N ° D'ORDRE : 08/ 2010 - M / M

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEURE ET DE LA RECHERCHE SCIENTIFIQUE

Université des Sciences et de la Technologie

« Houari Boumediene »

Faculté de Mathématiques

MEMOIRE

Présenté pour l'obtention du diplôme de MAGISTER

En : MATHEMATIQUES

Spécialité : Algèbre et Théorie des Nombres

Par : ZOUBIR Nouara

Sujet

Algorithme de calcul d'isogénies d'une Courbe Elliptique

Soutenue le : 21 / 10 / 2010 à 10 H, devant le jury composé de :

Mr Meziane AIDER	*Professeur à l'U.S.T.H.B*	*Président*
Mr Mohamed ZITOUNI	*Professeur à l'U.S.T.H.B*	*Directeur de thèse*
Mr Mohamed Saleh HACHAÏCHI	*Maître de conférence à l'U.S.T.H.B*	*Examinateur*
Mr Mohand Ouamar HERNANE	*Maître de conférence à l'U.S.T.H.B*	*Examinateur*

SOMMAIRE

INTRODUCTION

Le sujet de ma thèse concerne des algorithmes de calcul d'isogénies des Courbes Elliptiques.

La théorie des Courbes Elliptiques est basée sur les domaines des Courbes Algébriques planes, de la théorie des Nombres Algébriques (structure de groupe,…) , de la théorie des Nombres Analytiques (fonction zêta de RIEMANN, fonctions arithmétiques), de la théorie des Nombres Géométriques (points singuliers, points ordinaires), de la Géométrie Algébrique (Variétés Abéliennes, Variétés Projectives).

Les Courbes Elliptiques ont intéressé de nombreux chercheurs :
CASSELS [1], MAZUR [10], SILVERMAN [13], TATE[14], ZITOUNI[17],etc..

Certaines Courbes Elliptiques ont été utilisées pour des applications en codage, en cryptographie. Elles ont été utilisées par WILLES pour démontrer le théorème de FERMAT.

Ma thèse est composée de 3 chapitres :

Dans le chapitre I j'ai abordé les propriétés Algébriques et Arithmétiques des équations de WEIERSTRASS, les invariants. J'ai construit une loi de groupe additif abélien sur l'ensemble E(K) des points K-rationnels des courbes au moyen de la règle géométrique de ″3 points colinéaires des Courbes Elliptiques″.
J'ai obtenu les formules des coordonnées du symétrique –P, de la somme P+R et de la somme 2P des points P et R de ces courbes.
Ce groupe de MORDELL-WEIL a une structure de groupe additif abélien de type fini.
J'ai utilisé les travaux de SILVERMAN pour préciser quelques propriétés de ces groupes.

Dans le chapitre II j'ai établi les propriétés de quelques homomorphismes des Courbes Elliptiques : Isomorphismes, Endomorphismes, Automorphismes.

Dans le chapitre III j'ai étudié quelques propriétés des isogénies des Courbes Elliptiques. J'ai utilisé quelques algorithmes de calcul d'isogénies :
Algorithme de B. MAZUR, Technique de VELU.

Les isogénies des Courbes Elliptiques sont des homomorphismes particuliers des groupes E(K) de MORDELL -WEIL.

Nous avons estimé utile de commencer par des notions de base de la Théorie des Courbes Elliptiques.

C'est un domaine des Mathématiques qui touche à la Théorie des Nombres, à l'Arithmétique, à la Géométrie Euclidienne, à la Géométrie Algébrique, à l'Analyse Complexe.

L'ouvrage de référence cité par les spécialistes est celui de J.H.SILVERMAN, [13]

1-Cubiques de WEIERSTRASS : équations

***Définition 1* :**

Les Cubiques de WEIERSTRASS sont des courbes algébriques planes d'équations spécifiques formées de 7 monômes.

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

où K est un corps commutatif global, local ou fini.

Les deux variables x et y sont des éléments d'une clôture algébrique K_{alg} du corps K.

(1) est une équation de Weierstrass de E.

L'équation (1) possède plusieurs modèles selon les coefficients a_i

En voici quelques-uns

$E_1 : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x$ avec $a_6 = 0.$

$E_2 : y^2 = x^3 + a_2x^2 + a_4x + a_6$ avec $a_1 = a_3 = 0.$

$E_3 : y^2 = x^3 + a_4x + a_6$ avec $a_1 = a_2 = a_3 = 0.$

La nature du corps de base K de la cubique E/K dépend de sa caractéristique et du nombre de ses éléments.

***Définition 2* :**

Le corps $\mathbb{Q}$ des nombres rationnels est de caractéristique carac($\mathbb{Q}$) = 0; il est infini; c'est le corps global primitif.

Ce corps admet des extensions algébriques $\mathbb{Q}(\theta)$ par des nombres algébriques θ.

***Définition 3* :**

Un nombre algébrique est un zéro θ non rationnel d'un polynôme f(x) $\in \mathbb{Q}$ [x]
irréductible, de degré n $\geq$ 2.

Exemples :
$f(x) = x^2 - 5$ admet 2 zéros : $\Theta = \pm \sqrt{5}$
$f(x) = x^4 - 94x^2 + 1849$ admet 4 zéros non rationnels : $\Theta = \pm\sqrt{2} \pm 3\sqrt{5}$.
$f(x) = x^3 - 10$ admet 3 zéros :
$\Theta_1 = \sqrt[3]{10}$, $\Theta_2 = j\sqrt[3]{10}$, et $\Theta_3 = j^2\sqrt[3]{10}$
avec $j = \exp(2\Pi i/3)$ et i complexe.

***Définition 4* :**

Un nombre θ qui n'est pas algébrique est un nombre transcendant.

Exemples :

$\Pi = 3{,}14159\ldots$,sin (2°) , log 2 sont des nombres transcendants.

***Définition 5* :**

1) un corps global est un corps de nombres algébriques $K = \mathbb{Q}(\theta)$; il est infini et de carac(K) = 0.
2) un corps local est un corps infini K de carac(K) = p, premier.
3) un corps fini est un corps IF_q à $q = p^n$ éléments, p premier ; il est de carac(K) = p.

Exemples :

1- les corps p-adiques sont des corps locaux ;
2- les corps finis IF_q pour $q = 2, 2^3, 3, 3^5, 5, 5^4, 7, 7^2$.

Cette équation (1) est dans le plan affine $/A^2(K)$ **.**
Les plans affines $/A^{n+1}(K)$ impliquent des plans projectifs $IP^n(K)$ au moyen d'une relation d'équivalence .
D'après [4], la relation R définie par :
deux points $x = (x_1 , x_2 , \ldots, x_n , x_{n+1})$ et $y = (y_1 , y_2 , \ldots, y_n , y_{n+1})$ de l'espace affine $/A^{n+1}(K)$ sont équivalents si et seulement si il existe un élément $\lambda \neq 0$ dans K tel que :
$y = \lambda x = (\lambda x_1 , \lambda x_2 , \ldots, \lambda x_n , \lambda x_{n+1})$.
R satisfait les axiomes des relations d'équivalence **:** réflexivité, symétrie et transitivité.
1) xRx, 2) xRy implique yRx, 3) xRy et yRz impliquent xRz.

Définition 6 :

Le n - espace projectif est l'ensemble des classes modulo la relation R :

$$\mathbf{IP^n(\ K\ ) = (\ /A^{n+1}(K) - (0,...,0)\ )/\ R\ ;} \qquad \mathbf{(2)}$$

L'espace projectif peut donc être représenté par l'ensemble des droites passant par l'origine.

L'équation affine de WEIERSTRASS se met sous la forme d'équation projective :

$$E : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4X Z^2 + a_6 Z^3 ; \quad \in IP^2(K) \qquad (3)$$

Le passage des coordonnées affines aux coordonnées projectives s'obtient avec l'application :

$$/A^{n+1}(K) \longrightarrow IP^n(K)$$

$$(x_1,\ldots, x_{n+1}) \longrightarrow \left(\frac{x_1}{x_{n+1}}, \ldots, \frac{x_n}{x_{n+1}}\right), x_{n+1} \neq 0 \qquad (4)$$

suivie de l'application multiplication par x^d_{n+1} , où d = degré du polynôme $f \in K[x_1,\ldots, x_n]$.

$$\left(\frac{x_1}{x_{n+1}}, \ldots, \frac{x_n}{x_{n+1}}\right) \longrightarrow x^d_{n+1}\left(\frac{x_1}{x_{n+1}}, \ldots, \frac{x_n}{x_{n+1}}\right) \qquad (5)$$

Exemple de passage du plan affine $/A^2(K)$ au plan projectif $IP^2(K)$:
Soit le polynôme affine :

$$f(x,y) = x^3 - 3xy + 2y^2 - 4y - 7 \in /A^2(K) ;$$

La transformation (4) transforme le polynôme f en polynôme :

$$f\left(\frac{x}{z}, \frac{y}{z}\right) = \frac{x^3}{z^3} - \frac{3xy}{z^2} + 2\frac{y^2}{z^2} - 4\frac{y}{z} - 7 \in /A^2(K) .$$

Pour d = 3, la multiplication par z^3 transforme le polynôme $f\left(\frac{x}{z}, \frac{y}{z}\right)$ en polynôme homogène de degré 3 :

$$g(x,y,z) = x^3 - 3xyz + 2y^2z - 4yz^2 - 7z^3 \in IP^2(K) .$$

L'équation (1) de WEIERSTRASS peut être transformée au moyen de substitutions convenables.
Nous éliminons les monômes en xy et en y avec le changement de variables linéaire :

$$(x , y) \longrightarrow \left(x , \frac{1}{2}(y - a_1x - a_3)\right) ; \qquad (6)$$

Nous obtenons pour un corps K de carac (K) ≠ 2, l'équation de WEIERSTRASS :

$$E_1 : y^2 = 4x^3 + b_2x^2 + 2\,b_4x + b_6 \quad \in \quad K\,[\,x\,,\,y\,]\,; \qquad (7)$$

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

$\mathbb{Z}\,[a_1, a_2\,, a_3, a_4, a_6\,]$:

$$b_2 = a_1^{\,2} + 4a_2\,;\;\; b_4 = a_1a_3 + 2a_4\,;\;\; b_6 = a_3^{\,2} + 4a_6 \qquad (8)$$

L'élimination du coefficient 4 et du monôme en x^2 dans l'équation E_1 s'obtient avec le changement de variables linéaire :

$$(x\,,\,y) \longrightarrow \left(\frac{x - 3b_2}{36}\;,\;\frac{y}{108}\right) \qquad (9)$$

Pour carac (K) ≠ 2, 3, nous obtenons l'équation de WEIERSTRASS :

$$E_2 : y^2 = x^3 - 27c_4x - 54c_6 \quad \in \quad K\,[\,x\,,\,y\,]\,;$$

(10)

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

$$c_4 = b_2^{\,2} - 24b_4 \quad ; \quad c_6 = -b_2^{\,3} + 36\,b_2b_4 - 216b_6 \;; \qquad (11)$$

2- Cubiques de WEIERSTRASS : invariants

Les invariants des cubiques sont des fonctions rationnelles f $(a_1,\ldots,\,a_6)$; qui varient suivant les valeurs prises par les a_i , ces invariants permettent des classifications des cubiques de WEIERSTRASS.

Il y a plusieurs invariants ; citons en quelques uns.

a) Discriminant d'une Cubique de WEIERSTRASS :

Définition 7 :

Le discriminant d'une Cubique de WEIERSTRASS E est le polynôme « homogène de degré 12 » dans l'anneau $\mathbb{Z}\,[b_2\,,\,b_4\,,\,b_6\,,\,b_8]$ égal à :

$$\mathbf{\Delta\,(E) = 9b_2b_4b_6 - 8b_4^{\,3} - 27\,b_6^{\,2} - b_2^{\,2}\,b_8\,;} \qquad \mathbf{(12)}$$

sur un corps K de caractéristique p ≠ 2,3

Le coefficient b_8 est déterminé par la relation :

$$\mathbf{4b_8 = b_2b_6 - b_4^{\,2}.}$$

b) Invariant modulaire d'une Cubique de WEIERSTRASS :

Définition 8 :

L'invariant modulaire d'une Courbe Elliptique E est l'élément j(E) du corps K égal à :

$$\mathbf{j(E) = c_4^{\,3}/\,\Delta(E)\,;} \qquad \mathbf{(13)}$$

c) Invariant différentiel d'une Cubique de WEIERSTRASS :

Définition 9 :**[13]**

L'invariant différentiel d'une Courbe Elliptique E est l'élément différentiel :

$$\omega(E) = \frac{dx}{F_y'} = \frac{-dy}{F_x'} \quad ; \qquad (14)$$

lié à la forme différentielle :

$$dF = F_x' \, dx + F_y' \, dy \; ;$$

où $F(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0$ est l'équation de Weierstrass de la cubique E .

F_y' est la dérivée partielle de F par rapport à y et

F_x' est la dérivée partielle de F par rapport à x.

Proposition 1 : **[17]**

Soit une courbe algébrique C, d'équation implicite f(x, y) = 0. Alors, un point s de la courbe est singulier si les dérivées partielles de f s'annulent en s :

$$f_y'(s) = f_x'(s) = 0.$$

□

Définition 10 :**[4]**

Le genre d'une courbe algébrique plane C de degré n, ayant s points singuliers, est l'entier naturel positif ou nul :

$$g(C) = (1/2)(n-1)(n-2) - s \; ; \qquad (15)$$

Les rangs r(E), les régulateurs R(E), les séries L(E,s) de DIRICHLET –HASSE sont d'autres invariants.

Les invariants $c_4(E)$ et $\Delta(E)$ classifient les cubiques en 2 classes :
Classe des cubiques singulières et classe des cubiques non singulières.

Définition 11 :

Une Courbe Elliptique est une cubique de WEIERSTRASS E non singulière. Alors, son discriminant n'est pas nul,[13].

Le signe du discriminant implique 2 types de Courbes Elliptiques : type I (courbes formées de 2 branches) si $\Delta(E) > 0$ et type II(courbes formées d'une seule branche) si $\Delta(E) < 0$.

Exemple de Courbe Elliptique de type I : 2 branches
Soit la cubique de Weierstrass

$$E_1 : y^2 = (x+3)(x+1)(x-2) \in \mathbb{R}[x,y]$$

Calcul du discriminant : $\Delta(E_1) = 64^2 .143 > 0$
Les 3 points d'intersection de E_1 par Ox : (-3,0) , (-1,0) , (2,0)
Deux autres points : $(-2, \pm 2)$ et $(3, \pm\sqrt{24})$

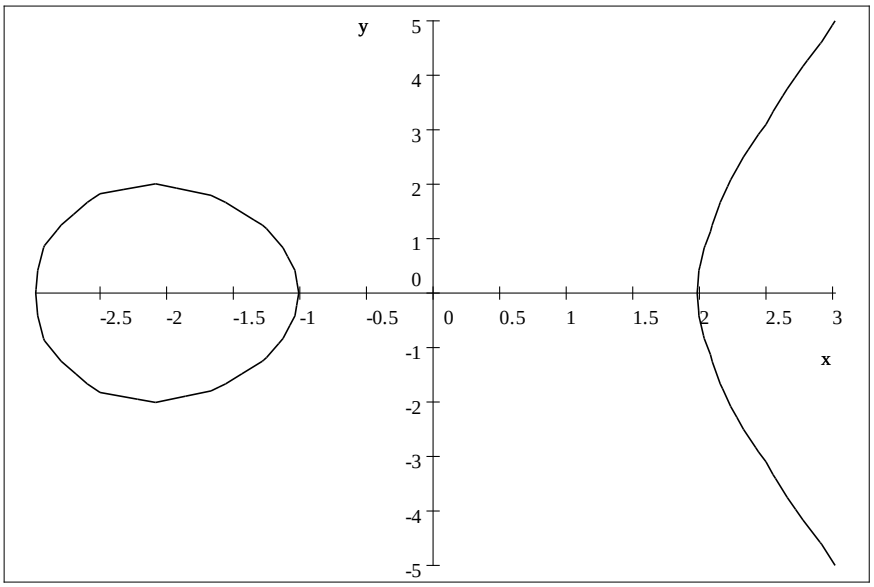


Figure 1(courbe tracée avec le logiciel Scientific Notebook 5.0)

Exemple de Courbe Elliptique de type II : une seule branche
Soit la cubique de Weierstrass

$$E_2 : y^2 = x^3 + 5x^2 + 11x + 15 \in \mathbb{R}[x,y]$$

Calcul du discriminant :

$$\Delta(E_2) = -16.501 < 0.$$

Quelques points de E_2 :

$(x = 0, y = \pm\sqrt{15})$; $(x = 1, y = \pm\sqrt{32})$; $(x = -1, y = \pm\sqrt{3})$;
$(x = -3, y = 0)$; $(x = -2, y = \pm\sqrt{5})$

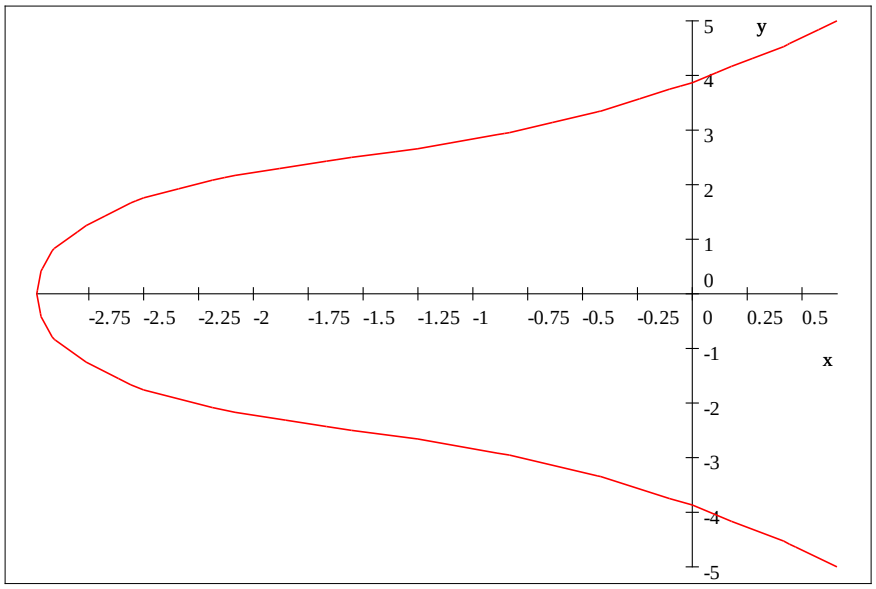


Figure 2(courbe tracée avec le logiciel Scientific Notebook 5.0)

3- Groupes de MORDELL-WEIL des Courbes Elliptiques et leurs sous groupes :

Une loi de groupe sur une Courbe Elliptique peut être déterminée par la théorie des diviseurs sur une Variété abélienne.

Cette loi peut être aussi déterminée par la propriété géométrique « de trois points colinéaires d'une Courbe Elliptique »; c'est cette loi que nous choisissons d'exposer et d'utiliser :

3-1- Structure de groupe additif abélien sur l'ensemble E(K) :

Soit une Courbe Elliptique E d'équation de WEIERSTRASS :

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

Sur l'ensemble E(K) des points rationnels de la Courbe Elliptique E, nous définissons une loi de groupe additif abélien, d'élément neutre le point à l'infini $O_E = (\infty,\infty)$ dans le plan affine $/A^2(K)$, et (0,1,0) dans le plan projectif $IP^2(K)$.
Ce point est déterminé par la direction de l'axe Oy d'après (0,1,0).

Proposition 2 :

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

$$f : E(K) \times E(K) \longrightarrow E(K)$$

de valeur : $f(P,Q) = P+Q$ et $f(O_E) = O_E$.

Preuve :

1) Axiome de l'élément neutre :

Le point O_E à l'infini joue le rôle d'élément neutre; il est déterminé par la direction de l'axe Oy.

Pour tout point P de l'ensemble E(K), la sécante PO_E est parallèle à l'axe Oy, la règle géométrique des 3 points colinéaires implique :

$$P + O_E = P = O_E + P.$$

L'axiome de l'élément neutre est vérifié.

2) Axiome du symétrique :

Le symétrique d'un point P de l'ensemble E(K) est le 2éme point R d'intersection de E par la parallèle à l'axe Oy qui passe par le point P. Il satisfait la règle géométrique des 3 points colinéaires :

$$P + R + O_E = O_E ;$$

Il en résulte le symétrique de P : $R = -P$.

3) Axiome de commutativité :

Toute sécante ST de la courbe E est confondue avec la sécante TS.

il en résulte la relation :

$$S+T = T+S.$$

L'axiome de commutativité est vérifié.

4) Axiome d'associativité :

Il est vérifié par le calcul des coordonnées des points (P + Q) +R et P+(Q + R);

□

Définition 12 :

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

3-2- Coordonnées des points –P, P_1+P_2, 2P, mP :

Calcul des coordonnées du symétrique –P d'un point P de la courbe E : (figure.3)

Soit un point $P = (x_p, y_p)$ du groupe E(K) et son symétrique

$$-P = (x,y) ; \quad P + (-P) = O_E$$

Le point –P est le $2^{éme}$ point d'intersection de la courbe E par la parallèle à Oy passant par P.

L'équation de cette parallèle est $x = x_p$.

L'équation (1) devient une équation en y de degré 2 ;

$$y^2 + y(a_1x+a_3) = x^3_p - a_2x^2_p - a_4x_p - a_6 \qquad (2)$$

Elle admet 2 racines y_p et y; leur somme est la fonction symétrique élémentaire « somme des 2 racines », égale à :

$$y_p + y = -(a_1x_p + a_3) \quad \text{cela implique} \quad y = -(y_p + a_1x_p + a_3)$$

Nous en déduisons les coordonnées du symétrique -P du point $P = (x_p , y_p)$:

$$-P = (x_p, -y_p - a_1x_p - a_3) \qquad (3)$$

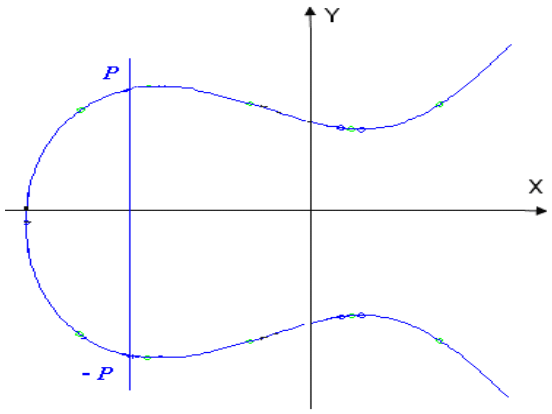


Figure.3

Calculons les coordonnées du point somme $P_1+P_2= M = (x_M ,y_M)$ de deux points $P_1 = (x_1 ,y_1)$, $P_2 = (x_2 ,y_2)$, pour $P_1 \neq \pm P_2$ (figure.4) :

La règle géométrique $P_1+P_2+P_3 = O_E$ implique :$P_1+P_2= -P_3 + O_E = -P_3 = M$

Le point P_3 est l'intersection de E par la droite P_1P_2 :

L'équation de la sécante P_1P_2 est :

$$y = \lambda (x - x_1) + y_1 \quad \text{avec la pente} \quad \lambda = (y_1 - y_2) / (x_1 - x_2) \qquad (4)$$

La sécante P_1P_2 coupe la Courbe Elliptique E en trois points simples P_1, P_2 et P_3 d'abscisses x_1, x_2 et x_3.

Ces trois abscisses sont les racines de l'équation algébrique en x de degré 3 obtenue avec (4)

$$[\lambda(x-x_1) + y_1]^2 + [\lambda(x-x_1) + y_1][a_1x + a_3] = x^3 + a_2x^2 + a_4x + a_6 \quad ; \qquad (5)$$

La fonction symétrique « somme des racines » vaut :

$$x_1+x_2+x_3 = \lambda^2 + a_1\lambda - a_2 \qquad (6)$$

La formule (6) implique les coordonnées du point P_3 :

$$P_3=(x_3 = \lambda^2+a_1\lambda-a_2-x_1-x_2,\ y_3=y_1+\lambda(x_3-x_1)) \ ;$$

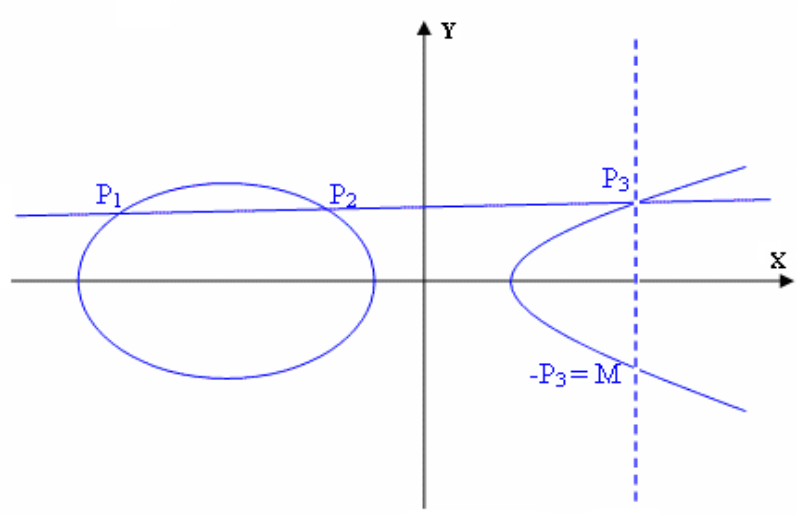
La relation géométrique $P_1+P_2+P_3 = O_E$ implique $M = P_1+P_2$ est le symétrique du point P_3 .

Avec le calcul j'obtiens les coordonnées du point M :

$$x_M = \lambda^2 + \lambda a_1 - a_2 - x_1 - x_2 ;$$

$$y_M = -\lambda^3 - 2a_1\lambda^2 + \lambda(a_2 - a_1^2 + 2x_1 + x_2) + a_1a_2 - a_3 + a_1(x_1 + x_2) - y_1 \quad (7)$$

avec la pente $\lambda = (y_1 - y_2) / (x_1 - x_2)$



□ **Figure.4**

Nous avons démontré la :

Proposition 3 :
Soit une Courbe Elliptique E d'équation de WEIERSTRASS :

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

1) le symétrique d'un point $P = (x_P, y_P)$ de E est le point $-P = (x_P, -y_P - a_1x_P - a_3)$;
2) la somme $P_1 + P_2 = M$ de deux points $P_1 \neq \pm P_2$ de la courbe E, est le point M de coordonnées :

$$X_M = \lambda^2 + \lambda a_1 - a_2 - x_1 - x_2 ;$$

$$Y_M = -\lambda^3 - 2a_1\lambda^2 + \lambda(a_2 - a_1^2 + 2x_1 + x_2) + a_1a_2 - a_3 + a_1(x_1 + x_2) - y_1 ;$$

avec la pente $\lambda = (y_1 - y_2) / (x_1 - x_2)$.

□

Calculons les coordonnées du point 2P :
Les coordonnées du point 2P sont déterminées par la :

Proposition 4 :
Soit une Courbe Elliptique E d'équation de Weierstrass :

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

Les coordonnées du point P + P = 2P = (x_{2P}, y_{2P}) pour tout point P = (x_P, y_P) de la courbe E sont égales à :

$$\mathbf{x_{2P} = y_P'^2 + a_1y_P' - a_2 - 2x_P} \quad \textbf{et} \quad \mathbf{y_P' = \frac{3x_P^2 + 2a_2x_P + a_4 - a_1y_P}{2y_P + a_1x_P + a_3}} \quad ;$$

$$\mathbf{y_{2P} = - y_P'^3 - 2a_1y_P'^2 + y_P'(a_2 - a_1^2 + 3x_P) + a_1a_2 - a_3 + 2a_1x_P - y_P} \ .$$

Preuve :(Figure.5)
Soit un point P = (x_P, y_P) de la Courbe Elliptique .
La tangente à la Courbe Elliptique E au point P a pour équation :

$$y = y_P' (x - x_P) + y_P ;$$

où y_P' est la pente de la tangente à la Courbe Elliptique E au point P = (x_P, y_P) :

$$y_P' = \frac{3x_P^2 + 2a_2x_P + a_4 - a_1y}{2y_P + a_1x_P + a_3} \ ; \qquad (8)$$

Cette tangente coupe la courbe E en un point P = (x_P, y_P) double et un point simple M = (x_M, y_M)
La règle de trois points colinéaires implique la relation :

$$2P + M = O_E \ \text{ et } \ 2P = - M \ ; \qquad (9)$$

Les abscisses de ces trois points sont les racines de l'équation cubique en x :

$$[y_P + y_P' (x - x_P)]^2 + a_1x [y_P' (x - x_P) + y_P] = x^3 + a_2x^2 + a_4x + a_6 \ ; \qquad (10)$$

La fonction symétrique élémentaire somme des racines de l'équation (10) implique la relation :

$$2x_P + x_M = y_P'^2 + a_1 y_P' - a_2 \ ; \qquad (11)$$

La relation (11) implique l'abscisse du point M :

$$x_M = y_P'^{\,2} + a_1 y_P' - a_2 - 2x_P \; ; \qquad (12)$$

(9), (12) et la formule du symétrique d'un point impliquent les coordonnées du point 2P :

$$x_{2P} = y_P'^{\,2} + a_1 y_P' - a_2 - 2x_P \quad \text{et} \quad y_P' = \frac{3x_P^2 + 2a_2x_P + a_4 - a_1y}{2y_P + a_1x_P + a_3} \; ;$$

$$y_{2P} = -y_P'^{\,3} - 2a_1 y_P'^{\,2} + y_P'(a_2 - a_1^2 + 3x_P) + a_1a_2 - a_3 + 2a_1x_P - y_P \; ; \qquad (13)$$

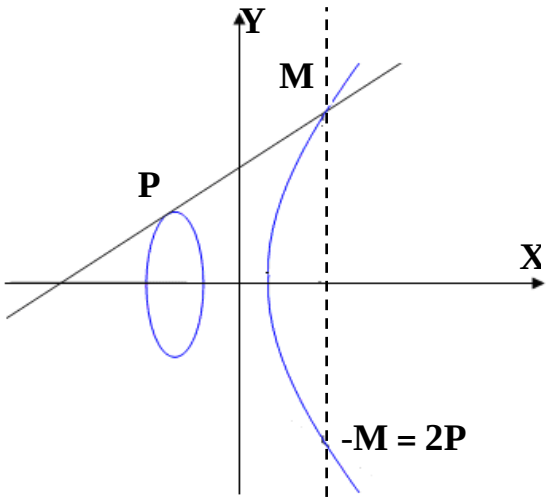


Figure.5

□

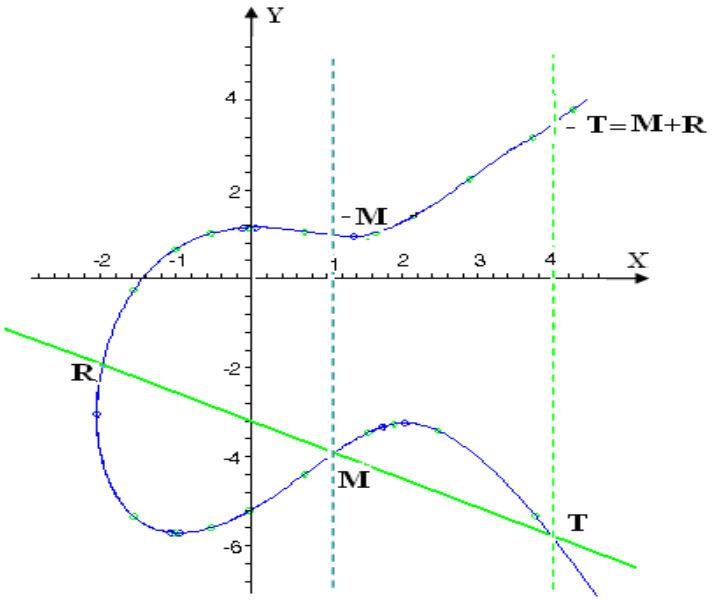
Exemple 1:

Soit la Courbe Elliptique E d'équation de WEIERSTRASS :

$$E : y^2 - xy + 4y = x^3 - 2x^2 - x + 6 \in \mathbb{Q}[x, y] \; ;$$

Le groupe de MORDELL-WEIL $E(\mathbb{Q})$ contient les deux points M = (1,-4) et R = (-2,-2) .
Calcul des coordonnées des points M + R, -M, -R, 2M, 2R :
Nous obtenons les résultats suivants :

M + R = (37/9,125/27) , -M = (1,1) , 2M = (6/25,96/125)



□ **Figure.6**

Avec les propositions 3 et 4, nous pouvons calculer les coordonnées de tout point mP, m > 2 .
Ainsi 3P = 2P + P, 4P = 2(2P), 5P = 4P + P, etc …

Les coordonnées de ces points sont des fractions rationnelles du corps $K(x, y, a_1,\ldots, a_6)$.

Calculons les coordonnées des points mP pour m = 2,3,4, …:

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

$$\begin{cases} mP = P + P + \ldots + P ; & m \text{ fois } P & \text{si } m > 0 . \\ mP = (-P) + (-P) + \ldots + (-P) ; & (-m) \text{ fois } (-P) & \text{si } m < 0 . \\ mP = O_E ; & & \text{si } m = 0 . \end{cases} \quad (14)$$

Les formules des coordonnées des points mP sont déterminées par la :

Proposition 5 :

Soit un point P = (x,y) du Groupe de MORDELL-WEIL E(ℚ) d'une Courbe Elliptique E d'équation de WEIERSTRASS :

$$y^2 = x^3 + Ax + B \in \mathbb{Q}[x, y] \text{ ; avec } 4A^3 + 27B^2 \neq 0 \text{ et } A, B \in \mathbb{Z}.$$

Alors un point mP = (x_m, y_m) a des coordonnées égales à :

$$x(mP) = \frac{\Phi_m(P)}{(\Psi_m(P))^2} \quad ; \quad \text{et} \quad y(mP) = \frac{\omega_m(P)}{(\Psi_m(P))^3} \quad ;$$

Les numérateurs et les dénominateurs Φ_m, Ψ_m et ω_m sont des polynômes de l'anneau $\mathbb{Z}[A, B, x, y]$.
Les polynômes Ψ_m sont égaux à:

$$\Psi_{-1} = -1 , \Psi_0 = 0 , \Psi_1 = 1 , \Psi_2 = 2y ;$$

$$\Psi_3 = 3x^4 + 6Ax^2 + 12Bx - A^2 ;$$

$$\Psi_4 = 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - A^3 - 8B^2) ;$$

Les polynômes Ψ_m, pour $m \geq 2$ satisfont les relations de récurrence :

$$\Psi_{2m} = 2\Psi_m (\Psi_{m+2} \Psi_{m-1}^3 - \Psi_{m-2} \Psi_{m+1}^2) \quad \text{et}$$

$$\Psi_{2m+1} = \Psi_{m+2} \Psi_m^3 - \Psi_{m-1} \Psi_{m+1}^3 \quad ; m \geq 2$$

Les polynômes Φ_m et ω_m satisfont les relations :

$$\Phi_m = x \Psi_m^2 - \Psi_{m-1} \Psi_{m+1} ; \quad m \geq 3 ;$$

$$\text{et } 4y\omega_m = \Psi_{m-2} \Psi_{m-1}^2 - \Psi_{m+2} \Psi_{m+1}^2 .$$

Preuve :
C'est le lemme 7-2 dans « Diophantine Equations with Special References to Elliptic Curves » de [1].
Pour m = -1, -P est le symétrique du point P ; il en résulte $\Psi_{-1} = -1$.
Pour m = 0, $0P = O_E = (\infty,\infty) = [\frac{\Phi_0}{\Psi_0^2}, \frac{\omega_0}{\Psi_0^3}]$; cela implique $\Psi_0 = 0$, $\Phi_0 = \omega_0 = 1$
Les formules se démontrent par récurrence sur l'entier naturel m.

En appliquant ces formules pour m = 2, nous obtenons les polynômes :

$$\begin{cases} \Psi_2 = 2y ; \\ \Phi_2 = x^4 - 2Ax^2 - 8Bx + A^2 ; \\ \omega_2 = x^6 + 5Ax^4 + 20Bx^3 - 5A^2 x^2 - 4ABx - A^3 - 8B^2 ; \end{cases} \quad (15)$$

Les coordonnées du point 2P sont donc égales à :

$$\begin{cases} x_{2P} = \dfrac{x^4 - 2Ax^2 - 8Bx + A^2}{(2y)^2} ; \\ y_{2P} = \dfrac{x^6 + 5Ax^4 + 20Bx^3 - 5A^2 x^2 - 4ABx - A^3 - 8B^2}{(2y)^3} ; \end{cases} \quad (16)$$

Pour m = 3, nous obtenons les polynômes :

$$\begin{cases} \Psi_3 = 3x^4 + 6Ax^2 + 12Bx - A^2 \\ \Phi_3 = x^9 - 12Ax^7 - 96Bx^6 + 30A^2x^5 - 24ABx^4 + 12(3A^3 + 4B^2)x^3 + 48A^2Bx^2 + \\ \quad 3A(3A^3 + 32B^2)x + 8B(3A^3 + 8B^2) \\ \omega_3 = y[x^{12} + 22A\,x^{10} + 220\,x^9 - 165\,A^2\,x^8 - 528AB\,x^7 - 4(23\,A^3 + 444\,B^2)\,x^6 + \\ \quad 264\,A^2Bx5a(37\,A^3 + 576\,B^2)\,x^4 - 80B(4B^2 + A^3)\,x^3 - 6\,A^2(15\,A^3 + 104\,B^2)\,x^2 - \\ \quad 28AB(3A^3 + 32B^2)x - 3A^6 - 96A^3B^2 - 512B^4] ; \end{cases} \quad (17)$$

Ψ_3 est un polynôme de l'anneau $\mathbb{Z}$ [x,A,B] de degré 4 en x.

Φ_3 un polynôme de l'anneau $\mathbb{Z}$ [x,A,B] de degré 9 en x .

ω_3 /y est un polynôme de l'anneau $\mathbb{Z}$ [x, A, B] de degré 12 en x.
Avec le calcul, nous obtenons le carré du polynôme Ψ_3 :

$$\Psi_3^2 = 9x^8 + 36Ax^6 + 72Bx^5 + 30A^2x^4 + 144ABx^3 + 12(12B^2 - A^3)x^2 - 24A^2Bx + A^4; \quad (18)$$

Ψ_3^2 est un polynôme de l'anneau [x,A ,B] de degré 8 en x , nous en déduisons le polynôme :

$\Psi_3^3 = 27x^{12} + 162Ax^{10} + 324Bx^9 + 297A^2x^8 + 1296ABx^7 + 108\,(A^3 + 12B^2)\,x^6 + 1080A^2Bx^5 + 9A(288B^2 - 11A^3)x^4 + 432B(4B^2 - A^3)x^3 + 18A^2(A^3 + 24B^2)x^2 - 12A^4Bx - A^6$; (19)

Ψ_3^3 est un polynôme de l'anneau $\mathbb{Z}[x, A, B]$ de degré 12 en x .

Les formules (17), (18) et (19) impliquent les coordonnées du point 3P :

$$x_{3p} = \frac{\Phi_3}{\Psi_3^2} \quad , \quad y_{3p} = \frac{\omega_3}{\Psi_3^3} \tag{20}$$

□

Exemple :
Pour appliquer les formules de la proposition 5 il faut une Courbe Elliptique de modèle:

$$y^2 = x^3 + Ax + B \in \mathbb{Q}[x , y] \text{ ; avec } 4A^3 + 27B^2 \neq 0 \text{ et } A , B \in \mathbb{Z}$$

.

Je choisis la Courbe Elliptique E pour A = -5, B = -2

$$y^2 = x^3 - 5x - 2 \in \mathbb{Q}[x , y]$$

(1)
Calcul des invariants de E :

$$b_2 = 0 , b_4 = -10, b_6 = -8 , b_8 = -25 , \Delta(E) = 2^7 \times 7^2 \neq 0 .$$

Je détermine les points de 2-torsion avec les formules de [1] :

$$\begin{cases} x_{2p} = \dfrac{\Phi_2}{\Psi_2^2} = \dfrac{x^4 + 10x^2 + 16x + 25}{(2y)^2} \\ y_{2p} = \dfrac{\omega_2}{\Psi_2^3} = \dfrac{x^6 - 25x^4 - 40x^3 - 125x^2 - 40x + 93}{(2y)^3} \end{cases} \tag{2}$$

Par définition, un point P de 2-torsion satisfait la relation :

$$2P = O_E = (\infty, \infty) \text{ ;} \tag{3}$$

Les formules (2) et (3) impliquent l'ordonnée du point 2P :

$$y = 0 \tag{4}$$

Les équations (1) et (4) impliquent trois solutions qui sont les abscisses de 3 points : $P_1 = (2, 0)$; $P_1 = (1-\sqrt{2}, 0)$; $(1+\sqrt{2}, 0)$

Par « ordre d'un point d'une Courbe Elliptique E », nous entendons l'ordre d'un point du groupe abélien E(K) de MORDELL-WEILL de E .

Définition 13 :

Pour tout entier rationnel m, un point P de E (K) d'ordre m satisfait la relation $mP = O_E$.

Le groupe E (K) de MORDELL -WEIL d'une Courbe Elliptique E, qui est additif, admet des sous groupes cycliques et des sous groupes abéliens.

Définition 14 :

1) Le sous groupe de m-torsion d'une Courbe Elliptique E, pour tout entier $m > 1$, est l'ensemble des points $P \in E(K)$ d'ordre m :

$$E(K)[m] = \{ P \in E(K); mP = O_E \}$$

Ces sous groupes sont cycliques ou abéliens d'ordre m.

2) Le groupe de torsion de la Courbe Elliptique, est l'ensemble des points P d'ordre fini.

C'est la réunion infinie des sous groupes de m torsion de E :

$$T(E) = \{ P \in E(K) ; mP = O_E , m \in \mathbb{Z}\} = \bigcup_m E(K)[m] .$$

Ce groupe de torsion T(E) est cyclique ou abélien, selon les invariants de la Courbe Elliptique.

La détermination du groupe de torsion T(E) a été réalisée pour les Courbes Elliptiques sur le corps $\mathbb{Q}$ des nombres rationnels. La structure de ce groupe a été conjecturée par OGG.

Cette conjecture a été démontrée par MAZUR.

Proposition 6 : **(Théorème de MORDELL-WEIL)**

Les groupes de MORDELL-WEIL E(K) des Courbes Elliptiques E sont de type fini.

Preuve dans [10]

□

La structure algébrique des groupes de MORDELL-WEIL des Courbes Elliptiques est précisée par le :

Corollaire :

Les groupes de MORDELL-WEIL E(K) des Courbes Elliptiques E sont isomorphes au produit de groupes abéliens additifs:

$$E(K) \cong T(E) \times \mathbb{Z}^r$$

où T(E) sont les groupes de torsion des Courbes Elliptiques E, ces groupes T(E) sont finis.
r = r(E) est un entier positif ou nul.

$\mathbb{Z}^r$ = r copies du groupe abélien additif infini $\mathbb{Z}^r$.

Preuve dans[5] S. LANG « Elliptic Curves. Diophantine analyses S. Verlag-1978 »

□

Définition 15 :

L'entier naturel r = r(E) ≥ 0 de cette formule d'isomorphisme est le rang de la Courbe Elliptique E. C'est aussi le nombre de générateurs P_1, …,P_r de la partie infinie du groupe E(K).

Le rang d'une Courbe Elliptique ne peut pas être obtenu à l'aide d'une formule, parce qu'il n'existe pas une telle formule.
Il peut être évalué à l'aide de fonctions particulières (hauteurs sur des groupes abéliens) et la série L(E, s) de DIRICHLET-HASSE [13], [14], [17].

CHAPITRE II : HOMOMORPHISMES DES GROUPES E(K).

Il existe plusieurs types d'homomorphismes.

$f : E(K) \longrightarrow E'(K)$:
des homomorphismes injectifs, des homomorphismes surjectifs, des isomorphismes, des endomorphismes, des automorphismes, des twists, des isogénies, des translations.

Ce vocabulaire est emprunté à la Théorie des Ensembles :
Ensembles finis, ensembles infinis, ensembles dénombrables; applications d'un ensemble A sur un ensemble B; applications injectives, applications surjectives, applications bijectives; applications réciproques, noyaux, compositions, diagrammes.

Définition1 :

Soit deux Courbes Elliptiques E et E', sur le même corps K, leurs points à l'infini respectifs O_E et $O_{E'}$. Un homomorphisme de Courbes Elliptiques E et E'est un homomorphisme de groupes abéliens $f : E(K) \longrightarrow E'(K)$.

Les homomorphismes que nous allons étudier dans ce chapitre sont les Isomorphismes, les Endomorphismes, les Automorphismes

1- Isomorphismes des Courbes Elliptiques :

Définition2 :

Un isomorphisme de 2 Courbes Elliptiques E et E'est une application de groupes de MORDELL-WEIL :

$$f : E(K) \longrightarrow E'(K)$$

qui satisfait les formules d'isomorphisme de groupes abéliens :

1) $f(O_E) = O_{E'}$.

2) $f(P_1 + P_1) = f(P_1) + f(P_2)$.

3) f est bijective.

Ces isomorphismes sont caractérisés par des formules spécifiques comme en le verra plus bas :

Proposition1 :

Un isomorphisme de deux Courbes Elliptiques E et E' est une application :

$$f : E(K) \longrightarrow E'(K)$$

de valeur :

$$f(x,y) = (u^2X + r, u^3Y + su^2X + t) , \qquad (1)$$

où $u \neq 0$, r, s, t sont des éléments de K.

Preuve :

Considérons une Courbe Elliptique d'équation de WEIERSTRASS :

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

La transformée de E par f est la courbe f(E) = E', d'équation de WEIERSTRASS :

$$Y^2 + a'_1XY + a'_3Y = X^3 + a'_2X^2 + a'_4X + a'_6 \in K[X,Y] ;$$

Pour vérifier les formules d'isomorphisme de groupe, il faut calculer l'image de la somme et la somme des images.
L'image du point à l'infini O_E est égale à f((0,1,0)) = (0,1,0) = O_E .
La condition $u \neq 0$ implique que l'image réciproque $f^{-1}(X,Y)$ contient un seul point (x,y).
Les coordonnées d'un point de la Courbe E' isomorphe à E sont :

$$X = \frac{(x - r)}{u^2} \quad \text{et} \quad Y = \frac{(y - su^2X - t)}{u^3}.$$

□

Les relations entre les coefficients et les invariants des Courbes isomorphes E et E' sont déterminées par le :

Corollaire :

Soit 2 Courbes Elliptiques E et E' isomorphes. Alors :

1) Les coefficients a_1 et a'_1 sont liés par les relations :

$$\begin{cases} \mathbf{ua'_1 = a_1 + 2s ;} \\ \mathbf{u^2a'_2 = a_2 - sa_1 + 3r - s^2 ;} \\ \mathbf{u^3a'_3 = a_3 + ra_1 + 2t ;} \\ \mathbf{u^4a'_4 = a_4 - sa_3 - (t + rs)a_1 + 2ra_2 + 3r^2 - 2st ;} \\ \mathbf{u^6a'_6 = a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1 ;} \end{cases} \qquad \textbf{(Is-1)}$$

2) Les relations entre les invariants b_{2i} et b'_{2i} sont :

$$\begin{cases} \mathbf{u^2b'_2 = b_2 + 12r;} \\ \mathbf{u^4b'_4 = b_4 + rb_2 + 6r^2 ;} \\ \mathbf{u^6b'_6 = b_6 + 2rb_4 + r^2 b_2 + 4 r^3 ;} \\ \mathbf{u^8b'_8 = b_8 + 3rb_6 + 3r^2b_4 + r^3b_2 + 3r^4 ;} \end{cases} \qquad \textbf{(Is-2)}$$

3) Les relations entre les invariants c_{2i} et c'_{2i} sont :

$$u^4c'_4 = c_4 \text{ et } u^6c'_6 = c_6 ; \qquad \textbf{(Is-3)}$$

4) La relation entre les discriminants :

$$u^{12}\Delta(E') = \Delta(E) ; \qquad \textbf{(Is-4)}$$

5) La relation entre les invariants modulaires :

$$j(E) = j(E') ; \qquad \textbf{(Is-5)}$$

6) La relation entre les invariants différentiels :

$$u^{-1}\omega(E') = \omega(E); \qquad \textbf{(Is-6)}$$

□

La formule (Is-5) ci-dessus caractérise les Courbes Elliptiques isomorphes.

Proposition 2 :

Deux Courbes Elliptiques E et E' sur un corps K de carac(K) = p ≠ 2, 3, sont isomorphes si et seulement si leurs invariants modulaires sont égaux.

Preuve :

Preuve de « E et E' sont isomorphes » implique « j(E) = j(E') ».

Soit 2 Courbes Elliptiques E et E' isomorphe ; alors les relations (Is-5) impliquent l'égalité :

$$j(E) = j(E').$$

Preuve de « j(E) = j(E') » implique « E et E' sont isomorphes ».

Nous examinons les 3 cas :

$$j(E) = j(E') = 0,1728 \quad \text{et} \quad t \neq 0, 1728.$$

1. Pour j(E) = j(E') = 0, nous prenons 2 équations de WEIERSTRASS de la forme :

$$E : y^2 = x^3 + a_4x + a_6 ; \quad \text{avec} \quad 4a_4^3 + 27a_6^2 \neq 0 ;$$

$$E' : y^2 = x^3 + a'_4x + a'_6 ; \quad \text{avec} \quad 4a_4'^3 + 27a_6'^2 \neq 0;$$

L'invariant modulaire d'une Courbe Elliptique est égal à :

$$j(E)=\frac{4(1728a_4^3)}{4a_4^3+27a_6^2};$$

L'hypothèse d'égalité des invariants j(E) = j(E') implique les relations :

$$a_4 = a'_4 = 0,\ a_6 \neq 0 \quad \text{et} \quad a'_6 \neq 0 ;$$

Par les formules (Is-1) d'isomorphisme, il existe un élément $u \in K_{al}$, tel que :

$$u^6 a'_6 = a_6 ;$$

Cette équation admet, dans une clôture algébrique K_{al}, 6 racines :

$$u = \left(\frac{a_6}{a'_6} \right)^{1/6} ;$$

Il en résulte les isomorphismes :

$$f : E(K) \to E'(K) \ , \quad \text{de valeur: } f(x,y) = (u^2 x , u^3 y)$$

2. Pour j(E) = j(E') = 1728, nous gardons les équations de WEIERSTRASS des Courbes E et E'.
L'hypothèse sur j(E) et j(E') implique les conditions :

$$a_4 \neq 0 \ , \ a'_4 \neq 0 \ \text{ et } a_6 = a'_6 = 0 ;$$

Par les formules (2) d'isomorphisme, il existe un élément $u \in K_{al}$, tel que :

$$u^4 a'_4 = a_4 ;$$

Cette équation admet 4 racines :

$$u = \left(\frac{a_4}{a'_4} \right)^{1/4} ;$$

Il en résulte les isomorphismes :

$$f : E(K) \to E'(K) \ , \quad \text{de valeur: } f(x,y) = (u^2 x , u^3 y);$$

3. Pour j(E) = j(E') = t ≠ 0 , nous gardons les équations de WEIERSTRASS.

La formule de j(E) et l'hypothèse j(E) = j(E') = t, impliquent l'équation :

$$4a_4^3 (1728 - t) = 27 a_6^2 t ,$$

Cette équation admet la solution :

$$a_4 = \frac{3t}{1728 - t} \quad , \quad a_6 = \frac{2t}{1728 - t};$$

L'égalité j(E) = j(E') implique la relation :

$$a_4^3 a_6'^2 = a_4'^3 a_6^2;$$

Par les formules (Is-1) d'isomorphisme, il existe un élément non nul u tel que :

$$u^4 a_4' = a_4 \text{ et } u^6 a_6' = a_6;$$

Nous en déduisons les solutions :

$$u = \left(\frac{a_4}{a_4'}\right)^{1/4} = \left(\frac{a_6}{a_6'}\right)^{1/6};$$

Il en résulte les isomorphismes :

$$f : E(K) \to E'(K) \quad , \quad \text{de valeur: } f(x,y) = (u^2 x, u^3 y);$$

Alors la Courbe Elliptique E a pour équation de WEIERSTRASS :

$$y^2 = x^3 + \frac{3tx}{1728 - t} + \frac{2t}{1728 - t};$$

□

Lorsque carac(K) = 2 ou 3, les formules des invariants des Courbes Elliptiques sont modifiées.

Exemple :

Soit une Courbe Elliptique E_1 d'équation de WEIERSTRASS :

$$E_1: y^2 + 4xy + 6y = x^3 + 3x^2 - 12x - 15 \in \mathbb{Q}[x,y]$$

Avec le calcul j'obtiens les valeurs :

$b_2 = 28$, $b_4 = 0$, $b_6 = -24$, $b_8 = -168$, $\Delta(E_1) = 2^6.3.5.11^2 > 0$, $c_4 = 28^2$

L'invariant modulaire $j(E_1) = 14^6/15 .121$

La relation $\Delta(E_1) > 0$ implique: la cubique E est une Courbe Elliptique qui coupe l'axe Ox ou une paralléle à l'axe Ox en 3 points simples .

Courbe Elliptique isomorphe E_2 obtenue par le changement de variables :

$$\begin{cases} x = 4X - 1 \qquad y = 8Y - 8X + 3 \\ u = 2 \; ; \; r = -1 \; ; \; s = -2 \; ; \; t = 3. \end{cases}$$

$E_2 : Y^2 + Y = X^3 + X^2 - (11/16)\,X - 1/4$

Les formules d'isomorphismes liant les invariants b_{2i} et les discriminants impliquent :

$b'_2 = 4$, $b'_4 = -11/8$, $b'_6 = 0$, $b'_8 = -121/256$, $\Delta(E_2) = 2^{-6}.3\,.5.11^2 = 2^{-12}\Delta(E_1)$.

$c_4 = 49$, $j(E_2) = 14^{\,6}/15\,.121 = j(E_1)$

La Courbe Elliptique E_1 coupe l'axe Ox en 3 points simples d'abscisses x_i , i = 1,2,3 obtenue avec le logiciel Maple : x_1 = -1, 0667 , x_2= -4,8392 , x_3= 2,9059

La Courbe Elliptique E_2 coupe l'axe Ox en 3 points simples d'abscisses x_i , i = 1,2,3 obtenue avec le logiciel Maple : x_1= -1, 36886, x_2= 0,64987, x_3= -0,281039

La Courbe Elliptique E_1 tracée avec le logiciel « Maple »:

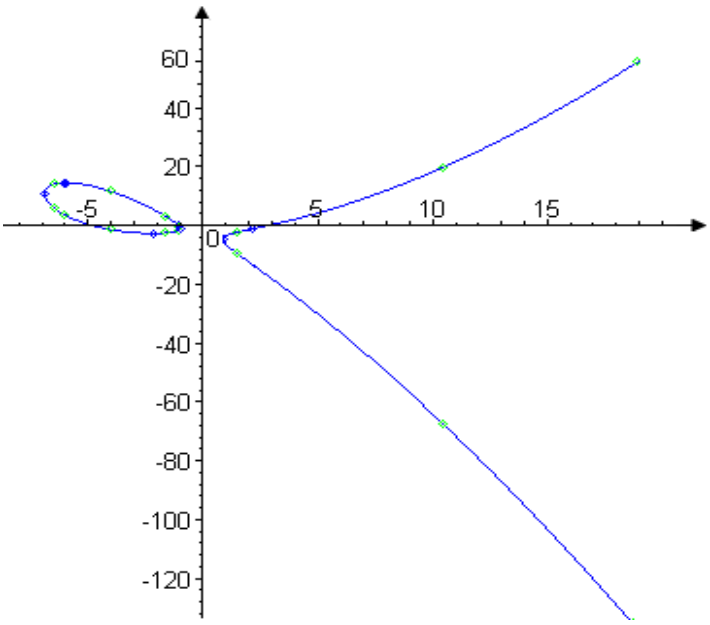


Figure.1

2- Endomorphismes des Courbes Elliptiques :

Définition 3:

Les endomorphismes des Courbes Elliptiques E/K sont des homomorphismes de leurs groupes E(K) sur E(K) :

$$f : E(K) \longrightarrow E(K) .$$

Les ensembles End (E(K)) sont des anneaux que DEURING a caractérisé par la

Proposition3 :

Les anneaux End (E(K)) des endomorphismes des Courbes Elliptiques E/K sont isomorphes à l'anneau $\mathbb{Z}$, ou à l'ordre d'un corps quadratique imaginaire, ou à un ordre de l'algèbre des quaternions.

Preuve : [12]. Corollary 9-4.

□

Définition 4 :

1) **Un ordre d'un corps quadratique imaginaire K = Q($\sqrt{-d}$) est un anneau O(f) = $\mathbb{Z}$ + f A(K), A(K) = anneau des entiers de K et f = conducteur de l'ordre, f entier naturel sans facteur carré.**
2) **l'algèbre des quaternions est la Q- algèbre :**

$$H = \mathbb{Q} + \mathbb{Q}(\alpha) + \mathbb{Q}(\beta) + \mathbb{Q}(\alpha\beta)$$

qui satisfait les conditions :

$$\alpha^2, \beta^2 \in \mathbb{Q}, \quad \alpha^2 < 0, \beta^2 < 0 \text{ et } \alpha\beta = -\beta\alpha .$$

ses éléments sont les quaternions.

$$x = r_1 + r_2\alpha + r_3\beta + r_4\alpha\beta \in H , \ r_i = \mathbb{Q} .$$

3) **les Courbes Elliptiques isomorphes à un ordre d'un corps quadratique imaginaire $\mathbb{Q}$($\sqrt{-d}$) sont des Courbes à Multiplication complexe par ce corps.**

3- Automorphismes des Courbes Elliptiques :

Indiquons quelques éléments de la théorie des automorphismes des Courbes Elliptiques.

Définition5 :

Un automorphisme d'une Courbe Elliptique est un endomorphisme bijectif du groupe abélien E (K).

L'ordre du groupe des automorphismes d'une Courbe Elliptique E est un diviseur de 24, comme le montre la :

Proposition4 :

Soit une Courbe Elliptique E sur un corps K, d'invariant modulaire j(E). Alors, le groupe Aut(E) de ses automorphismes est d'ordre :

1) 2 si j(E) ≠ 0, 1728 et carac(K) ≠ 2 et 3.
2) 4 si j(E) = 1728 et carac(K) ≠ 2 et 3.
3) 6 si j(E) = 0 et carac(K) ≠ 2 et 3.
4)12 si j(E) = 0, 1728 et carac(K) = 3.
5) 24 si j(E) = 0, 1728 et carac(K) = 2.
Où carac(K) est la caractéristique du corps K.

Preuve :cf [12], [16].

□

CHAPITRE III : ISOGENIES DES COURBES ELLIPTIQUES.

1- Eléments de la théorie :

Les isogénies des Courbes Elliptiques sont traitées par des spécialistes [1], [11], [13], [16].Elles sont des sujets de recherche par de nombreux chercheurs [2], [3], [5], [9], [10].

Définition 1 : **[12].**

Soient 2 Courbes Elliptiques E/K et E'/K sur un corps commutatif K; une isogénie de E sur E' est un homomorphisme de leurs groupes de MORDELL – WEIL

$$\lambda : E(K) \longrightarrow E'(K)$$

qui satisfait les conditions :

1) **λ n'est pas l'homomorphisme nul ;**
2) **le noyau de λ est un sous groupe d'ordre fini de E(K) ;**
3) **λ est un homomorphisme surjectif ;**
4) **$\lambda(O_E) = O_{E'}$ pour les points à l'infini O_E de E et $O_{E'}$ de E' ;**
5) **$\lambda(P+R) = \lambda(P) + \lambda(R)$ pour touts points P et R de E.**

L'homomorphisme nul est l'homomorphisme

$f : A \longrightarrow B$ de valeur $f(a) = O_{E'}$.

Le noyau de λ est l'image réciproque du point $O_{E'} = (\infty,\infty)$.

En anglais noyau = kernel ; donc

$$\ker \lambda = \{P \in E(K) ; \lambda(P) = O_{E'}\}.$$

Un homomorphisme $f : A \longrightarrow B$ est surjectif si l'équation $f(a) = b$ admet une solution a au moins pour tout élément $b \in B$.

Les 2 Courbes Elliptiques E et E' sont isogénes par l'isogénie

$$\lambda : E(K) \longrightarrow E'(K) .$$

Les isogénies sont caractérisées par un invariant.

Définition2 :

Le degré d'une isogénie λ est égal à l'ordre de son noyau.

Exemple :

Une isogénie $\lambda : E(K) \longrightarrow E'(K)$ de degré 6 admet un noyau F, sous groupe de E(K) d'ordre 6 :

$$F = \{P, 2P, 3P, 4P, 5P, 6P = O_E\}$$
$$= \{P, 2P, 3P, -P, -2P, O_E\}.$$

Exemple 4-5 dans [12]:

Soient 2 Courbes Elliptiques E/ $\mathbb{Q}$ et E'/ $\mathbb{Q}$.

$E : y^2 = x^3 + a x^2 + b x \in \mathbb{Q}[x,y]$;

$E' : y^2 = x^3 - 2a x^2 + (a^2 - 4b)x \in \mathbb{Q}[x,y]$;

Vérifions que E et E' sont des Courbes Elliptiques en calculant leurs discriminants.
Nous trouvons

$\Delta(E) = 16\, b^2 (a^2 - b) \neq 0$ pour $b \neq 0$ et $a^2 - b \neq 0$.

$\Delta(E') = 512\, b (a^2 - 4b)(a - 2b) \neq 0$ pour $a \neq 2b$, $b \neq 0$ et $a^2 - 4b \neq 0$.

.

Soit les 2 homomorphismes

$$\lambda : E(K) \longrightarrow E'(K) \text{ de valeur } \lambda(x, y) = \left(\frac{y^2}{x^2} , \frac{y(b - x^2)}{x^2} \right).$$

$$\lambda' : E'(K) \longrightarrow E(K) \text{ de valeur } \lambda'(x, y) = \left(\frac{y^2}{4x^2} , \frac{y(a^2 - 4b - x^2)}{8x^2} \right).$$

Le noyau de λ est le sous groupe F de $E(\mathbb{Q})$ égal à :

$$F = \ker(\lambda) = \{ P \in E(\mathbb{Q}) ; \lambda(P) = O_E \}.$$

Le point P = (0, 0) de E satisfait $2P = (\infty, \infty) = O_E$.
Donc λ est une isogénie de degré 2.
Le point P' = (0, 0) de E' satisfait $2P' = (\infty, \infty) = O_{E'}$.
Donc λ' est une isogénie de degré 2.
Il en résulte que leurs composées.

$$\lambda \circ \lambda' : E' \longrightarrow E' \quad \text{et} \quad \lambda' \circ \lambda : E \longrightarrow E.$$

sont des isogénies de degré 2.
Ces exemples impliquent une méthode de détermination des isogénies des Courbes Elliptiques.

Proposition1 :
Soit une Courbe Elliptique E/K sur un corps commutatif K. A chaque sous groupe fini F du groupe E(K) de MORDELL-WEIL de E il correspond une isogénie

$$\lambda : E(K)/F \longrightarrow E(K)$$

de noyau F.

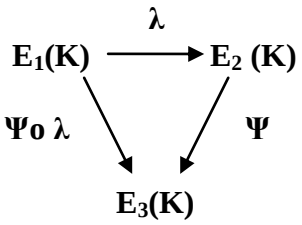
Preuve :
Le groupe quotient E(K)/F est additif abélien; le sous groupe F est dans la classe neutre .
Alors $\lambda(cl(F)) = O_E$ et $\lambda(P+R) = \lambda(P) + \lambda(R)$ pour tous points P et R tels que $cl(P) \neq F$ et $cl(R) \neq F$.
□

Proposition2 :

Soient 2 isogénies de Courbes Elliptiques

$\lambda : E_1(K) \longrightarrow E_2(K)$ et $\Psi : E_2(K) \longrightarrow E_3(K)$.

Alors la composée Ψ o $\lambda : E_1(K) \longrightarrow E_3(K)$ est une isogénie



Preuve :

Pour les points à l'infini des 3 Courbes Elliptiques.

$\Psi(O_{E_1}) = O_{E_2}$ et $f(O_{E_2}) = O_{E_3}$

Pour tous points P et R de E_1

$$\Psi\lambda\,(P+R) = \Psi(\lambda(P) + \lambda(R)) = \Psi(\lambda(P)) + \Psi(\lambda(R))$$

□

Proposition3 :

Soient 2 isogénies de Courbes Elliptiques

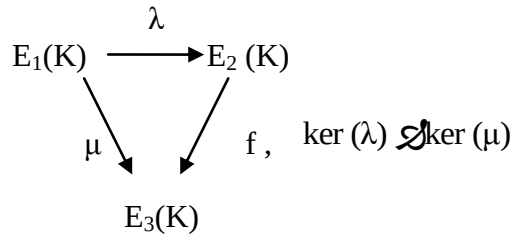
$\lambda : E_1(K) \longrightarrow E_2(K)$ et $\mu : E_1(K) \longrightarrow E_3(K)$.

Si $\ker(\lambda) \subset \ker(\mu)$ alors il existe une isogénie unique

$f : E_2(K) \longrightarrow E_3(K)$.

Preuve :

Soient 2 isogénies λ et μ et le diagramme commutatif.



Relations entre les points à l'infini

$f(O_{E_1}) = O_{E_2}$ et $\mu(O_{E_1}) = O_{E_3}$ Cela implique $f(O_{E_2}) = O_{E_3}$

Les formules d'homomorphismes

$$\lambda(P_1 + R_1) = \lambda(P_1) + \lambda(R_1)$$

$$\mu(S_1 + T_1) = \mu(S_1) + \mu(T_1)$$

et l'inclusion des noyaux ker(λ) ⊂ ker (μ) impliquent les homomorphismes

$$E_1(K)/\ker(\lambda) \longrightarrow E_2(K)$$

$$E_1(K)/\ker(\mu) \longrightarrow E_3(K)$$

et $E_1(K)/\ker(\lambda) \longrightarrow E_2(K) \longrightarrow E_3(K)$

soit $f : E_2(K) \longrightarrow E_3(K)$.

□

2-Multiplication par des entiers rationnels :

Ce sont des isogénies particulières de Courbes Elliptiques.

Pour tout entier rationnel $m \in \mathbb{Z}$, $m \neq 0$, le symbole mP, $P \in E(\mathbb{Q})$ représente les points

$m P = P + P + \ldots + P$, m fois P si $m > 0$,

$m P = (-P) + (-P) + \ldots + (-P)$, (-m) fois -P si $m < 0$,

$0P = O_E$ si $m = 0$.

Considérons l'endomorphisme de groupe

$$t_m : E(\mathbb{Q}) \longrightarrow E(\mathbb{Q})$$

de valeur $t_m(P) = m P$.

Proposition 4 :

Les multiplications t_m sur les Courbes Elliptiques E/◎sont des isogénies de degré m^2 pour $m \neq 0$.

Preuve :

Vérifions les propriétés des isogénies des Courbes Elliptiques,

l'hypothèse $m \neq 0$ implique :

$t_m(P) \neq O_E$, donc t_m n'est pas l'homomorphisme nul.

$t_m(O_E) = mO_E = O_E$:

$t_m(P+R) = m(P+R) = mP + mR$

$t_m(P) + t_m(R)$

Pour tous points P et R du groupe de MORDELL-WEIL $E(\mathbb{Q})$.

Le noyau de t_m est le sous groupe F de $E(\mathbb{Q})$ égal à :

$$F = \{P \in E(\mathbb{Q}) , mP = O_E \}$$

F est donc le sous groupe de m- torsion E[m] de E

Cette multiplication t_m est donc un endomorphisme surjectif du groupe $E(\mathbb{Q})$.

Avec un argument d'endomorphisme " dual ", on obtient le résultat :

ordre de $F = m^2$ = degré de la multiplication $t_m : E(K) \longrightarrow E(K)$

□

CHAPITRE III : ISOGENIES DES COURBES ELLIPTIQUES.

A chaque isogénie $\lambda : E_1(K) \longrightarrow E_2(K)$ est associée une isogénie duale.

Définition5 :

Soit une isogénie $\varphi : E_1(K) \to E_2(K)$ de degré d, l'isogénie duale de l'isogénie φ est l'homomorphisme surjectif: $\hat{\varphi} : E_2(K) \to E_1(K)$ tel que les 2 composées $\varphi \circ \hat{\varphi}$ et $\hat{\varphi} \circ \varphi$ soient des multiplications par d.

Indiquons quelques algorithmes de calculs : [2], [10]

3-Algorithme de B. MAZUR [10]

MAZUR s'est intéressé aux isogénies de degré premier N des Courbes Elliptiques E/ $\mathbb{Q}$.

Ce sont donc des N- isogénies cycliques.

Celles qui sont connues des spécialistes ont pour valeurs

N = 11, 17, 19, 37, 163 premiers
N = 14, 15, 21, pour N composé.

Les noyaux des isogénies des Courbes Elliptiques sont des sous groupes de torsion des groupes E($\mathbb{Q}$). MAZUR a prouvé la

Proposition5 :

Soit T(E) les groupes de torsion de MORDELL-WEIL E($\mathbb{Q}$) des Courbes Elliptiques E/$\mathbb{Q}$. Alors T(E) est isomorphe à l'un des 15 groupes additifs abéliens finis:

$\mathbb{Z}/m\mathbb{Z}$ pour $1 \leq m \leq 10$ ou $m = 12$.

$\mathbb{Z}/2d\mathbb{Z} \times \mathbb{Z}/2d\mathbb{Z}$ pour $1 \leq d \leq 4$.

Preuve [10] théorème 2.

La détermination des isogénies est liée aux courbes modulaires $X_0(N)$ dont la théorie est décrite dans "Modular Curve and the Eisenstein idéal"(Publi. Math. I.H.E.S. 47(1977)).

L'algorithme repose sur les réductions des Courbes Elliptiques et les caractères des groupes de Galois

$$v : Gal(K_{alg}/K) \longrightarrow (Z/NZ)^*$$

Les Courbes Elliptiques ont une structure de Variétés Abéliennes de dimension 1 et de courbes modulaires $X_0(N)$ de genre g = 1 pour

N = 11, 14, 15, 17, 19, 21 et 27.

Les ordres des points des groupes de torsion T(E)(Q) ont été obtenues par KUBERT.

Des propriétés de ces points sont utilisées pour la preuve.

□

CHAPITRE III : ISOGENIES DES COURBES ELLIPTIQUES.

Ces isogénies sont liées aux nombres des points non paraboliques des courbes modulaires X_0 (N). Ces courbes modulaires sont construites avec des sous groupes Γ du groupe spécial linéaire SL(2, $\mathbb{R}$) opérant sur le demi plan de POINCARE IH = {z $\in$ C , Imz > 0} ; la description des éléments de la théorie (points elliptiques, point paraboliques, …) se trouve dans [12].

4-Technique de VELU [16]:

Soit une Courbe Elliptique E d'équation de WEIERSTRASS :

$$E : y^2 + a_1xy + a_3y = x^3 + a_2 x^2 + a_4x + a_6 \in K[x,y] ; \quad (1)$$

Sur le corps K(E) = K(x,y) des fonctions rationnelles définies sur K , nous associons à tout point $P \neq O_E$,une valuation v_p de valeur :

$$v_p(x) \geq 0 ; \ v_p(y) \geq 0. \quad (2)$$

Au point à l'infini O_E , nous associons la valuation v_0 de valeur :

$$v_0(x) = -2 ; \ v_0(y) = -3 \text{ et } (y^2/ x^3)(0) = 1 \quad (3)$$

Mettons l'équation de E sous la forme :

$$g(x,y) = y^2 + a_1xy + a_3y – x^3 – a_2 x^2 – a_4x – a_6 = 0 ; \quad (4)$$

L'invariant différentiel de E est égal à :

$$w(E) = \frac{dx}{-g'_y} = \frac{dy}{g'_x} ;$$

où les dérivées partielles de la fonction g(x,y) sont égales à :

$$g'_x = 3x^2 + 2a_2 x + a_4 - a_1y \text{ et } g'_y = -(2y + a_1x + a_3). \quad (5)$$

En posant z = -x /y, nous obtenons les développements de x et de y en z :

$$x = z^{-2} - d_1z -1- d_2 – d_3 z – d_4z^2 – d_5z^3 \ldots\ldots\ldots ;$$
$$y = -x/z = – z^{-3} – d_1z^{-2} – d_2z^{-1} + d_3 z + d_4z + d_5z^2 + \ldots \quad (6)$$

les relations entre les coefficients d_i et a_i sont :

$d_1 = a_1$; $d_2 = a_2$; $d_3 = a_3$;

$d_4 = a_4 + a_1a_3$; $d_5 = a_1a_4 + a_2a_3 + a_1^2a_3$;

$d_6 = a_6 + a_1^2a_4 + a_1^3a_3 + a_2a_4 + 2a_1a_2a_3;\ldots\ldots$ (7)

L'invariant différentiel de E est une fonction de z :

$$w(E) = dz \{1 + a_1z + (a_1^2 + a_4)z^2 + (a_1^3 + 2a_1a_2 + a_3) + \ldots\} \quad (8)$$

Soit un point (X, Y) de la courbe isogéne à E.
A chaque point P = (x,y) de E , nous associons le point (X, Y) par les relations :

$$X = x + \sum_{T \neq F-O_E} (x(P+T) - x(T)) ;$$

$$Y = y + \sum_{T \neq F-O_E} (y(P+T) - y(T)) ;$$

Nous obtenons les développements de X et Y en z :

$$X = = z^{-2} - a_1 z - a_2 - a_3 z - \ldots . ;$$
$$Y = - z^{-3} + a_1 z^{-2} + a_2 z^{-1} + \ldots . \quad (10)$$

La formule Z=-X/Y implique le développement de Z en série :

$$Z = z + 2tz^3 + 3a_1 tz^6 + \ldots . \quad (11)$$

Nous en déduisons une relation entre X et Y indépendante de z :

$$Y^2 + A_1 XY + A_3 Y = X^3 + A_2 X^2 + A_4 X + A_6; \quad (12)$$

avec $A_1 = a_1$; $A_2 = a_2$; $A_3 = a_3$;
$A_4 = a_4 - 5t$; et $A_6 = a_6 - b_2 - 7w$; t et w de la formule (14) ci-dessous et b_2 se trouve dans l'équation de E :

$$y^2 = 4x^3 + b_2 x^2 + 2b_4 x + b_6 \qquad \text{avec } b_2 = a_1^2 + 4a_2 .$$

Algorithme de calcul des isogénies des Courbes Elliptiques E/©

1) Soit une Courbe Elliptique E d'équation de WEIERSTRASS (1) :
2) Choix d'un sous groupe fini F du groupe E(K).
3) Prendre $F_2 = \{ P \in F$, d'ordre 2 $\}$.
4) l'ensemble R des points de $F - F_2 - \{O_E\}$, et $-R = \{ -P ; P \in R \}$, tel que :
$F - F_2 - \{O_E\} = R \cup -R$ et $R \cap -R = \{\emptyset\}$.

5) Prendre la partie $S = F_2 \cup R$.

6) Calculer les dérivées partielles g'_x et g'_y avec la formule (4).

7) L'application $\lambda : E \to E / F = E'$; $(x, y) \to (X, Y)$ d'équation:

$$\begin{cases} X = x + \sum_{p \in S} \left[\dfrac{t_P}{x - x_P} + \dfrac{u_P}{(x - x_p)^2} \right] \\ Y = y - \sum_{P \in S} \left[u_P \dfrac{2y + a_1 x + a_3}{(x - x_p)^3} + t_P \dfrac{a_1 (x - x_p) + y - y_P}{(x - x_p)^2} + \dfrac{a_1 u_P - g_P^x g_P^y}{(x - x_p)^2} \right] \end{cases} \quad (13)$$

est une isogénie de Courbes Elliptiques.

8) Calculer les nombres :

$g_x^{'}(P)$; $g_y^{'}(P)$; $t_P = g_x^{'}(P)$ si $P \in F_2$; $t_P = 6x_P^2 + b_2 x_P + b_4$ si $P \notin F_2$.

$u_P = 4x_P^3 + b_2 x_P^2 + 2b_4 x_P + b_6$; $b_2 = 4a_2 + a_1^2$; $b_4 = a_1 a_3 + 2a_4$ et $b_6 = a_3^2 + 4a_6$.

$$t = \sum_{P \in S} t_P \; ; \; \omega = \sum_{P \in S} (u_P + x_P t_P). \tag{14}$$

9) L'équation de WEIERSTRASS de la Courbe isogène E' = E / F est

$$E' = E / F : Y^2 + a_1 XY + a_3 Y = X^3 + a_2 X^2 + (a_4 - 5t)X + a_6 - b_2 t - 7\omega ;$$

Exemple 1 :
Application de l'algorithme à la Courbe Elliptique E_1 d'équation de WEIERSTRASS :

$$E_1 : y^2 = x^3 + 5 ; \tag{1}$$

Le calcul implique les invariants

$$\Delta(E_1) = -10800 = -2^4 \times 3^3 \times 5^2 \text{ et } j(E_1) = 0. \tag{2}$$

Le groupe $E_1(K)$ a un sous groupe F d'ordre 3, formé des points :

$$F = \left\{ P = (0, \sqrt{5}), 2P = (0, -\sqrt{5}), 3P = O_E = (\infty, \infty) \right\}; \tag{3}$$

En utilisant la méthode de VELU, nous obtenons les ensembles :

$$F_2 = \{ O_E \} \quad , \quad R = \{P\} = S. \tag{4}$$

Avec le calcul nous obtenons les coordonnées du point (X , Y) :

$$(x,y) \rightarrow \left[X = x + \frac{20}{x^2}, Y = y - \frac{40y}{x^3} \right], \tag{5}$$

Avec le calcul nous obtenons les nombres de l'étape (8)

$$t = 0 \; , \; \omega = 20 ; \tag{6}$$

Nous en déduisons l'équation de WEIERSTRASS de la Courbe Elliptique isogène E_2 :

$$E_2 = E_1 / F : Y^2 = X^3 - 135. \tag{7}$$

Le calcul implique les invariants :

$$\Delta(E_2) = -7873200 = -2^4 \times 3^9 \times 5^2 \quad \text{et} \quad j(E_2) = 0. \tag{8}$$

La proposition 2 et la relation $j(E_1) = j(E_2) = 0$ impliquent que les Courbes isogènes E_1 et E_2 sont isomorphes.

Exemple 2 : [16]

Soit la Courbe Elliptique d'équation de WEIERSTRASS :

$$E : y^2 + xy + y = x^3 - x^2 - 3x + 3 \in \mathbb{Q}[x,y] ; \tag{1}$$

Le calcul implique les invariants :

$$b_2 = -3 , b_4 = -5 , b_6 = 13 ; b_8 = -16 ; \Delta(E) = -1664 \tag{2}$$

Le groupe $E(\mathbb{Q})$ a un sous groupe cyclique F d'ordre 7 formé des points :

$P = (1,0), 2P = (-1,-2), 3P = (3,-6), 4P = (3,2), 5P = (-1,2), 6P = (1,-2)$ et $7P = O_E$;
La relation $7P = O_E$ implique $P = -6P , 2P = -5P , 3P = -4P$;
Il en résulte les 3 parties :

$$F_2 = \{\emptyset\} , R = \{ P, 2P , 3P \} \quad \text{et} \quad S = \{ P , 2P ,3P \} \tag{3}$$

Avec le calcul nous obtenons les nombres $t = 42 , \omega = 198$ (4)
Il en résulte l'équation de WEIERSTRASS de la Courbe Elliptique isogène :

$$E' = E / F : Y^2 + XY + Y = X^3 - X^2 - 213X - 1257 \in \mathbb{Q}[x,y] ;. \tag{5}$$

$$\Delta(E') = -165544$$

Exemple 3 :
Soient deux Courbes Elliptiques sur un corps K de caractéristique $\neq 2$;

$$E_1 : y^2 = x^3 + ax^2 + bx \text{ ; avec } 4a^3 + 27b^2 \neq 0 \tag{1}$$

$$E_2 : Y^2 = X^3 - 2aX^2 + (a^2 - 4b)X ; b \neq 0 \text{ et } a^2 - 4b \neq 0. \tag{2}$$

Alors les deux applications f , g

$$f : E_1 \to E_2 \qquad (3)$$

$$(x,y) \to \left(\frac{y^2}{x^2}, \frac{y(b - x^2)}{x^2} \right)$$

$$g : E_2 \to E_1$$

$$(X,Y) \to \left(\frac{Y^2}{4X^2}, \frac{Y(a^2 - 4b - X^2}{8X^2} \right) \qquad (4)$$

sont des isogénies.

Les changements de variables sont des fonctions rationnelles. Les 2 applications ont des composées:

La composée $f \circ g : E_2 \to E_2$ est la multiplication par 2 sur $E_2(\mathbb{Q})$, c'est une isogénie de degré 4. (5)

La composée $g \circ f : E_1 \to E_1$ est la multiplication par 2 sur $E_1(\mathbb{Q})$, c'est une isogénie de degré 4. (6)

Les relations (5) et (6) impliquent que g est l'isogénie duale de l'isogénie *f*.

Le calcul implique les invariants de la Courbe Elliptique E_1 :

$$\Delta(E_1) = 16\, b^2 (a^2 - 4b),\ c_4(E_1) = 16(a^2 - 3b) \text{ et } j(E_1) = \frac{16^2 (a^2 - 3b)^3}{b^2 (a^2 - 4b)}; \qquad (7)$$

Les invariants de la Courbe Elliptique E_2 sont égaux à :

$$\Delta(E_2) = 64 \text{ x } 4b(a^2 - 4b)^2,\ c_4(E_2) = 16a^2 + 192b \text{ et } j(E_2) = \frac{(16a^2 + 192b)^3}{64 \text{ x } 4b(a^2 - 4b)^2}; \qquad (8)$$

Application pour a = 5, b = -8.

$$E_1 : y^2 = x^3 + 5x^2 - 8x \ ; \qquad (1)$$

$$E_2 : Y^2 = X^3 - 10X^2 + 57X \ ; \qquad (2)$$

Les isogénies de degré 2 sont les 2 homomorphismes :

$$f : E_1 \to E_2$$
$$(x,y) \to \left(\frac{y^2}{x^2}, \frac{y(-8-x^2)}{x^2} \right) \quad (3)$$

$$g : E_2 \to E_1$$
$$(X,Y) \to \left(\frac{Y^2}{4X^2}, \frac{Y(57-X^2)}{8X^2} \right) \quad (4)$$

Le calcul implique les invariants de la Courbe Elliptique E_1 :

$$\Delta(E_1) = 2^{10} \text{ x } 57,\ c_4(E_1) = 2^4 \text{ x } 7^2 \text{ et } j(E_1) = \frac{2^2 \text{ x } 7^6}{57}; \quad (5)$$

Les invariants de la Courbe Elliptique E_2 sont égaux à :

$$\Delta(E_2) = 2^{11} \text{ x } 3^2 \text{ x } 361,\ c_4(E_2) = -2^4 \text{ x } 71 \text{ et } j(E_2) = \frac{-2 \text{ x } (71)^3}{3^2 \text{ x } 361}; \quad (6)$$

Examinons le cas de Courbes Elliptiques E/$\mathbb{Q}$ ayant bonne réduction en dehors de 11 d'après [15-1]
Ces courbes sont deux à deux non isomorphes.

Courbes de conducteur N(E) = 11

Il y en a 3

Courbe Elliptique A :

$$A: y^2 + y = x^3 - x^2 \in \mathbb{Q}[x,y];$$

Valeurs des invariants :

$$\Delta(A) = -11 \ ; c_4 = 2^{11} \ ; \ c_6 = -2^3.19 \ ; \ j(A) = -2^{12}11^{-1}$$

Courbe Elliptique B :

$$B: y^2 + y = x^3 - x^2 - 10x - 20 \in \mathbb{Q}[x,y];$$

Valeurs des invariants :

$$\Delta(B) = -11^5 \ ; c_4 = 2^4.31 \ ; \ c_6 = -2^3.41.61 \ ; \ j(B) = -2^{12}.31^3.11^{-5}$$

Courbe Elliptique C :

$$C: y^2 + y = x^3 - x^2 - 7820x - 263\,580 \in \mathbb{Q}[x,y];$$

Valeurs des invariants :

$$\Delta(C) = -11 \ ; c_4 = 2^4.29.809 \ ; \ c_6 = 2^3.61.471\,281 \ ; \ j(C) = -2^{12}.29^{-3}.809^{-3}.11^{-1}$$

Ce sont des Courbes Elliptiques formées d'une seule branche.

Courbes de conducteur N(E) = 11^2

Il y en a 9

Courbe Elliptique D :

$$D : y^2 + y = x^3 - x^2 - 7x + 10 \in \mathbb{Q}[x,y];$$

Valeurs des invariants :

$$\Delta(D) = -11^3 \ ; c_4 = 2^5.11 \ ; \ c_6 = -2^3.7.11^2 \ ; \ j(D) = -2^{15}.$$

CHAPITRE III : ISOGENIES DES COURBES ELLIPTIQUES.

Courbe Elliptique D' :

$$D' : y^2 + y = x^3 - x^2 - 887x - 10143 \in \mathbb{Q}[x,y] ;$$

Valeurs des invariants :

$$\Delta(D') = -11^9 \; ; c_4 = 2^5.11^3 \; ; \quad c_6 = 2^3.7.11^2 \; ; \quad j(D') = -2^{15}.$$

Courbe Elliptique E :

$$E : y^2 + xy = x^3 + x^2 - 2x - 7 \in \mathbb{Q}[x,y] ;$$

Valeurs des invariants :

$$\Delta(E) = -11^4 \; ; c_4 = 11^2 \; ; \quad c_6 = 11^2.43 \; ; \quad j(E) = -11^2.$$

Courbe Elliptique F :

$$F : y^2 + xy = x^3 + x^2 - 3632x + 82757 \in \mathbb{Q}[x,y] ;$$

Valeurs des invariants :

$$\Delta(F) = -11^8 \; ; c_4 = 11^3.131 \; ; \quad c_6 = -11^4.4973 \; ; \quad j(F) = -11.131^3.$$

Courbe Elliptique E' :

$$E' : y^2 + xy + y = x^3 + x^2 - 305x + 7888 \in \mathbb{Q}[x,y] ;$$

Valeurs des invariants :

$$\Delta(E') = -11^{10} \; ; c_4 = 11^4 \; ; \quad c_6 = -11^5.43 \; ; \quad j(E') = -11^2.$$

Courbe Elliptique F' :

$$F' : y^2 + xy + y = x^3 + x^2 - 30x - 76 \in \mathbb{Q}[x,y] ;$$

Valeurs des invariants :

$$\Delta(F') = -11^2 \; ; c_4 = 11.131 ; \quad c_6 = -11.4973 \; ; \quad j(F') = -11.131^3.$$

Courbe Elliptique A' :

$$A' : y^2 + y = x^3 - x^2 - 40x - 221 \in \mathbb{Q}[x,y] ;$$

Valeurs des invariants :

$$\Delta(A') = -11^7 \; ; c_4 = 2^4.11^2 ; \quad c_6 = 2^3.11^3.19 \; ; \quad j(A') = -2^{12}.11^{-1}.$$

Courbe Elliptique B' :

$$B' : y^2 + y = x^3 - x^2 - 40x - 221 \in \mathbb{Q}[x,y] ;$$

Valeurs des invariants :

$$\Delta(B') = -11^{11} \; ; c_4 = 2^4.11^2.31 \; ; \quad c_6 = -2^3.11^3.41.61 \; ; \quad j(B') = -2^{12}.31^3.11^{-1}.$$

Courbe Elliptique C' :

$$C' : y^2 + y = x^3 - x^2 - 946260x + 354\,609\,639 \in \mathbb{Q}[x,y] ;$$

Valeurs des invariants :

$$\Delta(C') = -11^7 \; ; c_4 = 2^4.11^2.29.809 \; ; c_6 = -2^3.11^3.61.471\,281 \; ;$$
$$j(C') = -2^{12}.29^3.809^3.11^{-1}.$$

Ce sont des Courbes Elliptiques formées d'une seule branche.

1°- Equations des isogénies :

1-Une isogénie f : A ⟶ B est déterminée par les coordonnée des points de B.

$X = x + x^{-2} + 2(x-1)^{-1} + (x-1)^{-2}$
$Y = y-(2y+1)\,x^{-3} - yx^{-2} - (2y+1)(x-1)^{-3} - y(x-1)^{-2} - (x-1)^{-2}$

Le groupe de MORDELL-WEIL $A(\mathbb{Q})$ a un sous groupe cyclique d'ordre 5 formé des points :

$$P = (0,0)\ ,\ 2P = (1,-1)\ ,\ 3P = (1,0)\ ,\ 4P = (0,-1)\ ,\ 5P = (\infty,\infty).$$

2-Une isogénie $g : B \longrightarrow C$ est déterminée par les coordonnée des points de C.

$X = x + 2.5.11(x-5)^{-1} + 11^2 (x-5)^{-2} + 2^2.3.11^2(x-16)^{-1} + 11^4(x-16)^{-2}$
$Y = y - 11^2(2y+1)(x-5)^{-3} - 2.5.11y(x-5)^{-2} - 5.11(x-5)^{-2} - 11^4(2y+1)(x-16)^{-3} - 2.3.11^2(x-16)^{-2}$

Le groupe de MORDELL-WEIL $B(\mathbb{Q})$ a un sous groupe cyclique d'ordre 5 formé des points :

$P = (5,5)\ ,\ 2P = (16,-61)\ ,\ 3P = (16,60)\ ,\ 4P = (5,-6)\ ,\ 5P = (\infty,\infty).$

La théorie de TATE montre que la seule courbe isogène à A (resp. C) par une isogénie de degré 5 est B et que les seules courbes isogènes à B par une isogénie de degré 5 sont A et C.

2°- Les courbes A', B', C' deviennent isomorphes à A, B, C après extension du corps de base à $\mathbb{Q}(\sqrt{11})$ par conséquent, ells sont liées par des isogénies de degré 5 et à isomorphisme prés il n'y a pas d'autre courbe qui leur soit isogène.

3°- Les courbes ayant un sous-groupe rationnel d'ordre 11 sont celles pour lesquelles :

$j = -2^{15}$; $j = -11^2$; $j = -11.131^3$

Ces deux dernières valeurs s'échangent par isogénie. D'autre part, il n'existe pas d'autre courbe que D et D'(resp E et E', F et F') ayant pour invariant $j = -2^{15}$; (resp $j = -11^2$; resp $j = -11.131^3$) et bonne réduction en dehors de {11}.

Les courbes d'invariant modulaire $j = -2^{15}$ sont des courbes à Multiplication Complexe par l'anneau des entiers du corps quadratique imaginaire $\mathbb{Q}(\sqrt{11})$

Après ma thèse de magister, je compte étudier les Courbes Elliptiques sur les corps finis et leurs applications à la cryptographie et au codage.

.. REFERENCES

🕮 **[1] CASSELS – J-W-S:**
« Diophantine Equations with Special Reference to Elliptic Curves »
Journal London Mathematical Society 41 (1966) 193-291.

🕮 **[2]COUVEIGNES Jean Marc:**
1) « quelques calculs en Theorie des Nombres » ,
Thèse à l'Université de Bordeaux 1 (juillet 1994).
2) « Computing l- isogenies with p- torsion »,
Proc.ANTS-II-(janv 1996) p 1-7.

🕮 **[3] COUVEIGNES J M et MORAIN François :**
« Schoof's algorithm and isogenies cycles »(par internet), p 1-16 .

🕮 **[4] HARTSHORNE - Robin:**
« Algebraic Geometry », GTM 52-Springer (1983).
Graduate texte in Mathematics n° 52 (1980)

🕮 **[5] S. LANG :**
« Elliptic Curves. Diophantine analyses » S. Verlag-1978 .

🕮 **[6] LERCIER Reynald :**
« Algorithmique des Courbes Elliptiques dans les corps finis »
Thèse à l'Ecole Polytechnique de paris (16 juin 1997).

🕮 **[7] LERCIER- R and MORAIN- F :**
« Algorithms for computing isogenies between Elliptic Curves »
par internet (1996) p 1-14.
« Counting the Numbre of Points on Elliptic Curves over Finite Fields: Strategies and Performances » par internet (1995) p 1-10.

🕮 **[8] MASSER- D-W and WÜSTHOLZ- G:**
« Estimating isogenies on Elliptic Curves » Invent .math. 100 (1990) p1.24

🕮 **[9] MASSEY- J-L:**
« Shift- register and BCH decoding. IEEE Trans » on information theory IT- 15, 1 (Jan 1969) p122-127

🕮 **[10] MAZUR Barry:**
« Rational isogenies of prime degre » Invent. Math. 44 (1978), 129-162.

🕮 **[11] MOMOSE Fumiyuki:**
« Isogenies of prime degree over number fields » Compositio Mathematica 97(1995)- 329- 348.

🕮 **[12] SHIMURA Goro:**
«Introduction to the Arithmetic Theory of Automorphic Function », Princeton University Press (1971).

🕮 **[13] SILVERMAN Joseph-H:**
« The Arithmetic of Elliptic Curves », GTM 106 – Springer (1986). Classification AMS = 1401, 14G 99, 14H 05, 14 K 15.

🕮 **[14] TATE John:**
« The Arithmetic of Elliptic Curves », Inv Math 23 (1974) p179-206.

🕮 **[15] UMEGAKI Atsuki:**
« A construction of Everywhere Good Q-Curves with p-Isogeny» Tokyo Jour. Math .vol 21(1998) p-183-200.

🕮 **[16] VELU Jacques:**
1) «Courbes Elliptiques sur Q ayant bonne réduction en dehors de 11 » C.R.A.S. Paris,t,273 (12 juillet 1971)p-73-75.
2) « Isogénies entre Courbes Elliptiques », C.R.A.S. Paris,t,273 (26 juillet 1971).

🕮 **[17] ZITOUNI - Mohamed:**
«Géométrie, Arithmétique et Algorithmique des Courbes Elliptiques» OPU- Alger (2007).