UNIVERSITE D'ANTANANARIVO

Faculté des Sciences

Département de Mathématiques et Informatique

FACTORISATION DES GRANDS NOMBRES

Mémoire pour l'obtention d'un Diplôme d'Etudes Approfondis
présenté publiquement par RASAMIMANANTSOA Victor

21 mars 2006

President de jury : Pr. Michel RAJOELINA
Directeur de Mémoire : Dr. RAZAFIMANANTSOA Gérard
Examinateur : Dr. Daniel RASOAMIARAMANANA

REMERCIEMENTS

Ce mémoire n'aurait jamais vu le jour sans la grâce de Dieu que je tiens à remercier en premier lieu. Je voudrais remercier également mon directeur de mémoire, Docteur Gérard Razafimanantsoa pour ses nombreuses suggestions ainsi que ses commentaires utiles qui m'ont aidé à réaliser ce mémoire. De plus, je voudrais souligner la qualité de son enseignement, lequel a suscité mon intérêt pour le domaine de la Théorie des nombres. J'aimerais aussi remercier le Président du jury Professeur Michel Rajoelina, pour ses bons conseils et l'Examinateur, Docteur Daniel Rasoamiaramanana , pour avoir consacré son temps à donner une bonne orientation nécessaire à ce travail. Enfin, je remercie mon épouse, mon fils et ma fille, qui ont su créer autour de moi une ambiance favorable à l'écriture.

TABLE DES MATIÈRES

NOTATIONS

Symbole	Signification
$w(N)$	nombre des différents facteurs premiers de N
$o\left(f(x)\right)$	plus petit que $\epsilon f(x),\ \text{quand } \epsilon \to 0,\ x \to \infty$: $h(x) = o\left(f(x)\right)$ si $\lim_{x\to\infty} \frac{h(x)}{f(x)}$ existe et est égal à 0
$O\left(f(x)\right)$	plus petit que $Cf(x),\ \text{pour un } C > 0,\ x \to \infty$: $h(x) = O\left(f(x)\right)\ (x \to \infty)$ si $\exists C, x_0$ tels que $\lvert h(x)\rvert < Cf(x)(\forall x > x_0)$
$\Omega\left(f(x)\right)$	plus grand que $Cf(x),\ \text{pour un } C > 0,\ x \to \infty$: $h(x) = \Omega\left(f(x)\right)$ s'il existe un $\epsilon > 0$ et $x_1, x_2, x_3, \ldots \to \infty$ tels que $\forall j\ \lvert h(x_j)\rvert > \epsilon(f(x_j)$
$\pi(x)$	nombre des premiers $\leq x$
$\left(\frac{a}{b}\right)$	symbole de Legendre
$\text{pgcd}(a, b)$	plus grand diviseur commun de a et de b
$\text{ppcm}(a, b)$	plus petit multiple commun de a et de b
$f(x) \approx g(x)$	$f(x)$ est approximativement égal à g(x)
$[x]$	partie entière de x
$\lvert\phi\rangle$	état quantique de ϕ
$\prod$	symbole de produit : $\prod_{i=0}^{n} a^i = a_0 \cdot a_1 \cdot \cdots \cdot a_n$
$\sum$	symbole de sommation : $\sum_{i=0}^{n} a^i = a_0 + a_1 + \cdots + a_n$
$\sharp A$	cardinal d'un ensemble fini d'éléments A

INTRODUCTION

Le nombre de 129 chiffres $n = 114381625757888867669235779976146612010218296721242362562561842935706935245733897830597123563958705058989075147599290026879543541$ est un produit de deux nombres premiers ; lesquels ? Ce défi a été lancé aux lecteurs de *Pour la science de 1977* par les concepteur de RSA. Il a fallu 8 mois avec des milliers d'ordinateurs en réseaux pour factoriser ce nombre :

$$n = 3490529510847650949147849619903898133417764638493387843990820577 \times 327691329932667095499619881908344614131776429679929425397982885 33$$

Tout entier naturel N se décompose de manière unique en facteurs premiers : $N = \prod_{i=1}^{s} p_i^{\alpha_i}$ où les p_i sont des nombres premiers deux à deux distincts et $\alpha_i > 0$ pour tout i. Mais la démonstration de cette propriété ne donne aucun moyen pour trouver ces facteurs premiers. Il est donc facile de montrer qu'un nombre est composé en utilisant le test de composition [Coh93, p.415 section 8.2], mais pour determiner ses facteurs, cela demande une bonne méthode efficace de factorisation. La cryptographie ou communication sécurisée d'information se base généralement par l'utilisation d'une fonction trappe : cette une opération facile dans un sens et épineuse dans l'autre. On a besoin en général soit beaucoup de temps, soit d'aide ou des informations supplémentaires pour revenir en arrière. Cette aide est appelée la clef. Le processus Multiplication-Factorisation peut être considéré comme une fonction trappe car une factorisation d'un nombre de 250 chiffres reste encore du domaine de rêve actuellement.

La principale victime des avancées des algorithmes de factorisations : c'est le cryptographie qui , d'année en année, se voit obliger d'augmenter la taille de ses clefs. Heureusement que les tests de primalités sont bien plus rapides que les différentes méthodes de factorisations dit Morin. En effet, c'est bien à ce niveau que se joue l'avenir de la cryptographie, du moins de RSA (voir [RSA78]). Alors, le problème de factorisation des *grands nombres* a un énorme intérêt pour le gouvernement, les institutions financières qui font une transaction par internet, les organismes oeuvrant dans la communication,..., qui veulent tous protéger leurs messages secrets et ses authenticités.

Dans ce mémoire, notre travail se focalise tout simplement sur la méthode de factorisation des *grands nombres*. Signalons aussi que nous ne traitons pas dans ce mémoire la méthode de factorisation utilisant le crible de corps des nombres (NFS) car elle seule peut constituer un sujet d'un mémoire.

I. PRÉLIMINAIRES

1. Notion de divisions

Soient n et m deux entier positifs. Diviser n par m, c'est trouver un entier $q \geq 0$ (quotient) et un entier r (reste) tels que $0 \leq r < m$ et $n = mq + r$. On écrit aussi $r \equiv n \pmod{m}$. Si $r = 0$, on dit que m divise n ou m est un *diviseur* de n et on note $m \mid n$. Un nombre *premier* est un entier $p > 1$ qui n'est divisible que par 1 et par lui-même. Si n n'est pas premier , on dit que n est *composé*. Si n n'est pas premier, factoriser n, c'est trouver deux entiers $u > 1$ et $v > 1$ tels que $n = u \cdot v$. Un entier positif factorisable est un entier composé. Soient n et m deux entiers positifs. Le plus grand diviseur commun de n et m noté $\text{pgcd}(n, m)$ est l'entier d tel que :

- d divise n et d divise m.
- Si k divise n et k divise m et d est divisible par tous diviseurs communs de n et m.

Si $\text{pgcd}(n, m) = 1$, on dit que n et m sont premiers entre eux.

2. Théorème fondamental de l'arithmétique

Théorème 2.1. *Tout entier positif* > 1 *peut s'exprimer de manière unique en un produit des facteurs premiers.*

Lemme 2.2. *Le plus petit diviseur différent de* 1 *d'un entier est un nombre premier.*

Preuve. Soit p le plus petit diviseur de a où $p \neq 1$. Si p est premier on a le résultat . Si p est composé, on peut écrire $p = st$ où $s \neq 1$ et $t \neq 1$, comme $p \mid a$ alors $st \mid a$ et $s \mid a$ avec $s < p$, ce qui est absurde car p le plus petit diviseur de a . □

Preuve. Soit n un entier non nul et différent de 1 : si n est premier , on a le résultat, sinon n admet un diviseur d tel que $1 < d < n$. Soit p_1 le plus petit de ses diviseurs, d'après le lemme 2.2, p_1 est premier et $n = p_1 m_1$ avec $1 < m_1 < n$; si m_1 est premier on a le résultat, sinon m_1 est composé et on applique la même méthode à m_1, on aura m_2 tel que $1 < m_2 < m_1$ et $m_1 = p_2 m_2$ où p_2 est le plus petit diviseur de m_1, donc p_2 est premier. On a donc une suite d'entiers $(m_i)_i$, strictement décroissante dont les terms sont strictement plus grand que 1, nécessairement cette suite s'arrête. D'où n s'exprime sous la forme :

$$n = \prod_{i=1}^{s} p_i^{\alpha_i}$$

Si $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} = q_1^{\beta_1} q_2^{\beta_2} \cdots q_t^{\beta_t}$ où les p_i et q_j sont premiers vérifiant $p_i < p_{i+1}$ et $q_j < q_{j+1}$, alors p_i divise $q_1^{\beta_1} q_2^{\beta_2} \cdots q_t^{\beta_t}$. Donc p_i divise l'un des q_j et par suite p_i est l'un des q_j. Supposons qu'il existe $m > 1$ tel que $p_1 \mid q_m^{\beta_m}$ donc $p_1 \mid q_m$ et $p_1 = q_m$, donc il existe $s > 1$ tel que $p_s \mid q_1^{\beta_1}$ c'est-à-dire $p_s \mid q_1$ et $p_s = q_1$. Comme on a imposé l'ordre (ordre croissant), $q_m = p_1 < p_s = q_1$, cela donne $q_m < q_1$, ce qui est impossible car $m > 1$ donc $m = 1$, c'est à dire $p_1 \mid q_1^{\beta_1}$ et $p_1 = q_1$ appliquons la même méthode pour $p_2 = q_2$, ... , $p_r = q_r$, donc $r = t$ et chaque p est q, et chaque q est p. Si $\alpha_j > \beta_j$, en divisant par $p_j^{\beta_j}$, on a $p_1^{\alpha_1} \cdots p_j^{\alpha_j - \beta j} p_{j+1}^{\alpha_{j+1}} \cdots p_r^{\alpha_r} = p_1^{\beta_1} \cdots p_{j-1}^{\beta_{j-1}} p_{j+1}^{\beta_{j+1}} \cdots p_r^{\beta_r}$ avec $\alpha_j - \beta_j > 0$, dans ce cas p_j divise le nombre de droite, ce qui est impossible car les p_i sont premiers pour tout i. De la même manière pour $\alpha_j < \beta_j$, donc $\alpha_j = \beta_j$. D'où l'unicité de cette expression. □

Théorème 2.3 (Euclide d'Alexandrie, 365-300 A.C., Grèce)**.** *Il existe une infinité de nombres premiers.*

Preuve. Supposons qu'il n'existe seulement que n nombres premiers, notés $p_1, p_2, \ldots, p_n$. Considérons $N = p_1 p_2 \cdots p_n + 1$. Si N est composé alors il existe un $p_{i_0} \in \{p_1, p_2, \ldots, p_n\}$ qui divise N , cela revient à dire $p_{i_0} | 1$ car $N - p_{i_0}(p_1 p_2 \cdots p_{i_0-1} p_{i_0+1} \cdots p_n) = 1$, ce qui n'a pas de sens ; donc N est premier auquel cas on a une contradiction puisque $N > p_n$. Dans les deux cas, on obtient une contradiction, ainsi l'infinitude des nombres premiers est démontrée. □

3. Algorithme d'Euclide

Soient a et $b > 0$ entiers ,divisons a par b, on a $a = bq + r$ avec $0 \leq r < b$, si $r > 0$ divisons b par r, cela nous amène à trouver les équations suivantes :

$$\begin{cases} a = bq_1 + r_2 & \text{avec } 0 \leq r_2 < b \\ b = r_2 q_2 + r_3 & \text{avec } 0 \leq r_3 < r_2 \\ r_2 = r_3 q_3 + r_4 & \text{avec } 0 \leq r_4 < r_3 \\ \vdots & \vdots \\ r_{n-1} = r_n q_n + r_{n+1} & \text{avec } 0 \leq r_{n+1} < r_n \\ r_n = r_{n+1} q_{n+1} + r_{n+2} & \text{avec } r_{n+2} = 0 \end{cases}$$

Posons $r_0 = a$ et $r_1 = b$, donc $b = r_1 > r_2 > r_3 > \cdots$, la suite des entiers positifs $(r_n)_n$ est strictement décroissante, elle s'arrête nécessairement en 0. Si $r_{n+2} = 0$ dans cet algorithme, alors $\text{pgcd}(a, b) = r_{n+1}$. Pour le prouver il suffit d'utiliser les deux propriétés suivantes :

(i) Soient a et $b \in \mathbb{Z}$, si $a = bq + r$ avec $0 \leq r < b$, alors $\text{pgcd}(a, b) = \text{pgcd}(b, r)$ c'est-à-dire $\text{pgcd}(a, b) = \text{pgcd}(b, a \pmod b)$.

(ii) Si $r_n = r_{n+1} q_{n+1}$ c'est-à-dire $r_{n+2} = 0$, alors $\text{pgcd}(r_{n+1}, r_{n+2}) = \text{pgcd}(r_{n+1}, 0) = r_{n+1}$.

4. Analyse de la complexité de l'algorithme d'Euclide

Estimons maintenant le nombre d'étapes pour calculer $\text{pgcd}(a,b)$.

Proposition 4.1. *Le calcul de* $\text{pgcd}(a,b)$ *nécessite au plus* $2\log_2(\max\{2a,2b\})$ *opérations élémentaires.*

Preuve. Montrons tout d'abord que $r_{i+1} \leq \frac{1}{2}r_{i-1}$ où les r_i sont les restes successifs.
En effet, si $r_i \leq \frac{1}{2}r_{i-1}$ on a le résultat car $r_{i+1} < r_i$. Si $r_i > \frac{1}{2}r_{i-1}$, divisons r_{i-1} par r_i, $r_{i-1} = r_i q_i + r_{i+1}$, on a $r_{i+1} = r_{i-1} - r_i q_i < r_{i-1} - \frac{1}{2}r_{i-1}q_i$, alors $r_{i+1} < r_{i-1}(1 - \frac{q_i}{2})$
$q_i \neq 0$, sinon $r_{i+1} = r_{i-1}$, ce qui est en contradiction avec $(r_n)_n$ est strictement décroissante, donc $q_i \geq 1$, plus exactement $q_i = 1$, par suite $r_{i+1} \leq \frac{1}{2}r_{i-1}$.
Nous admettons que $a \geq b$, sinon on peut les intervertir. On a :

$$r_2 < b,\ r_4 < \frac{1}{2}b,\ r_6 < \frac{1}{2}r_4 < \frac{1}{2^2}b,\ r_8 < \frac{1}{2}r_6 < \frac{1}{2^3}b,\ \cdots,\ r_{2i} < \frac{1}{2^{i-1}}b$$

Quand $2^{i-1} \geq b$, on a $0 \leq r_{2i} < 1$, alors $r_{2i} = 0$ car r_{2i} est un entier. Autrement dit, si $i \geq 1 + \log_2 b = \log_2(2b)$ implique $r_{2i} = 0$. Donc le calcul de $\text{pgcd}(a,b)$ avec l'algorithme euclidien comprend au plus $2\log_2(2b)$ étapes. Comme la variation logarithmique est très lente, cela rend pratique le calcul de pgcd même avec des a, b assez grands. □

Remarque 4.2. Si $n = \prod_{i=1}^{s} p_i^{\alpha_i}$, on a $d(n) = \prod_{i=1}^{s}(1+\alpha_i)$ où $d(n)$ est le nombre de diviseur de n qui ne peut obtenir qu'à partir de la décomposition en facteur premier de n.

5. Petit théorème de Fermat

Théorème 5.1. *Soient n un entier positif et a un entier tels que* $\text{pgcd}(a,n) = 1$ *alors* $a^{\varphi(n)} \equiv 1 \pmod{n}$ *où* $\varphi(n) = \#\{a \in \mathbb{Z} \mid \text{pgcd}(a,n) = 1 \text{ avec } a < n\}$.

Preuve. Soit k l'ordre de a dans $(\mathbb{Z}/n\mathbb{Z})^*$, nous savons que k est le plus petit entier positif tel que $a^k \equiv 1 \pmod{n}$, et comme $\varphi(n) = \#\{a \in \mathbb{Z} \mid \text{pgcd}(a,n) = 1\} = \#(\mathbb{Z}/n\mathbb{Z})^*$, d'après le Théorème de Lagrange sur le groupe fini, k divise $\varphi(n)$, c'est-à-dire $\varphi(n) = kd$ pour un entier d et on a $a^{\varphi(n)} = a^{kd} = \left(a^k\right)^d \equiv 1 \pmod{n} \equiv 1 \pmod{n}$. □

Remarque 5.2. Si p est premier et $\text{pgcd}(a,p) = 1$ alors $a^{\varphi(p)} \equiv 1 \pmod{p}$, c'est-à-dire $a^{p-1} \equiv 1 \pmod{p}$. Autrement dit si $\text{pgcd}(a,n) = 1$ et $a^{n-1} \neq 1 \pmod{n}$, alors n est composé.

6. Détection d'une puissance d'un nombre premier

Si p est premier et $\text{pgcd}(a,p) = 1$ alors $a^{p-1} \equiv 1 \pmod{p}$, ou encore $a^p - a \equiv 0 \pmod{p}$. En s'inspirant à ce résultat, nous avons un algorithme pouvant verifier si n est une puissance de nombre premier [Coh93], c'est-à-dire si $n = p^\alpha$, en analysant $\text{pgcd}(a^n - a, n) = P$:

(i) Initialiser $a = 1$

(ii) Mettre $a \leftarrow a + 1$ et calculer $b \leftarrow a^n \pmod{n}$. Et puis, calculer $P \leftarrow \text{pgcd}(b - a, n)$

(iii) Si $P = 1$, n n'est pas de la forme p^α et l'algorithme est terminée.

(iv) Si $P > 1$, testons si n est composé en utilisant un test de composition [Coh93, p.415 section 8.2] , le cas échéant retourner à *(ii)*.

(v) Si P est premier, divisons successivement n par P.

7. Estimation de la grandeur des facteurs

Remarque 7.1. $\left[\frac{X}{p}\right]$ est égal au nombre d'entiers divisibles par p dans l'intervalle $[1, X]$. Comme tous les nombres composés dans $[1, X]$ admet un facteur inférieur ou égal à $\sqrt{X}$, alors il y a approximativement $\sum_{p_i \leq \sqrt{X}} \left[\frac{X}{p_i}\right]$ multiples des premiers inferieur ou égal à $\sqrt{X}$ dans $[1, X]$.

Remarque 7.2. Notons $\omega(N)$ le nombre de différents facteurs premiers de N. Soit $\epsilon > 0$, et soit $F(N)$ le nombre de $x \leq N$ ne vérifiant pas $(1-\epsilon) \ln\ln N \leq \omega(N) \leq (1+\epsilon) \ln\ln N$. On a $F(N) = o(N)$ [HW79, p.356]. C'est-à-dire que dans la plus part de cas $\omega(N) \approx (\ln\ln N)$.

Posons $N = p_s(N)p_{s-1}(N)\cdots p_2(N)p_1(N)$ où $p_s(N), p_{s-1}(N), \ldots, p_2(N), p_1(N)$ sont les facteurs premiers de N avec $p_s(N) \leq p_{s-1}(N) \leq \cdots \leq p_2(N) \leq p_1(N)$.
Comme $\frac{N}{p_1(N)}$ a seulement$(s-1)$ facteurs premiers, alors

$$\begin{aligned}(s-1) \approx \ln\ln\frac{N}{p_1(N)} &= \ln(\ln N - \ln p_1(N)) \\ &= \ln\ln N + \ln\left(1 - \frac{\ln p_1(N)}{\ln N}\right) \\ &= s + \ln\left(1 - \frac{\ln p_1(N)}{\ln N}\right).\end{aligned}$$

Cela nous permet d'écrire

$$\ln\left(1 - \frac{\ln p_1(N)}{\ln N}\right) \approx -1$$
$$\left(1 - \frac{\ln p_1(N)}{\ln N}\right) \approx \frac{1}{e}$$
$$\ln p_1(N) \approx \left(1 - \frac{1}{e}\right) \ln N$$
$$\ln p_1(N) \approx 0,632 \ln N$$
$$p_1(N) \approx N^{0,632}$$

Donc la taille de $p_1(N)$ est 63% de la taille de N. De même , dans le cas où $p_2(N) \neq p_1(N)$, la taille de $p_2(N)$ est 63% de $p_s(N)p_{s-1}(N)\cdots p_4(N)p_3(N)p_2(N) = N_1$,

$$\begin{aligned} p_2 &\approx N_1^{0,63} \\ &\approx \left(\frac{N}{p_1}\right)^{0,63} \\ &\approx \left(\frac{N}{N^{0,63}}\right)^{0,63} \\ &\approx \left(N^{1-0,63}\right)^{0,63} \\ &\approx \left(N^{0,37}\right)^{0,63} \\ &\approx N^{0,2331} \end{aligned}$$

Donc $p_2(N) \approx N^{0,23}$, c'est-à-dire 23% de la taille de N . Et ainsi de suite pour estimer la taille des autres facteurs. Ce résultat nous permet de localiser approximativement le plus petit et le plus grand facteur de l'entier que l'on souhaite factoriser.

8. Friabilité et probabilité de friabilité

8.1. Friabilité

Un entier n est dit B-friable si tous ses facteurs premiers sont inférieurs à B. C'est-à-dire que si $n = \prod_{i=1}^{s} p_i^{\alpha_i}$ est la décomposition de n en facteurs premiers, on a $p_i \leq B$ pour tout $i \in \{1, \ldots, s\}$. Soit $F = \{p_1, p_2, \ldots, p_m\}$ où les p_i sont des nombres premiers. On dit que F une *base de factorisation*. On dit qu'un entier n est *friable* dans F, si n est complètement factorisé en utilisant les éléments de F.

8.2. Probabilité de friabilité

Intuitivement, de moins le nombre est petit, de plus la probabilité de B-friabilité est grande :

Exemple 8.1. Il y a 39 nombres positifs 5-friables ≤ 143 et 29 nombres positifs 5-friables ≤ 72.

Soit n un nombre positif quelconque 5-friabilité $\leq m$ alors

- si $m = 72$, la probabilité de la friabilité de n est $\frac{29}{72} \approx 0,40$
- si $m = 143$, la probabilité de la friabilité de n est $\frac{39}{143} \approx 0,27$
- si $m = 1000$, la probabilité de la friabilité de n est $\frac{87}{1000} \approx 0,08$
- si $m = 10^6$, la probabilité de la friabilité de n est $\frac{508}{10^6} \approx 0,0005$

Cela illustre que la probabilité de friabilité varie en fonction de la taille de l'entier considéré. Nous allons introduire l'application (voir [Len00, p. 103]) :

$$L_x[u,v] = \exp\left(v(\ln x)^u (\ln\ln x)^{1-u}\right)$$

Proposition 8.2. *Soit α, β, r et s des réels tels que $\alpha,\ \beta > 0, 0 < r \leq 1$ et $0 < s < r$. Un entier positif quelconque $\leq L_x[r,\alpha]$ est $L_x[s,\beta] - friable$ avec la probabilité de la friabilité $L_x[r-s, -\alpha(r-s)/\beta + o(1)]$ quand $x \to \infty$*

Si $r = 1$ et $s = \frac{1}{2}$, un entier positif quelconque $\leq n^\alpha$ est $L_n\left[\frac{1}{2},\beta\right]$-friable avec la probabilité de la friabilité $L_n\left[\frac{1}{2}, -\alpha/(2\beta) + o(1)\right]$ quand $n \to \infty$

Remarque 8.3. La fonction L_n est utilisé pour estimer le temps d'execution d'un algorithme dans le cas où u varie de 0 à 1 :

(i) Pour $u = 0$, $L_n[0,v] = \exp(v \ln\ln n) = (\ln n)^v$: Temps polynomial.

(ii) Pour $u = 1$, $L_n[1,v] = \exp(v \ln n) = n^v$: Temps exponentiel.

(iii) Pour $0 < u < 1$ et v est constant : Temps sous-exponentiel.

II. LA COMPLEXITÉ DE L'ALGORITHME DÉPEND DE LA TAILLE DE FACTEURS

1. Méthode d'Eratosthène (Division triviale)

1.1. Efficience de la division triviale

Nous pouvons remarquer que le petit Théorème de Fermat peut tester seulement si n est composé, mais il ne donne pas les différent facteurs de n. Supposons que n est un *grand* entier composé à factoriser. On peut écrire $n = n_1 n_2$ alors $n_1 \leq \sqrt{n}$ ou $n_2 \leq \sqrt{n}$, si le plus petit facteur de n est supérieur à $\sqrt{n}$ alors n est premier ; visiblement la méthode qui semble la plus naturelle pour trouver le plus petit facteur premier de n, c'est de diviser n par les nombres entre 1 et $\sqrt{n}$, on a donc besoin de $\sqrt{n}$ d'opérations dans le pire de cas, cette méthode est appelée la méthode d'Eratosthène , elle est déterministe et qui marche avec beaucoup d'entiers car 88% d'entiers ont un facteurs < 100 et prèsque 92% ont un facteur < 1000 [Len00, p.107]. En effet , comme $\pi(100) = 25$ où $\pi(x)$ désigne le nombre des premiers inferieurs à x, nous allons noter $p_1 = 2, p_2 = 3, \cdots, p_{25} = 97$ ces 25 nombres premiers inferieurs à 100. Soit p premier :

$$
\begin{aligned}
Si\ x \equiv 0 \pmod{p}\ alors\ p \mid x \\
Si\ x \equiv 1 \pmod{p}\ alors\ p \nmid x \\
Si\ x \equiv 2 \pmod{p}\ alors\ p \nmid x \\
\cdots \\
Si\ x \equiv (p-1) \pmod{p}\ alors\ p \nmid x
\end{aligned}
$$

Dans cette présentation, il y a $\frac{1}{p}$ de chance pour que x soit divisible par p. Désignons par $T_{\overline{1,j}}$ la proportion des nombres qui ont un facteur premier dans $\{p_1, p_2, \ldots, p_j\}$:

$$
\begin{aligned}
T_{\overline{1,2}} &= \frac{1}{p_1} + \frac{1}{p_2} - \frac{1}{p_1 p_2} \\
T_{\overline{1,3}} &= T_{\overline{1,2}} + \frac{1}{p_3} - \frac{T_{\overline{1,2}}}{p_3} \\
T_{\overline{1,4}} &= T_{\overline{1,3}} + \frac{1}{p_4} - \frac{T_{\overline{1,3}}}{p_4} \\
&\cdots \\
T_{\overline{1,25}} &= T_{\overline{1,24}} + \frac{1}{p_{25}} - \frac{T_{\overline{1,24}}}{p_{25}}
\end{aligned}
$$

En remplaçant $p_1 = 2, p_2 = 3, \cdots, p_{25} = 97$ dans cette suite d'opérations, on trouve $T_{\overline{1,25}} \approx 88\%$, de la même manière pour trouver $T_{\overline{1,168}} \approx 92\%$ où $168 = \pi(1000)$.

1.2. Division triviale et le pire de cas

Seulement, il y a des cas que cette méthode d'Eratosthène qui consiste à diviser n par tous les nombres premiers inférieur à $\sqrt{n}$, n'est pas pratique :

- Soit n un entier de 60 chiffres à factoriser, nous devons diviser n par des nombres inférieur ou égal à 10^{30}, supposons qu'il n'y a que $0,1\%$ seulement parmis eux sont des nombres premiers, on a encore besoin de 10^{27} divisions à faire , admettons que l'ordinateur peut faire 10^{15} divisions par seconde, alors la factorisation se fait en 10^{12} secondes soit plus de 31000 années.
- d'après Tchebycheff , si $\pi(x)$ désigne le nombre premier inférieur à x, on a

$$\pi(x) > \frac{x}{\ln x} \cdot \ln\left(\frac{2^{\frac{1}{2}} 3^{\frac{1}{3}} 5^{\frac{1}{5}}}{30^{\frac{1}{30}}}\right)$$

Pour factoriser un nombre de 100 chiffres, produit de deux nombres de 50 chiffres, nécessiterait plus de

$$10^{50} \cdot 0,921 \left(\ln\left(10^{50}\right)\right)^{-1} = 8 \cdot 10^{47} \text{ opérations}$$

Et supposons que l'ordinateur(un super ordinateur) pourrait faire 1000 divisions par nanoseconde (10^{-9}s), alors le temps qu'il faudrait pour factoriser n est $\frac{8 \cdot 10^{47} \cdot 10^{-9}}{10^3}$ secondes $\approx 2 \cdot 10^{28}$ années, ce qui est bien plus que l'âge de l'univers !

2. Méthode $(p-1)$ de Pollard (1970)

2.1. Factorisation par la méthode $(p-1)$ de Pollard

soit n un entier que l'on souhaite factoriser, supposons que p est un facteur premier de n. Soit $a \in \{2, \ldots, n-1\}$ tel que $\text{pgcd}(a, n) = 1$ et soit K un entier tel que $p - 1 \mid K$ (c'est-à-dire $K = (p-1) \cdot m$). Comme $\text{pgcd}(a, n) = 1$ et que $p \mid n$, on a $\text{pgcd}(a, p) = 1$. Et d'après le petit théorème de Fermat (voir théorème 5.1), on a : $a^K = (a^{p-1})^m \equiv 1 \pmod{p}$, d'où $p \mid a^K - 1$. Or $p \mid n$, puis $p \mid \text{pgcd}(a^K - 1, n)$, ainsi $\text{pgcd}(a^K - 1, n) > 1$. Si l'on a de plus $a^K - 1 \neq 0 \pmod{n}$, alors $\text{pgcd}(a^K - 1, n)$ est un facteur propre de n. L'algorithme *(p-1)de Pollard* utilise une *borne de friabilité* B qui est choisie en début de calcul en posant :

$$K = \prod_{\substack{p\,:\ premier \leq B \\ s \in \mathbb{N}}} p^s \tag{2.1}$$

Si tous les facteurs de $p - 1$ sont inférieurs à B, alors on a plus de chance que $p - 1$ divise K ainsi choisi.

2.2. Algorithme de la méthode (p-1) de Pollard

Soit $n \geq 2$ un entier à factoriser :

(i) Choisir une borne B pour que si p est le facteur que l'on cherche, avec un peu de chance, tous les facteurs de $p-1$ soient plus petit que B.

(ii) Choisir un entier a tel que $1 < a < n$ et que $\text{pgcd}(a, n) = 1$.

(iii) Calculer l'entier K donné dans l'équation (2.1).

(iv) Calculer $\text{pgcd}(a^K - 1, n)$. Si $1 < \text{pgcd}(a^K - 1, n) < n$ alors $\text{pgcd}(a^K - 1, n)$ est un facteur non trivial de n. Sinon choisir une autre borne B plus grande.

Remarque 2.1. Comme K est B-friable, alors pour que $(p-1)$ ait plus de chance à diviser $K, (p-1)$ devrait être aussi B-friable. Et comme la probabilité de la friabilité de $(p-1)$ depend de la taille de p alors la rapidité de l'algorithme de $(p-1)$ de Pollard depend principalement de la taille du facteur p de n (voir Proposition 8.2).

Remarque 2.2. L'algorithme de $(p-1)$ de Pollard pourrait se terminer éventuellement parce que quand B sera égal à $\frac{1}{2}(p-1)$ pour un p qui divise n, alors $(p-1)$ divise K. Cependant si n est un très grand entier , il pourrait être très difficile de trouver K dans le cas pratique. De plus, cet algorithme a peu de chances de fonctionner, car il n'est pas fréquent que $(p-1)$ soit puissance de petits nombres premiers, d'autant que, dans les cryptosystèmes comme RSA, on fabrique l'entier n, et on peut s'arranger pour que n ne vérifie pas cette condition.

2.3. Analyse de la complexité de la méthode $(p-1)$ de Pollard

Soit n le nombre que l'on souhaite factoriser.

Proposition 2.3. *Pour calculer,* $\text{pgcd}(a^K - 1, n)$*, on a besoin de* $2\log_2 2Kn$ *opérations.*

Lemme 2.4. *Il est possible de calculer* $a^K \pmod n$ *en faisant au plus* $2\log_2 K$ *opérations où chaque opération comprend une multiplication et une congruence modulo* n*.*

Preuve. Ecrivons K en base 2, on a $K = k_0 + k_1 2^1 + k_2 2^2 + \cdots + k_r 2^r$ où $k_i = 0$ ou $k_i = 1$. Posons

$$A_0 = a$$
$$A_1 = A_0^2 = a^{2^1}$$
$$A_2 = A_1^2 = a^{2^2}$$
$$A_3 = A_2^2 = a^{2^3}$$
$$\cdots$$
$$A_r = A_{r-1}^2 = a^{2^r}$$

On peut donc écrire

$$\begin{aligned} a^K &= a^{k_0+k_1 2^1+k_2 2^2+\cdots+k_r 2^r} \\ &= a^{k_0} a^{k_1 2^1} a^{k_2 2^2} \cdots a^{k_r 2^r} \\ &= \prod_{(si\ k_i=1)} A_i \end{aligned}$$

On a alors besoin de r opérations pour calculer les A_i, et pour avoir a^K on a besoin également au plus r opérations, or $K = k_0 + k_1 2^1 + k_2 2^2 + \cdots + k_r 2^r \geq 2^r$, alors $\log_2 K \geq r$ et par suite pour calculer $a^K \pmod n$, on a besoin au plus $2\log_2 K$. □

Preuve. Revenons maintenant sur le calcul de $\text{pgcd}(a^K - 1, n)$. Pour calculer $a^K - 1$, on a besoin de $2\log_2 K$ opérations et pour l'algorithme euclidien de $\text{pgcd}(a^K - 1, n)$ selon la Proposition 4.1 au plus $2\log_2 2n$ opérations : c'est-à-dire $2\log_2 K + 2\log_2 2n = 2\log_2 2Kn$ opérations pour calculer $\text{pgcd}(a^K - 1, n)$. Cela est extrêmement pratique même avec un K assez grand comme 10^{1000}. □

Exemple 2.5. Nous allons factoriser $n = 246082373$. La première chose à faire c'est de tester si n est composé en utilisant le petit théorème de Fermat,

$$2^{246082373-1} = 2^{n-1} \neq 1 \pmod{246082373}$$

Donc n est composé. Mettons $a = 2$ et $K = 2^2 \cdot 3^2 \cdot 5 = 180$ 5-friables, cela nous permet d'écrire
$180 = 2^2 + 2^4 + 2^5 + 2^7$, et de calculer $2^{2^i} \pmod n$ pour $0 \leq i \leq 7$. Les résultats sont donnés dans le tableau suivant : Cela nous donne

i	$2^{2^i} \pmod{246082373}$
0	2
1	4
2	16
3	256
4	65536
5	111566955
6	166204404
7	214344997

Tab. II.1: Valeurs de $2^{2^i} \pmod n$ pour $0 \leq i \leq 7$

$$\begin{aligned} 2^{180} &= 2^{2^2+2^4+2^5+2^7} \\ 2^{180} &\equiv 16 \cdot 65536 \cdot 111566955 \cdot 214344997 \pmod{246082373} \\ 2^{180} &\equiv 121299227 \pmod{246082373} \end{aligned}$$

et $\text{pgcd}(2^{180}-1, n) = \text{pgcd}(121299226, 246082373) = 1$, cela veut dire que n n'a aucun facteur premier p tel que $(p-1)$ divise 180, dans ce cas, choisissons donc un autre K, 7-friables :

$$\begin{aligned} K &= 2^3 \cdot 3^2 \cdot 5 \cdot 7 \\ K &= 2520 \end{aligned}$$

et comme $2^{2520} = 2^3 + 2^4 + 2^6 + 2^7 + 2^8 + 2^{11}$, nous avons encore besoin de calculer $2^{2^i} \pmod n$ pour $8 \leq i \leq 11$:

i	$2^{2^i} \pmod{246082373}$
8	111354998
9	82087367
10	7262569
11	104815687

Tab. II.2: Valeurs de $2^{2^i} \pmod n$ pour $8 \leq i \leq 11$

cela nous donne

$$\begin{aligned} 2^{2520} &= 2^{2^3+2^4+2^6+2^7+2^8+2^{11}} \\ 2^{2520} &\equiv 101220672 \pmod{246082373} \end{aligned}$$

et $\text{pgcd}(2^{2520}-1, n) = \text{pgcd}(101220671, 246082373) = 2521$, finalement on trouve $n = 246082373 = 2521 \cdot 97613$

3. Méthode de factorisation par des Courbes Elliptiques de H. Lenstra (1987)

3.1. Courbes elliptiques : définitions et propriétés

Définition 1. (Plan projectif). On appelle plan projectif sur un corps $\mathbb{K}$, l'ensemble noté $\mathbb{P}^2(\mathbb{K})$, des classes d'équivalence $\left(\mathbb{K}^3 \setminus \{(0,0,0)\}\right) / \mathcal{R}$, où $\mathcal{R}$ est une relation d'équivalence définie par :

$$\forall \left((a,b,c), (a',b',c')\right) \in \left(\left(\mathbb{K}^3 \setminus \{(0,0,0)\}\right)^3\right)^2 ,$$
$$(a,b,c)\, \mathcal{R}\, (a',b',c') \Leftrightarrow \left[\exists t \in \mathbb{K} \setminus \{0\} \ , (a,b,c) = t\,(a',b',c')\right]$$

Définition 2. (Courbe elliptique). On appelle courbe elliptique sur un corps $\mathbb{K}$, notée $E(\mathbb{K})$, une courbe cubique dans le plan projectif $\mathbb{P}^2(\mathbb{K})$ définie par $F(X,Y,Z) = 0$ où F est un polynôme de degré 3, homogène en trois variables, à coefficients dans $\mathbb{K}$:

$$\begin{aligned} F(X,Y,Z) = \alpha_1 X^3 + \alpha_2 Y^3 + \alpha_3 Z^3 + \alpha_4 X^2 Y + \alpha_5 X^2 Z + \\ + \alpha_6 Y^2 X + \alpha_7 Y^2 Z + \alpha_8 Z^2 X + \alpha_9 Z^2 Y + \alpha_{10} XYZ = 0 \end{aligned}$$

et munie d'une origine $\mathcal{O} \in E(\mathbb{K})$.

Remarque 3.1. Dans la suite, nous nous intéresseront aux courbes elliptiques non singulières c'est à dire :

$$\forall P \in E(\mathbb{K}) \ , \ \left(\frac{\partial F}{\partial X}(P), \frac{\partial F}{\partial Y}(P), \frac{\partial F}{\partial Z}(P) \right) \neq (0,0,0)$$

définies sur un corps $\mathbb{K}$ de caractéristique différente de 2 ou 3,. Lors qu'il n'y a pas d'ambiguité sur le corps, nous noterons indifféremment les courbes $E(\mathbb{K})$ ou E.

Proposition 3.2. *Soit E une courbe elliptique. On peut se ramener à une équation de E, dite forme courte de Weiestrß :*

$$E : Y^2Z = X^3 + aXZ^2 + bZ^3$$

On peut alors écrire cette équation en coordonnées non homogènes en posant $x = \frac{X}{Z}$ et $y = \frac{Y}{Z}$:

$$E : y^2 = x^3 + ax + b \text{ avec } 4a^3 + 27b^2 \neq 0$$

plus le point $\mathcal{O} = (0,1,0)$ qui est le seul point à l'infini $(Z = 0)$ et que l'on choisit comme origine.

3.2. Structure de groupe abélien

Proposition 3.3. *Soit E une courbe elliptique et D une droite définies sur un corps $\mathbb{K}$. Si E a au moins deux points d'intersection (comptés avec leurs multiplicité) avec la droite D, alors E a exactement trois points d'intersection (comptés avec leurs multiplicité) avec la droite D.*

Approche géométrique de la loi de la sécante-tangente

Soit E une courbe elliptique définie sur $\mathbb{P}^2(\mathbb{K})$. On peut définir sur E une loi de composition $*$ dite loi de composition de la sécante-tangente :

- si $(P,Q) \in E^2$ avec $P \neq Q$, on définit $P * Q$ comme étant le troisième point d'intersection de la droite D passant par P et Q avec E ;
- si $P \in E$, on définit $P * P$ comme étant le troisième point d'intersection de la droite D tangente à la courbe en P avec E (P est alors consideré comme un point double d'intersection).

Expression analytique de la loi $*$

Soit E une courbe elliptique définie par :

$$E : f(x,y) = y^2 - \left(x^3 + ax + b\right) = 0 \cup \mathcal{O} = (0,1,0) \text{ avec } 4a^3 + 27b^2 \neq 0$$

Proposition 3.4. *Soient* $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ *et* $P_3 = (x_3, y_3)$ *trois points de* $E \setminus \{\mathcal{O}\}$ *tels que* $P_1 \neq P_2$. *Si* $x_1 \neq x_2$ *et si* $P_3 = P_1 * P_2$, *alors*

$$\begin{cases} x_3 = & \lambda^2 - x_1 - x_2 \\ y_3 = & \lambda\,(x_3 - x_1) + y_1 \end{cases} \quad avec\ \lambda = \frac{y_2 - y_1}{x_2 - x_1}$$

Remarque 3.5. Cette définition est encore vraie dans le cas où $x_1 = x_2$ et $y_2 = -y_1$ avec $P_1 * P_2 = \mathcal{O}$.

Proposition 3.6. *Soient* $P = (x_1, y_1)$ *et* $P_3 = (x_3, y_3)$ *deux points de* $E \setminus \{\mathcal{O}\}$.
Si $P_3 = P * P$, *alors*

$$\begin{cases} x_3 = & \lambda^2 - 2x_1 \\ y_3 = & \lambda\,(x_3 - x_1) + y_1 \end{cases} \quad avec\ \lambda = \frac{3x_1^2 + a}{2y_1}$$

Remarque 3.7. Le fait d'avoir imposé que la courbe soit non singulière nous permet d'être assurés que la tangente existera toujours.

Proposition 3.8. *On a* $\mathcal{O} * \mathcal{O} = \mathcal{O}$

Corollaire 3.9. *Soit* E *une courbe elliptique définies sur un corps* $\mathbb{K}$, *soit* P_1 *et* P_2 *deux points de* E. *Alors l'opération* $+$ *définie par*

$$\forall (P_1, P_2) \in E,\ P_1 + P_2 = \mathcal{O} * (P_1 * P_2)$$

permet de munir E *d'une structure de groupe abélien admettant* $\mathcal{O}$ *comme élément neutre. De plus, supposons* $P_1 = (x_1, y_1) \neq \mathcal{O}$ *et* $P_2 = (x_2, y_2) \neq \mathcal{O}$. *Si* $x_1 = x_2$ *et* $y_2 = -y_1$ *alors* $P_1 + P_2 = \mathcal{O}$ *; dans les autres cas , si* $P_3 = P_1 + P_2$, *alors*

$$\begin{cases} x_3 = & \lambda^2 - x_1 - x_2 \\ y_3 = & \lambda\,(x_1 - x_3) - y_1 \end{cases} \quad où\ \ \lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & si\ P \neq Q \\ \frac{3x_1^2 + a}{2y_1} & si\ P = Q \end{cases}$$

On a enfin

Propriété 3.10. $-\mathcal{O} = \mathcal{O}$.

Propriété 3.11. $\forall P \in E,\ P + \mathcal{O} = \mathcal{O} + P = P$ ($\mathcal{O}$ est un élément neutre).

Propriété 3.12. Si $P = (x; y)$, alors $-P = (x; -y)$.

Propriété 3.13. Si P et Q ont même abscisse, alors P est égal à Q ou à $-Q$.

Remarque 3.14. Le calcul de λ fait appel à un inverse dans $\mathbb{K}$ ce qui justifie la nécessité pour $\mathbb{K}$ d'être un corps.

Cardinalité

Notation 3.15. Si p est un nombre premier, on notera dans la suite $\mathbb{F}_p$ le corps fini de cardinal p.

Théorème 3.16 (**Théorème de Hasse**). *Soit p un nombre premier. Si $E(\mathbb{F}_p)$ est une courbe elliptique définie sur le corps fini $\mathbb{F}_p$ de cardinalité p alors la cardinalité $\sharp E(\mathbb{F}_p)$ de $E(\mathbb{F}_p)$ vérifie (voir[ST94]) :*

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

3.3. Méthode utilisant les Courbes elliptiques ou ECM(Elliptics Curves Methods)

L'algorithme de factorisation utilisant les courbes elliptiques est une variante de la méthode $(p-1)$ de Pollard dans $\mathbb{F}_p$. Comme nous pouvons remarquer que l'algorithme $(p-1)$ de Pollard se base sur le fait que les éléments non nuls de $(\mathbb{Z}/p\mathbb{Z})$ forme un groupe $(\mathbb{Z}/p\mathbb{Z})^*$ d'ordre $(p-1)$. Dans ce cas si $(p-1) \mid k$ on a $a^k = 1$ dans ce groupe. L'idée de Lenstra consiste à remplacer le groupe $(\mathbb{Z}/p\mathbb{Z})^*$ par un groupe de points $E(\mathbb{F}_p)$d'un courbe elliptique et l'entier a par un point $P \in E(\mathbb{F}_p)$. Signalons que, puisqu'on ne connait pas p, on ne connait pas cette courbe elliptique.

Méthode de Lenstra (1987)

Soit $n \in \mathbb{N}$ un entier , supposé composé, admettant un facteur premier p que l'on veut trouver.

Etape 1 : vérifions que n n'est divisible ni par 2, ni par 3 (sinon, nous avons trouvé un facteur de n) pour nous assurer que $(\mathbb{Z}/p\mathbb{Z})$ de caractéristique différente de 2 ou 3 et donc le groupe $(E(\mathbb{Z}/p\mathbb{Z}),+)$ est bien défini. Et vérifions également que n n'est pas de la forme m^r pour $r \geq 2$ (puissance parfaite).

Etape 2 : Choisissons la borne de la friabilité B : si p est un plus petit facteur premier d'un entier composé n, alors $p \leq \sqrt{n}$; or d'après le théorème de Hasse, on a $\sharp E(\mathbb{F}_p) < \left(\sqrt{p}+1\right)^2$. On peut donc prendre $B \geq \left[\left(n^{\frac{1}{4}}+1\right)^2\right]+1$. Et prenons

$$k = \prod_{p \text{ premier, } p \leq B} p^{\alpha_p} \text{ où } \alpha_p = \max\{\alpha |\ p^\alpha \leq B\}$$

Etape 3 : Choisissons deux entiers a et b dans $\{1, \cdots, n-1\}$ et considérons une courbe elliptique $E_{a,b}$ définie par :

$$E_{a,b} : y^2 = x^3 + ax + b \cup \mathcal{O} = (0,1,0)$$

Supposons que la cardinalité $\sharp E_{a,b}(\mathbb{F}_p)$ est B-friable.

Etape 4 : En notant $\Delta = 4a^3 + 27b^2$, vérifions que $\text{pgcd}(\Delta, n) = 1$ pour nous assurer que $E_{a,b}(\mathbb{Z}/n\mathbb{Z})$ est non singulière. Si $1 < \text{pgcd}(\Delta, n) < n$, alors $\text{pgcd}(\Delta, n)$ est un facteur non trivial de n et si $\text{pgcd}(\Delta, n) = n$ alors nous choisissons une autre courbe elliptique (d'autres valeurs de a, b et B).

Etape 5 : Si $\text{pgcd}(\Delta, n) = 1$, choisissons un point $P \in E_{a,b}(\mathbb{Z}/n\mathbb{Z}) \setminus \{\mathcal{O}\}$.

Le $\sharp E_{a,b}(\mathbb{F}_p)$ étant supposée B-friable, si $\sharp E_{a,b}(\mathbb{F}_p)$ divise un entier k B-friable, et d'après le théorème de Lagrange, l'ordre de P divise $\sharp E_{a,b}(\mathbb{F}_p)$, par suite l'ordre de P divise k et on a $kP = \mathcal{O}$ dans $E_{a,b}(\mathbb{F}_p)$. Si l'on calculait $kP = P + P + \cdots + P$ dans $E_{a,b}(\mathbb{F}_p)$, comme auparavant dans l'Algorithme $(p-1)$ de Pollard, le calcul de kP a besoin d'écrire aussi k dans la base 2 :

$$k = k_0 + k_1 2^1 + k_2 2^2 + \cdots + k_r 2^r \text{ où } k_i = 0 \text{ ou } k_i = 1$$

Cela exige de $r \leq \log_2 K$ opérations. Puis,

$$\begin{aligned} P_0 &= P \\ P_1 = 2P_0 &= 2^1 P \\ P_2 = 2P_1 &= 2^2 P \\ P_3 = 2P_2 &= 2^3 P \\ &\cdots \\ P_r = 2P_{r-1} &= 2^r P \end{aligned}$$

Finalement,

$$\begin{aligned} kP &= (k_0 + k_1 2^1 + k_2 2^2 + \cdots + k_r 2^r)P \\ &= k_0 P + k_1 2^1 P + k_2 2^2 P + \cdots + k_r 2^r P \\ &= \sum_{(si\ k_i = 1)} P_i \end{aligned}$$

Alors nous pouvons calculer kP au plus $2\log_2 K$ étapes.

On serait alors amené à calculer $Q + P = \mathcal{O}$ avec $Q = k'P$ et $k' < k$. En pratique, on va effectuer le calcul de kP non pas dans $E_{a,b}(\mathbb{F}_p)$ mais dans $E_{a,b}(\mathbb{Z}/n\mathbb{Z})$.
Rappelons les formules d'addition : $P_1 = (x_1, y_1) \neq \mathcal{O}$ et $P_2 = (x_2, y_2) \neq \mathcal{O}$. Si $x_1 = x_2$ et $y_2 = -y_1$ alors $P_1 + P_2 = \mathcal{O}$; dans les autres cas , si $P_3 = P_1 + P_2$, alors

$$\begin{cases} x_3 = & \lambda^2 - x_1 - x_2 \\ y_3 = & \lambda(x_1 - x_3) - y_1 \end{cases} \text{ où } \lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & si\ P \neq Q \\ \frac{3x_1^2 + a}{2y_1} & si\ P = Q \end{cases}$$

On aura $Q + P = \mathcal{O}$ donc $x_1 \equiv x_2 \pmod{p}$, soit $p \mid (x_1 - x_2)$. Lors du calcul de λ pour additionner Q et P, $(x_1 - x_2)$ ne sera alors pas inversible dans $\mathbb{Z}/n\mathbb{Z}$ car $p \mid \text{pgcd}((x_1 - x_2), n)$

donc $\text{pgcd}((x_1 - x_2), n) \neq 1$. Dans ce cas si $1 < \text{pgcd}((x_1 - x_2), n) < n$ alors nous avons trouvé un facteur non trivial de n. Mais il se peut que l'on ait : $x_1 \neq x_2 \pmod{n}$. Si $\text{pgcd}((x_1 - x_2), n) = n$ ou si le calcul de kP dans $E(\mathbb{Z}/n\mathbb{Z})$ aboutit, alors nous choisissons une autre courbe elliptique (d'autres valeurs de a, b et B).

Remarque 3.17. Le principe est que, si l'on considère une courbe elliptique $E_{a,b}(\mathbb{Z}/n\mathbb{Z})$, certains entiers ne seront pas inversibles modulo n. La somme de certains points provoquera alors une *erreur*. Ces *erreurs* sont particulièrement intéressantes, puisqu'elles permettent de donner un diviseur de n. En effet, cela veut dire que le plus grand diviseur commun du nombre dont on a tenté de prendre l'inverse et de n n'est pas égal à 1, et donne donc un diviseur propre de n. Le but est donc de rechercher des éléments non inversibles de $\mathbb{Z}/n\mathbb{Z}$.

Remarque 3.18. Le temps d'aboutissement de l'algorithme ECM depend principalement de la taille du facteur p de n qui a une influence à la probabilité de friabilité de $\sharp E(\mathbb{F}_p)$.

Exemple 3.19. Nous allons factoriser $n = 1715761513$. La première chose à faire c'est tester si n est composé. Appliquons le petit théorème de Fermat,

$$2^{1715761513-1} \equiv 93082891 \pmod{1715761513}$$

donc $2^{n-1} \neq 1 \pmod{n}$, donc n est composé. Maintenant, procédons à l'algorithme de Lenstra :

(i) Vérifions que n n'est pas de la forme m^r où $r \geq 2$ en utilisant l'algorithme dans la section 6. dans les Préliminaires.

(ii) Comme $\sqrt{1715761513} \approx 41422$, alors le plus petit facteur premier p de n est inférieur à 41422. Prenons $k = \text{ppcm}[1, 2, 3, \ldots, 17] = 12252240$ dont ses facteurs premiers sont plus petits que 41422 (k est 17-friables). Et

$$k = 12252240 = 2^4 + 2^6 + 2^{10} + 2^{12} + 2^{13} + 2^{14} + 2^{15} + 2^{17} + 2^{19} + 2^{20} + 2^{21} + 2^{23}$$

(iii) Nous allons fixer $P = (2, 1)$ et comme une courbe elliptique est de la forme $C : y^2 = x^3 + ax + b$, on a $b = -7 - 2a$, pour commencer, mettons $a = 1$, alors $b = -9$. Nous allons considerer donc la courbe elliptique $C : y^2 = x^3 + x - 9$ et $P = (2, 1)$. Pour calculer $kP \pmod{n}$, nous avons besoin tout d'abord calculer $2^iP \pmod{n}$. Les résultats $2^iP \pmod{n}$ pour $0 \leq i \leq 23$ sont donnés dans le tableau suivant :

i	$2^i P \pmod{1715761513}$
0	(2,1)
1	(1286821173,1072350709)
2	(1334478523,112522703)
3	(912789305,77695868)
4	(385062894,618628731)
5	(866358838,450284374)
6	(904716938,169383608)
7	(808696477,1201030016)
8	(572301268,107111567)
9	(1512647092,1695275444)
10	(1858186,1224662922)
11	(1550404618,825515387)
12	(1519325194,1657497846)
13	(522917322,524407354)
14	(25207285,1375034461)
15	(781360494,147273929)
16	(1108412304,25813532)
17	(435914774,323718902)
18	(1399483199,1203611423)
19	(778823593,192206539)
20	(853199887,1012680972)
21	(501929966,910060788)
22	(1315182921,305331845)
23	(257200250,318342966)

Tab. II.3: Valeurs de $2^i P \pmod{n}$ pour $0 \leq i \leq 23$

Cela nous permet de calculer kP :

$$2^4P = 16P = (385062894, 618628731)$$
$$(2^4 + 2^6)P = 80P = (831572269, 1524749605)$$
$$(2^4 + 2^6 + 2^{10})P = 1104P = (1372980126, 736595454)$$
$$(2^4 + 2^6 + 2^{10} + 2^{12})P = 5200P = (1247661424, 958124008)$$
$$(2^4 + \cdots + 2^{12})P + 2^{13}P = 13392P = (1548582473, 1559853215)$$
$$(2^4 + \cdots + 2^{13})P + 2^{14}P = 29776P = (201510394, 7154559)$$
$$(2^4 + \cdots + 2^{14})P + 2^{15}P = 62544P = (629067322, 264081696)$$
$$(2^4 + \cdots + 2^{15})P + 2^{17}P = 193616P = (844665131, 537510825)$$
$$(2^4 + \cdots + 2^{17})P + 2^{19}P = 717904P = (886345533, 3428565998)$$
$$(2^4 + \cdots + 2^{19})P + 2^{20}P = 1766480 = (370579416, 1254954111)$$
$$(2^4 + \cdots + 2^{20})P + 2^{21}P = 3863632P = (77302130, 514483068)$$
$$(2^4 + \cdots + 2^{21})P + 2^{23}P = 12252240P = (1225303014, 142796033)$$

Donc avec la courbe elliptique $C : y^2 = x^3 + x - 9$ modulo n, et le calcul de kP, nous avons $kP = 12252240(2, 1) \equiv (421401044, 664333727) \pmod{1715761513}$. Comme le calcul de kP dans $E(\mathbb{Z}/n\mathbb{Z})$ aboutit, alors nous choisissons une autre courbe elliptique (autre valeur de a et de b).

(iv) Nous gardons le même $k = 12252240$ et le même point $P = (2, 1)$, En faisant varier $a = 3, 4, 5, \ldots, 41$ et en répétant la même procedure de calcule de kP dans $E(\mathbb{Z}/n\mathbb{Z})$, le calcul de kP a abouti toujours. Essayons maintenant avec $a = 42$ et $b = -7 - 2a = -91$. En d'autres termes considérons la nouvelle courbe elliptique $C : y^2 = x^3 + 42x - 91$ avec $P = (2, 1)$. Et effectuons le calcul comme auparavant :

$$(2^4 + 2^6 + 2^{10} + \cdots + 2^{20} + 2^{21})P = 3863632P \equiv (1115004543, 1676196055) \pmod{n}$$

Pour avoir kP nous devons calculer $(2^4 + 2^6 + 2^{10} + \cdots + 2^{20} + 2^{21})P + 2^{23}P$, où $2^{23}P = (1267572925, 848156341) \pmod{n}$, en d'autres termes :

$$(1115004543, 1676196055) + (1267572925, 848156341) \pmod{n}$$

Mais lors du calcul de la différence de leurs abscisses, cette différence n'est pas inversible dans $\mathbb{Z}/n\mathbb{Z}$ car le

$$\text{pgcd}(1115004543 - 1267572925, n) = \text{pgcd}(-152568382, 1715761513) = 26927$$

Alors en essayant de calculer $12252240(2, 1)$ sur la courbe

$$C : y^2 = x^3 + 42x - 91 \pmod{1715761513}$$

Le calcul n'a pas abouti mais cette opération défaillante nous permet de factoriser $n = 1715761513 = 26927 \cdot 63719$

III. LA COMPLEXITÉ DE L'ALGORITHME NE DÉPEND PAS DE LA TAILLE DE FACTEURS

1. *Méthode de Fermat (1643)*

Fermat propose une méthode basée sur l'identité remarquable $x^2 - y^2 = (x-y)(x+y)$. L'idée c'est d'écrire un entier n à factoriser comme différence de carrés.
Remarquons que tout nombre composé impaire peut s'écrire comme différence de deux carrés : $ab = \left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2$. Soit n un entier composé, n peut s'écrire $n = p_1 p_2$ où p_1 et p_2 sont impairs, sinon $n = 2k$ où 2 et k sont des facteurs non triviaux de n.
Posons $p_1 < p_2, p_2 - p_1 = 2d, x = p_1 + d$ et $y = d$, on a $p_1 = x - y$ et $p_2 = x + y$. Come $n = p_1 p_2 = (x-y)(x+y) = x^2 - y^2$ c'est-à-dire $y^2 = x^2 - n$, alors pour résoudre cette équation, on peut tester la valeur de $x = \lfloor\sqrt{n}\rfloor + 1$, $\lfloor\sqrt{n}\rfloor + 2$, $\lfloor\sqrt{n}\rfloor + 3$, $\lfloor\sqrt{n}\rfloor + 4$,$\cdots$, jusqu'on trouve un carré parfait.

Exemple 1.1. $n = 143$, $\lfloor\sqrt{143}\rfloor + 1 = 12$ et $x^2 - n = 12^2 - 143 = 1$ alors $x = 12$ et $y = 1$ et $n = (12-1)(12+1) = 11 \cdot 13$

2. *Méthode de Kraïtchik (1926)*

La méthode de Kraïtchik est une version amélioré de l'idée de *Fermat* :
$x^2 \equiv y^2 \pmod{n}$ admet $x \equiv \pm y \pmod{n}$ comme solutions triviales. Si $n = p$, où p est premier impair et $y \neq 0 \pmod{p}$ alors $x^2 \equiv y^2 \pmod{p}$ admet exactement deux solutions $u \equiv \pm y \pmod{p}$. En effet, on sait que dans un anneau intègre $(\mathbb{Z}/p\mathbb{Z})$, une congruence quadratique admet au plus deux solutions. Supposons maintenant que $u \equiv -u \pmod{p}$, on a $2u \equiv 0 \pmod{p}$ et comme $pgcd(2,p) = 1$ car p est premier impair, cela donne $u \equiv 0 \pmod{p}$ or $u \equiv \pm y \neq 0 \pmod{p}$, donc les deux solutions sont triviales et distinctes. Alors, pour $x^2 \equiv y^2 \pmod{n}$ où $n = p^\alpha$, p est premier et $\alpha \in \mathbb{N}^*$, nous ne pouvons trouver que des solutions triviales.
Si $n = pq$, nou savons que $u^2 \equiv y^2 \pmod{p}$ admet $u \equiv \pm y \pmod{p}$ comme solutions et $v^2 \equiv y^2 \pmod{q}$ admet $v \equiv \pm y \pmod{q}$ comme solutions, alors $x^2 \equiv y^2 \pmod{pq}$ admet quatre solutions :

$$\begin{cases} u \equiv +y \pmod{p} \\ v \equiv +y \pmod{q} \end{cases} \tag{2.1}$$

donne $x \equiv +y \pmod{pq}$ d'après le théorème de Chinois,

$$\begin{cases} u \equiv -y \pmod{p} \\ v \equiv -y \pmod{q} \end{cases}$$
$$\text{donne } x \equiv -y \pmod{pq},$$

$$\begin{cases} u \equiv +y \pmod{p} \\ v \equiv -y \pmod{q} \end{cases}$$
$$\text{donne } x \equiv +z \pmod{pq},$$

$$\begin{cases} u \equiv -y \pmod{p} \\ v \equiv +y \pmod{q} \end{cases}$$
$$\text{donne } x \equiv -z \pmod{pq},$$

Où $+z$ et $-z$ sont des solutions non triviales de $x^2 \equiv y^2 \pmod{pq}$ (rappelons que si l'un de $(x+y)$ ou $(x-y)$ est divisible à la fois par p et q, cela conduit à la solution triviale $x \equiv \pm y \pmod{pq}$). Alors si $n = pq$ et si l'un de $(x+y)$ ou $(x-y)$ n'est pas divisible à la fois par p et q alors, l'un de $(x+y)$ et $(x-y)$ doit être divisible par p et l'autre par q . Le facteur p ou q sera trouvé en calculant le $\text{pgcd}(x-y,n)$ ou le $\text{pgcd}(x+y,n)$ qui nous permet par suite de factoriser n, cela veut dire qu'il y a 50% de chance (plus si n admet plus de deux facterus premiers) pour determiner un facteur de $n = pq$.
Si n admet plus de deux facteurs [Rie85, p.157] cette méthode reste valable en appliquant le même raisonnement par un de facteurs p et son co-facteur correspondant $q = n/p$ qui est composé dans ce cas .

Proposition 2.1. *Si* $x^2 \equiv y^2 \pmod{n}$ *et* $x \neq \pm y \pmod{n}$ *alors* $\text{pgcd}(x-y,n)$ *et* $\text{pgcd}(x+y,n)$ *sont des facteurs non triviaux de* n.

Preuve. Remarquons que $\text{pgcd}(x-y,n) \neq n$ et $\text{pgcd}(x+y,n) \neq n$ car $x \neq \pm y \pmod{n}$. Comme $x^2 \equiv y^2 \pmod{n}$, c'est-à-dire $n \mid (x-y)(x+y)$. Si $\text{pgcd}(x-y,n) = 1$ alors $n \mid (x+y)$, ce qui est impossible car $x \neq -y \pmod{n}$. Si $\text{pgcd}(x+y,n) = 1$, alors $n \mid (x-y)$, ce qui est impossible car $x \neq y \pmod{n}$. □

Remarque 2.2. Dans la pratique de la factorisation de n, nous avons besoin de trouver quelques pairs de (x,y) pour que $x^2 \equiv y^2 \pmod{n}$. Pour cela prenons arbitrairement un entier v et calculons $s_v \equiv v^2 \pmod{n}$. Si s_v est un carré parfait modulo n alors $s_v = y^2$ et $v = x$. Si $v < \sqrt{n}$ cela donne $x = y$ et $\text{pgcd}(x-y,n) = n$, il faut choisir un autre v.

Exemple 2.3. $n = 143$ et $\left[\sqrt{143}\right] = 11$

$v = 17$ on an $v^2 = 289 = 3 + 2 \cdot 143 \equiv 3 \pmod{143}$, c'est-à-dire $S_{17} = 3$ qui n'est pas un carré alors il faut trouver un autre v.

$v = 23$ on an $v^2 = 529 = 10 + 3 \cdot 143 \equiv 10^2 \pmod{143}$, c'est-à-dire $S_{23} = 10^2$ donc $x = 23$ et $y = 10$. En utilisant le résultat de la proposition précedante, $\text{pgcd}(23 + 10, 143) = 11$ et $\text{pgcd}(23 - 10, 143) = 13$ sont des facteurs non triviaux de $n = 143$. Finalement $143 = 11 \cdot 13$

Remarque 2.4. Considerons l'équation $s_v \equiv v^2 \pmod{n}$: comme il y a seulement $\sqrt{n}$ carrés inferieurs à n, donc la probabilité pour trouver un tel s_v est $\frac{1}{\sqrt{n}}$. Cela veut dire que cet algorithme de factorisation ne peut pas être espéré plus rapide que la division triviale.

Remarque 2.5. En combinant les s_v B-friables cela pourrait améliorer la rechereche de $(v; s_v)$

Exemple 2.6. $n = 143$ et $B = 5$, c'est-à-dire $F(B) = \{2, 3, 5\} \cup \{-1\}$

$v = 17$ et $17^2 = 289 = 3 + 2 \cdot 143 \equiv 3 \pmod{143}$, alors $s_{17} = 3$ est donc 5-friable. Comme $(v + 1)^2 = v^2 + 2v + 1$

$v = 18$ et $18^2 = 17^2 + 2 \cdot 17 + 1 \equiv 3 + 35 = 38 = 2 \cdot 19 \pmod{143}$, alors s_{18} n'est pas 5-friable

$v = 19$ et $19^2 = 18^2 + 2 \cdot 18 + 1 \equiv 38 + 37 = 75 \equiv \pmod{143}$, alors $s_{19} = 2^0 \cdot 3^1 \cdot 5^2$ est 5-friable

$(s_{17} \cdot s_{19})^2 \equiv (2^0 \cdot 3^1 \cdot 5^1)^2 \pmod{143}$, donc $x = 17 \cdot 19$ et $y = 3 \cdot 5$,

par suite $\text{pgcd}(323 - 15, 143) = 11$, $\text{pgcd}(323 + 15, 143) = 13$ et $143 = 11 \cdot 13$.

3. Méthode utilisant le Crible Quadratique de C. Pomerance (1981)

Lemme 3.1. *Si $m_1, m_2, \ldots, m_k$ sont des entiers B-friables et $k > \pi(B)$ où $\pi(B)$ est le nombre d'entiers premiers dans l'intervalle $[1, B]$, alors on peut trouver une sous suite $(m_i)_i$ où $i \in \{1, 2, \cdots, k\}$ dont le produit de ses termes est un carré.*

Preuve. Soit m_j un entier B-friables, $m_j = \prod_{i=1}^{\pi(B)} p_i^{\alpha_{ji}}$ où p_i premier et α_{ji} est l'exposant de p_i , $i-$ème facteur de m_j. Considérons le vecteur exposant $v(m_j) = (\alpha_{j1}, \alpha_{j2}, \ldots, \alpha_{j\pi(B)})$:
$m_1 \times m_2 \times \ldots \times m_s$ est un carré si et seulement si
$v(m_1) + v(m_2) + \cdots + v(m_s) = (0 \pmod 2, 0 \pmod 2, \ldots, 0 \pmod 2)$ où

$$\begin{cases} v(m_1) & = (\alpha_{11}, \alpha_{12}, \ldots, \alpha_{1\pi(B)}) \\ v(m_2) & = (\alpha_{21}, \alpha_{22}, \ldots, \alpha_{2\pi(B)}) \\ & \vdots \\ v(m_s) & = (\alpha_{s1}, \alpha_{s2}, \ldots, \alpha_{s\pi(B)}) \end{cases}$$

$$\sum_{i=1}^{s} v(m_i) = (\sum_{i=1}^{s} \alpha_{i1}, \sum_{i=1}^{s} \alpha_{i2}, \cdots, \sum_{i=1}^{s} \alpha_{i\pi(B)}) = (0 \pmod 2, 0 \pmod 2, \ldots, 0 \pmod 2)$$

Dans l'espace vectoriel $\mathbb{F}_2^{\pi(B)}$ de dimension $\pi(B)$ des vecteurs exposants sur le corps $\mathbb{Z}/2\mathbb{Z}$, si $k > \pi(B)$ alors les vecteurs $v(m_1), v(m_2), \ldots, v(m_k)$ sont linéairement dépendants, c'est-à -dire $\lambda_1 v(m_1) + \lambda_2 v(m_2) + \cdots + \lambda_k v(m_k) = 0-$vecteurs est une relation de dépendance, où $\lambda_i \in \mathbb{Z}/2\mathbb{Z}$ pour tout $i \in \{1, 2, \ldots, k\}$.

3.1. Déroulement de la méthode Crible Quadratique ou QS (Quadratic Sieve)

Soit n l'entier que l'on souhaite factoriser, considérons $S(X) = (X + [\sqrt{n}])^2 - n$, qui peut s'écrire aussi $S(X) \equiv (X + [\sqrt{n}])^2 \pmod{n}$:
Supposons que nous avons trouvé $X_1, X_2, \ldots, X_k$ tels que $S(X_1) \cdot S(X_2) \cdots (X_k)$ est un carré, notons $\prod_{i=1}^{k} S(X_i) = u^2$:

$$\begin{aligned}
(X_1 + \left[\sqrt{n}\right])^2 &\equiv S(X_1) \pmod{n} \\
(X_2 + \left[\sqrt{n}\right])^2 &\equiv S(X_2) \pmod{n} \\
&\cdots \\
(X_k + \left[\sqrt{n}\right])^2 &\equiv S(X_k) \pmod{n}. \\
(\prod_{i=1}^{k}(X_i + \left[\sqrt{n}\right]))^2 &\equiv \prod_{i=1}^{k} S(X_i) \pmod{n}
\end{aligned}$$

Posons $x = \prod_{i=1}^{k}(X_i + [\sqrt{n}])$ et $y = u$ qui nous donnera la solution de $x^2 \equiv y^2 \pmod{n}$. □

Remarque 3.2. Pour assurer qu'on obtient un carré de produit de $S(X_i)$, on doit collecter plus de $\pi(B)$ de $S(X_i)$ B-friables d'après le lemme 3.1 précédent.

Remarque 3.3. On doit considérer tout simplement X_i tel que $S(X_i)$ n'est pas divisible par un grand nombre premier, sinon si $S(X_i)$ est divisible par un grand nombre premier p, on est obligé de trouver un X_j tel que $S(X_j)$ est divisible par p ; ce qui ne sera pas toujours facile. D'où l'intérêt de collecter des $S(X_i)$ B-friables.

3.2. Base de factorisation du Crible Quadratique

Soit n l'entier que l'on souhaite factoriser, considérons $S(X) = (X + [\sqrt{n}])^2 - n$. Prenons un entier B positif et supposons que $S(X)$ est complètement factorisé dans une base de facteur $F(B) = \{p_1, p_2, \ldots, p_s\}$ où les p_i sont premiers et $s = \pi(B)$, on a $S(X) = \prod_{i=1}^{s} p_i^{\alpha_i}$:

Propriété 3.4. $p_i | S(X)$ pour chaque $i \in \{1, \ldots, s\}$

Propriété 3.5. Si $p_i \in F(B) = \{p_1, p_2, \ldots, p_s\}$ alors $p_i \nmid n$ pour chaque $i \in \{1, \ldots, s\}$, sinon on trouve un facteur non trivial de n.

Propriété 3.6.

$$S(X) = (X + \lceil\sqrt{n}\rceil)^2 - n$$
$$n = (X + \lceil\sqrt{n}\rceil)^2 - k_i p_i \ (car\ p_i | S(X)),\ k_i \in \mathbb{Z}$$
$$n \equiv (X + \lceil\sqrt{n}\rceil)^2 \pmod{p_i},\ pour\ tout\ i \in \{1, \ldots, s\}$$

c'est-à-dire n doit être résidu quadratique modulo p_i. Autrement dit une base de factorisation ne contient que des premiers p_i tels que $\left(\frac{n}{p_i}\right) = 1$

3.3. Crible Quadratique

Soit n l'entier que l'on souhaite factoriser. Soit $p \in F(B)$, on sait que $\left(\frac{n}{p}\right) = 1$, c'est-à-dire $n \equiv t^2 \pmod{p}$ ou $n \equiv (-t)^2 \pmod{p}$. Comme $n \equiv (X + [\sqrt{n}])^2 \pmod{p}$, on a :
$(X + [\sqrt{n}]) \equiv t \pmod{p}$ ou $(X + [\sqrt{n}]) \equiv -t \pmod{p}$.
On sait également que si $(X + [\sqrt{n}])^2 - n \equiv 0 \pmod{p}$, c'est-à-dire que si $p|S(X)$, alors $p|S(X + rp)$ où $r \in \mathbb{Z}$. En effet,

$$\begin{aligned} S(X + rp) &= ((X + rp) + \lceil\sqrt{n}\rceil)^2 - n && (3.2)\\ &= S(X) + p(2Xr + r^2 p + 2r\lceil\sqrt{n}\rceil) && (3.3)\\ &\equiv 0 \pmod{p}. && (3.4) \end{aligned}$$

Et d'une manière générale, si $p^\alpha \mid S(X)$, alors $S(X + rp^\alpha) \equiv 0 \pmod{p^\alpha}$. Cette propriété nous permet de localiser tous les nombres divisibles par p dans un intervalle donné $[-M; M]$ qui est appelé intervalle de criblage.

Remarque 3.7. Rappelons que le nombre d'étapes pour localiser tous les nombres B-friables inférieurs à Y en utilisant le Crible d'Ératosthène (Cribler les nombres B-friables inférieurs à Y par les nombres premiers inferieurs à B et leurs puissances) est approximativement égal à $Y \cdot \sum_{p \le B} \frac{1}{p} \approx Y \cdot \log\log B$. Cela veut dire que le nombre d'étapes pour localiser un candidat est environs $\log\log B$.

les étapes du Crible Quadratique

$S(X) = (X + [\sqrt{n}])^2 - n$ et $F(B) = \{p_1, \ldots, p_s\} \cup \{-1\}$ où p_i *premier* $\le B$ pour tout $i \in \{1, \ldots, s\}$ et $[-M, M]$ l'intervalle de criblage :

(i) Calculer $S(-M), S(-M+1), \ldots, S(0), \ldots, S(M-1), S(M)$

(ii) Résoudre les équations $S(X) \equiv 0 \pmod{p_i}$ où $p_i \in F(B)$, à l'aide l'algorithme de Shanks-Tonelli [Coh93, p32-33] (pour résoudre l'équation de la forme $x^2 \equiv a \pmod{p}$), autrement dit, résoudre $(X + [\sqrt{n}])^2 \equiv n \pmod{p_i}$. Si p_i impair, on obtient deux solutions s_{1i} et s_{2i} (voir[Lan01, p.3]) ; si $p_i = 2$ on a une seule solution $x_i \in \{0; 1\}$. On sait que $p_i | S(s_{ji} + kp_i)$ pour tout $k \in \mathbb{Z}$ et pour tout $j \in \{1, 2\}$, d'après l'équation (3.4).

(iii) Donner i la valeur 1

(iv) Cribler les $S(s_{ji} + kp_i)$, vérifiant $-M \leq s_{ji} + kp_i \leq M$, parmi les valeurs trouvées dans *(i)*, c'est-à-dire détecter les valeurs de $S(s_{ji} + kp_i)$ qui sont divisibles par p_i dans $[-M, M]$.

(v) Pour chaque k, tant que $p_i | S(s_{ji} + kp_i)$, remplacer $S(s_{ji} + kp_i)$ par $\frac{S(s_{ji}+kp_i)}{p_i}$ et à la fin, enregistrer dans un tableau les puissances maximales de p_i divisant $S(s_{ji} + kp_i)$.

(vi) Si $i \leq s$, donner à i la valeur $i + 1$ et recommencer l'étape *(iv)*

(vii) Si $S(k) = -1$ multiplier par (-1) et ajouter 1 dans le tableau de la puissance maximale de (-1) correspondant (étape *(v)*), où $-M \leq k \leq M$.

(viii) pour tout $-M \leq k \leq M$, si $S(k) = 1$ alors la valeur de $S(k)$ du départ qu'on avait enregistrée dans l'étape *(v)* est B-friable.

Exemple 3.8. $n = 7429$, $\lfloor \sqrt{n} \rfloor = 86$, $F(7) = \{-1, 2, 3, 5, 7\}$ la base de factorisation et $[-4, 4]$ l'intervalle de criblage,
(i)Calculer $S(-4), S(-3), S(-2), S(-1), S(0), S(1), S(2), S(3), S(4)$

$$\begin{aligned}
S(-4) &= (-4 + 86)^2 - 7429 = -705 \\
S(-3) &= (-4 + 86)^2 - 7429 = -540 \\
S(-2) &= (-4 + 86)^2 - 7429 = -373 \\
S(-1) &= (-4 + 86)^2 - 7429 = -204 \\
S(0) &= (-4 + 86)^2 - 7429 = -33 \\
S(1) &= (-4 + 86)^2 - 7429 = 140 \\
S(2) &= (-4 + 86)^2 - 7429 = 315 \\
S(3) &= (-4 + 86)^2 - 7429 = 492 \\
S(4) &= (-4 + 86)^2 - 7429 = 671
\end{aligned}$$

(ii) Résolution et Criblage :
Résolvons l'équation $(x + 86)^2 \equiv 7429 \pmod{p}$ pour chaque $p \in F(p)$:

$$(x + 86)^2 \equiv 7429 \pmod{2} \text{ admet } x = 1 \text{ comme solution.}$$

donc 2 divise $S(1), S(3), S(-1), S(-3)$.

$$(x + 86)^2 \equiv 7429 \pmod{3} \text{ admet } x = 0 \text{ et } x = 2 \text{ comme solution.}$$

donc 3 divise $S(0), S(2), S(3), S(-3), S(-1), S(-4)$

$$(x + 86)^2 \equiv 7429 \pmod{5} \text{ admet } x = 1 \text{ et } x = 2 \text{ comme solution.}$$

donc 5 divise $S(1), S(2), S(-4), S(-3)$

$$(x+86)^2 \equiv 7429 \pmod 7 \text{ admet } x=1 \text{ et } x=2 \text{ comme solution.}$$

Récapitulons :

$S(4)$ et $S(-2)$ ne sont pas 7-friables car aucun premier $p_i \in F(7) = \{-1, 2, 3, 5, 7\}$ ne divise

$S(k)$	$S(-4)$	$S(-3)$	$S(-2)$	$S(-1)$	$S(0)$	$S(1)$	$S(2)$	$S(3)$	$S(4)$
p_i	-705	-540	-373	-204	-33	140	315	492	671
2		-270		-102		70		246	
2		-135		-51		35		123	
3	235	-45		-17	-11		105	41	
3		-15					35		
3		-5							
5	47	-1				7	7		
7						1	1		

Tab. III.1: Criblage des $S(k)$ où $-4 \leq k \leq 4$.

$S(4)$ et$S(-2)$, donc on les rejette.

$$\frac{S(3)}{2} = 246$$
$$\frac{S(3)}{2^2} = 123$$
$$\frac{S(3)}{2^2 \cdot 3} = 41 \neq 1$$

Donc $S(3)$ n'est pas 7-friables, on rejette $S(3)$.

Comme $S(1) = 140$, on a :

$$\frac{S(1)}{2} = 70$$
$$\frac{S(1)}{2^2} = 35$$
$$\frac{S(1)}{2^2 \cdot 5} = 7$$
$$\frac{S(1)}{2^2 \cdot 5 \cdot 7} = 1.$$

Alors $S(1) = 2^2 \cdot 5 \cdot 7$

Comme $S(2) = 315$, on a :

$$\frac{S(2)}{3} = 105$$
$$\frac{S(2)}{3^2} = 35$$
$$\frac{S(2)}{3^2 \cdot 5} = 7$$
$$\frac{S(2)}{3^2 \cdot 5 \cdot 7} = 1.$$

Alors $S(2) = 3^2 \cdot 5 \cdot 7$

p_i	-1	2	3	5	7
$v(S(-3))$	1	2	3	1	0
$v(S(1))$	0	2	0	1	1
$v(S(2))$	0	0	2	1	1

Tab. III.2: Vecteurs exposants des facteurs premiers de $S(k)$ 7-friables

Dans l'espace vectoriel $\mathbb{F}_2^{\pi(7)}$ sur le corps $\mathbb{Z}/2\mathbb{Z}$

p_i	-1	2	3	5	7
$v(S(-3))$	1	0	1	1	0
$v(S(1))$	0	0	0	1	1
$v(S(2))$	0	0	0	1	1

Tab. III.3: Vecteurs exposants des facteurs premiers de $S(k)$ 7-friables

Ici il est évident que $v(S(1)$ et $v(S(2)$ sont linéairement dépendants, mais d'une manière générale, on doit collecter plus de $\pi(B)$ de $S(X_i)$ B-friables d'après le lemme 3.1 et la remarque 3.2 pour assurer qu'on obtient un carré de produit de $S(X_i)$.
(iii) Factorisation :
$S(1) = (87)^2 - n = 2^2 \cdot 5 \cdot 7$ c'est-à-dire $(87)^2 \equiv 2^2 \cdot 5 \cdot 7 \pmod{n}$
$S(2) = (88)^2 - n = 3^2 \cdot 5 \cdot 7$ c'est-à-dire $(88)^2 \equiv 3^2 \cdot 5 \cdot 7 \pmod{n}$
$(87 \cdot 88)^2 \equiv 2^2 \cdot 3^2 \cdot 5^2 \cdot 7^2 \pmod{n}$
On peut donc prendre $x = 87 \cdot 88 = 227$ et $y = 2 \cdot 3 \cdot 5 \cdot 7 = 210$
On a $\text{pgcd}(227 + 210, n) = 437$ et $\text{pgcd}(227 - 210, n) = 17$
$n = 7429 = 437 \cdot 17$

Choix d'une borne de friabilité dans le QS (C. Pomerance) :

Notons $\psi(X, B)$ le nombre d'entiers B-friables dans l'intervalle $[1, X]$, autrement dit $\psi(X, B) = \#\{m : 1 \leq m \leq X, m \; est \; B - friable\}$.

1. En prenant $B = X^{1/2}$

$$\begin{aligned} \psi(X, X^{1/2}) &= [X] - \sum_{X^{1/2} < p \leq X} \left[\frac{X}{p}\right] \\ \psi(X, X^{1/2}) &= X(1 - \sum_{X^{1/2} < p \leq X} \frac{1}{p}) + O(X/\log X), \end{aligned}$$

D'après le Théorème de Mertens : $\sum_{p \leq t} \frac{1}{p} = \log\log t + C + O(1/\log t)$ où C constante.

Alors,

$$\begin{aligned}\sum_{X^{1/2}\leq p\leq X}\frac{1}{p} &= \sum_{p\leq X}\frac{1}{p}-\sum_{p\leq X^{1/2}}\frac{1}{p}\\ &= \log\log X-\log\log(X^{1/2})+O(1/\log X^{1/2})\\ &= \log 2+O(1/\log X^{1/2}).\end{aligned}$$

Et

$$\begin{aligned}\psi(X,X^{1/2}) &= (1-\log 2)X+O(1/\log X),\\ \frac{\psi(X,X^{1/2})}{X} &\approx 1-\log 2 \quad \textit{quand } X\to\infty.\end{aligned}$$

$\frac{\psi(X,X^{1/2})}{X}$ est la probabilité pour q'un nombre choisi dans $[1,X]$ soit $X^{1/2}$-friable.

2. En prenant $B=X^{1/u}$ où $1\leq u\leq 2$, on démontre que $\frac{\psi(X,X^{1/u})}{X}\approx 1-\log u$.

Et $\frac{\psi(X,X^{1/u})}{X}$ est également la probabilité pour q'un nombre choisi dans $[1,X]$ soit $X^{1/u}$-friable, de plus $\frac{X}{\psi(X,X^{1/u})}$ est environ le nombre de tris pour localiser un entier $X^{1/u}$-friable. Pour le crible quadratique, nous avons besoin d'au moins $\pi(B)$ nombres B-friables et chaque candidat demande $\log\log B$ étapes pour être localisé. Donc les étapes pour localiser des entiers nécessaires et suffisants pour le crible quadratique sont environ :

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

D'après l'études faites par E. R. Canfield, P. Erdos et C. Pomerance, on a

$$\frac{\psi(X,X^{1/u})}{X}=u^{-(1+o(1))u}$$

Cela nous permet d'écrire une expression simple, en mettant $\pi(B)\cdot\log\log B\approx X^{1/u}$ et $\frac{\psi(X,X^{1/u})}{X}\approx u^u$, nous avons

$$\pi(B)\cdot\log\log B\cdot\frac{X}{\psi(X,X^{1/u})}\approx X^{1/u}\cdot u^u$$

Posons maintenant $\eta(u)=\log(X^{1/u}u^u)=\frac{1}{u}+u\log u$, alors $\eta'(u)=1/u^2\log X+\log u+1$ et $\eta'(u)=0\Leftrightarrow -1/u^2\log X+\log u+1=0$

$$\begin{gathered}\log X=u^2(\log u+1)\\ \log\log X=\log(u^2(\log u+1))\\ \log\log\ X=\log u^2+\log(\log u+1)\\ \log\log\ X=2\log u+\log(\log u+1)\\ \log u\approx\frac{1}{2}\log\log\ X.\end{gathered}$$

Et comme $u^2(\log u + 1) = \log X$, alors

$$u^2 = \frac{\log X}{1 + \log u}$$
$$u^2 \approx \frac{\log X}{\log u}$$
$$u \approx \sqrt{\frac{\log X}{1/2 \cdot \log\log X}}$$
$$u \approx (2\log X)^{\frac{1}{2}}(\log\log X)^{\frac{-1}{2}}$$

Cela nous mène à écrire

$$\begin{aligned} B &= X^{1/u} \\ &= \exp(u^{-1}\log X) \\ &= \exp(((2\log X)^{1/2}(\log\log X)^{-1/2})^{-1} \cdot \log X) \\ &= \exp(2^{-1/2}(\log X \cdot \log\log X)^{1/2}) \end{aligned}$$

Nous avons également

$$\begin{aligned} u\log u &\approx 1/2 \cdot \log\log X \cdot (2\log X)^{1/2}(\log\log X)^{-1/2}) \\ &\approx 2^{-1/2}(\log X \cdot \log\log X)^{1/2} \end{aligned}$$

Alors

$$\begin{aligned} X^{1/u} \cdot u^u &\approx X^{1/u} \cdot \exp(u\log u) \\ &\approx \exp(2^{-1/2}(\log X \cdot \log\log X)^{1/2}) \cdot \exp(2^{-1/2}(\log X \cdot \log\log X)^{1/2}) \\ &\approx \exp(2^{1/2}(\log X \cdot \log\log X)^{1/2}) \end{aligned}$$

En prenant $X = n^{1/2+o(1)}$ où n est l'entier que l'on souhaite factoriser, nous avons l'optimisation de B et la complexité du crible quadratique :

$$\begin{aligned} B &\approx \exp((\frac{1}{2} + o(1))(\log n \cdot \log\log n)^{1/2}) \\ X^{1/u} \cdot u^u &\approx \exp((1 + o(1))(\log n \cdot \log\log n)^{1/2}) \end{aligned}$$

Remarque 3.9. Soit n l'entier que l'on souhaite factoriser, considérons une base de factorisation $F(B) = \{p_1, \ldots, p_s\}$ où $s = \pi(B)$ et $S(X) = (X + [\sqrt{n}])^2 - n \approx X^2 + 2X\,[\sqrt{n}]$, alors $S(X)$ est de l'ordre de $2X\sqrt{n}$ pour X assez petit. Dans la pratique si $2X\sqrt{n} \approx \prod_{p_i|S(X)} p_i$, ou encore si $\log 2X\sqrt{n} \approx \sum_{p_i|S(X)} \log p_i$ avec une incertitude δ, alors $S(X)$ a plus de chance d'être friable.

$$\delta = \left| \log 2X\sqrt{n} - \sum_{p_i|S(X)} \log p_i \right| \leq \log p_{max} = \log p_s$$

ou d'après l'experience de J. Silverman :

$$\delta \leq \frac{1}{2}\ln n + \ln M - T\ln p_{max} = \ln\left(\frac{M\sqrt{n}}{p_{max}^{T}}\right)$$

où $T \approx 2$ ($T = 1,5$ pour le 30 chiffres, $T = 2$ pour le 45 et $T = 2,6$ pour le 66 chiffres) et M est une borne de l'intervalle du criblage.

3.4. MPQS (Multiple Polynomial Quadratic Sieve) variante de QS par P. Montgomery(1986)

Le polynôme utilisé en crible quadratique $S(x) = (x + [\sqrt{n}])^2 - n$ peut s'écrire aussi $S(x) = (x + b)^2 - n$ en posant $b = [\sqrt{n}]$, alors la taille de $S(x)$ s'accroit quand la valeur de x augmente, dans ce cas la chance de friabilité de $S(x)$ diminue. La variante Polynômes Multiples ou MPQS consiste à améliorer la chance pour le choix de polynôme dans QS. Considérons une forme plus générale $S_{a,b}(x) = (ax + b)^2 - n = a^2x^2 + 2abx + b^2 - n$ pour avoir plus de chance de factoriser n, où a, b sont entiers. Si nous imposons que $0 < b < a$, le graphe de $S_{a,b}(x)$ est un parabole et $S'_{a,b}(x) = 2a^2x + 2ab$. $x = \frac{-b}{a}$ est la solution de l'équation $S'_{a,b}(x) = 0$. En tenant compte la condition précedente $-1 < \frac{-b}{a} < 0$.

Détermination des paramêtres dans MPQS

(i) Choix de a : Soit $x \in [-M, M]$, la plus petite valeur de $S_{a,b}(x) = -n$. En effet

$$\begin{aligned} S_{a,b}\left(\frac{-b}{a}\right) &= a^2\left(\frac{-b}{a}\right)^2 + 2ab\left(\frac{-b}{a}\right) + b^2 - n \\ &= b^2 - 2b^2 + b^2 - n \\ &= -n \end{aligned}$$

Et la plus grande valeur de $S_{a,b}(x) \approx a^2M^2 - n$. En effet

$$\begin{aligned} S_{a,b}(M) &= (aM + b)^2 - n \\ &\approx a^2M^2 - n \end{aligned}$$

pour mettre la plus petite valeur et la plus grande valeur de $S_{a,b}(x)$ de même taille en valeur absolue :

$$\begin{aligned} a^2M^2 - n &= n \\ a^2M^2 &= 2n \\ a^2 &= \frac{2n}{M^2} \\ a &\approx \frac{\sqrt{2n}}{M} \end{aligned}$$

(ii) Choix de b : Choisissons b tel que $a|b^2 - n \Leftrightarrow b^2 - n = ac$ où c un entier, c'est-à-dire $n = b^2 - ac$

$$\begin{aligned} S_{a,b}(x) &= a^2x^2 + 2abx + b^2 - n \\ &= a^2x^2 + 2abx + ac \\ &= a(ax^2 + 2bx + c) \end{aligned}$$

Cela garantit que $a|S_{a,b}(x)$. De plus $(ax + b)^2 = n \cdot S_{a,b}(x)$ c'est-à-dire $(ax + b)^2 \equiv S_{a,b}(x) \pmod{n}$; si $a = q^2$ et que si $(ax^2 + 2bx + c)$ est complètement factorisé dans $F(B)$, alors $(ax + b)^2 \equiv q^2(ax^2 + 2bx + c) \pmod{n}$ est une relation de friabilité qui peut s'écire aussi $((ax + b)q^{-1})^2 \equiv (ax^2 + 2bx + c) \pmod{n}$.

Propriété 3.10. Si $x \in [-M, M]$, alors $\frac{S_{a,b}(x)}{a} = ax^2 + 2bx + c \leq M\sqrt{\frac{n}{2}}$

Preuve. $\frac{C}{a} \leq \frac{a^2M^2-n}{a}$ où $a \approx \frac{\sqrt{2n}}{M}$ et on a $\frac{S_{a,b}(x)}{a} \leq M\sqrt{\frac{n}{2}}$. □

Propriété 3.11. Comme $a|b^2 - n \Leftrightarrow b^2 \equiv n \pmod{q^2}$ où $q^2 = a$. Si q est premier alors n doit être résidu quadratique modulo q.

3.5. SIQS(Self Initializing Quadratic Sieve) variante de QS :

Nous savons dans MPQS que $S(x) = (x + b)^2 - n$ où $b^2 - n = ac$, de plus $S_{a,b}(x) = a(ax^2 + 2bx + c)$ où $a = q^2$ et que q est un assez grand nombre premier. Maintenant posons $a = \prod_{i=1}^{s} q_i$ où $q_i \in F(B)$ pout tout $i \in \{1, \ldots, s\}$. Dans ce cas $S_{a,b}(x)$ est friable si et seulement si $(ax^2 + 2bx + c)$ est friable. Et déterminons b tel que $b^2 \equiv n \pmod{a} \Leftrightarrow b^2 \equiv n \pmod{\prod_{i=1}^{s} q_i}$, alors il y a 2^s de $b \pmod{a}$ qui satisfont cette équation et comme les restes obtenus par $S_{a,b}(x)$ et $S_{a,-b}(x)$ sont les mêmes, donc il nous suffit de prendre la moitié, c'est-à-dire 2^{s-1} polynômes [Con97]. La variante SIQS nous permet beaucoup plus de chance d'avoir plusieurs choix de polynômes que la variante MPQS.

IV. ALGORITHME DE FACTORISATION DE NOMBRES UTILISANT L'ORDINATEUR QUANTIQUE

1. Introduction sur l'Information quantique et notion élémentaire au calcul quantique

1.1. Superposition

Définition 3 (Principe de superposition)**.** L'ensemble des caractéristiques d'un atome, d'un photon ou de tout autre système quantique constituent son *état*. Quand un système a plusieurs états possibles, la somme de ces états est également un état possible : le système se trouve alors dans une superposition d'états. Grâce à ce principe de superposition, une particule peut se trouver dans plusieurs états à la fois [Dou99].

Un ordinateur classique traite des informations élémentaires, des bits classiques(language binaire) ; un ordinateur quantique manipulerait, au lieu de bits classiques, des bits quantiques, appelés *qubits*. Ce sont les systèmes quantiques les plus simples, des systèmes à deux niveaux. Un qubit peut se trouver soit dans l'état $|0\rangle$, soit dans l'état $|1\rangle$. La mécanique quantique est linéaire. Si $|0\rangle$ et $|1\rangle$ sont des états possibles pour le qubit , $(|0\rangle + |1\rangle)/\sqrt{2}$ est aussi un état possible. Un qubit peut donc être suspendu dans une superposition quantique entre les deux états logiques.

Définition 4. On appelle état classique, l'état qu'on peut trouver quand on observe un état.

Définitions 1.1. On appelle état quantique (dont sa norme est égale 1) la superposition des états classiques , c'est-à-dire :

$$|\phi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$$

où $(\alpha_0, \alpha_1) \in \mathbb{C} \times \mathbb{C}$ et $|\alpha_0|^2 + |\alpha_1|^2 = 1$. Dans ce cas $\{|0\rangle, |1\rangle\}$ est une base orthonormale d'un éspace d'Hilbert de dimension 2. Autrement dit $|0\rangle = \binom{1}{0}$ et $|1\rangle = \binom{0}{1}$ sous forme vectorielle. Plus généralement, dans un registre de $n - qubits$, la superposition des états classiques en prenant comme base orthonormale $\left\{ |\underbrace{0\cdots00}_{n\ bits}\rangle, |0\cdots01\rangle, \cdots, |1\cdots11\rangle \right\}$ dans un éspace d'Hilbert de dimension 2^n :

$$|\phi\rangle = \alpha_0|0\cdots00\rangle + \alpha_1|0\cdots01\rangle + \cdots + \alpha_{2^n-1}|1\cdots11\rangle$$

avec $\alpha_k \in \mathbb{C}(k = 0, 1, \ldots, 2^n - 1)$ et $\sum_{k=0}^{2^n-1} |\alpha_k|^2 = 1$. Le nombre complexe α_k est appelé l'amplitude de probabilité de $|k\rangle$ dans $|\phi\rangle$. Intuitivement, l'état quantique $|\phi\rangle$ est dans tous ses états classiques possible en même temps (superposition d'états classiques).

1.2. Observation d'un bit quantique

Supposons que nous allons observer $|\phi\rangle$. Nous ne pouvons pas constater la superposition des états dans $|\phi\rangle$, mais lors d'une mesure ou observation de $|\phi\rangle$ nous trouvons tout simplement un et un seul état classique $|j\rangle$ comme resultat , alors $|\phi\rangle$ devient $|j\rangle$ dont nous ne savons pas préalablement ses caracteritiques, sauf la probabilité d'observer $|j\rangle$ est $|\alpha_j|^2$. Autrement dit, l'observation de $|\phi\rangle$ modifie irrémédiablement la superposition quantique de $|\phi\rangle$ en état classique $|j\rangle$ et toutes les informations pouvant être contenues dans l'amplitudes α_j sont aussi disparues.

Exemple 1.2. Le vecteur $|\phi\rangle = \sqrt{\frac{2}{3}}|0\rangle + \frac{1}{\sqrt{3}}|1\rangle$ est un vecteur unitaire, si l'on observe dans la base $\{|0\rangle, |1\rangle\}$, on a une chance sur trois ($|\frac{1}{\sqrt{3}}|^2$) de mesurer le bit $|1\rangle$, dans ce cas $|\phi\rangle$ devient $|1\rangle$.

Avec un *n bits* un ordinateur classique peut traiter un état parmi 2^n états différents : $00\ldots0$, $00\ldots1$, $\cdots$, $11\ldots1$, alors qu'un ordinateur quantique équipé de processeur de n qubits(quantum bits) permet de gérer 2^n états différents simultanément. Cette capacité de traitement des nombreuses informations simultanéments s'appelle paralélisme quantique. Il y a deux composantes principales en information quantique : d'une part la cryptographie quantique, qui apporte une sécurité accrue par rapport aux systèmes de cryptographie classique, et d'autre part le calcul quantique, pour lequel de nouveaux algorithmes basés sur les principes de la mécanique quantique permettent de diminuer radicalement les temps de calculs nécessaires pour résoudre certains problèmes [PM00]. En 1994, Peter Shor, avait imaginé un algorithme mettant à profit cette propriété pour factoriser de très grands nombres dans un temps *polynomial*, ce qui signifie que l'accroissement de la taille des clefs de cryptage ne serait plus un obstacle insurmontable.

1.3. Transformation quantique de Fourier

Définition 5. Soit $q \in \mathbb{N}$, pour chaque $a \in \mathbb{Z}_q = \{0, \ldots, q-1\}$ définissons l'application χ_a comme suit $\chi_a : \mathbb{Z}_q \longrightarrow \mathbb{C}$ et $\chi_a(b) = e^{2\pi i \frac{ab}{q}}$

Définitions 1.3. L'ensemble $\{|a\rangle / a \in \mathbb{Z}_q\}$ est appelé une base standard et que l'ensemble $\{|\chi_a\rangle / a \in \mathbb{Z}_q\}$ est une base de Fourier où $|\chi_a\rangle = \frac{1}{\sqrt{q}} \sum_{b \in \mathbb{Z}_q} \chi_a(b)|b\rangle$.

Définition 6. Une application qui transforme une base standard en une base de Fourier est appelée Transformation Quantique de Fourier (TQF). En appliquant TQF, chaque $|a\rangle$ devient $|\chi_a\rangle$.

2. Algorithme de Peter Shor(1994) :

2.1. Détermination des facteurs d'un entier n

Soit n l'entier que l'on souhaite factorisé qui n'est ni une puissance d'un nombre premier ni un nombre pair. Supposons que $n = s \cdot t$ où s et t sont premiers. Soit x un entier choisi au hasard tel que $0 < x < q - 1$ où q est de la forme 2^m $(m \in \mathbb{N})$ vérifiant $n^2 \leq q \leq 2n^2$. Notons que q est le seul nombre de la forme 2^m entre n^2 et $2n^2$ car $\left|\frac{1}{2^m} - \frac{1}{2^{m+1}}\right| = \frac{1}{2^m}$ et que $\left|\frac{1}{n^2} - \frac{1}{2n^2}\right| = \frac{1}{n^2}$ et comme $n^2 \leq 2^m \leq 2n^2$ donc $\frac{1}{2n^2} \leq \frac{1}{2^m} \leq \frac{1}{n^2}$. Si $\text{pgcd}(x, n) \neq 1$, alors $\text{pgcd}(x, n)$ est un facteur non trivial de n. Si $\text{pgcd}(x, n) = 1$ et soit r l'ordre de $x \pmod n$ (r est le plus petit entier tel que $x^r \equiv 1 \pmod n$).
$f_n(a) = x^a \pmod n$ est donc une fonction périodique de période r et $f_n(a + r) = f_n(a)$ c'est-à-dire $x^{a+r} \equiv x^a \pmod n$. Si r est pair, posons $y = x^{r/2}$ et nous avons $y^2 \equiv 1 \pmod n$ qui admet quatre solutions :

$$\begin{cases} y_1 \equiv +1 \pmod s \\ y_1 \equiv +1 \pmod t \end{cases}$$

$$\text{donne } y \equiv +1 \pmod{s \cdot t},$$

$$\begin{cases} y_2 \equiv -1 \pmod s \\ y_2 \equiv -1 \pmod t \end{cases}$$

$$\text{donne } y \equiv -1 \pmod{s \cdot t},$$

$$\begin{cases} y_3 \equiv +1 \pmod s \\ y_3 \equiv -1 \pmod t \end{cases}$$

$$\text{donne } y \equiv +k \pmod{s \cdot t},$$

$$\begin{cases} y_4 \equiv -1 \pmod s \\ y_4 \equiv +1 \pmod t \end{cases}$$

$$\text{donne } y \equiv -k \pmod{s \cdot t},$$

Où $y = +k$ et $y = -k$ sont des solutions non triviales de $y^2 \equiv 1 \pmod{s \cdot t}$ (rappelons que si l'un de $(y + 1)$ ou $(y - 1)$ est divisible à la fois par s et t cela conduit à la solution triviale $y \equiv \pm 1 \pmod{s \cdot t}$). Alors si $n = s \cdot t$ et si l'un de $(y+1)$ ou $(y-1)$ n'est pas divisible à la fois par s et t alors, l'un de $(y + 1)$ et $(y - 1)$ doit être divisible par s et l'autre par t. Le facteur s ou t sera trouvé en calculant le $\text{pgcd}(y - 1, n)$ ou le $\text{pgcd}(y + 1, n)$. Et comme $y = x^{r/2}$, cela nous permet par suite de factoriser n en calculant le $\text{pgcd}(x^{r/2} - 1, n)$ ou le $\text{pgcd}(x^{r/2} + 1, n)$[Sho01].

Remarque 2.1. Si n admet plus de deux facteurs cette méthode reste valable en appliquant le même raisonnement par un de facteurs s et son co-facteur correspondant $t = n/s$ qui est composé dans ce cas.

Remarque 2.2. Factoriser ou trouver l'ordre d'un entier arbitraire (c'est-à-dire le logarithme discret de 1 en base x) sont des problèmes équivalents. Tous deux sont difficiles avec un ordinateur classique (*pas de preuve mathématique*)

Exemple 2.3. $N = 15$ l'entier à factoriser, choisissons $x = 7$ (au hasard). Considérons $7^a \pmod{15}$ pour déterminer l'ordre r de $7 \pmod{15}$:

a	$7^a \pmod{15}$
1	7
2	4
3	13
4	1

Tab. IV.1: Détermination de l'ordre r de $7 \pmod{15}$

donc $r = 4$, par suite $\text{pgcd}(7^{4/2} - 1, 15) = \text{pgcd}(7^2 - 1, 15) = \text{pgcd}(4 - 1, 15) = 3$ et $\text{pgcd}(7^{4/2} + 1, 15) = \text{pgcd}(7^2 + 1, 15) = \text{pgcd}(4 + 1, 15) = 5$, cela donne $15 = 3 \times 5$.

2.2. *Détermination de la période r de $x^a \pmod{n}$*

Trouver la période, cas simple : r divise q

Prenons l'entier q de la forme 2^m ($m \in \mathbb{N}$) vérifiant $n^2 \leq q \leq 2n^2$ et préparons deux registres de $[\log q]$ et respectivement de $[\log n]$ zéros : $|0\rangle|0\rangle$.
Appliquons maintenant TQF pour le premier registre

$$|o\rangle|o\rangle \mapsto |\chi_0\rangle|o\rangle = \frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} \chi_0(a)|a\rangle|o\rangle = \frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a\rangle|o\rangle.$$

Calculons maintenant $x^a \pmod{n}$ à l'aide du parallélisme quantique :

$$\frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a\rangle|x^a \pmod{n}\rangle.$$

Observons maintenant le second registre, pour $a \in \mathbb{Z}_q$ de la forme $a = jr + s$ où $s < r$ et $0 \leq j < \frac{q}{r}$, nous avons $x^a \pmod{n} \equiv x^{jr+s} \pmod{n} \equiv x^s \pmod{n}$ (car r est le plus petit entier tel que $x^r \equiv 1 \pmod{n}$). Cela signifie qu'observer $x^a \pmod{n}$ est exactement équivalent à observer $x^s \pmod{n}$, dans ce cas le premier registre devient la superposition de $|s\rangle, |r+s\rangle, |2r+s\rangle, \ldots, |q-r+s\rangle$ et le second registre devient l'état classique $|x^s \pmod{n}\rangle$.
Nous pouvons ignorer maintenant le second registre et nous avons dans le premier registre :

$$\sqrt{\frac{r}{q}} \sum_{j=0}^{q/r-1} |jr + s\rangle.$$

En appliquant encore TQF, c'est-à-dire $|jr+s\rangle \mapsto |\chi_{jr+s}\rangle$, nous obtenons

$$\sqrt{\frac{r}{q}} \sum_{j=0}^{q/r-1} \frac{1}{\sqrt{q}} \sum_{b=0}^{q-1} e^{2\pi i \frac{(jr+s)b}{q}} |b\rangle = \frac{\sqrt{r}}{q} \sum_{b=0}^{q-1} e^{2\pi i \frac{sb}{q}} \left(\sum_{j=0}^{q/r-1} e^{2\pi i \frac{jrb}{q}} \right) |b\rangle. \tag{2.1}$$

En utilisant $\sum_{j=0}^{n-1} a^j = (1-a^n)/(1-a)$ pour $a \neq 1$, nous obtenons

$$\sum_{j=0}^{q/r-1} e^{2\pi i \frac{jrb}{q}} = \sum_{j=0}^{q/r-1} \left(e^{2\pi i \frac{rb}{q}} \right)^j = \begin{cases} q/r & \text{si } e^{2\pi i \frac{rb}{q}} = 1 \\ \frac{1-\left(e^{2\pi i \frac{rb}{q}} \right)^{q/r}}{1-e^{2\pi i \frac{rb}{q}}} = \frac{1-e^{2\pi i b}}{1-e^{2\pi i \frac{rb}{q}}} = 0 & \text{si } e^{2\pi i \frac{rb}{q}} \neq 1 \end{cases}$$

Remarquons que $e^{2\pi i \frac{rb}{q}} = 1$ si et seulement si rb/q est un entier, si et seulement si b est multiple de q/r, c'est-à-dire $b = cq/r$ où c est un entier tel que $0 \leq c < r$, alors nous avons un b tel que $\frac{b}{q} = \frac{c}{r}$ avec b, q sont connus et c, r sont inconnus. Quand nous avons un tel b, nous pouvons obtenir r comme le dénominateur de b/q écrite sous forme irréductible, c'est-à-dire c sera premier avec r avec la probabilité $\frac{\varphi(r)}{r} = \Omega\left(1/log\log r\right)$ car il y a $\varphi\left(r\right) = \Omega\left(r/log\log r\right)$ nombres plus petits que r et premiers avec r [HW79].

Trouver la période, cas difficile : r ne divise pas q

Dans le cas où r ne divise pas q, on peut montrer, en appliquant exactement le même algorithme, qu'on aura b avec une probabilité $P_r(b) = \frac{r}{q^2} \left| \sum_{j=0}^{q/r-1} e^{2\pi i \frac{jrb}{q}} \right|^2$ tel que $\left| \frac{b}{q} - \frac{c}{r} \right| \leq \frac{1}{2q} < \frac{1}{n^2}$ avec b, q sont connus et c, r sont inconnus [dW99]. Or deux fractions différentes de dénominateur au plus n sont séparées par au moins $\left| \frac{\alpha}{\beta} - \frac{\epsilon}{\delta} \right| = \left| \frac{\alpha\delta - \epsilon\beta}{\beta\delta} \right| \geq \frac{1}{\beta\delta} \geq \frac{1}{n^2} > \frac{1}{q}$, donc c/r est la seule fraction de dénominateur inférieur à n dans l'intervalle de centre b/q et de rayon $1/2q$. Le développement en fraction continue de b/q fournit une approximation diophantienne $\frac{c_s}{r_s}$ telle que $r_s < n \leq r_{s+1}$, $\frac{c_s}{r_s}$ est donc une fraction de dénominateur inférieur à n et cette fraction n'est autre que c/r. Le développement en fraction continue de b/q utilise les séquences suivantes :

$$\begin{aligned} a_0 &= \left[\frac{b}{q} \right] \\ \epsilon_0 &= \frac{b}{q} - a_0 \\ a_s &= \left[\frac{1}{\epsilon_{s-1}} \right] \\ \epsilon_s &= \frac{1}{\epsilon_{s-1}} - a_s \end{aligned}$$

$$c_0 = a_0$$
$$c_1 = a_1 a_0 + 1$$
$$c_s = a_s c_{s-1} + c_{s-2}$$
$$r_0 = 1$$
$$r_1 = a_1$$
$$r_s = a_s r_{s-1} + r_{s-2}.$$

Encore, en écrivant b/q sous forme irréductible nous obtiendrons c/r. De plus, si c et r sont premiers entre eux, par suite r sera la période .

Exemple 2.4. $N = 21$ l'entier à factoriser, choisissons $x = 11$ (au hasrd). Et comme $n^2 = 441 < 2^9 < 882 = 2n^2$, nous avons donc $q = 2^9$. Prenons $b = 427$ où $\text{pgcd}(b, q) = 1$, et en développant b/q en fraction continue, nous avons le tableau suivant :

i	a_i	c_i	r_i	ϵ_i
0	0	0	1	0,8339844
1	1	1	1	0,1990632
2	5	5	6	0,02352941
3	42	211	253	0,5

Tab. IV.2: Développement de b/q en fraction continue avec $b = 427$ et $q = 2^9$

On s'arrête pour $6 = r_2 < n = 21 \leq r_3 = 253$, donc $r_2 = 6$ peut être considéré comme la période de f telle que $f(a) = x^a \pmod n$. Par suite $\text{pgcd}(11^{6/2} - 1, 21) = \text{pgcd}(1330, 21) = 7$ et $\text{pgcd}(11^{6/2} + 1, 21) = \text{pgcd}(1332, 21) = 3$, cela donne $21 = 3 \cdot 7$. Remarquons ici que $r_2 \nmid q$.

Remarque 2.5. Dans les cas suivants il est nécessaire de répéter l'algorithme :

(i) La période de $f_n(a) = x^a \pmod n$ est impaire.

(ii) $x^{r/2} \equiv \pm 1 \pmod n$.

(iii) r et c admettent un facteur commun, c'est-à-dire le dénominateur obtenu n'est autre qu'un facteur de la période, non pas la période en question.

(iv) $\left|\frac{b}{q} - \frac{c}{r}\right|$ est assez grand que $\frac{1}{2q}$.

Remarques 2.6. Dans la pratique, nous pouvons prendre une valeur de q de la forme 2^l tel que $2n^2 < q < 3n^2$. Notons encore que q est le seul nombre de la forme 2^l entre $2n^2$ et $3n^2$ car $\left|\frac{1}{2^l} - \frac{1}{2^{l+1}}\right| = \frac{1}{2^l}$ et que $\left|\frac{1}{2n^2} - \frac{1}{3n^2}\right| = \frac{1}{6n^2}$ et comme $2n^2 \leq 2^l \leq 3n^2$ donc $\frac{1}{3n^2} < \frac{1}{2^l} < \frac{1}{2n^2}$. Posons $M \approx q/r$ et $\varsigma = e^{2\pi i \frac{rb}{q}}$, par suite en faisant le même algorithme

qu'auparavant l'équation (2.1) devient :

$$|\varphi\rangle = \sum_{b=0}^{q-1} \frac{e^{2\pi \frac{sb}{q}}}{\sqrt{qM}} \left(\sum_{j=0}^{M-1} \varsigma^j \right) |b\rangle \tag{2.2}$$

notons que :

$$\sum_{j=0}^{M-1} \varsigma^j = \frac{1-\varsigma^M}{1-\varsigma}$$

Si rb/q n'est pas proche d'un entier dans ce cas $\sum_{j=0}^{M-1} \varsigma^j = \frac{1-\varsigma^M}{1-\varsigma}$ est presque nul. Si $rb/q \approx c$ où c est un entier alors $\varsigma \approx 1$ et $P_r(b) = \frac{1}{qM} \left| \sum_{j=o}^{M-1} \varsigma^j \right|^2 \approx \frac{M}{qM} = \frac{1}{q}$ dans ce cas $\frac{b}{q} \approx \frac{c}{r}$. En développant $\frac{b}{q}$ en fraction continue comme le cas précédant, on peut trouver la période r. Si le développement en fraction continue de $\frac{b}{q}$ converge vers $\frac{c_1}{r_1}$, notons que les fractions $\frac{c_1}{r_1}, \frac{2c_1}{2r_1}, \frac{3c_1}{3r_1}, \ldots$ sont $\approx \frac{b}{q}$, il est raisonnable d'essayer à commencer par les petits multiples de r_1 pour les valeurs possible de r (Odlyzko a suggéré d'essayer $r_1, 2r_1, 3r_1, \ldots, \left[\log(n)^{1+\epsilon}\right] r_1$ pour les valeurs possible de r tels que $x^r \pmod n = 1$.

Exemple 2.7. $n = 55$ le nombre que nous allons factoriser, donc $q = 2^{13} = 8192$ car $2n^2 < q = 2^{13} < 3n^2$ et choisissons $x = 13$. Mettons $b = 4915$, cela nous donne $\frac{b}{q} = \frac{4915}{8192} \approx 0,599975585$

$$\frac{b}{q} = \frac{4915}{8192} = \frac{1}{1+\frac{1}{1+\frac{1}{2+\frac{1}{1638}}}}$$

Et comme

$$\frac{1}{1} = 1$$
$$\frac{1}{1+\frac{1}{1}} = \frac{1}{2}$$
$$\frac{1}{1\frac{1}{1+\frac{1}{2}}} = \frac{3}{5}$$
$$\frac{1}{1+\frac{1}{1+\frac{1}{2+\frac{1}{1638}}}} = \frac{4915}{8192}$$

Nous nous arrêtons quand le dénominateur dépasse la valeur de $n = 55$.

a	$13^a \pmod{55}$
5	43
10	34
15	32
20	1

Tab. IV.3: Détermination de la période r de $13^a \pmod{55}$

Alors $r_1 = 5$ le dénominateur de notre fraction juste avant $n = 55$. Donc les possible valeurs

de la période r est les multiples de $r_1 = 5$. Donc d'après le tableau (IV.3) $r = 20$ et $y = 13^{10} \pmod{55} = 34$ et les facteurs de $n = 55$ sont :

$$p = \text{pgcd}(y + 1, n) = \text{pgcd}(35, 55) = 5$$
$$q = \text{pgcd}(y - 1, n) = \text{pgcd}(33, 55) = 11$$

CONCLUSION

La confidentialité des systèmes de cryptographie à clé publique utilisés actuellement repose sur la difficulté algorithmique supposée de certains problèmes, comme par exemple la décomposition de grands nombres en facteurs premiers. Or notre score en utilisant l'ordinateur actuel et les méthodes que nous avons développées ici est encore limité. Un ordinateur quantique pourrait justement arriver à factoriser des grands nombres en un temps éxponentiellement plus court. La recherche pour la réalisation d'un ordinateur quantique est en cours d'experimentation. D'où la nécessité de développer d'autres méthodes de cryptographie, résistantes à une attaque quantique, et l'interêt suscité par les possibilités d'un ordinateur quantique.

La recherche et l'amélioration de l'algorithme de factorisation sont encore très vastes ; *Heureusement que les nombres que nous tentons de factoriser, eux, ne le savent pas* dit C. Pomerance avec humour.

BIBLIOGRAPHIE

[Coh93] H. Cohen, *A Course in Computational Algebraic Number Theory*, Springer-Verlag Berlin Heidelberg New York, 1993.

[Con97] Scott Patrick Contini, *Factoring Integrs with the Self-Initializing Quadratic Sieve*, Master's thesis, University of Georgia, 1997.

[Dou99] Jacqueline Dousson, *2021, l'Odyssée Quantique*, fi 3/99 (1999), pp.1.

[dW99] Ronald de Wolf, *Quantum Computation and Shor's Factoring Algorithm*, CWI and University of Amterdam (1999), pp.8.

[HW79] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, Oxford University Press (1979), pp.354–359.

[Lan01] Eric Landquist, *The Quadratic Sieve Factoring Algorithm*, Math 488 : Crypthographic Algorithm (2001), pp.1–11.

[Len00] A. K. Lenstra, *Integer Factoring*, Designs, codes and crypthography, City bank, N.A, North Gate Road, Mendham, NJ07945-3104, USA (2000), pp.101–128.

[PM00] J. Ph. Poizat and R. Mosseri, *Introduction à l'Information Quantique*, GdR-IQ (Information et communication quantique) (2000), pp.1.

[Rie85] H. Riesel, *Prime Numbers and Computer Methods for Factorization*, Birkhäuser, 1985.

[RSA78] R. L. Rivest, A. Shamir, and L. Adleman, *A Method for Obtaining Digital Sygnatures and Public Key Cryptosystems*, Comm. ACM **21** (1978), pp.120–126.

[Sho01] Peter W. Shor, *Introduction to Quantium Algorithms*, arXiv : quant-ph/0005003 v2 (2001), pp.1–17.

[ST94] Joseph H. Silverman and John Tate, *Rational Points on Elliptic Curves*, Springer-Verlag, 1994.

Nom : RASAMIMANANANTSOA
Prénom : Victor

Titre : METHODES DE FACTORISATION DES GRANDS NOMBRES

Résumé :

Dans ce travail, nous avons trouvés q'il y a deux catégories de méthodes de factorisation :

- Les méthodes dont la complexité de ses algorithmes dépend de la taille de facteurs comme la division trivial, la méthode *(p-1)* de Pollard et la méthode utilisant une courbe elliptique (ECM).
- Et celle qui ne dépend pas de la taille de facteurs comme le crible quadratique et ses variantes.

Dans la dernière partie de notre travail nous avons étudié l'Algorithme de Shor qui pourrait être exécuté avec des procédures utilisant la superposition quantique.

Mots clés: facteurs premiers, courbe elliptique, factorisation, grands nombres, crible, friabilité, quantique.

Title: LARGE INTEGER FACTORIZATION METHODS

Abstract :

In this paper, we have found that there are two types of factorization method:

- The method the algorithm's running time of which depends on the size of the factors like the trivial division, Pollard's *(p-1)-Method* and Elliptic Curve Method.
- And method which does not depend on the size of the factors like Quadratic Sieve and its variants.

In the last part of our study, we have analysed Shor's algorithm which can be realised with procedures using quantum computation.

Key words: primes factors, elliptic curve, factorisation, large integer, sieve, smoothness, quantic.

Encadreur: Docteur Gérard RAZAFIMANANTSOA