et retourner en 2.b

(3) Renvoyer $(x, f(x))$ pour tous les $x = 0, \ldots, T$ tels que $v[x] = f(x)$

Complexité. $O(K \log^3 B + T \log\log B)$; si $T \gg B$, coût par valeurs $\approx \log\log B$

Crible quadratique : Optimisation des paramètres

On prend $B = L(1/2, 1/2; N) = \exp\left(\frac{1}{2}\sqrt{\log N \log\log N}\right)$.
Donc

$$u = \frac{\log \sqrt{N}}{\log B} = \frac{\frac{1}{2}\log N}{\frac{1}{2}\sqrt{\log N \log\log N}} = \sqrt{\frac{\log N}{\log\log N}}$$

et $\log u \approx \frac{1}{2}\log\log N$ donc le nombre de valeurs à crible pour obtenir $K \approx B$ relations est

$$T = u^u B \approx B^2$$

Ainsi $T \gg B$ et le coût du crible est donc

$$O(B^2 \log\log B)$$

Ce qui est équivalent à la phase d'algèbre linéaire si on utilise les méthodes en $O(B^{2+\varepsilon})$ et donc le coût heuristique pour factoriser N par l'algorithme du crible quadratique de Pomerance est de l'ordre de

$$\exp\left((1+\varepsilon)\sqrt{\log N \log\log N}\right) = L(1/2, 1+\varepsilon; N)$$

Crible quadratique de Pomerance : Un exemple

On factorise $N = 344\,742\,577$. On trouve $B \approx 45$. La base des facteurs est $\{2, 3, 7, 11, 13, 17, 23, 31, 43\}$
On crible les valeurs de $f(x) = x^2 + 37\,136x + 28\,047$ pour $x = 0, \ldots 2025$
On trouve que $f(x)$ est B-friable pour $x =$ 29, 58, 66, 127, 159, 313, 463, 587, 687, 841, 908, 1055, 1713, 1758 et la matrice correspondante

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

dont le noyau est de rang 6, contenant par exemple le vecteur ${}^t(1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1)$.

Donc $f(29)f(587)f(1758)$ est un carré modulo N qui est congru à $(29 + M)^2(587 + M)^2(1758 + M)^2$.

En effet, on trouve

$$11\,879\,679^2 \equiv 272\,968\,322^2 \pmod N$$

et finalement

$$(11\,879\,679 - 272\,968\,322, N) = 14\,827$$

d'où la factorisation

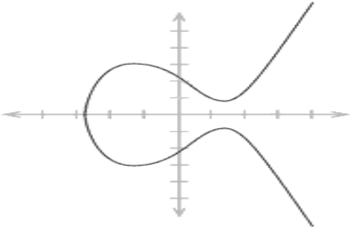
$$N = 14\,827 \cdot 23\,251$$

Méthode ECM de Lenstra : Courbe elliptique

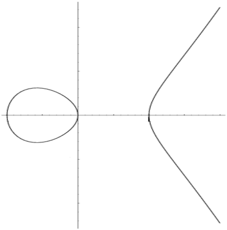
Définition. Soit K un corps. Une courbe elliptique sur K est une courbe cubique plane non singulière ayant un point rationnel sur K

Version explicite. Supposons que $\mathrm{char}(K) \neq 2, 3$. Alors une courbe elliptique sur K est l'ensemble des solutions $(x, y) \in K^2$ de l'équation $y^2 = x^3 + ax + b$ auquel on ajoute le point à l'infini, où $a, b \in K$ sont tels que $4a^3 + 27b^2 \neq 0$

Exemples.



$y^2 = x^3 - 6x + 6$



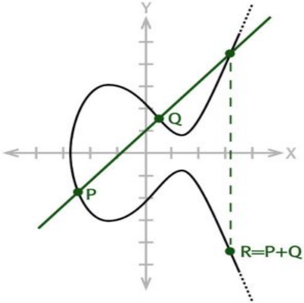
$y^2 = x^3 - x$

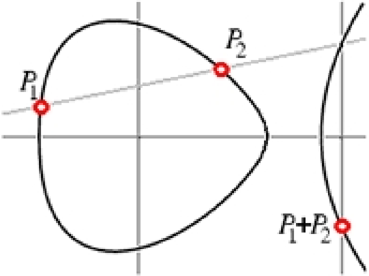
Méthode ECM de Lenstra : Groupe des points

Théorème

Le groupe des points d'une courbe elliptique E sur le corps K, noté $E(K)$, forment un groupe abélien dont l'élément neutre est le point à l'infini O.

Exemples.





Méthode ECM de Lenstra : Addition de points

Notations. Soient $P_1 = (x_1, y_1)$ et $P_2 = (x_2, y_2)$ deux points dans $E(K)$. On continue de noter O le point à l'infini.

Règles de calculs.

- $-O = O$, $O + P_1 = P_1$
- $-P_1 = (x_1, -y_1)$
- Si $P_2 = -P_1$, alors $P_1 + P_2 = O$
- Si $P_2 \neq -P_1$, alors $P_1 + P_2 = (x_3, y_3)$ avec

$$x_3 = m^2 - x_1 - x_2, \quad y_3 = m(x_1 - x_3) - y_1$$

où la pente m est donnée par $m = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & \text{si } x_1 \neq x_2 \\ \dfrac{3x_1^2 + a}{2y_1} & \text{sinon} \end{cases}$

Coût. Au plus 7 additions et 4 divisions/multiplications

Méthode ECM de Lenstra : Stucture de $E(\mathbb{F}_p)$

Soit p un nombre premier et soit E un courbe elliptique définie sur $\mathbb{F}_p$

Théorèmes de Cassels et Hasse

Le groupe $E(\mathbb{F}_p)$ est de rang 1 ou 2 et son cardinal vérifie

$$|\#E(\mathbb{F}_p) - (p+1)| \leq 2\sqrt{p}$$

Théorèmes de Deuring et Lenstra

Pour tout entier $m \in [p+1-2\sqrt{p}, p+1+2\sqrt{p}]$, il existe une courbe elliptique E sur $\mathbb{F}_p$ telle que $\#E(\mathbb{F}_p) = m$.
De surcroît, il existe $c > 0$ telle que si $p > 3$ et si $\mathcal{S}$ est un sous-ensemble de $\mathbb{Z} \cap [p+1-2\sqrt{p}, p+1+2\sqrt{p}]$ de cardinal ≥ 3, alors le nombre $N(\mathcal{S})$ de courbes elliptiques sur $\mathbb{F}_p$ dont le cardinal est dans $\mathcal{S}$ vérifie

$$N(\mathcal{S}) > \frac{c \cdot \#\mathcal{S} \cdot p^{3/2}}{\log p}$$

Méthode ECM de Lenstra

Méthode $p-1$ de Pollard revisitée. Soit $N = pq$, le théorème des restes chinois donne l'isomorphisme

$$(\mathbb{Z}/N\mathbb{Z})^\times \simeq (\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times$$

La méthode $p-1$ de Pollard consiste à trouver $M \geq 1$ et $a \in (\mathbb{Z}/N\mathbb{Z})^\times$ tels que $a^M \equiv 1 \pmod{p}$ et $a^M \not\equiv 1 \pmod{q}$

Méthode ECM. Soit $E : y^2 = x^3 + ax + b$ une pseudo-courbe elliptique sur $\mathbb{Z}/N\mathbb{Z}$ avec $(4a^3 + 27b^2, N) = 1$. On a une application naturelle

$$E(\mathbb{Z}/N\mathbb{Z}) \to E(\mathbb{F}_p) \times E(\mathbb{F}_q)$$

La méthode ECM de Lenstra consiste à trouver $M \geq 1$ et $P \in E(\mathbb{Z}/N\mathbb{Z})$ tel que $M \cdot P = O$ dans $E(\mathbb{F}_p)$ et $M \cdot P \neq O$ dans $E(\mathbb{F}_q)$

Avantages. Plus de choix de groupes donc plus de chance de trouver un groupe de cardinal B-friable

Méthode ECM de Lenstra

Algorithme.

(1) Prendre $(x, y, a) \in \{0, \ldots, N-1\}^3$ au hasard

(2) Faire $b \leftarrow y^2 - x^3 - ax \mod N$

(3) Calculer $d \leftarrow (4a^3 - 27b^2, N)$ et si $d = N$ alors retourner en 1

(4) Si $d \neq 1$ alors retourner d et terminer

(5) Faire $E \leftarrow y^2 = x^3 + ax + b$, $P \leftarrow (x, y)$

(6) Pour tous les premiers $p \leq B$, Faire

  (a) Trouver $e \geq 1$ maximal tel que $p^e \leq B$

  (b) Faire $P \leftarrow p^e \cdot P$ dans $E(\mathbb{Z}/N\mathbb{Z})$ si possible. Sinon, on a trouvé d tel que d n'est pas inversible modulo N, renvoyer (d, N) et terminer

(7) Retourner en 1 après avoir éventuellement augmenté B

Complexité. $O(B^{1+\varepsilon})$ exponentiations dans $E(\mathbb{Z}/N\mathbb{Z})$ pour chaque courbe

Méthode ECM de Lenstra : Complexité

Problème. Soit P un point au hasard sur une pseudo-courbe elliptique aléatoire E définie modulo N. Quelle est la probabilité que l'ordre de P dans $E(\mathbb{F}_p)$ est B-friable alors que l'ordre de P dans $E(\mathbb{F}_q)$ ne l'est pas ?

Réduction. On ignore la deuxième condition qui est très improbable si la première est vérifiée

Les bonnes courbes. Par le théorème de Lenstra, la probabilité qu'un courbe sur $\mathbb{F}_p$ prise au hasard soit d'ordre B-friable est plus grande que

$$\mathrm{prob}(B) = c \cdot \mathrm{card}\mathcal{S} \cdot \frac{p^{3/2}}{\log p} \cdot \frac{1}{p^2} \approx c \cdot \frac{\psi(\frac{3}{2}p, B) - \psi(\frac{1}{2}p, B)}{\sqrt{p}\log p}$$

avec $\mathcal{S}$ l'ensemble des entiers B-friables entre $p+1-2\sqrt{p}$ et $p+1+2\sqrt{p}$

Optimisation. Le coût de l'algorithme pour une courbe est de l'ordre de B opérations dans le groupe des points, donc on cherche à minimiser $B/\mathrm{prob}(B)$. On trouve $B = L(1/2, \sqrt{2}/2 + \varepsilon; p)$. La complexité finale est sous-exponentielle en la taille de p : $O(L(1/2, \sqrt{2} + \varepsilon; p)$

Amélioration. Comme pour la méthode $p-1$ de Pollard, il est possible de faire un second stage

Méthode ECM de Lenstra : Un exemple

On factorise $N = 3\,549\,331\,957$. On prend $a = 1\,078\,104\,638$, $x = 317\,359\,960$ et $y = 983\,830\,906$

Donc on trouve $b = y^2 - x^3 - ax \mod N = 1\,587\,719\,826$

On considère les multiples du point $P = (317\,359\,960, 983\,830\,906)$ sur la pseudo-courbe $E : y^2 = x^3 + 1\,078\,104\,638x + 1\,587\,719\,826$ définie modulo N

On prend $B = 1\,000$

- $P \leftarrow 2^9 \cdot P = (701\,738\,352, 991\,959\,613)$
- $P \leftarrow 3^6 \cdot P = (879\,549\,846, 58\,668\,168)$
- $P \leftarrow 5^4 \cdot P = (1\,040\,814\,202, 724\,918\,949)$
- $P \leftarrow 7^3 \cdot P$ impossible car $1\,050\,050\,212$ n'est pas inversible modulo N

En effet, on obtient $(1\,050\,050\,212, N) = 26\,861$ et la factorisation $N = 26\,861 \cdot 132\,137$

Crible du corps de nombres

Idée. Soit $f(X) \in \mathbb{Z}[X]$, unitaire et irréductible, et soit $m \in \mathbb{Z}$ tel que $f(m) \equiv 0 \pmod{N}$. On pose $\alpha = \bar{X}$ dans $\mathbb{Z}[X]/(f(X))$ et donc cet anneau est $\mathbb{Z}[\alpha]$

On pose $\phi : \mathbb{Z}[\alpha] \to \mathbb{Z}/N\mathbb{Z}$ définie par $\phi(P(\alpha)) = \overline{P(m)}$. C'est un morphisme d'anneaux

On va trouver $P(X) \in \mathbb{Z}[X]$ tel que $P(\alpha) = \gamma^2 \in \mathbb{Z}[\alpha]$ et $P(m) = b^2 \in \mathbb{Z}$. Si on pose $a = \phi(\gamma)$, on a alors

$$a^2 \equiv \phi(\gamma)^2 \equiv \phi(\gamma^2) \equiv \phi(P(\alpha)) \equiv P(m) \equiv b^2 \pmod{N}$$

d'où une possible factorisation de N

Méthode. On va cribler à la fois les valeurs $u - v\alpha$ dans $\mathbb{Z}[\alpha]$ et les valeurs $u - vm$ dans $\mathbb{Z}$

Avantages. Les valeurs à cribler sont plus petites donc plus probables à être friables donc il est plus facile à trouver la relation souhaitée. On peut montrer que la complexité est $L(1/3, \beta; N)$ avec $\beta > \sqrt[3]{32/9}$

Crible du corps de nombres

Construction de f. On prend $d \geq 5$ tel que $\frac{3}{2}(d/\log 2)^d < N$ et on pose $m = \lfloor N^{1/d} \rfloor$. On écrit le développement de N en base m

$$N = \lambda_d m^d + \lambda_{d-1} m^{d-1} + \cdots + \lambda_0$$

On peut montrer que $\lambda_d = 1$ et on pose

$$f(X) = X^d + \lambda_{d-1} X^{d-1} + \cdots + \lambda_0$$

Clairement, $f(m) = N$ et si $f(X) = P(X)Q(X)$ n'est pas irréductible alors on a une factorisation $N = P(m)Q(m)$

Norme. Soit $\alpha_1, \ldots, \alpha_d \in \mathbb{C}$ les racines de f. Pour $\beta = P(\alpha) \in \mathbb{Z}[\alpha]$, on pose

$$\mathcal{N}\beta = \prod_{i=1}^{d} P(\alpha_i) \in \mathbb{Z}$$

Remarque. Si $\beta \in \mathbb{Z}[\alpha]$ est un carré, alors $\mathcal{N}\beta$ est un carré dans $\mathbb{Z}$

Crible du corps de nombres : Criblage

On a pour $u, v \in \mathbb{Z}$

$$\mathcal{N}(u - v\alpha) = \prod_{i=1}^{d}(u - v\alpha_i) = v^d \prod_{i=1}^{d}(u/v - \alpha_i) = v^d f(u/v) = F(u, v)$$

où $F(X, Y) = Y^d f(X/Y)$ est l'homogénéisé de f.
On pose $G(X, Y) = X - Ym$
On crible pour trouver les $|a|, |b| \leq M$ tels que $F(a, b)$ et $G(a, b)$ sont B-friables
Par algèbre linéaire, on en déduit des a_i, b_i tels que

$$\prod(a_i - b_i\, m) \text{ est un carré dans } \mathbb{Z} \text{ et}$$
$$\prod \mathcal{N}(a_i - b_i\, \alpha) = \mathcal{N}\left(\prod(a_i - b_i\, \alpha)\right) \text{ est un carré dans } \mathbb{Z}$$

Problèmes. On peut avoir que $\mathcal{N}(\beta)$ est un carré sans que β soit un carré, et si c'est un carré, la racine carrée n'est pas forcément dans $\mathbb{Z}[\alpha]$ et surtout comment calculer cette racine carrée dans un anneau non factoriel ?

Crible du corps de nombres : Anneau d'entiers

Définition. Notons $K = \mathbb{Q}(\alpha)$. Alors

$$\mathcal{O}_K = \{\beta \in K \text{ tel que le polynôme minimal de } \beta \text{ est dans } \mathbb{Z}[X]\}$$

est un sous-anneau de K appelé l'anneau des entiers de K

Résultats. $\mathcal{O}_K$ est un anneau de Dedekind, en général non principal, et on a $\mathbb{Z}[\alpha] \subset \mathcal{O}_K$ et $f'(\alpha)\mathcal{O}_K \subset \mathbb{Z}[\alpha]$

Solutions. Si $\beta = \gamma^2$ avec $\gamma \in \mathcal{O}_K$ alors $f'(\alpha)^2\beta = (f'(\alpha)\gamma)^2$ et $f'(\alpha)\gamma \in \mathbb{Z}[\alpha]$

Problèmes. Soit β tel que $\mathcal{N}(\beta)$ est un carré, il faut tester si vraiment $\beta = \gamma^2$ et si oui, calculer γ

Crible du corps de nombres : Racines carrées dans $\mathbb{Z}[\alpha]$

Définition. On dit qu'un nombre premier ℓ est de degré 1 si ℓ ne divise pas le discriminant de f et si il existe s_ℓ un entier tel que $f(s_\ell) \equiv 0 \pmod{\ell}$. On a alors nécessairement $f'(s_\ell) \not\equiv 0 \pmod{\ell}$.

Théorème.

Soient $a_i, b_i \in \mathbb{Z}$ tels que $f'(\alpha)^2 \prod(a_i - b_i\alpha)$ est un carré dans $\mathbb{Z}[\alpha]$ et soit ℓ un premier de degré 1 qui ne divise aucun des $\mathcal{N}(a_i - b_i\alpha)$. Alors

$$\prod \left(\frac{a_i - b_i s_\ell}{\ell}\right) = 1$$

Idée. On ajoute des premiers ℓ_j de degré 1 – assez grands pour ne pas diviser aucun des $\mathcal{N}(a_i - b_i\alpha)$ considérés – au vecteur du crible et on ne garde que les valeurs qui vérifient aussi les conclusions du théorème

Calcul de la racine carrée. On détermine la racine carrée modulo ℓ, premier de degré 1, et on effectue un relèvement de Hensel

Crible du corps de nombres : Cas particuliers

Idée. Optimiser les choix du polynôme f et de l'entier m tels que $f(m) \equiv 0 \pmod{N}$ si on cherche à des factoriser des nombres de forme particulières

Nombres de Cunningham. $b^k \pm 1$ avec $b = 2, 3, 5, 6, 7, 10, 11, 12$ (généralise nombre de Fermat $2^k + 1$)

Exemple. Pour $N = F_9 = 2^{2^9} + 1 = 2^{512} + 1 =$ 13407807929942597099574024998205846127479365820592393377723561443721764030073546976801874298166903427690031858186486050853753882811946569946433649006084097,

on peut utiliser $f(X) = X^5 + 8$ et $m = 2^{103}$

Plus généralement, pour $b^k \pm 1$, si on veut un polynôme de degré d, on écrit $k = dl + r$, la division euclidienne, et on prend $f(X) = X^d \pm b^{d-r}$ et $m = b^{l+1}$. On a alors

$$f(m) = (b^{l+1})^d \pm b^{d-r} = b^{d(l+1)} \pm b^{d-r} = b^{d-r}(b^k \pm 1)$$

Exemple. $N = 10^{193} - 1 = 9 \cdots 9$ (193 neufs), le choix ci-dessus donne $X^5 - 100$ et $m = 10^{39}$. On remarque que $10^{193} \equiv 1 \pmod{N}$ donne $(10^{64})^3 \equiv 10^{-1} \pmod{N}$ et donc $(6 \cdot 10^{64})^3 \equiv 6^3 \cdot 10^-1 \equiv 108 \cdot 5^{-1} \pmod{N}$ et ainsi un meilleur choix $f(X) = 5X^3 - 108$ et $m = 6 \cdot 10^{64}$