MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEURE ET DE LA RECHERCHE SCIENTIFIQUE

Université de Jijel

Faculté des Sciences Exactes et Informatique
Département de Mathématiques

N° d'ordre:
N° de série:

Mémoire présenté pour obtenir le diplôme de
Magister en Mathématiques
Option : Algèbre

Par : Kenane Radia

Thème

Quelques éléments de l'arithmétique des courbes elliptiques

Soutenu le 07/12/2013 devant le jury composé de:

Président:	**T. Zerzaihi**	**Prof.**	**Université de Jijel**
Rapporteur:	**N. Touafek**	**M.C.A**	**Université de Jijel**
Examinateur:	**M. Kerada**	**M.C.A**	**Université de Jijel**
Invité:	**A. Bouchair**	**M.C.B**	**Université de Jijel**

Année universitaire 2012-2013

Remerciements

Tout d'abord mes remerciements vont à dieu le tout puissant de ma donner le courage d'accomplir ce travail malgré les obstacles qui m'a affronté.

J'adresse les premières remerciements à mon directeur de mémoire « Touafek Nouressadat », je le remercie de m'avoir fait l'honneur d'être le rapporteur de ce travail, ainsi pour son soutien et ses conseils ;

Je tien également à remercie les membres de mon jury :

« T. Zerzaihi », « M.Kerada » et « A. Bouchair » d'avoir accepté d'évaluer mon travail, de s'y être intéressé pour leurs remarques et encouragements.

Je remercie ma famille pour son soutien et son encouragement morale, mon père, ma mère, mes deux frères, mes sœurs et mon époux ;

J'adresse mes salutations et remerciements à tous mes anciens professeurs de l'université de Jijel, ainsi aux personnes qui ont des influences dans l'accomplissement de ce travail.

Table des matières

Introduction **2**

1 Généralités sur les courbes elliptiques **4**

1.1 Plan projectif 4
1.1.1 La droite projective réelle 4
1.1.2 Le plan projectif réel 5
1.1.3 Le plan projectif $\mathbb{P}_2(K)$ 7
1.2 Courbes planes projectives 7
1.3 Courbes elliptiques 10
1.3.1 Forme de Weierstrass d'une courbe elliptique 10
1.3.2 Nature des points singuliers 18
1.3.3 Loi de groupe 20
1.3.4 Courbes birationnellement équivalentes et courbes isomorphes . 25
1.3.5 Théorème de Mordell-Weil 27

2 Sur certaines courbes de genre 1 de bidegré (2,2) **32**

2.1 Algorithme de Harrache et Touafek 32
2.2 Applications 38

3 Sur les courbes de Huff et d'Edwards **54**
3.1 Courbes de Huff $H_{(a,b)}^{(c,d)} : ax(y^2 - c) = by(x^2 - d)$ sur un corps K de caractéristique différente de deux 54
3.2 Courbes de Huff binaire $ax\left(y^2 + y + 1\right) = by\left(x^2 + x + 1\right)$ 65
3.3 Des suites arithmétiques sur les courbes d'Edwards 70

Bibliographie **74**

Introduction

En mathématiques, une courbe elliptique est un cas particulier de courbes algébriques. Les courbes elliptiques jouent un rôle fondamental en mathématiques et notamment en théorie des nombres depuis plusieurs années. Les courbes elliptiques ont de nombreuses applications dans des domaines trés différents des mathématiques : elles interviennent ainsi en mécanique classique dans la description du mouvement des toupies, en cryptographie dans le problème de la factorisation des entiers ou pour fabriquer des codes performants. Contrairement à ce que son nom pourrait laisser croire, l'ellipse n'est pas une courbe elliptique. Le nom des courbes elliptiques vient historiquement de leurs associations avec les intégrales elliptiques, elles-même appelées ainsi car elles servent en particulier à calculer la longueur d'arcs d'ellipses.

A l'aide d'un choix adapté de coordonnées, une courbe elliptique E peut-être représentée dans un plan par une équation cubique (appelée équation de Weierstrass généralisée) de la forme

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{1}$$

i.e., les points de la courbe E sur un corps K ont pour coordonnées les solutions de l'équation (1), on y joint un point à l'infini. On note cet ensemble de points $E(\overline{K})$ et l'ensemble des points solutions de l'équation (1) à coordonnées dans K, $E(K)$. Les cœfficients a_1, a_2, a_3, a_4 et a_6 sont des éléments du corps K sur lequel est définie la courbe, mais ils ne sont pas déterminés par la courbe de manière unique. Réciproquement, pour qu'une telle équation décrive effectivement une courbe elliptique, il faut que la courbe ainsi définie ne soit pas singulière, c'est- à-dire qu'elle n'ait ni point de rebroussement, ni point double (en d'autre terme, son graphe a le non individue intersection).

Les courbes elliptiques possèdent des propriétés tout à fait exceptionnelles d'un point de vue arithmétique et d'un point de vue géométrique : ce sont des courbes de genre 1, et l'une des propriétés remarquable est que l'ensemble des solutions (x, y) de l'équation (1) est muni très naturellement d'une structure de groupe abélien dont la structure concrète est dictée par des considérations géométriques. Formellement, une courbe elliptique est une courbe algébrique non-singulière de genre 1 sur un corps K et dont un point à coordonnées dans K est spécifié (un point à l'infini). Enfin, la description des courbes elliptiques, ainsi que leurs applications possibles, dépend

beaucoup du corps de définition choisi.

Dans le premier chapitre, on rappelle l'essentiel des résultats connus sur les courbes elliptiques utiles pour la suite de notre mémoire.

Ensuite dans le chapitre deux, on s'intéresse à l'algorithme de Harrache et Touafek permettant de ramener des courbes de genre 1 de bidegré (2,2) en une forme de Weierstrass, on détermine sur des exemples concrets de courbes l'ordre de certaines points apparants ainsi que le type des fibres singuliers.

Enfin dans le troisième chapitre, on s'intéresse aux courbes de Huff sur un corps de caractéristique différente de deux, et les courbes de Huff binaires. A la fin de ce chapitre un intérêt particulier sera accordé aux suites (des points) arithmétiques sur les courbes d'Edwards.

Chapitre 1

Généralités sur les courbes elliptiques

Dans ce chapitre on rappelle les définitions et les résultats de base sur les courbes elliptiques utiles pour la suite de notre travail. Pour plus de résultats et plus de détails, on pourra consulter [1-2], [5], [10], [14], [17-18].

Tout au long de ce mémoire, K est un corps commutatif.

1.1 Plan projectif

1.1.1 La droite projective réelle

Soit $\sim$ une relation binaire sur $\mathbb{R}^2 - \{0_{\mathbb{R}^2}\}$ définie par

$$\begin{aligned} \forall (x,y),(a,b) \quad &\in \quad \mathbb{R}^2 - \{0_{\mathbb{R}^2}\} : \\ (x,y) \quad &\sim \quad (a,b) \iff \exists \lambda \in \mathbb{R}^* / (x,y) = \lambda (a,b) \end{aligned}$$

i.e., (x,y) et (a,b) sont linéairement dépendants. "$\sim$ " est une relation d'équivalence sur $\mathbb{R}^2 - \{0_{\mathbb{R}^2}\}$. L'espace quotient obtenu

$$\frac{\mathbb{R}^2 - \{0_{\mathbb{R}^2}\}}{\sim}$$

sera noté par $\mathbb{P}_1(\mathbb{R})$ est appelé **la droite projective réelle.**

On note par $[a,b]$ la classe d'équivalence

$$\{\lambda(a,b) / \lambda \in \mathbb{R}^*\}$$

Chaque classe d'équivalence $[a,b]$ contient tous les points qui se trouve sur la droite passant par (a,b) et l'origine $(0,0)$ sauf ce dernier. En d'autres termes $\mathbb{P}_1(\mathbb{R})$ est

l'ensemble des droites passant à l'origine sauf l'origine. Il est important de remarquer que si $[x, y] \in \mathbb{P}_1(\mathbb{R})$ avec $y \neq 0$, alors

$$(x, y) \sim \left(\frac{x}{y}, 1\right)$$

donc, la classe $[x, y]$ contient un seul représentant de la forme $(a, 1)$, avec $a = \frac{x}{y}$ et en écrit alors

$$\mathbb{P}_1(\mathbb{R}) = \{[x, 1] / x \in \mathbb{R}\} \cup \{[1, 0]\}.$$

les points $\{[x, 1] \ / \ x \in \mathbb{R}\}$ forme la droite réelle, et le point $[1, 0]$ est appelée le point à l'infini.

1.1.2 Le plan projectif réel

On peut généraliser cette construction (i.e. la droite projective réelle ci-dessus) pour construire un plan projectif contient le plan réel plus les points à l'infini. Soient alors

$$x, \ y, \ z, \ a, \ b, \ c \in \mathbb{R}$$

avec

$$(x, y, z), \ \ (a, b, c) \neq 0_{\mathbb{R}^3}.$$

Alors

$$(x, y, z) \sim (a, b, c)$$

si et seulement si

$$\exists \lambda \in \mathbb{R}^* \text{ tel que } \ \ (x, y, z) = \lambda (a, b, c).$$

Par suite, on définit la classe d'équivalence de $[a, b, c]$ par l'ensemble de tous les points qui se trouve sur la droite passant par (a, b, c) et l'origine $(0, 0, 0)$ sauf ce point dernier. On écrit alors

$$\mathbb{P}_2(\mathbb{R}) = \{[a, b, c] \ / \ a, b, c \in \mathbb{R} \wedge (a, b, c) \neq (0, 0, 0)\}.$$

Si $c \neq 0$, alors

$$(a, b, c) \sim \left(\frac{a}{c}, \frac{b}{c}, 1\right),$$

donc

$$\mathbb{P}_2(\mathbb{R}) = \{[a, b, 1] \ / \ a, b \in \mathbb{R}\} \cup \{[a, b, 0] / a, b \in \mathbb{R}\}.$$

L'ensemble des points de

$$\{[a, b, 0] \ / \ a, b \in \mathbb{R}\}$$

est appelé ensemble *des points à l'infini.*

Un résultat intéressant est que : *deux droites parallèles dans le plan réel (ou bien deux droites distinctes) s'intersectent en un point à l'infini.*

En effet, Soient

$$L : y = \alpha x + \beta,$$

et

$$L' : y = \alpha x + \beta'$$

deux droites parallèles dans le plan réel. Dans $\mathbb{P}_2(\mathbb{R})$

$$\begin{aligned} L &= \{[x, y, z] \ / \ \alpha x - y + \beta z = 0\}, \\ L' &= \left\{[x, y, z] \ / \ \alpha x - y + \beta' z = 0\right\}. \end{aligned}$$

Déterminant $L \cap L'$ l'ensemble des points qui vérifient

$$\alpha x - y + \beta z = \alpha x - y + \beta' z = 0$$

i.e.,

$$\left(\beta - \beta'\right) z = 0.$$

Mais $L \neq L'$, donc

$$\beta \neq \beta'$$

on obtient alors

$$z = 0.$$

Par suite

$$L \cap L' = \{[x, \alpha x, 0] \ / \ x \in \mathbb{R}\} = \{[1, \alpha, 0]\}$$

i.e., l'intersection de L et L' contient un seul point à l'infini $[1, \alpha, 0]$.

Plus généralement , on appelle le n-espace projectif réel noté $\mathbb{P}_n(\mathbb{R})$ l' ensemble des classes d'équivalences des $(n+1)$ uples suivants

$$\mathbb{P}_n(\mathbb{R}) = \frac{\left\{(a_0, a_1, ..., a_n) \in \mathbb{R}^{n+1} \ / \ a_0, \ a_1, ..., \ a_n \ \text{ non tous nul}\right\}}{\backsim}$$

avec

$$(a_0, \ a_1, ..., a_n) \sim (a_0^{'}, \ a_1^{'}, ..., \ a_n^{'})$$

s'il existe $\lambda \in \mathbb{R}^*$ tel que

$$(a_0, a_1, ..., a_n) = \lambda(a_0^{'}, a_1^{'}, ..., a_n^{'}).$$

La classe d'équivalence $\{(\lambda a_0, ..., \lambda a_n) : \lambda \in \mathbb{R}^*\}$ est notée $[a_0, ..., a_n]$, donc on peut écrire

$$\mathbb{P}_n(\mathbb{R}) = \left\{[a_0, ..., a_n] / a_i \in \mathbb{R}, \forall i = \overline{0, n}\right\}.$$

1.1.3 Le plan projectif $\mathbb{P}_2(K)$

La droite projective et le plan projectif peut se définir sur un corps quelconque K (ex.$K = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ ou $\mathbb{F}_p$). Le plan projectif $\mathbb{P}_2(K)$ est défini comme suit :

$$\mathbb{P}_2(K) = \{[a,b,c] \ / \ a,b,c \in K, \ (a,b,c) \neq (0,0,0)\}$$

avec

$$(a,b,c) \sim (x,y,z)$$

si et seulement si

$$\exists \lambda \in K^* : \ (a,b,c) = \lambda(x,y,z).$$

Si $P = [a,b,c]$, alors a, b, c sont appelés *les coordonnées homogènes du point* P.

1.2 Courbes planes projectives

Definition 1 *Le degré d'un monôme d'un polynôme P de l'anneau $K[X_1, ..., X_n]$ est la somme des exposants des variables X_i apparaissant dans ce monôme. Le degré de P est le plus grand degré de ses monômes.*

Definition 2 *1. Un polynôme $P \in K[X_1, ..., X_n]$ est un polynôme homogène de degré d si chacune de ses monômes est de degré d .*

2. Si P est un polynôme homogène de degré d défini sur un corps K et à n variables, alors on écrit

$$P \in K[X_1, ..., X_n]_d.$$

3. Un polynôme P est dit irréductible s'il ne peut s'écrire comme le produit non trivial de deux polynômes de $K[X_1, ..., X_n]$.

Proposition 3 *Soit P un polynôme non nul $P \ (X_1, X_2, ..., X_n)$ à coefficients dans K. Alors, P est un polynôme homogène de degré d si et seulement si, pour une variable auxiliaire t*

$$P \ (tX_1, tX_2, ..., tX_n) = t^d P(X_1, X_2, ..., X_n).$$

Preuve. 1. La condition nécessaire est évidente .

2. Démontrons la condition suffisante :

écrivons P comme une somme de polynômes homogènes non nuls de degré d_i

$$p = p_{d_1} + p_{d_2} + ... + p_{d_k}, d_1 < d_2 < .... < d_k.$$

La relation

$$p(tx_1, tx_2, ...tx_n) = t^d p(x_1, x_2, ..., x_n)$$

implique que

$$t^{d_1}p_{d_1} + t^{d_2}p_{d_2} + ... + t^{d_k}p_{d_k} = t^d p = t^d p_{d_1} + t^d p_{d_2} + ... + t^d p_{d_k}$$

donc $t^{d_i} = t^d, \forall i$, par conséquent $k = 1$, car $d_1 < d_2 < d_3 < .... < d_k$ et $p = p_{d_1} = p_d$. ■

Definition 4 *Une courbe plane projective C de $\mathbb{P}_2(K)$ est l'ensemble des points qui satisfait à*

$$P(X, Y, Z) = 0,$$

où P est un polynôme homogène de degré $d \geq 1$.

1. Si $d = 1$, alors C est une droite

$$C : P(X, Y, Z) = aX + bY + cZ = 0, \ (a, b, c) \neq 0_{k^3}.$$

2. Si $d = 2$, alors C est une conique

$$C : P(X, Y, Z) = aX^2 + bXY + cY^2 + dXZ + eYZ + fZ^2 = 0, \ \ (a, b, c, d, e, f) \neq 0_{k^6}.$$

3. Si $d = 3$, alors C est une cubique

$$\begin{aligned} C : P(X, Y, Z) \ &= aX^3 + bX^2Y + cXY^2 + dY^3 + eX^2Z + fXYZ + gY^2Z \\ &+hXZ^2 + jYZ^2 + kZ^3 = 0, (a, b, c, d, e, f, g, h, j, k) \neq 0_{k^{10}}. \end{aligned}$$

Le nombre d est appelé le degré de la courbe.

Definition 5 *Le plan usuel sur K appelé plan affine, noté $\mathbb{A}_2(K)$, est l'ensemble des points (x, y) appartient à $\overline{K}^2$, $\overline{K}$ désigne la clôture algébrique de K, tel que*

$$\mathbb{A}_2(K) = \left\{(x, y) \ / \ x, y \in \overline{K}\right\}.$$

Remarque 6 *Soit C une cubique définie par un polynôme de deux variables dans le plan affine*

$$C : f(x, y) = 0$$

avec $f \in K[x, y]$.

Pour des simplifications, prenons par exemple

$$C : y^2 - x^3 - 1 = 0.$$

Si nous introduisons les coordonnées homogènes X, Y, Z $(Z \neq 0)$ telles que

$$x = \frac{X}{Z}, \ y = \frac{Y}{Z}$$

alors à tout point (x, y) de $\mathbb{A}_2(k)$ correspond le point $[X, Y, Z]$ de $\mathbb{P}_2(K)$.

On obtient

$$\left(\frac{Y}{Z}\right)^2 - \left(\frac{X}{Z}\right)^3 - 1 = 0$$

i.e.,

$$ZY^2 - X^3 - Z^3 = 0.$$

Notons que le polynôme

$$F(X, Y, Z) = ZY^2 - X^3 - Z^3 = 0$$

est un polynôme homogène de degré 3 et

$$F\left(\frac{X}{Z}, \frac{Y}{Z}, 1\right) = f(x, y).$$

La courbe C dans $\mathbb{P}_2(K)$ est donnée par

$$\hat{C} : F(X, Y, Z) = ZY^2 - X^3 - Z^3 = 0$$

donc, si le point $(x, y) \in C$, alors

$$\left[\frac{X}{Z}, \frac{Y}{Z}, 1\right] \in \hat{C}$$

mais il y a des points sur $\hat{C}$ ne sont pas présentés sur C, ces points de $\hat{C}$ sont appelés ***points à l'infini.***

Rappelons que les points à l'infini se sont les points qui correspond à $Z = 0$. Donc

$$F(X, Y, 0) = -X^3 = 0, \ i.e., \ X = 0.$$

Ainsi, le seul point à l'infini dans $\hat{C}$ est $[0, 1, 0]$.

En général, si $C \subseteq \mathbb{A}_2(K)$ donnée par $f(x, y) = 0$, et si d est le degré de f, alors $\hat{C} \in \mathbb{P}_2(K)$ est donnée par

$$\hat{C} : F(X, Y, Z) = 0$$

avec

$$F(X, Y, Z) = Z^d f\left(\frac{X}{Z}, \frac{Y}{Z}\right).$$

Inversement, si

$$\hat{C} : F(X, Y, Z) = 0$$

est une cubique dans le plan projectif, alors

$$C : F(x, y, 1) = 0$$

est la courbe dans le plan affine. Dans ce cas, C est la projection de $\hat{C}$.

Definition 7 *Un point P d' une courbe C du plan projectif $\mathbb{P}_2(K)$ d'équation:*

$$F(X,Y,Z)=0$$

est dit singulier si

$$\frac{\partial F}{\partial X}(P)=\frac{\partial F}{\partial Y}(P)=\frac{\partial F}{\partial Z}(P)=0,$$

sinon P est dit non singulier ou simple.

La courbe C est appelée courbe non singulière si tous ses points sont simples.

Exemple 8 *La courbe*

$$C: ZY^2=X^3,\ K=\mathbb{R}$$

est une courbe singulière au point $P=[0,0,1]$.

En effet

$$F(0,0,1)=0,\ \frac{\partial F}{\partial X}(X,Y,Z)=-3X^2,\ \frac{\partial F}{\partial Y}(X,Y,Z)=2YZ,\ \frac{\partial F}{\partial Z}(X,Y,Z)=Y^2$$

donc

$$\frac{\partial F}{\partial X}(0,0,1)=\frac{\partial F}{\partial Y}(0,0,1)=\frac{\partial F}{\partial Z}(0,0,1)=0.$$

1.3 Courbes elliptiques

1.3.1 Forme de Weierstrass d'une courbe elliptique

Definition 9 *Une courbe elliptique sur K est une paire $(E,\mathcal{O})$ où E désigne une cubique $(d=3)$ irréductible, non-singulière et $\mathcal{O}$ un point de E, appelé point de base ou origine.*

Definition 10 *En pratique, une courbe elliptique sur K peut être représentée dans le plan projectif par une équation de Weierstrass :*

$$E:\quad Y^2Z+a_1XYZ+a_3YZ^2=X^3+a_2X^2Z+a_4XZ^2+a_6Z^3\ ,a_i\in K \qquad (1.1)$$

Nous disons que la courbe E est définie sur le corps K si tous les coefficients a_i sont dans K.

Definition 11 *Nous définissons l'ensemble $E(K)$ des points $K-$rationnels sur K par*

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

Le point $\mathcal{O}=[0,1,0]\in E(K)$ est appelé ***"point à l'infini".***

Definition 12 *Le genre $g(E)$ d'une courbe plane projective E de degré d est l'entier positif défini par :*

$$g(E) = \frac{(d-1)(d-2)}{2} - \sum_{P} \frac{m(P)(m(P)-1)}{2}$$

avec P désigne les points singuliers de la courbe E en comptant leurs multiplicités $m(P)$. Si E est une courbe elliptique, le genre $g(E)$ est :

$$g(E) = \frac{(d-1)(d-2)}{2} = 1.$$

Remarque 13 *1. Pour alléger les notations, on écrit l'équation (1.1) en coordonnées non-homogènes, nous effectuons la transformation projective suivante*

$$x = \frac{X}{Z},\ y = \frac{Y}{Z}$$

nous obtenons

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

2. Une courbe donnée par une telle équation est dite lisse, si le système suivant n'admet pas de solutions

$$\begin{cases} y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \\ a_1y = 3x^2 + 2a_2x + a_4 \\ 2y + a_1x + a_3 = 0 \end{cases}.$$

3. Le point $\mathcal{O} = [0,1,0]$ est le seul point à l'infini et qu'il n'est pas singulier. En effet

$$\frac{\partial F}{\partial Z}(0,1,0) = 1$$

avec

$$F(X,Y,Z) = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3.$$

.

Exemple 14

Considérons sur $\mathbb{R}$ les deux courbes E_1, E_2

$$\begin{aligned} E_1 &: y^2 = x^3 + x, \\ E_2 &: y^2 = x^3 + x^2, \end{aligned}$$

la courbe E_1 est lisse. En effet

$$(\frac{\partial f}{\partial x}(x,y), \frac{\partial f}{\partial y}(x,y)) = (0,0) \Leftrightarrow \begin{cases} 3x^2 + 1 = 0 \\ 2y = 0 \end{cases} \Leftrightarrow \begin{cases} x = \pm\frac{i}{\sqrt{3}} \\ y = 0 \end{cases}$$

or les points $\left(\pm\frac{i}{\sqrt{3}},0\right)$ *ne sont pas sur la courbe* E_1.

Pour la courbe E_2, *le point* $(0,0)$ *est un point sur la courbe et on vérifie aisément que*

$$\frac{\partial f}{\partial x}(0,0)=\frac{\partial f}{\partial y}(0,0)=0.$$

Ainsi le point $(0,0)$ *est un point singulier.*

La non-singularité d'une courbe elliptique donnée par une forme de Weierstrass est détecté par la valeur non-nulle du discriminant $\triangle$ de E.

Nous définissons les quantités suivantes :

$$\begin{aligned} b_2 &= a_1^2+4a_2,\\ b_4 &= 2a_4+a_1a_3,\\ b_6 &= a_3^2+4a_6,\\ b_8 &= a_1^2a_6-a_1a_3a_4+4a_2a_6+a_2a_3^2-a_4^2. \end{aligned}$$

Definition 15 ***Discriminant et j-invariant***

Le discriminant $\triangle$ *d'une courbe sur* K *donnée par une équation de Weierstrass généralisée*

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

est la quantité

$$\triangle=-b_2^2b_8-8b_4^3-27b_6^2+9b_2b_4b_6.$$

Le j-invariant de la courbe elliptique E *est la quantité*

$$j(E)=\frac{c_4^3}{\triangle}$$

avec

$$c_4=b_2^2-24b_4.$$

Corollaire 16 *Soit* E *une courbe elliptique sur* K *donnée par une équation de Weierstrass .*

1. Si $Car(K)\neq 2$, *la courbe* E *prend une forme simplifiée*

$$E:\quad y^2=4x^3+b_2x^2+2b_4x+b_6.$$

2. Si $Car(K)\neq 2,3$, *la courbe* E *prend une forme simplifiée*

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

et dans ce cas

$$\begin{cases} \triangle=-16\left(4A^3+27B^2\right)\\ j(E)=-1728\frac{(4A)^3}{\triangle} \end{cases}$$

Preuve. *1. Supposons* $Car\,(K) \neq 2$ *et que la courbe* E *est donnée par l'équation de Weierstrass (1)*

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

complétons le carré, nous obtenons

$$\begin{aligned}\left(y + \frac{1}{2}(a_1x + a_3)\right)^2 &= x^3 + a_2x^2 + a_4x + a_6 + \frac{1}{4}(a_1x + a_3)^2 \\ &= x^3 + \frac{1}{4}\left(a_1^2 + 4a_2\right)x^2 + \frac{1}{2}(a_1a_3 + 2a_4)\,x + \frac{1}{4}\left(a_3^2 + 4a_6\right) \\ &= x^3 + \frac{b_2}{4}x^2 + \frac{b_4}{2}x + \frac{b_6}{4}\end{aligned}$$

d'où

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

avec y *remplacé par*

$$\frac{1}{2}(y - a_1x - a_3)$$

2. Supposons $Car\,(K) \neq 2,\ 3$*, complétant le cube dans*

$$y^2 = x^3 + \frac{b_2}{4}x^2 + \frac{b_4}{2}x + \frac{b_6}{4}$$

nous obtenons

$$\begin{aligned}y^2 &= (x + \frac{b_2}{12})^3 - \frac{b_2^2}{48}x - \frac{b_2^3}{1728} + \frac{b_4}{2}x + \frac{b_6}{4} \\ &= (x + \frac{b_2}{12})^3 - \frac{1}{48}(b_2^2 - 24b_4)x - \frac{1}{1728}(b_2^3 - 432b_6) \\ &= x^3 - \frac{1}{48}(b_2^2 - 24b_4)(x - \frac{b_2}{12}) - \frac{1}{1728}(b_2^3 - 432b_6) \\ &= x^3 - \frac{1}{48}(b_2^2 - 24b_4)x + \frac{1}{576}b_2^3 - \frac{1}{24}b_2b_4 - \frac{1}{1728}b_2^3 + \frac{432}{1728}b_6) \\ &= x^3 - \frac{1}{48}(b_2^2 - 24b_4)x + \frac{1}{864}b_2^3 - \frac{1}{24}b_2b_4 + \frac{1}{4}b_6 \\ &= x^3 - \frac{1}{48}(b_2^2 - 24b_4)x - \frac{1}{864}(-b_2^3 + 36b_2b_4 - 216b_6)\end{aligned}$$

donc, la forme simplifiée de Weierstrass est

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

avec y *remplacé par* $y - \frac{1}{2}(a_1x + a_3)$ *et* x *remplacé par* $x - \frac{b_2}{12}$*. De plus*

$$A = -\frac{c_4}{48},\ B = -\frac{c_6}{864},\ c_6 = -b_2^3 + 36b_2b_4 - 216b_6.$$

Ainsi

$$\triangle = -16(4A^3 + 27B^2),\ j(E) = \frac{c_4^3}{\triangle} = -1728\frac{(4A)^3}{\triangle}.$$

■

Lemme 17 *Soit E une courbe sur K donnée par l'équation de Weierstrass*

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

Soient $\triangle$ son discriminant et $j(E)$ son j-invariant. Le changement de variables

$$(x, y) \leftarrow \left(u^2x + r\ , u^3y + u^2sx + t\right)$$

avec $r, s, t, u\ (\neq 0) \in K\ (\overline{K})$ transforme l'équation de Weierstrass précédente en l'équation

$$E' : y^2 + a_1'xy + a_3'y = x^3 + a_2'x^2 + a_4'x + a_6',\ a_i' \in K\ (\overline{K})$$

avec

$$\begin{aligned}
ua_1' &= a_1 + 2s\ , \\
u^2a_2' &= a_2 - sa_1 + 3r - s^2, \\
u^3a_3' &= a_3 + ra_1 + 2t\ , \\
u^4a_4' &= a_4 - sa_3 + 2ra_2 - (t + rs)\, a_1 + 3r^2 - 2st\ , \\
u^6a_6' &= a_6 + ra_4 + r^2a_2 - ta_3 - rta_1 + r^3 - t^2.
\end{aligned}$$

De plus

$$\begin{aligned}
u^{12}\Delta' &= \Delta, \\
j\left(E'\right) &= j(E)
\end{aligned}$$

avec Δ' et $j(E')$ le discriminant et le j-invariant de E'.

Preuve. *Il suffit de remplacer x et y par leurs nouvelles expressions pour obtenir les relations désirées.* ■

Definition 18 *Un changement de coordonnées de la forme*

$$\begin{cases} \acute{x} &= u^2x + r; \\ \acute{y} &= u^3y + u^2sx + t; \end{cases}$$

est dit admissible.

Théorème 19 *Soit E une courbe sur K donnée par une équation de Weiestrass. Alors*

$$E \text{ est non-singulière } \Leftrightarrow \Delta \neq 0.$$

Preuve. *1. Supposons que $\Delta \neq 0$, et montrons que E est lisse,*

Soit l'équation générale de Weierstrass

$$E : f(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0$$

regardons E comme une courbe de $\mathbb{P}_2(K)$:

$$F(X,Y,Z) = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3 = 0.$$

Le point à l'infini $\mathcal{O} = [0,1,0]$ n'est pas un point singulier de E , car

$$\frac{\partial F}{\partial Z}(\mathcal{O}) = 1 \neq 0.$$

Supposons que E admet un point singulier $P_0 = (x_0, y_0)$,
Par le changement de variable

$$(x,y) \leftarrow (x - x_0, y - y_0)$$

nous ramenons le point P_0 en le point $(0,0)$, ce changement de varibles est admissible car

$$u = 1,\ r = -x_0,\ s = 0,\ t = -y_0.$$

Cette transformation ne modifie pas le discriminant, donc

$$\acute{\Delta} = \Delta$$

avec $\acute{\Delta}$ le discriminant de la courbe $E^{'}$ d'équation

$$E' : f'(x,y) = y^2 + \acute{a}_1\ xy + \acute{a}_3y - x^3 - \acute{a}_2x^2 - \acute{a}_4x - \acute{a}_6$$

et isomorphe à E. On a

$$\acute{a}_6 = \acute{f}(0,0) = 0 \quad , \acute{a}_3 = \frac{\partial \acute{f}}{\partial y}(0,0) = 0, \acute{a}_4 = \frac{\partial \acute{f}}{\partial x}(0,0) = 0$$

donc, E' s'écrit

$$E' : \acute{f}(x,y) = y^2 + \acute{a}_1\ xy - x^3 - \acute{a}_2x^2.$$

Le disctiminant de cette équation est nul, ce qui contredit l'hypothèse ; c'est-à-dire E n'admet pas des points singuliers.

2. Supposons que E est lisse, et montrons que $\Delta \neq 0$;
Pour simplifier les calculs, nous allons supposer que $Car(K) \neq 2, 3$
a)Si $Car(K) \neq 2$, alors E s'écrit

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

$P_0 = (x_0, y_0) \in E$ *est un point singulier* $\Leftrightarrow 2y_0 = 12x_0^2 + 2b_2x_0 + 2b_4 = 0$.*En d'autre terme, les points singuliers sont éxactement les points de la forme* $(x_0, 0)$, *avec* x_0 *est une racine double de l'équation*

$$4x^3 + b_2x^2 + 2b_4x + b_6 = 0$$

or cette équation admet une racine double si et seulement si son discriminant qui égale $16\triangle$ *est nul.*

b)Si car $(E) \neq 3$, *donc la courbe* E *prend la forme simplifiée suivante :*

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

Si la coubre est singulière en un point $P_0 = (x_0, y_0)$, *alors*

$$\begin{cases} 2y_0 = 0 \\ 3x_0^2 + A = 0 \end{cases} \Leftrightarrow \begin{cases} y_0 = 0 \\ x_0^2 = -\frac{A}{3} \end{cases}$$

par conséquent

$$y_0^2 = 0 = x_0^3 + Ax_0 + B = \frac{2}{3}Ax_0 + B$$

donc

$$x_0 = -\frac{3B}{2A}$$

il s'ensuit que

$$x_0^2 = \frac{9B^2}{4A^2} = -\frac{A}{3} \Leftrightarrow -16\left(4A^3 + 27B^2\right) = 0 = \Delta.$$

■

On a vu qu'avec des changements de variables admissibles, on peut passer d'une forme de Weierstrass à une autre. Ici on donne un résultat qui permet de ramèner une quartique à la forme de Weierstrass (voir [2]). Considérons la courbe d'équation

$$y^2 = f_0 + f_1x + f_2x^2 + f_3x^3 + f_4x^4 \tag{1.2}$$

définie sur K. Supposons que $car\,(K) \neq 2$ et que f_4 est un carré dans K.

Proposition 20 *La courbe affine d'équation (1.2) se ramène à l'équation de Weierstrass*

$$Y^2 + 2g_1XY + 2h_1Y = X^3 - 4g_0X^2 - 4h_0X$$

avec g_1, g_0, h_1, *et* h_0 *vérifiant*

$$f_0 + f_1x + f_2x^2 + f_3x^3 + f_4x^4 = \left(x^2 + g_1x + g_0\right)^2 + h_1x + h_0.$$

Preuve. Supposons que $f_4 = 1$, si non on divise par f_4. Posons

$$y^2 = G(x)^2 + H(x)$$

avec

$$G(x) = x^2 + g_1x + g_0 \quad \text{et} \quad H(x) = h_1x + h_0$$

ainsi

$$(y - G(x))(y + G(x)) = H(x)$$

posons

$$T = y + G(x)$$

on obtient

$$y - G(x) = \frac{H(x)}{T}$$

$$2G(x) = T - \frac{H(x)}{T}. \tag{1.3}$$

En multipliant l'équation (1.3) par T^2 et en posant $S = Tx$, on obtient

$$2S^2 + 2g_1TS + h_1S = T^3 + 2g_0T^2 - h_0T$$

multiplions par 2^3 et posons

$$X = 2T,\ Y = 4S$$

nous obtenons la forme de Weierstrass

$$Y^2 + 2g_1XY + 2h_1Y = X^3 - 4g_0X^2 - 4h_0X.$$

Les changements de variables sont

$$\begin{cases} X &= 2(y + x^2 + g_1x + g_0) \\ Y &= 4x(y + x^2 + g_1x + g_0). \end{cases}$$

■

Exemple 21 *Trouvons la forme de Weierstrass par la méthode de Cassels pour la famille des courbes*

$$y^2 + (x^2 + kx + 1)y + (x + 1)^3 = 0,\ k \in \mathbb{Q}.$$

En multipliant par 4 *et en complétant le carré de* y*, on trouve*

$$W^2 = x^4+2(k-2)x^3+(k^2-10)x^2+2(k-6)x-3, W = 2y+x^2+kx+1... \tag{1}$$

posons

$$W^2 = G^2(x) + H(x),$$

avec

$$G(x) = x^2 + g_1 x + g_0,\ H(x) = h_1 x + h_0$$

on obtient

$$W^2 = x^4 + 2g_1 x^3 + (2g_0 + g_1)x^2 + (2g_1 g_0 + h_1)\, x + g_0^2 + h_0$$

par identification avec (1), *on trouve*

$$\begin{cases} g_1 &= k-2, \\ g_0 &= 2k-7, \\ h_1 &= -4k^2 + 24k - 40, \\ h_0 &= -4k^2 + 28k - 52, \end{cases}$$

par suite

$$\begin{cases} a_1 &= 2(k-2), \\ a_2 &= -4(2k-7), \\ a_3 &= -8(k^2 - 6k + 10), \\ a_4 &= 4k^2 - 28k + 52, \\ a_6 &= 0. \end{cases}$$

Ainsi la forme de Weierstrass est donnéé par

$$Y^2 + 2(k-2)XY - 8(k^2 - 6k + 10)Y = X^3 - 4(2k-7)X^2 + 4k^2 - 28k + 52.$$

Les changement de variables sont donnés par

$$\begin{aligned} X &= 2(y + x^2 + (k-2)x + (2k-7)), \\ Y &= 4x(y + x^2 + (k-2)x + (2k-7)). \end{aligned}$$

1.3.2 Nature des points singuliers

Soit E une courbe définie sur K par la forme de Weierstrass

$$f(x,y) = y^2 + a_1 xy + a_3 y - x^3 - a_2 x^2 - a_4 x - a_6 = 0$$

Supposons que la courbe E a un point singulier $P = (x_0, y_0)$, i.e.,

$$\frac{\partial f}{\partial x}(P) = \frac{\partial f}{\partial y}(P) = 0.$$

Faisons le devellopement de *Taylor* de f au voisinage de $P = (x_0, y_0)$, on obtient

$$f(x,y) - f(x_0,y_0) = [(y-y_0) - \alpha(x-x_0)]\,[(y-y_0) - \beta(x-x_0)] - (x-x_0)^3$$

avec

$$\alpha, \beta \in \overline{K}.$$

Definition 22 *Le point singulier P est dit :*

1. Un nœud si $\alpha \neq \beta$. Dans ce cas, la courbe E admet deux tangentes distinctes au point P

$$y - y_0 = \alpha (x - x_0) \ \ et \quad y - y_0 = \beta (x - x_0) \ .$$

2. Un point de rebroussement si $\alpha = \beta$. Dans ce cas, la courbe E admet deux tangentes confondues au point P

$$y - y_0 = \alpha (x - x_0) .$$

Aussi, la nature du point singulier P peut être déterminée par l'invariant

$$c_4 = b_2^2 - 24 b_4.$$

Proposition 23 *Soit une cubique E définie sur K par.*

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6.$$

Alors

1. La cubique E admet un nœud si et seulement si $\triangle = 0$ et $c_4 \neq 0$.

2. La cubique E admet un point de rebroussement si et seulement si $\triangle = 0$ et $c_4 = 0$.

Preuve. *Voir [18]* ■

Exemple 24 *1. Soit E la courbe définie sur $\mathbb{R}$ par*

$$E : y^2 = \left(x^2 + x + 14\right)(x + 1) = x^3 + 2x^2 + 15x + 14$$

on a

$$\triangle (E) = -172480 \neq 0.$$

Ainsi E est une courbe elliptique.

2. Soit E une courbe elliptique définie sur $\mathbb{R}$ par

$$E : y^2 = (x + 1)^2 (x + 5) ,$$

on a

$$\triangle (E) = 0 \ et \ \ c_4 = 256$$

donc E est singulière et admet un noeud.

3. Soit E une courbe elliptique définie sur $\mathbb{R}$ par

$$E : y^2 = x^3 + 6x^2 + 12x + 8 = (x + 2)^3$$

et

$$\triangle (E) = 0 \ \ et \ \ c_4 = 0$$

donc E est singulière et admet un point de rebroussement.

1.3.3 Loi de groupe

Soit E une courbe elliptique definie sur K, on montre ici qu'on peut munir E, (en particulier $E(K)$) de la structure d'un groupe abélien. Avant de définir la loi d'addition, rappellons deux résultats très utiles.

Théorème 25 *(Théorème de Bezout) Soient C et D deux courbes planes projectives, sans composante commune, définies respectivement par deux polynômes homogènes F et G de $\overline{K}[X,Y,Z]$, de degrés respectifs m et n. Alors le nombres de points d'intersection, comptés avec multiplicité, de ces deux courbes est égale à mn.*

En réalité, le résultat qui va vraiment nous intéresser est le cas ou' l'une des deux cubiques est la réunions de trois droites. Si une droite coupe une cubique en deux points, elle la coupera en un troisième point.

Lemme 26 *(Théorème des neuf points) Soient $P_1, ..., P_9$ les neuf points communs à deux cubiques C et D, dont l'une au moins est irréductible. Si les huit premiers points sont distincts, et qu'une cubique E passe par ces huit points, alors elle passe par le neuvième.*

Loi d'addition

L'addition de deux points sur une courbe elliptique E est rendu possible par la propriété suivante, qui est un cas particulier du théorème de Bézout sur l'intersection de courbes algériques, *une droite sécante passant par deux points de la courbe recoupe la courbe en un troisième point.* Pour définir l'addition de deux points distincts P, Q sur la courbe elliptique E, on remarque d'abord que par ces deux points passe une droite bien définie. A cause de la propriété indiquée, cette droite recoupe donc la courbe E en un troisième point R. Intuitivement, ce point R de la courbe, est bien défini à partir des deux points P et Q. Donc, si l'on veut donner un sens à l'addition de deux points P et Q sur une cubique, il semble assez naturel de décider que leur somme est le troisième point R (issu de l'intersection entre la cubique et la droite formée par les deux points qu'on veut additionner), en d'autre terme ce point R de la courbe serait un bon candidat pour être leur somme. Notons $R := P \oplus Q$.

Le problème de cette définition est que, la loi $\oplus$ n'admet aucun élément neutre, et donc a fortiori, ce ne peut pas être une loi de groupe. Pour réctifier cela, nons pouvons modifier la construction précédente comme nous allons le voir dans cette section .

On choisit arbitrairement un point $\mathcal{O}$ sur la cubique (le point à l'infini). Soient P et Q les deux points qu'on veut sommer. Définissons sur la cubique la loi + par

$$P + Q = \mathcal{O} \oplus (P \oplus Q).$$

Nous pouvons alors énoncer le théorème fondamental suivant.

Théorème 27 *La loi + confère à*

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

la structure de groupe abélien.

Pour prouver ce théorème il suffit de démontrer les axiomes qui définissent une loi de groupe abélien : caractère interne, associativité, existence d'un élément neutre, élément opposé et commutativité.

1. **caractère interne de la loi :** immédiat par construction.
2. **Existence d'un élément neutre :** c'est le point $\mathcal{O}$ qui joue le rôle de neutre :

$$P + \mathcal{O} = \mathcal{O} \oplus (P \oplus \mathcal{O}) = P.$$

3. **Commutativité :**
La sécante (PQ) coïncide avec la sécante (QP) ainsi

$$P + Q = \mathcal{O} \oplus (P \oplus Q) = \mathcal{O} \oplus (Q \oplus P) = Q + P.$$

4. **Construction de $-\mathbf{P}$:** Constriusons la tangente à E en $\mathcal{O}$ et notons R le deuxième point d'intersection entre cette cubique et la tangente. Alors

$$-P = P \oplus R.$$

En effet

$$P + (P \oplus R) = \mathcal{O} \oplus [P + (P \oplus R)] = \mathcal{O} \oplus R = \mathcal{O}$$

5. **l'associativité :** Soient P, Q et R trois points distincts de la cubique E. Nous souhaitons montrer que

$$(P + Q) + R = P + (Q + R)\,.$$

Remarquons qui'il suffit de montrer que

$$(P + Q) \oplus R = P \oplus (Q + R)\,,$$

puisqu'alors

$$\begin{aligned}
(P + Q) + R &= \mathcal{O} \oplus [(P + Q) \oplus R] \\
&= \mathcal{O} \oplus [\mathcal{O} \oplus (P \oplus Q) \oplus R] \\
&= \mathcal{O} \oplus [\mathcal{O} \oplus P \oplus (Q + R)] \\
&= \mathcal{O} \oplus [P \oplus (Q + R)] \\
&= P + (Q + R)\,.
\end{aligned}$$

Considérons les points $\mathcal{O}$, P, Q, R, $P \oplus Q$, $P + Q, Q \oplus R$ et $Q + R$ et soient

L_1 : la droite passant par P et Q

L_2 : la droite passant par Q et R
L_3 : la droite passant par $\mathcal{O}$et $(P \oplus Q)$
L_4 : la droite passant par $\mathcal{O}$ et $(Q \oplus R)$
L_5 : la droite passant par $(P+Q)$ et R
L_6 : la droite passant par $(Q+R)$ et P.

Soit C la cubique formée de la réunion des droites L_1, L_4, L_5, et C' celle définie de la même, mais avec les droites L_2, L_3 et L_6. Alors

$$\begin{aligned} E \cap C &= \{\mathcal{O}, P, Q, R, P \oplus Q, Q \oplus R, P+Q, Q+R, (P+Q) \oplus R\} \\ E \cap C' &= \{\mathcal{O}, P, Q, R, P \oplus Q, Q \oplus R, P+Q, Q+R, P \oplus (Q+R)\}. \end{aligned}$$

Le théorème des neuf points assure alors, comme E est irréductible, que

$$(P+Q) \oplus R = P \oplus (Q+R)$$

et

$$(P+Q) + R = P + (Q+R)$$

et donc la courbe E passe par le neuvième point.

Nous donnons maintenant le principe des calculs explicites de coordonnées :

Calculs analytique

Cette construction géométrique se traduit aussi par des équations, on peut calculer les coordonnées (x_{P+Q}, y_{P+Q}) du point $P+Q$ en fonction de celles de $P = (x_P, y_P)$ et $Q = (x_Q, y_Q)$.

Soit E une courbe elliptique sur K donnée par sa forme de Weierstrass

$$F(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0;$$

Coordonnées de $-P$. Soit $P = (x_P, y_P)$ un point de la courbe E.

Soit (L) la droite passant par P et $\mathcal{O}$, alors

$$L : aX + bY + cZ = 0,$$

tel que

$$(a,b,c) \neq 0_{K^3}.$$

La droite (L) passe par $\mathcal{O}$, donc

$$b = 0.$$

De même $P \in L$, alors

$$ax_P + c = 0$$

donc

$$c = -ax_P.$$

On trouve par suite la droite (L) comme suit

$$L : x - x_P = 0$$

donc

$$x = x_P.$$

Par substitution dans l'équation de la courbe E, on trouve

$$F(x_P, y) = y^2 + (a_1 x_P + a_3)\, y - \left(x_P^3 + a_2 x_P^2 + a_4 x_P + a_6\right) = 0.$$

Cette équation admet deux racines y_P et y_{-P} , avec

$$-P = (x_P, y_{-P}),$$

donc

$$F(x_P, y) = \alpha\,(y - y_P)\,(y - y_{-P})$$

avec

$$\alpha = 1, \quad y_P + y_{-P} = -a_1 x_P - a_3$$

i.e.

$$y_{-P} = -y_P - a_1 x_P - a_3$$

donc les coordonnées de $-P$ l'opposé de P sont

$$-P = (x_P, -y_P - a_1 x_P - a_3)$$

Coordonnées de $P+Q$ pour $P \neq Q$. Soient (x_P, y_P) et (x_Q, y_Q) les coordonnées de P et Q, avec P et Q deux points de la courbe E.

1. Si

$$x_P = x_Q,\ y_P + y_Q + a_1 x_P + a_3 = 0$$

alors on a

$$P + Q = \mathcal{O}$$

2. Si $x_P \neq x_Q$ la droite (PQ) a pour équation $y = \alpha x + \beta$, avec

$$\begin{aligned} \alpha &= \frac{y_Q - y_P}{x_Q - x_P}, \\ \beta &= y_P - \alpha x_P \quad \text{ou bien} \quad \beta = y_Q - \alpha x_Q\ . \end{aligned}$$

Par substitution dans l'équation de la courbe E, on trouve

$$F(x, \alpha x + \beta) = -x^3 + \left(\alpha^2 + \alpha a_1 - a_2\right) x^2 + (2\alpha\beta + \beta a_1 + \alpha a_3 - a_4)\, x + \beta^2 + \beta a_3 - a_6 = 0.$$

Cette équation a comme racines x_P, x_Q et x_R avec $R = (x_R, y_R)$ est le troisième point d'intersection entre la droite (PQ) et la courbe E. Donc

$$F(x, \alpha x + \beta) = \gamma\,(x - x_P)\,(x - x_Q)\,(x - x_R).$$

On trouve

$$\gamma = -1$$

et on déduit d'après les relations racines/coefficients chez les polynômes que

$$x_P + x_Q + x_R = \alpha^2 + \alpha a_1 - a_2$$

donc

$$\begin{aligned} x_R &= x_{P+Q} = \alpha^2 + \alpha a_1 - a_2 - x_P - x_Q \\ y_R &= y_{P+Q} = \alpha x_R + \beta \end{aligned}$$

c'est-à-dire, les coordonnées de R sont alors

$$R = \left(\alpha^2 + \alpha a_1 - a_2 - x_P - x_Q, \alpha x_R + \beta \right) = (x_R, y_R) \tag{1.4}$$

et donc

$$\begin{aligned} P + Q &= -R = (x_R, -y_R - a_1 x_R - a_3) \\ &= \left(x_R, -\left(\alpha + a_1\right) x_R - \left(a_3 + \beta\right)\right). \end{aligned}$$

Coordonnéés de $2P$. Le point $P + P$ se note naturellement $2P$. Dans ce cas, on considère la droite tangente en P à la courbe E d'équation

$$y = \alpha x + \beta$$

posons

$$f(x, y) = y^2 + a_1 xy + a_3 y - x^3 - a_2 x^2 - a_4 x - a_6$$

on a

$$df = \frac{\partial f}{\partial y} dy + \frac{\partial f}{\partial x} dx = 0$$

ce qui donne

$$\frac{dy}{dx} = \frac{3x^2 + 2a_2 x + a_4 - a_1 y}{2y + a_1 x + a_3}.$$

Ainsi

$$\alpha = \frac{3x_P^2 + 2a_2 x_P + a_4 - a_1 y_P}{2y_P + a_1 x_P + a_3}$$

en substituant α par cette valeur dans la formule trouvée (1.4), on obtient les coordonnées du troisième point d'intersection

$$R = (\overline{x}_{2P}, \overline{y}_{2P}).$$

Ainsi

$$2P = -R = \left(\overline{x}_{2P}, -\overline{y}_{2P} - a_1 \overline{x}_{2P} - a_3\right).$$

Exemple 28 *1. Soit E une courbe elliptique définie sur $\mathbb{Q}$ par*

$$E : y^2 = x^3 - 25x$$

Soient $P = (5, 0)$ et $Q = (-4, 6)$ deux points de la courbe E. On veut déterminer $P + Q$. La droite sécante (L) passant par P et Q a pour équation

$$L : y = \frac{-2}{3}(x - 5).$$

Pour trouver le troisième point R d'intersection de la courbe E avec la droite L, il suffit de résoudre le système

$$\begin{cases} y = \frac{-2}{3}(x - 5) & (1) \\ y^2 = x^3 - 25x & (2) \end{cases}$$

par substitution de l'équation (1) dans l'équation (2), on trouve

$$(x - 5)(x + 4)(9x + 5) = 0.$$

Ainsi

$$x_R = -\frac{5}{9} \ et \quad y_R = \frac{100}{27}$$

donc

$$P + Q = -R = \left(-\frac{5}{9}, -\frac{100}{27}\right).$$

1.3.4 Courbes birationnellement équivalentes et courbes isomorphes

Definition 29 *Soient E et $\acute{E}$ deux courbes planes projectives définissant des courbes elliptiques définies sur K, et soient P, Q, R trois polynômes homogènes de $K[X, Y, Z]$ de même degré d. Les trois polynômes définissent une application rationnelle (morphisme) ϕ de E dans $\acute{E}$ si pour tout point (X, Y, Z) de $E\left(\overline{K}\right)$, sauf peut-être un nombre fini,*

$$\phi(X, Y, Z) = (P(X, Y, Z),\ Q(X, Y, Z),\ R(X, Y, Z))$$

est définie et appartient à $\acute{E}\left(\overline{K}\right)$. En coordonnées affines, l'application ϕ sera :

$$\phi(x, y) \to \left(\frac{P(x, y, 1)}{R(x, y, 1)}, \frac{Q(x, y, 1)}{R(x, y, 1)}\right).$$

Definition 30 *Soient E et $\acute{E}$ deux courbes elliptiques du plan projectif $\mathbb{P}_2(K)$. Soit ϕ une application rationnelle de E dans $\acute{E}$, on dira que ϕ est birationnelle s'il existe une application rationnelle ψ telle qu'en tout point , sauf en un nombre fini, les applications $\phi \circ \psi$ et $\psi \circ \phi$ sont égales à l'identité. Dans ce cas on dit que les deux courbes E et $\acute{E}$ sont birationnellement équivalentes.*

Definition 31 ***(Isogénie).*** *Soit* $(E, \mathcal{O})$ *et* $\left(\acute{E}, \mathcal{O}'\right)$ *deux courbes elliptiques définies sur* K. *Une isogénie sur* K $(\overline{K})$ *(un homomorphisme de courbes elliptiques) de* E *dans* $\acute{E}$ *est une application rationnelle* ϕ *non identiquement nulle et telle que* $\phi(\mathcal{O}) = \mathcal{O}'$.

Théorème 32 *Tout isomorphisme (isogénie bijective) sur* K $(\overline{K})$ *entre courbes elliptiques données par leurs modèles de Weierstrass est de la forme :*

$$(x, y) \leftarrow \left(u^2 x + r\ , u^3 y + u^2 s x + t\right) \quad avec\ u(\neq 0), r, s, t \in K(\overline{K}).$$

Remarque 33 *En coordonnées projectives* $\left(u^2 x + r, u^3 y + u^2 s x + t\right)$ *devient*

$$\left(u^2 X + rZ\ , u^3 Y + u^2 s X + tZ, Z\right)$$

.

Théorème 34 *Soit* K *un coprs de caractéristique* $Car(K) \neq 2, 3$. *Deux courbes données par leurs équations de Weierstrass dont le discriminant est non nul sont isomorphes sur* $\overline{K}$ *si et seulement si elles ont le même* $j-$*invariant.*

Preuve. *Soient* E_1 *et* E_2 *deux courbes ;*

1. Supposons que E_1 *est isomorphe à* E_2, *donc il éxiste un changement de coordonnées admissible (sur* $\overline{K}$ *), Par le lemme* $(17 chapitre\ 1)$ *on déduit que*

$$j(E_1) = j(E_2)$$

2. Supposons que $j(E_1) = j(E_2)$, *montrons que* E_1 *et* E_2 *sont isomorphes (sur* $\overline{K}$*). Supposons que les équations de Weierstrass des deux courbes* E_1 *et* E_2 *sont*

$$E_1 \ : \ y^2 = x^3 + Ax + B; \qquad j(E_1) = -1728\frac{(4A)^3}{\triangle},$$
$$E_2 \ : \ y^2 = x^3 + \acute{A}x + \acute{B}; \quad j(E_2) = -1728\frac{(4A')^3}{\triangle'}.$$

Comme $j(E_1)$ *et* $j(E_2)$ *sont égaux, cela implique que*

$$A^3 \acute{B}^2 = B^2 \acute{A}^3$$

Cherchons un changement de variables admissible de la forme

$$(x, y) \leftarrow \left(u^2 x, u^3 y\right)$$

1. Si $A = 0$, *alors* $B \neq 0$ *car* $\Delta \neq 0$, *donc*

$$\acute{A} = 0, \quad \acute{B} \neq 0.$$

Nous obtenons un isomorphisme, en prenant

$$u = \left(\frac{B}{\acute{B}}\right)^{\frac{1}{6}} \in \overline{K}$$

2. Si $B = 0$, *alors* $A \neq 0$ *car* $\Delta \neq 0$, *donc*

$$\acute{B} = 0, \quad \acute{A} \neq 0.$$

Nous obtenons un isomorphisme, en prenant

$$u = \left(\frac{A}{\acute{A}}\right)^{\frac{1}{4}} \in \overline{K}.$$

3. Si A, $B \neq 0$, *alors*

$$A',\ B' \ \neq 0.$$

Nous obtenons un isomorphisme, en prenant

$$u = \left(\frac{A}{\acute{A}}\right)^{\frac{1}{4}} = \left(\frac{B}{\acute{B}}\right)^{\frac{1}{6}} \in \overline{K}.$$

■

1.3.5 Théorème de Mordell-Weil

Definition 35 *Soit* E *une courbe elliptique sur* K *definie par*

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad a_i \in K.$$

L'ensemble des points K-rationnels de E, *noté* $E(K)$ *est l'ensemble*

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

avec $\mathcal{O}$ *est le point à l'infini.*

Remarque 36 *L'ensemble* $E(K)$ *muni de la loi définie sur* E, *est un groupe abélien (sous groupe de* E*).*

Definition 37 *Un point* P *est dit d'ordre fini* $m \in \mathbb{N}^*$ *si*

$$mP = \underbrace{P + P + ... + P}_{m\ fois} = \mathcal{O} \ et \ \ nP \neq \mathcal{O} \ dèsque \ n < m.$$

Si un tel m *n'existe pas, le point* P *est dit point d'order infini.*

Remarque 38 *Pour tout entier* m *fini, les points d'ordre* m *forme un sous-groupe de* $E(K)$ *noté* $E(K)[m]$.

Le résultat le plus important est que tous les points à coordonnées rationnelles peuvent être construits par la méthode de la tangente et de la sécante à partir d'un nombre fini d'entre eux. plus précisement :

Théorème 39 *(Mordell-Weil) Le groupe des points $E(K)$, K corps des nombres est* ***de type fini,*** *en d'autre terme*

$$\exists\ P_1, ..., P_n \in E(K) : \forall Q \in E(K) : Q = m_1 P_1 + ... + m_n P_n,\ m_i \in \mathbb{Z}, i = \overline{1, n}$$

de plus

$$E(K) \simeq E(K)_{tors} \oplus \mathbb{Z}^r$$

avec

$$E(K)_{tors} = \{P \in E(K)\ /\ \exists m \in \mathbb{N}^* : mP = \mathcal{O}\}$$

et r entier positif, appelé ***le rang de la courbe*** *E, i.e. le nombre de copies de $\mathbb{Z}$, c'est donc le nombre de points d'ordre infini indépendant.*

Le groupe $E(K)$ prend le nom du **groupe de Mordell-Weil de** E, comme honneur pour les deux mathématiciens **Mordell (1922, $\mathbb{Q}$)** et **André Weil (1928, corps des nombres quelconque).**

Bien que le théorème de Mordell-Weil soit intéréssant telquel, il est en effet naturel de se demander, si on sait explicitement trouver le rang de la courbe elliptique, ainsi que les générateurs d'ordre fini ou non. Le cas des éléments d'ordre fini (qui forme le sous-groupe de torsion) est plus simple à résoudre à la main, et est même complètement résolu pour plusieurs cas de courbes elliptiques.

Maintenant, on donne quelques résultats sur le sous-groupe de torsion d'une courbe elliptique. Si la courbe E est définie sur $\mathbb{Q}$, le théorème de **Mazur** (conjecture d'**ogg**) décrit la structure possible du sous-groupe de torsion $E(K)_{tors}$.

Théorème 40 ***(Mazur)*** *Soit E une courbe elliptique sur $\mathbb{Q}$. Alors $E(\mathbb{Q})_{tors}$ est isomorphe à l'un des groupes suivants*

$$\begin{array}{cc} \mathbb{Z}/n\mathbb{Z}, & 1 \leq n \leq 10\ ,\ n = 12 \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z}, & 1 \leq m \leq 4. \end{array}$$

Remarque 41 *Nous savons que tous ces 15 cas peuvent se produisent. Voir le tableau suivant*

La courbe E	Le sous-groupe de torsion	Générateurs
$y^2 = x^3 - 2$	*triviale*	$\mathcal{O}$
$y^2 = x^3 + 8$	$\mathbb{Z}/2\mathbb{Z}$	$(-2, 0)$
$y^2 = x^3 + 4$	$\mathbb{Z}/3\mathbb{Z}$	$(0, 2)$
$y^2 = x^3 + 4x$	$\mathbb{Z}/4\mathbb{Z}$	$(2, 4)$
$y^2 - y = x^3 - x^2$	$\mathbb{Z}/5\mathbb{Z}$	$(0, 1)$
$y^2 = x^3 + 1$	$\mathbb{Z}/6\mathbb{Z}$	$(2, 3)$
$y^2 = x^3 - 43x + 166$	$\mathbb{Z}/7\mathbb{Z}$	$(3, 8)$
$y^2 + 7xy = x^3 + 16x$	$\mathbb{Z}/8\mathbb{Z}$	$(-2, 10)$
$y^2 + xy + y = x^3 - x^2 - 14x + 29$	$\mathbb{Z}/9\mathbb{Z}$	$(3, 1)$
$y^2 + xy = x^3 - 45x + 81$	$\mathbb{Z}/10\mathbb{Z}$	$(0, 9)$
$y^2 + 43xy - 210y = x^3 - 210x^2$	$\mathbb{Z}/12\mathbb{Z}$	$(0, 210)$
$y^2 = x^3 - 4x$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$	$[(2, 0), (0, 0)]$
$y^2 = x^3 + 2x^2 - 3x$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$	$[(3, 6), (0, 0)]$
$y^2 + 5xy - 6y = x^3 - 3x^2$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$	$[(-3, 18), (2, -2)]$
$y^2 + 17xy - 120y = x^3 - 60x^2$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$	$[(-40, 400), (30, -90)]$

L'utilité et l'avantage du théorème de **Mazur** est que si un point P d'une courbe elliptique à un d'ordre ≥ 13, alors P est forcément un point d'ordre infini. Le théorème de **Mazur** ne permet pas de calculer le sous-groupe de torsion d'une courbe elliptique, par contre le résultat suivant prouvé dit théorème de **Nagell-Lutz** donne un algorithme simple permettant de déterminer $E(\mathbb{Q})_{tors}$. Le théorème de Nagell-Lutz est un critère nécessaire pour qu'un point d'une courbe elliptique sur $\mathbb{Q}$ soit de torsion.

Théorème 42 ***(Nagell-Lutz)*** *Soient E une courbe elliptique définie sur $\mathbb{Q}$ donnée par une équation de Weierstrass*

$$y^2 = x^3 + Ax + B,\ A,\ B \in \mathbb{Z}$$

et supposons que $P = (x(P), y(P))$ un point de torsion non nul , $P \neq \mathcal{O}$. Alors

(**i**) *$x(P)$ et $y(P) \in \mathbb{Z}$.*

(**ii**) *Si P est d'ordre 2, alors*

$$y(P) = 0,\ x(P)^3 + Ax(P) + B = 0.$$

(**iii**) *Si P est d'ordre ≥ 3, alors :*

$$y(P)^2 \text{ divise } \left(4A^3 + 27B^2\right).$$

Exemple 43 *1. Considérons la courbe elliptique sur $\mathbb{Q}$ d'équation*

$$E_1 : y^2 = x^3 - 2$$

le polynôme x^3-2 *n'admet pas de racines rationnelles, donc* $E_1(\mathbb{Q})$ *ne contient aucun point d'ordre 2.*

Si $(x(P), y(P))$ *sont les coordonnées d'un point de torsion* P *d'ordre* ≥ 3*, alors* $y(P)$ *est un entier et* $y(P)^2$ *divise*

$$4A^3 + 27B^2 = 4 \times 27$$

ainsi

$$y(P) = \pm 1, \ \pm 2, \ \pm 3 \text{ ou } \pm 6$$

par suite $x(P)^3 = 3,\ 6,\ 11$ *ou* 38*, respectivement. Mais,* $x(P)$ *est un entier. On déduit que le sous-groupe de torsion* $E_1(\mathbb{Q})_{tors}$ *est trivial, i.e. contient seulement le point à l'infini*

$$E_1(\mathbb{Q})_{tors} = \{\mathcal{O}\}.$$

2. Considérons la courbe elliptique sur $\mathbb{Q}$ *d'équation*

$$E_2 : y^2 = x^3 - 43x + 166$$

le polynôme $x^3-43x+166$ *n'admet pas de racines rationnelles, donc* $E_2(\mathbb{Q})$ *ne contient aucun point d'ordre 2. On a*

$$4A^3 + 27B^2 = 2^{15}.13.$$

Alors, si $P = (x(P), y(P))$ *est un point de torsion d'ordre* ≥ 3*, on a*

$$y(P) \in \{\pm 1, \ \pm 2, \ \pm 4, \ \pm 8, \ \pm 16, \ \pm 32, \ \pm 64, \ \pm 128\}.$$

En résolvant l'équation

$$y^2 = x^3 - 43x + 166$$

pour ces valeurs de y*, on trouve que*

$$\{(3, \pm 8), (-5, \pm 16), (11, \pm 32)\}.$$

On a

$$\begin{aligned} 7(3,8) &= \mathcal{O}, \ 2(3,8) = (-5,-16), \ 3(3,8) = (11,-32), \\ 4(3,8) &= (11,32), \ 5(3,8) = (-5,16), \ 6(3,8) = (3,-8). \end{aligned}$$

Ainsi

$$E_2(\mathbb{Q})_{tors} = \{\mathcal{O}, (3,\pm 8), \ (-5,\pm 16), \ (11,\pm 32)\} = \langle (3,8) \rangle \simeq \mathbb{Z}/7\mathbb{Z}.$$

On a vu d'après le théorème de Mordell-Weil que le groupe $E(K)$ est isomorphe à $E(K)_{tors} \oplus \mathbb{Z}^r$. On essaye ici de déterminer la valeur de r (le rang de la courbe elliptique). Malheuresement on ne sait pas encore un algorithme pour déterminer exactement le rang r d'une courbe elliptique. Le théorème suivant nous donne une estimation du rang d'une courbe elliptique définie sur $\mathbb{Q}$:

Théorème 44 *Soit E une courbe elliptique sur $\mathbb{Q}$ donnée par la forme de Weierstrass*

$$y^2 = x^3 + Ax^2 + Bx,\ A, B \in \mathbb{Z}.$$

Alors,

$$r \leq \upsilon\left(A^2 - 4B\right) + \upsilon(B) - 1$$

avec $\upsilon(N)$ est le nombre des nombres premiers positifs qui divise l'entier N.

Exemple 45 *Soit E une courbe elliptique sur $\mathbb{Q}$ donnée par*

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

d'aprés le théorème ci-dessus, le rang r de cette courbe satisfait

$$r \leq \upsilon\left(3^2 - 4.2\right) + \upsilon(2) - 1 = \upsilon(1) + \upsilon(2) - 1 = 0$$

ainsi $r = 0$. Dans ce cas

$$E(\mathbb{Q}) = E(\mathbb{Q})_{tors}.$$

Chapitre 2

Sur certaines courbes de genre 1 de bidegré (2,2)

Dans ce chapitre, on s'intéresse à la recherche d'une forme de Weierstrass de certaines courbes de bidegré de genre 1. On présente l'algoritme de Harrache et Touafek qui permet à ramener une courbe de degré deux en x et y à la forme de Weierstrass. On souligne sur des exemples l'intérêt de la méthode pour mettre en évidence les points de torsion ou les points d'ordre infini, et pour obtenir des formes de Weierstrass tempérées, ainsi que la classification des fibres singuliers, pour plus de détailles, de résultats et le choix des exemples voir [9], [12-13], [16], [19-20].

2.1 Algorithme de Harrache et Touafek

La transformation classique exposée dans cassels faisant passer de l'équation d'une courbe de bidegré (2,2) à une équation de Weierstrass utilisent un point rationnel sur un corps K. Lorsque la courbe a plusieurs points définies dans un corps, il est parfois souhaitable d'obtenir une équation de Weierstrass où les autres points apparaissent de façon évidente.

Rappelons que si

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$$

est un modèle de Weierstrass pour une courbe elliptique E sur un corps K, la fonction X sur E possède (dans $\overline{K}$) deux zéros et un pôle double au point à l'infini $(\infty, \infty) = [0, 1, 0]$, tandis que la fonction Y possède (dans $\overline{K}$) trois zéros et un pôle triple en ce même point à l'infini.

1) Pour $X = 0$, on obtient

$$Y^2 + a_3Y = a_6$$

Cette équation admet deux racines Y_1, Y_2. Donc, la fonction X sur E possède deux zéros $(0, Y_1), (0, Y_2)$. Posons $X = \frac{1}{x}$, on trouve

$$x^3(Y^2 + a_1\frac{Y}{x} + a_3Y) = 1 + a_2x + a_4x^2 + a_6x.$$

Pour $x = 0$, on obtient $1 = 0$, impossible. Posons à nouveau $Y = \frac{1}{y}$ pour obtenir

$$x^3\left(1 + a_1\frac{y}{x} + a_3y\right) = y^2\left(1 + a_2x + a_4x^2 + a_6x^3\right).$$

Maintenant $x = 0$, implique que $y^2 = 0$, i.e.,

$$y = 0, 0 \Leftrightarrow Y = \infty, \infty.$$

En résumé, la fonction X sur E possède deux pôles $(\infty, \infty), (\infty, \infty)$.

2) Posons $Y = 0$, nous obtenons

$$X^3 + a_2X^2 + a_4X + a_6 = 0.$$

Cette équation admet trois racines X_1, X_2, X_3, i.e., on a trois zéros de la fonction Y

$$(X_1, 0), \ (X_2, 0), \ (X_3, 0).$$

En mettant $Y = \frac{1}{y}$, on obtient :

$$1 + a_1Xy + a_3y = y^2\left(X^3 + a_2X^2 + a_4X + a_6\right)$$

pour $y = 0$, on trouve $1 = 0$, impossible. Fnaisons le changement de variable suivant $X = \frac{1}{x}$, pour obtenir

$$x^3 + a_1x^2y + a_3x^3y = y^2\left(1 + a_2x + a_4x^2 + a_6x^3\right)$$

pour $y = 0$, on trouve : $x^3 = 0$, i.e.,

$$x = 0, \ 0, \ 0 \Leftrightarrow X = \infty, \ \infty, \ \infty$$

et la fonction Y possède trois pôles

$$(\infty, \infty), (\infty, \infty), (\infty, \infty).$$

Donc, lorsque la courbe de genre 1 (sur K) est donnée par un polynôme $F(x, y)$ du second degré en chaque variable, chercher une forme de Weierstrass revient à trouver deux fonctions X et Y sur la courbe E avec X (resp.Y) possédant un pôle double (resp.triple) à l'infini.

La méthode

Soit $F(x, y)$ un polynôme (sur K) de degré 2 en chacune de variables qui est une équation pour une courbe de genre 1 (i.e., le discriminant par rapport à l'une des

variables est de degré 3 ou 4). Considérons la courbe $F(x,y)=0$. En ordonnant le polynôme F par rapport à y puis par rapport à x, on obtient :

$$\begin{aligned} F(x,y) &= \left(ax^2+bx+c\right)y^2+\left(\acute{a}x^2+\acute{b}x+\acute{c}\right)y+\left(a^{"}x^2+b^{"}x+c^{"}\right) \\ &= \left(ay^2+\acute{a}y+a^{"}\right)x^2+\left(by^2+\acute{b}y+b^{"}\right)x+\left(cy^2+\acute{c}y+c^{"}\right). \end{aligned}$$

Notons :

$$\begin{aligned} M(x) &= ax^2+bx+c,\ N(x)=\acute{a}x^2+\acute{b}x+\acute{c},\ R(x)=a^{"}x^2+b^{"}x+c^{"}, \\ M_1(y) &= ay^2+\acute{a}y+a^{"},\ N_1(y)=by^2+\acute{b}y+b^{"},\ R_1(y)=cy^2+\acute{c}y+c^{"}. \end{aligned}$$

Posons

$$\begin{aligned} \widetilde{M}(x) &= x^2M\left(\frac{1}{x}\right),\ \widetilde{N}(x)=x^2N\left(\frac{1}{x}\right),\ \widetilde{R}(x)=x^2R\left(\frac{1}{x}\right), \\ \widetilde{M_1}(y) &= y^2M_1\left(\frac{1}{y}\right),\ \widetilde{N_1}(y)=y^2N_1\left(\frac{1}{y}\right),\ \widetilde{R_1}(y)=y^2R_1\left(\frac{1}{y}\right). \end{aligned}$$

Nous distinguons trois cas

I) : Un des huit polynômes M, R, M_1, R_1, $\widetilde{M}$, $\widetilde{R}$, $\widetilde{M_1}$, $\widetilde{R_1}$ **a un degré nul.**

En changeant au besoin x en y, x en $\frac{1}{x}$ ou y en $\frac{1}{y}$, on peut supposer que F s'écrit :

$$F(x,y) = a^{"}x^2+\left(by^2+\acute{b}y+b^{"}\right)x+\left(cy^2+\acute{c}y+c^{"}\right) \quad (1)$$

$$= (bx+c)y^2+\left(\acute{b}x+\acute{c}\right)y+\left(a^{"}x^2+b^{"}x+c^{"}\right). \quad (2)$$

Comme la courbe est de genre 1, on a $b\neq 0$. En considérons la forme (2), on voit que y possède deux pôles simples, l'un pour

$$x=\frac{-c}{b}$$

et l'autre noté A qui est un pôle de x. En considérant la forme (1) de F, on voit que x a un pôle double en A. En effet

$$F(x,y)=a^{"}x^2+\left(by^2+\acute{b}y+b^{"}\right)x+\left(cy^2+\acute{c}y+c^{"}\right).$$

Posons $X=\frac{1}{x}$, on obtient

$$F\left(\frac{1}{X},y\right)=a^{"}\frac{1}{X^2}+\left(by^2+\acute{b}y+b^{"}\right)\frac{1}{X}+\left(cy^2+\acute{c}y+c^{"}\right)$$

i.e.,

$$a^{"}+\left(by^2+\acute{b}y+b^{"}\right)X+\left(cy^2+\acute{c}y+c^{"}\right)X^2=0$$

pour $X = 0$, on trouve

$$a" = 0$$

ce qui est impossible. Considerons le changement de variable suivant

$$y = \frac{1}{Y}$$

on obient

$$a"Y^2 + \left(b + \acute{b}Y + b"Y^2\right) X + \left(c + \acute{c}Y + c"Y^2\right) X^2 = 0,$$

pour $X = 0$, on trouve

$$Y^2 = 0,$$

i.e.,

$$Y = 0, 0 \Leftrightarrow y = \infty, \infty.$$

Alors, x a un pôle double en

$$A = (\infty, \infty).$$

Considérons maintenant le changement de variable

$$y = \frac{1}{Y}$$

on obtient :

$$F\left(x, \frac{1}{Y}\right) = (bx + c) + \left(\acute{b}x + \acute{c}\right) Y + \left(a"x^2 + b"x + c"\right) Y^2 = 0.$$

Pour $Y = 0$, on trouve

$$x = \frac{-c}{b}$$

alors y a un pôle

$$\left(\frac{-c}{b}, \infty\right).$$

On met

$$x = \frac{1}{X}$$

on trouve

$$F\left(\frac{1}{X}, \frac{1}{Y}\right) = \left(a" + b"X + c"X^2\right) Y^2 + \left(\acute{b}X + \acute{c}X^2\right) Y + \left(bX + cX^2\right) = 0.$$

Pour $Y = 0$ (i.e., $y = \infty$), on trouve

$$X = 0 \Leftrightarrow x = \infty.$$

Donc, y a un pôle simple qui est

$$A = (\infty, \infty).$$

Par suite, la fonction

$$u = y\,(bx + c)$$

possède un pôle triple en A. Donc, en multipliant (2) par

$$(bx + c)$$

on trouve

$$u^2 + (bx + c)\,u = -a^{''}bx^3 - \left(bb^{''} + a^{''}c\right)x^2 - \left(bc^{''} + cb^{''}\right)x - cc^{''}$$

multiplions cette équation par $\left(ba^{''}\right)^2$ et on met à nouveau

$$X = -ba^{''}x,\ Y = ba^{''}u$$

on trouve

$$Y^2 - \acute{b}XY + (\acute{c}ba^{"})Y = X^3 - (ca^{"} + bb^{"})X^2 + ba^{"}\ (cb^{"} + bc^{"})X - (ba^{"})^2cc^{"}$$

qui est une forme de Weierstrass.

II) : Aucun des huit polynômes n'est constant mais l'un d'eux est de degré 1

On peut alors écrire

$$\begin{aligned} F(x,y) &= (bx + c)\,y^2 + \left(\acute{a}x^2 + \acute{b}x + \acute{c}\right)y + \left(a^{"}x^2 + b^{"}x + c^{"}\right) \quad (1)\\ &= \left(\acute{a}y + a^{"}\right)x^2 + \left(by^2 + \acute{b}y + b^{"}\right)x + (cy^2 + \acute{c}y + c^{"}) \quad (2)\end{aligned}$$

avec $b\acute{a} \neq 0$. Dans ce cas, x et y ont chacun deux pôles distincts, de plus x et y ont un pôle simple commun A.

La fonction

$$X = (bx + c)\left(\acute{a}y + a^{"}\right)$$

aura donc un pôle double en A, qui est un pôle simple de y. Alors le changement de variable

$$X = (bx + c)\left(\acute{a}y + a^{"}\right)$$

ramène l'équation

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

à l'équation

$$G(X,y) = 0$$

avec

$$\begin{aligned} G(X,y) &= \left(b^2X + c^2\acute{a}^2 - cb\acute{a}\acute{b} + b^2\acute{a}\acute{c}\right)y^2 \\ &\quad + \left(\left(b\acute{b} - 2c\acute{a}\right)X + 2c^2\acute{a}a^{"} - bc\acute{b}a^{"} - bc\acute{a}b^{"} + b^2ca^{"} + b^2\acute{a}c^{"}\right)y \\ &\quad + \left(X^2 + \left(bb^{"} - 2ca^{"}\right)X + c^2a^{"2} - bca^{"}b^{"} + b^2a^{"}c^{"}\right) \\ &= X^2 + \left(b^2y^2 + \left(b\acute{b} - 2c\acute{a}\right)y + \left(bb^{"} - 2ca^{"}\right)\right)X \\ &\quad + \left(b^2\acute{a}\acute{c} + c^2\acute{a}^2 - cb\acute{a}\acute{b}\right)y^2 + \left(2c^2\acute{a}a^{"} - bc\acute{b}a^{"} - bc\acute{a}b^{"} + b^2ca^{"} + b^2\acute{a}c^{"}\right)y \\ &\quad + \left(c^2a^{"2} - bca^{"}b^{"} + b^2a^{"}c^{"}\right). \end{aligned}$$

C'est-à-dire le cas **I.**

III) : Cas général, les huit polynômes sont de degré 2

On distingue deux cas :

a) La courbe affine définie par $F(x,y) = 0$ a un point $(x_0, y_0) \in K^2$.

Après une translation, on peut supposer que

$$x_0 = y_0 = 0$$

et on obtient

$$c^{"} = 0.$$

En posant

$$U = \frac{1}{x},\ V = \frac{1}{y}$$

on trouve

$$\begin{aligned} (c + \acute{c}V)U^2 + \left(b^{"}V^2 + \acute{b}V + b\right)U + \left(a^{"}V^2 + \acute{a}V + a\right) &= 0 \\ \left(a^{"} + b^{"}U\right)V^2 + \left(\acute{c}U^2 + \acute{b}U + \acute{a}\right)V + \left(cU^2 + bU + a\right) &= 0 \end{aligned}$$

et on est dans le cas **I** ou **II.**

b) Si la courbe projective d'équation affine $F(x,y) = 0$ a un point $K-$rationnel à l'infini, alors c'est le point double $(1,0,0)$ (ou $(0,1,0)$) et les tangentes au point $(1,0,0)$ (ou $(0,1,0)$) sont rationnelles. Il en résulte que le polynôme M a une racine $x_1 \in K$ (ou le polynôme M_1 a une racine $y_1 \in K$).

Soit

$$U = \frac{1}{x - x_1} \text{ (on peut poser } V = \frac{1}{y - y_1}\text{)}$$

l'équation $F(x,y) = 0$ devient alors

$$\begin{aligned} & y^2(a + U(2ax_1 + b)) + y(\acute{a} + U(2\acute{a}x_1 + \acute{b}) + U^2(\acute{a}x_1^2 + \acute{b}x_1 + \acute{c})) \\ & + a^{"} + U(2a^{"}x_1 + b^{"}) + U^2(a^{"}x_1^2 + b^{"}x_1 + c^{"}) \\ = \ & U^2(a^{"}x_1^2 + b^{"}x_1 + c^{"} + y(\acute{a}x_1^2 + \acute{b}x_1 + \acute{c})) \\ & + U((2ax_1 + b)y^2 + (2\acute{a}x_1 + \acute{b})y + 2a^{"}x_1 + b^{"}) + ay^2 + \acute{a}y + a^{"} = 0, \end{aligned}$$

et on est dans le cas **I** ou **II.**

Remarque 46 *Le cas d'une courbe de genre* 1 *définie par un polynôme de degré* 3 *en* x *et* y *avec un point rationnel* $(x_0, y_0) \in K^2$ *se ramène au calculs précédent. Supposons que* F *s'écrive :*

$$F(x,y) = x^3 + ax^2y + bxy^2 + cy^3 + dx^2 + exy + fy^2 + gx + hy + i$$

Après une translation,on peut supposer que $i = 0$. *Comme la courbe est lisse,* g *et* h *ne sont pas tous deux nuls, on peut se ramener par un changement de variables que la tangente en* $(0,0)$ *soit la droite* $y = 0$ *i.e.,*

$$g = 0.$$

En posant

$$x = \frac{U}{W},\ y = \frac{1}{W}$$

on obtient l'équation :

$$U^3 + (a + dW)U^2 + (b + eW)U + c + hW^2 + fW = 0.$$

Si

$$d = 0$$

on a la forme de Weierstrass, sinon en posant

$$W_1 = W + \frac{U}{d}$$

on se ramène au cas ***(I)*** *de l'algorithme*

$$\begin{aligned}\left(\left(a + \frac{h}{d^2} - \frac{e}{d}\right) + dW_1\right)U^2 + \left(\left(b - \frac{f}{d}\right) + \left(e - \frac{2h}{d}\right)W_1\right)U + \left(hW^2 + fW + c\right) &= 0\\ hW_1^2 + \left(dU^2 + \left(e - 2\frac{h}{d}\right)U + f\right)W_1 + \left(a + \frac{h}{d^2} - \frac{e}{d}\right)U^2 + \left(b - \frac{f}{d}\right)U + c &= 0.\end{aligned}$$

2.2 Applications

Dans cette partie, on applique l'algorithme pour trouver les formes de Weierstrass (tempérées) de certaines familles de polynômes à deux indéterminées et pour mettre en evidence l'ordre des points ainsi que le type des fibres singuliers.

Proposition 47 *La famille des courbes* $C_{1,k}$ *définie par*

$$P_1(x,y) = xy^2 + (x^2 + kx + 1)y + (x+1)^2 = 0,\ k \in \mathbb{Z}.$$

a pour modèle de Weierstrass

$$E_{1,k} : Y^2 - kYX + 2Y = X^3 - 3X^2 + 3X - 1 = (X-1)^3.$$

Preuve. On a

$$P_1(x,y) \quad = xy^2 + (x^2 + kx + 1)y + (x+1)^2 \quad = (y+1)x^2 + (y^2 + ky + 2)x + (y+1) = 0$$

c'est le cas **(II)** de l'algorithme avec

$$b = 1, \acute{a} = 1.$$

Posons

$$X = x(y+1)$$

on obtient

$$\begin{aligned} \acute{P}_1(X,y) &= (X+1)y^2 + (kX+2)y + (X^2+2X+1) \\ &= X^2 + (y^2 + ky + 2)X + (y+1)^2 = 0 \end{aligned}$$

et on est dans le cas **(I)** de l'algorithme. Posons à nouveau

$$Y = y(X+1)$$

on trouve

$$Y^2 + (kX+2)Y + (X+1)^3 = 0 \Leftrightarrow Y^2 + kXY + 2Y = (-X-1)^3.$$

En changeant X par -X on trouve

$$Y^2 - kXY + 2Y = (X-1)^3$$

qui est une forme de Weierstrass pour la famille $C_{1,k}$, les changements de variables sont

$$x \quad = \tfrac{X(X-1)}{Y-X+1} \ , \quad y \quad = \tfrac{-Y}{X-1} \ .$$

■

Pour la courbe

$$E_{1,k} : Y^2 - kXY + 2Y = (X-1)^3$$

on a

$$\triangle_{1,k} = (k-2)^3 (k-3)^2 (k+6)$$

ainsi notre courbe sera une courbe elliptique dés que $k \neq -6, 2, 3$. Le point $P = (1,0)$ est un point apparant de notre courbe.

Lemme 48 *Si $k \neq -6, 2, 3$, le point $P = (1,0)$ est un point de 3-torsion.*

Preuve. On a

$$P = (1,0),\ 2P = (1, k-2),\ 3P = \mathcal{O}.$$

■

Proposition 49 *La famille des courbes $C_{2,k}$ définie par*

$$P_2(x,y) = xy^2 + (x^2 + kx + 1)y + x^2 + 1 = 0,\ k \in \mathbb{Z},$$

a pour modèle de Weierstrass $E_{2,k}$:

$$Y^2 - kXY + 2Y = X^3 - X^2 + X - 1.$$

Preuve. On a :

$$P_2(x,y) = xy^2 + (x^2 + kx + 1)y + x^2 + 1 = (y+1)x^2 + (y^2 + ky)x + (y+1) = 0$$

c'est le cas **(II)** de l'algorithme. Le changement de variable

$$X = x(y+1),$$

nous donne

$$\acute{P}_2(X,y) = X^2 + (y^2 + ky)X + (y+1)^2 = (1+X)y^2 + (kX+2)y + (X^2+1) = 0,$$

c'est le cas **(I)** de la méthode. Posons

$$Y = y(1+X)$$

pour obtenir

$$Y^2 + kXY + 2Y = -X^3 - X^2 - X - 1.$$

En changeant X par $-X$, on trouve

$$Y^2 - kXY + 2Y = X^3 - X^2 + X - 1,$$

qui est une forme de Weierstrass pour la famille $C_{2,k}$, les changements de variables sont donnés par

$$x = \frac{X(X-1)}{Y - X + 1},\ y = \frac{-Y}{X-1}.$$

■

Pour la courbe

$$E_2, k :\ Y^2 - kXY + 2Y = X^3 - X^2 + X - 1, k \neq 1,$$

on a

$$\triangle_{2,k} = (k-1)\left(k^2 - 4k + 12\right)\left(k^2 + 4k - 4\right)$$

ainsi notre courbe sera une courbe elliptique pour $k \neq 1$. Le point $P = (1,0)$ est un point apparant de notre courbe.

Proposition 50 *Si $k \neq 0, 1, 2$, le point P est un point d'ordre infini.*

Preuve. Avec **Pari-GP,** on trouve

$$
\begin{array}{l}
P = (1,0),\\
2P = \left(\frac{k^2}{(k-2)^2}, \frac{k^4-4k^3+12k^2-16k+8}{(k-2)^3}\right)\\
3P = \left(\frac{\left(k^3-4k^2+8k-4\right)^2}{16(k-1)^2}, \frac{(2-k)\left(k^8-12k^7+68k^6-224k^5+456k^4-756k^3+480k^2-256k+64\right)}{64(k-1)^3}\right)\\
4P = \left(\frac{\left(k^5-8k^4+32k^3-56k^2+48k-16\right)^2}{k^2(k-2)^2(k^3-4k^2+12k-8)^2}, \frac{a(k)}{b(k)}\right)\\
5P = \left(\frac{(k^8-8k^7+32k^6-56k^5-16k^4+240k^3-384k^2+256k-64)^2}{(k^4-6k^3+20k^2-24k+8)^2(k^4-6k^3+20k^2-24k+8)^2}, \frac{c(k)}{d(k)}\right)\\
6p = \left(\frac{e(k)}{f(k)}, \frac{g(k)}{h(k)}\right)\\
-P = (1, k-2)\\
-2P = \left(\frac{k^2}{(k-2)^2}, \frac{-8(k-1)}{(k-2)^3}\right)\\
-3P = \left(\frac{\left(k^3-4k^2+8k-4\right)^2}{16(k-1)^2}, \frac{k(k-2)(k^3-4k^2+12k-8)(k^4-4k^3+12k^2-16k+8)}{64(k-1)^3}\right)\\
-4P = \left(\frac{\left(k^5-8k^4+32k^3-56k^2+48k-16\right)^2}{k^2(k-2)^2(k^3-4k^2+12k-8)^2}, \frac{\acute{a}(k)}{b(k)}\right)\\
-5P = \left(\frac{(k^8-8k^7+32k^6-56k^5-16k^4+240k^3-384k^2+256k-64)^2}{(k^4-6k^3+20k^2-24k+8)^2(k^4-6k^3+20k^2-24k+8)^2}, \frac{\acute{c}(k)}{d(k)}\right)\\
-6p = \left(\frac{e(k)}{f(k)}, \frac{\acute{g}(k)}{h(k)}\right)
\end{array}
$$

avec

$$
\begin{aligned}
a(k) &= 8(k-1)[k^{12}-16k^{11}+144k^{10}-848k^9+3536k^8-10656k^7\\
&\quad +23264k^6-36480k^5+40256k^4-30208k^3+14592k^2-4096k+512],
\end{aligned}
$$

$$
b(k) = k^3(k-2)^3(k^3-4k^2+12k-8)^3,
$$

$$
\begin{aligned}
c(k) &= k(k-2)(k^3-4k^2+12k-8)[k^{20}-24k^{19}+296k^{18}-2448k^{17}+15072k^{16}-72896k^{15}\\
&\quad +285472k^{14}-920576k^{13}+2464576k^{12}-5492224k^{11}+10185728k^{10}-15717376k^9\\
&\quad +20223488k^8-21803008k^7+19767296k^6-14983168k^5+9261056k^4-4440064k^3\\
&\quad +1523712k^2-327680k+32768],
\end{aligned}
$$

$$
d(k) = (k^4-6k^3+20k^2-24k+8)^3(k^4-6k^3+12k^2-16k+8)^3,
$$

$$
\begin{aligned}
e(k) &= k^2[k^{11}-16k^{10}+128k^9-656k^8+2368k^7-6272k^6+12384k^5-17920k^4\\
&\quad +18176k^3-12032k^2+4608k-768]^2,
\end{aligned}
$$

$$f(k) = (k-2)^2(k-1)^2(k^3-4k^2+8k-4)^2(k^5-6k^4+22k^3-32k^2+24k-8)^2,$$

$$\begin{aligned} g(k) &= (k^4-6k^3+20k^2-24k+8)(k^4-4k^3+12k^2-16k+8)(k^{28}-40k^{27}+792k^{26}-10288k^{25} \\ &\quad +98144k^{24}-730176k^{23}+4395360k^{22}-21936640k^{21}+92340928k^{20}-331974144k^{19} \\ &\quad +1029001216k^{18}-2770427904k^{17}+6517515776k^{16}-13462179840k^{15}+24505896960k^{14} \\ &\quad -39409147904k^{13}+56020877312k^{12}-70259752960k^{11}+77359169536k^{10}-74155622400k^9 \\ &\quad +61168713728k^8-42777444352k^7+24907612160k^6-11809587200k^5+4431282176k^4 \\ &\quad -1264582656k^3+257949696k^2-33554432k+2097152), \end{aligned}$$

$$h(k) = (k-2)^3(k-1)^3(k^3-4k^2+8k-4)^3(k^5-6k^4+22k^3-32k^2+24k-8)^3,$$

$$\begin{aligned} \acute{a}(k) &= (k^4-6k^3+20k^2-24k+8)(k^4-6k^3+12k^2-16k+8)(k^8-12k^7+68k^6-224k^5+ \\ &\quad 456k^4-576k^3+480k^2-256k+64), \end{aligned}$$

$$\begin{aligned} \acute{c}(k) &= (k-1)(k-2)(k^3-4k^2+8k-4)(k^5-6k^4+22k^3-32k^2+24k-8)(k^{12}-16k^{11} \\ &\quad +144k^{10}-848k^9+3536k^8-10656k^7+23264k^6-36480k^5+40256k^4 \\ &\quad -30208k^3+14592k^2-4096k+512), \end{aligned}$$

$$\begin{aligned} \acute{g}(k) &= (k^8-10k^7+48k^6-128k^5+168k^4-48k^3-160k^2+192k-64)(k^8-10k^7+ \\ &\quad 56k^6-200k^5+488k^4-752k^3+672k^2-320k+64)(k^{20}-24k^{19}+296k^{18} \\ &\quad -2448k^{17}+15072k^{16}-72896k^{15}+285472k^{14}-920576k^{13}+2464576k^{12} \\ &\quad -5492224k^{11}+10185728k^{10}-15717376k^9+20223488k^8-21803008k^7+ \\ &\quad 19767296k^6-14983168k^5+9261056k^4-4440064k^3+1523712k^2 \\ &\quad -327680k+32768). \end{aligned}$$

Discussion.

• On a

$$2P = \mathcal{O} \Leftrightarrow P = -P \Leftrightarrow k = 2,$$

puisque $k \neq 2$ le point P ne peut être un point de 2-torsion.

• Si

$$3P = \mathcal{O} \Leftrightarrow 2P = -P \Leftrightarrow \frac{k^2}{(k-2)^2} = 1 \Leftrightarrow k = 1.$$

de même, puisque $k \neq 1$, le point P ne peut être un point de 3-torsion.

• Si

$$4P = \mathcal{O} \Leftrightarrow 3P = -P$$

donc

$$\frac{\left(k^3 - 4k^2 + 8k - 4\right)^2}{16(k-1)^2} = 1$$

i.e.,

$$k(k-2)^2(k^3 - 4k^2 + 12k - 8) = 0$$

le polynôme $k^3 - 4k^2 + 12k - 8$ n'admet pas de racines dans $\mathbb{Z}$, et comme $k \neq 0, 2$ alors, le point P ne peut être un point de 4-torsion.

• Si

$$5P = \mathcal{O} \Leftrightarrow 4P = -P.$$

donc

$$\left(k^5 - 8k^4 + 32k^3 - 56k^2 + 48k - 16\right)^2 = k^2(k-2)^2(k^3 - 4k^2 + 12k - 8)^2$$

i.e.,

$$-4\,(k-1)\,(k^4 - 6k^3 + 20k^2 - 24k + 8)(k^4 - 6k^3 + 12k^2 - 16k + 8) = 0;$$

puisque les deux polynômes

$$k^4 - 6k^3 + 20k^2 - 24k + 8 \quad \text{et} \quad k^4 - 6k^3 + 12k^2 - 16k + 8$$

n'ont pas de racines dans $\mathbb{Z}$, et $k \neq 1$, le point P ne peut être un point de 5-torsion.

• Si

$$6P = \mathcal{O} \Leftrightarrow 4P = -2P.$$

donc

$$\frac{\left(k^5 - 8k^4 + 32k^3 - 56k^2 + 48k - 16\right)^2}{k^2(k-2)^2(k^3 - 4k^2 + 12k - 8)^2} = \frac{k^2}{(k-2)^2}$$

i.e.,

$$(k-2)^2\left(k^5 - 8k^4 + 32k^3 - 56k^2 + 48k - 16\right)^2 = k^4(k-2)^2(k^3 - 4k^2 + 12k - 8)^2$$

i.e.,

$$-8(k-1)(k^3 - 4k^2 + 8k - 4)\left(k^5 - 6k^4 + 22k^3 - 32k^2 + 24k - 8\right) = 0$$

puisque $k \neq 1$, le point P ne peut être un point de 6-torsion.

• Si

$$7P = \mathcal{O} \Leftrightarrow 4P = -3P.$$

i.e.,

$$\frac{\left(k^5-8k^4+32k^3-56k^2+48k-16\right)^2}{k^2(k-2)^2(k^3-4k^2+12k-8)^2}=\frac{\left(k^3-4k^2+8k-4\right)^2}{16(k-1)^2}$$

donc

$$\begin{aligned}&16(k-1)^2\left(k^5-8k^4+32k^3-56k^2+48k-16\right)^2\\ =\;& k^2(k-2)^2(k^3-4k^2+12k-8)^2\left(k^3-4k^2+8k-4\right)^2 \qquad (1)\end{aligned}$$

l'équation (1) n'admet pas de solutions dans $\mathbb{Z}$; i.e., le point P ne peut être un point de 7-torsion.

• Si

$$8P=\mathcal{O}\Leftrightarrow 5P=-3P$$

i.e.,

$$\begin{aligned}&\frac{(k^8-8k^7+32k^6-56k^5-16k^4+240k^3-384k^2+256k-64)^2}{\left(k^4-6k^3+20k^2-24k+8\right)^2(k^4-6k^3+20k^2-24k+8)^2}\\ =\;&\frac{\left(k^3-4k^2+8k-4\right)^2}{16(k-1)^2}\end{aligned}$$

alors

$$\begin{aligned}&-k\,(k-2)^2\,(k^3-4k^2+12k-8)(k^5-8k^4+32k^3-56k^2+48k-16)(k^{11}-16k^{10}\\ &+120k^9-568k^8+1856k^7-4464k^6+8192k^5-11520k^4+11776k^3\quad-7936k^2+\\ &3072k-512)\;=0 \qquad (2)\end{aligned}$$

l'équation (2) n'admet pas de solutions dans $\mathbb{Z}$, par suite le point P n'est pas un point de 8-torsion.

• Si

$$9P=\mathcal{O}\Leftrightarrow 5P=-4P$$

i.e.,

$$\begin{aligned}&\frac{(k^8-8k^7+32k^6-56k^5-16k^4+240k^3-384k^2+256k-64)^2}{\left(k^4-6k^3+20k^2-24k+8\right)^2(k^4-6k^3+20k^2-24k+8)^2}\\ =\;&\frac{\left(k^5-8k^4+32k^3-56k^2+48k-16\right)^2}{k^2(k-2)^2(k^3-4k^2+12k-8)^2}\end{aligned}$$

alors

$$\begin{aligned}&4(k-1)(k^{12}-16k^{11}+132k^{10}-696k^9+2544k^8-6672k^7+12704k^6-17792k^5\\ &+18624k^4-14720k^3+8448k^2-3072k+512)(3k^{12}-48k^{11}+388k^{10}-2008k^9\\ &+7280k^8-19216k^7+37472k^6-53632k^5+54976k^4-38784k^3+17664k^2\\ &-4608k+512)=0 \qquad (3)\end{aligned}$$

l'équation (3) n'admet pas de solutions dans $\mathbb{Z}$, donc le point P ne peut être un point de 9-torsion.

• Si

$$10P = \mathcal{O} \Leftrightarrow 6P = -4P$$

i.e.,

$$\frac{e(k)}{f(k)} = \frac{\left(k^5 - 8k^4 + 32k^3 - 56k^2 + 48k - 16\right)^2}{k^2(k-2)^2(k^3 - 4k^2 + 12k - 8)^2}$$

on trouve

$$k^4(k^3 - 4k^2 + 12k - 8)^2(k^{11} - 16k^{10} + 128k^9 - 656k^8 + 2368k^7 - 6272k^6 + 12384k^5 \\ -17920k^4 + 18176k^3 - 12032k^2 + 4608k - 768)^2 - (k-1)^2(k^3 - 4k^2 + 8k - 4)^2(k^5 - 6k^4 \\ +22k^3 - 32k^2 + 24k - 8)^2(k^5 - 8k^4 + 32k^3 - 56k^2 + 48k - 16)^2 = 0 \qquad (4)$$

l'équation (4) n'admet pas de solutions dans $\mathbb{Z}$, c'est-à-dire le point P ne peut être un point de 10-torsion.

• Si

$$12P = \mathcal{O} \Leftrightarrow 6P = -6P$$

donc

$$g(k) = \acute{g}(k)$$

de même cette équation n'admet pas de solutions dans $\mathbb{Z}$, alors P ne peut être un point de 12-torsion. Ce qui implique que $P = (1, 0)$ est un point d'ordre infini. ■

Remarque 51 *Si $k = 2$, alors*

$$P = -P \Leftrightarrow 2P = \mathcal{O}$$

donc le point P est un point de 2-torsion.

Si $k = 0$, alors

$$2P = -2P \Leftrightarrow 4P = \mathcal{O}$$

donc le point P est un point de 4-torsion.

Definition 52 *Soit*

$$P(x, y) = \sum_{(i,j)\in\mathbb{Z}^2} a_{ij} x^i y^j$$

un polynôme de Laurant, ($P \in \mathbb{C}\left[x^{\pm 1}, y^{\pm 1}\right]$). On appelle polygone de Newton $\triangle_P$, associé au polynôme P, l'enveloppe convexe dans $\mathbb{R}^2$ des points (i, j) satisfaisant $a_{ij} \neq 0$.

A une face τ du polygone de Newton, on associe un polynôme P_τ d'une seule variable t dont le degré est égale au nombre de points du réseau des entiers situés sur la face moins 1. On définit alors P_τ par

$$P_\tau(t) = \sum_{k=0}^{\infty} a_{\tau(k)} t^k, \ \tau \in \triangle$$

où la paramétrisation de la face est définie dans le sens indirect sur $\triangle$ de façon à noter $\tau(0), \tau(1), ...,$ les points consécutifs du réseau d'entiers situés sur la face τ de $\triangle_P$.

Definition 53 *Le polynôme P est dit **tempéré** si les polynômes associés aux faces de son polygone de Newton n'ont pour racines que des racines de l'unité.*

Proposition 54 *Soit $P \in \mathbb{Z}[X,Y]$ de bidegré $(2,2)$ définissant une courbe elliptique. On suppose P tempéré et vérifiant la condition **(I)** de l'algorithme. Alors, la forme de Weierstrass donnée par l'algorithme est tempérée.*

Preuve. Soit P tempéré, il s'écrit donc

$$P(x,y) = (x+\varepsilon)y^2 + (\acute{b}x + \acute{c})y + \acute{\varepsilon}x^2 + b^{"}x + \varepsilon^{"}$$

avec

$$\begin{cases} \varepsilon = \pm 1,\ \acute{\varepsilon} = \pm 1,\ \varepsilon^{"} = \pm 1 \\ \acute{c} = 0 \text{ ou } \acute{c} = \pm 2, \text{ si } \varepsilon\varepsilon^{"} = 1 \\ b^{"} = 0 \text{ ou } b^{"} = \pm 2, \pm 1 \text{ si } \acute{\varepsilon}\varepsilon^{"} = 1 \end{cases}$$

de sorte que les polynômes des faces

$$t+\varepsilon,\ \varepsilon t^2 + \acute{c}t + \varepsilon^{"},\ \varepsilon^{"}t^2 + b^{"}t + \acute{\varepsilon},\ \acute{\varepsilon}t + 1$$

ne possèdent que des racines de l'unité.

On a donc

$$\begin{aligned} P(x,y) &= (x+\varepsilon)y^2 + (\acute{b}x + \acute{c})y + \acute{\varepsilon}x^2 + b^{"}x + \varepsilon^{"} \\ &= \acute{\varepsilon}x^2 + \left(y^2 + \acute{b}y + b^{"}\right)x + \varepsilon y^2 + \acute{c}y + \varepsilon^{"}. \end{aligned}$$

Posons alors

$$Y = (x+\varepsilon)y$$

et l'on obtient, au besoin en posant $x = -X$, la forme de Weierstrass à partir de l'équation

$$Y^2 + \left(\acute{b}x + \acute{c}\right)Y + \left(\acute{\varepsilon}x^2 + b^{"}x + \varepsilon^{"}\right)(x+\varepsilon) = 0.$$

On vérifie aisément que ce dernier polynôme est tempéré. ■

Nous donnons maintenant des exemples des polynômes satisfaisant la proposition.

Exemple 55 ***1/*** *La famille des courbes elliptique $\{P(x,y) = 0,\}$ définie par*

$$\begin{aligned} P(x,y) &= y^2x + (kx+1)y + x^2 \\ &= x^2 + (y^2 + ky)x + y,\ k \neq 0,\ k \in \mathbb{Z} \end{aligned}$$

a la forme de Weierstrass tempérée :

$$Y^2 - kXY + Y = X^3$$

avec les changements de variables

$$\begin{cases} X & = -x \\ Y & = xy \end{cases}$$

2/ La forme de Weierstrass (par l'algorithme)

$$E_{k,3},: Y^2 - kXY + Y = X^3 - 2X^2 + X,\ k \neq 1,\ k \in \mathbb{Z}$$

est une forme de Weierstrass tempérée pour la famille des courbes elliptiques

$$P(x,y) = xy^2 + (x^2 + kx + 1)y + x^2 + x = 0,$$

les changements de variables

$$x = \frac{X(X-1)}{Y - X + 1}, y = \frac{-Y}{X-1}.$$

La courbe elliptique

$$E_{k,3}:\ Y^2 - kXY + Y = X^3 - 2X^2 + X, \quad k \neq 1,\ k \in \mathbb{Z}$$

a pour discriminant

$$\triangle_{3,k} = (k-1)^2 (k^3 - k^2 - 18k + 43).$$

Le point $P = (1,0)$ est un point apparant de la courbe $E_{k,3}$.

Proposition 56 *Supposons que $k \neq 1, 2, 3$, alors le point $P = (1,0)$ est un point d'ordre infini.*

Preuve. Avec **Pari**, on trouve

$$\begin{array}{ll} P = (1,0), & -P = (1, k-1) \\ 2P = (0,-1), & -2P = (0,0) \\ 3P = (2-k, -(k-1)(k-2)), & -3P = (-k+2, -k+1) \\ 4P = (3-k, 3-k), & -4P = \left(-k+3, -k^2+4k-4\right) \\ 5P = \left(\frac{1}{(k-2)^2}, \frac{k-1}{(k-2)^3}\right), & -5P = \left(\frac{1}{(k-2)^2}, \frac{-(k-1)(k-3)^2}{(k-2)^3}\right) \\ 6P = \left(\frac{k^2-5k+7}{(k-3)^2}, \frac{(k-2)^2(k^2-5k+7)}{(k-3)^3}\right), & -6P = \left(\frac{k^2-5k+7}{(k-3)^2}, \frac{-1}{(k-3)^3}\right) \end{array}$$

Discussion.

• On a

$$2P = \mathcal{O} \Leftrightarrow P = -P \Leftrightarrow k = 1$$

puisque $k \neq 1$, le point P ne peut être un point de 2-torsion.

• Si

$$3P = \mathcal{O} \Leftrightarrow 2P = -P \Leftrightarrow 0 = 1$$

impossible, donc le point P ne peut être un point de 3-torsion.

• Si

$$4P = \mathcal{O} \Leftrightarrow 2P = -2P \Leftrightarrow -1 = 0$$

impossible, le point P ne peut être un point de 4-torsion.

• Si

$$5P = \mathcal{O} \Leftrightarrow 3P = -2P \Leftrightarrow k = 2$$

puisque $k \neq 2$, le point P ne peut être un point de 5-torsion.

• Si

$$6P = \mathcal{O} \Leftrightarrow 4P = -2P \Leftrightarrow k = 3$$

puisque $k \neq 3$, le point P ne peut être un point de 6-torsion.

• Si

$$7P = \mathcal{O} \Leftrightarrow 5P = -2P \Leftrightarrow \frac{1}{(k-2)^2} = 0 \Leftrightarrow 1 = 0$$

impossible, alors le point P ne peut être un point de 7-torsion.

• On a

$$8P = \mathcal{O} \Leftrightarrow 5P = -3P \Leftrightarrow \frac{1}{(k-2)^2} = -k + 2 \Leftrightarrow k^3 - 6k^2 + 12k + 9 = 0$$

l'équation

$$k^3 - 6k^2 + 12k + 9 = 0$$

n'admet pas de racines sur $\mathbb{Z}$. Donc le point P ne peut être un point de 8-torsion.

• Si

$$9P = \mathcal{O} \Leftrightarrow 5P = -4P$$

i.e.,

$$\frac{1}{(k-2)^2} = -k + 3$$

donc

$$k^3 - 7k^2 + 16k - 11 = 0$$

cette équation n'admet pas de solutions dans $\mathbb{Z}$, on déduit que le point P ne peut être un point de 9-torsion.

• Si

$$10P = \mathcal{O} \Leftrightarrow 5P = -5P$$

i.e.,

$$\frac{k-1}{(k-2)^3} = \frac{-(k-1)(k-3)^2}{(k-2)^3}$$

donc

$$(k-1)(k^2 - 6k + 10) = 0$$

l'équation $k^2 - 6k + 10$ n'admet pas de solutions dans $\mathbb{Z}$, et comme $k \neq 1$, le point P ne peut être un point de 10-torsion.

• On a

$$12P = \mathcal{O} \Leftrightarrow 6P = -6P$$

i.e.,

$$\frac{(k-2)^2(k^2-5k+7)}{(k-3)^3} = \frac{-1}{(k-3)^3}$$

donc

$$(-2+k)^2(k^2-5k+7)+1=0,$$

les racines de cette équation ne sont pas dans $\mathbb{Z}$, on déduit que le point P ne peut être un point de 12-torsion. ■

Remarque 57 *Si $k=2$, alors*

$$3P = -2P \Leftrightarrow 5P = \mathcal{O}$$

donc le point P est un point de 5-torsion.

Si $k=3$, alors

$$4P = -2P \Leftrightarrow 6P = \mathcal{O}$$

donc le point P est un point de 6-torsion.

La courbe elliptique

$$E_{k,4}:\ Y^2 = X^3 + (k^2+4)X^2 + 8k(k-1)X + 16(k-1)^2,\ k \neq 1,\ k \in \mathbb{Z}$$

a pour discriminant

$$\Delta_{k,4} = (k-1)\left(k^7 - 2k^6 - 24k^5 + 80k^4 - 52k^3 + 80k^2 - 252k + 44\right)$$

et elle est un modèle de la courbe de genre 1

$$x^2y^2 + (2x^2 + kx + 1) + x^2 + x = 0,$$

avec les changements de variables

$$X = 4(k-1)x,\ Y = 2x^2y + (2x^2 + kx + 1).$$

Le point

$$P = (0, 4(k-1))$$

est un point apparant de notre courbe.

Proposition 58 *Supposons que $k \neq 1, 2, 3$, alors le point $P = (0, 4(k-1))$ est un point d'ordre infini.*

Preuve. Avec **Pari-GP,** on trouve

$$\begin{array}{ll}
P=(0,4(k-1)), & -P=(0,-4(k-1)) \\
2P=(-4,4), & -2P=(-4,-4) \\
3P=(-4(k-1),4(k-1)(k-3)), & -3P=(-4(k-1),-4(k-1)(k-3)) \\
4P=(-4(k-2),-4(k^2-5k+7)), & -4P=(-4(k-2),4(k^2-5k+7)) \\
5P=\left(\frac{-4(k-1)(k-3)}{(k-2)^2},\frac{-4(k-1)(k^2-6k+10)}{(k-2)^3}\right), & -5P=\left(\frac{-4(k-1)(k-3)}{(k-2)^2},\frac{4(k-1)(k^2-6k+10)}{(k-2)^3}\right) \\
6P=\left(\frac{k(k-2)}{(k-3)^2},\frac{-4(k^4-9k^3+31k^2-48k+29)}{(k-3)^3}\right), & -6P=\left(\frac{k(k-2)}{(k-3)^2},\frac{4(k^4-9k^3+31k^2-48k+29)}{(k-3)^3}\right)
\end{array}$$

Discussion.

• Si

$$2P=\mathcal{O}\Leftrightarrow P=-P\Leftrightarrow 4=-4$$

impossible, alors le point P ne peut être un point de 2-torsion.

• Si

$$3P=\mathcal{O}\Leftrightarrow 2P=-P\Leftrightarrow 4=0$$

impossible, par suite le point P ne peut être un point de 3-torsion.

• On a

$$4P=\mathcal{O}\Leftrightarrow 2P=-2P\Leftrightarrow 4=-4$$

impossible, alors le point P ne peut être un point de 4-torsion.

• Si

$$5P=\mathcal{O}\Leftrightarrow 4P=-P\Leftrightarrow k=2$$

puisque $k\neq 2$ le point P ne peut être un point de 5-torsion.

• Si

$$6P=\mathcal{O}\Leftrightarrow 5P=-P$$

donc

$$\frac{-4(k-1)(k-3)}{(k-2)^2}=0$$

ainsi

$$-4(k-1)(k-3)=0\Leftrightarrow k=1\vee k=3$$

puisque $k\neq 1,3$; le point P ne peut être un point d'ordre 6.

• Si

$$7P=\mathcal{O}\Leftrightarrow 5P=-2P$$

donc

$$\frac{-4(k-1)(k-3)}{(k-2)^2}=-4$$

on trouve $-1=0$, impossible. Alors : le point P ne peut être un point de $7-$torsion.

• Si

$$8P=\mathcal{O}\Leftrightarrow 5P=-3P$$

donc

$$\frac{-4(k-1)(k-3)}{(k-2)^2} = -4(k-1) \Leftrightarrow -1 = 0$$

impossible, alors le point P ne peut être un point de 8-torsion.

• Si

$$9P = \mathcal{O} \Leftrightarrow 6P = -3P$$

donc

$$\frac{k(k-2)}{(k-3)^2} = -4(k-1)$$

on trouve

$$4k^3 - 27k^2 + 58k - 36 = 0$$

cette équation n'admet pas de racines dans $\mathbb{Z}$. Par suite, le point P ne peut être un point de 9-torsion.

• Si

$$10P = \mathcal{O} \Leftrightarrow 5P = -5P \Leftrightarrow -4 = 4$$

impossible, donc le point P ne peut être un point de 10-torsion.

• Si

$$12P = \mathcal{O} \Leftrightarrow 6P = -6P \Leftrightarrow -4 = 4$$

impossible, donc le point P ne peut être un point de 12-torsion.

Donc le point P est un point d'ordre infini. ■

Remarque 59 *Si $k = 2$, alors*

$$2P = -3P \Leftrightarrow 5P = \mathcal{O}$$

donc le point $P = (0, 4)$ est un point de 5-torsion.

Si $k = 3$, alors

$$4P = -2P \Leftrightarrow 6P = \mathcal{O}$$

donc le point $P = (0, 8)$ est un point de 6-torsion.

Pour terminer ce chapitre, on s'intéresse aux types des fibres singuliers d'une surface elliptique donnée par une équation de Weierstrass

$$E(t) : Y^2 = X^3 + a(t)X + b(t),\ a(t),\ b(t) \in K(t)$$

avec K un corps algébriquement clos. Pour simplifier l'exposé on prend $K = \mathbb{C}$. Soit $t^* \in P_1(\mathbb{C})$ tel que

$$\triangle(t^*) = -16(4a^3(t^*) + 27b^2(t^*)) \neq 0$$

alors $E(t^*)$ sera une courbe lisse de genre 1(**un fibre régulier**). Pour tous $t^* \in P_1(\mathbb{C})$ tel que

$$\triangle(t^*) = -16(4a^3(t^*) + 27b^2(t^*)) = 0$$

$E(t^*)$ est appelé fibre singulier. Suivant la multiplicité du zéro t^* de $\triangle(t)$, $a(t)$, et $b(t)$ et par un algorithme de Tate [19] on détermine le type du fibre singulier $E(t^*)$. Nous utiliserons dans ce qui suit les symboles de Kodaira [13] des fibres (généralement appelés modèles de Néron [16]). Le type du fibre est donné par la table suivante obtenue par l'algorithme de Tate.

	$Ord_{t^*}(a(t))$	$Ord_{t^*}(b(t)$	$Ord_{t^*}(\triangle(t))$	*type du fibre*
(0)	arbitraire	arbitraire	0	régulier
(1)	0	0	b	$I_b(b \geq 1)$
(2)	≥ 2	≥ 3	$b+6$	$I_b^*(b \geq 0)$
(3)	≥ 1	1	2	II
(4)	≥ 2	2	4	$I\vee$
(5)	≥ 3	4	8	$I\vee^*$
(6)	≥ 4	5	10	II^*
(7)	1	≥ 2	3	III
(8)	3	≥ 5	9	III^*

Par exemple :

I_0 : est une courbe non singulière de genre 1.

I_1 : est une courbe rationnelle avec un noeud.

I_n : désigne n courbes rationnelles arrangées de façon à former un polygône à n côtés.

II : est une courbe rationnelle avec un point de rebroussement.

III : désigne deux courbes non singulières rationnelles tangentes en un point.

.

.

.

Considérons la surface elliptique $S(t)$ donnée par l'équation de Weierstrass($E_{1,k}$ partie 2.2)

$$\begin{aligned} S(t) &: \quad Y^2 - tXY + 2Y = (X-1)^3,\ t \in \mathbb{C}. \\ \triangle(t) &= (t-2)^3(t-3)^2(t+6). \end{aligned}$$

Proposition 60 *Les types des fibres singuliers de la surface elliptique $S(t)$, obtenus pour $t = -6, 2, 3$ sont donnés par*

$$\begin{array}{ccc} I_1 & I_3 & I_2. \\ \downarrow & \downarrow & \downarrow \\ {\scriptstyle -6} & {\scriptstyle 2} & {\scriptstyle 3} \end{array}$$

Preuve. La surface $S(t)$ se ramène à la surface elliptique

$$W(t) : \widetilde{Y}^2 = \widetilde{X}^3 - \frac{t}{48}\left(t^3 - 24t + 48\right)\widetilde{X} + \frac{\left(t^2-12\right)}{864}\left(t^4 - 24t^2 + 72t - 72\right),$$

avec le changement de variables

$$\widetilde{X} = X + \frac{t^2}{12} - 1,\ \widetilde{Y} = Y - \frac{t}{2}X + 1,$$

ainsi

$$\triangle(t) = \tilde{\triangle}(t).$$

Donc, le résultat découle de la table de Tate. ■

Chapitre 3

Sur les courbes de Huff et d'Edwards

Les courbes elliptiques peuvent se présenter sous différentes formes et leurs arithmétiques dépend du modèle choisi. Ici on s'intéresse aux courbes de Huff. A la fin de ce chapitre on construirera des suites arithmétiques sur un autre modèle de courbes elliptiques, le modèle d'Edwards. Pour plus de résultats et de détails voir [3-4], [6-8], [11], [15], [21].

3.1 Courbes de Huff $H_{(a,b)}^{(c,d)} : ax(y^2 - c) = by(x^2 - d)$ sur un corps K de caractéristique différente de deux

Les courbes de Huff sur un corps K de caractéristique différente de deux se présentent sous-différentes formes.

• Courbes de Huff (par lui même) sont données par

$$ax(y^2 - 1) = by(x^2 - 1)$$

avec

$$a^2 - b^2 \neq 0.$$

• La première forme généralisée de courbes de Huff (par Joy et al) est donnée par

$$ax(y^2 - d) = by(x^2 - d)$$

avec

$$abd(a^2 - b^2) \neq 0.$$

• La deuxième forme généralisée de courbes de Huff (parWu et al) est donnée par

$$x(ay^2 - 1) = y(bx^2 - 1)$$

avec

$$ab(a-b) \neq 0.$$

• Ici on s'intéresse à la troisième forme généralisée de courbes de Huff ([3]) donnée par

$$ax(y^2-c) = by(x^2-d)$$

avec

$$abcd(a^2c - b^2d) \neq 0.$$

Proposition 61 *Le polynôme*

$$H(x,y) = ax(y^2-c) - by(x^2-d) \in K[x,y]$$

est irréductible sur $\overline{K}[x,y]$ *si*

$$abcd\left(a^2c - b^2d\right) \neq 0.$$

Preuve. Supposons que

$$H(x,y) = ax(y^2-c) - by(x^2-d)$$

est réductible, donc H peut s'écrire sous la forme

$$H(x,y) = (f(x)y + g(x))(f_1(x)y + g_1(x))$$

avec $f(x)$, $g(x)$, $f_1(x)$ et $g_1(x) \in \overline{K}[x]$. Par identification, on trouve

$$f(x)f_1(x) = ax\ , \tag{3.1}$$

$$f(x)g_1(x) + g(x)f_1(x) = -b(x^2-d), \tag{3.2}$$

$$g(x)g_1(x) = -cax. \tag{3.3}$$

Par l'équation (3.1) on peut supposer que $\deg(f_1(x)) = 0$, i.e., $f_1 \in K$. Si non on change entre $f_1$et f. Par l'équation (3.2) et (3.3), on trouve que $\deg(g_1(x)) \neq 0$, donc par (3.3) on déduit que $\deg(g(x)) = 0, \deg(g_1(x)) = 1$. Alors

$$f(x) = \frac{ax}{f_1}$$

et

$$g_1(x) = \frac{-acx}{g}.$$

Par suite

$$f(x)g_1(x) = \frac{-a^2cx^2}{f_1 g}$$

d'autre part, par l'équation (3.2) on a

$$\begin{aligned} f(x)g_1(x) + gf_1 &= \tfrac{-a^2cx^2}{f_1 g} + gf_1 \\ &= -bx^2 + bd. \end{aligned}$$

Par identification, on trouve

$$gf_1 = bd,$$

i.e. ;

$$a^2c - b^2d = 0.$$

Contradiction. ■

Proposition 62 *La courbe*

$$H^{(c,d)}_{(a,b)} : ax(y^2 - c) = by(x^2 - d),\ abcd(a^2c - b^2d) \neq 0$$

est une courbe lisse.

Preuve. Posons

$$H(x, y) = ax(y^2 - c) - by(x^2 - d)$$

et supposons qu'il éxiste un point $P = (x, y)$ vérifie

$$H(x, y) = 0,\ \frac{\partial H}{\partial x}(x, y) = 0,\ \frac{\partial H}{\partial y}(x, y) = 0$$

donc

$$ax(y^2 - c) - by(x^2 - d) = 0, \tag{3.4}$$

$$ay^2 - 2bxy - ac = 0, \tag{3.5}$$

$$2axy - b(x^2 - d) = 0. \tag{3.6}$$

Multiplions l'équation (3.6) par y, on trouve

$$2axy^2 - by(x^2 - d) = 0$$

par l'équation (3.4), on trouve

$$2axy^2 - ax(y^2 - c) = 0$$

i.e.,

$$y^2 = -c$$

par l'équation (3.5), on trouve

$$ac + bxy = 0.$$

De même, par symétrie on trouve

$$bd + axy = 0.$$

Ainsi par élémination de xy on obtient

$$a^2c - b^2d = 0.$$

Contradiction. ■

Proposition 63 *La courbe*

$$\overline{H}_{(a,b)}^{(c,d)} : aX\left(Y^2 - cZ^2\right) = bY\left(X^2 - dZ^2\right),\ abcd(a^2c - b^2d) \neq 0$$

admet trois points à l'infini à savoir

$$P_1 = [0,1,0]\,,\ P_2 = [1,0,0]\,,\ P_3 = \left[1, \frac{b}{a}, 0\right],$$

de plus ces points sont non singuliers.

Preuve. On sait que les points à l'infini sont les points de la forme $[X, Y, 0]$. Donc, pour $Z = 0$ on trouve :

$$aXY^2 = bYX^2,$$

i.e.,

$$XY\,(aY - bX) = 0.$$

Ainsi, les points à l'infini sont

$$\begin{aligned} P_1 &= [0,1,0]\,, \\ P_2 &= [1,0,0]\,, \\ P_3 &= \left[1, \frac{b}{a}, 0\right]. \end{aligned}$$

On a

$$\frac{\partial \overline{H}}{\partial X}(P_1) = a \neq 0,$$

$$\frac{\partial \overline{H}}{\partial Y}(P_2) = -b \neq 0,$$

$$\frac{\partial \overline{H}}{\partial X}(P_3) = \frac{-b^2}{a} \neq 0,\ \frac{\partial \overline{H}}{\partial Y}(P_3) = b \neq 0,$$

d'où le résultat. ■

Proposition 64 *La courbe de Huff*

$$H_{(a,b)}^{(c,d)} : ax(y^2 - c) = by(x^2 - d),\ abcd\left(a^2c - b^2d\right) \neq 0$$

est birationnellement équivalente à la courbe de Weierstrass

$$E_{(a,b)}^{(c,d)} : Y^2 = X^3 + (a^4c - a^2b^2d)X^2 + a^4b^2cdX,$$

avec les changements de variables sont données par

$$\begin{aligned} (x,y) &= \left(\frac{aX\left(X - b^2d\right)}{bY}, \frac{Y}{a^4(X - b^2d)}\right), \\ (X,Y) &= \left(a^3bxy, a^4b\left(a^3xy - bd\right)y\right). \end{aligned}$$

Preuve. Posons

$$H(x,y) = ax(y^2-c) - by(x^2-d)$$

alors

$$\begin{aligned} H(x,y) &= axy^2 - b(x^2-d)y - acx \\ &= -byx^2 + a(y^2-c)x + bdy, \end{aligned}$$

on a $ab \neq 0$, donc on est dans le cas (**II**) de l'algorithme de Harrache et Touafek (chapitre 2). Posons

$$X = -abxy$$

on obtient

$$\begin{aligned} \acute{H}(X,y) &= \left(a^2X - a^2b^2d\right)y^2 - a^2cX + X^2 \\ &= X^2 + \left(a^2y - a^2c\right)X - a^2b^2dy \end{aligned}$$

et on est dans le cas (**I**) de l'algorithme de Harrache et Touafek. Posons à nouveau

$$Y = a^2y\left(X - b^2d\right)$$

on trouve

$$Y^2 = -a^2X^3 + a^2(a^2c + b^2d)X^2 - a^4b^2cdX.$$

Multiplions cette équation par a^4 et en changeant X par $-X$, on obtient

$$Y^2 = X^3 + a^2\left(a^2c + b^2d\right)X^2 - a^4b^2cdX.$$

Les changements de variables sont données par

$$\begin{aligned} (x,y) &= \left(\frac{aX\left(X - b^2d\right)}{bY}, \frac{Y}{a^4(X - b^2d)}\right) \\ (X,Y) &= \left(a^3bxy, a^4b\left(a^3xy - bd\right)y\right). \end{aligned}$$

■

Proposition 65 ***(Addition de deux points différents)*** *Soient $P_1 = (x_1,y_1)$, $P_2 = (x_2,y_2)$ deux points différents, $(x_1 - x_2)(y_1 - y_2) \neq 0$, de la courbe $H^{(c,d)}_{(a,b)}$ avec*

$$d \pm x_1x_2 \neq 0,\ c \pm y_1y_2 \neq 0.$$

Les coordonnées du point $P_3 = (x_3,y_3)$ la somme des deux points P_1 et P_2 sont données par :

$$\begin{aligned} x_3 &= \frac{d(x_1 + x_2)(c + y_1y_2)}{(d + x_1x_2)(c - y_1y_2)} \\ y_3 &= \frac{c(y_1 + y_2)(d + x_1x_2)}{(c + y_1y_2)(d - x_1x_2)}. \end{aligned}$$

Preuve. Posons

$$H(x,y) = ax(y^2 - c) - by(x^2 - d)$$

et soit $y = \alpha x + \beta$ l'équation de la droite (P_1P_2) passant par P_1 et P_2 avec

$$\alpha = \frac{y_2 - y_1}{x_2 - x_1},\ \beta = y_1 - \alpha x_1.$$

Cette droite recoupe la courbe $H^{(c,d)}_{(a,b)}$ en un troisième point $R = (x_R, y_R)$. En remplaçant par l'équation de la droite dans H, on obtient

$$H(x, \alpha x + \beta) = \left(a\alpha^2 - \alpha b\right) x^3 + (2a\alpha\beta - b\beta)\, x^2 + \left[a\left(\beta^2 - c\right) + \alpha\beta d\right] x + bd\beta = 0$$

cette équation admet trois racines x_1, x_2 et x_R, d'après les relations (racines ,coefficients) chez les polynômes, on trouve

$$x_1 + x_2 + x_R = -\frac{\beta(2a\alpha - b)}{\alpha(a\alpha - b)},$$

alors

$$-x_R = x_1 + x_2 + \frac{(y_1 - \alpha x_1)\left(2a\frac{y_2-y_1}{x_2-x_1} - b\right)}{\frac{y_2-y_1}{x_2-x_1}\left(a\frac{y_2-y_1}{x_2-x_1} - b\right)}$$

$$-x_R = x_1 + x_2 + \frac{[y_1(x_2 - x_1) - x_1(y_2 - y_1)]\,[2a(y_2 - y_1) - b(x_2 - x_1)]}{(y_2 - y_1)\,[a(y_2 - y_1) - b(x_2 - x_1)]}$$

donc

$$-x_R = x_1 + x_2 + \frac{(y_1x_2 - x_1y_2)\,[2a(y_2 - y_1) - b(x_2 - x_1)]}{(y_2 - y_1)\,[a(y_2 - y_1) - b(x_2 - x_1)]}.$$

Posons

$$A = y_1y_2(x_1 + x_2)\,[a(y_2 - y_1) - b(x_2 - x_1)]$$

on obtient

$$\begin{aligned}
A &= ay_1y_2(x_1 + x_2)(y_2 - y_1) - by_1y_2(x_1 + x_2)(x_2 - x_1) \\
&= a(x_1y_1y_2 + x_2y_1y_2)(y_2 - y_1) - by_1y_2\left(x_2^2 - x_1^2\right) \\
&= a\left(x_1y_1y_2^2 - x_2y_2y_1^2\right) + a\left(x_2y_1y_2^2 - x_1y_2y_1^2\right) - by_1y_2\left(x_2^2 - x_1^2\right) \\
&= a\left(x_1y_1y_2^2 - x_2y_2y_1^2\right) + a\left(x_2y_1y_2^2 - x_1y_2y_1^2\right) - y_1\left[by_2\left(\left(x_2^2 - d\right) + d\right)\right] + y_2\left[by_1\left(\left(x_1^2 - d\right) + d\right)\right].
\end{aligned}$$

Puisque $P_1, P_2 \in H^{(c,d)}_{(a,b)}$,donc

$$\begin{aligned}
ax_1(y_1^2 - c) &= by_1(x_1^2 - d) \\
ax_2(y_2^2 - c) &= by_2(x_2^2 - d)
\end{aligned}$$

alors

$$\begin{aligned} A &= a\left(x_1y_1y_2^2 - x_2y_2y_1^2\right) + a\left(x_2y_1y_2^2 - x_1y_2y_1^2\right) - y_1\left[ax_2(y_2^2-c) + bdy_2\right] + y_2\left[ax_1(y_1^2-c) + bdy_1\right] \\ &= ay_1y_2\left(x_1y_2 - x_2y_1\right) + ac\left(y_1x_2 - x_1y_2\right) \\ &= ay_1y_2\left(x_1y_2 - x_2y_1\right) - ac\left(x_1y_2 - x_2y_1\right) \\ &= a\left(x_1y_2 - x_2y_1\right)\left(y_1y_2 - c\right) \end{aligned}$$

donc

$$a\left(y_2 - y_1\right) - b\left(x_2 - x_1\right) = \frac{a\left(x_1y_2 - x_2y_1\right)\left(y_1y_2 - c\right)}{y_1y_2\left(x_1 + x_2\right)}$$

on obtient

$$\begin{aligned} -x_R &= x_1 + x_2 + \frac{\left(y_1x_2 - x_1y_2\right)\left[2a\left(y_2 - y_1\right) - b\left(x_2 - x_1\right)\right]}{\left(y_2 - y_1\right)\frac{a(x_1y_2 - x_2y_1)(y_1y_2 - c)}{y_1y_2(x_1 + x_2)}} \\ &= x_1 + x_2 - \frac{y_1y_2\left(x_1 + x_2\right)\left[2a\left(y_2 - y_1\right) - b\left(x_2 - x_1\right)\right]}{a\left(y_2 - y_1\right)\left(y_1y_2 - c\right)} \\ &= x_1 + x_2 - \frac{\left(a\left(y_2 - y_1\right)\left(x_1 + x_2\right)y_1y_2\right) + \left[a\left(y_2 - y_1\right) - b\left(x_2 - x_1\right)\right]\left(x_1 + x_2\right)y_1y_2}{a\left(y_2 - y_1\right)\left(y_1y_2 - c\right)} \\ &= x_1 + x_2 - \frac{\left(x_1 + x_2\right)y_1y_2}{\left(y_1y_2 - c\right)} - \frac{x_1y_2 - x_2y_1}{\left(y_2 - y_1\right)} \\ &= x_1 + x_2 - \frac{\left(x_1 + x_2\right)y_1y_2}{\left(y_1y_2 - c\right)} + \frac{x_2y_1 - x_1y_2}{\left(y_2 - y_1\right)} \\ &= \frac{\left(x_1 + x_2\right)\left(y_2 - y_1\right) + \left(x_2y_1 - x_1y_2\right)}{\left(y_2 - y_1\right)} - \frac{\left(x_1 + x_2\right)y_1y_2}{\left(y_1y_2 - c\right)} \\ &= \frac{x_2y_2 - x_1y_1}{y_2 - y_1} - \frac{\left(x_1 + x_2\right)y_1y_2}{\left(y_1y_2 - c\right)}. \end{aligned}$$

Posons

$$B = b\left(x_2y_2 - x_1y_1\right)\left(x_1x_2 + d\right)$$

on obtient

$$\begin{aligned} B &= b\left(x_2^2y_2x_1 - x_1^2y_1x_2\right) + bd\left(x_2y_2 - x_1y_1\right) \\ &= b\left[y_2\left(\left(x_2^2 - d\right) + d\right)x_1 - y_1\left(\left(x_1^2 - d\right) + d\right)x_2\right] + bd\left(x_2y_2 - x_1y_1\right) \\ &= x_1by_2\left(x_2^2 - d\right) + bdx_1y_2 - by_1\left(x_1^2 - d\right)x_2 - bdx_2y_1 + bd\left(x_2y_2 - x_1y_1\right) \\ &= ax_1x_2\left(y_2^2 - c\right) - ax_1x_2\left(y_1^2 - c\right) + bd(x_1y_2 - x_2y_1 + x_2y_2 - x_1y_1) \\ &= ax_1x_2\left(y_2^2 - y_1^2\right) + bd\left(y_2 - y_1\right)\left(x_1 + x_2\right) \\ &= \left(y_2 - y_1\right)\left[ax_1x_2\left(y_2 + y_1\right) + bd\left(x_1 + x_2\right)\right] \end{aligned}$$

alors

$$x_2y_2 - x_1y_1 = \frac{\left(y_2 - y_1\right)\left[ax_1x_2\left(y_2 + y_1\right) + bd\left(x_1 + x_2\right)\right]}{b\left(x_1x_2 + d\right)}$$

remplaçons cette formule dans $-x_R$ on obtient

$$\begin{aligned} -x_R &= \frac{ax_1x_2\left(y_2+y_1\right)+bd\left(x_1+x_2\right)}{b\left(x_1x_2+d\right)}-\frac{\left(x_1+x_2\right)y_1y_2}{\left(y_1y_2-c\right)} \\ &= \frac{ax_1x_2\left(y_2+y_1\right)\left(y_1y_2-c\right)+bd\left(x_1+x_2\right)\left(y_1y_2-c\right)-bd\left(x_1+x_2\right)y_1y_2-bx_1x_2\left(x_1+x_2\right)y_1y_2}{b\left(x_1x_2+d\right)\left(y_1y_2-c\right)}. \end{aligned}$$

On a

$$\begin{aligned} ax_1x_2\left(y_2+y_1\right)\left(y_1y_2-c\right) &= \left(ax_1y_1x_2+ax_1x_2y_2\right)\left(y_1y_2-c\right) \\ &= ax_1y_1^2y_2x_2-acx_1y_1x_2+ax_1x_2y_1y_2^2-acx_1x_2y_2 \\ &= ax_1\left[\left(y_1^2-c\right)+c\right]y_2x_2+ax_1y_1x_2\left[\left(y_2^2-c\right)+c\right]-acx_1y_1x_2-acx_1x_2y_2 \\ &= by_1y_2x_2(x_1^2-d)+bx_1y_1y_2\left(x_2^2-d\right) \\ &= by_1y_2\left[x_2(x_1^2-d)+x_1\left(x_2^2-d\right)\right] \\ &= by_1y_2\left[x_1x_2\left(x_1+x_2\right)-d\left(x_1+x_2\right)\right] \\ &= by_1y_2\left(x_1+x_2\right)\left(x_1x_2-d\right) \end{aligned}$$

remplaçons cette égalité dans $-x_R$, on trouve

$$\begin{aligned} -x_R &= \frac{by_1y_2\left(x_1+x_2\right)\left(x_1x_2-d\right)+bd\left(x_1+x_2\right)\left(y_1y_2-c\right)-by_1y_2\left(x_1+x_2\right)\left(d+x_1x_2\right)}{b\left(x_1x_2+d\right)\left(y_1y_2-c\right)} \\ &= \frac{\left(x_1+x_2\right)\left[y_1y_2\left(x_1x_2-d\right)-y_1y_2\left(d+x_1x_2\right)+\left(y_1y_2-c\right)\right]}{\left(x_1x_2+d\right)\left(y_1y_2-c\right)} \\ &= \frac{\left(x_1+x_2\right)\left(-d\right)\left(y_1y_2+c\right)}{\left(x_1x_2+d\right)\left(y_1y_2-c\right)} \end{aligned}$$

alors

$$x_R=\frac{d\left(x_1+x_2\right)\left(y_1y_2+c\right)}{\left(x_1x_2+d\right)\left(y_1y_2-c\right)}.$$

Par symétrie, on obtient

$$y_R=\frac{c\left(y_1+y_2\right)\left(x_1x_2+d\right)}{\left(y_1y_2+c\right)\left(x_1x_2-d\right)}.$$

Donc

$$P_3=P_1+P_2=-R=(-x_R,-y_R)=\left(\frac{d\left(x_1+x_2\right)\left(y_1y_2+c\right)}{\left(x_1x_2+d\right)\left(c-y_1y_2\right)},\frac{c\left(y_1+y_2\right)\left(x_1x_2+d\right)}{\left(y_1y_2+c\right)\left(d-x_1x_2\right)}\right).$$

■

Lemme 66 ***(Addition de deux points confondus)*** *Soit $P_1=(x_1,y_1)$ un point de la courbe $H^{(c,d)}_{(a,b)}$. Les coordonnées du point $P_3=2P_1$ sont données par*

$$\begin{aligned} x_3 &= \frac{2dx_1\left(c+y_1^2\right)}{\left(d+x_1^2\right)\left(c-y_1^2\right)} \\ y_3 &= \frac{2cy_1\left(d+x_1^2\right)}{\left(c+y_1^2\right)\left(d-x_1^2\right)} \end{aligned}$$

Preuve. Posons

$$H(x,y) = ax(y^2-c) - by(x^2-d)$$

et soit $y = \alpha x + \beta$ l'équation de la droite tangente en P_1 avec

$$\alpha = \frac{dy}{dx}(x_1,y_1) = \frac{ay_1^2 - 2bx_1y_1 - ac}{bx_1^2 - 2ax_1y_1 - bd}$$

et

$$\begin{aligned}
\beta &= y_1 - \left(\frac{ay_1^2 - 2bx_1y_1 - ac}{bx_1^2 - 2ax_1y_1 - bd}\right)x_1 \\
&= \frac{by_1\left[\left(x_1^2-d\right)+d\right] - 2ax_1y_1^2 - bdy_1 - ax_1\left[\left(y_1^2-c\right)+c\right] + 2bx_1^2y_1 + acx_1}{bx_1^2 - 2ax_1y_1 - bd} \\
&= \frac{by_1\left(x_1^2-d\right) + bdy_1 - 2ax_1y_1^2 - bdy_1 - ax_1(y_1^2-c) - acx_1 + 2bx_1^2y_1 + acx_1}{bx_1^2 - 2ax_1y_1 - bd} \\
&= \frac{2x_1y_2\left(bx_1 - ay_1\right)}{bx_1^2 - 2ax_1y_1 - bd}.
\end{aligned}$$

Cette droite recoupe la courbe $H_{(a,b)}^{(c,d)}$ en un troisième point $R = (x_R, y_R)$. En remplacant par l'équation de la droite dans H, on obtient

$$H(x, \alpha x+\beta) = \left(a\alpha^2 - \alpha b\right)x^3 + \left(2a\alpha\beta - b\beta\right)x^2 + \left[a\left(\beta^2 - c\right) + \alpha\beta d\right]x + bd\beta = 0.$$

Cette équation admet trois racines, une racine double en $x_1$et x_R, alors l'équation ci-dessus s'écrit comme suit

$$\begin{aligned}
H(x, \alpha x+\beta) &= \gamma\left(x-x_1\right)^2\left(x-x_R\right) \\
&= \gamma\left[x^3 - \left(2x_1+x_3\right)x^2 + \left(2x_1x_3 + x_1^2\right)x - x_1^2x_3\right]
\end{aligned}$$

par identification, on trouve

$$\begin{aligned}
\gamma &= \left(a\alpha^2 - \alpha b\right) \\
-\left(2x_1 + x_R\right) &= \frac{2a\alpha\beta - b\beta}{a\alpha^2 - \alpha b}
\end{aligned}$$

donc

$$-x_R = \frac{\beta\left(2a\alpha - b\right)}{\alpha\left(a\alpha - b\right)} + 2x_1$$

après des simplifications, on obtient, (en tenant compte du fait que $(x_3, y_3) = (-x_R, -y_R)$)

$$x_3 = -x_R = \frac{2dx_1\left(c + y_1^2\right)}{\left(d + x_1^2\right)\left(c - y_1^2\right)}$$

et par symétrie

$$y_3 = -y_R = \frac{2cy_1\left(d + x_1^2\right)}{\left(c + y_1^2\right)\left(d - x_1^2\right)}.$$

■

Remarque 67 ∘ *Remarquons que cette loi d'addition est* ***unifiée****, c'est-à-dire on peut trouver* $2P_1$ *à partir de la loi de* $P_1 + P_2$.

∘ *L'ensemble des points* (x, y) *de la courbe* H *tel que* $xy = 0$ *se rédui à* $\{(0, 0)\}$.

Lemme 68 *Soient* $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ *deux points de la courbe de Huff*

$$H^{(c,d)}_{(a,b)} : ax(y^2 - c) = by(x^2 - d),\ abcd(a^2c - b^2d) \neq 0$$

avec

$$x_1x_2 \neq \pm d,\ y_1y_2 \neq \pm c.$$

Alors, soit

$$P_1 = P_2,$$

soit

$$P_1 \neq P_2, avec\ (x_1 - x_2)(y_1 - y_2) \neq 0.$$

Preuve. On a quatre cas :

a). $P_1 = P_2$

b). $P_1 = (x_1, y_1)$, $P_2 = (x_1, y_2)$ et $x_1y_1y_2 \neq 0$

c). $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_1)$ et $x_1x_2y_1 \neq 0$

d). $P_1 = (x_1, y_1), P_2 = (x_2, y_2)$ et $(x_1 - x_2)(y_1 - y_2) \neq 0$.

Montrons que les deux cas b) et c) se ramènent au cas a). Considerons les deux points $P_1 = (x_1, y_1)$, $P_2 = (x_1, y_2)$ du cas b), alors de l'équation de la courbe H on obtient :

$$\begin{aligned} ax_1(y_1^2 - c) &= by_1(x_1^2 - d) \\ ax_2(y_2^2 - c) &= by_2(x_1^2 - d) \end{aligned}$$

i.e.,

$$\begin{aligned} \tfrac{y_1^2 - c}{by_1} = \tfrac{y_2^2 - c}{by_2} &\Leftrightarrow b(y_1 - y_2)(y_1y_2 + c) = 0 \\ &\Leftrightarrow y_1 = y_2 \end{aligned}$$

par suite

$$P_1 = P_2.$$

De même si $y_1 = y_2$, cas c), alors

$$\begin{aligned} \tfrac{x_1^2 - d}{ax_1} = \tfrac{x_2^2 - d}{ax_2} &\Leftrightarrow a(x_1 - x_2)(x_1x_2 + d) = 0 \\ &\Leftrightarrow x_1 = x_2 \end{aligned}$$

par suite

$$P_1 = P_2.$$

On résume, les deux points P_1 et P_2 sont soit $P_1 = P_2$ soit $P_1 \neq P_2$, avec $(x_1 - x_2)(y_1 - y_2) \neq 0$. ■

Remarque 69 *1. Si $x_1x_2 \neq \pm d$ et $y_1y_2 \neq \pm c$, alors on peut toujours trouver P_1+P_2 et on a les formules suivantes :*

$$x_3 = \frac{d\,(x_1+x_2)\,(y_1y_2+c)}{(x_1x_2+d)\,(c-y_1y_2)}\ ,\ y_3 = \frac{c\,(y_1+y_2)\,(x_1x_2+d)}{(y_1y_2+c)\,(d-x_1x_2)}.$$

2. Si $x_1^2 \neq \pm d$ et $y_1^2 \neq \pm c$, en particulier si c et d ne sont pas des carrés dans K, alors on peut trouver $2P_1$, et on a :

$$x_3 = \frac{2dx_1\left(c+y_1^2\right)}{\left(d+x_1^2\right)\left(c-y_1^2\right)},\ y_3 = \frac{2cy_1\left(d+x_1^2\right)}{\left(c+y_1^2\right)\left(d-x_1^2\right)}.$$

Remarque 70 *1. Soit $P=(x,y)$ un point de la courbe de Huff $H_{(a,b)}^{(c,d)}$. Par le changement de variables*

$$(X,Y) = \left(a^3bxy, a^4b\left(a^3xy-bd\right)y\right)$$

le point P correspond au point $Q=(X,Y)$ sur la courbe $E_{(a,b)}^{(c,d)}$ avec

$$Q = \left(a^3bxy, a^4b\left(a^3xy-bd\right)y\right).$$

Par suite, l'inverse de Q sur $E_{(a,b)}^{(c,d)}$ est

$$-Q = \left(a^3bxy, a^4by(bd-a^3xy)\right) = \left(\widetilde{X},\widetilde{Y}\right).$$

A ce point correspond le point $\widetilde{P}=(\widetilde{x},\widetilde{y})$ sur $H_{(a,b)}^{(c,d)}$, avec

$$\begin{aligned}\widetilde{x} &= \frac{a\widetilde{X}\left(\widetilde{X}-b^2d\right)}{b\widetilde{Y}} = \frac{a^4bxy\left(a^3bxy-b^2d\right)}{a^4b^2y\left(bd-a^3xy\right)} = -x\\ \widetilde{y} &= \frac{\widetilde{Y}}{a^4(\widetilde{X}-b^2d)} = \frac{y\left(bd-a^3xy\right)}{a^3xy-bd} = -y.\end{aligned}$$

2. On a

$$\begin{aligned}(x,y)+(0,0) &= (x,y)\,,\\ (0,0)+(x,y) &= (x,y)\,.\end{aligned}$$

Le point $(0,0)$ vérifie l'équation $H_{(a,b)}^{(c,d)}$ et

$$\begin{aligned}\frac{\partial H}{\partial x}(0,0) &= -ac,\\ \frac{\partial H}{\partial y}(0,0) &= bd,\end{aligned}$$

par suite le point $(0,0)$ n'est pas un point singulier.

3. Si $(0,0)$ est choisi comme un élément neutre, alors $\widetilde{P}=(\widetilde{x},\widetilde{y})=(-x,-y)$ sera l'inverse du point P.

3.2 Courbes de Huff binaire $ax\left(y^2+y+1\right)=by\left(x^2+x+1\right)$

Dans cette partie, nous rappelons quelques résultats sur les courbes de Huff (binaire) de caractéristique deux : $\mathbb{F}_{2^m}$.

Definition 71 *Une courbe de Huff binaire sur un corps $\mathbb{F}_{2^m}$ est l'ensemble des points (x,y) satisfaisant l'équation*

$$H_{/\,\mathbb{F}_{2^m}} : ax\left(y^2+y+1\right)=by\left(x^2+x+1\right)$$

avec $a,b\in\mathbb{F}_{2^m}^*$ et $a\neq b$.

Definition 72 *La courbe de Huff binaire définie sur le corps $\mathbb{F}_{2^m}$ s'écrit dans les coordonnées projectives $\mathbb{P}_2\left(\mathbb{F}_{2^m}\right)$*

$$\overline{H}_{/\,\mathbb{F}_{2^m}} :\ aX\left(Y^2+YZ+Z^2\right)=bY\left(X^2+XZ+Z^2\right),\ a,\ b\in\mathbb{F}_{2^m}^*,\ a\neq b.$$

Proposition 73 *La courbe $\overline{H}_{/\,\mathbb{F}_{2^m}}$ admet trois points à l'infini à savoir*

$$P_1=[0,1,0],\ P_2=[1,0,0],\ P_3=\left[1,\frac{b}{a},0\right],$$

de plus ces points sont non singuliers.

Preuve. Les points à l'infini sont les points de la forme $[X,Y,0]$. Donc pour $Z=0$ on trouve

$$aXY^2=bX^2Y,$$

i.e.,

$$XY\left(aY-bX\right)=0,$$

alors les points à l'infini sont

$$\begin{aligned} P_1 &= [0,1,0],\\ P_2 &= [1,0,0],\\ P_3 &= \left[1,\frac{b}{a},0\right]. \end{aligned}$$

On a

$$\frac{\partial\overline{H}}{\partial X}(P_1)=a\neq 0,$$

$$\frac{\partial\overline{H}}{\partial Y}(P_2)=-b\neq 0,$$

$$\frac{\partial\overline{H}}{\partial X}(P_3)=\frac{b^2}{a}\neq 0,\ \frac{\partial\overline{H}}{\partial Y}(P_3)=-b\neq 0,$$

d'où le résultat. ■

Proposition 74 *La courbe de Huff binaire*

$$H_{/\,\mathbb{F}_{2^m}} : ax\left(y^2+y+1\right) = by\left(x^2+x+1\right),\ a,\ b \in \mathbb{F}_{2^m}^*,\ a \neq b$$

est une courbe lisse.

Preuve. Posons

$$H(x,y) = ax\left(y^2+y+1\right) - by\left(x^2+x+1\right).$$

Supposons qu'il existe un point singulier $P=(x,y)$, donc

$$H(x,y)=0,\ \frac{\partial H}{\partial x}(x,y)=0,\ \frac{\partial H}{\partial y}(x,y)=0$$

i.e.,

$$ax\left(y^2+y+1\right)+by\left(x^2+x+1\right)=0, \tag{3.7}$$

$$a\left(y^2+y+1\right)+by=0, \tag{3.8}$$

$$ax+b\left(x^2+x+1\right)=0. \tag{3.9}$$

Multiplions l'équation (3.9) par y, on trouve

$$axy+by\left(x^2+x+1\right)=0$$

i.e.,

$$axy+ax\left(y^2+y+1\right)=0$$

donc

$$ax\left(y^2+1\right)=0$$

i.e.,

$$x=0 \text{ ou } y^2=1.$$

Si $x=0$, par (3.7) on obtient $by=0$, ainsi $y=0$, impossible. Si $y^2=1$, par l'équation (3.8) on trouve

$$y(a+b)=0$$

donc

$$a=b$$

contradiction. Ainsi la courbe $H_{/\mathbb{F}_{2^m}}$ est une courbe lisse. ■

Proposition 75 *La courbe de Huff $H_{/\,\mathbb{F}_{2^m}}$ est birationnellement équivalente à la courbe elliptique E sur $\mathbb{F}_{2^m}$ donnée par la forme de Weierstrass*

$$\begin{aligned} Y^2+(a+b)XY &= X^3+\left(a^2+b^2\right)X^2+a^2b^2X \\ &= X\left(X+a^2\right)\left(X+b^2\right). \end{aligned}$$

avec les changements de variables sont données par

$$\begin{aligned} X &= abxy,\ Y=aby(ax+b), \\ x &= \frac{bX}{Y+aX},\ y=\frac{Y+aX}{ab^2}. \end{aligned}$$

Preuve. Posons

$$\begin{aligned} H(x,y) &= ax\left(y^2+y+1\right)+by\left(x^2+x+1\right)=0 \\ &= axy^2+\left(bx^2+(a+b)x+b\right)y+ax \\ &= byx^2+\left(ay^2+(a+b)y+a\right)x+by \end{aligned}$$

on est dans le cas **(II)** de l'algorithme de Harrache et Touafek (chapitre 2). Posons

$$X=abxy$$

on obtient

$$\begin{aligned} G(X,y) &= a^2\left(X+b^2\right)y^2+a(a+b)Xy+X^2+a^2X=0 \\ &= X^2+\left(a^2y^2+a(a+b)y+a^2\right)X+a^2b^2y^2 \end{aligned}$$

et on est dans le cas **(I)** de l'algorithme de Harrache et Touafek. Posons

$$W=a^2y\left(X+b^2\right)$$

on obtient

$$W^2+a(a+b)XW=a^2X^3+a^2\left(a^2+b^2\right)X^2+a^4b^2X$$

divisons par a^2 cette dernière équation et posons $W=aY$, nous obtenons

$$Y^2+(a+b)XY=X^3+\left(a^2+b^2\right)X^2+a^2b^2X$$

qui est une forme de Weierstrass birationnellement équivalente à la courbe de Huff binaire $H_{/\mathbb{F}_{2^m}}$, les changements de variables sont donnés par

$$X=abxy,\ Y=aby(ax+b),$$

$$x=\frac{bX}{Y+aX},\ y=\frac{Y+aX}{ab^2}.$$

■

Remarque 76 *1) Il existe un autre changement de variables permettant de trouver la même forme de Weierstrass pour la courbe de Huff $H_{/\mathbb{F}_{2^m}}$,voir[6]. Ce changement est donné par*

$$\begin{aligned} X &= \frac{ab}{xy},\ Y=\frac{ab(axy+b)}{x^2y}, \\ x &= \frac{b\left(X+a^2\right)}{Y},\ y=\frac{a\left(X+b^2\right)}{y+(a+b)X}. \end{aligned}$$

2) Pour simplifier les calculs dans ce qui suit nous utilisons le changement de variables ci-dessus.

Lemme 77 *Soient* $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ *deux points de* $H_{/\mathbb{F}_{2^m}}$.

1) Si $x_1 x_2 = 1$ *et* $y_1 y_2 \neq 1$, *alors*

$$P_1 = (x_1, y_1), P_2 = \left(\frac{1}{x_1}, y_1\right).$$

2) Si $x_1 x_2 \neq 1$ *et* $y_1 y_2 = 1$, *alors*

$$P_1 = (x_1, y_1), \ P_2 = \left(x_1, \frac{1}{y_1}\right).$$

3) Si $x_1 x_2 = 1$ *et* $y_1 y_2 = 1$, *alors*

$$P_1 = (x_1, y_1), \ P_2 = \left(\frac{1}{x_1}, \frac{1}{y_1}\right).$$

Preuve. 1) Si $x_1 x_2 = 1$ et $y_1 y_2 \neq 1$, donc $x_2 = \frac{1}{x_1}$ (On a $x_1 \neq 0$ si non $by_1 = 0$, i.e., $b = 0$ contradiction). En remplaçant dans l'équation de $H_{/\mathbb{F}_{2^m}}$, on trouve

$$ax_1 \left(y_2^2 + y_2 + 1\right) = by_2 \left(x_1^2 + x_1 + 1\right),$$

donc

$$ax_1 \left(y_2^2 + y_2 + 1\right) = y_2 \left(\frac{a}{y_1} x_1\right) \left(x_1^2 + x_1 + 1\right),$$

i.e.,

$$ax_1 \left(y_1 + y_2\right) \left(1 + y_1 y_2\right) = 0,$$

alors

$$y_1 = y_2,$$

par suite

$$P_2 = \left(\frac{1}{x_1}, y_1\right).$$

2) Si $x_1 x_2 \neq 1$ et $y_1 y_2 = 1$, on trouve par la même méthode

$$x_1 = x_2,$$

i.e.,

$$P_2 = \left(x_1, \frac{1}{y_1}\right).$$

3) On touve immédiatement que

$$P_2 = \left(\frac{1}{x_1}, \frac{1}{y_1}\right).$$

■

Proposition 78 ***Loi d'addition***

Soient $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ *deux points de* $H_{/\mathbb{F}_{2^m}}$. *Alors*

$$P_1+P_2 = \begin{cases} \left(\frac{b(x_1+x_2)(1+x_1x_2y_1y_2)+(a+b)x_1x_2(1+y_1y_2)}{b(1+x_1x_2)(1+x_1x_2y_1y_2)}, \frac{a(y_1+y_2)(1+x_1x_2y_1y_2)+(a+b)y_1y_2(1+x_1x_2)}{a(1+y_1y_2)(1+x_1x_2y_1y_2)}\right) \\ si \quad (1+x_1x_2)(1+y_1y_2)(1+x_1x_2y_1y_2) \neq 0, \\ (a,b,0) \quad si \;\; x_1x_2y_1y_2 = 1, \; x_1x_2 \neq 1 \; et \;\; y_1y_2 \neq 1, \\ (1,0,0) \quad si \;\; x_1x_2 = 1 \; et \; y_1 = y_2, \\ (0,1,0) \quad si \quad y_1y_2 = 1 \; et \;\; x_1 = x_2. \end{cases}$$

Preuve. Voir [6]. ■

Remarque 79 *1) Soit* $P = (x, y)$ *un point de la courbe de Huff binaire* $H_{/\mathbb{F}_{2^m}}$. *Par le changement de variables*

$$\left(\frac{ab}{xy}, \; \frac{ab\,(axy+b)}{x^2y}\right),$$

ce point correspond au point $Q = (X, Y)$ *sur la courbe* E *avec*

$$Q = \left(\frac{ab}{xy}, \; \frac{ab\,(axy+b)}{x^2y}\right).$$

Par suite, l'inverse de Q *sur* E *est*

$$-Q = (X, -Y-(a+b)\,X) = (X, Y+(a+b)\,X) = \left(\tilde{X}, \tilde{Y}\right).$$

Au point $-Q$, *correspond sur* $H_{/\mathbb{F}_{2^m}}$, *le point* $\overline{P} = (\overline{x}, \overline{y})$ *avec*

$$\begin{aligned} \overline{x} &= \frac{b\left(\tilde{X}+a^2\right)}{\tilde{Y}} \\ &= \frac{b\left(X+a^2\right)}{Y+(a+b)\,X} \\ &= \frac{b\left(\frac{ab}{xy}+a^2\right)}{\frac{ab(axy+b)}{x^2y}+(a+b)\,\frac{ab}{xy}} \\ &= \frac{x\,(b+axy)}{b+axy+(a+b)\,x}, \end{aligned}$$

on a

$$a+b = \frac{(ax+by)+xy\,(ay+bx)}{xy},$$

alors

$$\overline{x} = \frac{y\,(b+axy)}{a+bxy}.$$

Par symétrie on trouve

$$\overline{y} = \frac{x\,(a+bxy)}{b+axy}.$$

2) On a

$$\begin{aligned}(x,y)+(0,0) &= (x,y),\\ (0,0)+(x,y) &= (x,y).\end{aligned}$$

Le point $(0,0)$ *vérifie l'équation* $H_{/\mathbb{F}_{2^m}}$ *et on a*

$$\begin{aligned}\frac{\partial H}{\partial x}(0,0) &= a,\\ \frac{\partial H}{\partial y}(0,0) &= b,\end{aligned}$$

par suite le point $(0,0)$ *n'est pas un point singulier.*

3) Si on choisit $(0,0)$ *comme un élément neutre pour la loi d'addition définie ci-dessus alors* $\overline{P}=(\overline{x},\overline{y})$ *sera l'inverse du point* $P=(x,y)$.

4) Soit $P=(x,y)\in H_{/\mathbb{F}_{2^m}}$ *avec* $a+bxy=0$, *i.e.,* $y=\frac{-a}{bx}$. *On a* $x\neq 0$, *sinon* $a+bxy=0$ *implique* $a=0$. *En remplaçant dans l'équation de la courbe* $H_{/\mathbb{F}_{2^m}}$ *on trouve*

$$a^2+b^2+bx\,(a+b)=0,$$

donc

$$x=\frac{a+b}{b},$$

et par suite

$$y=\frac{a}{a+b}.$$

Dans ce cas

$$-P=(1,0,0)\,.$$

5) De même, si $b+axy=0$, *i.e.,* $y=\frac{-b}{ax}$, *donc*

$$P=\left(\frac{b}{a+b},\frac{a+b}{a}\right),$$

et donc

$$-P=(0,1,0)\,.$$

3.3 Des suites arithmétiques sur les courbes d'Edwards

En 2007, H. M. Edwards introduit une nouvelle formule des courbes elliptiques qui porte son nom, il a montré que toute courbe elliptique sur un corps K avec $car\,(K)\neq 2$ peut s'écrire sous cette forme sur une extension du corps K. Ici on s'intéresse à la construction des suites (de points) arithmétiques sur les courbes d'Edwards.

Definition 80 *Une courbe d'Edwards est une courbe donnée par*

$$E_d: x^2+y^2=1+d\,x^2y^2,\ d\in K-\{0,1\}\,.$$

Remarque 81 • *La loi d'addition est donnée par*

$$P_1 + P_2 = P_3 = \left(\frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2} \right) \tag{3.10}$$

avec $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ *sont deux points de la courbe* E_d.

• *Cette loi d'addition est unifiée, c'est-à-dire elle peut s'effectuer par une formule unique que se soit pour l'addition de deux points ou pour le doublement d'un point. Elle est même fortement unifiée, i.e., l'addition du neutre, ici* $(0, 1)$, *se fait par la même formule.*

•*L'inverse d'un point* $P_1 = (x_1, y_1) \in E_d$ *est*

$$-P_1 = (-x_1, y_1) .$$

Lemme 82 *Le dénominateur de la loi défini dans (3.10) ne peut jamais égal à* 0 *si* d *n'est pas un carré dans* K.

Preuve. Soient $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ deux points de la courbe E_d, i.e.,

$$x_i^2 + y_i^2 = 1 + d\ x_i^2y_i^2,\ i = 1, 2.$$

Posons

$$\varepsilon = dx_1x_2y_1y_2,\ \varepsilon = \pm 1$$

alors

$$x_1, x_2, y_1, y_2 \neq 0$$

et on a

$$\begin{aligned} dx_1^2y_1^2 \left(x_2^2 + y_2^2\right) &= dx_1^2y_1^2 \left(1 + d\ x_2^2y_2^2\ \right) \\ &= dx_1^2y_1^2 + d^2x_1^2y_1^2x_2^2y_2^2 \\ &= dx_1^2y_1^2 + \varepsilon^2 \\ &= 1 + dx_1^2y_1^2 \\ &= x_1^2 + y_1^2. \end{aligned}$$

Montrons que $\varepsilon = \pm 1$ implique d est un carré. On a trouvé que

$$dx_1^2y_1^2 \left(x_2^2 + y_2^2\right) = x_1^2 + y_1^2$$

par suite

$$\begin{aligned} (x_1 + \varepsilon y_1)^2 &= x_1^2 + y_1^2 + 2\varepsilon x_1y_1 \\ &= dx_1^2y_1^2 \left(x_2^2 + y_2^2\right) + 2 \left(dx_1x_2y_1y_2\right) x_1y_1 \\ &= dx_1^2y_1^2 \left(x_2^2 + y_2^2\right) + 2dx_1^2y_1^2 \left(x_2y_2\right) \\ &= dx_1^2y_1^2 \left(x_2^2 + 2x_2y_2 + y_2^2\right) \\ &= dx_1^2y_1^2 \left(x_2 + y_2\right)^2 . \end{aligned}$$

Donc

$$d = \left(\frac{x_1 + \varepsilon y_1}{x_1 y_1 (x_2 + y_2)} \right)^2.$$

Alors, si

$$x_2 + y_2 \neq 0$$

d est un carée. De même

$$\begin{aligned} (x_1 - \varepsilon y_1)^2 &= x_1^2 + y_1^2 - 2\varepsilon x_1 y_1 \\ &= d x_1^2 y_1^2 (x_2 - y_2)^2. \end{aligned}$$

Donc

$$d = \left(\frac{x_1 - \varepsilon y_1}{x_1 y_1 (x_2 - y_2)} \right)^2$$

i.e., si

$$x_2 - y_2 \neq 0$$

d est un carré. Si $x_2 + y_2 = 0$ et $x_2 - y_2 = 0$, alors $x_2 = y_2 = 0$, contradiction. ■

Definition 83 *La suite des points rationnels* $(x_1, y_1), (x_2, y_2), ..., (x_n, y_n)$ *sur la courbe d'Edwards* E_d *est dite suite arithmétique si les* x_i, $i = 1, ..., n$ *forment une suite arithmétique.*

Théorème 84 *Il existe une infinité de choix pour le paramètre* d *pour que la courbe d'Edwards* E_d *admet neuf points dans la suite arithmétique.*

Preuve. Il est clair que les points $(-1, 0)$, $(0, 1)$ et $(1, 0)$ sont des points sur la courbe $E_d, \forall d \in K$. On va essayé de trouver d pour faire une extension à cette suite arithmétique. Pour que la courbe admet des points avec des $x = \pm 2$, on doit avoir

$$\begin{aligned} 4 + y^2 &= 1 + 4dy^2 \\ &\Leftrightarrow \quad y^2 = \frac{3}{4d - 1}. \end{aligned}$$

Pour que y soit rationnel, il faut que

$$4d - 1 = 3j^2$$

avec j un certain nombre rationnel, alors on obtient

$$d = \frac{3j^2 + 1}{4}. \tag{3.11}$$

De même, pour que la courbe admet des points avec des $x = \pm 3$, on doit avoir

$$\begin{aligned} 9 + y^2 &= 1 + 9dy^2 \\ &\Leftrightarrow \quad y^2 = \frac{8}{9d - 1}. \end{aligned}$$

Pour que y soit rationnel, il faut que

$$9d - 1 = 2k^2$$

pour un certain nombre rationnel k, et on a par suite

$$d = \frac{1 + 2k^2}{9}. \tag{3.12}$$

Par les deux équations (3.11) et (3.12), on trouve l'équation de la conique

$$C_d : 27j^2 - 8k^2 + 5 = 0.$$

Remarquons que $(1, 2)$ est un point de la courbe C_d, alors on peut utiliser ce point pour paramétriser tous les points rationnels de la courbe C_d.

Posons

$$\begin{cases} x + 1 = j \\ y + 2 = k \end{cases}, \quad \begin{cases} x = j - 1 \\ y = k - 2 \end{cases}$$

et

$$m = \frac{k-2}{j-1}$$

avec m est un point rationnel, donc

$$j = \frac{k - 2 + m}{m}.$$

Alors

$$\begin{aligned}
27\left(\frac{k-2+m}{m}\right)^2 - 8k^2 + 5 &= 0 \\
27\left[(k-2)^2 + m^2 + 2m\,(k-2)\right] - 8k^2m^2 + 5m^2 &= 0 \\
\left(27 - 8m^2\right)k^2 + (54m - 108)\,k + 32m^2 - 108m + 108 &= 0 \\
(k-2)\left[\left(27 - 8m^2\right)k - 16m^2 + 54m - 54\right] &= 0 \\
\left(27 - 8m^2\right)(k-2)\left(k + \frac{2\left(8m^2 - 27m + 27\right)}{8m^2 - 27}\right) &= 0
\end{aligned}$$

i.e.,

$$k = 2 \qquad \text{ou} \qquad k = -\frac{2\left(8m^2 - 27m + 27\right)}{8m^2 - 27}.$$

Par suite, on trouve

$$j = \frac{-\frac{2\left(8m^2-27m+27\right)}{8m^2-27} - 2 + m}{m}$$

et après des simplifications, on obtient

$$j = \frac{8m^2 - 32m + 27}{8m^2 - 27}.$$

La paramétrisation de tous les points rationnels sur la courbe C_d est

$$(j,k) = \left(\frac{8m^2 - 32m + 27}{8m^2 - 27}, -\frac{2\left(8m^2 - 27m + 27\right)}{8m^2 - 27} \right)$$

avec m un nombre rationnel. Par l'équation (3.11) [ou (3.12)] , on trouve

$$\begin{aligned} d &= \frac{3\left(\frac{8m^2-32m+27}{8m^2-27}\right)^2 + 1}{4} \\ &= \frac{3}{4}\left(\frac{64m^4 - 512m^3 + 1456m^2 - 1728m + 729}{\left(8m^2 - 27\right)^2}\right) + \frac{1}{4} \end{aligned} \tag{3.13}$$

donc, pour chaque m nombre rationnel, on trouve une courbe d'Edwards E_d qui admet des points rationnels avec les x valent -3, -2, -1, 0, 1, 2 et 3.

De même, pour un point rationnel avec $x = \pm 4$, on trouve

$$\begin{aligned} 16 + y^2 &= 1 + 16dy^2 \\ y^2 &= \frac{15}{16d - 1}. \end{aligned}$$

En substituant la valeur de d de l'équation (3.13), on obtient

$$\begin{aligned} y^2 &= \frac{15}{16\left[\frac{3}{4}\left(\frac{64m^4-512m^3+1456m^2-1728m+729}{\left(8m^2-27\right)^2}\right) + \frac{1}{4}\right] - 1} \\ &= \frac{15\left(8m^2 - 27\right)^2}{960m^4 - 6144m^3 + 16176m^2 - 20736m + 10935} \\ &= \frac{5\left(8m^2 - 27\right)^2}{320m^4 - 2048m^3 + 5392m^2 - 6912m + 3645}. \end{aligned}$$

Alors y est un nombre rationnel si

$$320m^4 - 2048m^3 + 5392m^2 - 6912m + 3645 = 5t^2 \tag{3.14}$$

pour un certain nombre rationnel t. Avec **Maple,** on trouve que le discriminant de

$$320m^4 - 2048m^3 + 5392m^2 - 6912m + 3645$$

est égale à

$$15342052678041600,$$

donc l'équation (3.14) définit une courbe elliptique E. Un modèle de Weierstrass est donné par (voir [15])

$$E : y^2 = x^3 - x^2 - 19633x - 762863.$$

La courbe E est de rang 2 avec les générateurs $(-99, 448)$ et $(-93, 500)$. Alors il existe une infinité de points rationnels sur la courbe E. Donc pour chaque point (m, t), si on substitue la valeur de m dans (3.13), on obtient la valeur de d pour que la courbe E_d admet une suite arithmétique de neuf points -4, -3, -2, -1, 0, 1, 2, 3 et 4. ■

Bibliographie

[1] L. R. Alvaro, Elliptic Curves, Modular Forms and their L-functions, Student Mathematical Library, Ias/Park City Mathematical Subseries, Volume 58, (2013).

[2] J. W. S. Cassels, Lectures on elliptic curves, London Math.Soc, Student texts 24, Cambridge University Press, Cambridge, (1991).

[3] A. Ciss and D. Sow, On a new generalization of Huff curves, Cryptology eprint archive (2011). eprint. iarc.org / 2011/ 580.pdf.

[4] A. Ciss and D. Sow, Pairings On Generalized Huff curves, Cryptology eprint archive (2012). eprint. iarc.org / 2012/ 632.pdf.

[5] I. Connell, Elliptic curve Hand book, biblioteca.ucm.es/mat/doc8354.pdf. http : //www. math. mcgill. ca /connell, (1999).

[6] J. Devigne, M. Joye, Binary Huff curves, Published in A. Kiayias. Ed., Topics in Cryptology- CT-RSA 2011. vol. **6558** of Lecture Notes in Computer Science, Springer, (2011), 340-355,

[7] M. H. Edwards, A Normal form for elliptic Curves, Bulletin (New Series) of the American Mathematical Society, **44**, **(**2007), 393-422.

[8] G. B. Huff, Diophantine problems in geometry and elliptic ternary forms, Duke Math. J., 15, 443-453, (1948).

[9] T. Harrache, N. Touafek, Une remarque sur certaines formes de Weierstrass, Ital. J. Pure Appl. Math. 28 (2011), 295-308.

[10] M. Joye, Introduction élémentaire à la théorie des courbes elliptiques, joye.site88.net/theses/Joye_DEA.pdf, (1995).

[11] M. Joye, M. Tibouchi and D. Vergnaud, Huff's Model for elliptic curves, Cryptology eprint archive (2010). eprint. iarc.org / 2010/ 383.pdf.

[12] M. Khalfaoui, Variations sur la mésure de Mahler de certaines familles de polynômes à deux variables, Mémoire de Magister, Université de Jijel, 2013.

[13] K. Kodaira, On compact analytic surfaces I-III, Ann.of math. **71**(1960), 111-152 ; **77**(1963), 563-626 ; **78**(1963), 1-40.

[14] J. S. Milne, Elliptic curves, Kea Books (2006).

[15] D. Moody, Arithmetic Progressions on Edwards Curves, Journal of Integer Sequences, Vol. **14** (2011), Article 11.1.7.

[16] A. Néron, Modèles minimaux des varirétés abéliennes sur les corps locaux et globaux, Publ. Math. IHES 21 (1964) 1–128.

[17] K. Rolshausen, Eléments explicites dans le K_2 d'une courbe elliptique, Thèse de doctorat, Université Louis Pasteur, Strasbourg, (1996).

[18] J. H. Silverman, The Arithmetic of elliptic curves, Graduate texts in mathematics 106, Springer-Verlag, New York, (1986).

[19] J. Tate, Algorithm for determining the type of a singular fiber in an elliptic pencil, in : Modular Functions of One Variable IV, Lecture Notes in Math. 476, Springer, Berlin-Heidelberg-New York, 1975.

[20] N. Touafek, Mesure de Mahler et régulateur elliptique : quelques nouvelles relations exotiques, Thèse de Doctorat, Université de Constantine, 2008.

[21] H. Wu and R. Feng, Elliptic curves in Huff's model, Cryptology eprint archive (2010). eprint. iarc.org / 2010/ 390.pdf.

Résumé

On s'intéresse dans ce mémoire à l'arithmétique des courbes elliptiques. Ces courbes peuvent être présentées par différentes formes. Les modèles de Weierstrass, Huff et Edwards (suites arithmétiques des points) feront l'objet de ce travail.

ملخص

نهتم في هذه المذكرة بالخواص الحسابية للمنحنيات الإهليليجية. هاته المنحنيات يمكن أن تكون بأشكال مختلفة. نماذج فايرشتراس، هوف و إدوارذز (نقاط في متتالية حسابية) ستكون محور الدراسة في هذا العمل.