N^0 d'ordre : 02 / 2013 – M / MT

REPUBLIQUE ALGÉRIENNE DEMOCRATIQUE ET POPULAIRE
MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEURE ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE DES SCIENCES ET DE LA TECHNOLOGIE
HOUARI BOUMEDIENE-ALGER
Faculté de Mathématiques

MÉMOIRE

Présenté pour l'obtention du diplôme de MAGISTER

En: MATHÉMATIQUES

Option : Algèbre et Théorie des Nombres

Par **Hafida LAIB**

Thème

Courbes Elliptiques et Applications

Soutenu publiquement , le 28/09/2013 devant le jury composé de :

Mr Farid BENCHERIF, Maître de Conférences /A à l'USTHB	Président
Mme.Leila BENFERHAT, Maître de Conférences /A à L'USTHB	Directrice de Mémoire
Mr Boualem BENSEBA, Maître de Conférences /A à L'USTHB	Examinateur
Mme Schehrazad SELMANE, Maître de Conférences /A à L'USTHB	Examinatrice
Mr Rachid BOUCHENNA , Maître Assistant /A à l'USTHB	Examinateur

Remerciements

Nous remercions tout d'abord et avant tout le tout puissant ALLAH qui nous a aidés à mener à terme ce travail.

Je tiens à remercier Mon Professeur et ma Directrice de mémoire, Madame Leila BENFERHAT, qui a accepté de diriger mon travail et de me suivre patiemment dans toutes les étapes de cette étude. Je lui suis reconnaissante de ses nombreuses remarques, sa gentillesse et sa patience.

Mes sincères remerciements vont à Monsieur Farid BENCHERIF pour m'avoir fait l'honneur de présider le jury et à Monsieur Boualem BENSEBA, Madame Schehrazad SELMANE et Monsieur Rachid BOUCHENNA d'avoir accepté d'examiner ce travail.

Je remercie également mes enseignants de la post-graduation.

Je remercie aussi l'ensemble de mes camarades de Magister, mes amis, ma famille qui m'ont soutenue durant ce travail.

J'adresse un remerciement particulier à mon époux pour son aide précieuse et ses encouragements.

Enfin merci à tous ceux qui m'ont aidée de près ou de loin.

Table des matières

Introduction **1**

1 Courbes elliptiques **4**
1.1 Espace projectif et point à l'infini 4
1.2 Courbes elliptiques sur un corps commutatif 6
1.2.1 Loi de groupe 10
1.2.2 Algorithme pour la multiplication 15
1.2.3 Points de torsion 16
1.3 Courbes elliptiques sur un corps fini 17
1.3.1 Rappels sur les corps finis 17
1.3.2 Caractérisation d'une courbe elliptique sur un corps fini 18
1.3.3 L'endomorphisme de Frobenius 18
1.4 Courbes elliptiques définies sur $\mathbb{Z}/n\mathbb{Z}$ 21

2 Dénombrement des points d'une courbe elliptique sur un corps fini **24**
2.1 Introduction 24
2.2 Rappels et définitions 25
2.3 L'algorithme de Schoof 27
2.4 Calcul dans le cas général 33
2.5 Complexité de l'algorithme de Schoof 34
2.6 Exemple 1 (Calcul de $\#E(\mathbb{F}_{19^9})$) 35
2.7 Exemple 2 (Calcul de $\#E(\mathbb{F}_{29^{2013}})$) 39

3 Factorisation et primalité avec les courbes elliptiques **45**
3.1 Introduction 45
3.2 Historique des tests de primalité 45
3.3 Test de primalité basé sur les courbes elliptiques 49
3.3.1 Critère de Pocklington 49
3.3.2 Le critère de Pocklington-Lehmer 50
3.3.3 Critère de Goldwasser-Kilian 51
3.4 Historique des méthodes de factorisation 54
3.5 Méthode de factorisation (ECM) 56
3.5.1 Méthode $(p-1)$ de Pollard 56
3.5.2 L'idée de la méthode des courbes elliptiques 58
3.5.3 Méthode de Lenstra (ECM) 58
3.5.4 Complexité de l'algorithme ECM 62

Conclusion **63**

A Applications sur le logiciel algébrique SAGE **66**
A.1 Introduction 66
A.2 Composants de Sage 66
A.3 Utilisation du logiciel Sage 67
A.3.1 Premiers graphiques 67
A.3.2 Aide en ligne 67
A.4 Manipulation des courbes elliptiques avec Sage 69
A.4.1 Définir une courbe elliptique sur Sage : 69
A.4.2 Calculer $\#E$ et kP sur Sage: 70
A.4.3 Le graphe des courbes elliptiques en 2D et 3D 70
A.5 Manipulation des polynômes sur Sage 71
A.5.1 Théorème des restes chinois sur Sage 71
A.5.2 Construction d'anneaux de polynômes 75
A.5.3 Polynômes et arithmétique euclidienne: 77
A.6 Calcul des exemples 2.6 et 2.7 de l'algorithme de Schoof 77

Liste des figures

1.1 Le point à l'infini O qui appartient à chaque droite verticale 6
1.2 Courbe elliptique qui coupe l'axe (OX) en un seul point 8
1.3 Courbe elliptique qui coupe l'axe (OX) en 3 points 9
1.4 Cubique avec un nœud 9
1.5 Cubique avec un point de rebroussement 10
1.6 Loi de groupe 13
1.7 Loi de groupe (1,0)+(0,2) 13
1.8 Courbe elliptique sur le corps fini Z/7Z 21
1.9 Courbe elliptique sur le corps fini Z/29Z 22
1.10 Courbe elliptique sur le corps fini Z/4999Z 22

3.1 Histoire des records de factorisation par GNFS 55
3.2 Histoire des records de factorisation par ECM 59

A.1 Graphe de la fonction f(x)=cos(2x^2) sur Sage 67
A.2 Surface paramétrée en 3D sur Sage 68
A.3 Utilisation de la touche de tabulation «tab» 68
A.4 Page de documentation de la fontion " EllipticCurve" 69
A.5 Définition des courbes elliptiques sur Sage 70
A.6 Calcul de kP et de l'ordre de E 71
A.7 Calcul des coordonnées de points d'une courbe elliptique sur Sage . . . 71
A.8 Courbe elliptique (FIG 2.2) en 2D sur Sage 72
A.9 Courbe elliptique (FIG 2.3) en 2D sur Sage 72
A.10 Courbe elliptique (FIG 1.2) en 3D sur Sage 73
A.11 Courbe elliptique (FIG 1.3) en 3D sur Sage 73
A.12 Courbe elliptique sur le corps fini Z/7Z sur Sage 74
A.13 Courbe elliptique sur le corps fini Z/29Z sur Sage 74
A.14 Courbe elliptique sur le corps fini Z/4999Z sur Sage 75
A.15 Théorème des restes chinois sur Sage 75
A.16 Polynômes et arithmétique Euclidienne sur Sage. 78
A.17 Calcul des ppcm et pgcd de 3 polynômes 79
A.18 Calculs de l'exemple 2.6 80
A.19 Calcul de l'ordre de la courbe E de l'exemple 2.7 et de ses points. . . 81
A.20 Calculs de l'exemple 2.7 (partie 1) 81
A.21 Calculs de l'exemple 2.7 (partie 2) 82

Liste des tableaux

1.1 Les formules explicites pour la loi de groupe sur une courbe elliptique 14

Résumé

Les courbes elliptiques ont de nombreuses applications dans différents domaines : en mécanique classique, en Théorie des Nombres et en cryptologie. En particulier, compter les points d'une courbe elliptique sur un corps fini et factoriser un entier sont très importants pour les méthodes de cryptage.

Dans ce mémoire nous présentons l'algorithme de Schoof, ainsi que sa démonstration détaillée et deux exemples d'application. Cet algorithme permet de dénombrer les points d'une courbe elliptique sur un corps fini.

Nous présentons également de façon détaillée les méthodes qui permettent d'étudier la primalité et la factorisation des grands nombres entiers en utilisant les courbes elliptiques. Notamment, l'algorithme de Goldwasser-Kilian basé sur le critère de Pocklington-Lehmer ainsi que la méthode de factorisation qui a été découverte par H. W. Lenstra. Des exemples explicites sont étudiés.

Tous les exemples ont été étudiés en utilisant le logiciel algébrique SAGE qui a pour ambition de devenir une alternative libre aux logiciels propriétaires comme Magma, Maple, Mathematica ou Matlab.

Introduction

Les courbes elliptiques constituent un sujet d'étude qui remonte au 19ème siècle. Ce sont par définition des cubiques sans singularité. Elles ont été introduites pour le calcul des intégrales des fonctions elliptiques sur $\mathbb{C}$ dans le cadre de l'Analyse Complexe.

Elles ont trouvé un regain d'intérêt considérable au 20ème siècle, en particulier pour leurs applications en Cryptographie.

Les courbes elliptiques utilisées en Cryptographie sont définies sur un corps fini. Une courbe elliptique définie sur un corps fini est un groupe fini et la connaissance de l'ordre de ce groupe est utile pour tester la primalité ou factoriser de très grands nombres.

Ces deux questions ont fasciné de nombreux mathématiciens à travers l'histoire, comme Eratosthène au 3ème siècle avant Jesus Christ, Mersenne et Fermat au 17ème siècle et, à partir du 18ème siècle, Euler, Legendre et Gauss.

Jusqu'aux 40 dernières années, beaucoup de travaux ont été développés pour répondre à ces questions. En particulier, l'invention du système de cryptage RSA (Rivest, Shamir, Adleman) en 1977 a poussé les mathématiciens à s'intéresser à la factorisation des grand nombres. Le système RSA se base sur la difficulté de factoriser de grands nombres et nécessite de grands nombres premiers pour fabriquer la clé publique. Par ailleurs, un des moyens pour décrypter un message codé avec le RSA sans connaître la clé publique est de savoir factoriser de grands nombres.

Pour trouver la décomposition en facteurs premiers d'un nombre donné, deux étapes peuvent être distinguées. Dans la première étape, on décide si le nombre est premier ou composé avec des *tests de primalité.* Les tests les plus connus sont le crible d'Eratosthène (250 av JC), le test de Fermat (1640), le critère de pocklington (1914), le test de Lucas-Lehmer (1930) pour les nombres de Mersenne, le test de Miller-Rabin (1980), le test de Solovay-Strassen (1977) et le test AKS (2002). Si le nombre est composé, on trouve un facteur non trivial, c'est le début de la deuxième étape qu'est la *factorisation.* La décomposition complète en facteurs premiers peut être obtenue en appliquant *un algorithme de factorisation.* Citons parmi ces algorithmes la méthode naïve des divisions successives (250 av JC), la méthode (p-1) de Pollard (1974), la méthode Rho de Pollard (1975), la méthode de Dixon (1981), le crible quadratique

(1981), l'algorithme (p+1) de William (1982) et le crible du corps de nombres (GNFS) (1988).

Les courbes elliptiques sont appliquées aussi bien aux tests de primalité qu'aux méthodes de factorisation et elles donnent lieu à des algorithmes avec une excellente performance en théorie et en pratique.

Dans ce mémoire, nous présentons l'algorithme de Schoof [15], qui permet de calculer le nombre de points d'une courbe elliptique sur un corps fini, le test de primalité de *Goldwasser-Kilian* (1986) [23], ainsi que la méthode de factorisation *ECM* (Elliptic Curve Method) de H.W.Lenstra (1985) [9].

En utilisant le test *Goldwasser-Kilian*, le record actuel est dû à *François Morain* [12] qui, en Avril 2011, a montré la primalité d'un nombre de 26642 chiffres décimaux qui est

$$60336838787923722145\ldots(26602\text{ autres chiffres})\ldots 97795227069490003443.$$

Ce mémoire est constitué de trois chapitres.

Dans le premier chapitre, nous rappelons quelques notions fondamentales de la théorie des courbes elliptiques. Ces courbes elliptiques sont définies aussi bien sur un corps commutatif, en particulier sur un corps fini, que sur l'anneau $\mathbb{Z}/n\mathbb{Z}$. Après avoir introduit la notion d'espace projectif, nous définissons une courbe elliptique dans l'espace projectif et dans l'espace affine ainsi qu'une loi qui lui confère une structure de groupe commutatif. Nous rappelons également les notions suivantes : points de torsion, endomorphisme de Frobenius, théorème de Hasse...etc, qui nous seront utiles pour les chapitres suivants.

Dans le second chapitre, nous présentons l'algorithme de Schoof [15] et sa démonstration détaillée, ainsi que deux exemples étudiés en utilisant le logiciel algébrique SAGE. Cet algorithme permet de calculer le nombre de points d'une courbe elliptique E sur un corps fini $\mathbb{F}_p$, où p est un nombre premier. La complexité de cet algorithme est $O(\log^8 p)$. Ensuite, nous montrons qu'il est facile de calculer l'ordre de $E(\mathbb{F}_q)$, où $q = p^n, n \in \mathbb{N}^*$, si nous connaissons l'ordre de $E(\mathbb{F}_p)$. Le calcul de $\#E(\mathbb{F}_q)$ est utile pour tester la primalité et factoriser de grands nombres par la méthode des courbes elliptiques ECM que nous verrons au chapitre trois.

Dans le troisième chapitre, nous présentons le test de primalité de Goldwasser-Kilian [23]. Ce test est basé sur le critère de Pocklington-Lehmer. Nous présentons également la méthode de factorisation ECM de H.W.Lenstra [9]. Cette méthode est un algorithme qui présente de grandes similitudes avec l'algorithme de factorisation $(p-1)$ de Pollard. C'est la meilleure méthode, connue à ce jour, qui permet d'extraire des facteurs premiers p de taille modérée, c'est-à-dire, $p < 10^{60}$, avec une complexité de $O(p) = e^{\sqrt{(2+o(1))\ln p \ln\ln p}}$. Elle est donc utilisé par les logiciels de calcul numérique

comme SAGE, Maple et Magma. Le record du plus grand facteur par la méthode ECM est :

$$2302872188505279576573535015926441913945044975483579529517513795897664211127797.$$

Il a été découvert par *Sam Wagstaff* le 12 Août 2012 [14]. C'est un facteur du nombre $11^{306} + 1$ à 79 chiffres.

En annexe, nous présentons le logiciel algébrique SAGE (*Software for Algebra and Geometry Experimentation*), qui est un logiciel de mathématiques qui rassemble de nombreux programmes et bibliothèques libres dans une interface commune basée sur le langage de programmation Python [17], [18], [19]. Il a pour ambition de devenir une alternative libre aux logiciels propriétaires comme Magma, Maple, Mathematica ou Matlab. Nous avons utilisé ce logiciel pour effectuer les calculs des exemples étudiés dans les chapitres deux et trois.

Chapitre 1

Courbes elliptiques

Dans ce chapitre, nous rappelons les notions fondamentales de la théorie des courbes elliptiques sur un corps commutatif et en particulier sur un corps fini et l'anneau $\mathbb{Z}/n\mathbb{Z}$ [7]. D'abord, nous introduisons l'espace projectif et le point à l'infini. Ensuite nous définissons une courbe elliptique dans l'espace projectif et dans l'espace affine ainsi qu'une loi qui lui donne une structure de groupe commutatif. Nous rappelons également les notions suivantes : points de torsion, endomorphisme de Frobenius, théorème de Hasse...etc, qui nous seront utiles pour les chapitres suivants.

Les références utilisées sont : L.C. Wachington [1] et P. Guillot [6].

1.1 Espace projectif et point à l'infini

Soit $\Bbbk$ un corps commutatif et n un entier, $n \geq 1$. On définit sur $\Bbbk^n - \{0\}$ une relation $\mathcal{R}$ par :

$$\forall (u, v) \in (\Bbbk^n - \{0\}) \times (\Bbbk^n - \{0\}) \quad u \mathcal{R} v \Longleftrightarrow \exists \lambda \in \Bbbk^* \ u = \lambda v.$$

On vérifie que $\mathcal{R}$ est une relation d'équivalence sur $\Bbbk^n - \{0\}$.

L'espace projectif $\mathbb{P}_{n-1}(\Bbbk)$ est par définition l'ensemble des classes d'équivalence

$$\frac{\Bbbk^n - \{0\}}{\mathcal{R}}$$

Si $n = 2$, l'espace projectif $\mathbb{P}_1(\Bbbk)$ s'appelle la droite projective sur $\Bbbk$.

Si $n = 3$, l'espace projectif $\mathbb{P}_2(\Bbbk)$ s'appelle le plan projectif sur $\Bbbk$.

Soit $u = (x_1, \ldots, x_{n-1}, x_n) \in \Bbbk^n - \{0\}$. La classe de u notée $(x_1 : \ldots : x_{n-1} : x_n)$, est la droite vectorielle passant par u. Elle est constituée de tous les vecteurs non nuls de $\Bbbk^n$ proportionnels à u.

Si $x_n \neq 0$, il existe un représentant de $(x_1 : \ldots : x_{n-1} : x_n)$ de la forme

$$(\frac{x_1}{x_n}, \cdots, \frac{x_{n-1}}{x_n}, 1).$$

Les points qui satisfont cette condition sont les points finis de l'espace projectif.

Si $x_n = 0$, alors les points de $\Bbbk^n$ de la forme

$$(x_1, \ldots, x_{n-1}, 0)$$

appartiennent tous au même hyperplan d'équation $x_n = 0$. Cet hyperplan est une réunion de classes d'équivalence dans l'espace projectif. Les points qui satisfont cette condition sont les points à l'infini. Ils constituent l'hyperplan projectif à l'infini.

L'espace projectif $\mathbb{P}_{n-1}(\Bbbk)$ peut ainsi être considéré comme étant la réunion de l'espace affine de dimension $n-1$ sur $\Bbbk$ et de l'hyperplan projectif à l'infini donc

La droit projective $\mathbb{P}_1(\Bbbk)$ est la réunion du corps $\Bbbk$ et du point à l'infini.

Le plan projectif $\mathbb{P}_2(\Bbbk)$ est la réunion de l'espace affine de dimension 2 et de la droite projective à l'infini D_O.

$$\mathbb{P}_2(\Bbbk) = \Bbbk^2 \cup D_O$$

Les coordonnées d'un point d'un espace projectif sont appelées coordonnées homogènes. Elles ne sont pas toutes nulles.

Définition 1 *Un polynôme est dit homogène de degré n s'il est la somme de termes de la forme $ax^iy^jz^k$ ou $a \in \Bbbk$ et $i+j+k = n$.*

Exemple 2 *$F(x,y,z) = x^3 + 3xyz + 2yz^2$ est un polynôme homogène de degré 3.*

Si F est un polynôme homogène de degré n alors $F(\lambda x, \lambda y, \lambda z) = \lambda^n F(x,y,z)$ pour tout $\lambda \in \Bbbk$. Il s'en suit que si $(x_1,y_1,z_1)\mathcal{R}(x_2,y_2,z_2)$ alors $F(x_1,y_1,z_1) = 0$ si et seulement si $F(x_2,y_2,z_2) = 0$.

Un zéro de F dans $\mathbb{P}_2(\Bbbk)$ ne dépend donc pas du choix du représentant de la classe d'équivalence. Ainsi, l'ensemble des zéros de F dans $\mathbb{P}_2(\Bbbk)$ est bien défini. Par contre, si F n'est pas homogène, nous ne pouvons pas parler d'un point de $\mathbb{P}_2(\Bbbk)$ lorsque $F(x,y,z) = 0$.

Exemple 3 *Si $F(x,y,z) = x^2 + 2y - 3z$ alors $F(1,1,1) = 0$ et $F(2,2,2) = 2$ bien que $(1:1:1) = (2:2:2)$.*

Pour contourner ce problème, nous travaillerons dans la suite avec des polynômes homogènes.

Si $f(x,y) \in \Bbbk[x,y]$, nous pouvons le rendre homogène en insérant des puissances de z.

Exemple 4 *Si $f(x,y) = y^2 - x^3 - Ax - B$, nous pouvons obtenir le polynôme homogène $F(x,y,z) = y^2z - x^3 - Axz^2 - Bz^3$.*
Si F est homogène de degré n alors, $F(x,y,z) = z^n f(\frac{x}{z}, \frac{y}{z})$ et $f(x,y) = F(x,y,1)$.

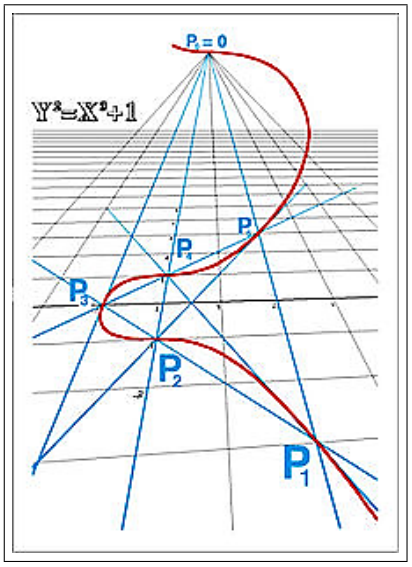


Figure 1.1: Le point à l'infini O qui appartient à chaque droite verticale

Regardons maintenant ce que cela signifie pour deux droites parallèles se rencontrant à l'infini.

Soient $y = mx + b_1$ et $y = mx + b_2$ deux droites parallèles avec $b_1 \neq b_2$.

Les formules homogènes sont : $y = mx + b_1 z, \quad y = mx + b_2 z$. En résolvant le système des deux équations, nous trouvons : $z = 0$ et $y = mx$. les deux droites ont donc pour intersection $(1 : m : 0)$ qui est un point infini de $\mathbb{P}_2(\mathbb{k})$. De même, deux droites verticales $x = c_1$ et $x = c_2$ ont pour intersection le point infini $(0 : 1 : 0)$, c'est le point noté O qui appartient à chaque droite verticale qui intersecte la courbe elliptique en ce point.(figure 1.1)

1.2 Courbes elliptiques sur un corps commutatif

La forme la plus générale d'un sous-ensemble du plan affine $\mathbb{k}^2$ défini par une équation polynomiale $f(x, y) = 0$ de degré 3 est :

$$\alpha_1 x^3 + \alpha_2 x^2 y + \alpha_3 x y^2 + \alpha_4 y^3 + \alpha_5 x^2 + \alpha_6 xy + \alpha_7 y^2 + \alpha_8 x + \alpha_9 y + \alpha_{10} = 0 \qquad (1.1)$$

$\alpha_i \in \mathbb{k}, i \in \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$

Pour que le polynôme soit de degré 3, il faudrait qu'au moins l'un des coefficients $\alpha_1, \alpha_2, \alpha_3$ ou α_4 soit non nul.

Il faut également que le polynôme $f(x, y)$ soit absolument irréductible, c.-à-d. qu'il est irréductible dans $\overline{\mathbb{k}}[x, y]$, ou $\overline{\mathbb{k}}$ désigne la clôture algébrique de $\mathbb{k}$, afin de ne pas se

ramener à des racines multiples sur un polynôme de degré inférieur.

Dans le plan projectif $\mathbb{P}_2(\Bbbk)$, l'équation homogène de (1.1) sera

$$\alpha_1 x^3+\alpha_2 x^2 y+\alpha_3 xy^2+\alpha_4 y^3+\alpha_5 x^2 z+\alpha_6 xyz+\alpha_7 y^2 z+\alpha_8 xz^2+\alpha_9 yz^2+\alpha_{10} z^3 = 0 \quad (1.2)$$

Les points du plan projectif solutions de l'équation (1.2) sont exactement les solutions de l'équation (1.1) qui sont solutions de (1.2) avec $z \neq 0$. Plus les points à l'infini de la courbe qui sont les solution de l'équation (1.2) avec $z = 0$.

Définition 5 *Une courbe donnée par l'équation* (1.2) *sur* $\Bbbk$ *est dite lisse si elle admet une tangente en chaque point, c.-à-d. si en tout point* (x, y, z) *de la courbe, l'application linéaire*

$$D_{xyz} : (dx, dy, dz) \mapsto f'_x(x, y, z)dx + f'_y(x, y, z)dy + f'_z(x, y, z)dz$$

est non nulle.

Par un choix judicieux des coordonnées, on peut simplifier l'équation (1.2) et se ramener à une forme dite de Weierstrass qui s'exprime en coordonnées affines.

Définition 6 *On appelle équation de Weierstrass sur* $\Bbbk$ *une équation du type*

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

où les coefficients a_1, a_2, a_3, a_4 *et* a_6 *sont dans* $\Bbbk$.

Définition 7 *Une courbe elliptique* E *définie sur* $\Bbbk$ *est une courbe lisse donnée par une équation de Weierstrass sur* $\Bbbk$ *à laquelle on rajoute un point à l'infini* O.

Proposition 8 *Si* $\Bbbk$ *est un corps de caractéristique différente de* 2 *ou* 3, *l'équation d'une courbe elliptique sur* $\Bbbk$ *peut s'écrire*

$$y^2 = x^3 + ax + b, \qquad a, b \in \Bbbk$$

avec la condition $4a^3 + 27b^2 \neq 0$.

Démonstration. *Comme la caractéristique du corps est différente de* 2, *éliminons les monômes en* y *et* xy *par le changement de variable linéaire*

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

Nous obtenons donc l'équation de Weierstrass

$$E_1 : y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6,$$

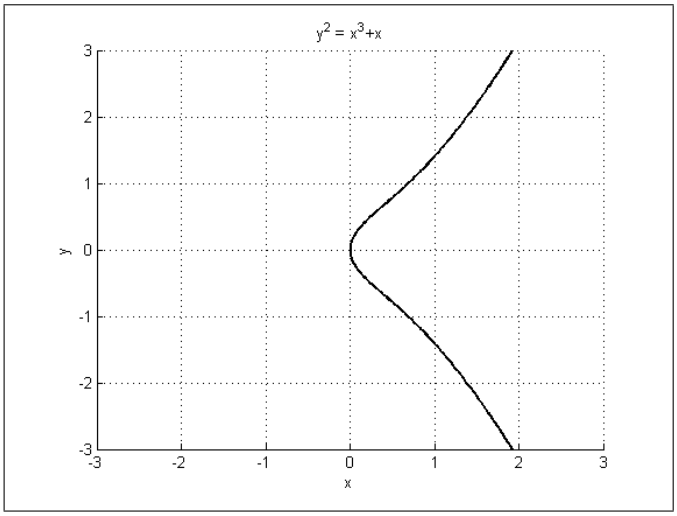


Figure 1.2: Courbe elliptique qui coupe l'axe (OX) en un seul point

où $b_2 = a_1^2 + 4a_2$, $b_4 = 2a_4 + a_1a_3$ *et* $b_6 = a_3^2 + 4a_6$. *Eliminons les monômes en* x^2 *et le coefficient* b_2, *lorsque le caractéristique de* $\mathbb{k}$ *est différente de* 2 *et* 3, *par le changement de variables*

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

On aura l'équation de Weierstrass

$$E_2 : y^2 = x^3 - 27c_4x - 54c_6,$$

où $c_4 = b_2^2 - 24b_4$ *et* $c_6 = -b^3 + 36b_2b_4 - 216b_6$.
Ainsi si le caractéristique de $\mathbb{k} \neq 2, 3$, *nous pouvons toujours travailler avec des courbes elliptiques de la forme*

$$E : y^2 = x^3 + Ax + B.$$

Dans ce cas la courbe est lisse si $4A^3 + 27B^2 \neq 0$. ■

Exemple 9 *Les figures* (1.2) *et* (1.3) *montrent l'aspect des courbes elliptiques définies sur le plan réel affine. Les cubiques dans les figures* (1.4) *et* (1.5) *ne sont pas des courbes elliptiques car* $4A^3 + 27B^2 = 0$. *Ces figures aident considérablement l'intuition pour comprendre les phénomènes sur les courbes elliptiques, mais n'ont de sens que dans le plan réel. Pour la factorisation et la primalité des grands nombres, le corps de base est un corps fini, et les représentations graphiques apportent peu à la compréhention (voir Figure 1.10)*

Nous allons dans tout ce qui suit, sauf mention contraire uniquement considérer des corps ayant une caractéristique différente de 2 ou 3 pour pouvoir écrire une courbe

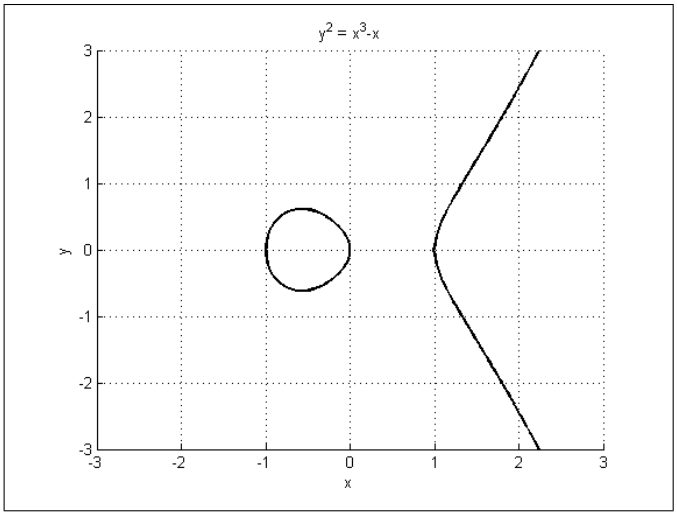


Figure 1.3: Courbe elliptique qui coupe l'axe (OX) en 3 points

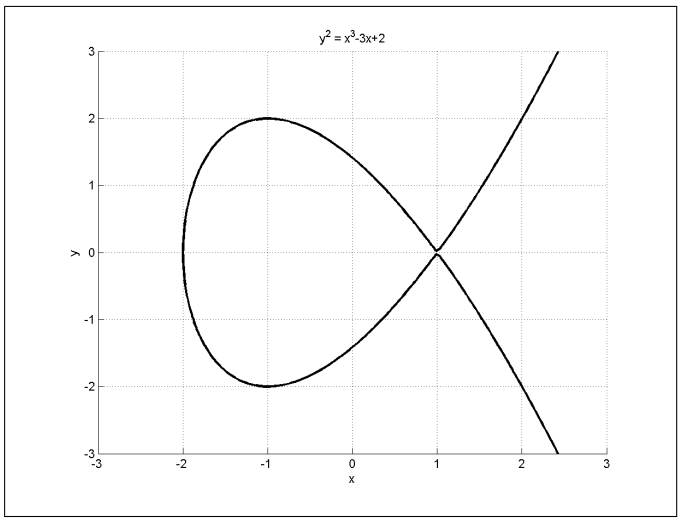


Figure 1.4: Cubique avec un nœud

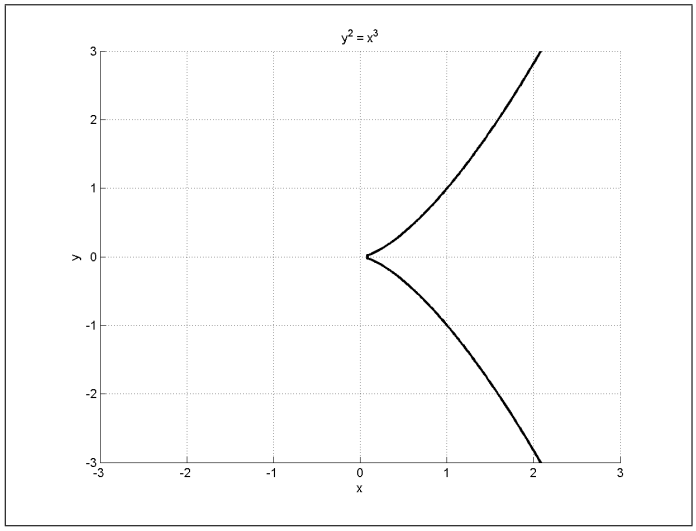


Figure 1.5: Cubique avec un point de rebroussement

elliptique sous la forme

$$E : y^2 = x^3 + Ax + B, \qquad A, B \in \Bbbk \text{ où } 4A^3 + 27B^2 \neq 0$$

1.2.1 Loi de groupe

L'ensemble des points $\Bbbk-$rationnels de E noté $E(\Bbbk)$ est :

$$E(\Bbbk) = \left\{(x, y) \in \Bbbk^2 |\ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\right\} \cup \{O\}$$

où O est le point à l'infini.

On définit une loi de groupe abélien $\oplus$ sur $E(\Bbbk)$ de la façon suivante :

• O est l'élément neutre i.e. $(x_1, y_1) \oplus O = O \oplus (x_1, y_1) = (x_1, y_1)$ pour tout $(x_1, y_1) \in E(\Bbbk)$.

• L'opposé de (x_1, y_1) est $\ominus(x_1, y_1) = (x_1, -y_1 - a_1x_1 - a_3)$.

• Soient P et Q deux points de $E(\Bbbk) - \{O\}$, la droite passant par P et Q "recoupe" la courbe E en un troisième point $R \in E(\Bbbk)$ qui est l'opposé de $P \oplus Q$ i.e. on a : $P \oplus Q = \ominus R$ (FIG 1.6). Si $P = Q$, on considère la droite tangente en P à la courbe E au lieu de la droite (PQ).

Le troisième point peut aussi s'énoncer de la façon suivante : la somme de 3 points alignés est nulle (en admettant que la loi est associative).

On peut obtenir des formules explicites pour l'addition de deux points.

Pour cela, soient $P = (x_1, y_1)$ et $Q = (x_2, y_2)$ deux points de $E(\Bbbk)$ avec $P \neq \ominus Q$ (sinon, on reconnait de suite que Q est l'opposé de P et on a $P \oplus Q = O$).

Supposons tout d'abord que $P \neq Q$. La droite passant par P et Q a pour équation $y = \lambda x + \mu$ avec

$$\lambda = \frac{y_1 - y_2}{x_1 - x_2} \quad \text{et} \quad \mu = y_1 - \lambda x_1$$

Remarquons que λ est bien défini car si $x_1 = x_2$ alors $P = Q$ ou $P = \ominus Q$, ce qui est exclu par hypothèse. L'intersection de la droite (PQ) avec la courbe E est donnée par :

$$(\lambda x + \mu)^2 + (a_1 x + a_3)(\lambda x + \mu) = x^3 + a_2 x^2 + a_4 x + a_6.$$

Ce qui donne l'équation suivante :

$$x^3 + (a_2 - \lambda^2 - a_1\lambda)x^2 + (a_4 - 2\lambda\mu - a_1\lambda - a_3\mu)x + (a_6 - \mu^2 - a_3\mu) = 0$$

On connait deux solutions de cette équation à savoir x_1 et x_2. Or la somme de trois racines est l'opposé du coefficient de degré 2 et on pose donc :

$$x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2 \quad \text{et} \quad \widetilde{y}_3 = \lambda x_3 + \mu$$

Le point $(x_3, \widetilde{y}_3)$ est le troisième point d'intersection cherché. On obtient alors :

$$\begin{aligned} P \oplus Q &= (x_3, y_3) = (\lambda^2 + a_1\lambda - a_2 - x_1 - x_2, -\lambda x_3 - \mu - a_1 x_3 - a_3) \\ &= (\lambda^2 + a_1\lambda - a_2 - x_1 - x_2, \lambda(x_1 - x_3) - y_1 - a_1 x_3 - a_3) \end{aligned}$$

Supposons maintenant que $P = Q = (x_1, y_1)$. La droite tangente à la courbe E au point P a pour équation $y = \lambda x + \mu$ avec :

$$\lambda = \frac{3x_1^2 + 2a_2 x_1 + a_4 - a_1 y_1}{2y_1 + a_1 x_1 + a_3} \quad \text{et } \mu = y_1 - \lambda x_1$$

Remarquons que λ est bien défini car si $2y_1 + a_1 x_1 + a_3 = 0$ alors $P = \ominus P$, ce qui est exclu par hypothèse. L'intersection de la droite avec la courbe E est donnée par :

$$(\lambda x + \mu)^2 + (a_1 x + a_3)(\lambda x + \mu) = x^3 + a_2 x^2 + a_4 x + a_6.$$

Ce qui donne l'équation suivante :

$$x^3 + (a_2 - \lambda^2 - a_1\lambda)x^2 + (a_4 - 2\lambda\mu - a_1\lambda - a_3\mu)x + (a_6 - \mu^2 - a_3\mu) = 0.$$

On connait une racine double (à savoir x_1) de cette équation, on en déduit la dernière solution et on pose :

$$x_3 = \lambda^2 + a_1\lambda - a_2 - 2x_1 \quad \text{et} \quad \widetilde{y}_3 = \lambda x_3 + \mu.$$

Le point $(x_3, \widetilde{y}_3)$ est le troisième point d'intersection cherché et on obtient :

$$\begin{aligned} P \oplus P = (x_3, y_3) &= (\lambda^2 + a_1\lambda - a_2 - 2x_1, -\lambda x_3 - \mu - a_1 x_3 - a_3) \\ &= (\lambda^2 + a_1\lambda - a_2 - 2x_1, \lambda(x_1 - x_3) - y_1 - a_1 x_3 - a_3) \end{aligned}$$

Proposition 10 *Soient $P = (x_1, y_1)$ et $Q = (x_2, y_2)$ deux points de E. On définit sur E la loi " $\oplus$ " comme suit :*

- $\ominus P = (x_1, -y_1 - a_1x_1 - a_3)$.
- $P \oplus Q = (x_3, y_3)$ *avec* $x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2$, $y_3 = \lambda(x_1 - x_3) - y_1 - a_1x_3 - a_3$ *et*

$$\lambda = \left\{ \begin{array}{ll} \frac{y_1 - y_2}{x_1 - x_2} & si \quad P \neq Q, \ominus Q \\ \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3} & si \quad P = Q \end{array} \right\}$$

Si $P = Q$ et $2y_1 + a_1x_1 + a_3 = 0$ alors $P \oplus Q = P \oplus P = O$.

Théorème 11 *Soit E une courbe elliptique définie sur k alors $(E(k), \oplus)$ est un groupe abélien de neutre O. En particulier, on a $(P \oplus Q) \oplus R = P \oplus (Q \oplus R)$.*

Démonstration. *La commutativité est évidente, il suffit alors seulement de vérifier par un calcul (long et fastidieux mais que l'on peut faire avec un logiciel de calcul formel) que la loi est associative.* ■

Dans toute la suite, la loi $\oplus$ sera noté $+$ (et donc, $\ominus$ sera noté $-$).

Exemple 12 *Sur le corps $\Bbbk = \mathbb{F}_{2011}$, on définit*

$$E : y^2 + xy + 3y = x^3 + 2x^2 + 4x + 5$$

On prend $P = (1, 2) \in E(\mathbb{F}_{2011})$ et $Q = (2, 470) \in E(\mathbb{F}_{2011})$.
On a $2P = P + P = (1161, 1551)$, $P + Q = (288, 128)$. De plus, on peut vérifier, en utilisant l'algorithme 15 de multiplication, que l'on a $723P = Q$.

Exemple 13 *Nous donnons un exemple pour illustrer la somme de deux point pour une courbe sur $\mathbb{R}$ (voir figure 1.6).*

Exemple 14 *On a la courbe elliptique $E(\mathbb{R}) : y^2 = x^3 - 5x + 4$ et les points $P_1(1, 0), P_2(0, 2)$*
On calcule $P_3(x_3, y_3)$
$\lambda = \frac{y_2 - y_1}{x_2 - x_1} = \frac{2-0}{0-1} = -2$
$x_3 = \lambda^2 - x_1 - x_2 = 3 \quad et \quad y_3 = \lambda(x_1 - x_3) - y_1 = 4 \quad$ *(voir figure 1.7)*

Nous allons maintenant donner dans le tableaux (1.1) les formules explicites pour la loi de groupe pour une courbe elliptique $E : y^2 = x^3 + Ax + B$, sur $\mathbb{R}$, pour expliquer visuellement la loi de groupe associée. Soient $P_1(x_1, y_1), P_2(x_2, y_2)$ des points de E avec $P_1, P_2 \neq O$. Le symétrique de $P(x, y)$ est $P(x, -y)$ et $P_1 + P_2 = P_3(x_3, y_3)$. De plus on a $P + O = P$ pour tout P sur E.

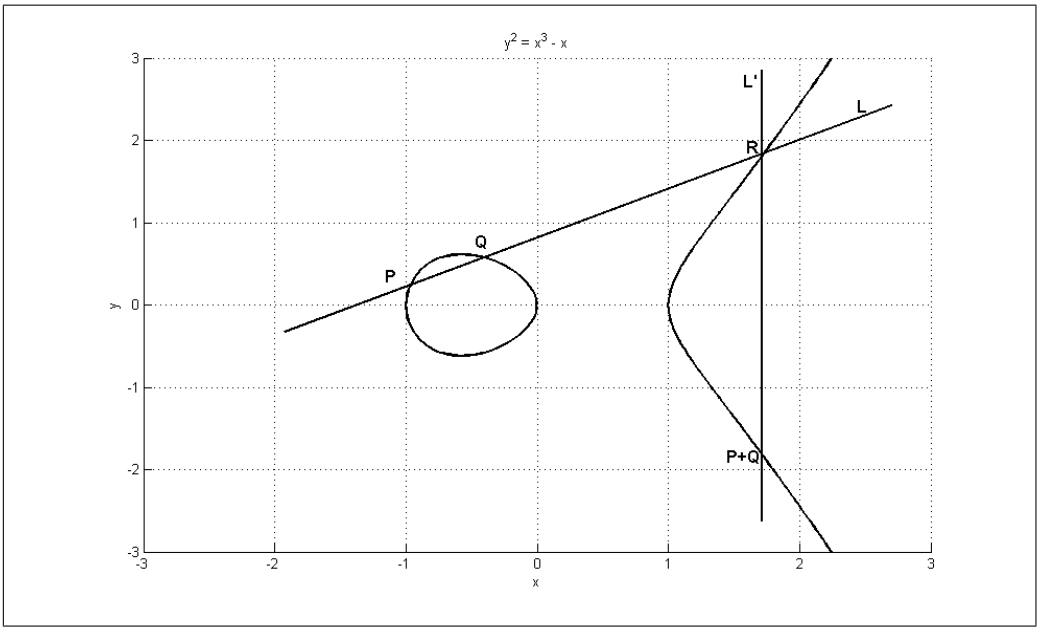


Figure 1.6: Loi de groupe

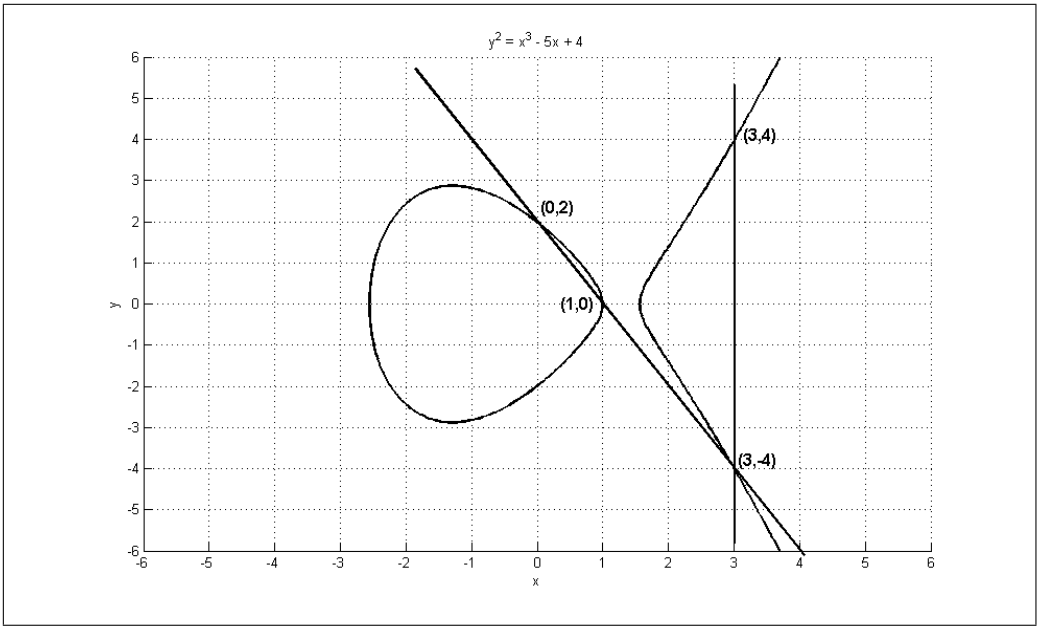


Figure 1.7: Loi de groupe (1,0)+(0,2)

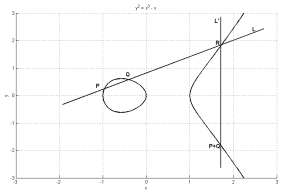
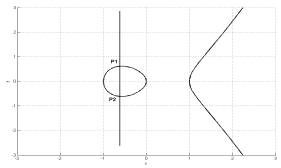
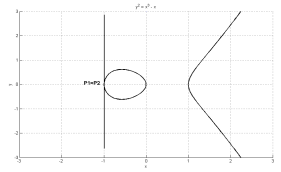
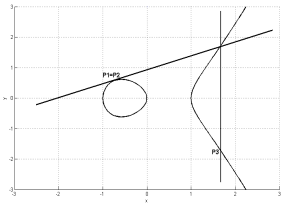
Condition	$P_3(x_3, y_3)$	Figure
$x_1 \neq x_2$	$x_3 = \lambda^2 - x_1 - x_2$ $y_3 = \lambda(x_1 - x_3) - y_1$ $avec \quad \lambda = \frac{y_2 - y_1}{x_2 - x_1}$	
$x_1 = x_2$	O (point à l'infini)	
$P_1 = P_2$ et $y_1 = 0$	O (point à l'infini)	
$P_1 = P_2$ et $y_1 \neq 0$	$x_3 = \lambda^2 - 2x_1$ $y_3 = \lambda(x_1 - x_3) - y_1$ $avec \quad \lambda = \frac{3x_1^2 + A}{2y_1}$	

Table 1.1: Les formules explicites pour la loi de groupe sur une courbe elliptique

1.2.2 Algorithme pour la multiplication

L'addition des points permet de définir pour tout entier n et tout point P de E, les multiples du point P :

$$nP = \underbrace{P + \cdots + P}_{n\ fois}$$

Cette opération est définie par récurrence par $0P = O$ et pour tout n entier naturel$(n+1)P = nP + P$. Elle est la plus chère "en terme de calcul" des protocoles basés sur les courbes elliptiques comme la factorisation et la primalité [11]. Pour réduire le temps de calcul, on peut utiliser des algorithmes très connus d'exponentiation pour le calcul de kP pour un k grand. On peut également améliorer le calcul pour un k petit.

Pour calculer kP où k est un entier et P un point, une méthode naïve consisterait à calculer $2P, 3P, \ldots, kP$ avec $k-1$ additions. Il est possible de réduire ce nombre en utilisant la méthode binaire.

L'idée principale est que si $k = (k_n, k_{n-1}, \ldots, k_1, k_0)_2$ est l'´écriture en base 2 de k alors

$$kP = \sum_{i=0}^{n} k_i(2^i P).$$

Cette méthode permet de calculer kP avec $O(ln\ n)$ opérations au lieu de $O(n)$ pour l'addition naïve.

Ainsi, à titre d'exemple, 11P s'écrit

$$11P = P + 2(P + 2(2P)) = 2^0P + 2^1P + 2^3P$$

l'´écriture en base 2 du nombre 11 est

$$11 = (1011)_2$$

en utilisant 5 additions au lieu de 10.

Algorithme 15 .

1. *Entrer* $k = (k_{t-1}, \ldots, k_1, k_0)_2$ *et point* $P \in E(\mathbb{F}_q)$
2. *Mettre* $Q = O$
3. *Pour* i *de* $t-1$ *à* 0 *faire*

   a) $Q = 2Q$

   b) *Si* $k_i = 1$ *alors* $Q = Q + P$

c) *Retourner* $Q = kP \in E(\mathbb{F}_q)$

Cet algorithme est le plus simple que l'on peut trouver pour calculer kP sans effectuer k additions.

1.2.3 Points de torsion

Définition 16 *Soit E une courbe elliptique définie sur un corps commutatif $\Bbbk$ et n un entier, $n \in \mathbb{Z}$. L'ensemble des points de $n-$torsion, noté $E[n]$, est l'ensemble des points $P \in E(\overline{\Bbbk})$ qui s'annulent par multiplication par n.*

$$E[n] = \{P \in E(\overline{\Bbbk}) \mid nP = O\}$$

Remarque 17 *On vérifie que $E[n]$ est un sous-groupe de $E(\overline{\Bbbk})$.*

Exemple 18 *Soit la courbe elliptique*

$$E(\mathbb{R}) : y^2 = x^3 + Ax + B,$$

$A, B \in \mathbb{R}$ et $4A^3 + 27B^2 \neq 0$.
$E[2]$ est le groupe des points de $2-$torsion, c.-à-d. des points P tels que $P + P = O$. Les points finis de $2-$torsion sont les points spéciaux de E

$$E[2] = \{O, P_1, P_2, P_3\},$$

avec $P_1 = (x_1, 0)$, $P_2 = (x_2, 0)$, $P_3 = (x_3, 0)$ et x_1, x_2,x_3 sont les trois racines distinctes du trinôme $x^3 + Ax + B$.

Théorème 19 *Tout groupe commutatif fini est isomorphe à un produit direct fini*

$$\frac{\mathbb{Z}}{n_1\mathbb{Z}} \times \frac{\mathbb{Z}}{n_2\mathbb{Z}} \times \cdots \times \frac{\mathbb{Z}}{n_k\mathbb{Z}},$$

où, pour tout $i \in \{1, \ldots, k-1\}$, n_i divise n_{i+1}.

Proposition 20 *Soit E une courbe elliptique définie sur un corps commutatif $\Bbbk$. Si la caractéristique de $\Bbbk$ ne divise pas n, alors*

$$E[n] \simeq \frac{\mathbb{Z}}{n\mathbb{Z}} \times \frac{\mathbb{Z}}{n\mathbb{Z}}$$

Démonstration. *D'après le théorème 19, on sait déjà que*

$$E[n] \simeq \frac{\mathbb{Z}}{n_1\mathbb{Z}} \times \frac{\mathbb{Z}}{n_2\mathbb{Z}} \times \cdots \times \frac{\mathbb{Z}}{n_k\mathbb{Z}} \qquad \text{avec} \qquad n_i | n_{i+1}.$$

Soit l un entier premier qui divise n_1. Il divise donc également tous les autres n_i. Il y a donc au moins l^k éléments de $E[n]$ qui sont d'ordre l. Comme $E[l]$ contient l^2 éléments; nécessairement; $k = 2$.Donc

$$E[n] \simeq \frac{\mathbb{Z}}{n_1\mathbb{Z}} \times \frac{\mathbb{Z}}{n_2\mathbb{Z}} \quad avec \quad n_1 | n_2$$

L'ordre maximal d'un élément de $E[n]$ est donc n_2. Comme pour tout point P de $E[n]$, on a $nP = O$. Cela implique que n_2 divise n. Comme d'autre part le produit $n_1 n_2$ vaut n^2, on a $n_1 = n_2 = n$. ■

Remarque 21 *Il existe donc une base de $E[n]$, constituée de deux points P_1 et P_2 de $E[n]$, chacun engendrant un groupe isomorphe à $\mathbb{Z}/n\mathbb{Z}$, donc d'ordre n et tel que tout point P de $E[n]$ se décompose:*

$$P = aP_1 + bP_2 \quad avec \quad a, b \in \mathbb{Z}/n\mathbb{Z}$$

1.3 Courbes elliptiques sur un corps fini

Dans ce paragraphe, nous donnons quelques rappels sur les corps finis ainsi que sur les courbes elliptiques définies sur un corps fini. Nous définissons également l'endomorphisme de Frobenius et donnons quelques propriétés de celui-ci.

1.3.1 Rappels sur les corps finis

Théorème 22 *Soit $\mathbb{F}_q$ un corps fini à q éléments. Alors:*

1. *$q = p^m$, où p est un nombre premier.*
2. *$\mathbb{F}_q$ contient le sous corps $\mathbb{F}_p$.*
3. *$\mathbb{F}_q$ est un espace vectoriel sur $\mathbb{F}_p$ de dimension m.*
4. *$p\alpha = 0$, $\forall \alpha \in \mathbb{F}_q$*
5. *$\mathbb{F}_q$ est unique à isomorphisme près.*

Théorème 23 *Soit $\mathbb{F}_q$ un corps fini a $q = p^n$ éléments. Les éléments de $\mathbb{F}_q$ sont les racines du polynôme $X^q - X$.*

Démonstration. Soit $\alpha \in \mathbb{F}_q$.
Si $\alpha = 0$ alors, il est racine de $X^q - X$.
Si $\alpha \neq 0$ alors $\alpha \in \mathbb{F}_q^*$(groupe multiplicatif)
Donc $\alpha^{q-1} = 1$ car $\left|\mathbb{F}_q^*\right| = q - 1$
Alors $\alpha^q - \alpha = 0$ implique que α est racine de $X^q - X$. ■

Proposition 24 *Soit $f(x) \in \mathbb{F}_p[x]$ un polynôme irréductible de degré m. Alors $\mathbb{F}_p[x]/(f(x))$ est un corps fini à p^m éléments.*

Théorème 25 *Pour tout nombre premier p et tout entier positif m, il existe un corps fini, unique à isomorphisme près, à $q = p^m$ éléments*

1.3.2 Caractérisation d'une courbe elliptique sur un corps fini

Théorème 26 (Cassel, 1966) *Soit E une courbe elliptique définie sur un corps fini $\mathbb{F}_q$. Alors*

1. *Soit E est un groupe cyclique;*
2. *Soit E est isomorphe à un produit direct $\dfrac{\mathbb{Z}}{n_1\mathbb{Z}} \times \dfrac{\mathbb{Z}}{n_2\mathbb{Z}}$ avec n_1 et n_2 des entiers tels que $n_1 | n_2$.*

Démonstration. Le groupe $(E, +)$ est fini et abélien, donc isomorphe à un produit direct des groupes cycliques $\frac{\mathbb{Z}}{n_1\mathbb{Z}} \times \frac{\mathbb{Z}}{n_2\mathbb{Z}} \times \cdots \times \frac{\mathbb{Z}}{n_k\mathbb{Z}}$ (théorème 19), où n_i divise n_{i+1}. Puisque, pour chaque i, le groupe $\frac{\mathbb{Z}}{n_i\mathbb{Z}}$ a n_1 éléments d'ordre divisant n_1, donc $E(\mathbb{F}_q)$ a n_1^k éléments d'ordre divisant n_1.Or par le théorème 20, nous savons qu'il existe au plus n_1^2 points d'ordre divisant n_1. Ainsi les seuls cas possibles sont $k = 1$ et $k = 2$. ■

Théorème 27 (Hasse) *Soit E une courbe elliptique définie sur $\mathbb{F}_q$. Alors*

$$|q + 1 - \#E(\mathbb{F}_q)| \leq 2\sqrt{q},$$

où $\#E(\mathbb{F}_q)$ désigne l'ordre de $E(\mathbb{F}_q)$.

1.3.3 L'endomorphisme de Frobenius

Définition 28 *Soit E une courbe elliptique sur un corps commutatif $\mathbb{k}$.*
Un endomorphisme de E est un homomorphisme

$$\alpha : E(\overline{\mathbb{k}}) \to E(\overline{\mathbb{k}})$$

tel que

$$\alpha(x, y) = (R_1(x, y), R_2(x, y)) \quad \forall (x, y) \in E(\overline{\mathbb{k}})$$

où R_1 et R_2 sont des fonctions rationnelles du corps de fonctions rationnelles de l'anneau quotient

$$\Bbbk[E] = \frac{\Bbbk[x,y]}{(y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6)}$$

où $(y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6)$ est l'idéal engendré par $y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6$.

L'endomorphisme trivial qui associe à tout point (x, y) le point à l'infini O est noté 0.

Définition 29 *Soit $\mathbb{F}_q$ un corps fini et $\overline{\mathbb{F}}_q$ sa clôture algébrique. On définit l'endomorphisme de Frobenius sur $\overline{\mathbb{F}}_q$ par :*

$$\begin{array}{rccc} \varphi_q : & \overline{\mathbb{F}}_q & \longrightarrow & \overline{\mathbb{F}}_q \\ & x & \longmapsto & x^q \end{array}$$

On peut étendre cette définition à $E(\overline{\mathbb{F}}_q)$:

$$\begin{array}{rccc} \phi_q : & E(\overline{\mathbb{F}}_q) & \longrightarrow & E(\overline{\mathbb{F}}_q) \\ & (x,y) & \longmapsto & (x^q, y^q) \\ & O & \longmapsto & O \end{array}$$

Lemme 30 *Soit E une courbe elliptique définie sur $\mathbb{F}_q$ et soit $(x, y) \in E(\overline{\mathbb{F}}_q)$*

1. $\phi_q(x, y) \in E(\overline{\mathbb{F}}_q)$.
2. $(x, y) \in E(\mathbb{F}_q)$ si et seulement si $\phi_q(x, y) = (x, y)$.
3. ϕ_q est un endomorphisme.

Démonstration. Soit $\mathbb{F}_q$ un corps fini de caractéristique p où p est un nombre premier. Nous avons $(a + b)^q = a^q + b^q$ pour $a, b \in \overline{\mathbb{F}}_q$. De plus $a^q = a$ pour tout $a \in \mathbb{F}_q$. Soit

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

Une courbe elliptique définie sur $\mathbb{F}_q$ (avec $a_i \in \mathbb{F}_q$). Si nous élevons les deux membres de cette équation à la puissance q, d'après ce qui précède, nous obtenons :

$$(y^q)^2 + a_1x^qy^q + a_3y^q = (x^q)^3 + a_2(x^q)^2 + a_4x^q + a_6.$$

Ce qui veut dire que $(x^q, y^q) \in E(\overline{\mathbb{F}}_q)$, d'où 1.

Pour prouver le point 2, il faut rappeler que $x \in \mathbb{F}_q$ si et seulement si $\varphi_q(x) = x$.

Ainsi :

$$\begin{aligned}(x,y) \in E(\mathbb{F}_q) &\iff x, y \in \mathbb{F}_q \\ &\iff \varphi_q(x) = x \text{ et } \varphi_q(y) = y \\ &\iff \phi_q(x,y) = (x,y).\end{aligned}$$

Pour la preuve du point 3, nous considérons la forme de Weierstrass courte $y^2 = x^3 + Ax + B$. On le démontre de la même manière avec la forme de Weierstrass longue.

Puisque ϕ_q est donnée par des fonctions rationnelles de degré q, il reste à démontrer que :

$$\phi_q : E(\overline{\mathbb{F}}_q) \longrightarrow E(\overline{\mathbb{F}}_q) \qquad \text{est un homomorphisme.}$$

Soit $(x_1, y_1), (x_2, y_2) \in E(\overline{\mathbb{F}}_q)$ avec $x_1 \neq x_2$ la somme est (x_3, y_3) avec

$$\begin{aligned} x_3 &= \lambda^2 - x_1 - x_2 \\ y_3 &= \lambda(x_1 - x_3) - y_1 \end{aligned} \quad \text{où} \quad \lambda = \frac{y_2 - y_1}{x_2 - x_1}.$$

En élevant tout à la puissance q-ième, on obtient

$$\begin{aligned} x_3^q &= \lambda'^2 - x_1^q - x_2^q \\ y_3^q &= \lambda'(x_1^q - x_3^q) - y_1^q \end{aligned} \quad \text{où} \quad \lambda' = \frac{y_2^q - y_1^q}{x_2^q - x_1^q}$$

Ceci signifie que

$$\phi_q(x_3, y_3) = \phi_q(x_1, y_1) + \phi_q(x_2, y_2)$$

Les cas où $x_1 = x_2$ ou lorsque l'un des points est O sont faits de manière similaire.

On a $2(x_1, y_1) = (x_3, y_3)$ avec

$$\begin{aligned} x_3 &= \lambda^2 - 2x_1 \\ y_3 &= \lambda(x_1 - x_3) - y_1 \end{aligned} \quad \text{où} \quad \lambda = \frac{3x_1^2 + A}{2y_1}$$

Lorsque nous élevons à la puissance q, nous obtenons:

$$\begin{aligned} x_3^q &= \lambda'^2 - 2x_1^q \\ y_3^q &= \lambda'(x_1^q - x_3^q) - y_1^q \end{aligned} \quad \text{où} \quad \lambda' = \frac{3^q (x_1^q)^2 + A^q}{2^q y_1^q}$$

Puisque $2, 3, A \in \mathbb{F}_q$, nous avons $2^q = 2, 3^q = 3, A^q = A$

Cela signifie que $\phi_q(x_3, y_3) = 2\phi_q(x_1, y_1)$. ■

Théorème 31 *Soit E une courbe elliptique définie sur $\mathbb{F}_q$.*

Posons $a = q + 1 - \#E(\mathbb{F}_q)$ alors

$$\phi_q^2 - a\phi_q + q = 0$$

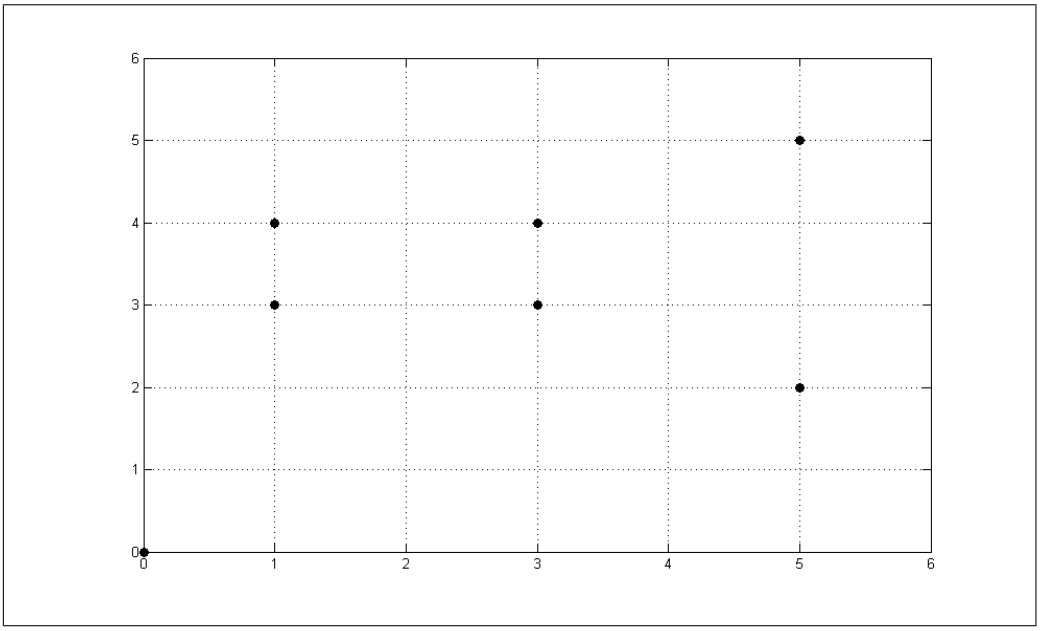


Figure 1.8: Courbe elliptique sur le corps fini Z/7Z

En tant qu'endomorphisme de $E(\mathbb{F}_q)$. Autrement dit, nous avons

$$(x^{q^2}, y^{q^2}) - a(x^q, y^q) + q(x, y) = O$$

Pour tout $(x, y) \in E(\overline{\mathbb{F}}_q)$. De plus, a est l'unique entier k tel que $\phi_q^2 - k\phi_q + q = 0$.

Démonstration. Voir [1] pages $101 - 102$. ■

Exemple 32 *Nous allons présenter la courbe elliptique $y^2 = x^3 + x$ sur les corps finis $\mathbb{Z}/7\mathbb{Z}$(FIG 1.8), $\mathbb{Z}/29\mathbb{Z}$ (FIG 1.9) et $\mathbb{Z}/4999\mathbb{Z}$ (FIG 1.10).*

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

Dans cette partie, nous allons définir la notion de courbe elliptique sur $\mathbb{Z}/n\mathbb{Z}$, où n est un entier positif tel que $\text{pgcd}(n, 6) = 1$.

Définition 33 *Une courbe elliptique E définie sur $\mathbb{Z}/n\mathbb{Z}$ est donnée par une équation de Weierstrass courte*

$$E : y^2 = x^3 + Ax + B,$$

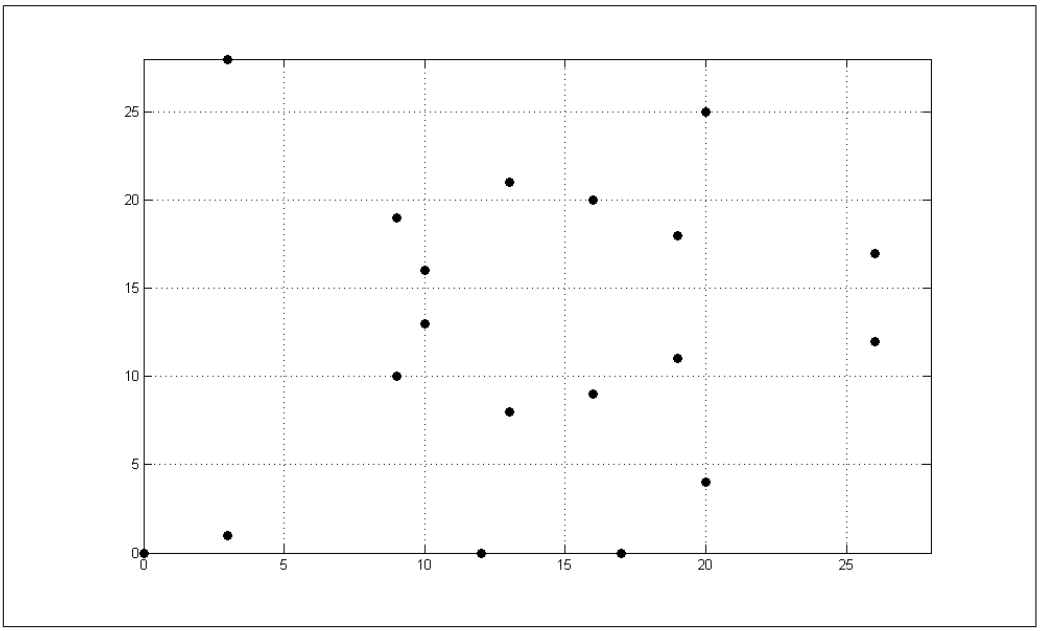


Figure 1.9: Courbe elliptique sur le corps fini Z/29Z

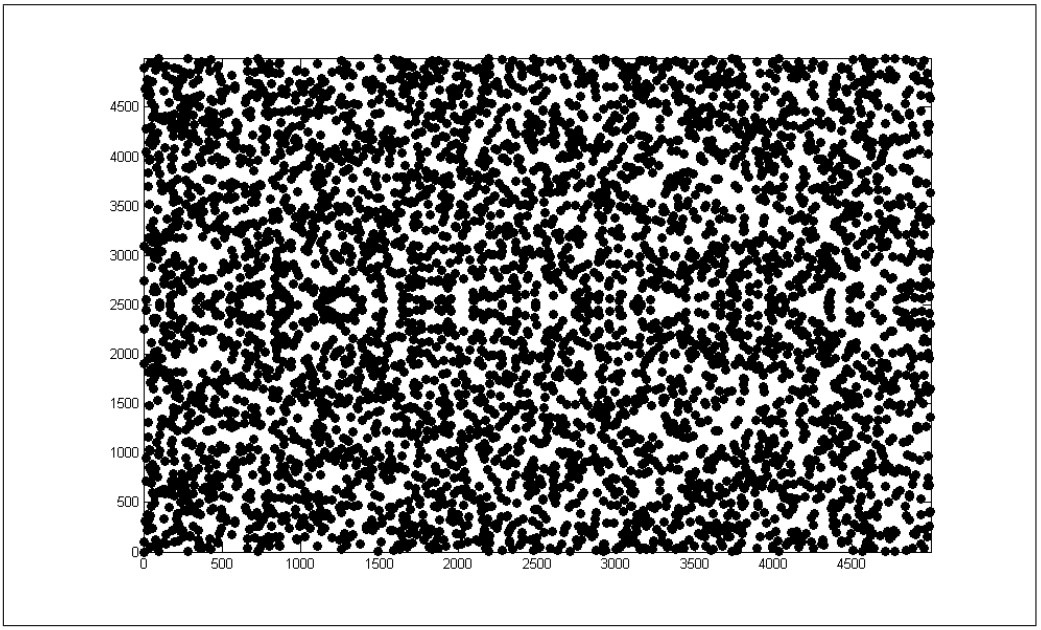


Figure 1.10: Courbe elliptique sur le corps fini Z/4999Z

où A, $B \in \mathbb{Z}/n\mathbb{Z}$ et $\Delta(E) = 4A^3 + 27B^2$ est premier avec n.
L'ensemble des points de la courbe E, noté $E(\mathbb{Z}/n\mathbb{Z})$, est défini par

$$E(\mathbb{Z}/n\mathbb{Z}) = \left\{(x_1, y_1) \in (\mathbb{Z}/n\mathbb{Z})^2,\ y_1^2 = x_1^3 + Ax_1 + B\right\} \cup \{O\}$$

Le point O est le point à l'infini.

On peut définir une opération " + "partielle sur $E(\mathbb{Z}/n\mathbb{Z})$: si $P = (x_1, y_1)$ et $Q = (x_2, y_2)$ sont deux points de $E(\mathbb{Z}/n\mathbb{Z}) - \{O\}$, on pose :

- $P + O = O + P$.
- Si $x_1 = x_2$ et $y_1 \neq y_2$ alors $P + Q = O$.
- Si $x_1 \neq x_2$ et si $L = x_2 - x_1$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ alors $P + Q = (x_3, y_3)$ avec $x_3 = \lambda^2 - x_1 - x_2$, $y_3 = -y_1 + \lambda(x_1 - x_3)$ et $\lambda = (y_2 - y_1)L^{-1}$.
- Si $P = Q$ et si $L = 2y_1$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ alors $P + Q = 2P = (x_3, y_3)$ avec

  $x_3 = \lambda^2 - 2x_1$, $y_3 = -y_1 + \lambda(x_1 - x_3)$ et $\lambda = (3x_1^2 + a)L^{-1}$.
- Si $P = Q = (x_1, 0)$ alors $P + Q = P + P = O$.

La loi que nous venons de définir n'est pas une une loi de groupe (sauf si n est premier).

Chapitre 2

Dénombrement des points d'une courbe elliptique sur un corps fini

2.1 Introduction

Dans ce chapitre, nous présentons l'algorithme de Schoof [15] et sa démonstration détaillée [1], ainsi que deux exemples étudiés en utilisant le logiciel algébrique SAGE. Cet algorithme permet de calculer le nombre de points d'une courbe elliptique E sur un corps fini $\mathbb{F}_p$, où p est un nombre premier. La complexité de cet algorithme est $O(\log^8 p)$. Ensuite, nous montrons qu'il est facile de calculer l'ordre de $E(\mathbb{F}_q)$, où $q = p^n, n \in \mathbb{N}^*$, si nous connaissons l'ordre de $E(\mathbb{F}_p)$. Le calcul de $\#E(\mathbb{F}_q)$ est utile pour tester la primalité et factoriser de grands nombres par la méthode des courbes elliptiques ECM que nous verrons au chapitre trois.

Nous allons, dans tout ce chapitre, considérer des courbes elliptiques sur $\mathbb{F}_q$ sous la forme

$$E : y^2 = x^3 + Ax + B \quad \text{avec} \quad A, B \in \mathbb{F}_q \text{ et } 4A^3 + 27B^2 \neq 0.$$

2.2 Rappels et définitions

Théorème 34 (des restes chinois) *Soit $m_1, m_2, ..., m_r$ une suite d'entiers positifs premiers entre eux deux à deux. Alors le système de congruence*

$$\begin{aligned} x &\equiv a_1 (\mathrm{mod}\, m_1) \\ x &\equiv a_2 (\mathrm{mod}\, m_2) \\ &... \\ x &\equiv a_r (\mathrm{mod}\, m_r) \end{aligned}$$

a une solution unique x modulo $M = m_1 \times m_2 \times ... \times m_r$,

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + ... + a_r M_r y_r$$

avec $M_i = \dfrac{M}{m_i}$, $y_i M_i \equiv 1 (\mathrm{mod}\, m_i)$.

Définition 35 (Polynômes de division) *Soient A et B des variables. Les polynômes de division $\psi_l \in \mathbb{Z}[x, y, A, B]$ sont définis ainsi*

$$\begin{aligned} \psi_0 &= 0 \\ \psi_1 &= 1 \\ \psi_2 &= 2y \\ \psi_3 &= 3x^4 + 6Ax^2 + 12Bx - A^2 \\ \psi_4 &= 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3 \\ &... \\ \psi_{2m} &= (2y)^{-1}(\psi_m)(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2) \text{ pour } m \geq 3 \\ \psi_{2m+1} &= \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3 \text{ pour } m \geq 2 \end{aligned}$$

Définition 36 *Si n est impair alors ψ_n est un polynôme de $\mathbb{Z}[x, y^2, A, B]$. Si n est pair, alors ψ_n est dans $2y\mathbb{Z}[x, y^2, A, B]$.*

Démonstration. La preuve se fait par récurrence. La propriété est vraie pour $n \leq 4$. Supposons qu'elle est vraie pour tout $n < 2m$. Nous allons montrer qu'elle est vraie pour $n = 2m$.

Nous pouvons supposer que $2m > 4$ donc $m > 2$. Alors $2m > m + 2$, donc les polynômes apparaissant dans la définition de ψ_{2m} satisfont l'hypothèse de récurrence. Si m est pair, alors ψ_m, ψ_{m+2} et ψ_{m-2} sont dans $2y\mathbb{Z}[x, y^2, A, B]$ donc ψ_{2m} est dans $2y\mathbb{Z}[x, y^2, A, B]$. Si m est impair, alors ψ_{m-1} et ψ_{m+1} sont dans $2y\mathbb{Z}[x, y^2, A, B]$. Nous trouvons donc de nouveau que ψ_{2m} est dans $2y\mathbb{Z}[x, y^2, A, B]$. La propriété est donc vraie pour $n = 2m$.

De même, on montre qu'elle est vraie pour $n = 2m + 1$. ■

Remarque 37 *Nous pouvons alors voir les polynômes de* $\mathbb{Z}[x, y^2, A, B]$ *comme des polynômes de* $\mathbb{Z}[x, A, B]$ *en remplaçant* y^2 *par* $x^3 + Ax + B$. *De même, nous pouvons voir les polynômes de* $2y\mathbb{Z}[x, y^2, A, B]$ *comme des polynômes de* $2y\mathbb{Z}[x, A, B]$.

Proposition 38 $\psi_n = \left\{ \begin{array}{ll} y(nx^{\frac{n^2-4}{2}} + \text{ termes en } x \text{ de degré plus petit }) & \text{si } n \text{ est pair} \\ nx^{\frac{n^2-1}{2}} + \text{termes en } x \text{ de degré plus petit} & \text{si } n \text{ est impair} \end{array} \right\}$

Démonstration. La preuve se fait par récurrence. Par exemple, si $n = 2m + 1$ où m est pair, alors le terme dominant de $\psi_{m+2}\psi_m^3$ est

$$(m + 2)m^3y^4x^{\frac{(m+2)^2-4}{2}+\frac{3m^2-12}{2}}$$

En remplaçant y^4 par $(x^3 + Ax + B)^2$, on obtient:

$$(m + 2)m^3x^{\frac{(2m+1)^2-1}{2}}.$$

De même, le terme dominant de $\psi_{m-1}\psi_{m+1}^3$ est

$$(m - 1)(m + 1)^3x^{\frac{(2m+1)^2-1}{2}}$$

En utilisant la relation de récurrence définissant ψ_{2m+1}, on obtient bien le terme dominant énoncé dans la Proposition. Les autres cas se traitent de la même manière. ■

Lemme 39 *Soit* n *un entier,* $n \geq 2$. *Posons*

$$\phi_n = x\psi_n^2 - \psi_{n+1}.\psi_{n-1} \quad et \quad \omega_n = (4y)^{-1}(\psi_{n+2}.\psi_{n-1}^2 - \psi_{n-2}.\psi_{n+1}^2).$$

On a

1. $\phi_n \in \mathbb{Z}[x, y^2, A, B]$ *pour tout* $n \in \mathbb{N}^*$.
2. *Si* n *est impair,* $\omega_n \in y\mathbb{Z}[x, y^2, A, B]$, *et si* n *est pair,* $\omega_n \in \mathbb{Z}[x, y^2, A, B]$.

Théorème 40 *Soit* $P(x, y)$ *un point de la courbe elliptique* $E : y^2 = x^3 + Ax + B$ *sur un corps de caractéristique différente de* 2 *et* 3, n *un entier positif. Alors:*

$$nP = \left(\frac{\phi_n(x)}{\psi_n^2(x)}, \frac{\omega_n(x, y)}{\psi_n^3(x, y)}\right)$$

Démonstration. Voir [1] partie 9.5. ■

Propriété 41 *Soient* $P(x, y) \in E(\overline{\mathbb{F}}_q)$ *et* n *un entier positif impair. Alors*

$$P \in E[n] \Leftrightarrow \psi_n(x) = 0.$$

Démonstration. En effet

$$\psi_n(x) = 0$$

équivaut à

$$\phi_{n-1}(x) = x\psi_{n-1}^2$$

c.-à-d

$$x = \frac{\phi_{n-1}(x)}{\psi_{n-1}^2(x)}$$

et donc P et $(n-1)P$ ont la même abscisse x, ce qui équivaut à

$$nP = P + (n-1)P = O,$$

c.à.d. $P \in E[n]$. ■

2.3 L'algorithme de Schoof

René Schoof a publié en 1985 (voir [15]) le premier algorithme polynômial qui permet de calculer exactement le nombre de points d'une courbe elliptique sur un corps fini $\mathbb{F}_p$, où p est un nombre premier impair. Cet algorithme est basé sur la restriction de l'endomorphisme de Frobenius aux points de m-torsion et sur les polynômes de division.

le groupe des points $\mathbb{F}_p-$rationnels $E(\mathbb{F}_p)$ a au plus $2p+1$ points : le point à l'infini plus $2p$ paires $(x, y) \in (\mathbb{F}_p)^2$. Ainsi,

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

Le théorème 27 de Hasse donne un meilleur encadrement

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

c-à-d

$$\#E(\mathbb{F}_p) = p + 1 - a \qquad \text{où} \quad |a| \leq 2\sqrt{p}.$$

Notons S le plus petit ensemble des premiers nombres premiers $\{2, 3, 5, ..., l_k\}$ vérifiant

$$\prod_{i=1}^{k} l_i > 4\sqrt{p}$$

Pour calculer a, il suffit de déterminer a modulo l_i pour tous les i entre 1 et k.

En effet, le théorème 34 des restes chinois nous donnera

$$a \bmod \prod_{i=1}^{k} l_i$$

et l'encadrement $|a| \leq 2\sqrt{p}$ permettra alors de déterminer a.

Premier cas: calcul de $a \bmod 2$

Comme p est impair et que $\#E(\mathbb{F}_p) = p + 1 - a$, on a :

$$a = \#E(\mathbb{F}_p) (\mathrm{mod}\, 2)$$

Si $a \equiv 0 (\mathrm{mod}\, 2)$, cela signifie que $E(\mathbb{F}_p)$ est d'ordre pair et donc il existe un élément d'ordre 2. Nous savons que les seuls éléments d'ordre 2 de $E(\mathbb{F}_p)$ sont de la forme $(x_0, 0)$ avec $x_0 \in \mathbb{F}_p$, c'est-à-dire que x_0 est racine de $x^3 + Ax + B$.

Rappelons que les éléments de $\mathbb{F}_p$ sont exactement les racines de $x^p - x$ (théorème 23). Ainsi, il nous suffit de calculer

$$\mathrm{pgcd}(x^3 + Ax + B, x^p - x)$$

par l'algorithme d'Euclide.

Si ce pgcd est différent de 1, alors $x^3 + Ax + B$ a une racine dans $\mathbb{F}_p$ et donc

$$a \equiv 0 (\mathrm{mod}\, 2)$$

Si ce pgcd est égal à 1, alors les polynômes $x^3 + Ax + B$ et $x^p - x$ n'ont pas de racines communes et donc $x^3 + Ax + B$ n'a pas de racines dans $\mathbb{F}_p$, d'où

$$a \equiv 1 (\mathrm{mod}\, 2)$$

Remarque 42 *Si p est un nombre premier assez grand, le polynôme x^p a un degré assez grand. Il est alors préférable de calculer*

$$x_p \equiv x^p (\mathrm{mod}\, x^3 + Ax + B),$$

puis d'utiliser le fait que:

$$\mathrm{pgcd}(x^3 + Ax + B, x^p - x) = \mathrm{pgcd}(x^3 + Ax + B, x_p - x).$$

Ceci termine le cas $l = 2$.

Second cas: calcul de $a \bmod l$ (où $l \neq 2$)

Soit $l \in S$ où $l \neq 2$ et $(x, y) \in E(\mathbb{F}_p) \cap E[l]$. Alors d'après le théorème 31 et la propriété 41, on a

$$\left\{ \begin{array}{l} (x^{p^2}, y^{p^2}) + p(x, y) = a(x^p, y^p) \\ \psi_l(x) = 0 \end{array} \right\}$$

La dernière équation permet de travailler modulo ψ_l dans tout ce qui suit afin de réduire le degré des polynômes.

Soit

$$p_l \equiv p (\mathrm{mod}\, l)\ ,\ |p_l| < \frac{l}{2}.$$

Nous avons donc

$$p(x,y) = p_l(x,y)$$

D'où

$$(x^{p^2}, y^{p^2}) + p_l(x,y) = a(x^p, y^p).$$

Ceci nous permet de travailler avec de plus petites valeurs. Puisque (x^p, y^p) est aussi d'ordre l (se rappeler que ϕ_p est un endomorphisme). La relation ci-dessus détermine a modulo l. Notons que si cette relation est vérifiée pour un point $(x,y) \in E[l]$, alors nous pourrons déterminer a modulo l et cette relation sera vraie pour tout $(x,y) \in E[l]$.

Premier cas : Supposons qu'il existe $(x,y) \in E[l]$ tel que $(x^{p^2}, y^{p^2}) \neq \pm p_l(x,y)$.

Posons alors

$$(x', y') \stackrel{def}{=} (x^{p^2}, y^{p^2}) + p_l(x,y) \neq O$$

donc $a \not\equiv 0 (\mathrm{mod}\, l)$. Dans ce cas, les premières coordonnées de (x^{p^2}, y^{p^2}) et $p_l(x,y)$ sont distinctes.

Nous allons utiliser la formule d'addition décrite dans le tableau 1.1.

Posons d'abord:

$$(x_j, y_j) \stackrel{def}{=} j(x,y)$$

pour tout entier j. On s'aperçoit en regardant la loi d'addition que x_j est une fraction rationnelle en x. Notons donc $x_j = r_{1,j}(x)$ où $r_{1,j}(x)$ est une fraction rationnelle en x. De même, y_j peut être mis sous la forme $y_j = r_{2,j}(x)y$ où $r_{2,j}(x)$ est également une fraction rationnelle en x.

La formule d'addition $(x^{p^2}, y^{p^2}) + (x_{p_l}, y_{p_l})$ donne alors:

$$x' = \left(\frac{y^{p^2} - y_{p_l}}{x^{p^2} - x_{p_l}} \right)^2 - x^{p^2} - x_{p_l}$$

Nous pouvons exprimer $(y^{p^2} - y_{p_l})^2$ en fonction de x :

$$\begin{aligned}(y^{p^2} - y_{p_l})^2 &= y^2 \left(y^{p^2-1} - r_{2,p_l}(x) \right)^2 \\ &= (x^3 + Ax + B) \left(\left(x^3 + Ax + B \right)^{\frac{p^2-1}{2}} - r_{2,p_l}(x) \right)^2\end{aligned}$$

Il y va de même avec $(x^{p^2} - x_{p_l})^2$. Ainsi, x' est une fraction rationnelle en x.

Nous cherchons j tel que

$$(x', y') = j(x^p, y^p) = (x_j^p, y_j^p)$$

Soit $(x,y) \in E[l]$, alors

$$(x', y') = \pm(x_j^p, y_j^p) \text{ si et seulement si } \quad x' = x_j^p.$$

Nous avons vu que si cette relation est vraie pour un point de $E[l]$, alors elle est vraie pour tous les points de $E[l]$. Puisque les racines de ψ_l sont les premières coordonnées des points de $E[l]$, ceci implique que

$$x' - x_j^p \equiv 0 (\mathrm{mod}\, \psi_l)$$

(Ceci signifie que le numérateur de $x' - x_j^p$ est un multiple de ψ_l).

Nous utilisons en fait que les racines de ψ_l sont simples (sinon nous pourrions uniquement conclure que ψ_l divise une puissance de $x' - x_j^p$). Ceci se prouve en remarquant qu'il y a $l^2 - 1$ points distincts d'ordre l (proposition 20). Il y a donc $\frac{l^2-1}{2}$ premières coordonnées différentes (car si $(x, y) \in E[l]$ alors $-(x, y) = (x, -y) \in E[l]$) et ce sont toutes des racines de ψ_l (ψ_l est de degré $\frac{l^2-1}{2}$ d'après la proposition 39). Ainsi, les racines de ψ_l sont simples.

Supposons maintenant que nous ayons trouvé j tel que

$$x' - x_j^p \equiv 0 (\mathrm{mod}\, \psi_l)$$

Alors

$$(x', y') = \pm(x_j^p, y_j^p) = (x_j^p, \pm y_j^p)$$

Pour déterminer le signe de a, il nous faut regarder y'. Les expressions $\frac{y'}{y}$ et $\frac{y_j^p}{y}$ peuvent toutes les deux être exprimées en fonction de x. Si

$$\frac{y' - y_j^p}{y} \equiv 0 (\mathrm{mod}\, \psi_l)$$

alors $a \equiv j (\mathrm{mod}\, l)$. Sinon $a \equiv -j (\mathrm{mod}\, l)$.

Second cas: Supposons que $(x^{p^2}, y^{p^2}) = \pm p_l(x, y)$ pour tout $(x, y) \in E[l]$

Si $\phi_p^2(x, y) = (x^{p^2}, y^{p^2}) = -p_l(x, y)$

alors

$$a(x^p, y^p) = (x^{p^2}, y^{p^2}) + p_l(x, y) = O$$

c-à-d

$$a\phi_p P = (\phi_p^2 + p)P = O$$

pour tout $P \in E[l]$. Il en résulte que

$$a \equiv 0 (\mathrm{mod}\, l)$$

Si $\phi_p^2(x, y) = (x^{p^2}, y^{p^2}) = p_l(x, y)$, alors

$$(x^{p^2}, y^{p^2}) - p_l(x, y) = O$$

c-à-d

$$(\phi_p^2 - p)P = O$$

donc

$$a\phi_p(x,y) = \phi_p^2(x,y) + p(x,y) = 2p(x,y),$$

d'où

$$a^2 p(x,y) = a^2\phi_p^2(x,y) = (2p)^2(x,y),$$

ainsi

$$a^2 p \equiv 4p^2 (\mathrm{mod}\, l)$$

donc p est un carré modulo l. Notons alors $w^2 \equiv p(\mathrm{mod}\, l)$. Il vient

$$(\phi_p + w)(\phi_p - w)(x,y) = (\phi_p^2 - p)(x,y) = O,$$

pour tout $(x,y) \in E[l]$.

Soit P un point de $E[l]$. Nous avons deux possibilités:

Soit $(\phi_p - w)P = O$, c'est-à-dire $\phi_p P = wP$.

Soit $P' = (\phi_p - w)P$ est un point fini qui vérifie $(\phi_p + w)P' = O$.

Dans les deux cas, il existe un point $P \in E[l]$ tel que $\phi_p P = \pm wP$.

Supposons qu'il existe un point $P \in E[l]$ tel que $\phi_p P = wP$. Alors

$$O = (\phi_p^2 - a\phi_p + p)P = (p - aw + p)P,$$

d'où $aw = 2p \equiv 2w^2 (\mathrm{mod}\, l)$. Ainsi

$$a \equiv 2w (\mathrm{mod}\, l)$$

De même, s'il existe $P \in E[l]$ tel que $\phi_p P = -wP$, alors

$$a \equiv -2w (\mathrm{mod}\, l).$$

Nous pouvons savoir dans quel cas nous nous trouvons par la méthode qui suit. En fait, nous voulons savoir s'il existe $(x,y) \in E[l]$ tel que

$$\phi_p(x,y) = (x^p, y^p) = \pm w(x,y) = \pm(x_w, y_w) = (x_w, \pm y_w).$$

Pour cela, nous calculons $x^p - x_w$ qui est une fraction rationnelle en x.

Si

$$\mathrm{pgcd}(\text{ numérateur}(x^p - x_w), \psi_l) \neq 1,$$

alors il existe $(x,y) \in E[l]$ tel que $\phi_p(x,y) = \pm w(x,y)$. Dans ce cas, nous utiliserons la seconde coordonnée pour déterminer le signe.

Par contre, si

$$\text{pgcd}(\text{ numérateur}(x^p - x_w), \psi_l) = 1,$$

nous ne pouvons pas être dans le cas

$$(x^{p^2}, y^{p^2}) = p(x, y).$$

Nous sommes alors dans le cas

$$(x^{p^2}, y^{p^2}) = -p(x, y),$$

qui a déjà été traité.

Algorithme 43 *Soit E une courbe elliptique définie sur $\mathbb{F}_p$ donnée par*

$$y^2 = x^3 + Ax + B$$

L'algorithme suivant nous permet de calculer

$$\#E(\mathbb{F}_p) = p + 1 - a$$

1. *Soit $S = \{2, 3, 5, ..., l_i\}$ l'ensemble des nombres premiers vérifiant $\prod_{i=1}^{k} l_i > 4\sqrt{p}$.*
2. *Si $l = 2$, alors $a \equiv 0 (\text{mod } 2)$ si et seulement si*

$$\text{pgcd}(x^3 + Ax + B, x^p - x) \neq 1$$

3. *Pour chaque nombre premier impair $l \in S$, faire ce qui suit:*

   a) *Soit $p_l \equiv p (\text{mod } l)$ tel que $|p_l| < \frac{l}{2}$.*

   b) *Calculer x', la première coordonnée de*

$$(x', y') = (x^{p^2}, y^{p^2}) + p_l(x, y) (\text{mod } \psi_l).$$

   c) *Pour $j = 1, 2, ..., \frac{l-1}{2}$, faire ce qui suit:*

      i- Calculer x_j, la première coordonnée de

$$(x_j, y_j) = j(x, y)$$

      ii- Si $x\prime - x_j^p \equiv 0 (\text{mod } \psi_l)$, aller à l'étape (iii).Sinon retourner en (i) avec l'entier j suivant. Si toutes les valeurs $1 \leq j \leq \frac{l-1}{2}$ ont été essayées, aller à l'étape (d).

iii- Calculer y' et y_j. Si

$$\frac{y' - y_j^p}{y} \equiv 0 (\mathrm{mod}\, \psi_l)$$

alors $a = j (\mathrm{mod}\, l)$, sinon $a = -j (\mathrm{mod}\, l)$.

d) *Si toutes les valeurs $1 \leq j \leq \frac{l-1}{2}$ ont été essayées sans succès, posons*

$$w^2 \equiv p (\mathrm{mod}\, l).$$

Dans le cas où w n'existerait pas, alors $a \equiv 0 (\mathrm{mod}\, l)$.

e) *Si (numérateur $(x^p - x_w), \psi_l) = 1$ alors $a \equiv 0 (\mathrm{mod}\, l)$. Sinon calculer*

$$\mathrm{pgcd}(\textit{numérateur}\ (\frac{y^p - y_w}{y}, \psi_l)$$

Si ce pgcd *est différent de 1 alors $a \equiv 2w (\mathrm{mod}\, l)$, sinon $a \equiv -2w (\mathrm{mod}\, l)$.*

4. Puisque nous connaissons a modulo l pour tout $l \in S$, nous pouvons calculer

$$a \bmod \prod_{l \in S} l$$

grâce au théorème 34 des restes chinois. Choisir ensuite la valeur de a qui satisfait cette congruence et telle que $|a| \leq 2\sqrt{p}$. Le nombre de points dans $E(\mathbb{F}_p)$ est alors

$$\#E(\mathbb{F}_p) = p + 1 - a$$

2.4 Calcul dans le cas général

Nous connaissons le cardinal de $E(\mathbb{F}_p)$ grâce à l'algorithme précédent. Dans cette partie, nous allons voir comment calculer $\#E(\mathbb{F}_q)$ où $q = p^n$ en connaissant $\#E(\mathbb{F}_p)$.

Théorème 44 *Soit $\#E(\mathbb{F}_p) = p + 1 - a$. Posons $X^2 - aX + p = (X - \alpha)(X - \beta)$, où $\alpha, \beta \in \mathbb{C}$. Alors*

$$\#E(\mathbb{F}_{p^n}) = p^n + 1 - (\alpha^n + \beta^n)$$

pour tout $n \geq 1$.

Démonstration. Montrons d'abord que $\alpha^n + \beta^n$ est un entier. Considérons la suite

$$S_n = \alpha^n + \beta^n.$$

Nous avons $S_o = 2$ et $S_1 = a$. Montrons que

$$S_{n+1} = aS_n - pS_{n-1},$$

pour tout $n \geq 1$, ce qui justifiera que $\alpha^n + \beta^n$ est un entier.

En multipliant la relation $\alpha^2 - a\alpha + p = 0$ par α^{n-1}, nous obtenons

$$\alpha^{n+1} = a\alpha^n - p\alpha^{n-1}.$$

De même, en multipliant la relation $\beta^2 - a\beta + p = 0$ par β^{n-1}, nous obtenons

$$\beta^{n+1} = a\beta^n - p\beta^{n-1}.$$

En additionnant les deux égalités précédentes, nous avons l'égalité souhaitée:

$$S_{n+1} = aS_n - pS_{n-1}.$$

Posons

$$f(X) = (X^n - \alpha^n)(X^n - \beta^n) = X^{2n} - (\alpha^n + \beta^n)X^n + p^n$$

α et β sont des racines de f donc $(X - \alpha)(X - \beta) = X^2 - aX + p$ divise $f(X)$. Il existe donc un polynôme Q tel que

$$f(X) = Q(X)(X^2 - aX + p).$$

Remarquons que f et $X^2 - aX + p$ ont des coefficients entiers (se rappeler que $\alpha^n + \beta^n$ est un entier) et que le coefficient dominant de $X^2 - aX + p$ est 1, on peut donc, affirmer que Q a également des coefficients entiers.

D'après le théorème 31, $\phi_p^2 - a\phi_p + p = 0$ donc

$$f(\phi_p) = (\phi_p^n)^2 - (\alpha^n + \beta^n)\phi_p^n + p^n = Q(\phi_p)(\phi_p^2 - a\phi_p + p) = 0,$$

comme endomorphisme de E. Remarquons que $\phi_p^n = \phi_{p^n}$, ainsi

$$\phi_{p^n}^2 - (\alpha^n + \beta^n)\phi_{p^n} + p^n = 0.$$

Par le théorème 31, nous obtenons

$$\alpha^n + \beta^n = p^n + 1 - \#E(\mathbb{F}_{p^n}). \quad \blacksquare$$

2.5 Complexité de l'algorithme de Schoof

Définition 45 *La complexité d'un calcul arithmétique est le nombre maximal d'opérations à effectuer pour avoir le résultat en fonction de la taille d'entrée des données de ce calcul.*

On montre que la complexité de l'algorithme est $O(\log^8 p)$:

Les calculs les plus importants sont ceux de (x^p, y^p) et (x^{p^2}, y^{p^2}) dans l'anneau $\mathbb{F}_p[x,y]/(\psi_l(x), y^2 - x^3 - Ax - B)$. Sachant que le degré de $\psi_l(x)$ est en $O(\log^2 p)$, chaque multiplication modulo $\psi_l(x)$ nécessite $O(\log^4 p)$ multiplications dans $\mathbb{F}_p$, et donc $O(\log^6 p)$ multiplications dans notre anneau. On a besoin de faire $O(\log p)$ multiplications, et ceci pour $O(\log p)$ nombres l différents, soit une complexité en tout de $O(\log^8 p)$.

2.6 Exemple 1 (Calcul de $\#E(\mathbb{F}_{19^9})$)

Dans cet exemple, nous voulons calculer l'ordre du groupe $E(\mathbb{F}_{19^9})$ en utilisant l'algorithme de Schoof et les différentes étapes de calcul ont été faites sur le logiciel algébrique SAGE (Voir la partie 4.6).

Première partie: Calcul de $\#E(\mathbb{F}_{19})$

Considérons la courbe elliptique $E : y^2 = x^3 + 2x + 1$ définie sur $E(\mathbb{F}_{19})$.

Nous avons donc:

$$\#E(\mathbb{F}_{19}) = 19 + 1 - a$$

et nous cherchons à déterminer a.

Comme $p = 19$, nous avons $S = \{2, 3, 5\}$ vérifiant $2 \times 3 \times 5 = 30 > 4\sqrt{19} \simeq 17,44$.

Nous allons calculer $a \pmod 2$, $a \pmod 3$, $a \pmod 5$

Calcul de a modulo 2

Nous réduisons d'abord x^{19} modulo $x^3 + 2x + 1$:

$$x^{19} \equiv x^3 + 13x + 14 (\mathrm{mod}\, x^3 + 2x + 1).$$

Ensuite, calculons le pgcd suivant:

$$\mathrm{pgcd}(x^{19} - x, x^3 + 2x + 1) = \mathrm{pgcd}(x^3 + 12x + 14, x^3 + 2x + 1) = 1.$$

Ainsi, $x^3 + 2x + 1$ n'a pas de racines dans $\mathbb{F}_{19}$ et donc

$$a \equiv 1 (\mathrm{mod}\, 2)$$

Calcul de a modulo 3

Aller à l'étape 3 de l'algorithme.

(a) Nous avons $p = 19 \equiv 1 (\mathrm{mod}\, 3)$ donc $p_l = 1$.

(b) Il nous faut encore connaître $p^2 = 361$.

Le troisième polynôme de division est:

$$\psi_3 = 3x^4 + 12x^2 + 12x - 4.$$

Ensuite, calculons la première coordonnée de $(x', y') = \left(x^{361}, y^{361}\right) + (x, y)$:

$$\begin{aligned} x' &= \left(\tfrac{y^{361}-y}{x^{361}-x}\right)^2 - x^{361} - x \\ &= \left(x^3+2x+1\right)\left(\tfrac{\left(x^3+2x+1\right)^{180}-1}{x^{361}-x}\right)^2 - x^{361} - x, \end{aligned}$$

où nous avons utilisé la relation $y^2 = x^3 + 2x + 1$.

Nous avons besoin de réduire cette relation modulo ψ_3. Une idée serait d'utiliser l'algorithme d'Euclide généralisé pour trouver l'inverse de $x^{361} - x (\mathrm{mod}\, \psi_3)$. Cependant,

$$\mathrm{pgcd}(x^{361} - x, \psi_3) = x + 11 \neq 1,$$

donc cet inverse n'existe pas

(c)

i- pour $j = 1$, la première coordonée de $(x_1, y_1) = 1(x, y)$ est x.

ii- Puisque l'inverse de $x^{361} - x (\mathrm{mod}\, \psi_3)$ n'existe pas alors

$$x' - x^{19} \not\equiv 0 (\mathrm{mod}\, \psi_3).$$

(d) Toutes les valeurs $1 \leq j \leq \frac{3-1}{2}$ ont été essayées sans succés. Posons

$$w^2 \equiv 19 (\mathrm{mod}\, 3).$$

Donc

$$w^2 \equiv 1 (\mathrm{mod}\, 3)$$

$$w = 1$$

(e) Calculer

$$\mathrm{pgcd}(\text{ numérateur}(x^{19} - x), \psi_3) = x + 11 \neq 1$$

$$\mathrm{pgcd}(\text{ numérateur}(\frac{y^{19} - y}{y}), \psi_3) = \mathrm{pgcd}((x^3 + 2x + 1)^9 - 1, \psi_3) = x + 11 \neq 1.$$

Alors

$$a \equiv 2 (\mathrm{mod}\, 3)$$

Remarque 46 *Nous pouvons constater ce résultat après calcul de x' où nous retrouvons* $\mathrm{pgcd}(x^{361} - x, \psi_3) = x + 11 \neq 1$
Alors $x = 8 \in \mathbb{F}_{19}$ est une racine de ψ_3. Le point $(8, 4) \in E(\mathbb{F}_{19})$ est d'ordre 3 et donc 3 divise $\#E(\mathbb{F}_{19})$, donc

$$\#E(\mathbb{F}_{19}) = 19 + 1 - a \equiv 0 (\mathrm{mod}\, 3),$$

d'où

$$a \equiv 2 (\mathrm{mod}\, 3)$$

Calcul de a modulo 5

Nous poursuivons l'algorithme de Schoof. Aller à l'étape 3.

(a) $p = 19 \equiv -1 (\mathrm{mod}\, 5)$ donc $p_l = -1$. De plus,

$$19(x, y) = -(x, y) = (x, -y) \text{ pour tout } (x, y) \in E[5].$$

Le cinquième polynôme de division est:

$$\begin{aligned} \psi_5 &= \psi_4 \psi_2^3 - \psi_1 \psi_3^3 \\ \psi_5 &= 5x^{12} + 10x^{10} + 17x^8 + 5x^7 + x^6 + 9x^5 + 12x^4 + 2x^3 + 5x^2 + 8x + 8 \end{aligned}$$

(b) Calculer $x' (\mathrm{mod}\, \psi_5)$. La première coordonnée de

$$(x', y') = \left(x^{361}, y^{361}\right) + (x, -y).$$

On a

$$\begin{aligned} x' &= \left(x^3 + 2x + 1\right) \left(\frac{\left(x^3 + 2x + 1\right)^{180} + 1}{x^{361} - x} \right)^2 - x^{361} - x \\ &= 3x^{11} + 9x^{10} + 18x^9 + 11x^8 + 16x^7 + x^6 + 3x^5 + 12x^4 + 4x^3 + 17x^2 + 6x + 16 \end{aligned}$$

(c)

i- Pour $j = 1$, la première coordonée de $(x_1, y_1) = 1(x, y)$ est x.

ii- Nous calculons $x' - x^{19} (\mathrm{mod}\, \psi_5)$.

$$x' - x^{19} = 11x^{11} + 15x^{10} + 18x^9 + 2x^8 + 17x^7 + 2x^6 + 4x^5 + 8x^4 + 18x^3 + 8x^2 + 6x + 18$$

Aller à l'étape (i) pour $j = 2$

La première coordonée de $(x_2, y_2) = 2(x, y)$ modulo ψ_5 est

$$\begin{aligned} x_2 &= \left(\frac{3x^2 + 2}{2y} \right)^2 - 2x = \frac{\left(3x^2 + 2\right)^2}{4\left(x^3 + 2x + 1\right)} - 2x \\ &= 12x^{11} + 4x^{10} + 18x^9 + 7x^8 + 14x^7 + 5x^6 + 6x^5 + 5x^4 + 15x^3 + 8x^2 + 4x + 7 \end{aligned}$$

ii- Nous calculons

$$x' - x_2^{19} \equiv 0 (\mathrm{mod}\, \psi_5).$$

Après calcul, on s'aperçoit que la relation ci-dessus est vérifiée. Ainsi,

$$a \equiv \pm 2 (\mathrm{mod}\, 5).$$

iii- Calculer y' et y_j

Pour déterminer le signe, nous allons regarder les secondes coordonnées modulo ψ_5.

La seconde coordonnée de $(x\prime, y\prime) = (x^{361}, y^{361}) + (x, -y)$ est :

$$\begin{aligned} y' &= y\left(\frac{\left(x^3+2x+1\right)^{180}+1}{x^{361}-x}\left(x^{361}-x'\right)-\left(x^3+2x+1\right)^{180}\right) \\ &= y\left(9x^{11}+13x^{10}+15x^9+15x^7+18x^6+17x^5+8x^4+12x^3+8x+6\right) \end{aligned}$$

La seconde coordonnée de $(x_2, y_2) = 2(x, y)$ est

$$\begin{aligned} y_2 &= y\left(\frac{3x^2+2}{2(x^3+2x+1)}(x-x_2)-1\right) \\ &= y(13x^{10}+15x^9+16x^8+13x^7+8x^6+6x^5+17x^4+18x^3+8x+18. \end{aligned}$$

Alors

$$\begin{aligned} y_2^{19} &= y\left((x^3+2x+1)^9(\frac{3x^2+2}{2(x^3+2x+1)}(x-x_2)-1)^{29}\right) \\ &= y\left(10x^{11}+6x^{10}+4x^9+4x^7+x^6+2x^5+11x^4+7x^3+21x^2+11x+13\right). \end{aligned}$$

Après calcul,

$$\frac{y'+y_2^{19}}{y} \equiv 0 (\mathrm{mod}\, \psi_5).$$

Cela signifie que

$$(x', y') \equiv (x_2^{19}, -y_2^{19}) = -2(x^{19}, y^{19}) (\mathrm{mod}\, \psi_5),$$

et donc

$$\begin{aligned} a &\equiv -2 (\mathrm{mod}\, 5) \\ &\equiv 3 (\mathrm{mod}\, 5). \end{aligned}$$

Ce qui termine le cas $l = 5$.
Nous avons montré que

$$\begin{aligned} a &\equiv 1 (\mathrm{mod}\, 2) \\ a &\equiv 2 (\mathrm{mod}\, 3) \\ a &\equiv 3 (\mathrm{mod}\, 5). \end{aligned}$$

D'aprés le théorème 34, on en déduit que

$$a \equiv 23 (\mathrm{mod}\, 30).$$

Comme $|a| < 2\sqrt{19} < 9$, on aura finalement $a = -7$.
D'où :

$$\#E(\mathbb{F}_{19}) = 19 + 1 - a = 27.$$

Seconde partie: Calcul de $\#E(\mathbb{F}_{19^9})$

Nous savons que $a = -7$. Nous avons ainsi le polynôme:

$$X^2 - aX + p = X^2 + 7x + 19 = \left(X - \frac{-7 - i\sqrt{27}}{2}\right)\left(X - \frac{-7 + i\sqrt{27}}{2}\right).$$

D'après le théorème 44, le cardinal recherché vaut donc :

$$\begin{aligned} \#E(\mathbb{F}_{19^9}) &= 19^9 + 1 - \left(\tfrac{-7-i\sqrt{27}}{2}\right)^9 - \left(\tfrac{-7+i\sqrt{27}}{2}\right)^9 \\ &= 322688674476 \end{aligned}$$

2.7 Exemple 2 (Calcul de $\#E(\mathbb{F}_{29^{2013}})$)

Première partie: Calcul de $\#E(\mathbb{F}_{29})$

Considérons la courbe elliptique $E : y^2 = x^3 + 2x + 1$ définie sur $E(\mathbb{F}_{29})$.

Nous avons donc:

$$\#E(\mathbb{F}_{29}) = 29 + 1 - a.$$

Nous cherchons à déterminer a.

Comme $p = 29$, nous avons $S = \{2, 3, 5\}$ vérifiant $2 \times 3 \times 5 = 30 > 4\sqrt{29} \simeq 21,54$.

Nous allons calculer $a \pmod 2$, $a \pmod 3$, $a \pmod 5$

Calcul de a modulo 2

Nous réduisons d'abord x^{29} modulo $x^3 + 2x + 1$:

$$x^{29} \equiv 14x^2 + 18x + 9 (\mathrm{mod}\, x^3 + 2x + 1),$$

Ensuite, calculons le pgcd suivant:

$$\mathrm{pgcd}(x^{29} - x, x^3 + 2x + 1) = \mathrm{pgcd}(14x^2 + 17x + 9, x^3 + 2x + 1) = 1.$$

Ainsi, $x^3 + 2x + 1$ n'a pas de racine dans $\mathbb{F}_{29}$ et donc

$$a \equiv 1 (\mathrm{mod}\, 2)$$

Calcul de a modulo 3

Aller à l'étape 3 de l'algorithme.

(a) Nous avons $p = 29 \equiv -1 (\mathrm{mod}\, 3)$ donc $p_l = -1$.

(b) $p^2 = 841$ et $-(x, y) = (x, -y)$.

Le troisième polynôme de division est:

$$\psi_3 = 3x^4 + 12x^2 + 12x - 4.$$

Calculons la première coordonnée de $(x', y') = \left(x^{841}, y^{841}\right) + (x, -y)$:

$$\begin{aligned} x' &= \left(\tfrac{y^{841}+y}{x^{841}-x}\right)^2 - x^{841} - x \\ &= \left(x^3 + 2x + 1\right)\left(\tfrac{\left(x^3+2x+1\right)^{420}+1}{x^{841}-x}\right)^2 - x^{841} - x, \end{aligned}$$

où nous avons utilisé la relation $y^2 = x^3 + 2x + 1$.
(c)
i- Pour $j = 1$, la première coordonée de $(x_1, y_1) = 1(x, y)$ est x.

ii- Nous calculons

$$x' - x_j^p = \left(x^3 + 2x + 1\right)\left(\frac{\left(x^3 + 2x + 1\right)^{420} + 1}{x^{841} - x}\right)^2 - x^{841} - x - x^{29} (\mathrm{mod}\, \psi_3).$$

Nous avons besoin de réduire cette relation modulo ψ_3. On a

$$\mathrm{pgcd}(x^{841} - x, \psi_3) = x^4 + 4x^2 + 4x + 18 \neq 1$$

donc cet inverse n'existe pas et

$$x' - x^{29} \not\equiv 0 (\mathrm{mod}\, \psi_3)$$

(d) toutes les valeurs $1 \leq j \leq \frac{3-1}{2}$ ont été essayées sans succés. Posons

$$w^2 \equiv 29 (\mathrm{mod}\, 3).$$

Donc

$$w^2 \equiv 2 (\mathrm{mod}\, 3).$$

w n'existe pas, alors

$$a \equiv 0 (\mathrm{mod}\, 3)$$

Remarque 47 *Nous pouvons constater ce résultat après calcul de x' où nous retrouvons* $\mathrm{pgcd}(x^{841} - x, \psi_3) = x^4 + 4x^2 + 4x + 18 \neq 1$ *et comme*

$$x^4 + 4x^2 + 4x + 18 = (x + 13)(x + 27)(x^2 + 18x + 6),$$

alors $x = 2 \in \mathbb{F}_{29}$ est une racine de ψ_3. Le point $(2, 10) \in E(\mathbb{F}_{29})$ est d'ordre 3 et donc 3 divise $\#E(\mathbb{F}_{29})$, donc

$$\#E(\mathbb{F}_{29}) = 29 + 1 - a \equiv 0 (\mathrm{mod}\, 3),$$

d'où

$$a \equiv 0 (\mathrm{mod}\, 3)$$

Calcul de a modulo 5

Nous poursuivons l'algorithme de Schoof. Aller à l'étape 3.
(a) $p = 29 \equiv -1 (\mathrm{mod}\, 5)$ donc $p_l = -1$. De plus,

$$29(x, y) = -(x, y) = (x, -y) \text{ pour tout } (x, y) \in E[5].$$

Le cinquième polynôme de division est:

$$\begin{aligned}\psi_5 &= \psi_4\psi_2^3 - \psi_1\psi_3^3\\ \psi_5 &= 5x^{12} + 8x^{10} + 3x^9 + 15x^8 + 16x^7 + 28x^6 + 18x^4 + 22x^3 + 21x^2 + 20x + 16\end{aligned}$$

(b) Calculons $x'(\mathrm{mod}\,\psi_5)$, la première coordonnée de

$$(x', y') = \left(x^{841}, y^{841}\right) + (x, -y).$$

On a

$$\begin{aligned}x' &= \left(x^3 + 2x + 1\right)\left(\frac{\left(x^3 + 2x + 1\right)^{420} + 1}{x^{841} - x}\right)^2 - x^{841} - x\\ &= 4x^{11} + 19x^{10} + 7x^8 + 18x^7 + 25x^6 + 19x^5 + 12x^4 + 20x^3 + 21x^2 + 28x + 11\end{aligned}$$

(c)

i- Pour $j = 1$, la première coordonnée de $(x_1, y_1) = 1(x, y)$ est x.

ii- Nous calculons $x' - x^{29}(\mathrm{mod}\,\psi_5)$

$$x' - x^{29} = 4x^{11} + 28x^{10} + 20x^9 + 5x^8 + 15x^7 + 3x^6 + 24x^5 + 11x^4 + 12x^3 + 11x^2 + x + 18.$$

Aller à l'étape (i) pour $j = 2$

La première coordonnée de $(x_2, y_2) = 2(x, y)$ modulo ψ_5 est

$$\begin{aligned}x_2 &= \left(\frac{3x^2 + 2}{2y}\right)^2 - 2x = \frac{\left(3x^2 + 2\right)^2}{4\left(x^3 + 2x + 1\right)} - 2x\\ &= 6x^{11} + 4x^{10} + 22x^9 + 25x^8 + x^7 + 4x^6 + 23x^5 + x^4 + 5x^3 + 10x^2 + 21x + 6\end{aligned}$$

ii- Nous avons

$$x' - x_2^{29} = x' - \frac{\left(3x^{58} + 2\right)^2}{4\left(x^3 + 2x + 1\right)^{29}} + 2x^{29} = 0(\mathrm{mod}\,\psi_5).$$

Après calcul, on s'aperçoit que la relation ci-dessus est vérifiée. Ainsi,

$$a \equiv \pm 2(\mathrm{mod}\,5).$$

iii- Calculer y' et y_j

Pour déterminer le signe, nous allons regarder les secondes coordonnées modulo ψ_5.

La seconde coordonnée de $(x\prime, y\prime) = (x^{841}, y^{841}) + (x, -y)$ est :

$$\begin{aligned}y' &= y\left(\frac{\left(x^3 + 2x + 1\right)^{420} + 1}{x^{841} - x}\left(x^{841} - x'\right) - \left(x^3 + 2x + 1\right)^{420}\right)\\ &= y\left(21x^{11} + 18x^{10} + 25x^9 + 15x^8 + 15x^7 + 6x^6 + 13x^5 + 16x^4 + 6x^3 + 21x^2 + 23x + 26\right)\end{aligned}$$

La seconde coordonnée de $(x_2, y_2) = 2(x, y)$ est

$$y_2 = y\left(\frac{3x^2+2}{2(x^3+2x+1)}(x-x_2)-1\right).$$

Alors

$$\begin{aligned} y_2^{29} &= y\left((x^3+2x+1)^{14}(\frac{3x^2+2}{2(x^3+2x+1)}(x-x_2)-1)^{29}\right) \\ &= y\left(21x^{11}+18x^{10}+25x^9+15x^8+15x^7+6x^6+13x^5+16x^4+6x^3+21x^2+23x+26\right). \end{aligned}$$

Après calcul,

$$\frac{y'-y_2^{29}}{y} \equiv 0 (\mathrm{mod}\, \psi_5).$$

Cela signifie que

$$(x', y') \equiv (x_2^{19}, y_2^{19}) = 2(x^{19}, y^{19}) (\mathrm{mod}\, \psi_5),$$

et donc

$$a \equiv 2 (\mathrm{mod}\, 5)$$

Ce qui termine le cas $l = 5$.

Nous avons montré que

$$\begin{aligned} a &\equiv 1 (\mathrm{mod}\, 2) \\ a &\equiv 0 (\mathrm{mod}\, 3) \\ a &\equiv 2 (\mathrm{mod}\, 5) \end{aligned}$$

D'aprés le théorème 34, on en déduit que

$$a \equiv 27 (\mathrm{mod}\, 30)$$

Et comme $|a| < 2\sqrt{29} < 10$, on aura finalement $a = -3$.

D'où:

$$\#E(\mathbb{F}_{29}) = 29 + 1 - a = 33.$$

Seconde partie: Calcul de $\#E(\mathbb{F}_{29^{2013}})$

Nous savons que $a = -3$. Nous avons ainsi le polynôme :

$$X^2 - aX + p = X^2 + 3x + 29 = \left(X - \frac{-3 - i\sqrt{107}}{2}\right)\left(X - \frac{-3 + i\sqrt{107}}{2}\right).$$

Le cardinal recherché vaut donc :

$\#E(\mathbb{F}_{29^{2013}}) = 29^{2013} + 1 - \left(\frac{-3-i\sqrt{107}}{2}\right)^{2013} - \left(\frac{-3+i\sqrt{107}}{2}\right)^{2013} =$

641460281620499961805967164034824142458125349589860006572913337121 16\

185945130607432089160281568874760805220888412317865575160723647193 87\

308473897928203334997564133189656303144801618592873817243269227000 67\

$$
\begin{aligned}
&088897274365037913575031831924092011559239778369005400459409876541 43\backslash\\
&753982198464986862644864901432104644691178711518084639259455512270 69\backslash\\
&368421582173735655023466779666994708589278071326391482765932975909 86\backslash\\
&353219925694903482128632289774920682918909327176779302108216619181 72\backslash\\
&329550296342750231196371257945284074895800510876617183794757495831 11\backslash\\
&821584131361568580663338710756779105567109853485745057947032103367 94\backslash\\
&341739382318779438859655626041360142117312269802493637188426016142 64\backslash\\
&413517586208272318741569676900550768377709675766364662844956490418 65\backslash\\
&668935123987759651214794362893366674462556773337990874016646426700 24\backslash\\
&185176164797969478489114567766618788727113916285427917212789650640 93\backslash\\
&107498677694846605939188956735102263004493991705543438536260587913 24\backslash\\
&217737023619197776293241409545325920730854045545215973350600504122 59\backslash\\
&195106963633409030214463153194169407503193300552284370449015125148 82\backslash\\
&967109108265027772546928051056761807476926158488911519699248133397 80\backslash\\
&139339005030656802051753670958115715296764540502650813049223369850 49\backslash\\
&898101290803878167485280713934883736222760542258084975509391994500 87\backslash\\
&618981319633715030492802127320310979961646162538372921784309096742 78\backslash\\
&682885311333920359502237360842974374709012496167102595854977509798 78\backslash\\
&412852180430784424107289771435001112576051667336548439282079906248 40\backslash\\
&757074580242608850916823494414535206335705577363190112392401773522 06\backslash\\
&887481507736743421744111190196236163932734844874702816792678014878 59\backslash\\
&939310767110691414657462934029580373166177890337127623636346201455 45\backslash\\
&748619575439865055467320246105789222447682385791791591862797792464 17\backslash\\
&049624818727854611273203831073275229379413021140683550714874874158 05\backslash\\
&989207409522800491154610962663837160812203236793908757483365341287 27\backslash\\
&201860151436809413226204950565376178689031377354682226605002140339 93\backslash\\
&911517767091738007969882239362370479240924419297815192829895361556 86\backslash\\
&086798062412067933775049353445638745880906439423715597312151674890 61\backslash\\
&341332195970636428182518051925800970552202434705317092543102628460 07\backslash\\
&081063551845883198632304723723356209269243639602217619977011659082 61\backslash\\
&587404833136918920450970563020788671232778821763522923423185399231 04\backslash\\
&231336336384650500499778941810102151076235867309059928593081823714 99\backslash\\
&100301322125437806013579663728601029420542874915076956554088176802 36\backslash\\
&041097943949214196928119239920221652180988533323264447056939956338 38\backslash\\
&176174800865095432694610956072859785441547363564361531903265115544 18\backslash\\
&182791347860908769227787653907831989462210596563112254405253681194 99\backslash\\
&427275154387292609434135101031056342142233255667742401018911221067 45\backslash\\
&509493995725276669289003812105478122892233932838525886312422568212 98\backslash
\end{aligned}
$$

48805106255894102182481858821503749119407036816811940837493257369364\
14534503430807752296364614546434308811663503153317077108128252326297\
36056810899718929324

Il est donc assez rapide de calculer le cardinal d'un groupe $E(\mathbb{F}_{p^n})$ par cet algorithme.

Le dénombrement des points d'une courbe elliptique est actuellement un sujet en pleine expansion.

A.O.L Atkin et N. Elkies ont réussi à réduire la complexité de cet algorithme à $O(\log^6 p)$ grâce à l'introduction des polynômes modulaires. R.Schoof a donc reécrit un article en 1995 [16], qui résume tout ce qui a été fait sur le dénombrement des points en utilisant les améliorations d'Atkin et d'Elkies, ce qui a donné lieu à l'algorithme S.E.A.

En utilisant cet algorithme, un nouveau record [21] a été annoncé le 26/11/2006 par F.Morain, permettant de calculer le cardinal de la courbe elliptique:

$$E : y^2 = x^3 + 4589x + 91128 \text{ modulo } p = 10^{2499} + 7131$$

qui est $\#E = p + 1 - a$ avec
a = 90292932371132482786949150770587475516693215732338830236781058120\
86157561659588940358775745866172773431898251944841561968158533187342 3\
86451010042079574311991522324244885259324275360356018387099873453524 1\
90337127734742616052957456139347848273032219281963368357568573186063 3\
30859472313340463370165034764260993170876499703763557640712637346542 8\
61635530248560688747230776560970782387372349274130452135885965128390 7\
03779853746144223235045275340826091926290612524515094221467986424645 5\
11793004805487116360047431376657953293805586016188358341987968688933 9\
12932041213536620068401362096449335889632073987400880836072043167819 4\
35435301254203874045015052903920000684954273930329146242200332391479 2\
61419450212412234359567926125956045661604383975789837928136025620011 7\
98249384004045008584520449871951575828394360571538638262212279062566 0\
82789503189389888533081257831399326969461811284372534591159778680258 2\
64252916301362853676864774949480662948026993998954835831387765095297 1\
44723348697799906289840994365491033569740327060706750249114604748474 6\
52942090296113230374057634336407195747708572709834152984206107126756 0\
08468830444900096128819421831993330186896198507602922873338235789659 4\
01987876050689627089477490717366754410230986360942010122625495852602 5\
30360613170

Ce cardinal contient 2500 chiffres décimaux

Chapitre 3

Factorisation et primalité avec les courbes elliptiques

3.1 Introduction

Dans ce chapitre, nous présentons le test de primalité de Goldwasser-Kilian (1986). Ce test est basé sur le critère de Pocklington-Lehmer. Nous présentons également la méthode de factorisation ECM[1] de H.W.Lenstra (1985). Cette méthode est un algorithme qui présente de grandes similitudes avec l'algorithme de factorisation $(p-1)$ de Pollard. C'est la meilleure méthode, connue à ce jour, qui permet d'extraire des facteurs premiers p de taille modérée, c'est-à-dire, $p < 10^{60}$, avec une complexité de $O(p) = e^{\sqrt{(2+o(1))\ln p \ln\ln p}}$. Elle est donc utilisé par les logiciels de calcul numérique comme SAGE, Maple et Magma. Le record du plus grand facteur par la méthode ECM est :

$$165598199251072799631805738859758610717629818982386167243844257989325146883490202 87.$$

Il a été découvert par R. Propper le 07 Septembre 2013 [14]. C'est un facteur du nombre $7^{337}+1$ à 83 chiffres.

3.2 Historique des tests de primalité

Définition 48 *Un nombre premier est un entier naturel $p > 1$ ayant exactement deux diviseurs (positifs) : 1 et p.*
Un nombre composé est un entier naturel $n > 1$ qui n'est pas premier.

[1] Elliptic Curve Method

Qu'en est-il pour $2^{127} - 1 = 170141183460469231731687303715884105727$? et comment reconnaître un nombre premier ?

Il existe des algorithmes très performants pour prouver qu'un entier est premier avec une forte probabilité. De tels algorithmes sont appelés tests de primalité. Nous allons voir certains d'entre eux.

a. La méthode des divisions successives (250 Av. JC)

Pour tester si un nombre n est premier ou non, on peut effectuer les divisions par tous les nombres premiers successifs plus petit que $\sqrt{n}$. Si aucun de ces nombres ne divise n alors n est premier, sinon n est composé et on obtient même une factorisation. Cette méthode a été proposée par Eratosthène vers 250 Av. JC. Elle n'est pas efficace pour les grands nombres.

Le crible d'Ératosthène est un procédé qui permet de trouver tous les nombres premiers inférieurs à un certain entier naturel donné n. Son algorithme procède par élimination : il s'agit de supprimer de la table des entiers de 2 à n tous les multiples d'un entier. En supprimant tous les multiples, il ne restera que les entiers qui ne sont multiples d'aucun entier, et qui sont donc les nombres premiers.

b. Le test de Fermat(1640)

Théorème 49 (petit théorème de Fermat) *Soit p un nombre premier et a un entier premier avec p. Alors*

$$a^{p-1} \equiv 1 (\mathrm{mod}\, p)$$

Il est donc facile d'en déduire un test de non-primalité : si n est un entier donné, on choisit un nombre a premier avec n, et on calcule a^{n-1} : si on ne trouve pas 1 modulo n, c'est que n n'est pas premier. Ce test est très rapide, car on calcule a^{n-1} en effectuant au plus $2 \ln n$ opérations.

c. Test de Lucas (1876)

Théorème 50 *Soient a et $n \geq 2$ deux entiers tels que*

$$a^{n-1} \equiv 1 (\mathrm{mod}\, n).$$

On suppose que pour tout diviseur premier p de $n-1$

$$a^{\frac{n-1}{p}} \not\equiv 1 (\mathrm{mod}\, n).$$

Alors n est premier et tout élément non nul de $\mathbb{Z}/n\mathbb{Z}$ est une puissance de a.

Ce théorème fournit un test simple de primalité mais qui ne s'applique qu'à une petite classe d'entiers : les entiers n pour lesquels il est possible d'expliciter la factorisation de $n-1$.

d. Le critère de Pocklington (1914)

Le critère de Pocklington remonte à 1914 et fournit une condition suffisante à la primalité d'un nombre (voir 3.3.1). Il a été affiné par *Lehmer* (voir 3.3.2)

e. Test de Lucas-Lehmer (1930)

Le test de Lucas-Lehmer est un test de primalité pour les nombres de Mersenne. Le test fut originellement développé par Edouard Lucas en 1878 et amélioré de façon notable par Derrick Henry Lehmer dans les années 1930.

Définition 51 (Nombres de Mersenne) *Pour tout entier naturel n, on appelle n-ième nombre de Mersenne le nombre entier M_n défini par*

$$M_n = 2^n - 1$$

Théorème 52 *Soit la suite d'entier $(L_n)_{n\in\mathbb{N}}$ définie par:*

$$\left\{ \begin{array}{l} L_0 = 4 \\ L_n = L_{n-1}^2 - 2 \quad pour \quad n \geq 1 \end{array} \right\}$$

Pour tout entier $n \geq 3$, le nombre de Mersenne $M_n = 2^n - 1$ est premier si et seulement si on a $L_{n-2} \equiv 0 (\mathrm{mod}\, M_n)$.

En février 2013, 48 nombres premiers de Mersenne étaient connus. Le plus grand identifié à ce jour, a été mis à jour le 25 janvier 2013 par une équipe de l'université de Central Missouri [22]. Ce nombre premier, qui vaut $2^{57885161} - 1$, comporte plus de 17 millions de chiffres (précisément, il en contient 17 425 170). Le précédent record, datant de 2008, comportait moins de 13 millions de chiffres.

f. Algorithme de Solovay-Strassen (1977)

Cet algorithme utilise le symbole de *Jacobi*. Soit n un entier impair, $n > 1$, et a un entier quelconque. Si n est premier, et a est premier avec n, alors $\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} (\mathrm{mod}\, n)$ (c'est le théorème d'*Euler*). Mais si n est un entier composé, il est possible que cette égalité soit tout de même vérifiée, on dit alors que n est pseudo-premier en base a. Par exemple $\left(\frac{10}{91}\right) = -1 \equiv 10^{45} (\mathrm{mod}\, 91)$ et $91 = 7 \times 13$. D'où le test de primalité suivant :

Pour a allant de 1 à $n-1$

- Calculer $\left(\frac{a}{n}\right)$.

- Calculer $a^{\frac{n-1}{2}}$.

- Si ces deux nombres sont différents, afficher "n est composé".

Fin Pour.

Si le programme n'affiche pas "n est composé", c'est que le nombre testé est premier.

g. Test de Miller-Rabin(1980)

Le test de *Miller-Rabin* est en fait une modification du test de *Fermat*. Il est donné par le théorème suivant :

Théorème 53 *Soit n un nombre premier impair et a un entier premier à n.* Si $n-1$ *est un nombre premier à n. Si $n-1=2^e q$, où q est un entier impair, alors*

1. Soit $a^q \equiv 1 (\mathrm{mod}\, n)$
2. Soit il existe $r \in \{0, 1, \ldots, e-1\}$ tel que $a^{2^r q} \equiv -1 (\mathrm{mod}\, n)$.

la réciproque est fausse, comme le montre l'exemple où $n = 3277$ et $a = 2$. Si un entier $a \in \{1, \cdots, n-1\}$ vérifie l'une des propriétés (1) ou (2) du théorème de Rabin-Miller, on dit que n est pseudo-premier (de Miller-Rabin) pour la base a.

Ce test est un renforcement du test de Fermat.

h. Test ECPP[2](1986)

En 1986 *Goldwasser et Kilian* ont donné une première version théorique de cet algorithme basée sur l'algorithme donné par Schoof (voir chapitre 2) pour calculer le nombre de points d'une courbe elliptique sur un corps fini.

Ensuite A.O.L Atkin a remplacé l'utilisation de cet algorithme par la construction de courbes elliptiques particulières dont on peut calculer plus simplement le nombre de points.

Ce test est considéré comme le plus rapide pour de très grands nombres sous forme particulière et le meilleur algorithme déterministe de test de primalité connu.

Avec ce test, le record actuel est dû à *Fracnçois Morain* [12] qui en Avril 2011 a montré la primalité d'un nombre de 26642 chiffres décimaux qui est

60336838787923722145 . . . (26602 autres chiffres) . . . 97795227069490003443.

Le calcul distribué avec un logiciel conçu par *François Morain* a commencé en Janvier 2011 et s'est terminé en Avril 2012.

Le temps d'exécution cumulé à un processeur est de 2255 jours (plus de 6 ans).

[2] Elliptic Curve Primality Proving

i. Test AKS[3](2002)

Au début du mois d'août 2002 [8], trois chercheurs de l'*Indian Institute of Technology*, soit le professeur *Marindra Agrawal* et ses deux étudiants *Neeraj Kayal* et *Nitin Saxena*, ont annoncé la découverte d'un test de primalité dont le nombre d'étapes est borné approximativement par d^{12}, où d est le nombre de chiffres du nombre testé. En 2004, ils ont réduit ce nombre d'étapes à d^6.

Ce nouveau test des trois indiens est d'autant plus remarquable qu'il n'utilise que des notions de théorie élémentaire des nombres, soit le petit théorème de Fermat ($a^p \equiv a(\mathrm{mod}\, p)$) pour tout entier positif a et tout nombre premier p) et le fait que $(x+y)^p \equiv x^p + y^p(\mathrm{mod}\, p)$ pour tout nombre premier p.

3.3 Test de primalité basé sur les courbes elliptiques

Le test de primalité utilisant les courbes elliptiques est une variante du test de Pocklington dans $(\mathbb{Z}/n\mathbb{Z})^*$ [1], [2].

3.3.1 Critère de Pocklington

Théorème 54 *Soit $n \in \mathbb{N}^*$. Notons $n-1 = \prod_{j=1}^{n} p_j^{e_j}$, la décomposition de $n-1$ en facteurs premiers. S'il existe un entier a_{p_i}, $i \in \{1, 2, \ldots, n\}$, tel que : $a_{p_i}^{n-1} \equiv 1(\mathrm{mod}\, n)$ et $(a_{p_i}^{(n-1)/p_i} - 1) \wedge n = 1$,*
alors :
Si d est un facteur de n, $d \equiv 1(\mathrm{mod}\, p_i^{e_i})$.

Démonstration. Comme tout facteur d de n est le produit de nombres premiers, il suffit de démontrer le théorème pour tout facteur premier q de n. Comme $a_{p_i}^{n-1} \equiv 1(\mathrm{mod}\, n)$, il s'ensuit que $un + a_{p_i}^{n-2} a_{p_i} = 1$. Cela signifie que $\mathrm{pgcd}(a_{p_i}, n) = 1$ et $\mathrm{pgcd}(a_{p_i}, q) = 1$. Nous avons donc $a_{p_i}^{q-1} \equiv 1(\mathrm{mod}\, q)$ d'après le petit théorème de Fermat. Notons o_i l'ordre de a_{p_i} modulo q (o_i est la plus petite puissance positive telle que $a_{p_i}^{o_i} \equiv 1(\mathrm{mod}\, q)$), alors la relation précédente implique que $o_i | q-1$. D'autre part, comme $a_{p_i}^{n-1} \equiv 1(\mathrm{mod}\, n)$ et $(a_{p_i}^{\frac{n-1}{p_i}} - 1) \wedge n = 1$, nous avons

$$\begin{gathered} a_{p_i}^{n-1} \equiv 1(\mathrm{mod}\, n) \\ \text{et} \quad a_{p_i}^{\frac{n-1}{p_i}} \not\equiv (1 \,\mathrm{mod}\, q) \end{gathered}$$

$$\Longrightarrow o_i | p_i^{e_i} \prod_{j=1, j\neq i}^{n} p_j^{ej} \text{ et } o_i \nmid p_i^{e_i - 1} \prod_{j=1, j\neq i}^{n} p_j^{e_j}$$

[3] Agrawal Kayal Saxena

$\Longrightarrow \exists(\alpha,\beta)\in\mathbb{N}^*,\ o_i\alpha = p_i^{e_i}M$ et $o_i\beta \neq p_i^{e_i-1}M$ où $M=\prod_{j=1,j\neq i}^{n} p_j^{e_j}$
$\Longrightarrow \alpha \neq p_i\beta$
$\Longrightarrow p_i^{e_i}|o_i$
Finalement, nous avons $p_i^{e_i}|o_i|q-1$ et donc $q\equiv 1(\mathrm{mod}\, p_i^{e_i})$. ■

Corollaire 55 *Si q est un facteur premier de $n-1$ strictement supérieur à $\sqrt{n}-1$, s'il existe un entier a vérifiant $a^{n-1}\equiv 1(\mathrm{mod}\, n)$ et $\mathrm{pgcd}(a^{\frac{n-1}{q}}-1,n)=1$, alors n est premier.*

Le critère de Pocklington a été affiné par Lehmer de la manière suivante :

3.3.2 Le critère de Pocklington-Lehmer

Corollaire 56 *Soit n un entier assez grand. S'il existe $(F,U)\in\mathbb{N}^2$ tel que :*

1. $n-1=FU$
2. $F\wedge U=1$
3. $F>\sqrt{n}-1$
   et pour tout facteur premier p de F, il existe a_p tel que : $a_p^{n-1}\equiv 1(\mathrm{mod}\, n)$ et $(a_p{}^{\frac{n-1}{p}}-1)\wedge n=1$, alors n est premier.

Démonstration. On pose que $a_p^{n-1}\equiv 1(\mathrm{mod}\, n)$ et $((a_p{}^{\frac{n-1}{p}}-1)\wedge n)=1$.
D'après le théorème 54, tout facteur de n est congru à 1 modulo F.
Les facteurs de n sont donc de la forme $\alpha F+1$ (avec $\alpha\in\mathbb{N}^*$). Or comme $F>\sqrt{n}-1$ tout facteur de n est strictement supérieur à $\sqrt{n}$.
Donc n est premier. ■

Exemple 57 *Nous voulons prouver la primalité de $n=153533$*
$n-1=153532=2^2.131.293$. *On prend $F=2^2.131$ et $U=293$*
$F\wedge U=2^2.131\wedge 293=1$.
$2^2.131>\sqrt{153533}-1\simeq 390,83$.
Les facteurs premiers de F sont 2 et 131.
On prend $a_2=a_{131}=2$ et on a
$a_2^{n-1}=2^{153532}\equiv 1(\mathrm{mod}\, 153533)$ *et*
$(a_2{}^{\frac{n-1}{2}}-1)\wedge n=(2^{2.131.293}-1)\wedge 153533=1$ *et*
$(a_{131}^{\frac{n-1}{131}}-1)\wedge n=(2^{2^2.293}-1)\wedge 153533=1$.
d'où, 153533 est un nombre premier. Mais pour faire la preuve complète, il faut prouver que 131 est premier. On va utiliser le critère Pocklington-Lehmer pour la deuxième

fois.
On a $130 = 2.5.13$ *, on prend* $F = 13$ *et* $U = 2.5$ *.*
$F \wedge U = 13 \wedge 2.5 = 1$ *et* $13 > \sqrt{131} - 1 \cong 10,45$.
On choisi $a_{13} = 2$ *qui vérifie*
$a_{13}^{n-1} = 2^{130} \equiv 1 (\mathrm{mod}\, 131)$ *et* $(a_{13}^{\frac{n-1}{13}} - 1) \wedge n = 2^{2.5} - 1 \wedge 131 = 1$.
Ainsi 131 *est premier.*

3.3.3 Critère de Goldwasser-Kilian

Le critère de Goldwasser est le critère de Pocklington adapté aux courbes elliptiques. Il a été inventé par Shafi Goldwasser et Joe Kilian en 1986 [23]. Soit n un entier tel que $\mathrm{pgcd}(n, 6) = 1$. $E : y^2 = x^3 + ax + b$, une courbe elliptique définie sur $\mathbb{Z}/n\mathbb{Z}$.

Proposition 58 *S'il existe un entier* m *et un point* P *de la courbe elliptique*

$$E : y^2 = x^3 + ax + b (\mathrm{mod}\, n)$$

tels que :

1. *Il existe un facteur premier* q *de* m *vérifiant* $q > (n^{\frac{1}{4}} + 1)^2$
2. $mP = O$
3. $\frac{m}{q}P = (x, y, z)$ *avec* $z \in (\mathbb{Z}/n\mathbb{Z})^*$.
   Alors n *est premier*

Démonstration. On fait un raisonnement par l'absurde. Supposons que n a un facteur premier p. On note E' la courbe elliptique modulo p, m' l'ordre de E' et P' le point de E' correspondant au point P de E.

Par hypothèse, $mP = O$ et $\frac{m}{q}P \neq O$ sur E. Donc, $mP' = O$ et $\frac{m}{q}P' \neq O$ sur E'. Alors l'ordre de P' divise m et ne divise pas $\frac{m}{q}$. Ceci implique que le nombre premier q divise l'ordre de P' comme point de E' et par suite q divise m' (théorème de Lagrange)[4]. D'après le théorème 27 (Hasse), il en résulte que : $q \leq m' \leq (\sqrt{p} + 1)^2 \leq (n^{\frac{1}{4}} + 1)^2$ car $p \leq \sqrt{n}$. Contradiction avec l'hypothèse. ■

La proposition 58 affirme que si nous déterminons un entier m satisfaisant les hypothèses $1, 2, 3$, alors n est premier, mais ne donne pas de méthode pour trouver un tel m. Cependant il est assez naturel de prendre $m = \#E(\mathbb{Z}/n\mathbb{Z})$. Ainsi l'hypothèse 2 sera automatiquement satisfaite. En fait on a la proposition suivante

[4] La théorème de Lagrange montre que l'ordre d'un élément divise toujours l'ordre de son groupe

Proposition 59 *Soit n un nombre premier tel que* $\text{pgcd}(n, 6) = 1$*, E une courbe elliptique définie sur $\mathbb{Z}/n\mathbb{Z}$ et soit $m = \#E(\mathbb{Z}/n\mathbb{Z})$. S'il existe un nombre premier q avec $q \mid m$ tel que $q > (n^{\frac{1}{4}} + 1)^2$.*
Alors il existe un point $P \in E(\mathbb{Z}/n\mathbb{Z})$ tel que $mP = O$ et $\frac{m}{q}P = (x, y, z)$ avec $z \in (\mathbb{Z}/n\mathbb{Z})^*$

Démonstration. Notons d'abord que tout point P satisfait $mP = O$. De plus, puisque n est premier, $z \in (\mathbb{Z}/n\mathbb{Z})^*$ veut dire que $z \neq 0$ et donc que $\frac{m}{q}P \neq O$.

Posons $G = E(\mathbb{Z}/n\mathbb{Z})$ et supposons par l'absurde que pour tout $P \in G$ nous avons $\frac{m}{q}P = O$. Alors l'ordre de G divise $\frac{m}{q}$.

Par le théorème 26 (Cassel) nous avons $G \cong \frac{\mathbb{Z}}{n_1\mathbb{Z}} \oplus \frac{\mathbb{Z}}{n_2\mathbb{Z}}$ avec n_1 divise n_2 ($n_1 = 1$ si G est cyclique). Ainsi l'ordre de G est n_2, puisque $\#G = n_1 n_2 \leq n_2^2$.

Nous avons donc

$$m = \#G \leq n_2^2 \leq \left(\frac{m}{q}\right)^2$$

Ce qui veut dire que $q^2 \leq m$. Utilisant notre hypothèse sur la taille de q et le théorème 27 de Hasse, nous avons

$$(n^{\frac{1}{4}} + 1)^2 < \sqrt{n} + 1$$

Ce qui est absurde. ■

Remarque 60 *Nous faisons tous les calculs comme si n était premier.*
La cardinalité de $E(\mathbb{Z}/n\mathbb{Z})$ se calcule avec l'algorithme de Schoof que nous avons déjà vu dans le chapitre 2. S'il n'aboutit pas alors cela signifie que n est composé.
De même, dans le calcul de mP et de $\frac{m}{q}P$, il est possible que le dénominateur dans le calcul de λ (la pente de la tangente au point P) ne soit pas inversible, cela signifie que $\mathbb{Z}/n\mathbb{Z}$ n'est pas un corps et donc que n est composé.

Algorithme 61 *Ce test a été utilisé pour prouver la primalité d'un nombre n. Soit n un entier positif différent de* 1 *et premier avec* 6*. Si n n'est pas premier, l'algorithme le détectera ou tournera indéfiniment. C'est pourquoi il faut absolument utiliser le test de Rabin-Miller[5] avant d'utiliser cet algorithme [2].*

1. *Posons $i \leftarrow 0$ et $n_i \leftarrow n$.*
2. *Si $n_i < 2^{30}$, diviser par tous les premiers jusqu'à 2^{15}. Si n_i n'est pas premier aller à l'étape* 9*.*

[5] Pour plus de détails sur le test de Rabin-Miller, le lecteur peut voir ([2] page 422)

3. *Choisir a et b dans $\mathbb{Z}/n_i\mathbb{Z}$ et vérifier que $4a^3 + 27b^2 \in (\mathbb{Z}/n_i\mathbb{Z})^*$. poser $E : y^2 = x^3 + ax + b$.*

4. *Avec l'algorithme de Schoof, calculer $m \leftarrow \#E(\mathbb{Z}/n_i\mathbb{Z})$. Si l'algorithme de Schoof bloque, aller à l'étape 9.*

5. *Diviser m par des petits nombres premiers dont on note m' le facteur qu'on a trouvé. On suppose $m = m'q$ avec $q > (n^{\frac{1}{4}} + 1)^2$ ayant passé le test de Rabin-Miller. Si ce n'est pas le cas, aller à l'étape 3.*

6. *Choisir un $x \in \mathbb{Z}/n_i\mathbb{Z}$ tel que le symbole de Legendre*[6] $(\frac{x^3 + ax + b}{n_i}) = 0$ *ou* 1. *Utiliser l'algorithme de Tonelli-Shanks*[7] *pour trouver $y \in \mathbb{Z}/n_i\mathbb{Z}$ tel que $y^2 = x^3 + ax + b$. Si l'algorithme bloque, aller à l'étape 9.*

7. *Calculer $P_1 \leftarrow mP$ et $P_2 \leftarrow \frac{m}{q}P$. Si pendant les calculs une division était impossible, aller à l'étape 9. Sinon vérifier si $P_1 = O$. si $P_1 \neq O$, aller à l'étape 9. Si $P_2 = O$, aller à l'étape 6.*

8. *Poser $i \leftarrow i + 1$ et $n_i \leftarrow q$ et aller à l'étape 2.*

9. *Si $i = 0$, n est composer, on arrête. Sinon, poser $i \leftarrow i - 1$ et aller à l'étape 3.*

Exemple 62 *Supposons que nous voulons prouver la primalité de* 1283 *qui a passé avec succès le test de Miller-Rabin.*
On a $\text{pgcd}(1283, 6) = 1$.
Considérons la courbe elliptique $E : y^2 = x^3 - x (\text{mod}\, 1283)$.
Le point $P(121, 30) \in E$.
Avec l'algorithme de Schoof $m = \#E = 1284$.
Comme $m = 1284 = 12.107$, *vérifions les hypothèses de la proposition 58.*

1. $q = 107$ *est premier et* $107 > (1283^{\frac{1}{4}} + 1)^2 \simeq 49$

2. $1284P = 2(2(P + 2(2(2(2(2(P + 2(2P))))))))) = O$

3. $1284/107P = 12P = 2(2(P+2P)) = 2(2((121, 30)+(1066, 377))) = 2(2(1083, 1155) = 2(704, 284) = (903, 1038) \neq O$.

Alors nous avons prouvé que 1283 *est premier.*

[6] Si p un nombre premier impair et a un entier, alors le symbole de Legendre $(\frac{a}{p})$ vaut :
1) 0 si p divise a
2) $+1$ si a est un résidu quadratique modulo p.
3) -1 si non

[7] C'est un algorithme pour calculer la racine carré dans F_p (voir [2] pages 32,34)

3.4 Historique des méthodes de factorisation

Il y a plusieurs méthodes pour factoriser un nombre :

a. Divisions successives (250 Av. JC)

Nous avons vu déjà dans le paragraphe 3.2 que cette méthode de factorisation est inéfficace.

b. Méthode (p-1) de Pollard(1974)

Cette méthode est particulièrement adaptée pour trouver des facteurs premiers p tels que $p-1$ n'a que des petits diviseurs premiers. conçu par John Pollard en 1974 (Plus précisément voir la partie 3.5.1).

c. Méthode Rho de Pollard (1975)

Elle est seulement effective pour factoriser des entiers avec des petits facteurs. Il fut conçu par *John M. Pollard* en 1975.

d. La méthode de Dixon (1981)

La méthode de Dixon est basée sur la recherche d'une congruence de carrés. La méthode naïve de recherche d'une telle congruence est la sélection aléatoire de valeurs x satisfaisant la congruence

$$x^2 \equiv y^2 (\mathrm{mod}\, n) \qquad \text{et} \qquad x \equiv \pm y (\mathrm{mod}\, n)$$

Où n est l'entier à factoriser. Dans la pratique, sélectionner aléatoirement les valeurs de x pour trouver une congruence de carrés prendra enormément de temps.

Cette méthode est intéressante du point de vue théorique mais elle n'a jamais été utilisée en pratique.

e. La méthode du crible quadratique (1981)

C'est l'une des méthodes de factorisation les plus efficaces. L'algorithme mis au point en 1981 par *Carl Pomerance*, est un raffinement de la méthode de factorisation de *Dixon*, elle-même basée sur celle de *Fermat*: on essaye d'établir une congruence de carrés module n (l'entier à factoriser) qui souvent, conduit bien à une factorisation de n.

f. Algorithme (p+1) de William (1982)

Il a été inventé par *Hugh.C.William* en 1982. Cela fonctionne bien si le nombre à factoriser n possède un ou plusieurs facteurs premiers p tel que $(p+1)$ possède seulement des petits facteurs.

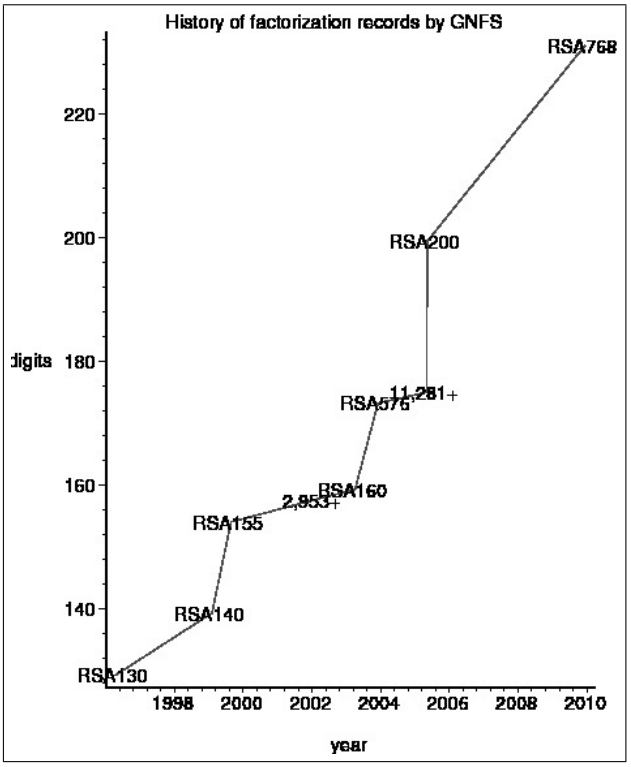


Figure 3.1: Histoire des records de factorisation par GNFS

g. Le crible du corps des nombres (GNFS[8])(1988)

Lancée en 1988 par *John Pollard*. Cette nouvelle méthode était à l'origine destinée à factoriser des nombres de forme particulière, par exemple $2^k \pm 1$. Elle attire l'attention lorsqu'en 1990, les frères *Lenstra* et *Manasse* l'utilisèrent pour factoriser le nombre de Fermat $F_9 = 2^{2^9} + 1$ qui a 155 chiffres (les nombres de Fermat sont sous forme $F_i = 2^{2^i} + 1$).

Par exemple, l'annonce de factorisation [13] de RSA-768 (c'est un entier n de 232 chiffres décimaux) en janvier 2010 est

$n = 123018668453011775513049495838496272077285356959533479219732245215172640050726365751874520219978646938995647494277406384592519255732630345373154826850791702612214291346167042921431160222124047927473779408066535141959745985690214341 3$

Peut se factoriser comme

$$n = p \times q$$

où

$p = 33478071698956898786044169848212690817704794983713768568$

[8] General Number Field Sieve

$$912431388982883793878002287614711652531743087737814467999489$$
$$q = 367460436667995904282446337996279526322791581643430876426760322838157396665112792333734171433968102700927987363089 17$$

Les facteurs p, q ont 384 bits[9] et 116 chiffres décimaux. (voir FIG 3.1).

Le crible du corps de nombres est une méthode meilleure que celle du crible quadratique.

3.5 Méthode de factorisation (ECM)

Etant donné un nombre naturel n, la méthode consiste à trouver un facteur premier de n. Cet algorithme présente de grandes similitudes avec l'algorithme de factorisation $(p-1)$ de Pollard.

Avant de décrire en détail la méthode ECM, nous rappelons la méthode $(p-1)$ de Pollard [4].

3.5.1 Méthode $(p-1)$ de Pollard

Définition 63 (B-lissité) *Soit $n \in \mathbb{N}$, $n = \prod_{i=1}^{m} p_i^{\alpha_i}$ la décomposition de n en facteurs premiers.*
*n est dit B-**lisse** si est seulement si:*

$$\forall i \in \{1, 2, \ldots, m\}, \quad p_i \leq B$$

*n est dit B-**superlisse** si est seulement si:*

$$\forall i \in \{1, 2, \ldots, m\}, \quad p_i^{\alpha_i} \leq B.$$

Ainsi $30 = 2.3.5$ est B-superlisse pour $B = 5, 7$. Mais $150 = 2.3.5^2$ n'est pas 5-superlisse (il est 25-superlisse).

Soit n un entier positif. Pour factoriser n, on va utiliser la méthode $(p-1)$ de Pollard. Pour cela, on choisit un entier positif B, en pratique $B \leq 10^6$. On suppose qu'il existe un diviseur premier p de n tel que $p-1$ est B-superlisse. On essaie de trouver p en utilisant ce qui suit. Si $a > 1$ est un entier non divisible par p, alors d'après le petit théorème de Fermat

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

On a alors $(p-1) \mid \mathrm{ppcm}(1, 2, \ldots, B)$

$$a^{\mathrm{ppcm}(1,2,\ldots,B)} \equiv 1 (\mathrm{mod}\, p).$$

[9] Le bit est un chiffre binaire, c'est-à-dire 0 ou 1

Par conséquent

$$l = [(a^{\text{ppcm}(1,2,\ldots,B)} - 1) \wedge n] > 1.$$

Si $l \neq n$, on a alors trouvé un facteur non trivial de n, sinon on calcule l pour une autre valeur de a ou alors on diminue la valeur de B.

Algorithme 64 ((p-1) de Pollard) *Soit n un nombre entier positif et B une borne. Cet algorithme permet de trouver un facteur l non trivial de n tel que chaque nombre premier p divisant l vérifie que $(p-1)$ est B-superlisse.*

1. *Calculer* $m = \text{ppcm}(1, 2, \ldots, B)$
2. *Poser* $a = 2$
3. *Calculer* $x = a^m - 1 (\text{mod } n)$ *et* $l = \text{pgcd}(x, n)$
4. *Si* $1 < l < n$, *alors* l *est un facteur de* n, *on arrête.*
5. *Si* $l = n$ *et* $a < 10$ *remplacer* a *par* $a + 1$ *et aller à l'étape 3. Sinon on arrête.*
6. *Si* $l = 1$, *sélectionner un* B *plus grand et aller à l'étape 1. Sinon on arrête.*

Exemple 65 *Soit* $n = 5917$. *On pose* $B = 5$ *et* $a = 2$
$\text{ppcm}(1, 2, 3, 4, 5) = 60$ *et* $2^{60} - 1 \equiv 3416 (\text{mod } 5917)$.
$\text{pgcd}(2^{60} - 1, 5917) = \text{pgcd}(3416, 5917) = 61$.
Ainsi 61 *est un facteur de* 5917.

Exemple 66 *Dans cet exemple, on remplace n par un nombre entier plus grand.*
Soit $n = 779167$ *avec* $B = 5$ *et* $a = 2$.
On a $2^{60} - 1 \equiv 710980 (\text{mod } 779167)$ *et* $\text{pgcd}(2^{60} - 1, 779167) = 1$.
Maintenant on essaie avec $B = 15$ *on trouve* $\text{ppcm}(1, 2, \ldots, 15) = 360360$.
$2^{360360} - 1 \equiv 584876 (\text{mod } 779167)$ *et* $\text{pgcd}(2^{360360} - 1, n) = 2003$.
Donc 2003 *est un facteur non trivial de* 779167.

Exemple 67 *Dans cet exemple, on remplace n par un nombre entier plus petit.*
Soit $n = 4331$ *avec* $B = 7$ *et* $a = 2$.
$\text{ppcm}(1, 2, \ldots, 7) = 420$ *et* $2^{420} - 1 \equiv 0 (\text{mod } 4331)$,
et $\text{pgcd}(2^{420} - 1, 4331) = 4331$
Donc on ne peut pas obtenir un facteur de n.
Remplacer B *par* 5, *on trouve*
$2^{60} - 1 \equiv 1464 (\text{mod } 4331)$ *et* $\text{pgcd}(2^{60} - 1, 4331) = 61$.
Donc on a factorisé 4331.

Exemple 68 *Dans cet exemple, on va voir que* $a = 2$ *ne marche pas mais* $a = 3$ *marche.*

Soit $n = 187$*,* $B = 15$ *et* $a = 2$ *alors* $\text{ppcm}(1, 2, \ldots, 15) = 360360$.

$2^{360360} - 1 \equiv 0 (\text{mod } 187)$ *et* $\text{pgcd}(2^{360360} - 1, 187) = 187$.

Donc on ne peut pas obtenir un facteur de 187*. Si on remplace* $a = 2$ *par* $a = 3$*, la méthode de Pollard va bien marcher.*

$3^{360360} - 1 \equiv 66 (\text{mod } 187)$ *et* $\text{pgcd}(3^{360360} - 1, 187) = 11$.

Alors $187 = 11.17$.

3.5.2 L'idée de la méthode des courbes elliptiques

En 1980, un algorithme de factorisation basé sur les courbes elliptiques a été mis au point. C'est un algorithme très efficace pour factoriser les nombres de l'ordre de 10^{60} et de plus grands nombres s'ils ont des facteurs premiers de l'ordre de 10^{20} à 10^{30}.

Cette méthode est basée sur la méthode $(p-1)$ de Pollard en remplaçant le groupe multiplicatif $\mathbb{F}_p^*$ par le groupe des points d'une courbe elliptique. Pour trouver un diviseur non trivial d'un entier n, on choisit une courbe elliptique $E \pmod n$, un point P de la courbe à coordonnées $(\text{mod } n)$ et un entier $m = ppcm(2, 3, \cdots, B)$. On calcule mP en espérant qu'il existe un diviseur premier p de n pour lequel mP et l'élément neutre O de la courbe soient égaux $(\text{mod } p)$.

3.5.3 Méthode de Lenstra (ECM)

Soit n le nombre que nous voulons factoriser. L'idée est de regarder une courbe elliptique E sur l'anneau $\mathbb{Z}/n\mathbb{Z}$ de manière naïve, c'est-à-dire en réduisant les coefficients et les coordonnées des points sur cette courbe elliptique modulo n. Pour additionner deux points, nous calculons la pente de la droite passant par ces points et la réduisant modulo n. C'est pourquoi nous n'utiliserons pas la notation $E(\mathbb{Z}/n\mathbb{Z})$ mais $E(\text{mod } n)$.

Il est clair que si n n'est pas premier, cette pente n'existera pas toujours car les nombres qui ne sont pas premier avec n ne sont pas inversibles modulo n. L'idée clé de cette méthode est justement se retrouver dans une telle situation. En effet, dans ce cas nous aurons une pente dont le dénominateur d n'est pas inversible modulo n, ce qui veut dire que $\text{pgcd}(n, d) \neq 1$ et nous aurons trouvé un facteur non trivial de n.

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 $a_i (\text{mod } n)$ et des points $P_i(x_i, y_i) (\text{mod } n)$. Nous définissons ensuite les b_i tels que

$$b_i = y_i^2 - x_i^3 - a_i x_i (\text{mod } n)$$

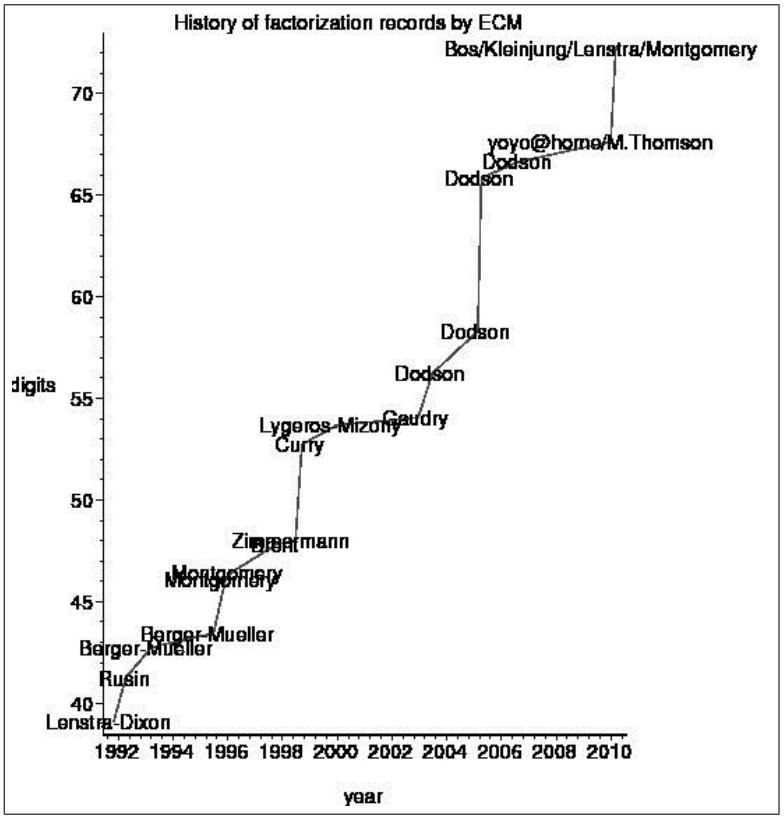


Figure 3.2: Histoire des records de factorisation par ECM

Nous obtenons ainsi des courbes elliptiques $E_i : y^2 = x^3 + a_i x + b_i$ avec des point P_i. Cette méthode est beaucoup plus efficace que de choisir des entier a_i, b_i, x_i et ensuite de chercher y_i, puisque calculer la racine carrée modulo n est équivalent à factoriser n.

Voici les étapes du déroulement de la méthode de Lenstra pour la factorisation d'un entier n.

Algorithme 69 (de Lenstra) *Pour factoriser un entier n avec la méthode des courbes elliptiques, nous pouvons procéder comme suit :*

1. *Choisir entre dix et vingt courbes elliptiques $E_i : y^2 = x^3 + a_i x + b_i$ et des points $P_i \pmod n$ sur les courbes E_i par la méthode énoncée ci-dessus*
2. *Choisir un entier B (de l'ordre de 10^8) et calculer $(B!)P_i$ sur E_i pour chaque i.*
3. *Si l'étape 2. bloque parce que l'une des pentes n'existe pas modulo n, alors nous avons trouvé un facteur de n.*

4. Sinon augmenter la valeur de B ou recommencer à l'étape 1.

Cette méthode est très efficace pour trouver des facteurs premiers p de n lorsque $p < 10^{60}$. Les valeurs de n qui sont utilisées en cryptographie sont généralement choisies telles que $n = p.q$ avec p et q de l'ordre de 10^{75}. Dans ce cas, cette méthode n'est plus efficace et il faut avoir recours à des méthodes plus performantes.

Remarque 70 (Choix de la borne de lissité) *On peut suivre le raisonnement suivant pour choisir la borne B :*
tout nombre composé a un diviseur premier inférieur à $\sqrt{n}$, si p est un facteur premier de n on a : $p < \sqrt{n}$.
De plus, d'après le théorème 27 de Hasse $\#E(\mathbb{F}_p) \leq (\sqrt{p}+1)^2$.
Il nous suffit donc de prendre $B \geq (n^{\frac{1}{4}}+1)^2$.

Remarque 71 *On a*

1. *Dans la pratique, pour des raisons de rapidité de calcul, on ne prend pas $k = \text{ppcm}(1, 2, \ldots, B)$ mais simplement $k = \text{ppcm}(B-1, B)$. Cela diminue la probabilité de trouver un facteur premier, mais améliore beaucoup la rapidité de l'algorithme.*

2. *Pour le choix de P dans la courbe elliptique $E : y^2 = x^3 + ax + b$, on peut poser $b = -a$, ce qui permet de prendre $P = (1, 1)$ qui appartient à la courbe elliptique.*

Exemple 72 *Pour factoriser 143 considérons $B = 3$ et la courbe elliptique :*

$$E : y^2 = x^3 + x + 1 (\text{mod}\, 143).$$

Soit le point $P = (0, 1)$ et $k = \text{ppcm}(1, 2, 3)$.
Essayons de calculer $6P$ avec les formules d'addition (Tableau 1.1).
On calcule $2P = P + P = (0, 1) + (0, 1) = (x_{2P}, y_{2P})$
On a

$$\lambda = \frac{3x_P^2 + a}{2y_P} \text{ et } \begin{array}{l} x_{2P} = \lambda^2 - 2x_P \\ y_{2P} = \lambda(x_P - x_{2P}) - y_P. \end{array}$$

Donc $\lambda = \frac{1}{2} \equiv 72 (\text{mod } 143)$,
$x_{2P} = 72^2 - 2.0 \equiv 36 (\text{mod } 143)$
$y_{2P} = 72(0 - 36) - 1 \equiv 124 (\text{mod}\, 143)$.
Donc $2P(36, 124)$
Maintenant on calcule $R = 3 \times (2P) = 2(2P) + (2P)$.
On a $2(2P) = 2P + 2P = (36, 124) + (36, 124) = (127, 71)$.
Donc $R = (127, 71) + (36, 124)$,

$\lambda = \frac{-53}{91}$ *car* $\text{pgcd}(91, 143) = 13 \neq 1$.

Donc 91 *ne possède pas un inverse.*

Donc le calcul de ces points est impossible et alors on obtient un facteur de 143.

$$143 = 13.11$$

Exemple 73 *Nous voulons factoriser* 4453*. On pose* $B = 3$*. Soit* E *la courbe elliptique d'équation :*

$$y^2 = x^3 + 3x (\text{mod}\, 4453).$$

Soit $P(1, 2)$*. Essayons de calculer* $6P$*.*

Calculons tout d'abord $2P$*.*

La pente de la tangente au point P *est :* $\lambda = \frac{3x_P^2 + a}{2y_P} = \frac{3}{2} \equiv 2228 (\text{mod}\, 4453)$.

En effet, $\text{pgcd}(2, 4453) = 1$.

Donc 2 *est inversible modulo* 4453 *et* $2^{-1} \equiv 2227 (\text{mod}\, 4453)$.

$$x_{2P} \equiv 3340 (\text{mod}\ \ 4453)$$
$$y_{2P} \equiv 1669 (\text{mod}\ \ 4453).$$

Nous calculons maintenant $3P$ *en additionnant* P *et* $2P$*.*

$$3P(x_{3P}, y_{3P}) = (1, 2) + (3340, 1669),$$
$$\lambda = \frac{1669 - 2}{3340 - 1} = \frac{1667}{3339}.$$

En effet

$$\text{pgcd}(3339, 4453) = 1.$$

Donc 3339 *est inversible modulo* 4453 *et* $3339^{-1} \equiv 1483 (\text{mod}\ 4453)$.

Alors

$$\lambda \equiv 746 (\text{mod}\, 4453).$$

D'où, les coordonnées de $3P$ *sont*

$$x_{3P} \equiv 1003 (\text{mod}\ \ 4453)$$
$$y_{3P} \equiv 610 (\text{mod}\ \ 4453).$$

Calculons maintenant $6P = 3P + 3P = (1003, 610) + (1003, 610)$

$$\lambda = \frac{3x_{3P}^2 + 3}{2y_{3P}} = \frac{3349}{1220}$$

Nous voyons $\text{pgcd}(1220, 4453) = 61 \neq 1$*. Ainsi nous ne pouvons pas inverser* $1220 (\text{mod}\, 4453)$ *et ne pouvons pas trouver la pente.*

Donc 61 *est un facteur de* 4453.

$$4453 = 61.73$$

Exemple 74 *Nous voulons factoriser* $n = 6887$. *Soit* $P = (1512, 3166)$ *et* $a = 14$ *donc*

$b = 3166^2 - 1512^3 - 14.1512 \equiv 19 (\text{mod } 6887)$.

Soit P *un point modulo* n *sur la courbe elliptique*

$$E : y^2 = x^3 + 14x + 19.$$

Nous calculons successivement

$$2P \equiv (3466, 2996)$$

$$3!P = 3.2P \equiv (3067, 396)$$

$$4!P = 4.(3!P) \equiv (6507, 2654)$$

$$5!P = 5.(4!P) \equiv (2783, 6278)$$

$$6!P = 6.(5!P) \equiv (6141, 5581).$$

Pour faciliter la notation, on met $Q = 6!P = (6141, 5581)$. *Nous utilisons la Méthode binaire pour calculer* $7Q = 7!P$ *(l'algorithme 15). Ainsi*

$$Q \equiv (6141, 5881),\ 2Q \equiv (5380, 174),\ 4Q = 2(2Q) \equiv (203, 2038),$$

et

$$7Q = (Q + 2Q) + 4Q$$

$$7Q \equiv ((6141, 5581) + (5380, 174) + (203, 2038) \equiv (984, 589) + (203, 2038).$$

Pour calculer la somme des deux derniers points, nous calculons la pente

$$\lambda = \frac{2038 - 589}{203 - 984}.$$

Donc il faut calculer l'inverse de $203 - 984 (\text{mod } 6887)$, *mais*
$\text{pgcd}(203 - 984, 6887) = 71$, *donc*

$$6887 = 71.97$$

3.5.4 Complexité de l'algorithme ECM

Se référer à *R. P. Brent* [10].

La complexité de cet algorithme est $e^{\sqrt{(2+o(1)) \ln p \ln \ln p}}$.

Cette complexité signifie que le temps nécessaire à l'algorithme pour trouver le facteur p de n est égal au temps mis pour réaliser $e^{\sqrt{(2+o(1)) \ln p \ln \ln p}}$ multiplications modulo n.

Conclusion

La primalité et la factorisation des grands nombres en utilisant les courbes elliptiques est actuellement un sujet en pleine expansion. Dans ce mémoire nous avons présenté l'algorithme de Schoof qui permet de calculer le nombre de points d'une courbe elliptique E sur un corps fini $\mathbb{F}_p$, c'est-à-dire le cardinal du groupe $E(\mathbb{F}_p)$ avec une complexité de $O(\log^8 p)$. R.Schoof a réécrit un article en 1995 [16] qui résume tout ce qui a été fait sur le dénombrement des points avec les améliorations d'Atkin et d'Elkies, ce qui a donné lieu à l'algorithme S.E.A (Schoof, Atkin, Elkies) avec une complexité de $O(\log^6 p)$. Ensuite nous avons vu comment prouver la primalité d'un nombre en utilisant le test de primalité de Goldwasser-Kilian et comment factoriser un entier avec la méthode de factorisation ECM. A la fin nous avons fait des applications sur le logiciel algébrique SAGE qui a pour ambition de devenir une alternative libre aux logiciels propriétaires comme Magma, Maple, Mathematica ou Matlab. Les problèmes de primalité et factorisation restent jusqu'à aujourd'hui des problèmes très difficiles à résoudre et trouver le meilleur algorithme de primalité ou factorisation est encore une préoccupation des cryptographes et mathématiciens.

Bibliographie

[1] L.C. Wachington. Elliptic Curves Number Theory end Cryptography – Second Edition- Chapman & Hall /CRC, 2008

[2] H. Cohen, A Course in Computational Algebraic Nunber Theory -3.corr.print- Springer, Heidelberg, 1996.

[3] J.H. Silverman. The Arithmetic of Elliptic Curves –Second Edition- Springer, Heidelberg, New Yourk, 2009.

[4] W. Stein, Elementray Number Theory, September 2004.

[5] Hagler Michael, Courbes elliptiques et Cryptographie, février 2006.

[6] Philippe Guillot, Courbes Elliptiques, Hermes-Lavoisier, 2010.

[7] L.Benferhat. Courbes elliptiques et formes modulaires. Cours de P.G 2012/2013. Fac Math. USTHB.

[8] M.Agrawal, N.Kayal, N.Saxena, PRIMES is in P. August 6, 2002.

[9] H.W.Lenstra, Jr. Factoring Integers With Elliptic Curves. Ann. of Math(2), 126(3) :649-673,1987.

[10] R.P.Brent. Some Integer Factorization Algorithms Using Elliptic Curves. 9th Australian Computer Science Conference, February 1986.

[11] Thomas Izard, Optimisation de la Multiplication Scalaire sur les Courbes Elliptiques pour de Petits Scalaires. Juin 2008.

[12] Le site web de Fracnçois Morain: `http://www.lix.polytechnique.fr/~morain`

[13] Laboratory for cryptologic algorithms - LACAL, site web: `http://lacal.epfl.ch/`

[14] 50 largest factors found by ECM, disponible online: `http://www.loria.fr/~zimmerma/records/top50.html`

[15] R. Schoof. Elliptic Curves over Finite Fields and the Computation of Square Roots mod p. Math. Comp., 44(170):483-494, 1985.

[16] R. Schoof. Counting points on elliptic curves over finite fields J. Théorie des Nombres de Bordeaux, 7: 219–254, 1995.

[17] Calcul mathématique avec Sage – version 1.0.9 – décembre 2011: `http://sagebook.gforge.inria.fr/`

[18] Tutoriel Sage – version – 5.2, 30 juillet 2012, disponible online sur le site officiel de Sage: `http://sagemath.org`.

[19] Le site web de Sage: `http://sagemath.org`

[20] Les courbes elliptiques de la base de données de Cremona, disponible online: `http://homepages.warwick.ac.uk/~masgaj/book/fulltext/table1.pdf`

[21] Les records de SEA: `http://www.lix.polytechnique.fr/~morain/sea.records.html`

[22] Le site web de GIMPS (Great Internet Mersenne Prime Search): `http://www.mersenne.org/`

[23] S.Goldwasser and J. Kilian. "Almost All Primes Can Be Quickly Certified." Proc. 18th STOC. pp. 316-329, 1986. disponible online: `http://groups.csail.mit.edu/cis/pubs/shafi/1986-stoc-gk.pdf`

Annexe A

Applications sur le logiciel algébrique SAGE

A.1 Introduction

Le logiciel Sage (*Software for Algebra and Geometry Experimentation*) est un logiciel de mathématiques qui rassemble de nombreux programmes et bibliothèques libres dans une interface commune basée sur le langage de programmation Python [17], [18], [19].

Il a pour ambition de devenir une alternative libre aux logiciels propriétaires comme Magma, Maple, Mathematica ou Matlab.

Ce logiciel s'inscrit dans un environnement de logiciels dédiés aux mathématiques tels que la Théorie des Nombres, la Théorie des Graphes, la Cryptographie...etc.

La particularité de Sage est d'être distribué sous licence libre, selon les termes de la GNU General Public License (GPL) version 2 ou ultérieure. Cette dernière autorise la copie, l'étude, la modification, l'amélioration et la distribution de Sage et de son code source.

Dans cette annexe, nous présentons le système algébrique SAGE que nous avons utilisé pour effectuer les calculs des exemples étudiés dans les chapitres deux et trois.

A.2 Composants de Sage

Sage rassemble une grande quantité de logiciels et de bibliothèques spécialisées sous une même interface.

Il intègre notamment le logiciel d'algèbre GAP, le langage de calcul Octave, le logiciel de statistique R, le logiciel d'arithmétique pari/GP, le logiciel pour l'algèbre commutative et non commutative et de manipulation de polynômes multi variés Singular, le logiciel de calcul formel Maxima. Il comprend aussi le logiciel GMP-ECM pour la factorisation des entiers en utilisant des courbes elliptiques, une librairie cryptographique généraliste Libgcrypt, ECLib pour l'énumération des courbes elliptiques.

Il offre également une interface avec les logiciels propriétaires Magma, Maple et Mathematica.

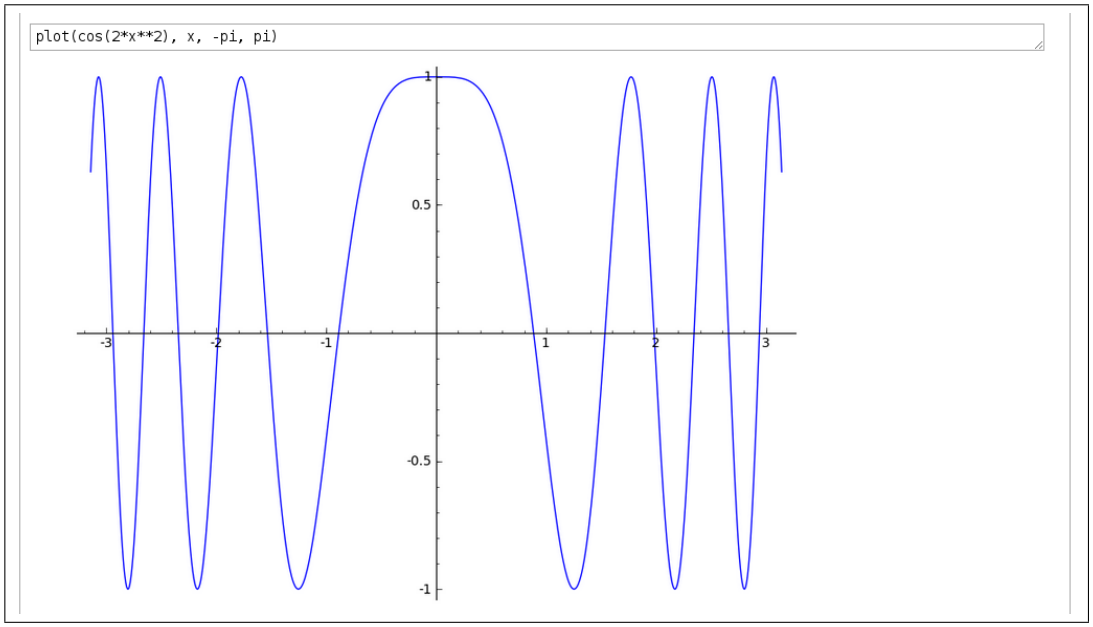


Figure A.1: Graphe de la fonction f(x)=cos(2x^2) sur Sage

A.3 Utilisation du logiciel Sage

Le logiciel Sage a plusieurs modes d'utilisation :

1. Il peut être utilisé en ligne de commande.
2. Il peut exécuter des programmes interprétés ou compilés.
3. Le mode le plus convivial est l'interface graphique notebook.

A.3.1 Premiers graphiques

La commande « plot » permet de tracer facilement la courbe représentative d'une fonction réelle sur un intervalle donné.

La commande « plot3d » sert aux tracés en trois dimensions, comme le graphe d'une fonction réelle de deux variables. Voici par exemple les commandes utilisées pour produire les graphiques qui apparaissent sur la capture d'écran en figures (4.1), (4.2).

```
sage: plot(cos(2*x**2), x, -pi, pi)
sage: plot3d(sin(pi*sqrt(x^2 + y^2))/sqrt(x^2+y^2),(x,-5,5), (y,-5,5))
```

Les capacités graphiques de Sage vont bien au-delà de ces exemples. Pour plus de détails sur ce sujet voir la référence [17], chapitre 5.

A.3.2 Aide en ligne

La touche de tabulation « tab » à la suite d'un début de mot montre quelles sont les commandes commençant par ces lettres :

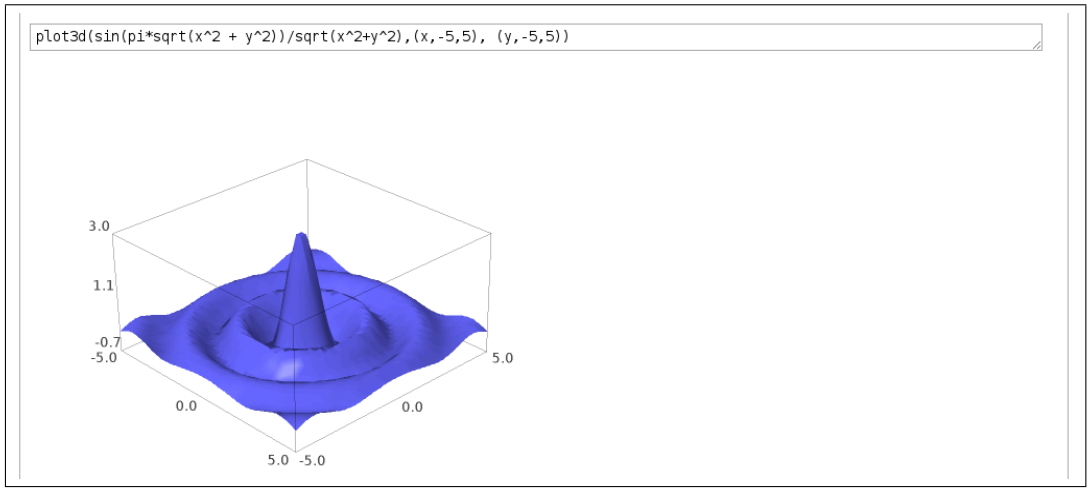


Figure A.2: Surface paramétrée en 3D sur Sage

`sage : Ellip`

Suivi de la touche « tab » (Voir la figure 4.3), elle donne comme résultat:

```
Ellipsis
EllipticCurve
EllipticCurveIsogeny
EllipticCurve_from_c4c6
EllipticCurve_from_cubic
EllipticCurve_from_j
EllipticCurve_from_plane_curve
EllipticCurves_with_good_reduction_outside_S
```

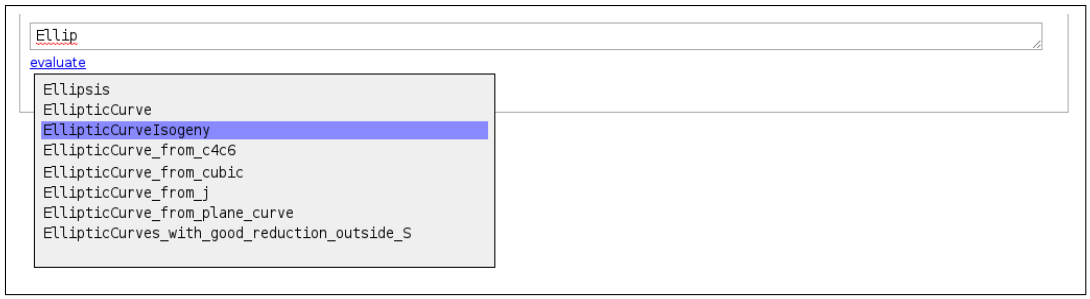


Figure A.3: Utilisation de la touche de tabulation «tab»

On peut accéder interactivement au manuel de référence de toute fonction, constante ou commande en la faisant suivre d'un point d'interrogation ? Par exemple:

`sage: EllipticCurve?`

La page de documentation contient la description de la fonction, sa syntaxe et surtout des exemples(Voir la figure 4.4).

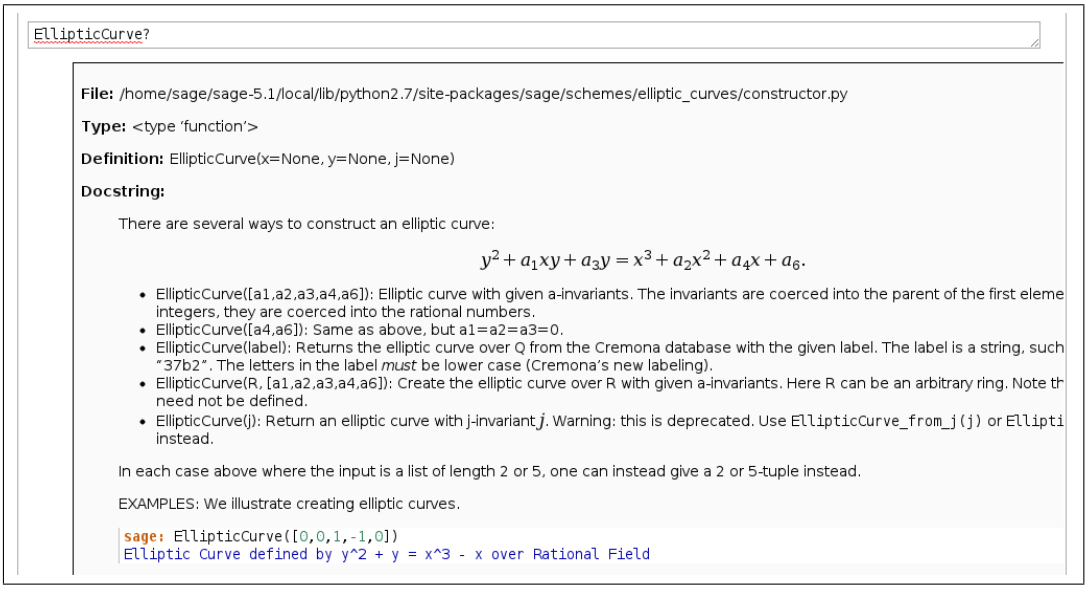


Figure A.4: Page de documentation de la fontion " EllipticCurve"

A.4 Manipulation des courbes elliptiques avec Sage

Les fonctionnalités relatives aux courbes elliptiques comprennent la plupart des fonctionnalités de PARI, l'accès aux données des tables en ligne de Cremona (ceci requiert le chargement d'une base de donnée optionnelle [20]), les fonctionnalités de mwrank (mwrank est un programme permettant le calcul des groupes de Mordell-Weil de courbes elliptiques sur $\mathbb{Q}$ par 2-descente et très souvent le rang est déterminé ainsi que des générateurs probables), l'algorithme SEA (Schoof-Elkies-Atkin), le calcul de toutes les isogénies, plusieurs nouveaux codes pour les courbes sur $\mathbb{Q}$ et une partie du code de descente algébrique de Denis Simon.

A.4.1 Définir une courbe elliptique sur Sage :

La commande « `EllipticCurve` » permet de créer une courbe elliptique.

`sage: EllipticCurve`$([a_1, a_2, a_3, a_4, a_6])$

Renvoie la courbe elliptique $y^2 + a_1xy + a_3y^2 = x^3 + a_2x^2 + a_4x + a_6$. Où les (a_i) sont convertis par coercition dans le parent de (a_1). Si tous les (a_i) ont pour parent $\mathbb{Z}$, ils sont convertis par coercition dans $\mathbb{Q}$.

`sage: EllipticCurve`$([a_4, a_6])$

Idem avec $a_1 = a_2 = a_3 = 0$.

`sage: EllipticCurve` $(label)$

Renvoie la courbe elliptique sur $\mathbb{Q}$ de la base de données de Cremona selon son nom dans la nouvelle nomenclature de Cremona [21]. Les courbes sont étiquetées par une chaîne de caractère telle que `"11a3"`, `"37a1"`, `"35a3"` ou `"99b1"`. La lettre doit être en minuscule (pour faire la différence avec l'ancienne nomenclature).

`sage: EllipticCurve`$([\mathbb{A}, a_1, a_2, a_3, a_4, a_6])$:

Crée la courbe elliptique sur l'anneau $\mathbb{A}$ donnée par les coefficients a_i comme ci-dessus.

Illustrons chacune de ces constructions sur Sage dans la figure 4.5:

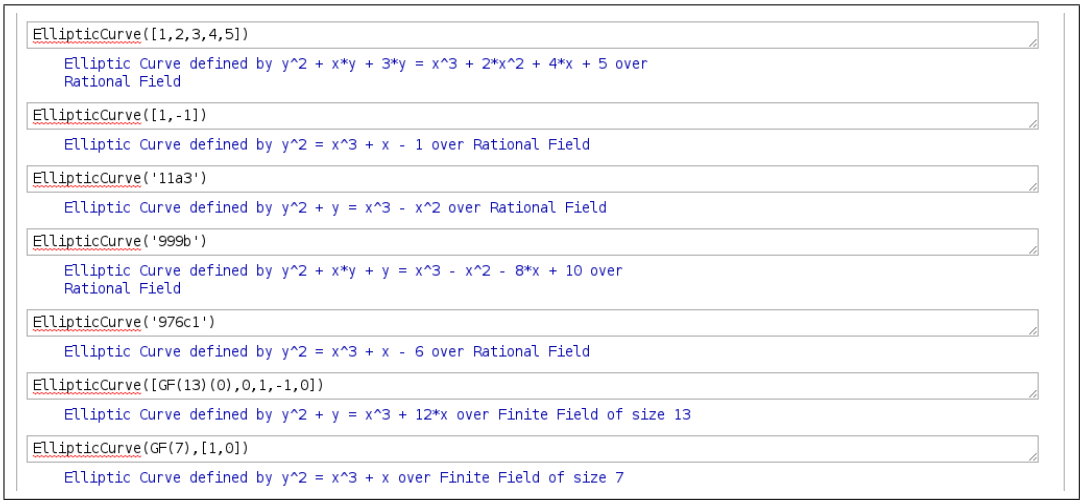


Figure A.5: Définition des courbes elliptiques sur Sage

A.4.2 Calculer $\#E$ et kP sur Sage:

Sage peut calculer l'ordre d'une courbe elliptique avec la commande «`E.cardinality()`». Il peut additionner les points sur une telle courbe elliptique et aussi calculer la somme kP (rappelons qu'une courbe elliptique possède une structure de groupe additif où le point à l'infini représente l'élément neutre $O = (0 : 1 : 0)$ et où trois points alignés de la courbe sont de somme nulle). Pour créer un point avec Sage, il convient de taper `E([a, b])`.

Dans l'exemple 62, chapitre 3:

Le couple $(121, 30)$ est un point de la courbe elliptique E définie par $y^2 = x^3 - x (\mathrm{mod}\, 1283)$, $\mathrm{pgcd}(1283, 6) = 1$, $\#E = 1284$, la factorisation de 1284, le calcul de $12P$ et $1284P$.

La figure 4.6 montre l'application des calculs présents sur cet exemple par le logiciel Sage.

En plus, le logiciel Sage donne la possibilité de calculer les coordonnées des points d'une courbe elliptique définie sur un corps fini. Ceci est montré dans la figure 4.7:

A.4.3 Le graphe des courbes elliptiques en 2D et 3D

Nous avons vu dans la section 4.3.2 comment tracer une fonction en 2D et 3D. Les figures (1.2) et (1.3) dans le chapitre 1 sont générées par le logiciel de calcul MATLAB, elles representent des courbes elliptiques sur le corps $\mathbb{R}$. Les commandes de Sage qui

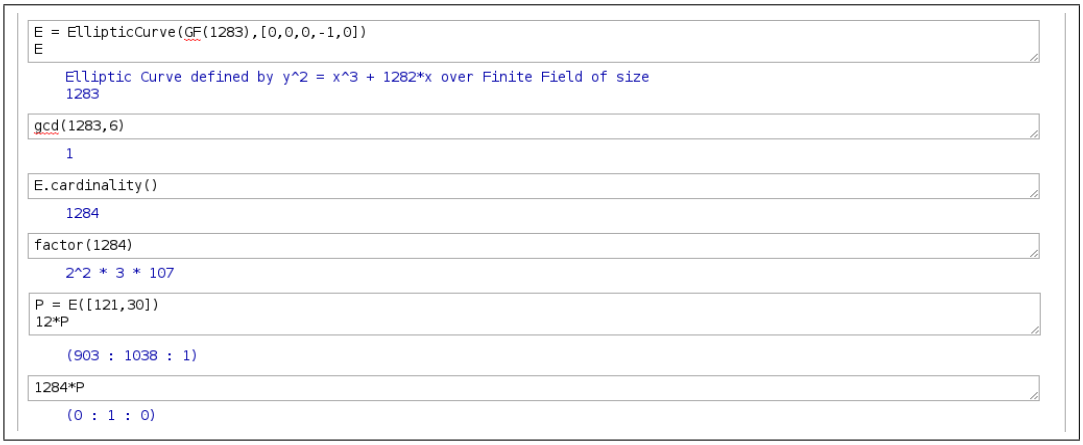


Figure A.6: Calcul de kP et de l'ordre de E

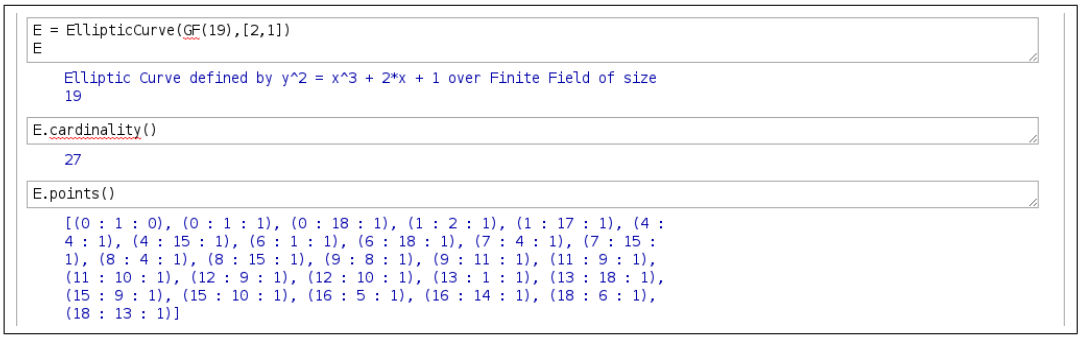


Figure A.7: Calcul des coordonnées de points d'une courbe elliptique sur Sage

correspondent à ces figures en 2D sont montrées dans les figures 4.8 et 4.9 et en 3D dans les figures 4.10 et 4.11 respectivement. D'une facon similaire sur un corps fini,

Les figures (1.8), (1.9) et (1.10) sont produits par les fonctions Sage illustrées dans les figures 4.12, 4.13, 4.14 respectivement.

A.5 Manipulation des polynômes sur Sage

A.5.1 Théorème des restes chinois sur Sage

Une autre application utile des calculs modulaires est ce qu'on appelle communément les « restes chinois » que nous avons utilisés dans le chapitre 2. Etant donnés deux modules m_1 et m_2 premiers entre eux, soit x un entier inconnu tel que $x \equiv a_1 (\mathrm{mod}\, m_1)$ et $x \equiv a_2 (\mathrm{mod}\, m_2)$. Alors le théorème des restes chinois permet de calculer de façon unique la valeur de x modulo le produit $m_1 m_2$.

On a décrit ici la variante la plus simple des restes chinois. On peut également considérer le cas où m_1 et m_2 ne sont pas premiers entre eux, ou bien le cas de plusieurs modulo m_1,m_2, . . . ,m_k.

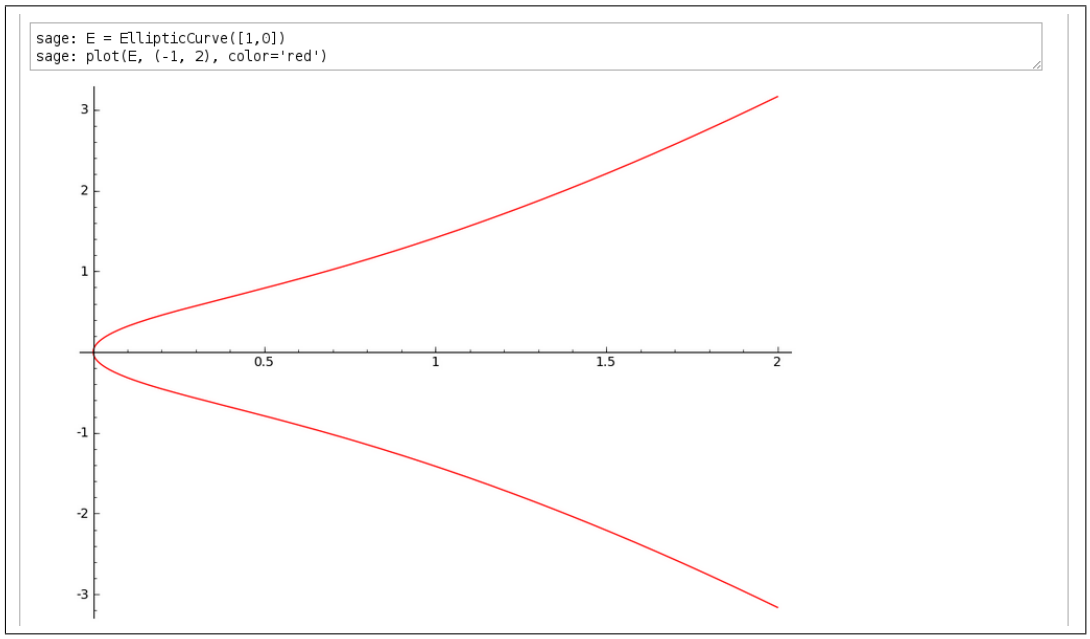


Figure A.8: Courbe elliptique (FIG 2.2) en 2D sur Sage

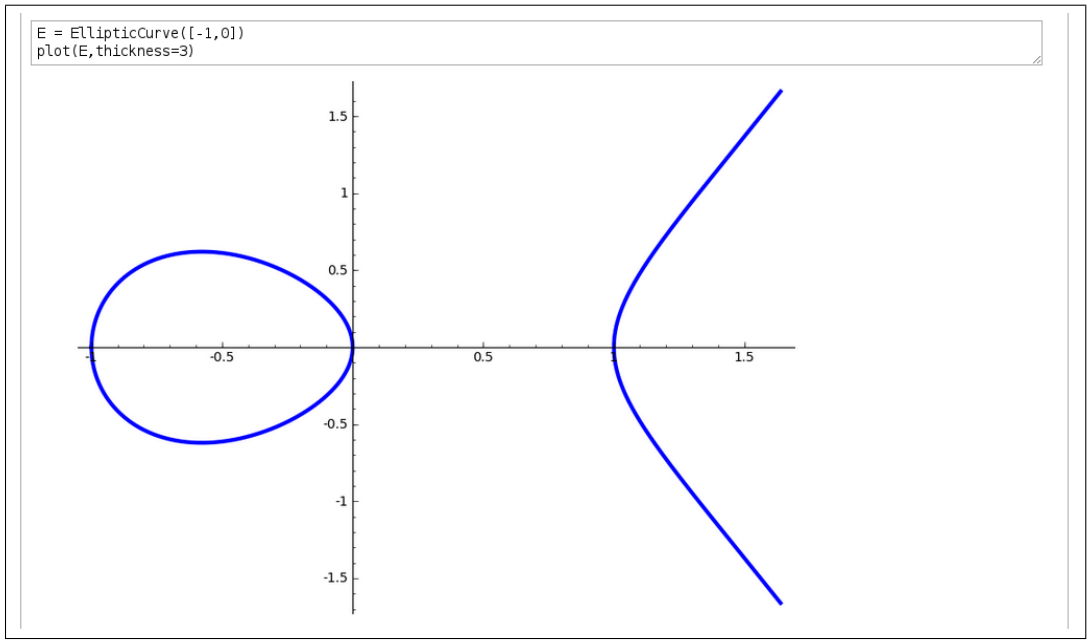


Figure A.9: Courbe elliptique (FIG 2.3) en 2D sur Sage

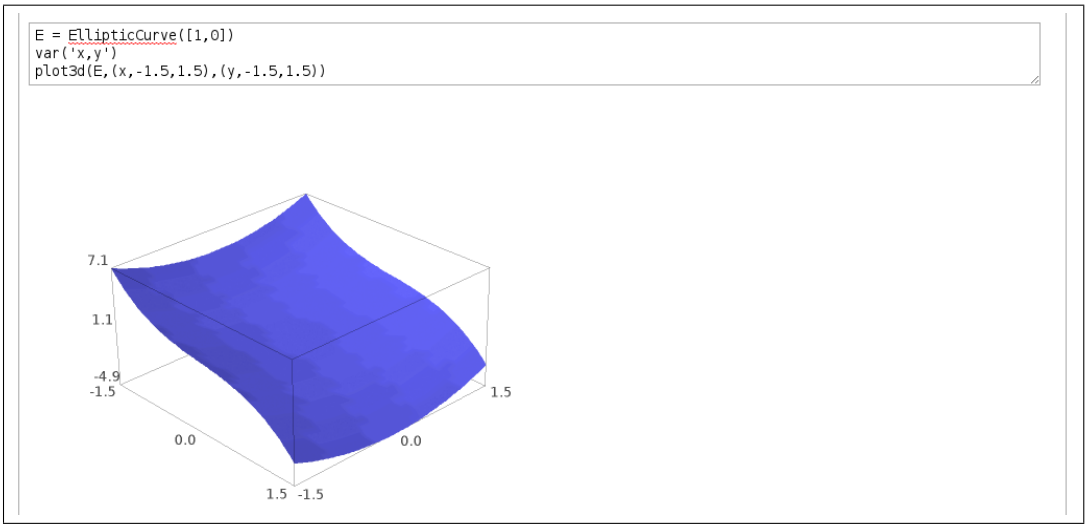


Figure A.10: Courbe elliptique (FIG 1.2) en 3D sur Sage

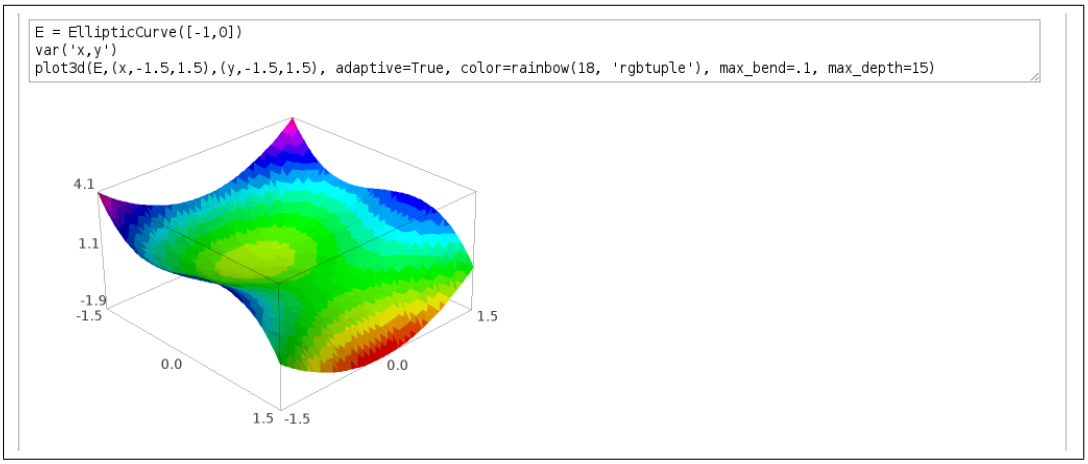


Figure A.11: Courbe elliptique (FIG 1.3) en 3D sur Sage

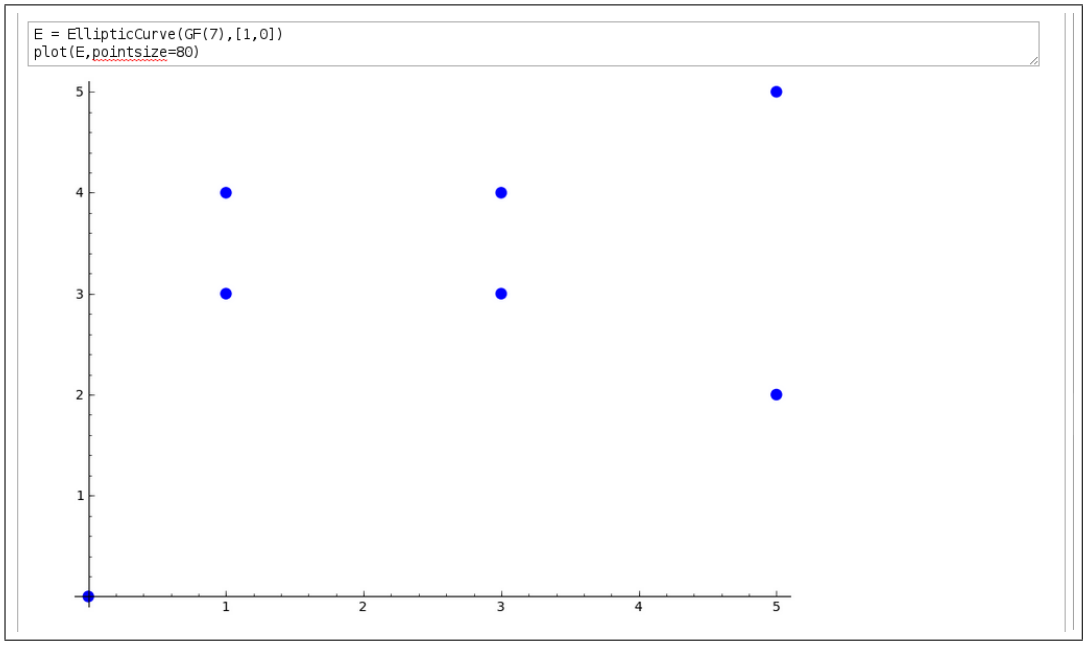


Figure A.12: Courbe elliptique sur le corps fini Z/7Z sur Sage

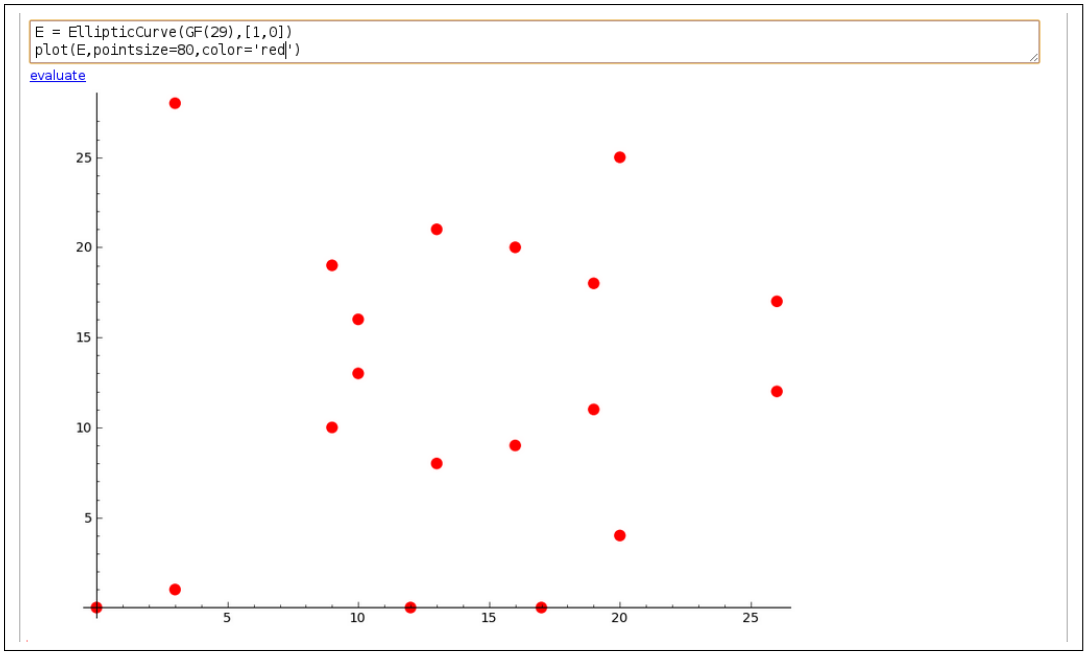


Figure A.13: Courbe elliptique sur le corps fini Z/29Z sur Sage

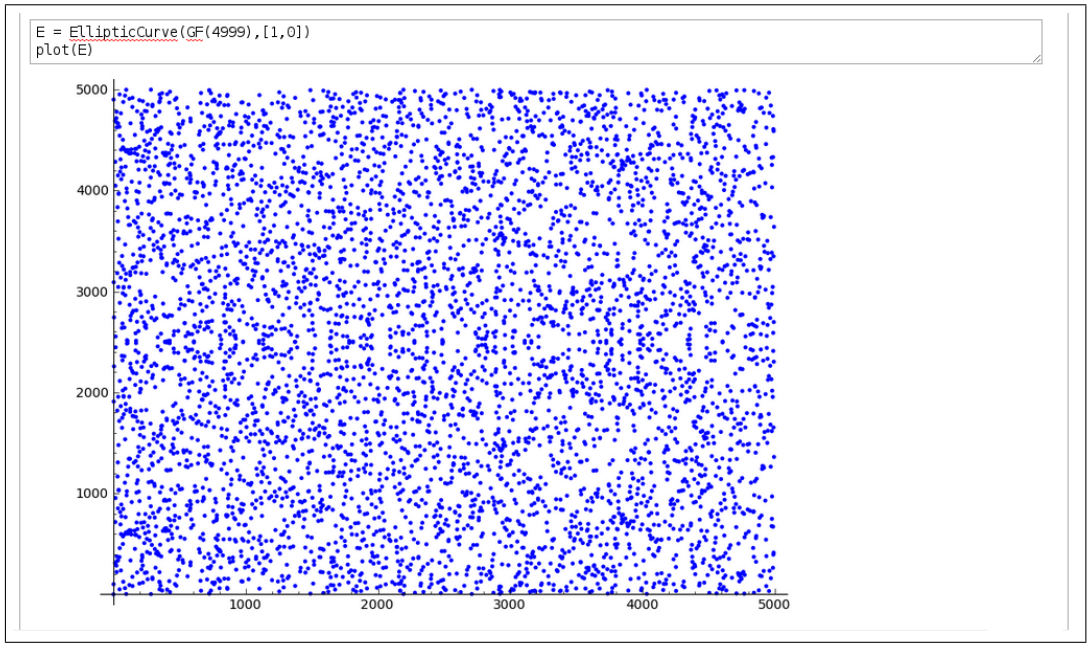


Figure A.14: Courbe elliptique sur le corps fini Z/4999Z sur Sage

Figure A.15: Théorème des restes chinois sur Sage

La commande Sage pour trouver x modulo le produit $m_1 m_2$ est `crt(a1,a2,m1,m2)` (Voir la figure 4.15).

Pour trois congruences est `crt([a1, a2, a3], [m1, m2, m3])`.

Ainsi pour k congruences la commande est `crt([a1, a2,..., ak], [m1, m2,..., mk])`.

A.5.2 Construction d'anneaux de polynômes

Dans ce logiciel, les polynômes, comme beaucoup d'autres objets algébriques, sont en général à coefficients dans un anneau commutatif.

Pour utiliser des polynômes, il faut tout d'abord définir l'anneau ou corps de base (exemple : $\mathbb{Z}[x]$, $\mathbb{Q}[x]$, $\mathbb{R}[x]$, $\mathbb{Z}/n\mathbb{Z}[x]$, sont `ZZ['x']`, `QQ['x']`, `RR['x']`, `Integers(n)['x']`).

Il existe trois façons de créer des anneaux de polynômes.

```
sage: R = PolynomialRing(QQ, 'x')
sage: R
```

```
Univariate Polynomial Ring in x over Rational Field
```

Ceci crée un anneau de polynômes et indique à Sage d'utiliser (la chaîne de caractère) `'x'` comme indéterminée lors de l'affichage à l'écran. Toutefois, ceci ne définit pas le symbole `x` pour son utilisation dans Sage. Aussi, il n'est pas possible de l'utiliser pour saisir un polynôme (comme $x^2 + 1$) qui appartient à R.

Une deuxième manière de procéder est

```
sage: S = QQ['x']
sage: S == R
True
```

Ceci a les mêmes effets en ce qui concerne `x`.

Une troisième manière de procéder, très pratique, consiste à entrer

```
sage: R.<x> = PolynomialRing(QQ)
```

ou

```
sage: R.<x> = QQ['x']
```

ou

```
sage: R.<x> = QQ[]
```

ou même

```
sage: x = polygen(QQ, 'x')
```

L'effet secondaire de ces dernières instructions est de définir la variable `x` comme l'indéterminée de l'anneau des polynômes. Ceci permet de construire très aisément des éléments de R, comme décrit ci-après. (Noter que cette troisième manière est très semblable à la notation par constructeur de Magma

Par exemple

```
Sage : R.<x> =QQ['x']
p = (2*x+1)*(x+2)*(x^4-1)
p
sage : 2*x^6 + 5*x^5 + 2*x^4 - 2*x^2 - 5*x - 2
```

Observons que le polynôme est automatiquement développé. Les polynômes « algébriques » sont toujours représentés sous forme normale.

On peut aussi utiliser « `print` » ou « `show` » pour afficher

```
sage :  R.<x> =ZZ['x']
print (R)
Univariate Polynomial Ring in x over Integer Ring
```

et avec "`show`"

```
sage: R.<x> = Integers(14)['x']
show (R)
Z/14Z[x]
```

A.5.3 Polynômes et arithmétique euclidienne:

On peut faire de l'arithmétique sur les polynômes dans un anneau de polynômes à une indéterminée (voir figure 4.16):

- Opérations de base $p+q$, $p-q$, $p\times q$, p^k : `p + q, p - q, p * q, p^k`
- Degré de p : `p.degree()`
- Connaitre l'indéterminée : `p.variables()`
- Coefficient de x^k : `p[k]`
- Coefficient dominant : `p.leading_coefficient()`
- Liste des coefficient : `p.coeffs()`
- Liste des coefficient non nuls : `p.coefficients()`
- Dérivée : `p.derivative()` ou `diff(p)`
- Test d'irréductibilité : `p.is_irreducible()`
- Factorisation sur le corps de base : `p.factor()`
- Développement : `p.expand()` (attention par défaut, le polynôme est stocké sous forme développée et Sage renvoie une erreur si on lui demande de développer un polynôme déjà développé).
- Racines dans le corps de base : `p.roots()`
- Racines dans une extension (ici C) : `p.roots(CC)`

Dans cette partie, on suppose que l'on a défini des polynômes $p1$, $p2$ et $p3$ dans $\mathbb{k}[x]$ ou $\mathbb{k}$ est un corps commutatif (voir les figures 4.17).

- Test de divisibilité : `p1.divides(p2)`
- division euclidienne de $p1$ par $p2$: `q=p1//p2, r=p1%p2 , q,r = p1.quo_rem(p2)`
- pgcd$(p1;p2)$: `p1.gcd(p2), gcd(p1,p2)`
- ppcm$(p1;p2)$: `p1.lcm(p2), lcm(p1,p2)`
- pgcd$(p1;p2;p3)$, ppcm$(p1;p2;p3)$: `gcd([p1,p2,p3]), lcm([p1,p2,p3])`

A.6 Calcul des exemples 2.6 et 2.7 de l'algorithme de Schoof

Dans cette partie, nous avons calculé l'ordre de la courbe elliptique $E : y^2 = x^3+2x+1$ sur $\mathbb{F}_{19^9}$ et les différents calculs sont dans la figure (4.18). Ensuite sur $\mathbb{F}_{29^{2013}}$ et tous les points de $E(\mathbb{F}_{19})$ pour Assurer notre résultats (Voir figure 4.19) et les différentes étapes sont dans les figures (4.20), (4.21).

```
R = PolynomialRing(QQ, 'x')
p = (2*x^2+1)*(x^2+2)*(x^2+1)
q = 2*x**2+4*x+x+2
```

```
p+q
```
```
2*x^6 + 7*x^4 + 9*x^2 + 5*x + 4
```

```
p-q
```
```
2*x^6 + 7*x^4 + 5*x^2 - 5*x
```

```
p*q
```
```
4*x^8 + 10*x^7 + 18*x^6 + 35*x^5 + 28*x^4 + 35*x^3 + 18*x^2 + 10*x + 4
```

```
p^3
```
```
8*x^18 + 84*x^16 + 378*x^14 + 955*x^12 + 1491*x^10 + 1491*x^8 + 955*x^6
+ 378*x^4 + 84*x^2 + 8
```

```
p.degree()
```
```
6
```

```
p[2]
```
```
7
```

```
p.leading_coefficient()
```
```
2
```

```
p.coeffs()
```
```
[2, 0, 7, 0, 7, 0, 2]
```

```
p.coefficients()
```
```
[2, 7, 7, 2]
```

```
p.derivative()
```
```
12*x^5 + 28*x^3 + 14*x
```

```
p.is_irreducible()
```
```
False
```

```
p.factor()
```
```
(2) * (x^2 + 1/2) * (x^2 + 1) * (x^2 + 2)
```

```
expand((2*x^2+1)*(x^2+2)*(x^2+1))
```
```
2*x^6 + 7*x^4 + 7*x^2 + 2
```

```
q.roots()
```
```
[(-1/2, 1), (-2, 1)]
```

```
p.roots()
```
```
[]
```

```
p.roots(CC)
```
```
[(-1.41421356237310*I, 1), (-1.00000000000000*I, 1),
(-0.707106781186548*I, 1), (0.707106781186548*I, 1),
(1.00000000000000*I, 1), (1.41421356237310*I, 1)]
```

Figure A.16: Polynômes et arithmétique Euclidienne sur Sage.

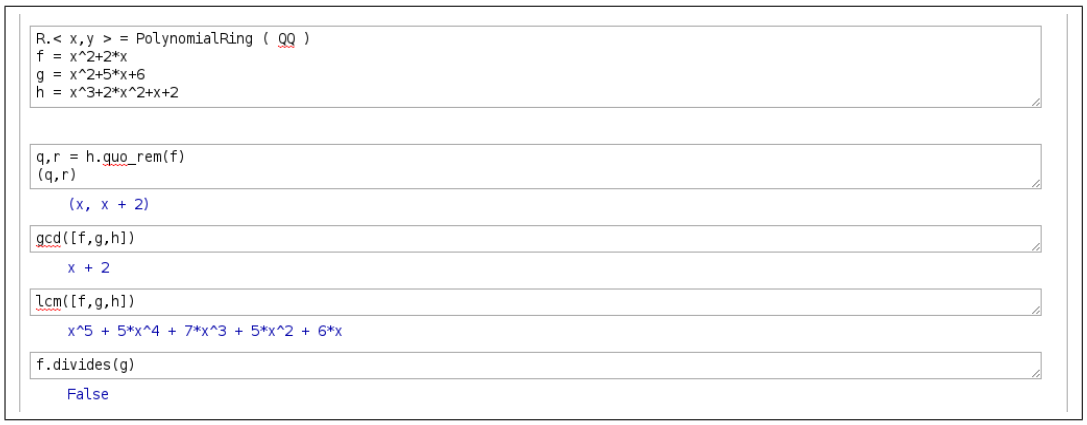


Figure A.17: Calcul des ppcm et pgcd de 3 polynômes

```
R.<x> = GF(19)['x']
x^19 % (x^3+2*x+1)
```

```
x^2 + 13*x + 14
```

```
gcd(x^2 + 12*x + 14,x^3+2*x+1)
```

```
1
```

```
psi3=3*x^4+12*x^2+12*x-4
gcd(x^361-x,psi3)
```

```
x + 11
```

```
gcd(x^19-x,psi3)
```

```
x + 11
```

```
gcd((x^3+2*x+1)^9-1,psi3)
```

```
x + 11
```

```
psi5=5*x^12 + 10*x^10 + 17*x^8 + 5*x^7 + x^6 + 9*x^5 + 12*x^4 + 2*x^3 + 5*x^2 + 8*x + 8
```

```
inverse_mod((x^361-x)^2,psi5)
```

```
x^11 + x^10 + 2*x^9 + 13*x^8 + 7*x^7 + x^6 + 7*x^5 + 14*x^4 + 11*x^3 +
10*x^2 + 10*x + 12
```

```
((x^3+2*x+1)*(x^11 + x^10 + 2*x^9 + 13*x^8 + 7*x^7 + x^6 + 7*x^5 + 14*x^4 + 11*x^3 + 10*x^2 + 10*x + 12)*
((x^3+2*x+1)^180+1)^2-x^361-x)%psi5
```

```
3*x^11 + 9*x^10 + 18*x^9 + 11*x^8 + 16*x^7 + x^6 + 3*x^5 + 12*x^4 +
4*x^3 + 17*x^2 + 6*x + 16
```

```
(3*x^11 + 9*x^10 + 18*x^9 + 11*x^8 + 16*x^7 + x^6 + 3*x^5 + 12*x^4 + 4*x^3 + 17*x^2 + 6*x + 16-x^19)%psi5
```

```
11*x^11 + 15*x^10 + 18*x^9 + 2*x^8 + 17*x^7 + 2*x^6 + 4*x^5 + 8*x^4 +
18*x^3 + 8*x^2 + 6*x + 18
```

```
inverse_mod(4*(x^3+2*x+1),psi5)
```

```
x^11 + 5*x^10 + 9*x^9 + 18*x^8 + 6*x^7 + 11*x^6 + 2*x^5 + 18*x^4 + 2*x^3
+ 2*x^2 + 14*x + 8
```

```
((x^11 + 5*x^10 + 9*x^9 + 18*x^8 + 6*x^7 + 11*x^6 + 2*x^5 + 18*x^4 + 2*x^3 + 2*x^2 + 14*x + 8)*(3*x^2+2)^2-2*x)%psi5
```

```
12*x^11 + 4*x^10 + 18*x^9 + 7*x^8 + 14*x^7 + 5*x^6 + 6*x^5 + 5*x^4 +
15*x^3 + 8*x^2 + 4*x + 7
```

```
((3*x^11 + 9*x^10 + 18*x^9 + 11*x^8 + 16*x^7 + x^6 + 3*x^5 + 12*x^4 + 4*x^3 + 17*x^2 + 6*x + 16)-(12*x^11 + 4*x^10 +
18*x^9 + 7*x^8 + 14*x^7 + 5*x^6 + 6*x^5 + 5*x^4 + 15*x^3 + 8*x^2 + 4*x + 7)^19)%psi5
```

```
0
```

```
inverse_mod((x^361-x),psi5)
```

```
7*x^11 + 15*x^10 + 13*x^9 + 5*x^8 + 9*x^7 + 7*x^6 + 14*x^5 + 2*x^4 +
4*x^3 + 3*x^2 + x + 16
```

```
((7*x^11 + 15*x^10 + 13*x^9 + 5*x^8 + 9*x^7 + 7*x^6 + 14*x^5 + 2*x^4 + 4*x^3 + 3*x^2 + x + 16)*((x^3+2*x+1)^180+1)*
(x^361-(3*x^11 + 9*x^10 + 18*x^9 + 11*x^8 + 16*x^7 + x^6 + 3*x^5 + 12*x^4 + 4*x^3 + 17*x^2 + 6*x + 16))-
(x^3+2*x+1)^180)%psi5
```

```
9*x^11 + 13*x^10 + 15*x^9 + 15*x^7 + 18*x^6 + 17*x^5 + 8*x^4 + 12*x^3 +
8*x + 6
```

```
inverse_mod(2*(x^3+2*x+1),psi5)
```

```
2*x^11 + 10*x^10 + 18*x^9 + 17*x^8 + 12*x^7 + 3*x^6 + 4*x^5 + 17*x^4 +
4*x^3 + 4*x^2 + 9*x + 16
```

```
((2*x^11 + 10*x^10 + 18*x^9 + 17*x^8 + 12*x^7 + 3*x^6 + 4*x^5 + 17*x^4 + 4*x^3 + 4*x^2 + 9*x + 16)*(3*x^2+2)*(x-(12*x^11
+ 4*x^10 + 18*x^9 + 7*x^8 + 14*x^7 + 5*x^6 + 6*x^5 + 5*x^4 +15*x^3 + 8*x^2 +4*x + 7))-1)%psi5
```

```
13*x^10 + 15*x^9 + 16*x^8 + 13*x^7 + 8*x^6 + 6*x^5 + 17*x^4 + 18*x^3 +
8*x + 18
```

```
((x^3+2*x+1)^9*((2*x^11 + 10*x^10 + 18*x^9 + 17*x^8 + 12*x^7 + 3*x^6 + 4*x^5 + 17*x^4 + 4*x^3 + 4*x^2 + 9*x + 16)*
(3*x^2+2)*(x-(12*x^11 + 4*x^10 + 18*x^9 + 7*x^8 + 14*x^7 + 5*x^6 + 6*x^5 + 5*x^4 +15*x^3 + 8*x^2 +4*x + 7))-1)^19)%psi5
```

```
10*x^11 + 6*x^10 + 4*x^9 + 4*x^7 + x^6 + 2*x^5 + 11*x^4 + 7*x^3 + 11*x +
13
```

```
((9*x^11 + 13*x^10 + 15*x^9 + 15*x^7 + 18*x^6 + 17*x^5 + 8*x^4 + 12*x^3 + 8*x + 6)+(10*x^11 + 6*x^10 + 4*x^9 + 4*x^7 +
x^6 + 2*x^5 + 11*x^4 + 7*x^3 + 11*x + 13))%psi5
```

```
0
```

```
crt([1,2,3],[2,3,5])
```

```
23
```

```
r=19^9+1-((-7-I*sqrt(27))/2)^9-((-7+I*sqrt(27))/2)^9
r.expand()
```

```
322688674476
```

Figure A.18: Calculs de l'exemple 2.6

```
E = EllipticCurve(GF(29),[2,1])
E
```

```
Elliptic Curve defined by y^2 = x^3 + 2*x + 1 over Finite Field of size
29
```

```
E.cardinality()
```

```
33
```

```
E.points()
```

```
[(0 : 1 : 0), (0 : 1 : 1), (0 : 28 : 1), (1 : 2 : 1), (1 : 27 : 1), (2 :
10 : 1), (2 : 19 : 1), (3 : 11 : 1), (3 : 18 : 1), (5 : 7 : 1), (5 : 22
: 1), (8 : 6 : 1), (8 : 23 : 1), (9 : 9 : 1), (9 : 20 : 1), (10 : 8 :
1), (10 : 21 : 1), (11 : 7 : 1), (11 : 22 : 1), (12 : 10 : 1), (12 : 19
: 1), (13 : 7 : 1), (13 : 22 : 1), (15 : 10 : 1), (15 : 19 : 1), (19 : 5
: 1), (19 : 24 : 1), (21 : 13 : 1), (21 : 16 : 1), (23 : 11 : 1), (23 :
18 : 1), (25 : 4 : 1), (25 : 25 : 1)]
```

Figure A.19: Calcul de l'ordre de la courbe E de l'exemple 2.7 et de ses points.

```
R.<x> = GF(29)['x']
x^29 % (x^3+2*x+1)
```

```
14*x^2 + 18*x + 9
```

```
gcd(14*x^2 + 17*x + 9,x^3+2*x+1)
```

```
1
```

```
psi3=3*x^4+12*x^2+12*x-4
gcd(x^841-x,psi3)
```

```
x^4 + 4*x^2 + 4*x + 18
```

```
q=x^4 + 4*x^2 + 4*x + 18
q.factor()
```

```
(x + 13) * (x + 27) * (x^2 + 18*x + 6)
```

```
(3*2^4+12*2^2+12*2-4)%29
```

```
0
```

```
P=E([2,10])
3*P
```

```
(0 : 1 : 0)
```

```
psi5=5*x^12 + 8*x^10 + 3*x^9 + 15*x^8 + 16*x^7 + 28*x^6 + 18*x^4 + 22*x^3 + 21*x^2 + 20*x + 16
```

```
inverse_mod((x^841-x)^2,psi5)
```

```
24*x^11 + 8*x^10 + 14*x^9 + 11*x^8 + 19*x^6 + 10*x^5 + 14*x^4 + 8*x^3 +
15*x^2 + 15*x + 16
```

```
((x^3+2*x+1)*(24*x^11+8*x^10+14*x^9+11*x^8+19*x^6+10*x^5+14*x^4+8*x^3+15*x^2+15*x+16)*((x^3+2*x+1)^420+1)^2-x^841-
x)%psi5
```

```
4*x^11 + 19*x^10 + 7*x^8 + 18*x^7 + 25*x^6 + 19*x^5 + 12*x^4 + 20*x^3 +
21*x^2 + 28*x + 11
```

```
(22*x^11+14*x^10+28*x^9+27*x^8+14*x^7+21*x^6+11*x^5+x^4+3*x^3+24*x^2+18*x+21-x^29)%psi5
```

```
4*x^11 + 28*x^10 + 20*x^9 + 5*x^8 + 15*x^7 + 3*x^6 + 24*x^5 + 11*x^4 +
12*x^3 + 11*x^2 + x + 18
```

```
inverse_mod(4*(x^3+2*x+1),psi5)
```

```
4*x^11 + 19*x^10 + 25*x^9 + 14*x^8 + 19*x^7 + 20*x^6 + 24*x^5 + 20*x^4 +
13*x^3 + 22*x^2 + 4*x + 12
```

```
((4*x^11 + 19*x^10 + 25*x^9 + 14*x^8 + 19*x^7 + 20*x^6 + 24*x^5 + 20*x^4 +13*x^3 + 22*x^2 + 4*x + 12)*(3*x^2+2)^2-
2*x)%psi5
```

```
6*x^11 + 4*x^10 + 22*x^9 + 25*x^8 + x^7 + 4*x^6 + 23*x^5 + x^4 + 5*x^3 +
10*x^2 + 21*x + 6
```

```
((4*x^11+19*x^10+7*x^8+18*x^7+25*x^6+19*x^5+12*x^4+20*x^3+21*x^2+28*x+11)-
(6*x^11+4*x^10+22*x^9+25*x^8+x^7+4*x^6+23*x^5+x^4+5*x^3+10*x^2+21*x+6)^29)%psi5
```

```
0
```

Figure A.20: Calculs de l'exemple 2.7 (partie 1)

```
inverse_mod((x^841-x),psi5)
```

```
2*x^11 + 5*x^10 + x^9 + 15*x^8 + 26*x^7 + 17*x^6 + 26*x^5 + 5*x^4 +
16*x^3 + 7*x^2 + 20*x + 23
```

```
((2*x^11 + 5*x^10 + x^9 + 15*x^8 + 26*x^7 + 17*x^6 + 26*x^5 + 5*x^4 +16*x^3 + 7*x^2 + 20*x + 23)*((x^3+2*x+1)^420+1)*
(x^841-(4*x^11+19*x^10+7*x^8+18*x^7+25*x^6+19*x^5+12*x^4+20*x^3+21*x^2+28*x+11))-(x^3+2*x+1)^420)%psi5
```

```
21*x^11 + 18*x^10 + 25*x^9 + 15*x^8 + 15*x^7 + 6*x^6 + 13*x^5 + 16*x^4 +
6*x^3 + 21*x^2 + 23*x + 26
```

```
inverse_mod(2*(x^3+2*x+1),psi5)
```

```
8*x^11 + 9*x^10 + 21*x^9 + 28*x^8 + 9*x^7 + 11*x^6 + 19*x^5 + 11*x^4 +
26*x^3 + 15*x^2 + 8*x + 24
```

```
((x^3+2*x+1)^14*((8*x^11 + 9*x^10 + 21*x^9 + 28*x^8 + 9*x^7 + 11*x^6 + 19*x^5 + 11*x^4 +26*x^3 + 15*x^2 + 8*x + 24)*
(3*x^2+2)*(x-(6*x^11+4*x^10+22*x^9+25*x^8+x^7+4*x^6+23*x^5+x^4+5*x^3+10*x^2+21*x+6))-1)^29)%psi5
```

```
21*x^11 + 18*x^10 + 25*x^9 + 15*x^8 + 15*x^7 + 6*x^6 + 13*x^5 + 16*x^4 +
6*x^3 + 21*x^2 + 23*x + 26
```

```
((21*x^11 + 18*x^10 + 25*x^9 + 15*x^8 + 15*x^7 + 6*x^6 + 13*x^5 + 16*x^4 +6*x^3 + 21*x^2 + 23*x + 26)-(21*x^11 + 18*x^10
+ 25*x^9 + 15*x^8 + 15*x^7 + 6*x^6 + 13*x^5 + 16*x^4 +6*x^3 + 21*x^2 + 23*x + 26))%psi5
```

```
0
```

```
crt([1,0,2],[2,3,5])
```

```
27
```

```
r=29^2013+1-((-3-I*sqrt(107))/2)^2013-((-3+I*sqrt(107))/2)^2013
r.expand()
```

```
641460281620499961805967164034824142458125349589860006572913337121161859\
451306074320891602815688747608052208884123178655751607236471938730847389\
792820333499756413318965630314480161859287381724326922700067088897274365\
037913575031831924092011559239778369005400459409876541437539821984649868\
626448649014321046446911787115180846392594555122706936842158217373565502\
346677966699470858927807132639148276593297590986353219925694903482128632\
289774920682918909327176779302108216619181723295502963427502311963712579\
452840748958005108766171837947574958311182158413136156858066333871075677\
910556710985348574505794703210336794341739382318779438859655626041360142\
117312269802493637188426016142644135175862082723187415696769005507683777\
096757663646628449564904186566893512398775965121479436289336667446255677\
333799087401664642670024185176164797969478489114567766618788727113916285\
427917212789650640931074986776948466059391889567351022630044939917055434\
385362605879132421773702361919777629324140954532592073085404554521597335\
060050412259195106963633409030214463153194169407503193300552284370449015\
125148829671091082650277725469280510567618074769261584889115196992481333\
978013933900503065680205175367095811571529676454050265081304922336985049\
898101290803878167485280713934883736222760542258084975509391994500876189\
813196337150304928021273203109799616461625383729217843090967427868288531\
133392035950223736084297437470901249616710259585497750979878412852180430\
784424107289771435001112576051667336548439282079906248407570745802426088\
509168234944145352063357055773631901123924017735220688748150773674342174\
411119019623616393273484487470281679267801487859939310767110691414657462\
934029580373166177890337127623636346201455457486195754398650554673202461\
057892224476823857917915918627977924641704962481872785461127320383107327\
522937941302114068355071487487415805989207409522800491154610962663837160\
812203236793908757483365341287272018601514368094132262049505653761786890\
313773546822266050021403399391151776709173800796988223936237047924092441\
929781519282989536155686086798062412067933775049353445638745880906439423\
715597312151674890613413321959706364281825180519258009705522024347053170\
925431026284600708106355184588319863230472372335620926924363960221761997\
701165908261587404833136918920450970563020788671232778821763522923423185\
399231042313363363846505004997789418101021510762358673090599285930818237\
149910030132212543780601357966372860102942054287491507695655408817680236\
041097943949214196928119239920221652180988533323264447056939956338381761\
748008650954326946109560728597854415473635643615319032651155441818279134\
786090876922778765390783198946221059656311225440525368119499427275154387\
292609434135101031056342142233255667742401018911221067455094939957252766\
692890038121054781228922339328385258863124225682129848805106255894102182\
481858821503749119407036816811940837493257369364145345034308077522963646\
145464343088116635031533170771081282523262973605681089971892932 4
```

Figure A.21: Calculs de l'exemple 2.7 (partie 2)