N° d'ordre : 32/2010-M/MT

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE
Université des Sciences et de la Technologie
Houari Boumediene
Faculté de Mathématiques

THESE

Présentée pour l'obtention du diplôme de MAGISTER

En : MATHEMATIQUES

Spécialité : Algèbre et Théorie des Nombres

Par Mlle AMRI Hanene

Sujet

FACTORISATION DES GRANDS NOMBRES

Soutenue le : 22 / 07 / 2010, devant le jury composé de :

AIDER Meziane,	**Professeur à l'USTHB,**	**Président.**
ZITOUNI Mohamed	**Professeur à l'USTHB,**	**Directeur de thèse.**
BOUTABIA Hacène	**Professeur, Université d'ANNABA,**	**Examinateurs.**
HACHAÏCHI Mohamed Saleh	**Maitre de conférences à l'USTHB,**	**Examinateurs.**
HERNANE Mohand Ouamar	**Maitre de conférences à l'USTHB,**	**Examinateurs.**

Dédicace

A ma mère Ghania,

A mon père Abdenacer,

A ma Sœur Meriem,

A mon frère Kheireddine,

A mes cousines

Samira, Sarah et Nora,

A mes oncles et tantes,

A mes amies

Sarah, Amira, BEKHOUCHE Saida

et BENATIA Saida,

A mes collègues

ZERIFI Souad, LAANANI Ahlem

et ADRAR Rbiha,

A Anissa, Hafid et leurs enfants Sarah et Akrem,

A tata Malika et ses adorables filles

Soumia, Imen et Fella,

A tous ceux qui m'ont témoigné leur soutien de prés ou de loin.

Remerciements

J'adresse en premier lieu mes remerciements à Monsieur ***ZITOUNI Mohamed****, mon directeur de thèse, pour l'intéressant sujet qu'il m'a proposé. Sa disponibilité alliée à sa gentillesse et ses conseils et ainsi que pour toute la documentation qu'il a mis à ma disposition ont été des éléments décisifs dans l'aboutissement de cette thèse. Je lui dois toute ma reconnaissance. Il m'est impossible de lui exprimer toute ma gratitude en seulement quelques lignes.*

Je tiens a remercie Monsieur ***AIDER Meziane,*** *Professeur à l'USTHB pour m'avoir fait l'honneur de présider le jury de cette thèse.*

J'adresse aussi mes profonds remerciements à Monsieur ***BOUTABIA Hacène*** *Professeur à l'université d'Annaba, l'université ou j'ai passé mes années de graduation.*

Je remercie vivement Monsieur ***HERNANE Mohand Oumar*** *Maitre de conférences à l'USTHB d'avoir accepté d'examiner ce travail en consacrant son temps à lire cette thèse Je remercie aussi Monsieur* ***Mohamed Salah HACHAÏCHI****, Maître de Conférences à l.U.S.T.H.B d'avoir accepté d'examiner ce travail*

TABLE DES MATIERES

INTRODUCTION…… 1

CHAPITRE I : NOMBRES PREMIERS

1-Monoïde *IN* et anneau *ZI* des nombres entiers…….. 2

2-Nombres premiers-Théorème d'Euclide…. 4

3-Nombres premiers entre eux-Théorème de Bezout…… 5

4-Théorème fondamental de l'Arithmétique……. 6

5-Congruences-Corps finis-Théorème chinois des restes…… 7

CHAPITRE II : TESTS DE PRIMALITE

1-Algorithme d'Euclide-Crible d'Eratosthène…….. 12

2-Nombres particuliers :

- Nombres de Mersenne (test de Lucas),…….. 14
- Nombres de Fermat (critère de Pepin),…... 16
- Nombres de Fibonacci……... 18

3-Fonctions arithmétiques…… 19

CHPITRE III : FACTORISATIONS

1- Méthode *RHO* de Pollard……... 24

2- Méthode $p-1$ de Pollard…….. 25

3- Méthode de Fermat…. 28

4- Méthode des cribles…… 29

CHAPITRE IV : FACTORISATION AVEC LES COURBES ELLIPTIQUES

1-Groupes additifs abéliens de Mordell-Weil des Courbes Elliptiques……... 32

2-Méthode de Lenstra…..…… 41

3- Application au codage……..... 50

Quelques résultats ……... 52

CONCLUSION…… 53

BIBLIOGRAPHIE

Introduction

Le problème de factorisation de nombres est résolu par des méthodes arithmétiques élémentaires pour des entiers de moins de 4 chiffres. Pour des nombres plus grands les méthodes sont plus compliquées.

Dans cette thèse de magister sur la « Factorisation des grands Nombres » j'ai réparti mes résultats dans 4 chapitres.

Dans le premier chapitre, j'ai étudié les nombres premiers, le théorème d'Euclide, le théorème de Bezout, le théorème fondamental de l'Arithmétique et le théorème des restes chinois.

Dans le deuxième chapitre, j'ai exposé quelques tests de primalité. J'ai étudié quelques nombres particuliers qui ont un lien avec la factorisation des nombres, j'ai décrit quelques fonctions arithmétiques utiles.

Dans le troisième chapitre, j'ai détaillé quelques méthodes de factorisation ; j'ai trouvé quelques exemples d'application.

Dans le 4éme chapitre, consacré à la méthode de factorisation par des Courbes Elliptiques, j'ai commencé par les notions de base de la théorie des Courbes Elliptiques.

J'ai choisi la méthode de factorisation de LENSTRA.

Chapitre I : NOMBRES PREMIERS

Dans la Théorie des Nombres, les Nombres sont classifiés en plusieurs classes : entiers naturels, entiers rationnels, entiers algébriques, nombres rationnels, nombres transcendants.

1. Monoïde *IN des entiers naturels* et anneau *ZI* des nombres entiers rationnels

Les monoïdes et les anneaux ont des structures algébriques particulières [8],[11].

Définition 1

a) *Un monoïde est un ensemble M muni de deux lois internes :*
Une addition $M^2 \to M, (a,b) \to a+b$, commutative, associative, d'élément neutre 0 :
$$a+b=b+a,\ (a+b)+c=a+(b+c)=a+b+c,\ a+0=0+a=a,$$
pour tous éléments a, b, c de M .

b) *Une multiplication $M^2 \to M, (a,b) \to ab$, commutative, associative, d'élément neutre 1 :*
$$ab=ba,\ (ab)c=a(bc)=abc,\ 1a=a1=a,$$
pour tous éléments a, b, c de M .

c) *La multiplication est distributive par rapport à l'addition :*
$$a(b+c)=ab+ac \quad et \quad (a+b)c=ac+bc.$$
pour tous éléments a, b, c de M .

d) *Les monoïdes ne contiennent ni les symétriques -a des éléments a de M, ni leurs inverses 1/a.*
Donc les monoïdes ne sont ni des groupes additifs, ni des groupes multiplicatifs.

Pour compter des objets, on utilise des entiers naturels.

Définition 2

Les entiers naturels ont pour symboles mathématiques 0, 1, 2, 3, ..., n, ... ; leur ensemble a pour symbole IN= {0, 1, 2,..., n,...}.

Proposition 1

L'ensemble IN des entiers naturels est un monoïde.

Preuve :

L'addition des entiers naturels est commutative, associative, d'élément neutre 0 ;

Pour tout entier naturel *a*, *-a* n'est pas un entier naturel et 1/*a* n'est pas un entier naturel.

□

Corollaire

Le monoïde IN= {0, 1, 2,…, n,…} des entiers naturels est infini.

Preuve :

Soit deux entiers naturels *a* et *b* ; alors *a+b* est un entier naturel.

En particulier, $a+1=a_1,\ (a+1)+1=a_2,\ldots,\ a_n+1=a_{n+1},\ldots$ sont des entiers naturels.

La suite $a,\ a_1=a+1,\ldots,\ a_{n+1}=a_n+1,\ldots$ est donc infinie.

□

C'est la théorie des ensembles qui fournit les notions d'ensembles finis et d'ensembles infinis.
Un ensemble fini est un ensemble qui n'est en bijection qu'avec lui-même ;
Un ensemble infini est un ensemble qui est en bijection avec au moins une de ses parties.

Exemples :

1) L'ensemble $E_{10}=\{0,\ 1,\ldots,\ 10\}$ contient 11 entiers naturels, les parties A= {0, 2, 4, 6, 8} formée de 5 entiers et B= {1, 3, 5, 7} formée de 4 entiers ne sont pas en bijection avec E_{10} ; donc E_{10} est fini.

2) Les ensembles $E_{2n}=\{0,\ 2,\ 4,\ldots\}$ des entiers naturels pairs et $E_{2n+1}=\{1,\ 3,\ 5,\ldots\}$ des entiers naturels impairs sont en bijection avec l'ensemble *IN* par les applications

$$IN\to E_{2n}\ ,\ n\to 2n,\ \ et\ \ \ IN\to E_{2n+1}\ ,\ n\to 2n+1\,.$$

Donc ces ensembles sont infinis.
Le monoïde *IN* des entiers naturels permet de construire un autre ensemble de nombres entiers : les entiers rationnels.

Définition 3

Les entiers rationnels sont les nombres $0,\ \pm 1,\ \pm 2,\ \pm 3,\ldots,\ \pm n,\ldots$ *leur ensemble est* $ZI=\{0,\ \pm 1,\ \pm 2,\ldots\}$

Le symbole Z/ vient de Zahlen=entiers en allemand.

La structure algébrique de cet ensemble *ZI* est précisée par la :

Proposition 2

L'ensemble ZI des entiers rationnels est un anneau principal.

Preuve :

L'addition $ZI^2 \to ZI$; $(a,b) \to a+b$, est commutative et associative ; *ZI* contient les éléments $\pm a$; donc *ZI* est un groupe additif abélien.

ZI contient les entiers rationnels *a* mais pas leurs inverses *1/a* ; donc *ZI* n'est pas un groupe multiplicatif.

Les idéaux de l'anneau *ZI* sont de la forme $I = d\mathbb{Z},\ d \in IN$.

Ces idéaux, admettant un seul générateur, sont des idéaux principaux ; l'anneau *ZI* est principal.

□

2. Nombres premiers –Théorème d'Euclide

Définition 4

a) *Un nombre premier est un entier naturel* $n > 1$ *qui n'est divisible que par lui même et par 1.*

b) *Un nombre composé est un nombre naturel* n *qui admet au moins un diviseur propre* $d \neq 1, n$.

Exemple de nombres premiers

n= 2, 3, 5, 7, 11, 13, 97, 113, 251, 15017.

Exemple de nombres composés

$n = 2 \times 3 = 6$, $5 \times 7 = 35$, $11 \times 97 = 1067$, $13 \times 97 = 1261$.

Théorème de Gauss

1/ Si un entier naturel n ***divise un produit*** ab ***de deux entiers naturels et si*** n ***est premier à*** a***, alors*** n ***divise*** b***.***

2/ Si un nombre premier p ***divise un produit*** ab ***alors*** p ***divise*** a ***ou*** b***.***

□

Dans l'ensemble ci-dessus de nombres premiers, la différence de deux nombres premiers consécutifs n'est pas constante. Il n'y a pas de règle permettant de trouver tous les nombres premiers, d'après Robin la distribution des nombres premiers est irrégulière. [18]

C'est avec des logiciels performants et des algorithmes spéciaux que des spécialistes ont pu calculer un grand nombre de nombres premiers.

Théorème d'Euclide

La suite des nombres premiers est infinie.

Preuve par l'absurde :

Supposons que la suite des nombres premiers est finie.

Soit $p_1 = 2,\ p_2 = 3,\ p_3 = 5, \ldots,\ p_s$, des nombres premiers successifs. (1)

Soit $N = p_1 p_2 \ldots p_n$ leur produit (2)

Alors le nombre $N + 1$ n'est divisible ni par p_1 ni par p_2, ni par p_n (théorème de Gauss) (3)

Il en résulte que $N + 1$ est premier (4)

Ce résultat (4) est donc en contradiction avec l'hypothèse (1).

Il en résulte que (1) est absurde. (5)

Donc la suite des nombres premiers est infinie. (6)

□

3. Nombres premiers entre eux-Théorème de Bezout

Définition 5

Deux entiers rationnels a et b sont premiers entre eux si leur plus grand diviseur commun est égal à 1.

Exemples :

6 et 35 sont premiers entre eux ;

6 et 39 sont divisibles par 3 ; ils ne sont pas premiers entre eux.

Deux nombres premiers p_1 et p_2 sont premiers entre eux.

3 entiers rationnels *a*, *b*, *c* peuvent être premiers entre eux 2 à 2 :

10, 21 et 143 sont premiers entre eux 2 à 2.

3 entiers rationnels *a*, *b*, *c* peuvent être premiers entre eux dans leur ensemble si leur plus grand diviseur est égal à 1 :

10, 21 et 55 sont premiers entre eux dans leur ensemble mais 10 et 55, divisibles par 5, ne sont pas premiers entre eux.

Dans la définition 5, on peut remplacer « deux entiers a et b » par n entiers rationnels $a_1, a_2, ..., a_n$.

Bezout Etienne (1730-1763) a énoncé deux théorèmes : l'un concerne les courbes algébriques, l'autre concerne les entiers rationnels.

Théorème I (de Bezout)

Etant donné deux courbes algébriques planes de l'espace IR^2 ***réel, de degrés*** m ***et*** n ***, le nombre de points d'intersection de ces deux courbes est égal à*** mn ***, en comptant les multiplicités de chaque point.***

□

Points multiples d'ordre 2, 3, …comptés 2 fois, 3 fois,…

Pour plus d'information consulter [14].

Théorème II (de Bezout)

Deux éléments a ***et*** b ***d'un anneau principal A sont premiers entre eux si et seulement si il existe deux éléments*** u ***et*** v ***tels que*** $au + bv = 1$.

La paire (u, v) ***n'est pas unique.***

□

Exemple :

$a = 10$ et $b = 13$ sont premiers entre eux ; alors $10u + 13v = 1$ pour les paires :

$(u, v) = (4, -3), (9, -7), (-10, 7), (-12, 11)$.

4. Théorème fondamental de l'Arithmétique

Tout entier rationnel n ***admet une factorisation unique en produit de puissances de nombres premiers de la forme*** $n = \pm p_1^{n_1} p_2^{n_2} ... p_t^{n_t}$ **,** p_i ***premiers,*** $n_i \in IN^*$**.**

Idée de la preuve :

On effectue les divisions de n par les nombres premiers.

□

Pour les divisions par 2, 3, 5, 9, on utilise les règles de divisibilités

les nombres pairs sont divisibles par 2 ;

les nombres terminés par 0 et par 5 sont divisibles par 5 ;

les nombres dont la somme des chiffres est multiple de 3 sont divisibles par 3 ;

les nombres dont la somme des chiffres est multiple de 9 sont divisibles par 9.

Exemples :

142, 258 et 694 sont des nombres pairs, terminés par les nombres pairs 2, 8, 4.

303 et 744, sont divisibles par 3 ;

234 et 567 sont divisibles par 9.

Pour factoriser des grands entiers, il y a deux méthodes élémentaires.

1) La division euclidienne de n par les nombres premiers $p < \sqrt{n}$,
2) Le crible d'Ératosthène : tableau des entiers naturels $n < N$ où l'on souligne successivement les nombres pairs, les multiples de 3, de 7,…

Les autres méthodes font appel à des techniques particulières ; elles sont décrites dans les chapitres suivants.

5. Congruences-Corps finis-Théorème des restes chinois

La théorie des congruences est un domaine de la Théorie des Nombres.

Définition 6

Deux entiers rationnels a et b sont congrus modulo un entier naturel m si la différence a-b est multiple de m.

$$a \equiv b(\mathrm{mod} m) \quad \text{si et seulement si} \quad a - b = km, \quad k \in ZI.$$

Exemple :

$13 \equiv a(\mathrm{mod} 5)$ *pour* $a = 13 + 5k$, *soit* $a = 13,\ 18,\ 3,\ -12, \ldots$
$a \equiv 7(\mathrm{mod} 8)$ *pour* $a = 7 + 8k$, *soit* $a = 7,\ 15,\ -1,\ 23,\ -9, \ldots$

Définition 7

Les corps finis sont des ensembles IF_q *à* q *éléments,* $q = p^n$, $n \geq 1$, *p premier, munis d'une structure algébrique de corps commutatif,* $IZ/qIZ = IZ/p^n IZ$.

Exemples :

Corps fini $IF_2 = \{0,1\}$, $q = 2$

Corps fini $IF_8 = \{0,1,2,3,4,5,6,7\}$, $q = 2^3$

Corps fini $IF_5 = \{0,1,2,3,4\}$, $q = 5$

Corps fini $IF_9 = \{0,1,2,3,4,5,6,7,8\}$, $q = 3^2$.

Proposition 3

Pour chaque nombre $q = p^n$ ***puissance d'un nombre premier p, il existe un seul corps fini*** IF_q ***à q éléments. Ce corps est une extension algébrique du corps fini*** IF_p ***de dimension*** $\lfloor IF_q : IF_p \rfloor = n$.

Preuve : cf. [10]

□

Les corps finis IF_q sont liés aux polynômes $f_q(X) = X^q - X$.

Définition 8

Soit un polynôme $f(X)$ *de l'anneau* $ZI[X]$*, de degré n, de zéros* $\theta_1, \theta_2, ..., \theta_n$.

Alors , le corps de décomposition de $f(X)$ *est le corps engendré par tous les zéros de F :* $K = Q(\theta_1, \theta_2, ..., \theta_n)$.

Un corps de rupture de f est un corps engendré par un ou plusieurs zéros : $Q(\theta_1), Q(\theta_1, \theta_2)...$

Exemple :

Le polynôme $f(X) = (X^2 - 2)(X^2 - 5)$ *a 4 zéros* $\theta_1 = \sqrt{2},\ \theta_2 = -\sqrt{2},\ \theta_3 = \sqrt{5},\ \theta_4 = -\sqrt{5}$.

Alors $K = Q(\sqrt{2}), Q(\sqrt{5})$ sont des corps de rupture de *f,* $K = Q(\sqrt{2}, \sqrt{5})$ est le corps de décomposition de *f.*

Proposition 4

Pour chaque nombre $q = p^n$***, puissance d'un nombre premier p, le corps fini*** IF_q ***à q éléments, est le corps de décomposition du polynôme*** $f_q(X) = X^q - X$.

Idée de la preuve :

Le polynôme $f_q(X)$ possède *q* zéros :

$\theta_1 = 0, \theta_2 = 1, ..., \theta_q$.

Les zéros $\theta_1 = 0$ *et* $\theta_2 = 1$ sont les éléments neutres du corps.

Les autres zéros sont des éléments du corps fini.

□

Corollaire

Soit un corps fini à q éléments. Alors l'ensemble $IF_q - \{0\}$ ***est un groupe cyclique.***

Preuve : cf. [10]

Un générateur de IF_q est un élément *x* du corps premier à $q-1$.

□

Tout corps fini IF_q possède des automorphismes

$h: IF_q \to IF_q, \quad h(0)=0, \; h(1)=1, \; h(a+b)=h(a)+h(b) \quad et \quad h(ab)=h(a)h(b).$

Proposition 5

Les groupes $Aut(F_q)$ ***des automorphismes des corps finis*** IF_q, $q=p^n$ ***sont cycliques de degré n ; ils sont engendrés par les automorphismes de Frobenius :***

$$Frob: F_q \to F_q, \quad Frob(x)=x^p.$$

Preuve :

Chaque automorphisme *Frob* implique la suite :

$Frob(x), \; Frob^2(x), \; Frob^3(x),...,Frob^n(x)=x^{p^n}=x^q.$

Il en résulte la proposition 5.

□

Examinons les cas des systèmes de plusieurs congruences.

Théorème des restes chinois

Soit n ***entiers naturels*** $m_1, m_2,...,m_n$ ***premiers entre eux deux à deux et leur produit*** $M = m_1 m_2 .. m_n$.

Soit n ***entiers naturels*** $b_j, \quad j=1,2,...,n$ ***qui satisfont les congruences***

$$b_j \frac{M}{m_j} \equiv 1 (\mathrm{mod} m_j),$$

Alors le système des n ***congruences :***

$$\begin{cases} x \equiv a_1 (\mathrm{mod} m_1) \\ x \equiv a_2 (\mathrm{mod} m_2) \\ \ldots\ldots\ldots\ldots\ldots \\ x \equiv a_n (\mathrm{mod} m_n) \end{cases}$$

admet une solution de la forme :

$$x \equiv a_1 b_1 \frac{M}{m_1} + a_2 b_2 \frac{M}{m_2} + \ldots + a_n b_n \frac{M}{m_n} (\mathrm{mod} M)$$

pour tous entiers naturels $a_1, a_2, \ldots, a_n$**.**

Preuve : Dans [13], [19]

□

Exemple 1 :

$$\begin{cases} x \equiv 5 (\mathrm{mod} 7) \\ x \equiv 8 (\mathrm{mod} 19) \end{cases}$$

alors $M = 7 \times 19 = 133$; $b_1 \frac{M}{m_1} = 3 \times 19 = 57$ et $b_2 \frac{M}{m_2} = -8 \times 7 = -56$

Cela implique la solution

$$x = 5 \times 57 + 8(-56) \equiv 103 (\mathrm{mod}\ 133)$$

Exemple 2 :

$x \equiv 4 (\mathrm{mod} 7)$ et $x \equiv 16 (\mathrm{mod} 19)$, alors $M = 7 \times 19 = 133$

$x \equiv 4 \times 57 + 1(-56) \equiv 130 (\mathrm{mod}\ 133)$

Exemple 3 :

Soit le système de congruences :

$x \equiv 3 \pmod 7;\ x \equiv 2 \pmod{10},\ x = 5 \pmod{13}$. Alors $m_1 = 7,\ m_2 = 10$ *et* $m_3 = 13$sont premiers entre eux 2 à 2.

Calcul des b_i

$$\begin{cases} b_1 \times 10 \times 13 \equiv 1 \pmod 7; \\ b_2 \times 7 \times 13 \equiv 1 \pmod{10}; \\ b_3 \times 7 \times 10 \equiv 1 \pmod{13}. \end{cases} \quad \begin{cases} 4b_1 \equiv 1 \pmod 7 \\ b_2 \equiv 1 \pmod{10} \\ 5b_3 \equiv 1 \pmod{13} \end{cases} \quad \begin{cases} b_1 \equiv 2 \pmod 7 \\ b_2 \equiv 1 \pmod{10} \\ b_3 \equiv 8 \pmod{13} \end{cases}$$

Le système admet une solution de la forme :

$$x \equiv a_1 b_1 M' + a_2 b_2 M_2' + a_3 b_3 M_3' \pmod M.$$

$$x \equiv 122 \pmod{910}.$$

Chapitre II : TESTS DE PRIMALITE

Etant donné deux entiers naturels *D* et *d*, $D > d > 0$, ces deux entiers peuvent être premiers entre eux ou divisibles par un entier *a*. le plus grand commun diviseur de D et d est le PGCD de *D* et *d* noté *PGCD(D, d)*.

1. Algorithme d'Euclide-crible d'Ératosthène

Euclide est un mathématicien grec (300 B-C) qui a laissé une œuvre considérable sur les nombres. Il a inventé une méthode de calcul du PGCD de deux entiers naturels qui porte son nom.

La division euclidienne de deux entiers naturels ou algorithme d'Euclide.

Décrivons cet algorithme.

Soient deux entiers naturels $D > d > 0$. (1)

La division euclidienne de *D* par *d* comporte plusieurs étapes.

$$D = dq + r_1 \text{ avec } 0 \le r_1 < d \tag{2}$$

D est le dividende, *d le* diviseur, *q* le quotient et r_1 le reste de la division euclidienne.

Si $r_1 = 0$ alors $D = dq$ et le *PGCD (D, d)=q ;* (3)

Si $r_1 \neq 0$, on poursuit la division euclidienne.

On obtient une suite d'équations diophantiennes

$$\begin{aligned} & d = r_1 q_2 + r_2 \ , \quad 0 \le r_2 < r_1 \ ; \\ & r_1 = r_2 q_3 + r_3 \ , \quad 0 \le r_3 < r_2 \ ; \\ & \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ & r_{n-2} = r_{n-1} q_n + r_n \ , \quad 0 \le r_n < r_{n-1} \ ; \\ & et \quad r_{n-1} = r_n q_{n+1} . \end{aligned} \tag{4}$$

Alors le PGCD des entiers *D* et *d* est égal à : $PGCD(D,d) = r_n$.

Exemple 1 :

D=1683 et d=731

Appliquons l'algorithme d'Euclide :

$1683 = 731 \times 2 + 221;$
$731 = 221 \times 3 + 68;$
$221 = 68 \times 3 + 17;$
$68 = 17 \times 4.$

Il en résulte le résultat : *PGCD (1683 ; 731)=17.*

Exemple 2 :

D=1157 et *d*=681

$1157 = 681 \times 1 + 476;$
$681 = 476 \times 1 + 205;$
$476 = 205 \times 2 + 66;$
$205 = 66 \times 3 + 7;$
$66 = 7 \times 9 + 3;$
$7 = 3 \times 2 + 1.$

Il en résulte que les entiers 1157 et 681 sont premiers entre eux : *PGCD (1157, 681)=1*

L'existence d'une infinité de nombres premiers est établie par le

Théorème de Dirichlet

Soient deux entiers naturels a ***et*** m ***premiers entre eux ; alors il existe une infinité de nombres premiers dans la progression arithmétique de premier terme*** a ***et de raison*** m ***:***

a, a+m, a+2m, …, a+nm,…(forme $a+km$***)***

Preuve : cf. [7]

□

Exemple :

Progression arithmétique de 1^{er} terme *a=6* et de raison *m=5*:

6, 11, 16, 21, 26, 31, 36, 41, 46, 51, 56, 61, 66, 71, 76, 81, 86,…

Dans cette progression arithmétique on trouve les nombres premiers 11, 31, 41, 61, 71, 101,

131, 151, 181, 211,…

Crible d'Ératosthène

Il a été inventé par le mathématicien grec Ératosthène (276-194-B-C). Pour savoir si un entier naturel n est premier, il faut le diviser par tous les nombres premiers $p < \sqrt{n}$.
Dans la suite des entiers naturels de 1 à n, il suffit de souligner les multiples des nombres premiers $p < \sqrt{n}$, les entiers non soulignés sont des entiers premiers.

Dressons le crible pour *n* de *1* à *150*

1 – 2 – 3 – 4 – 5 – 6 – 7 – 8 – 9 – 10 – 11 – 12 – 13 – 14 – 15 – 16 – 17 – 18 – 19 – 20 – 21 – 22 – 23
24 – 25 – 26 – 27 – 28 – 29 – 30 – 31 – 32 – 33 – 34 – 35 – 36 – 37 – 38 – 39 – 40 – 41 – 42 – 43
44 – 45 – 46 – 47 – 48 – 49 – 50 – 51 – 52 – 53 – 54 – 55 – 56 – 57 – 58 – 59 – 60 – 61 – 62 – 63
64 – 65 – 66 – 67 – 68 – 69 – 70 – 71 – 72 – 73 – 74 – 75 – 76 – 77 – 78 – 79 – 80 – 81 – 82 – 83
84 – 85 – 86 – 87 – 88 – 89 – 90 – 91 – 92 – 93 – 94 – 95 – 96 – 97 – 98 – 99 – 100 – 101 – 102
103 – 104 – 105 – 106 – 107 – 108 – 109 – 110 – 111 – 112 – 113 – 114 – 115 – 116 – 117 – 118
119 – 120 – 121 – 122 – 123 – 124 – 125 – 126 – 127 – 128 – 129 – 130 – 131 – 132 – 133 – 134
135 – 136 – 137 – 138 – 139 – 140 – 141 – 142 – 143 – 144 – 145 – 146 – 147 – 148 – 149 – 150.

Il en résulte les nombres premiers :

$p = 2 – 3 – 5 – 7 – 11 – 13 – 17 – 19 – 23 – 29 – 31 – 37 – 41 – 43 – 47 – 53 – 59 – 61 – 67 –$
$71 – 73 – 79 – 83 – 89 – 97 – 101 – 103 – 107 – 109 – 113 – 127 – 131 – 137 – 139 – 149.$

2. Nombres particuliers

Il en existe plusieurs : nombres de Fermat, nombres de Mersenne, nombres de Fibonacci,…

Nombres de Mersenne

Définition 1

Les nombres de Mersenne sont les entiers naturels de la forme :

$$M_q = 2^q - 1 \ \ pour \ \ q = 0,\ 1,\ 2,\ 3,...$$

Mersenne est un mathématicien français (1586-1648)
Avec cette formule nous obtenons les nombres de Mersenne

$M_0 = 0$; $M_1 = 1$; $M_2 = 3$; $M_3 = 7$; $M_4 = 15$; $M_5 = 31$; $M_6 = 63$; $M_7 = 127$; $M_8 = 255$
$M_9 = 511$; $M_{10} = 1023$; $M_{11} = 2047$; $M_{12} = 4095$;…

En 1886, Perrusin et Soelhoff ont montré que M_{61} est premier.

En 1876, le test de Lucas a permis de déterminer les nombres M_q premiers.

Hurwitz, Selfridge, Riesel ont trouvé les M_q premiers pour q=89, 107, 521, 607, 1279, 2203, 2281, …, 11213.

Le nombre M_{11213} possède 3375 chiffres.

Nelson et Gage (1996) Cameron et Kurowski (2001) ont étudié les M_q

Dans la suite $M_0, M_1, ..., M_{12}$ ci dessus $M_2 = 3,\ M_3 = 7,\ M_7 = 127$ sont des nombres premiers ; cette propriété ne se généralise pas.

Jusqu'à ce jour on connait 47 nombres de Mersenne premiers. Le dernier a été découvert en 2008, il comporte 12978189 de chiffres, il a été découvert dans le projet GIMPS (Great Internet Mersenne Prime Search).

Théorème 1

Si le nombre de Mersenne $M_q = 2^q - 1$ ***est premier, alors q est premier,*** $q > 1$**.**

Preuve :

Factorisation de M_q .

$$M_q = (2-1)\left(2^{q-1} + 2^{q-2} + ... + 2 + 1\right)$$

L'hypothèse « M_q premier » implique :

$$2^{q-1} + 2^{q-2} + ... + 2 + 1 = N \quad \text{est premier}$$

Si q n'est pas premier, alors q=ab, produit de deux entiers naturels.

Alors

$$M_q = 2^q - 1 = 2^{ab} - 1 = \left(2^a - 1\right)\left(2^{a(b-1)} + 2^{a(b-2)} + 2^a + 1\right),$$

Ainsi $M_q = 2^q - 1$ n'est pas premier.

□

Par exemple, les nombres de Mersenne M_{23}, M_{29}, M_{37}, M_{41} ne sont pas premiers.

Théorème 2 (Test de Lucas-Lehmer)

Si les entiers a et n satisfont les congruences

$a^{(n-1)} \equiv 1 \pmod{n}$ et $a^{(n-1)/p} \neq 1 \pmod{n}$ ***pour tout diviseur premier*** p ***de*** $n-1$, ***alors*** n ***est premier.***

Exemple :

Soit $n = 2003$ et $a = 5$

Alors les diviseurs premiers de $n - 1 = 2002$ sont: $2, 7, 11, 13$

On a : $a^{(n-1)} \equiv 5^{2002} \equiv 1 \pmod{2003}$, (1)

pour $p=2$ on trouve: $a^{(n-1)/p} \equiv 5^{1001} \equiv -1 \pmod{2003}$, (2)

pour $p=7$ on trouve: $a^{(n-1)/p} \equiv 5^{286} \equiv 874 \pmod{2003}$, (3)

pour $p=11$ on trouve: $a^{(n-1)/p} \equiv 5^{182} \equiv 886 \pmod{2003}$, (4)

pour $p=13$ on trouve: $a^{(n-1)/p} \equiv 5^{154} \equiv 633 \pmod{2003}$, (5)

(1), (2), (3), (4) et (5) impliquent que $n = 2003$ est premier.

Théorème 3

Soit un entiers naturel $n>1$ ***impair qui satisfait les congruences***

$a^{(n-1)/2} \equiv -1 \pmod{n}$ et $a^{(n-1)/2p} \neq -1 \pmod{n}$ ***pour tout diviseur premier*** p ***de*** $n-1$, ***alors*** n ***est premier.***

□

Théorème 4 (Test de Lucas-Lehmer)

Soit p un nombre premier impair, le nombre de Mersenne $M_q = 2^q - 1$ ***est premier, si et seulement si*** $2^p - 1$ ***divise*** $S(p-1)$ ***où*** $S(n+1) = S(n)^2 - 2$ ***et*** $S(1) = 4$.

Preuve: cf. [9]

□

Exemple:

Je prends $p=7$, $M_p = 127$ je calcule $S(6)$.

$S(1) = 4$

$S(2) = 4^2 - 2 = 14$

$S(3) = 14^2 - 2 = 194$

$S(4) = 194^2 - 2 = 37634$

$S(5) = 37634^2 - 2 = 1416317954$

$S(6) = 2005956548822746114 = 127 \times 15794933493549182$

Donc M_7 est premier car $M_p = 127$ divise $S(6)$.

Nombres de Fermat

Définition 2

Les nombres de Fermat sont les entiers naturels de la forme

$$F_n = 2^h + 1 \quad avec \quad h = 2^n, n \in IN$$

Exemples :

$F_0 = 3$; $F_1 = 5$; $F_2 = 17$; $F_3 = 257$; $F_4 = 65.537$; $F_5 = 641 \times 6700417$;

$F_6 = 274177 \times 67280421310721$,

Ce sont des entiers naturels avec un grand nombre de chiffres.

Ces nombres sont premiers pour n = 0, 1, 2, 3, 4, 8, 9, 10, 11, …ils sont composés pour n = 5, 6, 7, et $12 \le n \le 24$. Le nombre F_{24} a été factorisé, en 1999, par l'équipe de 3 chercheurs Crandall-Mayer-Papadopoulos. En 2001, les 2 chercheurs Kruppa et Forbes ont trouvé un diviseur d de 23 chiffres de F_{31} :

$$d = 4693163567\ 7864055013\ 377$$

Fermat est un mathématicien français (1601-1665).

Il est célèbre par la conjecture qu'il a énoncée :

Conjecture de Fermat

L'équation diophantienne :

$$x^n + y^n = z^n$$

n'admet pour $n > 2$*, que les solutions triviales*

$$(x, y, z) = (1, 0, 1), (0, 1, 1)$$

Cette conjecture ne sera complètement démontrée qu'aux 19éme Journées Arithmétiques, à Bordeaux, en 1993.

La démonstration fait intervenir la courbe elliptique de Fermat :

$$x^3 + y^3 = z^3$$

Théorème (Petit théorème de Fermat)

Pour tout nombre premier *p****, tout entier naturel*** *a* ***premier à*** *p* ***satisfait la congruence modulo*** *p*

$$a^p \equiv a (\mathrm{mod} p)$$

Preuve : cf. [21], [1]

□

Avec la fonction arithmétique φ d'Euler, ce théorème devient :

Théorème (Euler-Fermat)

Pour tout entier naturel m***, tout entier naturel*** a ***premier à*** m ***satisfait la congruence modulo*** m***, avec la fonction arithmétique*** φ ***d'Euler.***

$$a^{\varphi(m)} \equiv 1(\mathrm{mod} m)$$

Preuve : cf. [21]

□

Pour tester si un Nombre de Fermat est premier on peut utiliser le

Test (Pepin-1877)

Soit n un entier naturel non nul, F_n *est premier si et seulement si*

$$3^{\frac{(F_n-1)}{2}} \equiv -1(\mathrm{mod} F_n).$$

Ces test sont appliqués par l'intermédiaire d'algorithmes et de programmes exécutés par ordinateur.

Nombres de Fibonacci

Définition 3

Les nombres de Fibonacci sont les entiers naturels u_n *satisfaisant les récurrences :*

$$u_0 = 0,\ u_1 = 1 \quad \text{et} \quad u_{n+2} = u_{n+1} + u_n\ ,\ \text{pour} \quad n \geq 0$$

Exemples :

$u_2 = 1$; $u_3 = 2$; $u_4 = 3$; $u_5 = 5$; $u_6 = 8$; $u_7 = 13$; $u_8 = 21$; $u_9 = 34$; $u_{10} = 55$;

$u_{11} = 89$; $u_{12} = 144$; $u_{13} = 233$; $u_{14} = 377$; $u_{15} = 610$; $u_{16} = 987$; $u_{17} = 1597$; $u_{18} = 2684$

$u_{19} = 4181$; $u_{20} = 6765$.

Les nombres de Fibonacci satisfont plusieurs relations

1) $u_n = \frac{1}{\sqrt{5}}\left\{\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right\}; n = 2,3,...$

2) $\left(\frac{1+\sqrt{5}}{2}\right)^{n-1} < u_{n+1} < \left(\frac{1+\sqrt{5}}{2}\right)^n \qquad pour \quad n > 1$

3) $u_n = \binom{n-1}{0} + \binom{n-2}{1} + \binom{n-3}{2} + ... + \binom{n-j}{j-1} \qquad pour \quad n \geq 2 \qquad et \quad 2j \leq n+1$

Il s'agit des coefficients du binôme $\binom{a}{b}$, a et b entiers naturels $a > b$

$\binom{a}{b} = \frac{a!}{b!(a-b)!}$, où $a! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot a =$ produit des entiers de 1 à a.

$\binom{a}{b} = \frac{a(a-1)..(a-b+1)}{b(b-1)..3 \times 2 \times 1}$

$\binom{a}{0} = \binom{a}{a} = 1$

3. Fonctions arithmétiques

Elles sont nombreuses

Définition 4

Une fonction arithmétique est une fonction des entiers naturels

$f : IN \to A \subset \mathbb{C}$, $\mathbb{C}$= corps des nombres complexes

Exemples :

Fonction plus grand entier, fonction d'Euler, fonction de Möbius,…

Fonction arithmétique Phi d'Euler

Définition 6

La fonction d'Euler est la fonction arithmétique

$$\varphi : IN^{\times} \to IN,$$

de valeurs

$$\varphi(n) = \sum_{\substack{d \text{ premier} \\ \text{à } n \quad d<n}} 1 = \text{nombre d'entiers } d < n \text{ et premiers à } n$$

et $\varphi(1) = 1$

Exemples :

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
$\varphi(n)$	1	1	2	2	4	2	6	4	6	4	10	4	12	6	8	8	16	6	18	8

Théorème

La fonction arithmétique $\phi(n)$ ***d'Euler satisfait les relations***

1) $\phi(mn)=\phi(m)\phi(n)$ ***pour tous entiers naturels*** m ***et*** n ***premiers entre eux ;***

2) $\phi(n)=n\prod_{p/n}\left(1-\frac{1}{p}\right)$***, p premier.***

3) $\phi(p^r)=p^r-p^{r-1}=p^{r-1}(p-1)$***, pour tout nombre premier*** p ***et tout entier*** r ***;***

4) $\varphi(2n)=\varphi(n)$ ***pour tout nombre impair*** n ***;***

5) $\varphi(p_1^{r_1}\ldots p_t^{r_t})=\prod_i\varphi(p_i^{r_i})$ avec $p_i\neq p_j,\ i\neq j$ ***;***

6) $\sum_{d/n}\varphi(d)=n$**.**

Preuve : cf. [1]
□

Exemples :

$$\phi(3^2\times5^4)=\phi(3^2)\times\phi(5^4)=(3\times2)(5^3\times4)=24\times5^3$$

$$\phi(49)=\phi(7^2)=7\times6=42$$

$$\phi(2^2)=2;\phi(2^3)=2^2=4;\phi(2^4)=2^3=8;\phi(2^r)=2^{r-1},\ r\geq1.$$

Fonction arithmétique Tau

Définition 6

La fonction arithmétique Tau est égale à : $\tau(n)=$ *nombre de diviseurs positifs de n*

$$\tau(n)=\sum_{d/n}1.$$

Exemples :

$$\tau(1)=1,\ \tau(2)=\tau(3)=\tau(4),\ \tau(5)=\tau(7)=2$$

et pour tous p premier, on a $\tau(p)=1$

Définition 7

La fonction arithmétique Sigma est égal à :

$$\sigma(n)=\text{Somme des diviseurs positifs de } n=\sum_{\substack{d/n\\ d>n}}d,\ .$$

Exemples :

$\sigma(1)=1, \sigma(2)=3, \sigma(5)=6, \sigma(10)=18.$

Théorème

Les fonctions σ et τ sont multiplicatives :

$$\sigma(mn)=\sigma(m)\sigma(n) \text{ et } \tau(mn)=\tau(m)\tau(n).$$

Preuve : cf. [1]

□

Corollaire

Pour tout nombre premier p , et tout entier $r \geq 1$ on a:

$$\sigma(p^r)=(p^{r+1}-1)/(p-1) \text{ et } \tau(p^r)=r+1.$$

Définition 8

La fonction de Möbius est la fonction arithmétique $\mu : \mathrm{N} \to ZI$ de valeurs

$$\begin{cases} \mu(1)=1 \\ \mu(n)=0 \quad si \quad n \ a \ un \ facteur \ carré \\ et \ \mu(n)=(-1)^t \ si \ n=p_1 p_2 \ldots p_t, \ p_i \ premiersdistints \end{cases}$$

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$\mu(n)$	1	-1	-1	0	-1	1	-1	0	0	1	-1	0	-1	1

Le problème de l'inversion de la fonction $\mu(n)$ a été résolu par Möbius lui-même (1790-1868). [1]

Théorème (formule d'inversion de Möbius)

Soient deux fonctions arithmétiques f et g .

Si $f(n)=\sum_{d/n} g(d)$, alors $g(n)=\sum_{d/n} f(d)\mu\left(\frac{n}{d}\right)$, où μ = fonction de Möbius.

Preuve : cf. [1]

□

Ce théorème admet deux corollaires.

Corollaire 1

$\sum_{1\le m\le n} \mu(m)\left[\frac{n}{m}\right] = 1$, $\left[\frac{n}{m}\right]$ = ***plus grand entier de*** $\frac{n}{m}$

Preuve : avec $f = \mu$ et $g = \upsilon$, $\upsilon(n) = 1$

□

Corollaire 2

Soit la fonction $\tau(n)$ = ***somme des diviseurs*** $d > 0$ ***de*** n***. Alors :***

$$\sum_{1\le m\le n} \tau(m) = \sum_{1\le m\le n} \left[\frac{n}{m}\right]$$

Preuve : cf. [1]

□

Définition 9

La fonction de Von Mangoldt $\Lambda : IN^* \to IR$ *a pour valeurs*

$$\begin{cases} \Lambda(n) = \log p \text{ si } n = p^r \text{ avec } p \text{ premier et } k \ge 1 \\ et\ \Lambda(n) = 0 \quad \text{sinon} \end{cases}$$

Cette fonction intervient en Théorie des Nombres.

Il existe une multiplication spécifique des fonctions arithmétiques : le produit de Dirichlet (produit de convolution) de deux fonctions arithmétiques.

Définition 10

Le produit de Dirichlet de deux fonctions arithmétiques f *et* g *est la fonction arithmétique* $f * g : IN^* \to IN$ *de valeur* $(f*g)(n) = \sum_{d/n} f(d)g(n/d) = \sum_{d_1 d_2 = n} f(d_1)g(d_2)$

Ce produit est commutatif : $f * g = g * f$.

Ce produit est associatif :

$$((f*g)*h)(n) = \sum_{d_1 d_2 d_3 = n} f(d_1)g(d_2)h(d_3).$$

Théorème

L'ensemble des fonctions arithmétiques f ***telles que*** $f(1) \neq 0$ ***est un groupe pour le produit de Dirichlet.***

Preuve : cf. [15]

Chapitre III : FACTORISATIONS

Elles sont nombreuses et variées d'après les références

1. La méthode *RHO* de POLLARD [6]

Cet algorithme a été présenté par J. Pollard en 1975.

Algorithme de la méthode de factorisation RHO de Pollard

Soit un ensemble $S=\{0,1,...,l-1\}$, une fonction aléatoire $f: S \to S$ et les suites de valeurs itérées :

$$s,\ f(s),\ f^2(s),...$$

Cette suite prend un nombre fini *l* de valeurs ; donc des termes peuvent être répétés.

Pour $l=p$ premier, $S=\{0,1,...,p-1\}$, soit $f(x)=x^2+1(\mathrm{mod}\,p)=F(x)$.

Soit $F^{(j)}(s)=F^{(k)}(s)$. Alors $PGCD\left(F^{(j)}(s)-F^{(k)}(s),n\right)$ est divisible par *p*.

POLLARD calcule ces $PGCD\left(F^{(j)}(s)-F^{(k)}(s),n\right)$ pour $i=1,2,...$ jusqu'à la factorisation de *n*.

Soit un nombre *n* composé. *C*et algorithme comporte plusieurs étapes décrites ci-dessous.

1. ***Choix des éléments pour trouver un facteur de n***

   Choisir un nombre aléatoire $a\in[1,n-3]$;

   Choisir $U,V\in[0,n-1]$.

   Définir la fonction $F(x)=(x^2+a)\ \mathrm{mod}n$;

2. ***Chercher les facteurs***

   $U=F(U)$;

   $V=F(V)$;

   $V=F(V)$; ***// Remplacer*** *V* ***par*** $F(V)$ ***deux fois.***

   $g=PGCD(U-V,n)$;

   Si $(g=1)$ ***aller à l'étape 2;***

3. ***Mauvais choix***

   Si $(g=n)$ ***aller à l'étape 1 ;***

4. ***Succès***

   g ***est un facteur non trivial de*** *n*

Exemple :
Factoriser n=8051(n est un nombre composé), avec le polynôme $f(x)=x^2+1$.

Soit $U = V = 1$, appliquons l'algorithme :

u	***v***	***u-v***	***g=PGCD (U-V, n)***
1	1		
2	2		
2	5	3	1
5	26		
5	677	672	1
26	7474		
26	2839	2813	1
677	871		
677	1848	1171	97

Le facteur non trivial est 97, J'obtiens la factorisation de n : $8051 = 97 \times 83$.

2. Méthode *p-1* de Pollard

La Méthode *p-1* de J. Pollard utilise le petit théorème de Fermat pour factoriser n.

Donc, si p est un facteur premier d'un entier n, alors p divise le $PGCD\left(2^{p-1}-1, n\right)$. Si nous trouvons un entier g multiple de p -1, le $PGCD\left(2^{p-1}-1, n\right)$ sera égal à un facteur non trivial de n.

Algorithme (la méthode *p*-1 de Pollard)

Soit un nombre composé n et une borne $B \in IN^*$. Cet algorithme permet de trouver un facteur non trivial de n.

1. ***Suite des nombres premiers***

   Calculer $p_1 < p_2 < \ldots < p_m \leq B$ ***, et pour chaque nombre premier*** p_i ***,***

   l'exposant maximal e_i ***tel que*** $p_i^{e_i} \leq B$ ***;***

2. ***Exécution des échelles de puissance***

   $c = 2$ ***;***

   Pour $(1 \leq i \leq m)$ {

   Pour $(1 \leq i \leq e_i)$

   $c = c^{p_i^{e_i}} \pmod{n}$ ***;***

3. ***Test du pgcd***

   $g = PGCD\ (c-1, n)$**, Le facteur non trivial est trouvé si** 1< g < n**.**

Il y a deux cas où cette méthode *p-1* de Pollard peut échouer

1) Si *PGCD (c-1, n) = 1,* ou
2) Si *PGCD (c-1, n) = n*,

Dans ces deux cas, nous augmentons la valeur de *B* et nous recommençons l'algorithme.

Exemple :

Factoriser n = 136 838 612 177(n est un nombre composé).

Je prends c = 2, B = 100

1. $2^6 \le B$ puis $c^{2^6} \pmod{n} = 122567948276$ et $PGCD(c^{e_1} - 1, n) = 1$
2. $3^4 \le B$ puis $c^{e_1 3^4} \pmod{n} = 256944916212$ et $PGCD(c^{e_2} - 1, n) = 1$
3. $5^2 \le B$ puis $c^{e_2 5^2} \pmod{n} = 256944916212$ et $PGCD(c^{e_3} - 1, n) = 1$
4. $7^2 \le B$ puis $c^{e_3 7^2} \pmod{n} = 108770095004$ et $PGCD(c^{e_4} - 1, n) = 1$
5. $11 \le B$ puis $c^{e_4 11} \pmod{n} = 845988529959$ et $PGCD(c^{e_5} - 1, n) = 1$
6. $13 \le B$ puis $c^{e_5 13} \pmod{n} = 260882728880$ et $PGCD(c^{e_6} - 1, n) = 1$
7. $17 \le B$ puis $c^{e_6 17} \pmod{n} = 577952173440$ et $PGCD(c^{e_7} - 1, n) = 1$
8. $19 \le B$ puis $c^{e_7 19} \pmod{n} = 131992584210$ et $PGCD(c^{e_7} - 1, n) = 1$
9. $23 \le B$ puis $c^{e_8 23} \pmod{n} = 890645994557$ et $PGCD(c^{e_9} - 1, n) = 133723$

D'où la factorisation $n = 133723 \times 1023299$

Il existe plusieurs versions de la deuxième phase de cet algorithme :

Soit $M = M(k)$ = *PPCM (1,..., k) ;* le plus petit commun multiple des nombres entiers jusqu'à k. Alors,

$$M(1) = 1,\ M(2) = 2,\ M(3) = 6,\ M(4) = 12,\ldots \text{ etc.}$$

La suite $M(1),\ M(2),\ M(3),\ldots$ peut être calculée par récurrence comme suit :

Si *k +1* n'est pas un nombre premier ou une puissance d'un nombre premier, alors

$$M(k+1) = M(k).$$

Si $k+1 = p^a$, où p est un nombre premier, alors

$$M(k+1) = pM(k).$$

A l'aide de la méthode d'Eratosthène décrite dans le deuxième chapitre nous pouvons trouver tous les nombres premiers jusqu'à une certaine limite.

Ainsi, la suite $M(1),\ M(2),\ M(3),...$ peut être obtenue ;

Algorithme

1- Choisir un entier $B \in N^*$ et un entier $k \in N$ tels que :

$$k = PPCM(1,...,B).$$

2- Choisir un nombre *c* de l'ensemble {2,…, *n*-2} et calculer

$$c^k \pmod{n} \text{ et } d = PGCD(c^k - 1, n) \text{ avec l'agorithme d'Euclide.}$$

Si *d* est différent de 1 et *n*, alors nous avons trouvé un facteur non trivial de *n* et l'algorithme est terminé.

Si *d* est égal à 1 ou *n* nous faisons un autre choix de *c* dans {2,…, *n*-2} et un autre choix de *k* et nous augmentons la valeur de *B*.

Nous supposons que *n* admet un facteur premier *p* tel que *p*-1 est une puissance de petit nombre premier inférieur à la borne *B* ; alors *p*-1 divise *k*, d'après le petit théorème de FERMAT, $c^k \equiv 1 \pmod{p}$ donc *p* divise $c^k - 1$, ainsi *p* divise $PGCD(c^k - 1, n)$.

L'algorithme de Pollard a peu de chance de fonctionner, car il n'est pas fréquent que *p*-1 soit puissance de petit nombres premiers.

Exemple :

Factoriser *n*=2546907 ; *n* est un nombre composé puisque la somme de ses chiffres est multiple de 3.

Je choisis *B*=16 et *c*=5 ;

k=PPCM (1,2,…, 16)= $2^4 \times 3^2 \times 5 \times 7 \times 11 \times 13 = 720720$

$5^{720720} \pmod{2546907} = 1678051$

Je calcule le $PGCD(1678050,\ 2546907)$ par l'algorithme d'Euclide.

Je trouve le $PGCD(1678050, 2546907) = 3729$,

La factorisation de *n* est égale à : 3729×683 .

Pour factoriser 3729, j'utilise les mêmes étapes de la méthode :

Je prends *B*=7 et *c*=5 et j'obtiens $3729 = 33 \times 113$

D'où la factorisation de *n* : $n = 3 \times 11 \times 113 \times 683$.

Avec une version « optimisée », un facteur de 39 chiffres du 575^{éme} nombre de FIBONACCI a été découvert par P.L. Montgomery.

3. La méthode de Fermat

En 1643, Fermat propose une méthode basée sur l'identité algébrique « différence de 2 carrés »

$$x^2 - y^2 = (x + y)(x - y),$$

ainsi l'objectif est de trouver deux entiers *a* et *b* tels que

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

Algorithme

1. Remplacer *a* par $\lfloor \sqrt{n} \rfloor$
2. Calculer $a^2 - n$
3. Si $a^2 - n$ est un carré, calculer $b = \sqrt{a^2 - n}$, la factorisation de *n* est trouvée
$$n = (a - b)(a + b)$$
Sinon remplacer *a* par *a+1* et revenir a l'étape 2.

Exemple 1 :

Factoriser 8051

$8051 = 8100 - 49 = 90^2 - 7^2$ d'où $8051 = 97 \times 83$.

Exemple 2 :

Factoriser *n* = 10 235 789, *n* est un nombre composé.

a	a^2-n	$\sqrt{a^2-n}$	a	a^2-n	$\sqrt{a^2-n}$
3200	4211	64.892	3213	87580	295.939
3201	10612	103.015	3214	94007	306.606
3202	17015	130.442	3215	100436	316.916
3203	23420	153.036	3216	106867	326.905
3204	29827	172.705	3217	113300	336.601
3205	36236	190.358	3218	119735	346.027
3206	42647	206.511	3219	126172	355.207
3207	49060	221.495	3220	132611	364.158
3208	55475	235.531	3221	139052	372.897
3209	61892	248.781	3222	145495	381.438
3210	68311	261.364	3223	151940	389.795
3211	74732	273.371	3224	158387	397.979
3212	81155	284.877	3225	164836	406.000

J'obtiens la factorisation de *n :*

$$n=(3225-406)(3225+406)=2819\times 3631$$

4. Méthode des cribles

Pour la recherche de diviseurs d'un nombre *n* composé, on peut employer une autre méthode ; elle est basée sur la recherche des nombres entiers naturels *X* et *Y* tels que *n* soit un diviseur de X^2-Y^2.

Si *n* divise X^2-Y^2, il divise aussi $(X-Y)(X+Y)$. Si *n* n'est pas un diviseur de $X+Y$ ou de $X-Y$, alors un diviseur propre de *n* doit diviser $X-Y$, et un autre diviseur propre de *n* doit diviser $X+Y$. Ainsi le plus grand diviseur commun de *n* et de $X-Y$, est plus grand que 1, et donc est l'un des diviseurs cherchés. Choisissions par exemple *n=7429, X=227* et *Y=210*. Le nombre 7429 est un diviseur de $X^2-Y^2=7429$, mais il n'est pas un diviseur de $X-Y=17$ ni un diviseur de $X+Y=437$. Le pgcd de 17 et de 7429 est 17, et c'est un diviseur propre de 7429.

Alors pour trouver *X* et *Y*, on établit d'abord un système d'équations linéaires : puis on détermine *X* et *Y* à partir des solutions de ce système. Le nombre d'équations dépend de la taille du nombre à factoriser ; pour un nombre de 120 chiffres il faut à peu prés 245000

équations pour autant d'inconnues donc c'est la taille du nombre à factoriser qui détermine le temps de calcul.

Soit une suite de carrés ayant deux propriétés : ils sont proches de *n* et leur différence avec *n* est au signe prés, un produit de petits nombres premiers. Pour *n=7429*, les carrés 83^2, 87^2 et 88^2 conviennent, car les différences sont des produits des nombres premiers 2, 3, 5 et 7 :

$$83^2 - 7429 = -540 = (-1) \times 2^2 \times 3^3 \times 5$$

$$87^2 - 7429 = 140 = 2^2 \times 5 \times 7$$

$$88^2 - 7429 = 315 = 3^2 \times 5 \times 7.$$

D'après [4], quand on multiplie membre à membre certaines de ces lignes les unes par les autres, les exposants des décompositions s'additionnent. Si la somme des exposants est paire pour chaque facteur premier, alors le produit est un carré. Par exemple,

$$(87^2 - 7429) \times (88^2 - 7429) = 2^2 \times 3^2 \times 5^2 \times 7^2 = (2 \times 3 \times 5 \times 7)^2 = 210^2.$$

Dés lors, pour trouver *X* et *Y*, on applique les règles des calculs de congruences.

On obtient

$$(87 \times 88)^2 \equiv (87^2 - 7429) \times (88^2 - 7429) \pmod{7429}.$$
$$\text{donc} (87 \times 88)^2 \equiv 210^2 \pmod{7429}$$

Dans cette équation, on remplace 87×88 par son reste dans la division par 7429.

On obtient

$$227^2 \equiv 210^2 \pmod{7429},$$

ce qui implique que 7429 est un diviseur de $227^2 - 210^2$.

On peut donc prendre X=227 et Y=210. Ces valeurs fournissent le diviseur 17 de 7429.

L'algorithme du « crible quadratique » doit son nom aux identités : différence de deux carrés, on cherche des carrés de nombres dont la différence avec *a* se décompose en petits facteurs premiers.

On fixe d'abord les nombres premiers qui peuvent intervenir dans les relations. Dans l'exemple considéré précédemment, on a pris 2, 3, 5 et 7. Pour obtenir le signe, on ajoute le nombre -1. L'ensemble de ces nombres premiers forme une base des facteurs de la méthode.

Ensuite on calcule des carrés de nombres qui sont proches de *n.*

Pour $m = 86, \sqrt{86} = \sqrt{m}.$

$(m-3)^2 = 83^2, (m-2)^2 = 84^2, (m-1)^2 = 85^2, m^2 = 86^2, (m+1)^2 = 87^2, (m+2)^2 = 88^2$,...,et en général tous les $(m+u)^2$, où u est un nombre entier positif ou négatif petit par rapport à *m*.

Enfin on se fixe l'intervalle de crible, c'est-à-dire le domaine des nombres *u*. On écrit la différence $(m+u)^2 - n$.

On détermine maintenant les carrés dont tous les facteurs premiers sont dans la base de facteurs.

Dans l'exemple, le crible par 2 s'applique de la façon suivante : comme $(m+1)^2 - n$ par exemple 140 est divisible par 2, il en est de même pour $(m-1)^2 - n$, $(m-3)^2 - n$ et $(m+3)^2 - n$. On divise ces nombres par 2 jusqu'à ce que l'on obtienne un nombre impair. On divise 140 par 2 puis encore par 2 pour obtenir 35, le crible par 2 conduit à cette valeur [4].

CHAPITRE IV : FACTORISATION AVEC LES COURBES ELLIPTIQUES.

1. Groupes additifs abéliens de Mordell-Weil des Courbes Elliptiques

Définition 1

Une cubique de Weierstrass est une courbe algébrique plane de degré 3. Elle est définie par des équations spécifiques de la forme :

$$E\ :\ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \in K[x, y] \qquad (1)$$

C'est un polynôme à 2 variables de l'anneau *K[x, y],* sur un corps commutatif K, global, local, ou fini.

Dans cette équation (1) de Weierstrass, il n'y a pas de monômes en y^3 ni en yx^2, ni en xy^2; les coefficients a_i des monômes en *xy* et en *y* sont d'indices impairs: a_1 et a_3 ; pas de a_5. Les coefficients a_i des monômes en x^2, *x* et x^0 sont d'indices pairs : a_2, a_4 et a_6.

Cette particularité n'est pas dû e au hasard ; cette indexation implique des polynômes homogènes qui apparaissent dans les formules $b_{2i}, c_{2i}, \Delta(E)$.

Cette équation (1) peut être transformée par des changements linéaires convenables des variables *x* et *y.* Pour éliminer les monômes en *xy* et en y, nous prenons le changement de variables.

$$x = X\ ,\ y = \frac{1}{2}\left(Y - a_1X - a_3\right) \quad \text{pour} \quad car\ K \neq 2 \quad ; \qquad (2)$$

Nous obtenons l'équation de Weierstrass

$$E_1\ :\ Y^2 = 4X^3 + b_2X^2 + 2b_4X + b_6 \in K[x, y] \qquad (3)$$

Les coefficients b_{2i} sont des polynômes « homogènes » de degré *2i* de l'anneau

$\mathbb{Z}\left[a_1\ ,\ a_2\ ,\ a_3\ ,\ a_4\ ,\ a_6\right]$.

$$b_2 = a_1^2 + 4a_2 \ ;$$

$$b_4 = a_1 a_3 + 2a_4 \ ; \qquad (4)$$

et $\quad b_6 = a_3^2 + 4a_6 \ ;$

Pour éliminer le coefficient 4 et le monôme en X^2 dans l'équation (3), nous prenons le changement linéaire de variables:

$$X = (x - 3b_2)/36 \ , \ Y = y/108 \quad \text{pour} \quad car\ K \neq 2,3 \ ; \qquad (5)$$

Nous obtenons l'équation de Weierstrass:

$$E_2 \ : \ y^2 = x^3 - 27c_4 x - 54c_6 \in K[x, y] \qquad (6)$$

Les coefficients c_{2i} sont des polynômes « homogènes » de degré $2i$ de l'anneau $\mathbb{Z}[b_2 , b_4 , b_6]$;

$$c_4 = b_2^2 - 24b_4 \ \text{ et } \ c_6 = b_2^3 - 36b_2 b_4 - 216b_6 ,$$

Il existe d'autres modèles d'équations de Weierstrass :

1) **Modèle de Legendre :**

$$E_3 \ : \ y^2 = x(x-1)(x-d), \ \text{avec d} \neq 0,1 ;$$

2) ***Modèle de Cassels :***

$$E_4 \ : \ y^2 = x^3 + Ax + B \in ZI[x, y] \ \text{ et } \ 4A^3 + 27B^2 \neq 0;$$

3) ***Modèle de Deuring :***

$$E_5 \ : \ y^2 + axy + y = x^3 ;$$

4) **Modèle de Tate :**

$$E_6 \ : \ y^2 + xy = x^3 + ax + b \in C[x, y].$$

Définition 2

Le discriminant d'une cubique de Weierstrass E est le polynôme homogène de degré 12 égal à

$$\Delta(E) = 9b_2 b_4 b_6 - 8b_4^3 - 27b_6^2 - b_2^2 b_8 , \ pour \ \ car\ K \neq 2,3 \ \ et \ \ 4b_8 = b_2 b_6 - b_4^2 ;$$

Définition 3

Une Courbe Elliptique est une cubique de Weierstrass non singulière.

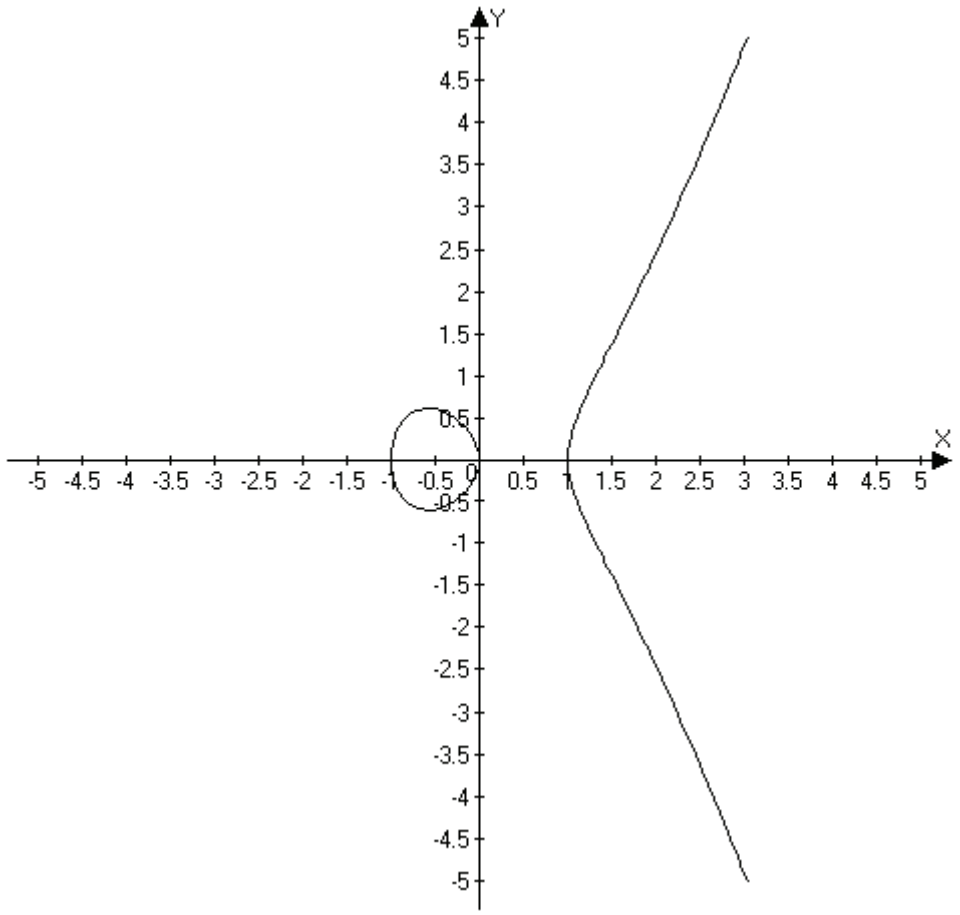
D'après la classification des cubiques, il y a deux types de Courbes Elliptiques : type de courbes E formées d'une branche finie et d'une branche infinie pour $\Delta(E) > 0$ et type de courbes E formées d'une seule branche infinie pour $\Delta(E) < 0$.

Exemple de Courbe Elliptique où $\Delta(E) > 0$

$E : y^2 = x^3 - x$

$b_2 = 0,\ b_4 = -2,\ b_6 = 0,\ b_8 = -1$

et $\Delta(E) = 2^6$, E est de type à 2 branches.

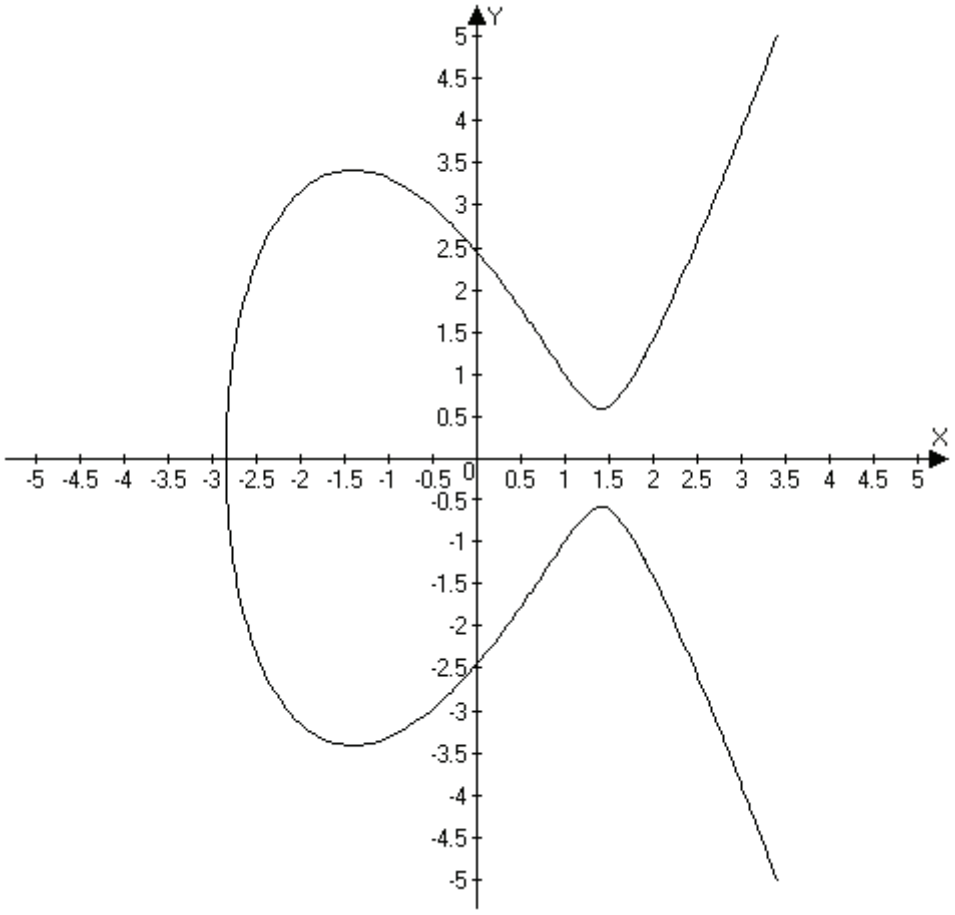


Exemple de Courbe Elliptique où $\Delta(E) < 0$

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

$b_2 = 0,\ b_4 = -2^3 \times 3,\ b_6 = 2^3 \times 3,\ b_8 = -2^2 \times 3^2$

et Δ(E)= $-2^6 \times 3^3$, *E* de type à 1 seule branche.



Structure de groupe additif abélien sur l'ensemble $E(K)$

Sur l'ensemble $E(K)$ des points rationnels de *E*, nous définissons une loi de groupe additif abélien, d'élément neutre le point $O_E = (0,1,0) \in IP^2$, $O_E = (\infty, \infty) \in IA^2$, à l'infini sur *E*, par la

Proposition 1

L'ensemble $E(K)$ ***des points rationnels d'une courbe Elliptique E, admet une structure de groupe additif abélien, d'élément neutre*** O_E***, avec la règle géométrique : « 3points colinéaires de E ont une somme nulle :*** $P + R + S = O_E$ ***, et la loi de composition interne :***

$$f : E(K) \times E(K) \to E(K), \text{avec } f(P, R) = P + R.$$

Preuve :

1) Le point à l'infini $O_E = (0,1,0)$ est déterminé par la direction de l'axe Oy , c'est un point simple sur les courbes E.
   Pour tout point P de l'ensemble $E(K)$, la règle géométrique de 3 points colinéaires implique :
   $$P + O_E = P = O_E + P.$$
   L'axiome de l'élément neutre est vérifié.
2) Le symétrique d'un point P de $E(K)$ est le 2ème point R d'intersection de E par la parallèle à Oy qui passe par P. il satisfait la règle des 3 points colinéaires :
   $$P + R + O_E = O_E$$
   Il en résulte le symétrique de P :
   $$R = -P.$$
3) Pour deux points *T* et *S* la sécante *ST* de la courbe *E* est confondue avec la sécante *TS*. Il en résulte la relation :
   $$S + T = T + S.$$
   L'axiome de commutativité est vérifié.
4) Pour vérifier l'axiome d'associativité, il n'y a pas de construction géométrique utilisable. Il faut calculer les sommes de 3 points $P + R + S$:
   $$P + R = M; M + S; R + S = T \text{ et } P + T.$$
   Alors nous obtenons l'égalité :
   $$M + S = P + T.$$
   Il en résulte la formule d'associativité :
   $$(P + R) + S = P + (R + S) = P + R + S.$$

□

Définition 4

Le groupe additif abélien $E(K)$ est le groupe de MORDELL-WEIL de la Courbe Elliptique E.

Coordonnées des points *–P et* $P_1 + P_2$ *du groupe* $E(K)$

Pour obtenir les coordonnées du symétrique d'un point, de la somme de 2 points et du point *2P* des Courbes Elliptiques il faut utiliser la règle géométrique des 3 points colinéaires de la courbe et la théorie des intersections des courbes par des droites.

a) Coordonnées du symétrique –P d'un point $P = (x, y)$

Equation de la parallèle à Oy passant par le point P : $x = x_p$.

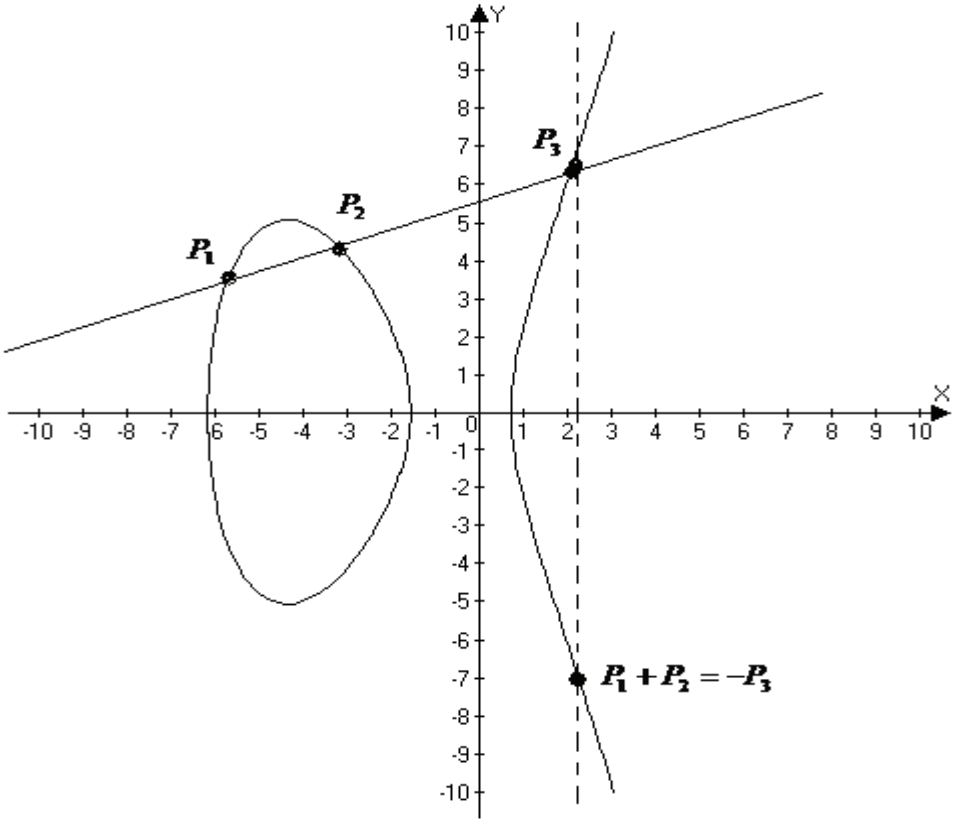
L'équation de Weierstrass de *E* devient une équation en y de degré 2, donc l'équation de Weierstrass admet deux racines ; la somme de ses deux racines est égale à :

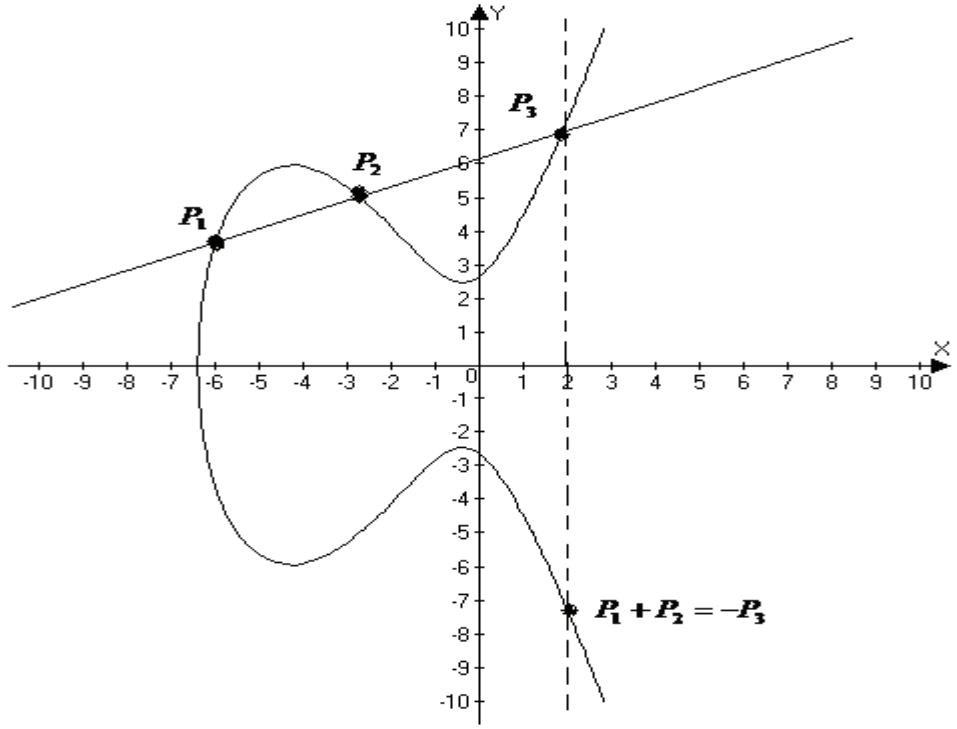
$$y + y(-P) = -a_1 x - a_3.$$

Nous en déduisons les coordonnées du symétrique –P de P :

$$P=(x,y) \text{ et } -P=(x,-y-a_1x-a_3) \tag{1}$$

b) Coordonnées de la somme de 2 points $P_i=(x_i,y_i)$ tels que $P_1 \neq \pm P_2$





La sécante P_1P_2 a pour équation :

$$y = t(x - x_1) + y_1, \text{ et } t = \frac{y_1 - y_2}{x_1 - x_2},\ x_1 \neq x_2.$$

Elle recoupe la courbe *E* en un point P_3. Ces 3 points satisfont la relation: $P_1 + P_2 + P_3 = O_E$;

L'équation de Weierstrass de *E* devient une équation en *x* cubique. La fonction symétrique élémentaire « somme des racines » implique la somme des 2 points :

$$P_1 + P_2 = -P_3 \ ;$$

Avec la théorie de l'intersection d'une courbe par une sécante, nous obtenons les coordonnées de la somme

$$\begin{aligned}
&P_1 + P_2 = M = (x_M, y_M):\\
&x_M = t^2 + a_1 t - a_2 - x_1 - x_2;\\
&y_M = -t^3 - 2a_1 t^2 + \left(a_2 - a_1^2 + 2x_1 + x_2\right) t + a_1 a_2 - a_3 + a_1(x_1 + x_2) - y_1;
\end{aligned}$$

$$\text{pour} \quad t = \frac{y_1 - y_2}{x_1 - x_2} \ \text{ et } \ x_1 \neq x_2 \tag{2}$$

Nous avons démontré la :

Proposition 2

Soit une Courbe Elliptique E d'équation de Weierstrass :

$$E : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \in K[x, y]$$

1) ***Le symétrique d'un point*** $P = (x, y)$ ***de*** $E(K)$ ***est le point :***
$$-P = (x; -y - a_1 x - a_3).$$
2) ***La somme*** $P_1 + P_2$ ***pour*** $P_1 \neq \pm P_2$ ***et le point*** $M = P_1 + P_2$ ***:***
$x_M = t^2 + a_1 t - a_2 - x_1 - x_2$; $P_i = (x_i; y_i)$ ***;***

$$y_M = -t^3 - 2a_1 t^2 + \left(a_2 - a_1^2 + 2x_1 + x_2\right)t + a_1 a_2 - a_3 + a_1 a_2 - a_3 - y \ ; \text{ et } \ t = \frac{y_1 - y_2}{x_1 - x_2}.$$

□

Points d'ordre fini des Courbes Elliptiques

Un point P d'ordre *m* d'une Courbe Elliptique *E* est un point *P* du groupe additif abélien *E(K) tel que* $mP = O_E$

Définition 5

Pour tout entier rationnel m, un point P du groupe E(K) d'ordre m satisfont la relation $mP = O_E$, le symbole *mP* représente les sommes :

$mP = P + P + \ldots + P$, m fois P, si m est positif;
$mP = (-P) + (-P) + \ldots + (-P)$, $(-m)$ fois $(-P)$, si m est négatif;
et $OP = O_E$, si $m = 0$.

Définition 6

Pour tout rationnel m, l'ensemble $E(K)[m] = E[m]$*, des points d'ordre m des Courbes Elliptiques E est le sous-groupe de m-torsion de E.*

La réunion infinie des sous groupes de m-torsion de E est un groupe.

Définition 7

Le groupe de torsion d'une courbe elliptique E est l'ensemble :

$$T(E) = \bigcup_{m \in IZ} E(K)[m].$$

des points de E d'ordre fini.

c) Coordonnées du point $P + P = 2P$

Nous utilisons l'équation de la tangente à la courbe *E* au point *P*.

Elle coupe la courbe en un point simple *T*.

$$y = y'(x - x_p) + y_p$$

L'équation de Weierstrass de *E* devient une équation en *x* cubique. Nous utilisons la fonction symétrique élémentaire « somme » des racines de cette équation pour calculer l'abscisse du point *T*. nous obtenons les coordonnées de 2P pour $P = (x, y)$,

$2P = (x_{2P}, y_{2P})$;

$$x_{2P} = y'^2 + a_1 y' - 2x; \text{ et } \quad y' = \frac{3x^2 + 2a_2 x - a_4 - a_1 y}{2y + a_1 x + a_3};$$
$$y_{2P} = -y'^3 - 2a_1 y'^2 + (a_2 - a_1^2 + 3x)y' + a_1 a_2 - a_3 + 2a_1 x - y.$$

Nous avons démontré la :

Proposition 3

Soit une courbe elliptique E d'équation de Weierstrass:

$$E: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \in K[x, y]$$

Les coordonnées du point 2P, pour tout point $P = (x, y)$ ***de la courbe E sont égales à :***

$$2P = M\ ;\ x_M = y'^2 + a_1y' - 2x; \text{ et } \ y' = \frac{3x^2 + 2a_2x - a_4 - a_1y}{2y + a_1x + a_3};$$
$$y_M = -y'^3 - 2a_1y'^2 + (a_2 - a_1^2 + 3x)y' + a_1a_2 - a_3 + 2a_1x - y.$$

□

Le groupe de Galois $G = G(K_{alg}/K)$ opére sur le groupe *E(K)* et sur les sous groupes *E[m]* de *m*-torsion par *K*-automorphismes.

Courbes Elliptiques sur les corps finis

Une Courbe Elliptique *E*, sur un corps fini IF_q à q éléments, $q = p^n$, p premier possède un groupe *E(K)* de Mordell-Weil fini. L'ordre de ce groupe fini a été évalué par HASSE dans la formule :

$$|card(E(K) - q - 1)| \le 2\sqrt{q}.$$

Tout point rationnel de la courbe E est d'ordre égal à un diviseur de l'ordre du groupe *E(K).*

Le nombre de ces points rationnels a des applications arithmétiques (primalité, factorisation de grands entiers), des applications en cryptographie, en codage (sécurité des messages, sécurité des cartes bancaires.)

Proposition 4

Soit une courbe Elliptique E sur un corps fini IF_q ***à*** $q = p^n$ ***éléments, p, premiers.***

1) ***L'ordre du groupe*** $E(IF_q)$ ***est égal à :***

$$A_q = 1 + q - Tr(frob).$$

où $Tr(frob)$ ***est la trace de l'endomorphisme de Frobenius de E ;***

2) ***Cet ordre satisfait les inégalités :***

$$q + 1 - 2\sqrt{q} \le A_q \le q + 1 + 2\sqrt{q}$$

Preuve

Soit l'application frob de Frobenius

$$frob : E \to E, \qquad frob(x) = x^p .$$

Alors l'application *frob(E)* est séparable.

L'endomorphisme de Frobenius est une isogénie purement inséparable. Son degré est précisément égal à :

$$A_q = 1 - Tr(frob) + \deg(frob) = 1 + q - Tr(frob).$$

Selon DEURING, la trace $Tr(frob)$ est un élément d'un corps quadratique imaginaire qui satisfait l'inégalité :

$$Tr(frob)^2 - 4\deg(frob) \le 0 .$$

Cela implique l'inégalité de la proposition.

□

2. Méthode de Lenstra

Lenstra commence par l'étude des Courbes Elliptiques du point de vue arithmétique.

a. Courbes Elliptiques de modèle :

$$E(a,b): \quad y^2 = x^3 + ax + b \in K[x,y] \tag{1}$$

$$car\, K \neq 2,3 \text{ et } 4a^3 + 27b^2 \neq 0 \tag{2}$$

avec le point à l'infini $O_E = (\infty, \infty)$ dans le plan affine $IA^2(IR)$ et $O_E = (0,1,0)$ dans le plan projectif $IP^2(IR)$

b. Anneau IZ/nIZ

Pour les entiers naturels *n* à factoriser soit l'anneau :

$$IZ/nIZ = \{0,\ 1, \ldots,\ n-1\} \tag{3}$$

Soit l'ensemble $E(a,b;n)$ des cubiques de Weierstrass

$$y^2 = x^3 + ax + b \in (IZ/nIZ)[x,y] \tag{4}$$

Ce sont des Courbes Elliptiques pour :

$$car\, K \neq 2,3 \text{ et } 6\left(4a^3 + 27b^2\right) \neq 0 \tag{5}$$

c. Courbe Elliptiques sur l'anneau IZ/nIZ [10]

Nous prenons un nombre entier naturel *n,* et nous construirons une Courbe Elliptique

$$\mathrm{E}: y^2 = x^3 + ax + b \in (IZ/nIZ)[x, y] \qquad (6)$$

Nous considérons les points $P = (x, y)$ dont les abscisses et les ordonnées sont des nombres entiers naturels modulo *n*.

Exemple :

Si *a=26* et *b=3* et *n=35*, je note la Courbe Elliptique *E (26,3 ; 35) d'équation*

$$\mathrm{E}: y^2 = x^3 + 26x + 3 \in (IZ/35IZ)[x, y]$$

1) Le point *M* de coordonnées *M= (2, 1)* n'est pas un point de la Courbe Elliptique *E* car il ne satisfait pas l'équation de la Courbe Elliptique *E* :

$$1^2 = 1 \pmod{35} \text{ mais } 2^3 + 26 \times 2 + 3 = 63 = 28 \pmod{35}$$

2) Le point *L* de coordonnées *L=(6,5)* est un point de la Courbe Elliptique *E* car il satisfait l'équation de la Courbe Elliptique *E* :

$$5^2 = 25 \pmod{35} \text{ et } 6^3 + 26 \times 6 + 3 = 375 = 25 \pmod{35}$$

d. Opérations « Somme » et « Produit » sur l'anneau IZ/nIZ

Soient deux points $P_i = (x_i, y_i)$ dans les groupes additifs abéliens *E (a, b ; n)*.

Alors $O_E = (0, 0)$

Soit $P_1 + P_2 = P_3 = (x_3, y_3)$ (1)

A vec le calcul, il obtient les coordonnées

$$x_3 = t^2 - x_1 - x_2 \text{ et } y_3 = t(x_1 - x_3) - y_1, \; t = (y_1 - y_2)/(x_1 - x_2) \qquad (2)$$

$$\text{et } t = (3x_1^2 + a)/(2y_1) \text{ si } P_1 = P_2 \qquad (3)$$

Congruences modulo *n*

1- Soient deux entiers rationnels *a* et *b, n > 0,*

$$a \equiv b \pmod{n} \text{ si } a = nq + b, \text{ avec } q \in IZ$$

Exemple 1 :

$38 \equiv 3 \pmod{35}$

$532 \equiv 7 \pmod{35}$

Nous utiliserons aussi les nombres négatifs $32 \equiv -3 \pmod{35}$

2- Soient a, b, a', b' des entiers rationnels, tels que

$$a \equiv b \pmod{n}$$
$$a' \equiv b' \pmod{n}$$
$$\text{Alors } (a+a') \equiv (b+b') \pmod{n}$$
$$\text{et } aa' \equiv bb' \pmod{n}$$

Exemple 2 :

$$25+19=44 \equiv 9 \pmod{35}$$
$$25 \times 19 = 475 \equiv 20 \pmod{35}$$

Nous pouvons construire une table d'addition et une table de multiplication.

3- Par définition *a* et *b* sont inverses modulo 35 si $ab \equiv 1 \pmod{n}$

Exemple 3 :

$2 \times 53 = 106 \equiv 1 \pmod{35}$, 2 est l'inverse de 53 et 53 est l'inverse de 2.

4- Pour diviser *a* par *b* nous multiplions *a* par l'inverse de *b* :

$$\frac{a}{b} = a \times b^{-1}$$

Exemple 4 :

$$\frac{10}{3} = 10 \times 3^{-1} = 10 \times 12 = 120 \equiv 15 \pmod{35}$$

5- extraction de racine carrée, l'équation $y^2 = 29$ a plusieurs solutions $y = 8$, $y = 13.$, $y = 22$ et $y = 27$ modulo35(d'aprés la table de multiplication modulo 35 ci - dessous)

Dans le cas *n=35*, j'ai construit une table de multiplication modulo 35

Table de multiplication modulo 35

	1	2	3	4	5	6	7	8	9		11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34
1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34
2	2	4	6	8	10	12	14	16	18	20	22	24	26	28	30	32	34	1	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31	33
3	3	6	9	12	15	18	21	24	27	30	33	1	4	7	10	13	16	19	22	25	28	31	34	2	5	8	11	14	17	20	23	26	29	32
4	4	8	12	16	20	24	28	32	1	5	9	13	17	21	25	29	33	2	6	10	14	18	22	26	30	34	3	7	11	15	19	23	27	31
5	5	10	15	20	25	30	0	5	10	15	20	25	30	0	5	10	15	20	25	30	0	5	10	15	20	25	30	0	5	10	15	20	25	30
6	6	12	18	24	30	1	7	13	19	25	31	2	8	14	20	26	32	3	9	15	21	27	33	4	10	16	22	28	34	5	11	17	23	29
7	7	14	21	28	0	7	14	21	28	0	7	14	21	28	0	7	14	21	28	0	7	14	21	28	0	7	14	21	28	0	7	14	21	28
8	8	16	24	32	5	13	21	29	2	10	18	26	34	7	15	23	31	4	12	20	28	1	9	17	25	33	6	14	22	30	3	11	19	27
9	9	18	27	1	10	19	28	2	11	20	29	3	12	21	30	4	13	22	31	5	14	23	32	6	15	24	33	7	16	25	34	8	17	26
10	10	20	30	5	15	25	0	10	20	30	5	15	25	0	10	20	30	5	15	25	0	10	20	30	5	15	25	0	10	20	30	5	15	25
11	11	22	33	9	20	31	7	18	29	5	16	27	3	14	25	1	12	23	34	10	21	32	8	19	30	6	17	28	4	15	26	2	13	24
12	12	24	1	13	25	2	14	26	3	15	27	4	16	28	5	17	29	6	18	30	7	19	31	8	20	32	9	21	33	10	22	34	11	23
13	13	26	4	17	30	8	21	34	12	25	3	16	29	7	20	33	11	24	2	15	28	6	19	32	10	23	1	14	27	5	18	31	9	22
14	14	28	7	21	0	14	28	7	21	0	14	28	7	21	0	14	28	7	21	0	14	28	7	21	0	14	28	7	21	0	14	28	7	21
15	15	30	10	25	5	20	0	15	30	10	25	5	20	0	15	30	10	25	5	20	0	15	30	10	25	5	20	28	15	30	10	25	5	20
16	16	32	13	29	10	26	7	23	4	20	1	17	33	14	30	11	27	8	24	5	21	2	18	34	15	31	12	21	9	25	6	22	3	19
17	17	34	16	33	15	32	14	31	13	30	12	29	11	28	10	27	9	26	8	25	7	24	6	23	5	22	4	14	3	20	2	19	1	18
18	18	1	19	2	20	3	21	4	22	5	23	6	24	7	25	8	26	9	27	10	28	11	29	12	30	13	31	7	32	15	33	16	34	17
19	19	3	22	6	25	9	28	12	31	15	34	18	2	21	5	24	8	27	11	30	14	33	17	1	20	4	23	28	26	10	29	13	32	16
20	20	5	25	10	30	15	0	20	5	25	10	30	15	0	20	5	25	10	30	15	0	20	5	25	10	30	15	21	20	5	25	10	30	15
21	21	7	28	14	0	21	7	28	14	0	21	7	28	14	0	21	7	28	14	0	21	7	28	14	0	21	7	14	14	0	21	7	28	14
22	22	9	31	18	5	27	14	1	23	10	32	19	6	28	15	2	24	11	33	20	7	29	16	3	25	12	34	7	8	30	17	4	26	13
23	23	11	34	22	10	33	21	8	32	20	8	31	19	7	30	18	6	29	17	5	28	16	4	27	15	3	26	28	2	25	13	1	24	12
24	24	13	2	26	15	4	28	16	6	30	19	8	32	21	10	34	23	12	1	25	14	3	27	16	5	29	18	21	31	20	9	33	22	11
25	25	15	5	30	20	10	0	24	15	5	30	20	10	0	25	15	5	30	20	10	0	25	15	5	30	20	10	14	25	15	5	30	20	10
26	26	17	8	34	25	16	7	32	24	15	6	32	23	14	5	31	22	13	4	30	21	12	3	29	20	11	2	7	19	10	1	27	18	9
27	27	19	11	3	30	22	14	5	33	25	17	9	1	28	20	12	4	31	23	15	7	34	26	18	10	2	29	28	13	5	32	24	16	8
28	28	21	14	7	0	28	21	13	7	0	28	21	14	7	0	28	21	14	7	0	28	21	14	7	0	28	21	21	7	0	28	21	14	7
29	29	23	17	11	5	34	28	21	15	10	4	33	27	21	15	9	3	32	26	20	14	8	2	31	25	19	13	14	1	30	24	18	12	6
30	30	25	20	15	10	5	0	29	25	20	15	10	5	0	30	25	20	15	10	5	0	30	25	20	15	10	5	7	30	25	20	15	10	5
31	31	27	23	19	15	11	7	2	34	30	26	22	18	14	10	6	2	33	29	25	21	17	13	9	5	1	32	28	24	20	16	12	8	4
32	32	29	26	23	20	17	14	10	8	5	2	34	31	28	25	22	19	16	13	10	7	4	1	33	30	27	24	21	18	15	12	9	6	3
33	33	31	29	27	25	23	21	18	16	15	13	11	9	7	5	3	1	34	32	30	28	26	24	22	20	18	16	14	12	10	8	6	4	2
34	34	33	32	31	30	29	28	26	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1

Exemple :

1) $19 \times 27 = 23$
2) La diagonale principale du tableau (1) permet de trouver les racines carrées.
3) Pour trouver l'inverse, il suffit de chercher le 1 dans le tableau par exemple l'inverse de 22 est 8.

e. Recherche d'un diviseur non trivial de *n*

Choisir une Courbe Elliptique $E(a,b)(ZI/nZI)$ d'équation :

$$E: y^2 = x^3 + ax + b \in (ZI/nZI)[x, y];$$

et un point *P(x,y)* sur cette Courbe ;

choisir une borne $B \in IN^*$, et considérons tous les $p_i^{e_i} < B$ tel que les p_i^i sont des nombres premiers et e_i est l'exposant maximal, et nous remplaçons les coordonnées du point *P* par les coordonnées des points $p_i^{e_i} P$; nous distinguons 2 cas :

1- Cas de l'addition de deux points
Je calcule $d = PGCD(x_1 - x_2, n)$ par l'algorithme d'Euclide ;
Si $d = 1$ remplaçons les coordonnées du point *P* par les coordonnées des points $p_i^{e_i} P$ en utilisant les formules d'addition de deux points, avec « d »
Si $d = n$ alors aller dans le deuxième cas ;
Sinon si $d \neq 1, n$ alors *d* est le diviseur non trivial de *n* ;

2- Cas du double d'un point
Je calcule $d = PGCD(2y_P, n)$;
Si $d = 1$ remplaçons les coordonnées du point *P* par les coordonnées des points $p_i^{e_i} P$ en utilisant les formules du double d'un point, avec « d »;
Si $d = n$ alors $y_1 = -y_2$ choisir une autre Courbe Elliptique et un autre point et reprendre les étapes;
Sinon si $d \neq 1, n$ alors *d* est le diviseur non trivial de *n* ;

L'algorithme peut être répété jusqu'à ce que la factorisation complète de *n* soit obtenue, nous choisissons à chaque fois une nouvelle courbe Elliptique et un nouveau point sur cette courbe.

Nous cherchons alors l'ordre du point *P* choisi sur la Courbe Elliptique *E* (*a, b ; n*) modulo un des facteurs premiers *p* de *n* ; nous avons calculé pour cela $p_i^{e_i} P$, comme le facteur *p* est inconnu, le calcul de $p_i^{e_i} P$ se fait dans ZI/nZI et non dans ZI/pZI. Ces calculs font intervenir des divisions et ceci n'est pas toujours possible modulo *n*.

Si le $PGCD(x_1 - x_2, n) \neq 1$ et $PGCD(2y_P, n) \neq 1$ nous ne pouvons pas dans ce cas calculer les inverses de $x_1 - x_2$ et y_P dans les formules d'addition et du double d'un point.

Dans ce cas un diviseur de *n* est $d = PGCD(x_1 - x_2, n)$ ou $d = PGCD(2y_P, n)$

Si nous avons pu mener les calculs jusqu'au bout, nous recommençons les étapes en changeant de Courbe Elliptique ou en augmentant la valeur de la borne *B*.

Théorème (Hasse)

Toute Courbe Elliptique E sur un corps fini IF_p à p éléments, p premier possède un groupe E(K) de Mordell-Weil fini. L'ordre de ce groupe fini a été évalué par Hasse dans la formule suivante :

$$\left|card(E(K) - p - 1)\right| \leq 2\sqrt{p}$$

Tout point rationnel de la Courbe Elliptique *E* est d'ordre égal à un diviseur de l'ordre du groupe *E* (*K*).

Choix de la borne :

Nous pouvons suivre le raisonnement suivant pour choisir la borne *B* :

Tout nombre composé a un diviseur premier inférieur à $\sqrt{n}$, si *p* est un facteur premier de *n* nous avons : $p < \sqrt{n}$

D'après le théorème de HASSE, le cardinal du groupe $E(IF_p)$ est inférieur à $\left(\sqrt{p} + 1\right)^2$.il nous suffit donc de prendre une borne

$$B \geq \left[\left(n^{1/4} + 1\right)^2\right]$$

Exemple 1 :

Factoriser *n = 35*, je prends la Courbe Elliptique *E* d'équation :

$$E : y^2 = x^3 + 3x + 1;$$

de discriminant $\Delta(\mathrm{E}) = -2^4 \times 3^3 \times 5$

soit le point *P=(0,1)* sur la Courbe Elliptique *E et B=4.*

pour trouver *3P*, je commence par calculer *2P=P+P* suivant les formules (2) et (3) je trouve :

$$t = \frac{3x_p{}^2 + 3}{2y_p} = \frac{3}{2} \equiv 19 \pmod{35} ;$$

je calcule le $PGCD(2y_p, n)$

pgcd (2, 35)=1, je calcule les cordonnées de *2P*

$$x_{2P} = t^2 - 2x_P = (19)^2 \equiv 11 \pmod{35}$$
$$y_{2p} = t(x_P - x_{2P}) - y_P = 19(0-11) - 1 \equiv 0 \pmod{35}$$

Je trouve *2P = (11,0)*

Ensuite, je calcule le $PGCD(x_{2P} - x_P, n)$

$PGCD(11, 35) = 1$, alors je calcule *3P=2P+P*

$$t = \frac{y_{2P} - y_P}{x_{2P} - x_P} = \frac{18}{11} \equiv 8 \pmod{35}$$

les coordonnées du point *3P* sont :

$$x_{3P} = t^2 - 2x_P = (8)^2 - 11 = 53 \equiv 18 \pmod{35}$$
$$y_{3P} = t(x_P - x_{3P}) - y_P = 8(11-18) = -56 \equiv 14 \pmod{35};$$

je trouve *3P = (18,14)*

Et ainsi, je calcule le $PGCD(2y_{3P}, n)$

$PGCD(28, 35) = 7 \neq 1, n$

Alors j'ai trouvé le diviseur non trivial de *n*, d'où la factorisation de *n* : $n = 7 \times 5$

Exemple 2 :

Factoriser *n=4453*

Soit la Courbe Elliptique d'équation $y^2 = x^3 + 3x \pmod{4453}$, de discriminant $\Delta(E) = -2^6 \times 3^3$.

Soit un point *P= (1, 2)* sur cette Courbe et la borne *B*=4.

Je calcule *2P* en utilisant les formules (3)

$$t = \frac{3x_p^{\ 2} + 3}{2y_p} = \frac{3}{2} \equiv 2228 \pmod{4453}$$

PGCD(2,4453)=1, donc je calcule les coordonnées du point *2P :*

$$x_{2P} \equiv 3340 \pmod{4453}$$
$$y_{2p} \equiv 1669 \pmod{4453}$$

Maintenant, je calcule *3P=2P+P*

$$t = \frac{y_{2P} - y_P}{x_{2P} - x_P} = \frac{1669-2}{3340-1} = \frac{1667}{3339} \equiv 746 \pmod{4453}$$

PGCD (3339, 4453)=1, donc je calcule les coordonnées du point *3P :*

$$x_{3P} \equiv 1003 (\mathrm{mod} 4453)$$
$$y_{3p} \equiv 610 (\mathrm{mod} 4453);$$

je trouve 3P= (1003, 610) ;

Calcul de 6P=3P+3P

Je calcule d'abord le $PGCD(2y_{3P}, n)$

$PGCD(2y_{3P}, n) = PGCD(1220,4453) = 61 \neq 1, n$

Donc j'ai trouvé le facteur 61 de 4453 et la factorisation de *n* :

$$n = 4453 = 61 \times 73$$

D'après [10], la détermination d'un facteur de *n* est fournie par la

Proposition 5

Soient 3 entiers naturels $n, v, w \in IN^*$ *, 3 éléments* $a, x, y \in ZI/nZI, b = y^2 - x^3 - ax \in ZI/nZI$

et des points P=(x, y) dans le groupe $E(a, b; n) = E(a, b)(ZI/nZI)$.

Supposons que n admet 2 diviseurs premiers p et q satisfont les 5 conditions

(1) $p < v$ *;*

(2) $6(4a^3 + 27b^2) \neq 0$ dans IF_p;

(3) Chaque nombre premier r divisant le cardinal

$$card\, E(a, b)(IF_p) \text{ satisfait: } r \leq w.$$

(4) $6(4a^3 + 27b^2) \neq 0$ dans IF_q;

(5) L'ordre du groupe $E(a, b)(IF_q)$ *n'est pas divisible par l'ordre du point* $P_p \in E(a, b; n)$.

Alors l'algorithme $"P,\ 2P, \ldots,\ kP = Q_p"$ *fournit un diviseur non trivial de n.*

Preuve : cf. [12]

Les étapes de l'algorithme sont

1- Prendre $(x, y, a) \in \{0, 1, \ldots, n-1\}$ au hasard ;
2- Calculer $b = y^2 - x^3 - ax (\mathrm{mod} n)$
3- Calculer $d = PGCD(4a^3 - 27b^2, n)$
   Si *d=n*, revenir à l'étape 1 ;
4- Si $d \neq 1$, *n*alors d est un facteur non trivial de *n* ;

5- Si $d = 1$, alors choisir une Courbe Elliptique E d'équation de Weierstrass

$$E : y^2 = x^3 + ax + b;$$

un point sur *E* de coordonnées $P = (x, y)$ et une borne *B*;

6- Considérons tous les nombres premiers $p \leq B$

a- Trouver *e* maximal tel que $p^e \leq B$

b- Calculer les produits $p^e P$ en remplaçant les coordonnées du point *P* par $p^e P$ dans $E(ZI/nZI)$ si possible en utilisant les formules (2) et (3), sinon nous avons trouver *d* tel que d n'est pas inversible modulo n, donc le facteur est le *PGCD(d, n) ;*

7- Sinon, revenir à l'étape 1 après avoir augmenté B.

Exemple :

Soit *n* = 3549331957

Je prends

$$a = 107810463$$
$$x = 317359960$$
$$y = 983830906$$

je trouve

$$b = y^2 - x^3 - ax \pmod{n} = 158771982$$

nous considérons les multiples du point *P*= (*x*, *y*) sur la Courbe Elliptique *E* d'équation de Weierstrass :

$$E : y^2 = x^3 + 107810463x + 158771982$$

définie modulo *n*,

je choisis B=1000,

1- Remplacer les coordonnées du point P par les coordonnées de $2^9 \cdot P = (701738352, 991959613)$;

2- Remplacer les coordonnées du point $2^9 P$ par les coordonnées de $3^6 \cdot P = (879549846, 586681683)$;

3- Remplacer les coordonnées du point $3^6 P$ par les coordonnées de $5^4 \cdot P = (1040814202, 724918949)$;

4- Remplacer les coordonnées du point $5^4 P$ par les coordonnées de $7^3 \cdot P$ impossible car 1050050212 n'est pas inversible modulo *n*,

j'obtiens

$$PGCD(1050050212, n) = 26861$$

et la factorisation : n = 26861 . 132137

Le temps moyen d'exécution de l'algorithme est $O\left(e^{(1+\varepsilon)\ln n \ln\ln n}\right)$

Le temps de calcul de cette méthode dépend de la taille du diviseur premier recherché. La méthode de Lenstra convient bien pour la recherche de facteurs qui ont jusqu'à 30 chiffres. A ce jour le plus grand facteur premier trouvé par la méthode de Lenstra a 47 chiffres, il a été découvert par Peter Montgomery.

1. Application au codage

Pour coder un message *M*, il faut produire un nouveau message M' à l'aide d'une fonction de codage *f*. Cette fonction *f* doit être construite de sorte que M' soit très différent de *M* et que le décodage soit possible à l'aide d'une autre fonction *g*, elle aussi très différente de *f* ; *f* et *g* sont les clés du système de codage.

Dans les systèmes à clé publique, *f* n'est pas secrète et g est secrète. Seule la clé *g* peut les décoder. Le problème du codage revient donc à construire deux fonctions *f* et *g* réciproques l'une de l'autre et telles que *g* soit difficile à trouver même si l'on connaît *f*.

Système cryptographique de VIGENERE

Chiffrer l'alphabet modulo 26

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Soit *m* un entier strictement positif, et la clé $K = (k_1, k_2, ..., k_m) \bmod 26$, on définit les deux fonctions :

Fonction de chiffrement :

$$e_K(x_1, x_2, ..., x_m) = (x_1 + k_1, x_2 + k_2, ..., x_m + k_m) \pmod{26}$$

Fonction de déchiffrement :

$$d_K(y_1, y_2, ..., y_m) = (y_1 - k_1, y_2 - k_2, ..., y_m - k_m) \pmod{26}$$

Exemple :

Soit *m*=6 et la clé CIPHER.

$$\text{Motclef} = \text{CIPHER} \rightarrow \text{clef } K = (k_1, ..., k_6) = (2, 8, 15, 7, 4, 17)$$

Soit le message à chiffrer :

factorisationdesentiers

On convertit les blocs du message en résidus modulo 26, par groupes de six, et on ajoute le mot clef modulo 26 :

5	0	2	19	14	17	8	18	0	19	8	14	13	3	4	18	4	13	19	8	4	17	18
2	8	15	7	4	17	2	8	15	7	4	17	2	8	15	7	4	17	2	8	15	7	4
7	8	17	0	18	8	10	0	15	0	12	5	15	11	19	25	8	4	21	16	19	24	22

Le message chiffré est :

HIRASIKAPAMFPLTZIEVQTYW

Pour déchiffrer, on utilise la même clé, et une soustraction modulo 26 suivant la fonction de déchiffrement.

Quelques résultats intéressants réalisés par JOHN BUCHMAN [3]

1- Temps de factorisation, par la méthode des Courbes Elliptiques exécutée sur un ordinateur puissant : à gauche, on lit le nombre de chiffres des nombres à factoriser et à droite, le temps moyen nécessaire pour trouver un facteur ayant ce nombre de chiffres.

Nombre de chiffres	Temps de calcul
6	6 secondes
9	20 secondes
12	2.5 minutes
15	16 minutes
19	7.2 heures
21	33.6 heures
24	140 heures
27	574 heures
30	

2- Avec la méthode des Courbes Elliptique on trouve un diviseur d'un nombre n, le temps de la recherche croit avec l'ordre de grandeur du diviseur cherché. Ce tableau indique, dans la première ligne, cet ordre de grandeur en nombre de chiffres ; dans la deuxième ligne, nous indiquons la borne B ; dans la troisième ligne apparait le nombre de Courbes Elliptique que l'on devra tester pour trouver un diviseur de n.

Nombre de chiffres	6	9	12	16	118	21	21	27	30
B	117	682	2162	8318	23162	63502	162730	395808	915922
Nombre de Courbes Elliptiques	10	21	12	111	231	115	833	1501	2531

3- Pour déterminer de très grands facteurs d'un nombre n, on emploie le crible quadratique. Lors de l'exécution de l'algorithme. On doit construire un système d'équations linéaires qui selon la taille de n, peut contenir un nombre considérable d'équations.

Nombre de chiffres de n	50	60	70	80	90	100	110	120
Nombre d'équations	3000	1000	7100	15000	30000	51000	120000	215000

CONCLUSION

Dans cette thèse, j'ai exposé quelques méthodes de factorisation des grands nombres.

J'envisage de poursuivre dans deux directions :

1) Factoriser des grands nombres de FERMAT, de MERSENNE, de FIBONACCI, de LUCAS.

2) Dans le domaine de la cryptographie, trouver des clés de codage de messages secret difficiles à casser.

TABLEAU RECAPITULATIF

1) Nombres naturels : $\{0,1,2,...,n,...\} = IN$;
nombres entiers rationnels : $\{0,\pm 1,\pm 2,...,\pm n,...\} = ZI$;
nombres rationnels : $\{a/b; a \in ZI; b \in IN^*\} = Q$;
nombres de Mersenne : $M_q = 2^q - 1, q = 0,1,2,...;$
nombres de Fermat : $F_n = 2^h + 1, h = 2^n, n = 0,1,2,...;$
nombres de Fibonacci : $u_0 = 0; u_1 = 1$ et $u_{n+2} = u_{n+1} + u_n$;
Nombres premiers = nombres naturels p divisibles seulement par ± 1 et $\pm p$.

2) Fonction arithmétique $f : IN \to \mathbb{C}$ = corps de nombres complexes ;
Euler, $\varphi(n) = \text{nombres des entiers naturels } d < n \text{ et premiers à } n$;
Möbius, $\mu(1) = 1, \mu(n) = 0$ si n a un facteur carré et $\mu(n) = (-1)^t$
si $n = p_1 p_2 ... p_t = \text{produit de } t \text{ nombres premiers}$

3) Corps finis
$IF_p = \{0,1,2,...,p-1\}, p$ premier
$IF_q = \{0,1,2,...,q-1\}, q = p^n, p$ premier;

4) Congruences modulo un nombre naturel n.
"$a \equiv b \pmod{n}$" équivaut à "$a - b \equiv kn,\ a,b,k \in ZI$";
Théorème chinois des restes :
Soit n nombres naturels $m_1, m_2, ..., m_n$ premiers entre eux 2 à 2 et les n congruences :
$x \equiv a_1 \pmod{m_1}; x \equiv a_2 \pmod{m_2}; ..., x \equiv a_n \pmod{m_n}.$

Alors ce système de n congruences admet une solution unique x modulo $m_1 m_2 .. m_n$

BIBLIOGHRAPHIE

[1] T.M.APOSTOL : *Introduction to analytic number theory*, Undergraduate Texts in Mathematics - Springer (1976) - Verlag New York lnc.

[2] R.P.BRENT : *Some integer factorization algorithms using Elliptic Curves* CMA R 32-85 The Australian N. University Camberra (1985)

[3] D.M.BRESSOUD : *Factorizations and Primality Testing*-Springer(1989)

[4] Johanes BUCHMAN (Professeur Informatique-Darmstadt) : *Factorisation des grands nombres* (1998)

[5] Florian CARO : *Factorisation des entiers à l'aide des Courbes Elliptiques* Institut N. Recherche Informatique et Automatique(INRIA) Paris (1998)

[6] Richard CRANDAL et Carl POMERANCE : *Prime Numbers*-Springer(2002)

[7] Jean Paul DELAHAYE: *Merveilleux Nombres premiers*-Belin-Paris(2000)

[8] Roger GODEMENT : *Cours d'algèbre*-Hermann-Paris(1973)

[9] G.H.HARDY and E.M.WRIGHT : *An introduction to the Theory of Number*- oxford university press 1975, fourth edition.

[10] Martin HELLMAN : *Le crible quadratique*-Pour la science n°251-(Septembre 1998)-p.88/96

[11] Anatoly KOSTRIKIN : *Introduction à l'Algèbre*-Ed. Mir Moscou (1986)

[10] Serge LANG : Algebra, New york 1970

[12] Hans W. LENSTRA Jr : *Factoring integers with Elliptic Curves*-Annals of Mathematic n°126(1987)p-649/673

[13] Reynald LERCIER: *Factorisation des entiers par la méthode des Courbes Elliptiques*-Ecole Polytechnique-Palaiseau-Paris-(1996)

[14] François Le LIONAIS, *Dictionnaire des Mathématiques* par Presses Universitaires de France (1979)

[15] P.L.MONTGOMERY: Speeding *the POLLARD methods of factorization*-Mathematic of Computation 48(1987) p-243/266.

[16] Hans RIESEL:(1) *Prime Numbers and Computer Methods for Factorization* Progress Mathematics-57-Birkhauser-Boston (1985)
(2) *Prime Numbers and Computer Methods for factorization*
II-Auflage Birkhuser-Bassel (1994)

[17] Paulo-RIBENBOIN: *The Book of Prime Numbers Record*-Springer (1989)

[18] Guy ROBIN (1) *Algorithmique et cryptographie*-Mathématiques et applications-S-SMAI-Ellipses (1991)
(2)Conférences au Séminaire Algèbre Théorie des Nombres-(B-H-Z)-USTHB (1998)

[19] R.J.SCHOOF : *Quadratic Fields and Factorization*-Math-Centre Tracts Amsterdam (1982) p-235/286

[20] C.P.SHNOR et H-W-LENSTRA: *Monte Carlo factoring algorithms with linear storage*-Mathematics of Computation 16-vol 43 (1984) p-289/311.

[21] B.L.VAN DER WAERDEN: *Algebra I* (1967) et II (1971) Springer-Berlin

[22] H.C.WILLIAMS: *A p+1 method of factoring*-Mathematic of Computation vol 39 (july 1982) p-225/234.

[23] H.C.WILLIAMS and J-S-JUDD: *Determination of the primality of N by using factors of* N^2+1 *and* N^2-1-Mathematic of Computation-133-vol 30 (janvier 1976)p-157/172

[24] Mohamed ZITOUNI: *Géométrie, Arithmétique et Algorithmique des Courbes Elliptiques*-Ed. O.P.U. Ben Aknoun-Alger (2007)