RÉPUBLIQUE ALGÉRIENNE DÉMOCRATIQUE ET POPULAIRE
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Dr. Yahia Fares, Médéa
Département de Mathématique



Mémoire de fin d'études pour l'obtention du diplôme de Master en Mathématiques

Option :

Analyse et Modélisation Mathématique

Présenté par :

FODILI Fahima

THEME :

Sur la factorisation par les courbes elliptiques

Soutenu :

le 13 juin 2017 à Médéa devant le jury

K. SREIER ABDALLAH	M.A.A	Université de Médéa	Présidente
O. GHERABA	M.A.A	Université de Médéa	Examinatrice
N. AIT AMRANE	M.A.A	Université de Médéa	Directrice
A. BOUTAGHOU	Professeur	Université de Médéa	Invité

REMERCIEMENT

Au terme de ce modeste travail, je tiens à remercier en premier lieu :

Dieu le Miséricordieux qui m'a donné la force et la patience d'achever ce mémoire.

J'adresse mes plus sincères remerciements et toute ma gratitude, à :

Madame ***Ait Amrane*** ma promotrice, qui s'est montrée disponible tout au long de la réalisation de ce travail, ainsi, que pour son aide et le temps qu'elle a bien voulu me consacrer.

Tous ***les enseignants*** du département de mathématiques de l'université de *YAHIA FARES DE MEDEA*.

Tous ***les membres de jury*** qui m'ont fait l'honneur d'examiner mon travail.

Enfin, j'adresse mes plus sincères remerciements, à tous ***mes proches*** et ***amis(es)*** qui m'ont toujours soutenus et encouragé au cours de la réalisation de ce mémoire.

DEDICACES

`Je dédie cette thèse à . . .`

Mes très chers parents qui étaient présents pour moi durant toute ma vie.

Mes frères et mes soeurs.

Toute la famille ***FODILI*** sans exception.

Ma chère et dynamique promotrice.

Tous les professeurs et enseignants qui ont collaboré à ma formation depuis mon premier cycle d'étude jusqu'à la fin de mes études universitaires.

Mes chères ami(e)s.

Tous ceux que j'aime, tous ceux qui m'aiment et tous ceux qui me Sont chers.

Fahima

Table des matières

Résumé **6**

Introduction **7**

1 Les courbes elliptiques **9**

1.1 Plan projectif 9

1.2 Plan affine 10

1.3 Les courbes elliptiques 10

1.3.1 Structure algébrique de la courbe elliptique 13

1.3.2 Les différentes équations de Weierstrass de courbes elliptiques 16

1.4 Les courbes elliptiques sur les corps de nombres 26

1.5 Les courbes elliptiques sur les corps finis 28

1.5.1 Les corps finis 28

1.5.2 Caractéristique d'un corps 28

1.6 Le choix de la courbes elliptique et de son corps de définition 38

2 La factorisation des entiers **40**

2.1 L'historique de la factorisation 40

2.2 Le petit théorème de Fermat 42

2.3 Friabilité 42

2.4 Test de primalité 43

2.5 La complexité algorithmique 46

2.6 Quelques algorithmes de factorisation 47

2.6.1 La factorisation par la méthode du Congruences de carrés 47

2.6.2 La factorisation par l'algorithme $p-1$ de Pollard 51
2.6.3 La factorisation par la méthode des courbes elliptiques 54
2.7 Comment factoriser par courbes elliptiques 56
2.8 Quelques exemple de la factorisation par la méthode des courbes elliptiques . 57
2.9 Avantage de la méthode ECM 61

3 Problèmes traité par la factorisation par courbes elliptiques 62
3.1 Calcul de l'ordre d'un point et d'une courbe elliptique 62
3.2 Le problème de criptage 63

4 Application 69

conclusion 75

Des problèmes ouverts 77

Bibliographie 79

Résumé

Les systèmes de chiffrement à clefs publiques et plus particulièrement le système "RSA" en 1976 sont à l'origine d'un regain d'intérêt pour des problèmes comme la factorisation d'entiers, la primalité ou encore le logarithme discret. De nouveaux algorithmes prenant en compte la faisabilité des calculs sur les machines actuelles ont ainsi vu le jour ces dernières années.

En ce qui concerne les algorithmes de factorisation d'entiers, trois algorithmes majeurs sont apparu entre 1980 et 1990 : le crible quadratique, la méthode des courbes elliptiques et le crible algébrique.

En mathématiques, une courbe elliptique est un cas particulier de courbe algébrique, munie entre autres propriétés d'une addition géométrique sur ses points. Les courbes elliptiques ont plusieurs applications dans différents domaines des mathématiques, on les trouve aussi en mécanique classique, en théorie des nombres dans la preuve du dernier théorème de Fermat démontré par Andraw Weil en 1994, en cryptologie dans le problème de la factorisation des entiers ou pour fabriquer des codes performants.

Le nom des courbes elliptiques vient historiquement de leur association avec les intégrales elliptiques, elles-mêmes appelées ainsi car elles servent en particulier à calculer la longueur d'arcs d'ellipses. Par contre à ce que son nom pourrait laisser croire, l'ellipse n'est pas une courbe elliptique.

Les systèmes modernes de cryptage de données seront sûrs tant que la décomposition des nombres de plus de 100 chiffres en facteurs restera difficile.

Introduction

L'objectif de ce mémoire est l'étude de la factorisation par les courbes elliptiques dans un cadre de mathématiques appliquées, organisé en quatre chapitres tels que dans le premier sera présenté quelques outils liées aux courbes elliptiques nécessaires pour le devellopement de ce travail.
Une courbe elliptique peut être représentée dans un plan affine par une équation cubique de la forme :

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

Les coefficients a_1, a_2, a_3, a_4 et a_6 sont des éléments du corps $\mathbb{K}$ sur lequel est définie la courbe, mais ils ne sont pas déterminés par la courbe de manière unique.
Formellement, une courbe elliptique est une courbe algébrique projective non singulière de genre 1 sur un corps $\mathbb{K}$.
L'équation d'une courbe elliptique définie sur un corps peut être mise sous la forme plus simple dite équation courte de Weierstrass :

$$y^2 = x^3 + ax + b,$$

Selon le choix des coefficients a et b, les graphes correspondants ont essentiellement deux formes possibles. Les points de la courbe sont tout ceux dont les coordonnées vérifient l'équation, ainsi que le point à l'infini. Ce point à l'infini est essentiel car ce sera l'élément neutre pour l'addition des points de la courbe.
Algébriquement, ceci se traduit sur l'équation de la courbe par le fait qu'une certaine combinaison des coefficients nommée Δ = -16($4a^3$ + $27b^2$), ne s'annule pas. La quantité Δ s'appelle le discriminant de l'équation de la courbe.
Dans le deuxième chapitre sera devellopé le côté pratique de ce mémoire, représenté par les

differents algorithmes de factorisation : l'algorithme des congruences de carrés, l'lgorithme $p-1$ de polard, et la méthode des courbes elliptiques.

La factorisation de Lenstra par les courbes elliptiques est un algorithme probabiliste rapide pour la décomposition en produit de facteurs premiers qui utilise les courbes elliptiques, c'est une amélioration de la traditionnelle méthode de factorisation p -1 de Pollard.

Le troixième chapitre sera consacré à quelques problèmes résolus par la factorisation par courbes elliptiques ainsi que quelques problèmes ouverts.

Finalement, le quatrième chapitre c'est une application qui met en pratique la méthode de la factorisation d'entier par les courbes elliptiques.

Chapitre 1

Les courbes elliptiques

1.1 Plan projectif

Définition 01

Soit $\mathbb{K}$ un corps. L'espace projectif de dimension n sur $\mathbb{K}$, noté $\mathbb{P}^n(\mathbb{K})$ est l'ensemble $\mathbb{K}^{n+1}\backslash\{0\}$ quotienté par la relation d'équivalence $\sim$ définie par :

$$(x_0, \ldots , x_n) \sim (y_0, \ldots ,y_n),$$

si et seulement s'il existe un elément non nul $\lambda \in \mathbb{K}$ tel que :

$$x_i = \lambda y_i, \text{ pour } 0 \leq i \leq n.$$

La classe d'équivalence de $(x_0, \ldots , x_n) \in \mathbb{K}^{n+1}\backslash\{0\}$ est noté $(x_0 : \ldots : x_n)$.
L'espace projectif de dimension 2 est appelé plan projectif noté $\mathbb{P}_2(\mathbb{K})$.
Dans la suite il nous arrivera d'écrire $\mathbb{P}_2$ à la place de $\mathbb{P}_2(\mathbb{K})$.
Nous allons plus tard définir la notion de courbe sur le plan projectif. Nous utiliserons pour cela des polynômes à trois variables.
Par la définition du plan projectif, un point peut être représenté par plusieurs triplets différents mais équivalents. Il semble alors naturel de ne considérer que des polynômes $F(x, y, z)$ tels que si

$$F(a, b, c) = 0 \text{ alors } F(ta, tb, tc)= 0,$$

pour tout t non nul.

1.2 Plan affine

Définition 02

Le plan affine $\mathbb{A}^2_K$ est l'espace affine de dimension 2 défini sur $\mathbb{K}$.
Soit $\mathbb{K}'$ un corps contenant $\mathbb{K}$. L'ensemble des points $\mathbb{K}'$-rationels de $\mathbb{A}^2_K$ est :

$$\mathbb{A}^2_K(\mathbb{K}') = \{(x,\, y) \in \mathbb{K}' \times \mathbb{K}'\}.$$

Nous pouvons choisir des fonctions coordonnées affines x, y et obtenons $\mathbb{A}^2_{\mathbb{K}}(\mathbb{K}')$ comme l'ensemble des valeurs $\mathbb{K}'$ -rationelles de la paire des fonctions $(x\ ,\ y)$.
Les quotients des polynômes :

$$f(x,y),\ g(x,y) \neq 0 \text{ dans } \mathbb{K}[x,y],$$

sont les fonctions rationelles sur $\mathbb{A}^2_{\mathbb{K}}$ définies sur $\mathbb{K}$. Ces fonctions forment le corps $\mathbb{K}[x,y]$.

1.3 Les courbes elliptiques

Soit $\mathbb{K}$ un corps : $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{F}_p$,....

Sur le plan projectif

Définition 03

Une courbe elliptique non singulière E sur le plan projectif $\mathbb{P}_2$ est l'ensemble des solutions d'une équation polynomiale :

$$E : F(x,y,z) = 0,$$

Où F est un polynôme homogène de degré 3. Le degré de la courbe est le degré de ce polynôme.
Pour vérifier qu'un point $P = (x,y,z)$ appartient à la courbe, il suffira de vérifier que :

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

En effet :
Si on choisit une autre représentation de ce point dans le plan projectif $\mathbb{P}_2$, soit (tx,ty,tz), on a :

$$F(tx, ty, tz) = t^3 F(x, y, z) = 0.$$

Ainsi toute représentation d'un point de la courbe est un zéro du polynôme F. Son équation projective dans le plan projectif $\mathbb{P}_2$ est de la forme :

$$E : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3, \tag{1.1}$$

Les cinq coefficients a_i sont des éléments d'un corps commutatif $\mathbb{K}$, les triplets de variables (x, y, z) sont des zéros de l'équation de Weierstrass, ce sont donc des éléments d'une clôture algébrique d'un corps $\mathbb{K}$.
L'équation algébrique précédente est l'équation de Weierstrass de la courbe elliptique E sur le plan projectif $\mathbb{P}_2$.

Sur le plan affine

Pour se ramener au plan affine il suffit de considérer le changement de variables :

$$\begin{cases} x = X/Z, \\ y = Y/Z, avecZ \neq 0 \end{cases}$$

dans l'équation (1, 1) qui devient :

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{1.2}$$

plus le point (0, 1, 0) qui est le seul point à l'infini ($Z = 0$) et que l'on choisit comme point distingué O_E.

Définition 04

Une courbe elliptique E est une cubique plane non dégénérée, non singulière, de genre 1 et d'équation affine particulière (1.2).

Points rationnels

Dans cette partie, on considère une courbe elliptique E définie sur un corps $\mathbb{K}$ par l'équation (1.2).

Définition 05

L'ensemble des points $\mathbb{K}$-rationnels de E, noté $E(\mathbb{K})$ est :

$$E(\mathbb{K}) = \{(x, y) \in \mathbb{K}^2 \ / \ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{O_E\}$$

Exemple

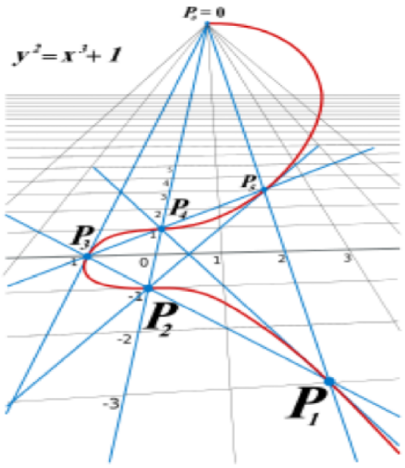


Fig 01. Les points rationnels de la courbe $y^2 = x^3 + 1$.

Remarques

1. Le point à l'infini O_E défini sur $\mathbb{K}$, par convention, l'est aussi sur toute extension de $\mathbb{K}$.

   Ainsi, si $\mathbb{L}$ est une extension du corps $\mathbb{K}$, $E(\mathbb{L})$ est aussi une courbe elliptique définie sur $\mathbb{L}$ et O_E est encore le point à l'infini de $E(\mathbb{L})$.

2. On a :

   $$E(\mathbb{K}) = \{(x, y) \in \mathbb{K}^2 \ / \ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{O_E\}$$

   de même :

$$E(\overline{\mathbb{K}}) = \{(x, y) \in \overline{\mathbb{K}}^2 \ / \ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{O_E\}$$

Si :

$$\mathbb{K} \subset \mathbb{L} \subset \overline{\mathbb{K}},$$

il vient alors :

$$E(\mathbb{K}) \subset E(\mathbb{L}) \subset E(\overline{\mathbb{K}}).$$

1.3.1 Structure algébrique de la courbe elliptique

Dans tout la suite on travaillera sur le plan affine.
Dans la théorie de l'intersection, l'intersection d'une cubique et d'une droite contient exactement trois points, ce qui donne la règle géométrique de la sécante suivante :

"trois points colinéaires de la courbe elliptique E ont une somme nulle"

sur laquelle est basé la loi de groupe sur une courbe elliptique.

La loi de groupe sur une courbe elliptique

Soit E une courbe elliptique donc non singulière et $E(\mathbb{K})$ l'ensemble des points $\mathbb{K}$-rationnels de la courbe E.
En considérant le point à l'infini $O_E = (0,\ 1,\ 0)$ comme élément neutre et en munissant l'ensemble d'une loi de groupe définie plus haut on a la somme de deux points est le symétrique du troisième point colinéaire issu de l'intersection. Avec laquelle nous obtenons une structure de groupe abélien.
Le point à l'infini O_E est déterminé par la direction de l'axe O_y. Pour tout point P, la droite PO_E est donc parallèle à l'axe O_y.
La théorie de l'intersection des cubiques planes montre qu'une sécante coupe la courbe elliptique en trois points simples, ou en un point double et un point simple, ou en deux points simples et le point à l'infini.
Dans le premier cas, la règle géométrique donne la formule :

$$P_1 + P_2 + P_3 = 0_E,$$

où $P_1 \neq P_2$, et on a les composants analytiques pour $P_1 = (x_1, y_1) \neq P_2 = (x_2, y_2), P_3 = (x_3, y_3)$:

$$\begin{cases} x_3 = \lambda^2 - x_1 - x_2 \\ y_3 = \lambda(x_1 - x_3) - y_1 \quad , avec : \lambda = (y_1 - y_2)/(x_1 - x_2). \end{cases}$$

Dans le deuxième cas, la règle géométrique donne la formule :

$$P_1 + P_1 + P_3 = 2P_1 + P_3 = 0_E \,;$$

qui permet le calcul d'un point P de 2-torsion.Voir [3].
Dans le troisième cas, la règle géométrique donne la formule :

$$P_1 + P_2 + 0_E = P_1 + P_2 = 0_E \,;$$

qui permet le calcul du symétrique P_2 d'un point P_1.

Théorème 01 :

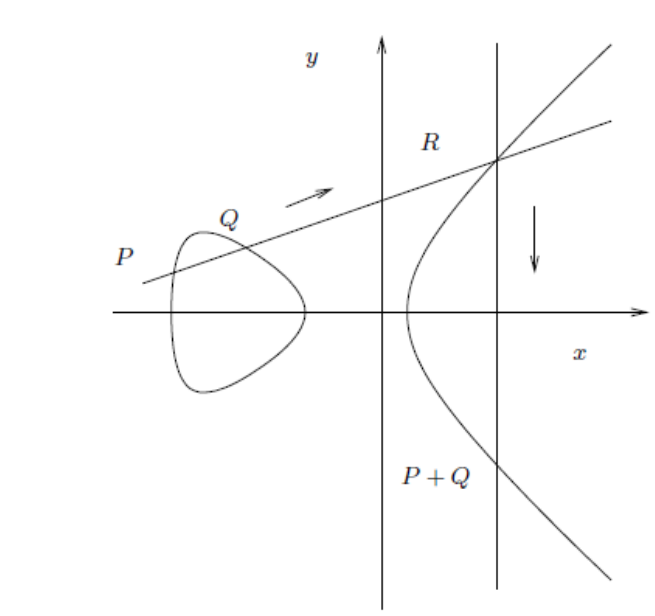
$(E(\mathbb{K}), +)$ est un groupe abélien.

Preuve.

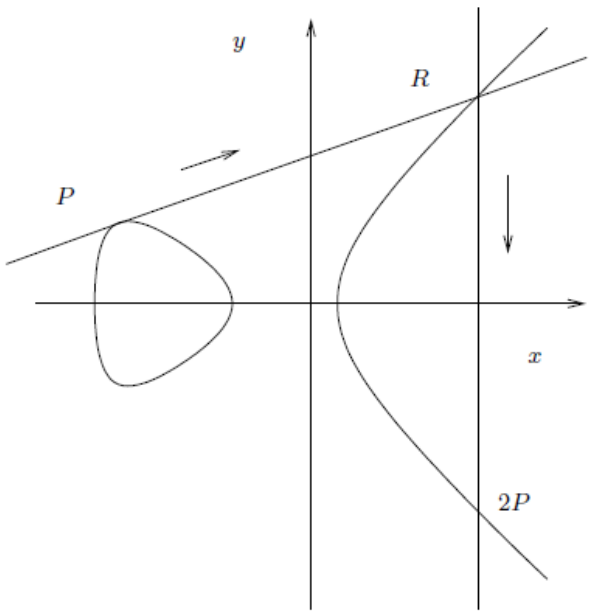
1. La stabilité de la somme et de l'inverse se vérifie par construction.
2. L'associativité a besoin d'un lemme technique.

Lemme

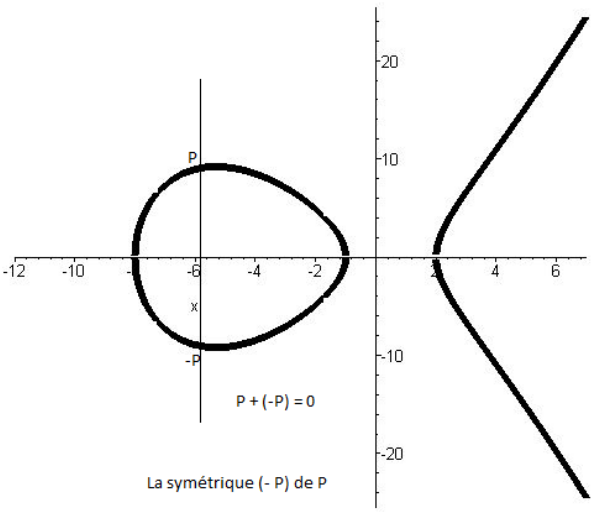
Soient $P_1, \ldots, P_8 \in P_2(\mathbb{K})$ distincts. Supposons que 4 d'entre eux ne sont jamais alignés et que 7 d'entre eux n'appartiennent jamais à une même conique. Alors l'espace vectoriel des polynômes homogènes de degré 3 s'annulant en $P_1, \ldots, P_8$ est de dimension 2.
Sous l'hypothèse du théorème de Bézout, l'intersection d'une cubique et d'une droite contient trois points exactement, et l'intersection d'une cubique et d'une conique contient six points exactement.



Si $P \neq Q$,
on trace la sécante (PQ).



Si $P = Q$,
on trace la tangente en P.



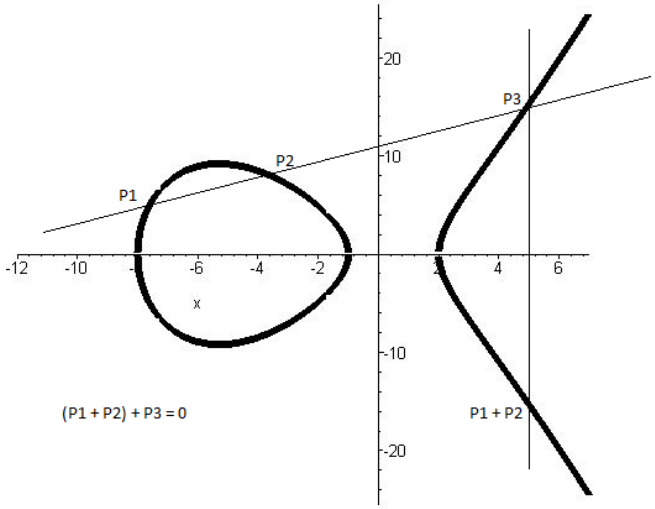


Fig 02. Interprétation géométrique de la loi de groupe sur une courbe elliptique.

Ce qui est résumé dans cette proposition :

Proposition 01

L'application :

$$\begin{cases} f: & E(\mathbb{K}) \times E(\mathbb{K}) & \longrightarrow & E(\mathbb{K}) \\ & (P_1, P_2) & \longrightarrow & f(P_1, P_2) = P_1 + P_1. \end{cases}$$

qui satisfait la règle géométrique des trois points colinéaires est une loi de groupe abélien d'élément neutre le point à l'infini 0_E.

Preuve.

Voir[3].

1.3.2 Les différentes équations de Weierstrass de courbes elliptiques

Comme on l'a vue dans la section'1.3', toute courbe elliptique peut être representée par l'ensemble des points qui verifient une équation dite de Weierstrass qui est relativement homogène qui peut être rendue courte par des transformations linéaires, cette étape est bien utile car selon l'équation les calcules sont plus simples.

Les transformations linéaires de l'équation de Weierstrass

Proposition 02

L'équation (1.2) peut être transformée en d'autres équations plus courtes.

Preuve.

Lorsque le corps $\mathbb{K}$ est de caractéristique différente de 2, le changement linéaire de variables :

$$(x, y) \mapsto (x, \tfrac{1}{2}(y - a_1x - a_3)),$$

élimine les monômes xy et y dans l'équation (1.2).

L'équation (1.2) de la courbe elliptique devient :

$$E : y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6, \tag{1.3}$$

les coefficients b_i sont des polynômes "homogènes de degré i" dans l'anneau $\mathbb{Z}[a_1, a_2, a_3, a_4, a_6]$:

$$\begin{cases} b_2 = a_1^2 + 4a_2 \\ b_4 = a_1a_3 + 2a_4 \\ b_6 = a_3^2 + 4a_6 \end{cases}$$

Lorsque le corps est de caractéristique différente de 2 et de 3, le changement linéaire de variables :

$$(x, y) \mapsto (\tfrac{x-3b_2}{36}, \tfrac{y}{108}),$$

élimine le monôme x^2 et le coefficient 4 dans l'équation(1.3).

L'équation (1.3) de la courbe elliptique devient :

$$E : y^2 = x^3 - 27c_4x - 54c_6. \tag{1.4}$$

Les coefficients c_i sont des polynômes "homogènes de degré i" de l'anneau $\mathbb{Z}[b_2, b_4, b_6]$:

$$\begin{cases} c_4 = b_2^2 - 24b_4 \\ c_6 = 36b_2b_4 - b_2^3 - 216b_6 \end{cases}$$

L'équation (1.4) de la courbe elliptique E peut se mettre sous la forme :

$$E : y^2 = x^3 + Ax + B. \tag{1.5}$$

Les coefficients A et B sont des polynômes de l'anneau $\mathbb{Z}[c_4,c_6]$:

$$\begin{cases} A = -27c_4 \\ B = -54c_6 \end{cases}$$

Les invariants : Discriminant et j-invariant modulaire

Voici quelques notions utiles à l'étude et à la classification des courbes algébriques définies par une équation de Weierstrass :

Définition 06

Pour une courbe algébrique E donnée par son équation de la forme (1.3), on calcul la quantité :

$$\Delta = -b_2^2\ b_8 - 8b_4^3 - 27b_6^2 + 9b_2\ b_4\ b_6,$$

Δ appelé discriminant de la courbe elliptique E.

Proposition 03

- Si $\Delta = 0$, la courbe E n'est pas elliptique.
- Si $\Delta \neq 0$, la courbe E est une courbe elliptique.

Définition 07

Dans le cas d'une courbe de discriminant non nul, on définit le j-invariant modulaire de la courbe elliptique E, et on note j, la quantité :

$$j = c_4^3\ \Delta^{-1}$$

L'utilité des invariants

- Par le discriminant Δ on vérifie si la courbe est elliptique ou non.
- Le j-invariant classe les courbes elliptiques isomorphes ainsi : deux courbes elliptiques définies par leurs équations de Weierstrass à coefficients sur un corps algébriquement clos si et seulement si elles ont le même j-invariant comme le montre la proposition suivant :

proposition 04

Soient deux courbes elliptiques E et $E^{'}$ définies sur un corps algébriquement clos $\mathbb{K}$. On dit que E et $E^{'}$ sont isomorphes si et seulement si leurs $j-invariants$ sont égaux, ce que l'on note :

$$j(E) = j(E^{'}).$$

preuve.

1. **"les deux courbes elliptiques E et $E^{'}$ sont isomorphes" implique "leurs-deux j-invariants sont égaux" :**
   Soit deux courbes elliptiques E et $E^{'}$ isomorphes, alors l'equation de E est transformée en équation de $E^{'}$ par les changements de variables suivants :
   $$\begin{cases} x = \mu^2 x^{'} + r \\ y = \mu^3 y^{'} + \mu^2 s x^{'} + t, avec \mu \in \mathbb{K}^* etr, s, t \in \mathbb{K} \end{cases}$$
   Cela implique que :
   $$j(E) = j(E^{'}).$$
2. **"$j(E) = j(E^{'})$" implique "les deux courbes elliptiques E et $E^{'}$ sont isomorphes" :**
   Soient E et $E^{'}$ deux courbes elliptiques définies par les equations de Weierstrass :
   $$E : y^2 = x^3 + Ax + B,$$
   $$E^{'} : y^{'2} = x^{'3} + A^{'}x^{'} + B^{'},$$
   satisfaisant les deux conditions :
   $$4A^3 + 27B^2 \neq 0 \text{ et } 4A^{'3} + 27B^{'2} \neq 0$$
   L'hypothèse :
   $$j(E) = j(E^{'}),$$
   et la formule de l'invariant modulaire :
   $$j = 1728 \times 4 \times A^3 \ / \ \Delta(E),$$
   implique la relation :
   $$A^3 B^{'2} = A^{'3} B^2$$

Les relations d'isomorphismes de courbes elliptiques donnent les relations entre les coefficients A, $A^{'}$, et B, $B^{'}$:

$$\mu^4 A^{'} = A \text{ et } \mu^6 B^{'} = B$$

Examinons les cas possibles :

Soit les deux formules :

$$(*) \qquad \mu^4 A^{'} = A \text{ et } \mu^6 B^{'} = B,$$
$$(**) \qquad \mu^4 c_4^{'} = c_4 \text{ et } \mu^6 c_6^{'} = c_6,$$

(a) Si $A = 0$ et $B \neq 0$:

les formules $(*)$ et $(**)$ des isomorphismes impliquent

$$A^{'} = 0 \text{ et } B^{'} \neq 0,$$

$(*)$ implique les six valeurs

$$\mu = (B/B^{'})^{1/6},$$

qui déterminent les six isomorphismes λ de E dans $E^{'}$ de valeur :

$$\lambda(x, y) = (\mu^3 x, \mu^2 y).$$

(b) Si $B = 0$ et $A \neq 0$:

les formules $(*)$ et $(**)$ des isomorphismes impliquent

$$A^{'} \neq 0 \text{ et } B^{'} = 0,$$

$(*)$ implique les quatre valeurs

$$\mu = (A/A^{'})^{1/4},$$

qui déterminent les quatre isomorphismes θ des deux courbes de valeurs

$$\theta(x, y) = (\mu^3 x, \mu^2 y).$$

(c) Si $AB \neq 0$:

les formules $(*)$ et $(**)$ des isomorphismes impliquent

$$A^{'} \neq 0 \text{ et } B^{'} \neq 0,$$

alors $(*)$ implique

$$\mu = (A/A^{'})^{1/4} = (B/B^{'})^{1/6}.$$

Il en résulte l'isomorphisme ϕ de E dans $E^{'}$ de valeur :

$$\phi(x, y) = (\mu x, \mu y).$$

Les équations des courbes elliptiques isomorphes :

$$E : y^2 = x^3 + A^{'}\mu^4 x + B^{'}\mu^6,$$
$$E^{'} : y^2 = x^3 + A^{'}x + B^{'}.$$

donc les deux courbes elliptiques E et $E^{'}$ sont isomorphes.

— Comme le $j - invariant$ classe aussi les courbes supersingulières comme le montre la définition suivante :

Définition 08

Une courbe elliptique est dite supersingulière lorsque son j-invariant est nul, i.e.

$$j = 0.$$

Exemple

Soit E la courbe définie sur $\mathbb{R}$ par l'équation de Weierstrass :

$$y^2 = x^3 \text{ - } x.$$

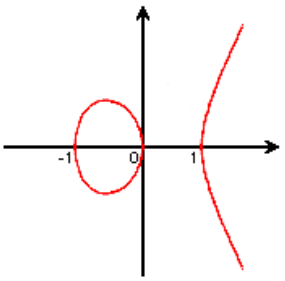


Fig 03. Représentation graphique de E.

On a :

$$\begin{cases} a_1 = a_2 = a_3 = a_6 = 0 \\ a_4 = -1 \end{cases}$$

après les transformations linéaires b_i on obtient :

$$y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6 = 4(x^3 - x)$$

avec :

$$\begin{cases} b_2 = b_6 = 0 \\ b_4 = -2 \\ b_8 = -1 \end{cases}$$

et par les transformations linéaires c_i on obtient :

$$y^2 = x^3 - 27c_4x - 54c_6 = x^3 - 1296x$$

avec :

$$\begin{cases} c_4 = 48 \\ c_6 = 0 \end{cases}$$

Donc le calcul du discriminant donne : $\Delta = 64 \neq 0$, et l'invariant modulaire vaut : $j = 1728$, alors :

- comme $\Delta \neq 0$, la courbe E n'est pas singulière donc elle est elliptique.
- comme $j \neq 0$, la courbe E n'est pas supersingulier.

Proposition 05

Les Cubiques de Weierstrass E de discriminant Δ et $c_4(E)$ sont classifiées comme suit :

1. Classe des cubiques singulières qui ont un noeud lorsque $\Delta = 0$ et $c_4(E) \neq 0$,
2. Classe des cubiques singulières qui ont un point de rebroussement lorsque $\Delta = 0$ et $c_4(E) = 0$,
3. Classe des Courbes Elliptiques de type 1 , avec deux composantes , lorsque $\Delta > 0$,
4. Classe des Courbes Elliptiques de type 2 , avec une seule composante , lorsque $\Delta < 0$.

Voir les fig 4, 3, 6, et 7.

Quelques exemples des cubiques de Weierstrass et leurs représentations graphiques

Exemple 1

Soit $E(\mathbb{R})$ définie par :

$$E : y^2 + 6\ xy + 2y = x^3 - 9x^2 - 6x - 1 \in \mathbb{R}[x, y]$$

On a les coefficients :

$a_1 = 6$, $a_3 = 2$, $a_2 = -9$, $a_4 = -6$, $a_6 = -1$,

donc :

$b_2 = 36 - 36 = 0$, $b_4 = 12 - 12 = 0$, $b_6 = 4 - 4 = 0$,

ce qui donne les invariants :

$\Delta = 0$, $c_4 = 0$,

d'où la courbe est singulières admet un point de rebroussement.

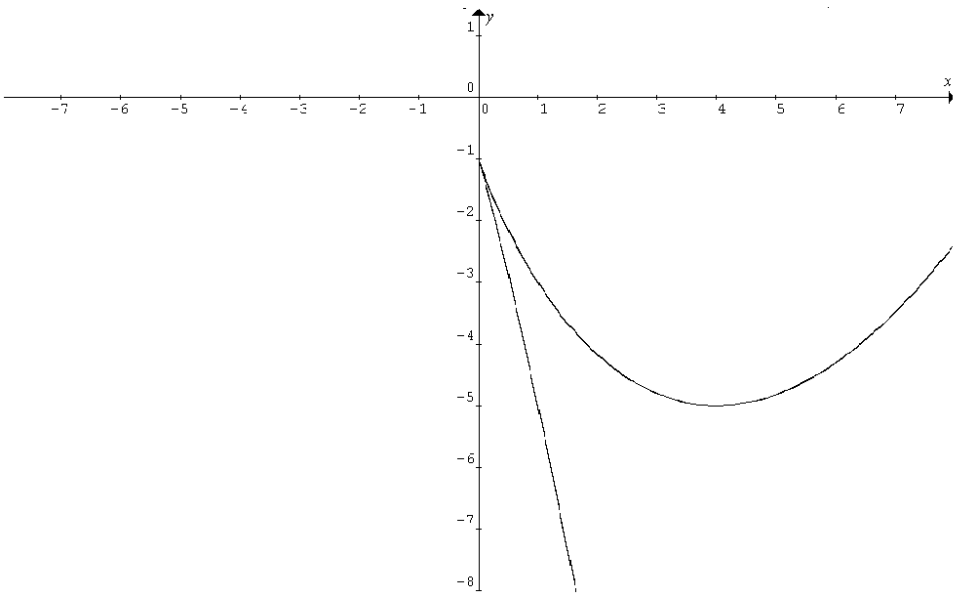


Fig 04. Cubique de Weierstrass singulière avec un point de rebroussement.

Exemple 2

Soit $E(\mathbb{R})$ définie par :

$$E : y^2 + 4\ xy - 6y = x^3 + 5x^2 + 12x - 9 \in \mathbb{R}[x, y]$$

On a les coefficients :

$a_1 = 4$, $a_3 =$ -6, $a_2 = 5$, $a_4 = 12$, $a_6 =$ -9 ;

donc :

$b_2 = 36$, $b_4 = 0$, $b_6 = 0$, $b_8 = 0$,

qui donne les invariants :

$\Delta = 0$, $c_4 = b_2^2$ - $24b_4 = 36^2 \neq 0$.

alors d'après la proposition 05 cette cubique admet un nœud comme singularité donc elle n'est pas elliptique.

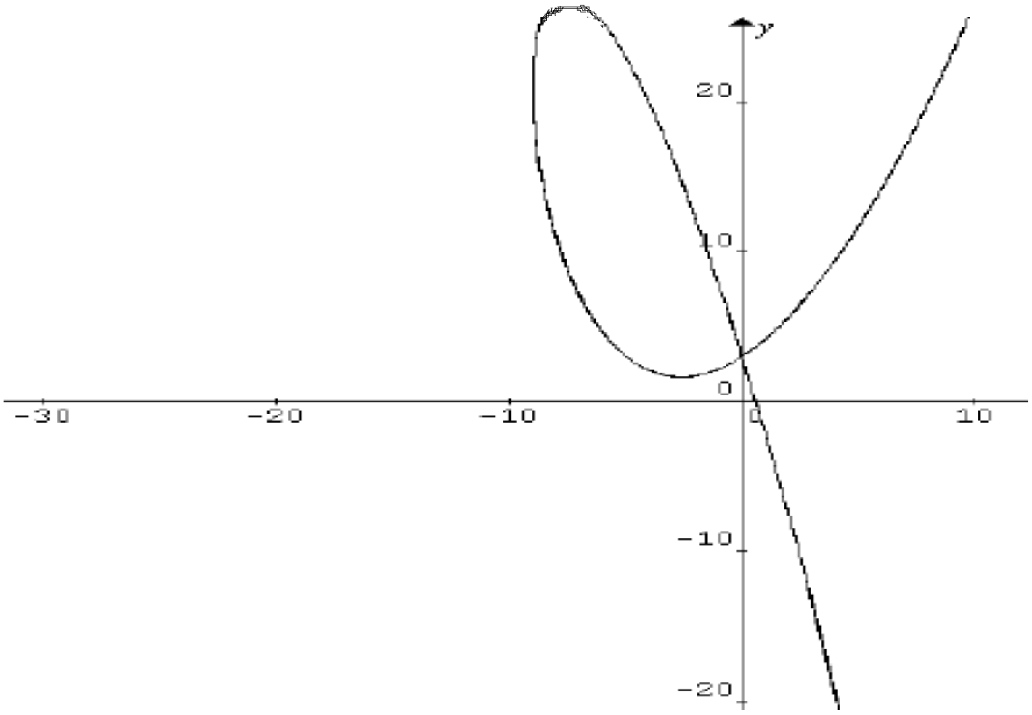


Fig 05. Cubique de Weierstrass singulière avec un nœud.

Exemple 3

Soit $E(\mathbb{R})$ définie par :

$$E : y^2 = x^3 - x^2 - 2x + 40 \in \mathbb{R}[x, y]$$

On a les coefficients :

$a_1 = 0$, $a_3 = 0$, $a_2 =$ -1, $a_4 =$ -2,$a_6 = 40$;

donc :

b_2 = -4, b_4 = -4, b_6 = 160, b_8 = -176 ;

ce qui donne les invariants :

$\Delta = 32 \times 689$, $c_4 = 16 + 4 \times 24 = 112 = 16 \times 17$;

point d'intersection avec Ox :

$y = 0$, x_1 = -5, $x_2 = 2$, $x_3 = 4$;

$P_1(-5, 0)$, $P_2(2, 0)$, $P_3(4, 0)$: 3 points simples.

comme $j = \frac{c_4^3}{\Delta} = \frac{21952}{689} \neq 0$, donc E n'est pas supersingulier.

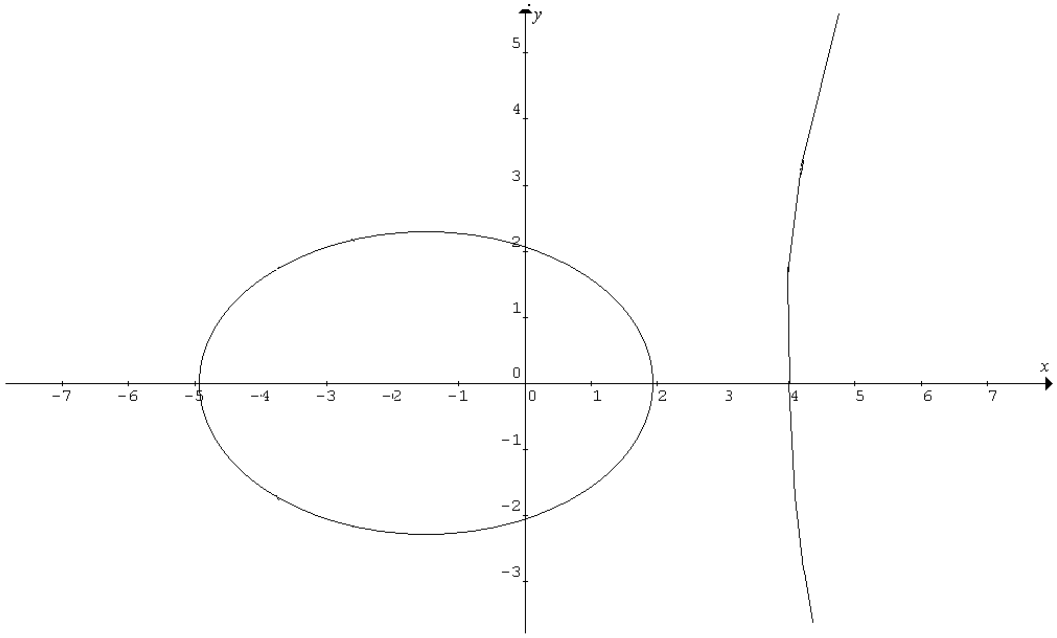


Fig 06. Courbe elliptique de type 1 ($\Delta > 0$), avec deux composantes.

Exemple 4

Soit $E(\mathbb{R})$ définie par :

$$E : y^2 + 3x = x^3 - 3x^2 + 5x + 9 \in \mathbb{R}[x, y]$$

On a les coefficients :

$a_1 = 0$, $a_3 = 3$, a_2 = -3, $a_4 = 5$, $a_6 = 9$;

donc :

b_2 = -12, $b_4 = 10$, $b_6 = 45$, b_8 = -52 ;

ce qui donne les invariants :

$\Delta = 9(-12)10 \times 45 - 8 \times 10^3 - 27 \times 45^2 + 12^2 \times 52 = -32 \times 2657 \neq 0$;

donc E est une courbe elliptique.

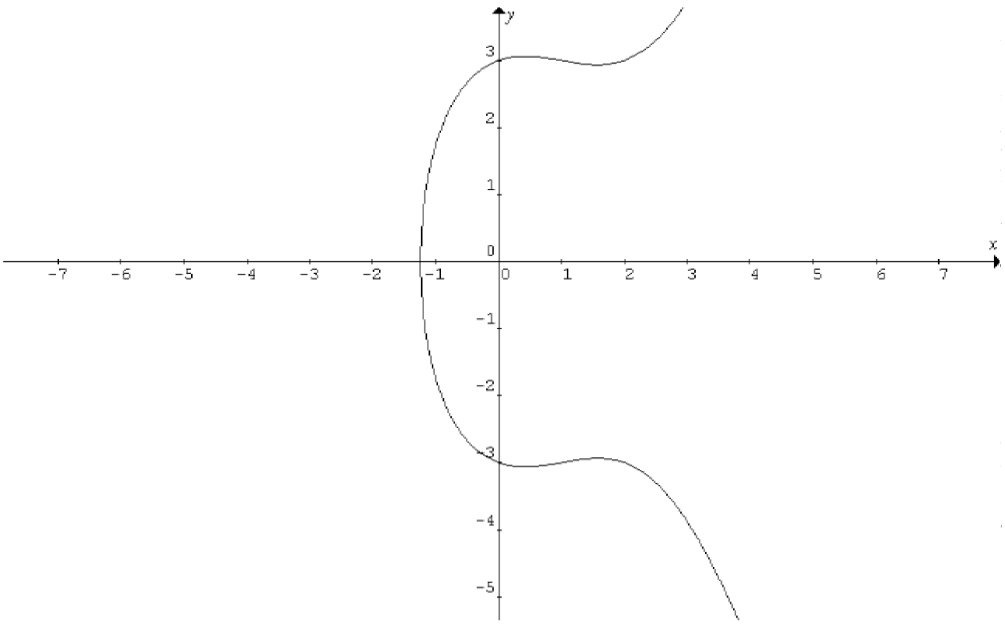


Fig 07. Courbe elliptique de type 2 ($\Delta < 0$), avec une seule composante.

1.4 Les courbes elliptiques sur les corps de nombres

Le groupe de Mordell-Weil

Définition 09

Le groupe abélien $E(\mathbb{K})$ des points $\mathbb{K}$-rationnels d'une courbe elliptique E est le groupe de Mordell-Weil de la courbe elliptique E sur un corps $\mathbb{K}$.

Définition 10

On appelle point de m-torsion un point $P \in E(\mathbb{K})$, où $\mathbb{K}$ est la clôture algébrique de $\mathbb{K}$, tel que :

$$mP = O.$$

Proposition 06

Le groupe de Mordell-Weil d'une courbe elliptique E est de type fini. Il est isomorphe au produit de groupes abéliens :

$$E(\mathbb{K}) \cong E(\mathbb{K})_{tor} \times \mathbb{Z}^r,$$

où : $E(\mathbb{K})_{tor}$ est le sous groupe de torsion du groupe de Mordell-Weil $E(\mathbb{K})$
$\mathbb{Z}$ est l'anneau des entiers rationnels.
$r(E) =$ r est un entier positif ou nul.

Preuve :

On peut la trouver dans les articles de Mordell Weil,elle comporte deux parties dont l'une a pour objet de montrer la finitude du groupe quotient $E(\mathbb{K})/mE(\mathbb{K})$,l'autre partie utilise une fonction hauteur sur un groupe abélien.
Voir[3].

Définition 11

L'entier naturel $r(E) = r \geq 0$ est le rang de la courbe elliptique E.
La détermination de ce rang exige un bagage théorique important, il n'existe pas de formule effective donnant la valeur du rang $r(E)$ d'une courbe elliptique E, contrairement au rang du groupe des unités $U(K)$ d'un corps de nombres $\mathbb{K}$, qui admet $2r_2$ conjugués complexes et r_1 conjugués réels :

$$r(U(K)) = r_1 + r_2 \text{ - } 1,$$

et

$$U(K) \cong W \times \mathbb{Z}^{r_1+r_2-1},$$

où W est le groupe des racines de l'unité contenues dans le corps $\mathbb{K}$ (théorème de Dirichlet).

1.5 Les courbes elliptiques sur les corps finis

1.5.1 Les corps finis

Le corps $\mathbb{F}_p$=$\mathbb{Z}/p\mathbb{Z}$

Définition 12

Soit $p \in \mathbb{N}$. On définit la relation d'équivalence $\sim$ sur $\mathbb{Z}$ par $x \sim y$ si et seulement si p divise $x - y$.

On note $\mathbb{Z}/p\mathbb{Z}$ l'ensemble des classes d'équivalences :

La classe d'équivalence d'un entier x est le sous-ensemble de $\mathbb{Z}$ formé des entiers de la forme $kn + x$ avec $k \in \mathbb{Z}$.

Dans la suite, on représentera la classe d'équivalence de x par le reste

$r \in \{0, \ldots, p-1\}$ de la division euclidienne de x par p. On note également $(x \ mod \ p)$ la classe d'équivalence de x.

La loi de groupe sur $\mathbb{Z}/p\mathbb{Z}$ est définie par :

$$(x \ mod \ p) + (y \ mod \ p) = (x + y) \ mod \ p.$$

Cette addition ne dépend pas du choix de x et de y dans la classe d'équivalence.

Exemple

L'anneau $\mathbb{Z}/4\mathbb{Z}$ est-il un corps ? Sinon, comment peut-on définir un corps à 4 éléments ? $\mathbb{Z} = n\mathbb{Z}$ est un corps si et seulement si n est premier. 4 n'est pas premier donc $\mathbb{Z} = 4\mathbb{Z}$ n'est pas un corps. On peut aussi dire directement que 2 est un diviseur de 0 dans $\mathbb{Z} = 4\mathbb{Z}$ donc $\mathbb{Z} = 4\mathbb{Z}$ n'est pas un corps.

On définit un corps à 4 éléments en quotientant $\mathbb{F}_2$ le corps à 2 éléments par un polynôme irréductible de degré 2 sur $\mathbb{F}_2$.

1.5.2 Caractéristique d'un corps

Définition 13

Soit $(\mathbb{K}, +, \times)$ un corps commutatif d'élément unité 1.

Considérons pour $n \in \mathbb{Z}$, l'ensemble des éléments de $\mathbb{K}$ de la forme $n1$ (multiples de 1 au

sens de la notation additive).

De deux choses l'une :

— Soit $\exists\ n \in \mathbb{Z}^* \mid n1 = 0$,

— Soit le contraire $\forall\ n \in \mathbb{Z}^*\ n1 \neq 0$.

Considérons le premier cas et soit p le plus petit entier $p > 0$ tel que $p1{=}0$. Alors p est nécessairement premier. En effet sinon on a :

$$p = kh \text{ et } (k1)(h1) = 0 \Rightarrow k1 = 0 \text{ où } h1 = 0,$$

car il n'y a pas de diviseurs de zéro dans un corps. Ce qui contredit la définition de p.

Dans ce cas on dit que "$\mathbb{K}$ est de caractéristique p".

Dans le cas contraire on dit que "$\mathbb{K}$ est de caractéristique 0".

Désignons maintenant par $\mathbb{P}$ le plus petit sous-corps de $\mathbb{K}$. c'est à dire le plus petit des sous-groupes de $\mathbb{K}$ contenant l'unité, stable pour la loi $\times$ et tel que pour tout élément x de $\mathbb{P}$ l'inverse de x est encore élément de $\mathbb{P}$.

Dans le cas de la caractéristique 0, il est clair que $\mathbb{P}$ doit contenir les nombres de la formes $m.1$ ainsi que leurs inverses de la fome $1/n1$ et les produits de tels éléments donc les éléments de la forme $m1/n1$. Alors l'application :

$$\tfrac{m}{n} \to \tfrac{m1}{n1} \text{ de } \mathbb{Q} \text{ dans } \mathbb{K},$$

est un isomorphisme de $\mathbb{Q}$ sur $\mathbb{P}$.

Dans le cas de la caractéristique p, l'application $n \to n1$ est un homorphisme de $\mathbb{Z}$ dans $\mathbb{P}$ et $p\mathbb{Z}{=}\{n \mid n1 = 0\}$.

On démontre que cet homomorphisme induit un homomorphisme injectif de $\mathbb{Z}/p\mathbb{Z}$ dans $\mathbb{P}$ et que $\mathbb{P}$ est alors isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

En résumé dans le théorème suivant :

Théorème 02

Tout corps contient un sous-corps isomorphe soit à $\mathbb{Q}$ soit à $\mathbb{Z}/p\mathbb{Z}$ où p est un nombre premier.

Preuve.

Voir[14].

Proposition 07

Si $\mathbb{F}_p$ un corps fini de caractéristique p, avec p un nombre premier.
Tout corps de caractéristique p est une extension de $\mathbb{F}_p$. En particulier, tout corps fini de caractéristique p est un espace vectoriel de dimension finie sur $\mathbb{F}_p$. Son nombre d'éléments est donc une puissance de p.

L'équation de Weierstrass et la caractéristique du corps de définition

Soit E une courbe elliptique donnée dans $\mathbb{K}$ par une équation de Weierstrass.
Alors il existe un isomorphisme $(x, y) \to (u^2x + r, u^3y + u^2sx + t)$ qui ramène cette courbe à l'une des courbes dont l'équation canonique est résumé dans le tableau suivant :

Condition	*Equation*	*Discriminant*Δ	$j - invariant$
$car(\mathbb{K}) \neq 2, 3$	$y^2 = x^3 + a_4x + a_6$	$-16(4a_4^3 + 27a_6^2)$	$1728.a_4^3/(4a_4^3 + 27a_6^2)$
$car(\mathbb{K}) = 2$	$y^2 + a_3y = x^3 + a_4x + a_6$	a_2^4	0
$car(\mathbb{K}) = 2$	$y^2 + xy = x^3 + a_2x^2 + a_6$	a_6	$1/a_6$
$car(\mathbb{K}) = 3$	$y^2 = x^3 + a_4x + a_6$	$-a_4^3$	0
$car(\mathbb{K}) = 3$	$y^2 = x^3 + a_2x^2 + a_6$	$-a_2^3a_6$	$-a_2^3/a_6$

Courbes elliptiques sur $\mathbb{Z}/n\mathbb{Z}$

Soit n un entier non premier tel que $pgcd(n, 6) = 1$.

Définition 14

L'ensemble des points de la courbe elliptique E définie sur $\mathbb{Z}/n\mathbb{Z}$ d'équation de Weierstrass courte :

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

telle que $\Delta(E) = 4a^3 + 27b^2$ est premier avec n, est :

$$E(\mathbb{Z}/n\mathbb{Z}) = \{(x_1, y_1) \in (\mathbb{Z}/n\mathbb{Z})^2, y_1^2 = x_1^3 + ax_1 + b\} \cup \{O_E\}$$

où O_E est le point à l'infini.

Exemple

On considère le nombre $n = 21$ et la courbe elliptique sur $\mathbb{Z}/21\mathbb{Z}$ définie par :

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

On a $\Delta(E) = 8 \neq 0$ et :

$$E(\mathbb{Z}/21\mathbb{Z}) = \{(0, 1), (0, 8), (0, 13), (0, 20), (7, 6), (7, 15), (9, 2), (9, 5), (9, 16), (9, 19), (16, 9), (16, 12)\} \cup \{O_E\}$$

$E(\mathbb{Z}/n\mathbb{Z})$ n'est pas un groupe car n n'est pas premier.

Les courbes elliptiques sur les corps finis

Dans tout ce paragraphe, $\mathbb{K}$ désignera un corps fini de caractéristique ≥ 5 et E une courbe elliptique définie sur $\mathbb{K}$ d'équation :

$$E : y^2 = x^3 + ax + b, \text{ avec } a, b \in \mathbb{K}$$

Notons p le cardinal de $\mathbb{K}$. Le corps $\mathbb{K}$ est donc le corps fini á p éléments noté $\mathbb{F}_p$. Pour toute extension finie $\mathbb{L}$ de $\mathbb{F}_p$, le groupe $E(\mathbb{L})$ est fini. On notera $\mid E(\mathbb{L}) \mid$ son ordre.
Un résultat fondamental de la théorie des courbes elliptiques sur les corps finis est le théorème de Hasse, démontré par Hasse vers 1933, concernant le cardinal de $E(\mathbb{F}_p)$.
Remarquons d'abord que pour chaque valeur $x \in \mathbb{F}_p$, il y à au plus deux valeurs de y satisfaisant l'équation de E. On a donc évidemment :

$$\mid E(\mathbb{F}_p) \mid \leq 2p + 1.$$

Puisque qu'un élément de $\mathbb{F}_p$ choisi au hasard a environ une chance sur deux d'être un carré dans $\mathbb{F}_p$, on doit donc s'attendre á ce que l'ordre de grandeur de $|E(\mathbb{F}_p)|$ soit p. Ce qui est confirmée par l'énoncé suivant.

Théorème 03 : Hasse

On a l'inégalité :

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

Il peut se reformuler par l'inégalité :

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

En fait, la détermination de l'ordre $E(\mathbb{F}_p)$ a de nombreuses applications en cryptographie. On dit parfois que :

$$H_p = [\ p + 1 - 2\sqrt{p}\,;\, p + 1 + 2\sqrt{p}\ ]$$

est l'intervalle de Hasse pour p.
Le théoréme de Hasse permet parfois de déterminer facilement l'ordre de $E(\mathbb{F}_p)$ si l'on parvient á détecter un point de $E(\mathbb{F}_p)$ d'ordre d assez grand. L'ordre d'une courbe elliptique E sur $\mathbb{F}_p$ vaut : $p + 1 - t$ avec $| t | \leq 2\sqrt{p}$.
Et réciproquement, pour tout $m \in [2(\sqrt{p} - 1), 2(\sqrt{p} + 1)]$, il existe une courbe elliptique E d'ordre m. Ainsi, pour un p donné, il existe un grand nombre de courbes elliptiques d'ordres distincts.

Preuve.

Voir [15].

Cardinalité

Si p est un nombre premier, on notera dans la suite $\mathbb{F}_p$ un corps fini de cardinal p.
d'aprés le 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 de $E(\mathbb{F}_p)$ vérifie :

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

Inversement, Deuring a montré que pour tout entier premier p, pour tout entier e compris entre $p + 1 - 2\sqrt{p}$ et $p + 1 + 2\sqrt{p}$, il existe une courbe elliptique $E(\mathbb{F}_p)$ telle que :

$$card(E) = e.$$

C'est donc le meilleur encadrement possible.

L'algorithme de Schoof

Définition 15 :(Frobenius)

Soit E une courbe elliptique définie sur un corps fini $\mathbb{F}_q$ de caractéristique p (q = p^n). L'automorphisme de Frobenius est défini par :

$$\phi_E : E(\overline{\mathbb{F}_q}) \rightarrow \mathrm{E}(\overline{\mathbb{F}_q})$$

$$P \rightarrow \begin{cases} 0 & siP = 0, \\ (x^q,\, y^q) & siP = (x, y), \end{cases}$$

L'lgorithme de Schoof

Soit E une courbe elliptique définie sur $\mathbb{F}_p$.
L'idée de Schoof est de restreindre l'équation caractéristique du Frobenius aux sous-groupes $E[l]$ (où $l \in \mathbb{N}^*$). et $E(\overline{\mathbb{F}_p})$ ce qui donne :

$$E : \forall\ l \in N^*,\ \phi^2_{E[l]} + [pmodl]_{E[l]} = [cmodl]_{E[l]} \circ \phi_{E[l]}$$

soit encore :

$$\forall\ l \in N^*,\ \forall (x, y) \in E[l],\ (x^{p^2}, y^{p^2}) + [p\ mod\ l](x, y) = [c\ mod\ l](x^p, y^p)$$

où c est un constant tel que :

$$E(\mathbb{F}_p) = p + 1 - c.$$

L'algorithme consiste à calculer le membre de gauche de l'équation de E pour un point P d'ordre l, dans $E(\overline{\mathbb{F}_p})$; puis à calculer $[\theta]_{E[l]}(\phi_{E[l]}(P))$ pour θ dans $\mathbb{F}_l$ jusqu'à ce que l'égalité de E soit vérifiée.
Lorsque c'est le cas, nous avons :

$$c \equiv \theta (mod\ l).$$

Il ne reste plus qu'à répéter ce calcul pour des entiers l premiers entre eux et vérifiant :

$$\prod l_i > 4\sqrt{p},$$

pour trouver c à l'aide du théorème chinois qui stipule que si $l_1, \ldots, l_n$ sont n entiers de $\mathbb{N} \setminus \{0, 1\}$ premiers entre eux deux à deux alors :

$$\mathbb{Z}/l_1\mathbb{Z} \times \ldots \times \mathbb{Z}/l_n\mathbb{Z},$$

est isomorphe à $\mathbb{Z}/(\prod_{i=1}^{n} l_i)\mathbb{Z}$.
La complexité totale de l'algorithme est :

$$O(ln^8\ p).$$

Méthodes de comptage

On considère dans ce paragraphe un nombre premier $p \geq 5$. Soit E une courbe elliptique sur $\mathbb{F}_p$ d'equation :

$$y^2 = x^3 + ax + b,$$

Définition 16

On appelle point de m-torsion un point $P \in E(\overline{\mathbb{F}_p})$, où $\overline{\mathbb{F}_p}$ est la clôture algébrique de $\mathbb{F}_p$, tel que :

$$mP = O.$$

Proposition 08

Soit E une courbe elliptique d'équation $y^2 = x^3 + ax + b$, avec a et $b \in \mathbb{F}_p$, le groupe des points rationnels $E(\mathbb{F}_p)$ est fini, et en particulier, tous les points sont des points de torsion.

Dans les algorithmes de primalité et de factorisation utilisant les courbes elliptiques, il importe de pouvoir disposer de courbes elliptiques sur $\mathbb{F}_p$, pour lesquelles on sache determiner l'ordre de $E(\mathbb{F}_p)$. On va décrire deux méthodes permettant parfois d'y parvenir.

1. **Méthode du symbole de Legendre**

   Soit $x \in \mathbb{F}_p$, on définit l'application χ par :

   $$\chi : \mathbb{F}_p \to \{\text{ -1, 0, 1}\}$$
   $$\chi(\text{x}) = (\tfrac{x}{p})$$

   Rappelons que l'on a $\chi(0) = 0$, $\chi(x) = 1$ si x est un carré non nul dans $\mathbb{F}_p$ et $\chi(\text{x}) = \text{-1}$ si x n'est pas un carré dans $\mathbb{F}_p$.

2. **Méthode de Shanks - L'algorithme Baby step - Giant step**

   L'algorithme qui suit est dû á Shanks. Rappelons que :

$$H_p = [\ p + 1 - 2\sqrt{p}\,;\, p + 1 + 2\sqrt{p}\ ]$$

   est l'intervalle de Hasse pour p.

   1) On choisit un point P aléatoirement dans $E(\mathbb{F}_p)$. Pour cela, on détermine une abscisse x au hasard jusqu'à ce que $x^3 + ax + b$ soit un carré dans $\mathbb{F}_p$ et on extrait une racine carrée y de $x^3 + ax + b$ pour obtenir l'ordonnée. On prend alors $P = (x, y)$.

   2) On détermine ensuite un entier m tel que :

$$I : mP = \mathrm{O} \text{ et } m \in H_p.$$

   Il existe un tel entier m, car $|\ \mathrm{E}(\mathbb{F}_p)|P = \mathrm{O}$ et $|\ E(\mathbb{F}_p)|$ est dans H_p. Si m est le seul entier de H_p réalisant cette condition, alors m est l'ordre de $E(\mathbb{F}_p)$.

Exemple

On se propose d'étudier le groupe $E(\mathbb{F}_p)$ issu de la courbe :

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

Le calcul du discriminant nous donne :

$$\Delta = -\ 16(4a^3 + 27b^2)\ mod\ 7 = 5 \times (4 - 3^2) = -\ 45 = 4 \neq 0\ mod\ 7$$

donc E définit bien une courbe elliptique sur $\mathbb{F}_7$.

Et l'ensemble des points $(x, y) \in \mathbb{F}_7 \times \mathbb{F}_7$ de cette courbe sont :

On calcule tout d'abord les carrés pour $y \in \mathbb{F}_7$:

y	0	1	2	3	4	5	6
y^2	0	1	4	2	2	4	1

puis on calcule les $x^3 + x + 3$ pour $x \in \mathbb{F}_7$ et lorsque la valeur de $x^3 + x + 3$ correspond à y^2 dans la table ci-dessus alors (x, y) est un point de la courbe elliptique :

x	x^3+x+3	*Points*
0	3	
1	5	
2	6	
3	5	
4	1	$(4,1),(4,6)$
5	0	$(5,0)$
6	1	$(6,1),(6,6)$

On a donc 5 points rationnels plus le point à l'infini soit 6 points sur la courbe et le cardinal de $E(\mathbb{F}_p)$ est 6, donc la courbe $E : y^2 = x^3 + x + 3$ n'est pas à anomalie, alors E est une bonne courbe elliptique.

Alors le point (4, 1) est d'ordre 6 dans $E(\mathbb{F}_p)$, en effet :

Soit $P_1 = (4, 1)$. On sait que l'ordre de P_1 divise le cardinal de $E(\mathbb{F}_p)$ donc est un diviseur de 6, ce n'est pas 1, c'est donc 2, 3 ou 6.

On calcule donc $P_2 = 2P_1$ et $P_3 = 3P_1$ et si aucun de ces points n'est O alors P_1 est d'ordre 6.

On calcule :

— $P_2 = 2P_1 : \lambda = \frac{3x_1^2+a}{2y_1} = 0$,

d'où

$$\begin{cases} x_2 = \lambda^2 - 2x_1 = 0 - 2 \times 4 = 6 mod 7 \\ y_2 = \lambda(x_1 - x_2) - y_1 = -1 = 6 mod 7 \end{cases}$$

donc

$P_2 = 2P_1 = (6\ ,\ 6)$.

— $P_3 = 3P_1 = P_1 + P_2 : \lambda = \frac{y_2-y_1}{x_2-x_1} = \frac{6-1}{6-4} = \frac{5}{2} = 5 \times 4 = 6 \bmod 7$,

d'où

$$\begin{cases} x_3 = \lambda^2 - x_1 - x_2 = 36 - 4 - 6 = 5 mod 7 \\ y_3 = \lambda(x_1 - x_3) - y_1 = 6 \times (4 - 5) - 1 = 0 mod 7 \end{cases}$$

donc

$P_3 = 3P_1 = (5, 0)$.

On en déduit que P_1 est d'ordre 6 et par conséquent P_3 est d'ordre 2. Donc, de précédement on peut représenté la table d'addition de $E(\mathbb{F}_p)$ comme suite :

Pour cela on complète notre énumération précédente :

— $P_4 = 4P_1 : \lambda = \frac{3x_2^2+a}{2y_2} = \frac{3\times 6+1}{2\times 6} = \frac{4}{5} = 4 \times 3 = 5 mod 7$,

d'où

$$\begin{cases} x_4 = \lambda^2 - 2x_2 = 25 - 2 \times 6 = 6 mod 7 \\ y_4 = \lambda(x_2 - x_4) - y_2 = 5 \times (6-6) - 6 = 1 \end{cases}$$

donc

$P_4 = 4P_1 = (6\ ,\ 1)$.

— $P_5 = 5P_1 = P_1 + P_4 : \lambda = \frac{y_4 - y_1}{x_4 - x_1} = \frac{1-1}{6-4} = 0$,

d'où

$$\begin{cases} x_5 = \lambda^2 - x_1 - x_4 = 0 - 4 - 6 = 4 mod 7 \\ y_5 = \lambda(x_1 - x_5) - y_1 = -1 = 6 mod 7 \end{cases}$$

donc

$P_5 = 5P_1 = (4,\ 6)$.

On obtient donc :

O	O	$(4,1)$	$(6,6)$	$(5,0)$	$(6,1)$	$(4,6)$
$(4,1)$	$(4,1)$	$(6,6)$	$(5,0)$	$(6,1)$	$(4,6)$	O
$(6,6)$	$(6,6)$	$(5,0)$	$(6,1)$	$(4,6)$	O	$(4,1)$
$(5,0)$	$(5,0)$	$(6,1)$	$(4,6)$	O	$(4,1)$	$(6,6)$
$(6,1)$	$(6,1)$	$(4,6)$	O	$(4,1)$	$(6,6)$	$(5,0)$
$(4,6)$	$(4,6)$	O	$(4,1)$	$(6,6)$	$(5,0)$	$(6,1)$

Remarque

L'ordre du point (4, 1) peut être donnés sans aucun calcul. Il est clair d'après le tableau d'addition que $2(4,\ 1) = (6,\ 6)$ et comme (6, 6) et (4, 1) ne partagent pas la même abscisse, il est impossible, d'après la définition géométrique de l'addition des points d'une courbe elliptique, que $3(4,\ 1) = 2(4,\ 1) + (4,\ 1) = (6,\ 6) + (4,\ 1)$ soit égal à l'élément neutre. Ainsi, (4, 1) est ni d'ordre 2 ni d'ordre 3 dans $E(\mathbb{F}_p)$ qui est d'ordre 6, ce point est donc d'ordre 6 et générateur de $E(\mathbb{F}_p)$. Le tableau d'addition peut aussi être déduit très facilement sans aucun calcul.

En suite, on conclut les formes possibles pour le groupe $E(\mathbb{F}_p)$, D'après le théorème de structure,

$$E(\mathbb{F}_p) \simeq \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z},$$

avec $d_1 \mid d_2$ et $d_1 \mid p-1$. Ici on travaille sur $\mathbb{F}_7$ donc $d_1 \mid d_2$ et $d_1 \mid 6$. Le cardinal de $E(\mathbb{F}_p)$ est égal à 6. On sait que la factorisation de 6 ne contient pas de carré, la seule possibilité est que $d_1 = 1$ et $d_2 = 6$, c'est-à-dire que $E(\mathbb{F}_p)$ est isomorphe à $\mathbb{Z} = 6\mathbb{Z}$ et donc $E(\mathbb{F}_p)$ est cyclique. On aurait pu répondre plus rapidement en disant que (4, 1) est d'ordre 6 (le cardinal de $E(\mathbb{F}_p)$) et donc $E(\mathbb{F}_p) = \langle(4, 1)\rangle$ est un groupe cyclique par définition.

1.6 Le choix de la courbes elliptique et de son corps de définition

Les courbes elliptiques à anomalies

Définition 17

Une courbe elliptique E définie sur $\mathbb{F}_p$ telle que :

$$card\ E(\mathbb{F}_p) = p,$$

on appelle une courbe à anomalie.

Remarque

Il faut éviter les courbes elliptiques à anomalies sur lesquelles il est facile de casser les codes.

Choix du corps de définition

Il faut avant tout choisir le corps dans lequel on va définir la courbe elliptique. Pour éviter certaines attaques, il est préférable de choisir :

- Soit un corps premier $\mathbb{F}_p$ où p est un grand nombre premier.
- Soit un corps $\mathbb{F}_{p^r}$ de caractéristique p petite (par exemple $p = 2$) où r est un nombre premier tel que l'ordre de 2 dans $\mathbb{F}_r^*$ est grand.

Choix de la courbe elliptique

Le corps $\mathbb{F}_q$ étant choisi, de caractéristique p. Soit E la courbe elliptique considérée, t la trace du Frobenius, $G \in E(\mathbb{F}_q)$ le point de base et ℓ son ordre dans $E(\mathbb{F}_q)$.Également pour éviter certaines attaques, on note que :

- Si ℓ n'est pas premier, la réduction de Pohlig-Helman permet de simplifier le calcul du logarithme discret.
- Si $t = 1$, on dit que la courbe E est anormale (cas rare). Si de plus $q = p$ est premier, le problème du logarithme discret sur E peut être résolu en un temps linéaire (attaque de Smart).
- Si v est le plus petit entier tel que $\ell \mid q^v$ - 1, alors grâce au pairing de Weil, on peut ramener le problème du logarithme discret sur la courbe elliptique à un problème de logarithme discret sur le corps fini $\mathbb{F}_{q^v}$

On définit le degré MOV comme le plus petit entier v tel que $|\mathrm{E}(\mathbb{F}_q)| \mid q^v$ - $1|$. On doit donc s'assurer que v n'est pas petit (il n'est pas nécessaire de calculer exactement v). En particulier, la courbe E ne doit pas .être supersingulière (si E est une courbe supersingulière, on peut montrer que son degré MOV est ≤ 6).

Chapitre 2

La factorisation des entiers

Introduction à la factorisation

Un précurseur de la factorisation est la méthode de $P-1$ de Polard, cette méthode est du J.M Polard est repose sur le petit théorème de Fermat.
La factorisation consiste à écrire une expression algébrique notamment une somme, un nombre, une matrice sous la forme d'un produit. Cette transformation peut se faire suivant différentes techniques .
Les enjeux de la factorisation sont très divers : à un niveau élémentaire, le but peut être de ramener la résolution d'une équation à celle d'une équation produit-nul, ou la simplification d'une écriture fractionnaire ; à un niveau intermédiaire, la difficulté algorithmique présumée de la factorisation des nombres entiers en produit de facteurs premiers est à la base de la friabilité du cryptosystéme RSA.

2.1 L'historique de la factorisation

La décomposition en facteurs premiers de grands entiers reste très difficile à réaliser jusqu'à nos jours, malgré l'évolution des ordinateurs, il n'est toujours pas possible de factoriser certains nombres qui possèdent plusieurs centaines de chiffres et dont les facteurs premiers sont peu nombreux et dont le plus petit d'entre eux possède très grand nombre de chiffres, c'est d'ailleurs la base de la cryptographie modèrne.
En **octobre 1977**,Martin Gardner posa la question suivante :

Le nombre

1143816257578888676692357799761466120102182967212423625625618429357069352457338
9783059712356395870505898907514759929002687954354 1

est le produit de deux nombres premiers, lesquels ?

Cette question est posé aux lecteurs de science dans la rubrique de "jeux mathématiques", mais une réponce ne fut donnée que 16 ans plus tard.

En **avril 1994**, Paul Leyland, de l'université d'Oxford, Michael Graff, de l'université de l'Iowa, et Derek Atkins, de l'institut de technologie du Massachusetts, identifièrent les deux facteurs, après avoir distribué des parties de la tâche, grâce au réseau Internet, à quelques 600 volontaires, qui laissèrent fonctionner sur leurs ordinateurs, pendant de nombreuses nuits, le programme écrit par Arjen Lenstra, du centre de recherches de la société Bell Communications.

En 1978, Ronald Rivest, de l'Institut de technologie du Massachusetts, Adi shamir, de l'Institut Weizmann à Rehovot, et Leonard Adleman, de l'université de californie du sud, ont mis au point un protocole de criptage, nommé RSA d'après leurs initiaes, qui est fondé sur la factorisation.

Le juriste francais Pierre de Fermat(1601-1665), notamment célèbre pour sa conjecture démentrée, pensait avoir trouvé une méthode pour fabriquer des nombres premiers aussi grands que l'on voulait.

Cependant, le mathématicien suisse Leonhard Euler trouva que :

la machine à congruences de l'officier français Eugène Carissan(1880-1925) est particulièrement adaptée pour la recherche de nombres convenant pour le cible quadratique, utilisée pour la factorisation des nombres. Elle est aujourd'hui au conservatoire national des arts et matiers, à paris.

De 1880 jusqu'à 1990, les mathématiciens découvrient les nombres de Fermat de ($F_5 = 2^{2^5}+1$) en 1880 jusqu'à F_9 en 1990.Voir la section (2.2)

Cette histoire des nombres de Fermat montre combien la factorisation est difficile, les mathématiciens mirent 240 ans pour factoriser le nombre de Fermat F_7, et même équipés d'ordinateurs ils ont mis 20 ans à décomposer le nombre F_9 de 155 chiffres.

En 1985, Hendrik Lenstra à trouvé un algorithme de factorisation qui utilise des courbes elliptiques. Ces objets mathématiques, qui ont notamment été employée par le mathéma-

ticien britannique Andrew Wiles dans sa démonstration de la conjecture de Fermat, sont également utilisés dans des protocoles cryptographiques.
H.Lenstra a démontré aussi que, pour tout nombre composé n, il existe des courbes elliptiques qui fournissent un diviseur.
En 1987, Hendrik Lenstra proposé l'lgorithme ECM qui consiste à factoriser par les courbes elliptiques.

2.2 Le petit théorème de Fermat

Définition 18

Un nombre de Fermat est un nombre qui peut s'écrire sous la forme $2^{2^n} + 1$, avec n entier naturel. Le n-ième nombre de Fermat, $2^{2^n} + 1$, est noté F_n.
La raison historique de l'étude des nombres de Fermat est la recherche de nombres premiers. Fermat connaissait déjà la proposition suivante :

Proposition 09

Soit k un entier strictement positif, si le nombre $2^k + 1$ est premier alors k est une puissance de 2.

Théorème 04

Soit p un entier premier, alors quelque soit l'entier a, on a p divise a^p - a.

2.3 Friabilité

La notion de friabilité est une notion importante en factorisation, elle mesure, en un certain sens, la difficulté d'un nombre à être factorisé.

Définition 19

Soit a, $b \in \mathbb{N}$. L'entier a est dit b-friable (ou b-lisse) si pour tout premier p divisant a alors p est inférieur à b. L'entier a est dit b-superfriable si pour tout premier p et pour tout entier e tels que p^e divise a alors p^e est inférieur à b.

Exemple

L'entier $424242 = 2 \times 3^2 \times 7^2 \times 13 \times 37$ est 37-friable mais pas 37-superfriable.

2.4 Test de primalité

Le teste de primalité est effectuer avant d'entammer la factorisation
Il consiste à vérifier si un nombre est premier, si non essayer de le factoriser en nombre premier.
La décomposition en produit de facteurs premiers peut être très longue, voir parfois impossible, même pour nos ordinateurs modernes.
Il existe des conteurs disponibles aux internauts munis de programmes testant les grands nombres.
Parmi ces conteurs on a par exemple le programme calculis (voir [7])
Ce programme fait les trois opérations suivants :

- Tester si un grand nombre est premier ou non.
- Il factorise ce nombre si n'est pas premier.
- Il nous donne le temps nécessaire pour faire l'opération.

dont voici quelques exemples de ce programme :



Fig 08. Cas d'un nombre n'est pas premier.



Fig 09. Cas d'un nombre premier.

Proposition 10

Soit n $\in \mathbb{N}$ premier avec 6 (i.e. divisible ni par 2, ni par 3). S'il existe un entier m et un point P de la courbe elliptique :

$$E : \{y^2 \equiv x^3 + ax + b\ (modN)\} \cup \{O_E\} = (0,\ 1,\ 0)$$

vérifiant :

1. il existe un facteur premier q de m strictement supérieur à $(n^{1/4}+1)^2$
2. $mP = \mathrm{O} = (0,\ 1,\ 0)$
3. $\frac{m}{q}\ P = (x, y, z)$ avec $z \in (\mathbb{Z}/n\mathbb{Z})^*$.

alors n est premier.

Démonstration.

Raisonnons par l'absurde :

Supposons que n à un facteur premier p. Notons la courbe $E^{'}$ par :

$$E^{'} : E \text{ modulo } p,$$

$m^{'}$ la cardinalité de $E^{'}$ et $P^{'}$ le point de $E^{'}$ correspondant au point P de E. Par hypothèse :

$$mP = O \text{ et } \tfrac{m}{q}\ P \neq O, \text{ sur } E,$$

donc :

$$mP^{'} = O \text{ (car } p|n, \text{ et } \tfrac{m}{q}\ P^{'} \neq O \text{ car } z \in (\mathbb{Z}/n\mathbb{Z})^*).$$

Ceci implique que q divise l'ordre de $P^{'}$ comme point de $E^{'}$, d'où, d'après le théorème de Lagrange, q divise $m^{'}$. Il s'ensuit, d'après le théorème de Hasse que :

$$q \leq m^{'} \leq p + 1 + 2\sqrt{p} = (\sqrt{p}+1)^2 \leq (n^{1/4}+1)^2$$

car p étant un facteur premier de n, $p \leq \sqrt{n}$, il y a une contradiction avec l'hypothèse, donc n est premier.

Remarque

Nous faisons tous les calculs comme si n était premier. Si l'algorithme de Schoof qui est l'algorithme le plus efficace pour calculer la cardinalité de E n'aboutit pas, alors cela signifie que n est composé. De même, lors du calcul de mP et de $\frac{m}{q}\ P$, il est possible que le dénominateur intervenant dans le calcul de λ ne soit pas inversible. Cela signifie que $\mathbb{Z}/n\mathbb{Z}$ n'est pas un corps et donc que n n'est pas premier donc il est composé. Nous avons alors prouvé que n n'est pas premier.

2.5 La complexité algorithmique

Pour pouvoir comparer deux algorithmes indépendamment de leurs implémentations, on utilise la notion de complexité. La complexité d'un algorithme est définie comme le nombre d'opérations élémentaires nécessaires pour résoudre le probléme posé.
Le nombre exactes d'opérations élémentaires est rarement calculable alors ce que l'on étudie est l'évolution de la complexité en fonction de la taille des données d'entrée de l'algortihme. Pour les algorithmes de factorisation, on exprimera la complexité en fonction de n (l'entier que l'on veut factoriser) ou du plus petit facteur premier de n (que l'on note souvent p).
Par exemple, l'algorithme de factorisation classique qui consiste à diviser par tous les premiers inférieurs á la racine de n à une complexité en $O(p)$, si l'on compte les divisions comme des opérations élementaires.

La Notation de la complexité

Pour simplifier les notations, on utilise souvent la fonction suivante pour exprimer la complexité des algorithmes de factorisation.

Définition 20

On définit, pour toute constante c positive et pour tout $\alpha \in [0\,;\,1]$ la fonction en la variable x suivante :

$$L_x(\alpha,\, \mathrm{c}) = e^{((c+o(1))(\ln x)^{\alpha}(\ln\ln x)^{1-\alpha})}$$

Remarque

Remarquons d'abord les deux cas particulier :

— α=0 : $L_x(0,\ c)$=$e^{((c+o(1))\ln\ln x)} = (\ln x)^{((c+o(1))}$

— α=1 : $L_x(1,\ c)$=$e^{((c+o(1))\ln x)} = x^{((c+o(1))}$

La valeur de α permet de classer les algorithmes ayant une complexité en $L_n(\alpha,\ c)$.
Dans le cas de $\alpha = 0$, on parle de complexité polynomiale, pour $\alpha = 1$, on parle de complexité exponentielle et pour $0 < \alpha < 1$, on parle de complexité sous-exponentielle.
Dans la suite on utilisera cette notation pour exprimer la complexité des algorithmes en fonction de n ou p. Par exemple, l'algorithme de factorisation classique ainsi qui celle de la factorisation par ECM ont une complexité exponentielle ($L_n(1/2,\ 1) = O(\sqrt{n})$) tandis que tous les algorithmes qui seront présentés dans la partie suivante ont un complexité sous exponentielle.
Il n'existe à ce jour aucun algorithme de factorisation ayant une complexité polynomiale.

2.6 Quelques algorithmes de factorisation

Nous commençons par expliquer un algorithme qui n'a rien à voir avec les courbes elliptiques, mais qui est une bonne introduction à notre sujet, On va dans cette partie, décrire trois algorithmes de factorisations et soulever les problèmes qui peuvent apparaître lors de leurs implémentations.

2.6.1 La factorisation par la méthode du Congruences de carrés

La congruences de carrés est plus une méthode générale qu'un algorithme particulier. Elle a donné lieu à plusieurs algorithmes, dont un seul sera présenté dans cette partie :

l'algorithme de Dixon

L'idée principale remonte à Fermat :
il suffit d'écrire n comme une différence de deux carrées.
Par exemple :

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

De plus l'identité :

$$ab=(\tfrac{1}{2}(a+b))^2 \text{ - } (\tfrac{1}{2}(a-b))^2$$

nous montre que cette méthode fonctionne pour tous les nombres impairs. Elle fonctionne bien si $n = ab$ est tel que a et b sont proche de la racine de n. Sinon la recherche exhaustive de la différence de carré devient trop longue.
Dans les années 1920, Kraitchik remarqua qu'il suffisait de trouver deux entiers u et v tels que :

$$u^2 \text{ - } v^2 \equiv 0 \ (mod\ n),$$

en espérant que l'on n'ait pas $u \equiv \mp v \ (mod\ n)$.
Pour un n impair divisible par au moins deux premiers, on a $u \neq \mp\ v \ (modn)$ dans plus de la moitié des cas.
Un facteur non trivial peut alors être trouvé en calculant :

$$pgcd(u-v, n).$$

Kraitchik remarqua aussi que si t^2 et s^2 ne sont pas des carrés modulo n on peut les multiplier et espérer que leur produit soit un carré modulo n. C'est ce qu'on appelle la combinaison de congruence.
Toutes ces idées ont été formalisées par Dixon dans l'algorithme qu'il a proposé en 1981.

Description de l'algorithme :

- Choisir un entier B. On note :
$$P = \{p \text{ premier}, p < B\}$$
et k le nombre de premiers inférieurs à B (c'est-à-dire le cardinal de P).
- Pour x pris aléatoirement dans $[\sqrt{n},\ n-1]$, calculer :
$$y = x^2\ mod\ n.$$
Si y est B-friable, on garde le couple (x, y), appelé relation.
- On appelle R l'ensemble des relations et m son cardinal.On répète l'étape précedente jusqu'à avoir $m > k$.
- Pour $1 \leq i \leq m$, on note $(x_i,\ y_i)$ la i^{me} relation et on définit $v_{i,p}$ par :

$$x_i^2 \ mod n = y_i = \prod_{p \in P} P^{v_{i,p}} \ .$$

— Construire la matrice :

$$\text{M}=(v_{i,p} \ mod \ 2) \text{ telque } p \in \text{P} \ ; 1 \leq \text{i} \leq m.$$

— Trouver un vecteur non nul $(e_1, \ldots, e_m) \in \mathbb{Z} = 2\mathbb{Z}^m$ du noyau de M.

— On obtient la congruence de carrés voulu en calculant

$$\prod_{1 \leq i \leq m} x_i^{2e_i}$$

La dernière étape fournit bien une congruence de carrés car :

$$\prod_{1 \leq i \leq m} x_i^{2e_i} \equiv \prod_{1 \leq i \leq m} \prod_{p \in P} P^{v_{i,p}e_i} \equiv \prod_{p \in P} P^{\sum_{1 \leq i \leq m} v_{i,p}e_i} \ mod \ n.$$

Et par définition du vecteur $(e_1, \ldots, e_m)$,

$$\sum_{1 \leq i \leq m} v_{i,p} \ e_i \equiv 0 \ mod \ 2.$$

On a donc bien une congruence de carrés :

$$u^2 \equiv v^2 \ mod \ n,$$

avec :

$$u = \prod_{1 \leq i \leq m} x_i^{e_i},$$

et :

$$v = \prod_{p \in P} P^{\frac{1}{2} \sum_{1 \leq i \leq m} v_{i,p}e_i}),$$

qui avec une probabilité supérieure à $1/2$ (si n est impair et posséde au moins deux facteurs premiers), donnera un facteur non trivial de n.

De même que pour les autres algorithmes, le choix de B est très important. Si l'on choisit B trop grand, le nombre de relations nécessaires est trop important et si l'on choisit B trop petit on passe trop de temps pour trouver une relation.

Le meilleur compromis donne un complexité en $O(L_n(1/2, 2))$. On remarque que, contrairement aux algorithmes décrit précédement, la complexité dépend de n et non du plus petit facteur premier p.

En effet, les algorithmes reposant sur la congruence de carrés sont plus efficaces pour factoriser des entiers de type $n = pq$ avec p et q premiers que pour trouver des petits facteurs de grands entiers.

Différentes méthodes pour touver une congruence de carrés qui ont donné lieu à différents algorithmes :

- La méthode CFRAC utilisant les fractions continues ;
- La méthode QS (Quadratic Sieve) et MPQS (Multiple Polynomial Quadratic Sieve) introduisant au passage une nouvelle méthode pour trouver plusrapidement des relations : le crible.
- La méthode SNFS (Special Number Field Sieve) puis GNFS (General Number Field Sieve) utilisant de la théorie algébrique des nombres et reposant sur la factorisation d'idéaux dans des anneaux d'entiers.

  La fin de l'algorithme (recherche d'un vecteur dans le noyau d'une matrice et calcul du *pgcd*) est identique pour tous ces algorithmes. Pour une description historique et mathématique de ces algorithmes on pourra consulter GNFS a une complexité en :

  $$L_n(1/3, \sqrt[3]{\tfrac{64}{9}}) ;$$

  c'est actuellement la meilleure complexité pour un algorithme de factorisation, et c'est donc l'algorithme le plus adapté pour factoriser des très grands entiers (plus de 100 chiffres).

Remarque

L'implémentation des ces algorithmes dans cette méthode a soulevé de nouveaux problèmes :

- Ces algorithmes demandent énormément de calculs, on peut donc se demander quelles sont les étapes que l'on peut paralléliser (i.e. effectuer en même temps sur plusieurs ordinateurs).
- Lors de la dernière étape de l'algorithme, la matrice peut être très grande (plusieurs millions de ligne et colonnes) mais possède des propriétés particulères (elle est creuse). Il est donc nécessaire d'avoir des algorithmes efficaces pour ce genre de matrices contre lesquelles le pivot de Gauss est innefficace.

  Cette méthode présente des inconvenients.

Pour palier à certains problèmes on introduit les courbes elliptiques qui permettent l'adoption de nouveaux cryptosystèmes. Elles sont en effet à l'origine d'une méthode élégante de factorisation, due à H.W.Lenstra.

2.6.2 La factorisation par l'algorithme $p-1$ de Pollard

La méthode $p-1$ de Pollard est une méthode efficace pour factoriser des entiers n admettant un facteur premier p tel que la décomposition en facteurs premiers de $p-1$ ne fait apparaitre que de petits nombres premiers. Supposons qu'on à un tel entier n, et que tous les facteurs premiers de $p-1$ sont inférieurs ou égaux à r. On choisit également a un autre entier. Alors, $p-1$ divise r (on suppose aussi que tous les facteurs premiers de $p-1$ sont simples).
D'après le petit théorème de Fermat :

$$a^r \equiv 1[p].$$

En particulier, p divise a^r - 1 et n, et donc le $pgcd(n,\, a^r - 1)$ donne un diviseur strict de n. Bien sûr, cet algorithme à 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. Voir[17].

Factorisation des petits nombres

La première catégorie de nombres à factoriser est celle des moins de 20 chiffres. Un algorithme trés efficace et est celui de Pollard. L'algorithme ne nécessite que quelques lignes de code une quarantaine seulement et est trés simple à programmer : l'idée est de calculer une suite du type :

$$u_{k+1} \equiv f(u_k\ ).$$

En effet, on peut montrer que pour certains écarts fixés entre k_1 et $k_2 = g(k_1\ )$, alors :

$$u_{k_2}\ \text{-}\ u_{k_1},$$

est un multiple d'un facteur de m.
Il s'agit alors de calculer $pgcd(u_{g(k)}$ - u_k, $m)$ pour les différentes valeurs de k, celui-ci finira par tomber sur un facteur non trivial de m.
Si l'on prend :

$$f(u) = u^2 + 1,$$

il faudra de l'ordre de $\sqrt{p}$ itérations si p est le plus petit facteur de m.
En pratique, cet algorithme factorise en quelques secondes les nombres de 1 à environ 25 chiffres avec des facteurs de 12 ou 13 chiffres, cela donne environ 10 millions d'itérations et devient très rapidement inutilisable pour des facteurs au delá de 15 chiffres.

Le choix des paramètres

Choix de k : le nombre d'iteration

On commence par se fixer un paramètre v qui est de l'ordre d'un majorant des facteurs premiers de n. On peut prendre la partie entière de$\sqrt{n}$.
Ensuite on fixe w qui est le temps passé sur une courbe. w est pris égal à :

$$L(v)^{\frac{1}{\sqrt{2}}},$$

avec :

$$\mathrm{L}(x) = e^{\sqrt{\ln(x)\ln(\ln(x))}}$$

En effet, si :

$$u = \text{card } \{s \in \mathbb{Z} \ / \ |s \text{ - } (p+1)| < \sqrt{p}, \text{ et tout nombre premier divisant } s \text{ est} \leq w\},$$

alors :

$$f(w) = \frac{u}{2\sqrt{p}+1}$$

est la probabilité qu'un entier choisi au hasard dans l'intervalle $(p + 1$ - $\sqrt{p}$, $p + 1 + \sqrt{p})$ ait tous ses facteurs premiers infeérieurs ou égaux à w.
Alors, pour tout $h \in \mathbb{N}, > 1$, il existe une constante calculable $c > 1$ telle que la probabilité de succès de l'algorithme est au moins

$$1 - c^{-h\frac{f(w)}{\ln(v)}}$$

Ainsi pour avoir une chance raisonnable de succés on doit choisir h de même ordre de grandeur que $ln(v)/f(w)$, h devant être minimal on doit choisir w tel que $w/f(w)$ soit minimal.
Un théorème de Canfield, Erdös et Pomerance dit que si α est un réel positif, la probabilité qu'un entier positif $s \leq x$ choisi au hasard ait tous ses facteurs premiers inférieurs ou égaux á $L(x)^\alpha$ est :

$$L(x)^{\frac{-1}{2\alpha}+O(1)}.$$

Une conjecture non prouvée dit que le résultat est encore vrai si s est un entier pris au hasard dans l'intervalle $(x+1 - \sqrt{x},\ x+1 + \sqrt{x})$. Ainsi
f$(L(x)^\alpha) = L(x)^{\frac{-1}{2\alpha}+o(1)}$. Donc pour $x = v$, et $w = L(v)^\alpha$, on a :

$$w/f(w) = L(x)^{\frac{-1}{2\alpha}+\alpha+o(1)}$$

ce qui est minimal pour $\alpha = 1/\sqrt{2}$
A partir de là on choisit k de la manière suivante :
pour tout entier r ≥ 2 on note $e(r)$ le plus grand entier m tel que :

$$r^m \leq v + 2\sqrt{v} + 1.$$

On prend alors :

$$k = \prod_{r=2}^{w} r^{e(r)}$$

Ce choix résulte d'une simple conjecture mais il semble que ce soit la meilleure estimation possible.

Choix de h :

Dáprès le paragraphe précédent h doit être de l'ordre de grandeur de $\ln(v)/f(w)$ et comme $f(w)$ est du même ordre de grandeur que $L(v)^{\frac{-1}{\sqrt{2}}}$, on choisit h égal à :

$$\ln(v)\ L(v)^{\frac{1}{\sqrt{2}}}$$

2.6.3 La factorisation par la méthode des courbes elliptiques

La factorisation de Lenstra

La factorisation de Lenstra par les courbes elliptiques est un algorithme probabiliste rapide pour la décomposition en produit de facteurs premiers qui utilise les courbes elliptiques. Cette méthode fut le meilleur algorithme pour la décomposition en produit de facteurs premiers jusqu'au développement du crible général de corps de nombres (GNFS).
Il est encore le meilleur pour l'extraction des diviseurs dont la taille ne dépasse pas 20 chiffres (64 bits), comme son temps d'exécution dépend de la taille d'un facteur p plutôt que de la taille du nombre n à factoriser.
C'est une amélioration de la traditionnelle méthode de factorisation $p-1$ de Pollard. Dans cette méthode, il était supposé que le nombre donné n possède un facteur premier p tel que $p-1$ possède seulement des "petits" facteurs premiers (les nombres dont les facteurs premiers sont tous "petits" sont dits friables).
Alors, par le petit théorème de Fermat :

$$a^e = 1 \ mod \ p, \text{ si } p-1 \text{ divise } e \text{ et } p \text{ ne divise pas } a.$$

En prenant e comme un produit de petits nombres premiers élevés aux petites puissances, et a comme un résidu aléatoire $mod\ n$, nous pouvons espérer factoriser n en calculant :

$$pgcd(n,\ a^e\ -\ 1),$$

comme les autres diviseurs q de n ne semblent pas avoir la propriété $q-1$ divise e, les valeurs friables sont rares.
Néanmoins, l'on ne pourra pas factoriser n si n n'a pas un facteur premier p avec $p-1$ friable.
La factorisation de Lenstra contourne cet obstacle en considérant le groupe d'une courbe elliptique aléatoire sur le corps fini $\mathbb{F}_p$, plutôt que sur le groupe multiplicatif de $\mathbb{F}_p$ qui a toujours un ordre $p-1$.
L'ordre du groupe d'une courbe elliptique sur $\mathbb{F}_p$ varie entre $p+1-2\sqrt{p}$ et $p+1+2\sqrt{p}$ (un théorème de Helmut Hasse(voir 1.8)) aléatoirement, et doit être probablement friable pour certaines courbes elliptiques.
Voir [18].

La factorisation par la méthode des courbes elliptiques(ECM)

L'algorithme ECM (Elliptic Curve Method), proposé par H. Lenstra en 1987, utilise les propriétés des courbes elliptiques sur les corps finis pour factoriser des entiers.
L'algorithme ECM repose sur les mêmes idées que l'algorithme $p-1$ où l'on remplace les groupes $(\mathbb{Z}/n\mathbb{Z})^*$ et $(\mathbb{Z}/p\mathbb{Z})^*$ par des groupes de courbes elliptiques sur les corps finis. Car le travail est beaucoup plus rapide.

Description de l'algorithme :

— Choisir une courbe elliptique E sur $\mathbb{K}$ d'élément neutre O_E.
Soit P un point de E qui n'est pas un point de torsion. On suppose que la courbe à bonne réduction modulo tous les premiers p divisant n -cela se vérifie à l'aide de calculs de *pgcd*-, sinon on en choisit une autre. Cela signifie que vu modulo p, la courbe est encore une courbe elliptique, i.e $\Delta \neq 0$[p].

— Choisir un entier B. On pose, comme lors de l'algorithme $p-1$,
$$s = \prod_{\pi \leq B} \pi^{\frac{\log(B)}{\log(\pi)}},$$
telque π est premier.

— Calculer le point
$$(x, y) = [s]P = P + ... + P \text{ (répété } s \text{ fois)},$$
en effectuant tous les calculs intermédiaires modulo n.
Cela revient à ne plus voir la courbe sur $\mathbb{K}$ mais sur $\mathbb{Z}/n\mathbb{Z}$. La seule opération qui n'existe pas toujours dans $\mathbb{Z}/n\mathbb{Z}$ est l'inverse. Mais un élément non inversible de $\mathbb{Z}/n\mathbb{Z}$ est un élément qui n'est pas premier avec n, il fournit donc un facteur de n différent de 1.

— Si le calcul termine ou si l'on tombe sur le point à l'infini de la courbe modulo n, on recommence le calcul avec une autre courbe.

Factorisation des grands nombres

Pour aller plus loin, la méthode de Lenstra est une solution. Celle-ci utilise des courbes elliptiques du type y^2=x^3+ax+b par exemple, sa programmation reste simple (environ 150 lignes de code) et nous pouvons donner quelques idées des propriétés

de cet algorithme : il est conjecturé que cet algorithme nécessite un nombre moyen d'opérations de l'ordre de

$$O(\ln\ (m)^2\ e^{\sqrt{2\ln(p)\ln(\ln(p))}}),$$

En pratique, cet algorithme factorise en quelques secondes les nombres de à chiffres (avec deux facteurs de tailles semblables).

En outre, si l'on a de la chance et que l'on choisit une courbe elliptique particuliere, celle-ci peut permettre de factoriser très rapidement.

Le problème est que les bonnes courbes elliptiques varient pour chaque nombre a factoriser et qu'il n'existe pas encore de moyen de trouver la bonne courbe pour un nombre donné. Toutefois, cette rapidité de calcul lorsque l'on à une "bonne" courbe elliptique est à l'origine du programme de factorisation, en effet, de nombreux internautes peuvent récupérer le programme ECM et le lancer pour qu'il essaye différentes courbes elliptiques

Ainsi, un nombre très important de courbes elliptiques peut être exploré dans le même temps et accélérer potentiellement la recherche de facteurs premiers.

2.7 Comment factoriser par courbes elliptiques

L'idée de l'algorithme de factorisation de Lenstra permettant de trouver un facteur d'un nombre donné n, que l'on doit factoriser, cette algorithme fonctionne de la manière suivante : On note p un diviseur premier de n que l'on ne connait pas.

Etape 1 : choix d'une courbe elliptique

On choisit a et b tel que $4a^3 + 27b^2$ soit premier avec n. Si en les prenant au hasard remarquons que, puisque $4a^3 + 27b^2$ est premier avec n, il est premier avec p et est inversible dans $\mathbb{Z}/p\mathbb{Z}$, p diviseur de n non connu.

L'équation

$$y^2 = x^3 + ax = b,$$

définit une courbe elliptique sur $\mathbb{Z}/p\mathbb{Z}$, que nous noterons $E(a, b, p)$ (signalons que, puisqu'on ne connait pas p, on ne connait pas cette courbe elliptique).

Etape 2 : choix d'un point sur la courbe elliptique

On trouve deux entiers x et y tels que :

$$y^2 = x^3 + ax + b.$$

En particulier, $P(x, y)$ est un point de la courbe elliptique $E(a, b, p)$.

Etape 3 : choix d'un entier auxiliaire

On choisit k un entier pas très grand, mais qui est produit de petits facteurs premiers à des exposants déjà élevés. Par exemple, $k = 2^{10}3^85^67^4$.

Etape 4 : calcul sur les courbes elliptiques

On calcule les coordonnées du point kP, en utilisant les formules classiques, les calculs s'effectuant modulo n. Ces calculs font intervenir des divisions, et ceci n'est pas toujours possible modulo n, il faut que le dénominateur d soit premier avec n.
Mais ce qu'on espère, c'est que ce n'est pas le cas. En effet, si d n'est pas premier avec n, $pgcd(d, n)$ donne un diviseur premier de n. Si on a pu mener les calculs jusqu'au la fin, on recommence à l'étape 1, en changeant de courbe elliptique.

2.8 Quelques exemple de la factorisation par la méthode des courbes elliptiques

Exemple 01 : Factorisation d'un petit nombre

Nous voulons factoriser 4453. Soit E la courbe elliptique d'équation

$$y^2 = x^3 + 3x \ (mod\ 4453)$$

et soit $P = (1, 2)$. Essayons de calculer $6P$. Calculons tout d'abord $2P$, la pente de la tangente au point P est :

$$\frac{3x^2+3}{2y} = \frac{3}{2} \equiv 2228 \ (mod\ 4453).$$

En effet :

$$pgcd(2,\ 4453) = 1,$$

donc 2 est inversible *mod* 4453 et

$$2^{-1} \equiv 2227\ (mod\ 4453).$$

Utilisant la pente, nous trouvons $2P = (x, y)$, avec :

$$x \equiv 3340 \text{ et } y \equiv 1669\ (mod\ 4453).$$

Nous calculons maintenant 3P en additionnant P et 2P. La pente est :

$$\tfrac{1669-2}{3340-1} = \tfrac{1667}{3339} \equiv 746\ (mod\ 4453).$$

En effet,

$$pgcd(3339,\ 4453) = 1,$$

donc 3339 est inversible modulo 4453 et

$$3339^{-1} \equiv 1483\ (mod\ 4453).$$

Nous pouvons donc trouver $3P = (x, y)$ avec :

$$x \equiv 1003 \text{ et } y \equiv 610\ (mod\ 4453).$$

Calculons maintenant $6P = 3P + 3P$.
Si nous regardons le dénominateur de la pente, qui est $2 \times 610 = 1220$, nous voyons que :

$$pgcd(1220,\ 4453) = 61 \neq 1.$$

Ainsi nous ne pouvons pas inverser 1220 modulo 4453 et ne pouvons pas trouver la pente voulue.
Par contre, nous avons trouvé que 61 est un facteur de 4453 et nous pouvons factoriser

$$4453 = 61 \times 73.$$

Nous avons que :

$$E(\mathbb{Z}/4453\mathbb{Z}) \cong E(\mathbb{Z}/61\mathbb{Z}) \oplus E(\mathbb{Z}/73\mathbb{Z}).$$

Regardons les multiples de P $(mod\ 61)$,

$$P \equiv (1,\ 2),\ 2P \equiv (46,\ 22),\ 3P \equiv (27,\ 0),\ 6P = \mathrm{O},\ \ldots\ (mod\ 61).$$

Les multiples de P $(mod\ 73)$ sont :

$$P \equiv (1,\ 2),\ 2P \equiv (55,\ 63),\ 3P \equiv (54,\ 26),\ 6P \equiv (65,\ 11),\ \ldots\ (mod\ 73).$$

Ainsi, lorsque nous calculons $6P$ $(mod\ 4453)$, nous obtenons O modulo 61 et un point fini modulo 73 .

Pour factoriser un nombre n par la méthode des courbes elliptiques il nous faut donc différentes courbes elliptiques E_i définies sur $\mathbb{Z}/n\mathbb{Z}$ et des points P_i sur ces courbes. Un moyen pour trouver ceci est de choisir des entiers A_i $(mod\ n)$ et un point $P_i = (u_i,\ v_i)$ $(mod\ n)$. Nous définissons ensuite les C_i tels que :

$$C_i = v_i^2 \text{ - } u_i^3 \text{ - } Au\ (mod\ n).$$

Nous obtenons ainsi des courbes elliptiques :

$$E_i : y^2 = x^3 + A_i x + C_i$$

avec un point P_i.

Cette méthode est beaucoup plus efficace que de choisir des entiers A_i, C_i, u_i et ensuite de chercher v_i puisque calculer la racine carrée $mod\ n$ est équivalent à factoriser n.

Exemple 02 : Factorisation d'un grand nombre

On veut factoriser avec la méthode des courbes elliptiques le nombre :

$$n = 203131958479987807 = 2011 \times 10000019 \times 10101023,$$

Bien sûr, à priori on ne connait pas la factorisation à l'avance, mais on va voir comment la méthode des courbes elliptiques est capable de détecter le facteur premier $p = 2011$. Tout d'abord, on choisit le nombre B, pour cela on calcule :

$$\exp((\tfrac{\sqrt{2}}{2})\log(2011)^{1/2}\log(\log(2011))^{1/2}) \approx 16.08,$$

On pose alors $B = 16$ (dans la pratique, on ne peut pas calculer B de cette manière puisque l'on ne connait pas le nombre p, mais on prend B de plus en plus grand jusqu'à ce que la méthode finie). Ainsi le nombre r donné par :

$$r = 2^4 \times 3^2 \times 5 \times 7 \times 11 \times 13,$$

On choisit une courbe E aléatoirement sur $\mathbb{Z}/n\mathbb{Z}$ et on considère que le nombre $|E_{2011}(F_{2011})|$ est un nombre au hasard plus petit que $2012 + 2\sqrt{2011}$.

On peut montrer que les diviseurs premiers d'un tel nombre sont tous plus petits que B avec une probabilté $\approx 1/B$. En testant donc quelques dizaines de courbes, on a une bonne chance de détecter le facteur 2011. Nous prenons les courbes elliptiques suivantes :

$$E : y^2 = x^3 + x + (y_1^2 - x_1^3 - x_1),$$

pour $x_1, y_1 = 1, 2, 3$. Dans le tableau suivant, nous donnons la factorisation de $|E_{2011}(F_{2011})|$ pour chacune de ces 9 courbes.

$y_1 \backslash x_1$	1	2	3
1	$2^2 \times 11 \times 47$	$2^2 \times 503$	$2 \times 7 \times 11 \times 13$
2	$2^5 \times 3^2 \times 7$	43×47	2×991
3	$2^2 \times 3 \times 167$	$2^2 \times 11 \times 47$	$2^2 \times 7 \times 73$

Ainsi, le couple $(x_1, y_1) = (3, 1)$ devrait permettre de détecter le facteur 2011. Dans ce cas, on a $P = (3, 1)$ et la courbe E est définie par :

$$E : y^2 = x^3 + x - 29 \text{ sur } \mathbb{Z}/n\mathbb{Z}.$$

On a successivement :

$P_1 = 2^4 P = (113335492298694779,120072510320811350)$,

$P_2 = 3^2 P_1 = (88473308409788250,44958990040955827)$,

$P_3 = 5P_2 = (62528891122227755,4402639539853129)$,

$P_4 = 7P_3 = (80943592970473600,19944167038863674)$,

$P_5 = 11P_4 = (176914498221880419,88610394536361644)$,

Par contre le calcul de $13P_5$ aboutit à la détection du facteur 2011. En effet, par exemple, on calcule facilement :

$12P_5 = (126794386927080337, 169864995554483396)$

Maintenant, le calcul de $12P_5 + P_5 = 13P_5$ demande l'inversion de :

$$176914498221880419 - 126794386927080337 = 50120111294800082,$$

Or, on a :

$$pgcd(50120111294800082,\, n) = 2011.$$

Les multiplications par 3^2 et par 5 étaient inutiles mais on ne peut pas le savoir à l'avance.

2.9 Avantage de la méthode ECM

Que faire face à un entier que l'on veut factoriser et dont on ne connait pas a priori la taille des facteurs. Tout d'abord il ne faut pas négliger la méthode classique pour éliminer les petits facteurs.

Un entier aléatoire à 92 ·/. de chance de posséder un facteur inférieur à 1000. Et pour des petits facteurs -moins de 10 chiffres-, la méthode classique est la plus rapide.

Ensuite on peut essayer l'algorithmes $p-1$ de Pollard mais c'est surtout la méthode de factorisation par courbes elliptiques de ECM qui sert à trouver les facteurs de taille moyenne.

Alors de ce qui précéde on conclut la déffirence entre la méthode $p-1$ de Pollard et la méthode de factorisation de Lenstra telque :

la traditionnelle méthode de $p-1$ de Pollard sa nombre donné n possède un facteur premier p telque $p-1$ possède seulement des petits facteurs premier p, mais par la méthode de de factorisation de Lenstra factorise des grandes nombres en quelques secondes elle est très rapide par rapport la première.

L'avantage de cette méthode, c'est qu'a chaque courbe elliptique correspond des ordres différents, ainsi en cas d'echec lors de la factoeisation de n, il suffit de changer de courbe elliptique et de recommencer en espérant avoir plus de chance. Il est de plus possible d'utiliser plusieurs courbes et points à la fois.

Chapitre 3

Problèmes traité par la factorisation par courbes elliptiques

3.1 Calcul de l'ordre d'un point et d'une courbe elliptique

Calcul de l'ordre d'un point P

Déterminer les coordonnées d'un point P d'une courbe elliptique $E(\mathbb{F}_p)$ revient à fixer aléatoirement un élément x de $\mathbb{F}_p$ et vérifier que l'équation de Weierstrass définissant cette courbe, alors ramenée à une équation du second degré, admet une solution $y \in \mathbb{F}_p$.
De par la structure de corps de $\mathbb{F}_p$, les formules de résolution des racines d'un trinôme sont valables,On peut donc facilement déterminer $y \in \mathbb{F}_p$.
Connaissant les coordonnés d'un point P et la factorisation en produit de facteurs premiers de l'ordre de $E(\mathbb{F}_p)$, il est possible de déterminer l'ordre de P en temps polynomial.

Calcul de l'ordre d'une courbe $E(\mathbb{K})$

Le théorème de Hasse sur le nombre de points d'une courbe elliptique fournit l'approximation :

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

A fin de trouver le nombre exact de points, il est suffisant de trouver ce nombre modulo R $> 4\sqrt{p}$.
L'algorithme de Schoof calcule donc :

$$p + 1 - |\mathrm{E}(\mathbb{F}_p)| \ (mod\ r_i)$$

pour plusieurs petits nombres premiers r_i, où :

$$\prod r_i = R.$$

Le résultat final est obtenu par combinaison via le théorème des restes chinois.

L'algorithme de Schoof

Voir la section[1.5]

3.2 Le problème de criptage

En cryptographie, les courbes elliptiques, des objets mathématiques, peuvent être utilisées pour des opérations asymétriques comme des échanges de clés sur un canal non sécurisé ou un chiffrement asymétrique, on parle alors de cryptographie sur les courbes elliptiques ou ECC (du sigle anglais elliptic curve cryptography). L'usage des courbes elliptiques en cryptographie a été suggéré, de manière indépendante, par Neal Koblitz et Victor Miller en 1985.
Les clés employées pour un chiffrement par courbe elliptique sont plus courtes qu'avec un système fondé sur le problème de la factorisation comme RSA. De plus l'ECC procure un niveau de sécurité équivalent ou supérieur aux autres méthodes. Un autre attrait de l'ECC est qu'un opérateur bilinéaire peut être défini entre les groupes. Cet opérateur se base sur le couplage de Weil ou le couplage de Tate. Les opérateurs bilinéaires se sont récemment vus appliqués de nombreuses façons en cryptographie, par exemple pour le chiffrement basé sur l'identité. Un point négatif est que les opérations de chiffrement et de déchiffrement peuvent avoir une plus grande complexité que pour d'autres méthodes.

Le système RSA

le système RSA est le problème de l'inversion de la fonction de chiffrement du système de cryptographie asymétrique RSA. Etant donné que RSA est un chiffrement surjectif, ce problème a toujours une solution.
La difficulté calculatoire supposée de ce problème implique la sécurité sémantique du chiffrement RSA avec un remplissage adéquat, puisque le chiffrement RSA tel qu'il est usuellement décrit est déterministe et ne peut donc pas être sémantiquement sûr.

Définition 21

Plus formellement, le problème RSA est le problème d'arithmétique modulaire suivant.
$n, e, c \in \mathbb{N}$(données), et e premier avec $\phi(n)$.
Le problème est de trouver une racine e-ième de C modulo n.
Autrement dit trouver un entier m tel que :

$$m^e \equiv C \ mod \ n$$

avec les notations précédentes.
Le problème à toujours une solution qui est unique modulo n. En effet
$\phi(n) = (p-1)(q-1)$ est l'ordre du groupe des éléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$, donc si e est inversible d'inverse d modulo $\phi(n)$, alors :

$$m = Cd \ mod \ n,$$

par le théorème d'Euler.
En revanche si e n'est plus premier avec $\phi(n)$, alors le problème perd l'unicité de la solution, et son existence pour tout C. On peut le voir à l'aide d'un exemple jouet du problème RSA avec :

$$n = 65 = 5 \times 13 \text{ et } e = 3,$$

de telle manière que :

$$e \mid \phi(65) = 48,$$

alors en "chiffrant" 5, on obtient :

$$5^3 \equiv 60 \; mod \; 65,$$

mais si on "chiffre" 45, on obtient aussi :

$$45^3 \equiv 60 \; mod \; 652.$$

En transmettant uniquement 60 comme chiffré, il est donc impossible de remonter au message initial. Le chiffrement n'est plus injectif.
Mathématiquement, cela vient du fait qu'un inverse de e modulo $\phi(n)$ est un élément d tel que :

$$ed = 1 + r\phi(n),$$

pour un certain entier relatif r.
Ainsi e inversible modulo $\phi(n)$ est équivalent à écrire qu'il existe deux entiers relatifs d et r tels que :

$$ed \text{ - } r\phi(n) = 1.$$

Cette relation n'est réalisable que si $pgcd(e, \phi(n)) = 1$ par le théorème de Bézout.

Lien avec la factorisation

La sécurité de l'algorithme RSA repose sur le fait que ce problème devient impossible à résoudre calculatoirement pour n un produit de deux nombres premiers suffisamment grands, n étant connu mais pas sa factorisation.
En revanche, si l'on dispose de la factorisation de n, il devient facile de calculer $\phi(n)$, qui est la clef privée du chiffrement RSA. Résoudre ce problème revient alors à lancer l'algorithme de déchiffrement du cryptosystème. C'est pour cela que l'on considère la fonction :

$$m \rightarrow m^e \; mod \; n,$$

comme étant une fonction à sens unique avec trappe.
De plus, comme résoudre le problème de la factorisation nous donne une solution pour résoudre le problème RSA, RSA est au moins aussi facile que la factorisation. Savoir si les deux problèmes sont équivalents reste en 2016 une question ouverte.
Une autre manière de dire la même chose est de dire que le problème devient calculatoirement

facile à résoudre si les deux facteurs p et q sont connus, donc $\phi(n)$, ce sur quoi s'appuie le déchiffrement. On pourrait donc résoudre (sur le plan calculatoire) le problème RSA si on savait résoudre le problème de la factorisation d'un entier (la recherche de sa décomposition en facteurs premiers par une méthode calculatoirement efficace). On ne sait toutefois pas s'il existe des méthodes plus efficaces.

Création des clés

L'étape de création des clés est à la charge d'Alice. Elle n'intervient pas à chaque chiffrement car les clés peuvent être réutilisées, la difficulté première, que ne règle pas le chiffrement, est que Bob soit bien certain que la clé publique qu'il détient est celle d'Alice. Le renouvellement des clés n'intervient que si la clé privée est compromise, ou par précaution au bout d'un certain temps (qui peut se compter en années).

— Choisir p et q, deux nombres premiers distincts ;
— calculer leur produit $n = pq$, appelé module de chiffrement ;
— calculer $\phi(n) = (p-1)(q-1)$ (c'est la valeur de l'indicatrice d'Euler en n) ;
— choisir un entier naturel e premier avec $\phi(n)$ et strictement inférieur à $\phi(n)$, appelé exposant de chiffrement ;
— calculer l'entier naturel d, inverse de e modulo $\phi(n)$, et strictement inférieur à $\phi(n)$, appelé exposant de déchiffrement ; d peut se calculer efficacement par l'algorithme d'Euclide étendu.

Comme e est premier avec $\phi(n)$, d'après le théorème de Bachet-Bézout il existe deux entiers d et r tels que :

$$ed + r\phi(n) = 1,$$

c'est-à-dire que :

$$ed \equiv 1 \ (mod\ \phi(n)),$$

e est bien inversible modulo $\phi(n)$.
Le couple (n, e) est la clé publique du chiffrement, alors que le nombre d est sa clé privée, sachant que l'opération de déchiffrement ne demande que la clef privée d et l'entier n, connu par la clé publique (la clé privée est parfois aussi définie comme le triplet (p, q, d)

Chiffrement et déchiffrement du message

Pour le chiffrement :

Si M est un entier naturel strictement inférieur à n représentant un message, alors le message chiffré sera représenté par :

$$C \equiv M^e \ (modn),$$

l'entier naturel C étant choisi strictement inférieur à n.

Pour le déchiffrement :

Pour déchiffrer C, on utilise d, l'inverse de e modulo $(p-1)(q-1)$, et l'on retrouve le message clair M par :

$$M \equiv C^d \ (mod \ n).$$

Exemple

Un exemple avec de petits nombres premiers (en pratique il faut de très grands nombres premiers) :

- on choisit deux nombres premiers $p = 3$, $q = 11$;
- leur produit $n = 3 \times 11 = 33$ est le module de chiffrement ;
- $\phi(n) = (3 - 1) \times (11 - 1) = 2 \times 10 = 20$;
- on choisit $e = 3$ (premier avec 20) comme exposant de chiffrement ;
- l'exposant de déchiffrement est $d = 7$, l'inverse de 3 modulo 20,
  en effet, $ed = 3 \times 7 \equiv 1 \ mod \ 20$.

La clé publique d'Alice est :

$$(n, e) = (33, 3),$$

et sa clé privée est :

$$(n, d) = (33, 7).$$

Bob transmet un message à Alice.

Le chiffrement de $M = 4$ par Bob avec la clé publique d'Alice :

$$4^3 \equiv 31 \ mod \ 33,$$

le chiffré est $C = 31$ que Bob transmet à Alice ;

Le déchiffrement de $C = 31$ par Alice avec sa clé privée :

$$31^7 \equiv 4 \; mod \; 33.$$

Alice retrouve le message initial M = 4.

Le mécanisme de signature par Alice, à l'aide de sa clé privée, est analogue, en échangeant les clés.

Chapitre 4

Application

Voici trois exemples qui mettent en pratique la factorisation des entiers par les courbes elliptiques :

Exemple 01

Factorisons le nombre $n = 10^{50} + 3$.
On trouve par divisions successives les facteurs 19, 97 et 283. Reste a factoriser

$$n_1 = \frac{n}{19\times97\times283} = 191729186358851848940408651587805256830831587,$$

Avec la courbe elliptique E sur $\mathbb{Z}/n_1\mathbb{Z}$ d'équation :

$$y^2 = x^3 + 360x + 1\,;$$

le point $P = (0,\ 1)$ et comme constante

$$B = 1000\,;$$

on constate que $p = 994327748569$ est un diviseur premier de n_1. L'équation choisie de E est de la forme

$$y^2 = x^3 + ax + 1,$$

et $a = 360$ est le plus entier permettant de conclure avec cette valeur de B.
On verifie que l'on a

$$\mid E(\mathbb{F}_p) \mid = 2^3 \times 3 \times 5^2 \times 29 \times 41 \times 61 \times 73 \times 313\,;$$

qui est B-friable, donc la condition $\mid E(\mathbb{F}_p) \mid$ soit B-friable est satisfaite dans ce cas.
Posons ensuite

$$n_2 = \frac{n_1}{994327748569} = 192822926479504827993164286570523,$$

En prenant la courbe elliptique $E^{'}$ sur $\mathbb{Z}/n_2\mathbb{Z}$ d'équation :

$$y^2 = x^3 + 2016x + 1,$$

$P = (0, 1)$ et $B = 1000$, on trouve que

$$q = 61236769827829,$$

est un diviseur premier de n_2.
Notons que l'on a dans ce cas

$$\mid E^{'}(\mathbb{F}_q) \mid = 2 \times 3^2 \times 5 \times 19 \times 157 \times 521 \times 641 \times 683\,;$$

On obtient ainsi la décomposition complète de n_2, et donc celle de n,

$$n_2 = 61236769827829 \times 3148809563627188687.$$

Exemple 02

Posons $n = 2^{211}$ - 1. Il est facile de vérifier que l'on a :

$$n = 15193 \times n_1,$$

où n_1 est un nombre composé de soixante chiffres. Recherchons, à priori, des diviseurs premiers de n_1 ayant au plus vingt-cinq chiffres décimaux. On choisit la courbe elliptique E sur $\mathbb{Z}/n_1\mathbb{Z}$ d'équation :

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

et le point $P = (1, 1)$. En suivant l'éstimation :

$$B = L(A)^{1/\sqrt{2}} \text{ où } L(A) = \exp(\sqrt{\log A \log\log A}),$$

il convient d'essayer de calculer $B!P$ avec B de l'ordre de 50000. Posons pour cela :

$$m = 1000\,! \prod_{k=169}^{5134} p_k,$$

où p_k est le k-ième nombre premier. On a :

$$p_{169} = 1009 \text{ et } p_{5134} = 50021.$$

En essayant de calculer mP, on trouve que :

$$p = 60272956433838849161,$$

qui a vingt chiffres décimaux, est un diviseur premier de n_1. On a choisi ici une équation de la forme :

$$y^2 = x^3 + ax - a,$$

et $a = 6$ est le plus petit entier permettant de conclure. On constate que :

$$\mid E(\mathbb{F}_p) \mid = 2^4 \times 3^2 \times 5 \times 11 \times 293 \times 467 \times 947 \times 3517 \times 16699,$$

dont tous les diviseurs premiers sont plus petits que 50000. En posant :

$$q = \frac{n_1}{p} = 35938757044958237573881998942687731534 39,$$

on vérifie que q est premier, et l'on obtient la décomposition complète de n,

$$n = 15193 \times pq.$$

Exemple 03

Factorisons l'entier :

$$n = \frac{10^{131}-1}{9}$$

qui a cent trente et un chiffres.
3.1) Par la methode des divisions successives, on trouve les diviseurs premiers

$$q_1 = 80173 \text{ et } q_2 = 109517.$$

3.2) Avec la methode rho de Pollard, on trouve les diviseurs premiers :

$$q_3 = 446790173,\ q_4 = 141811693 \text{ et } q_5 = 7370364319027.$$

Il reste a factoriser l'entier de quatre-vingt-onze chiffres :

$$n_1 = \frac{n}{q_1 q_2 q_3 q_4 q_5}.$$

On utilise la methode ECM, en effectuant les calculs avec la même constante m, et des courbes elliptiques de la forme :

$$y^2 = x^3 + ax + 1$$

avec le point $P = (0, 1)$.

3.3) Avec la courbe elliptique sur $\mathbb{Z}/n_1\mathbb{Z}$ d'équation :

$$y^2 = x^3 + 34x + 1$$

on detecte le diviseur premier de vingt-sept chiffres

$$q_6 = 180222062287834025451247081.$$

3.4) Posons $n_2 = \frac{n_1}{q_6}$. Avec la courbe elliptique sur $\mathbb{Z}/n_2\mathbb{Z}$ d'équation :

$$y^2 = x^3 + 116x + 1,$$

on trouve le diviseur premier de vingt-deux chiffres :

$$q_7 = 7317723970031057677693.$$

3.5) Posons $n_3 = \frac{n_2}{q_7}$. Avec la courbe elliptique sur $\mathbb{Z}/n_3\mathbb{Z}$ d'équation :

$$y^2 = x^3 + 370x + 1,$$

on trouve le diviseur premier de vingt-quatre chiffres :

$$q_8 = 131758351065116151205213.$$

3.6) On verifie ensuite que :

$$q_9 = \frac{n_3}{q_8} = 15594845538029429933,$$

est un nombre premier. On obtient ainsi la decomposition complète de n,

$$n = \prod_{i=1}^{9} q_i.$$

Quelques résultats :

Le programme étant écrit en turbo pascal, on a été limité par la taille des nombres à factoriser, à savoir des entiers inférieurs à 2147483647 (il faut aussi tenir compte du choix de v : s'il est trop grand on ne peut calculer w). Par contre en testant le programme, on voit que les nombres non premiers sont factorisés de manière immédiate :

$$2304167 = 2089 \times 1103$$

où

$$1037929037 = 27449 \times 37813.$$

Dans les cas les plus défavorables (lorsque $n = pq$ avec p et q premiers et assez proches), on obtient de bons résultats.
Par exemple le test avec

$$3196943 = 1787 \times 1789$$

(277-ème et 278-ème nombres premiers) ou

$$753667193 = 27449 \times 27457$$

(3000-ème et 3001-ème nombres premiers) renvoie un résultat immédiat.
On a aussi fait quelques tests avec des nombres premiers et l'ordinateur renvoie un message de non factorisation (il n'a pas trouvé de facteur) au bout de 5 secondes avec 3529, 30 secondes avec 11497 et 2 minutes avec 479909.

Limite en ligne de la factorisation en nombres premiers :

21 chiffres semble être la limite afin d'obtenir la factorisation en ligne, par exemple :
$215525392304898663817(21) = 697499261(9) \times 308997305597(12)$ en 5 secondes,
$325812389847171218723(21) = 985717937(9) \times 330533084179(12)$ en 8 secondes,
$911257405449760897039(21) = 5649231271(10) \times 161306443609(12)$ en 8 secondes,
Quelques nombres "cassés" avec ce script sur un serveur hors ligne :
$262158157939114458143411(24) = 534377194849(12) \times 490586350739(12)$,
$647566049626292397956681(24) = 80262788779(11) \times 8068073131739(13)$,

$244049688486973187356571 9(25) = 761838257287(12) \times 3203431780337(13)$,

$219175188923080736688592 63(26) = 288142510391(12) \times 76064857151993(14)$,

$542902577288070739255724 2027(27) = 8284874025851(13) \times 655293702226577(15)$,

$440283994636873004272980 5927(28) = 9096582498011(13) \times 484010335456357(15)$,

$475377826091035800510139 18973(29) = 9166735005257(13) \times 5185901259482389(16)$,

$157127558679069541525864 491061(30) = 28552680542909(14) \times 5503075567386329(16)$,

$649825047254615206673880 715789(30) = 85452603461273(14) \times 7604508475263893(16)$,

$157127558679069541525864 4910617(31) = 4261 \times 223224703987(12) \times 1651956369903431(16)$,

$327296187632434589277316 15853893(32) = 530667019817041(15) \times 61676376222753973(17)$,

2^{168} - 1 = 37414441915671114706014331717536845303191873100185 5(51) =

$15 \times 29 \times 43 \times 113 \times 127 \times 147 \times 221 \times 241 \times 337 \times 1429 \times 3361 \times 5419 \times 14449 \times 15790321 \times 88959882481$

$= 32 \times 5 \times 72 \times 13 \times 17 \times 29 \times 43 \times 113 \times 127 \times 241 \times 337 \times 1429 \times 3361 \times 5419 \times 14449 \times 15790321 \times 88959882481$

2^{169} - 1 = 74828883831342229412028663435073690606383746200371 1(51)

$= 4057 \times 8191 \times 6740339310641 \times 33407622839523953295063270230 33$

Les 2 derniers exemples illustrent bien la difficulté de factoriser des grands nombres. Le temps ne dépend pas du nombre de chiffres du nombre à factoriser mais du nombre de chiffres de ses facteurs premiers.

Remarque

Le plus grand nombre premier découvert en 7 janvier 2016 est le nombre de Merseinne $2^{74207281}$ - 1 ,qui comporte 22 millions de chiffres en écriture décimale.

Conclusion

La méthode de factorisation par les courbes elliptiques découverte par Hendrik W. Lenstra, Jr en 1985 a une complexité sous exponentielle en la taille du plus petit facteur p de n, consiste à rechercher l'ordre d'un élément du groupe défini par une courbe elliptique sur $\mathbb{F}_p$ grâce à une arithmétique modulo m.

Les plus grands facteurs découverts par cette méthode ont une quarantaine de chiffres.

$quoi$	par	$chiffres$	$quand$
$11^{118}+1$	$ArjenK.Lenstra, etMarcS.Manasse$	38	1991
F_{467}	$RobertD.Silverman$	38	1992
F_{667}	$PeterL.Montgomery$	38	1992
$p(1127)$	$ArjenK.Lenstra$	40	1992
$10^{201}-1$	$DaveRusin$	42	1992
$p(19997)$	$Franz-DieterBerger, etThomasDenny$	43	1993

Nous avons donc présenté des factorisations basés sur les courbes elliptiques et différents problèmes qui y sont liés.

Les courbes elliptiques sont des objets mathématiques modèrnes importants pour la factorisation des grandes entiers qu'on retrouve dans plusieurs domaines comme la théorie des codages et en cryptographie où on utilise des cryptosystèmes à clés publiques dont l'éfficacité repose sur la difficulté de pouvoir résoudre le groupe multiplicatif d'un corps fini.

L'arithmétique sur le groupe des points rationnels d'une courbe elliptique sur un tel corps peut être rendue très rapide et les clefs sont plus petites à sécuriser : là où il faut 1024 bits pour RSA, il suffit de 160 bits pour les courbes elliptiques.

La terminologie ECPP utilise la théorie des courbes elliptiques pour résoudre des problèmes de primalité.

Finalement, les techniques de factorisation progressent rapidement, et les systèmes modernes de cryptage de données seront sûrs tant que la décomposition des nombres de plus de 100 chiffres en facteurs restera difficile.

Des problèmes ouverts

Une citation :

"Arthur Hennessy dit : En observant les nombres premiers, on éprouve le sentiment dêtre en présence d'un des plus inexplicables secrets de la création."

— Existe-t-il une infinité de nombres premiers de Mersenne ?

Autrement dit, existe-t-il une infinité de nombres premiers de la forme $2n$ -1 ?

À ce jour, on en connaît 40 nombres : les 5 plus petits sont :

$$2^2 \text{ - } 1,\ 2^3 \text{ - } 1,\ 2^5 \text{ - } 1,\ 2^7 \text{ - } 1 \text{ et } 2^{13} \text{ - } 1,$$

les 4 plus grands connus sont :

$$2^{3012377} \text{ - } 1,\ 2^{6972593} \text{ - } 1,\ 2^{13466917} \text{ - } 1 \text{ et } 2^{20996011} \text{ - } 1.$$

Ce dernier nombre est le plus grand nombre premier connu. Un prix de 100 000 dollars US est offert à la première personne qui trouvera un nombre premier ayant au moins un million de chiffres.

— Existe-t-il une infinité de nombres premiers de Fermat ?

Les nombres de Fermat sont les nombres de la forme $2^{2^n} + 1$.

À ce jour, les seuls connus qui soient premiers sont

$2^{2^0} + 1 = 3$

$2^{2^1} + 1 = 5$

$2^{2^2} + 1 = 17$

$2^{2^3} + 1 = 257$

$2^{2^4} + 1 = 65537$

— Existe-t-il une infinité de nombres de Fibonacci qui soient premiers ?

Les 12 plus petits nombres de Fibonacci qui sont premiers sont

2, 3, 5, 13, 89, 233, 1597, 28657, 514229, 433494437, 2971215073, 99194853094755497.

Rappelons que la suite des nombres de Fibonacci est la suite 1, 1, 2, 3, 5, 8, 13,21, 34,. . . , où chaque terme (à partir du 3^e) est la somme des deux précédents.

— Existe-t-il une infinité de nombres premiers de la forme $n^2 + 1$?

Les nombres premiers 2, 5, 17, 37, 101, 197, 257, 401, 577, 677, 1297, . . . sont tous de la forme $n^2 + 1$.

Nous sommes tous convaincus que cette suite est infinie, mais une preuve nous échappe.

Toutefois, en 1998, John Friedlander et Henryk Iwaniec ont démontré qu'il existait une infinité de nombres premiers de la forme :

$$a^2 + b^4.$$

— Les nombres de la forme $n! + 1$:

Le nombre $n! + 1$ est premier lorsque n vaut 1, 2, 3, 11,27, 37, 41, 73, 77, 116, 154, 320, 340, 399, 427, 872, 1477,6380 et 26951. Y en a-t-il d'autres ? Sûrement !

— Les nombres de la forme $n! - 1$:

Le nombre n ! - 1 est premier lorsque n vaut 3, 4, 6, 7, 12,14, 30, 32, 33, 38, 94, 166, 324, 379, 469, 546, 974, 1963,3507, 3610, 3697, 21480 et 34790. Y en a-t-il d'autres ?

— Les fascinants nombres premiers de Wieferich :

D'après le petit théorème de Fermat, on sait que si p est un nombre premier impair, alors $2^{p-1} \equiv 1\ (mod\ p)$ (ce qui veut dire que p divise 2^{p-1} - 1).

Existe-t-il des nombres premiers p tels que $2^{p-1} \equiv 1\ (mod\ p^2)$?

Oui ! On en connaît deux, soit 1093 et 3511.

Tout nombre premier p>2 qui satisfait la congruence :

$$2^{p-1} \equiv 1(mod\ p^2)$$

est appelé un nombre premier de Wieferich (en l'honneur de A. Wieferich qui y a vu un lien avec le dernier théorème de Fermat). À part 1093 et 3511, on sait qu'il n'y a aucun autre nombre premier de Wieferich inférieur à 10^{15}. On croit qu'il en existe une infinité, mais on ne sait pas le démontrer. On a même des raisons de croire que la quantit'e de nombres premiers de Wieferich. x est environ $\log\log x$. Ce qui est particulièrement troublant, c'est qu'on ne sait même pas d'emontrer qu'il y a une infinit'e de nombres premiers qui ne sont pas des nombres premiers de Wieferich.

Bibliographie

[1] AIT-AMRANE Nacima Rosa. *Rangs d'une Famille de Twists Quadratiques de Courbes Elliptiques*, mémoire de magistère.UST HOUARI BOUMEDIENNE(ALGER), 2002.

[2] Joseph H. Silverman, *The Arithmetic of Elliptic cuves*. Springer-Verlag New York Inc, 1986.

[3] H. Silverman, John Tate, *Rational Ponts on Elliptic Curves*. Springer-Verlag New York Inc, 1992.

[4] A.V.Pogorelov. *Topics in the Theory of Surfaces in Elliptic Space*, RICHARD SACKS-TEDER, Institute of Mathematical Sciences, New York University, 1960.

[5] Dale.Husemoller, *Elliptic Curves, Second Edition*, Springer-Verlag New York Inc, 1987.

[6] G. Cornell, J. Silverman, et G. Stevens, *Modular Forms and Fermat's last theorem*, Springer, 1997.

[7] http ://calculis.net/grand-nombre-premier, 2012.

[8] Hagler Michael.*Courbes elliptiques et cryptographie*, mémoire, 19 février 2006.

[9] Yves Gerard.*Cryptographie et sécurité*, mémoire, université Lion 1, 09 février 2009.

[10] Thomas Baingnères.*Factorisation de grands nombres à l'aide de Courbes Elliptiques*, Projet de semestre, Ecole polytechnique. Fédération de Lausanne. Mars 2003.

[11] A. Shamir L. M. Adleman, R. L. Rivest. A method for obtaining digital signa-tures and public-key cryptosystems. Comm. ACM, 21(2) : 120-126, 1978.

[12] http ://www.apprendre-en-ligne. net/crypto/rsa/251088096.pdf.

[13] Arjen K. Lenstra. Massively parallel computing and factoring. LNCS 583, LATIN'92 proceedings, 1987.

[14] http ://iml. univ-mrs. fr/kohel/tch/M2-CryptoSymetrique/CM/RappelCorps-finis. pdf.

[15] Hasse, H : Number Theory-Springer(1980).

[16] Joseph H. Silverman. The arithmetic of elliptic curves. Springer, 2009.

[17] J. M. Pollard. Theorems on factorization and primality testing. Proc. Cambr. Philos. Soc. 76 :521-528, 1974.

[18] Hendrik W. Lenstra, Jr. Factoring integers with elliptic curves. Annals of Math. 126 :649-673, 1987.