N° d'ordre : 06/2007 – M / MT

RÉPUBLIQUE ALGÉRIENNE DÉMOCRATIQUE ET POPULAIRE
MINISTÈRE D'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE SCIENTIFIQUE
UNIVERSITÉ DES SCIENCES ET DE LA TECHNOLOGIE
HOUARI BOUMEDIENE
FACULTÉ DE MATHÉMATIQUES

MÉMOIRE
Présenté pour l'obtention du diplôme de MAGISTER
EN : MATHÉMATIQUES

Spécialité : ALGÈBRE ET THÉORIE DES NOMBRES

Par : SAHLI Safia

Sujet

COURBES ELLIPTIQUES SUPERSINGULIÈRES

Soutenu le 15/02/2007, devant le jury composé de :

M[r] Méziane AÏder	Professeur à l'USTHB	Président
M[r] Mohamed ZITOUNI	Professeur à l'USTHB	Directeur de thèse
M[r] Mohamed Salah HCHAÏCHI	Professeur à l'USTHB	Examinateur
M[r] Abdelkader KHELLADI	Professeur à l'USTHB	Examinateur
M[r] Mohand Ouamar HERNANE	Professeur à l'USTHB	Examinateur

À la mémoire de mon père
À ma mère, à ma famille du Maroc
À ma famille, à Sanae(Kaboul)
À A.BENAMARA

Remerciements

Je tiens à remercier vivement mon directeur de thèse, le Professeur Mohamed Zitouni qui a dirigé et guidé cette étude ; Sa disponibilité, ses remarques claires et encourageantes m'ont permis de la finaliser.

Toute ma gratitude revient à :

Monsieur : Méziane AÏDER qui me fait l'honneur de présider le jury.

Messieurs : Mohamed Salah HACHAÏCHI
Mohand Ouamar HERNANE
Abdelkader KHELLADI

Qui ont accepté d'examiner mon travail.

Cette thèse n'aurait probablement pas abouti sans le soutien constant de monsieur Abderrahman BENAMARA , en plus de mes remerciements, il a toute ma reconnaissance.

Table des matières

INTRODUCTION

La théorie des courbes elliptiques a des liens avec la Théorie des Nombres, (corps de base), l'Analyse Complexe (fonctions elliptiques), la Géométrie Algébrique, (Variétés, Diviseurs).
Elle admet des applications en codage et en cryptographie [9], [12], [15], [17]

1) la factorisation des nombres entiers utilise les courbes elliptiques sur le corps des nombres rationnels, cette théorie est utilisée par Schoof, Couveignes, Morain,…

2) Le théorème de Fermat relatif à l'équation Diophantienne
$x^n + y^n = z^n$ a été démontré en 1994 par Wiles avec la théorie des Courbes Elliptiques.

3) Tunnel a relié le problème des Nombres Congruents à la Théorie des Courbes Elliptiques.

Le sujet de ma thèse de magister concerne les courbes elliptiques supersingulières ; leur corps de base est un corps fini IF_q à $q = p^n$ éléments, p premier.

Dans le premier chapitre je traite la structure des courbes algébriques planes, dans cet ensemble il y a les cubiques de Weierstrass.[3], [13]
Le second chapitre est consacré à la structure algébrique des corps finis
IF_q à $q = p^n$ éléments pour p premier.[6]
Dans le troisième chapitre je traite le groupe des points rationnels $E(IF_q)$ d'une courbe elliptique E sur un corps fini IF_q, Le théorème de Hasse permet de trouver une borne de $|E(IF_q|$. J'utilise la théorie des groupes formels pour introduire l'invariant de Hasse.

Dans le quatrième chapitre j'utilise l'invariant de Hasse qui classifie l'ensemble des courbes elliptiques sur un corps fini en classe de courbes elliptiques ordinaires et en classe de courbes elliptiques supersingulières. J'utilise trois critères de reconnaissance des courbes elliptiques supersingulières.Ces notions sont décrites dans [3], [7], [13], [14].

CHAPITRE I

COURBES ALGÉBRIQUES PLANES

1- Courbes algébriques planes

2- Cubiques de Weierstrass

3- Invariants des cubiques de Weierstrass

4- Groupe de Mordell-Weil d'une courbe elliptique

5- Points d'ordre fini d'une courbe elliptique

6- Isomorphismes et isogénies de courbes elliptiques

Nous allons considérer la structure de courbe algébrique plane dans un espace K^2, sur un corps K commutatif.

1-Courbes algébriques planes : degré, singularité, genre.

Définition 1: Une *courbe algébrique plane est l'ensemble des points P= (x,y) qui satisfont un polynôme f(x,y) = 0 dans l'anneau K[x,y].*

Un polynôme $f(x,y)=\sum d_{ij}x^i y^j$; i,j ≥0,a un degré égal au maximum

n des sommes i+j.

Exemples :

Pour n = 1, $f(x,y) = d_1x + d_2y + d_3$ est l'équation d'une droite

Pour n = 2, $f(x,y) = d_2x^2 + d_3y^2 + d_4xy + d_5$ est l'équation d'un cercle

$f(x,y) : y^2 = ax + b$ est l'équation d'une parabole

$f(x,y) = \frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$ est l'équation d'une ellipse, $a \neq b \neq 0$

$f(x,y) = \frac{x^2}{a^2} - \frac{y^2}{b^2} = 1$ est l'équation d'une hyperbole $a \neq b \neq 0$

les paraboles, les ellipses et les hyperboles forment la classe des coniques ; géométriquement ce sont des intersections d'un cône par un plan.

$f(x,y) = (d_1x + d_2y + d_3)(d_4x + d_5y + d_6) = 0$ est l'équation du produit de 2 droites.

Pour n = 3, un polynôme irréductible est de la forme $f = f_3 + f_2 + f_1 + f_0 = 0$, f_t est un polynôme homogène de degré t.

Un polynôme dégénéré est soit un produit de 3 droites, soit un produit d'une droite par une courbe irréductible de degré 2.

La propriété d'irréductibilité des polynômes permet de classer les courbes algébriques en classe des courbes irréductibles et en classe des courbes dégénérées.

Une courbe algébrique C de degré n peut admettre des points singuliers.

Définition 2 : Soit C une courbe algébrique plane d'équation $f(x,y) = o$,
un point $S = (x_s,y_s)$ de C est singulier s'il est solution du système:

$$f(x_s,y_s) = f_x(x_s,y_s) = f_y(x_s,y_s) = o$$

Le nombre s de points singuliers d'une courbe algébrique C de degré n permet de définir l'invariant genre de C.

Définition 3 : *le genre d'une courbe algébrique C de degré n, qui possède s points singuliers (comptés avec leur multiplicité), est l'entier positif ou nul :*

$$g(C) = \frac{(n-1)(n-2)}{2} - s \geq 0$$

Les droites, les cercles, les coniques, les cubiques singulières ont un genre égal à zéro :

Exemple :
Soit la courbe algébrique E_1 d'équation :

$$E_1 : f(x,y) = y^2 - x^3,$$

Les dérivées partielles sont égales à :
$f'_x(x,y) = -3x^2$ et $f'_y(x,y) = 2y$; le système $f = f'_x = f'_y = 0$ admet une solution (0,0), il en résulte un point singulier S = (0,0).

Le genre de E_1 est égal à : $g(E_1) = 0$

Les cubiques irréductibles non singulières ont un genre égal à un :

Exemple :
Soit la courbe algébrique E_2 d'équation :

$$E_2 : f(x,y) = y^2 - x^3 - x ;$$

E_2 n'admet pas de point singulier, il en résulte le genre $g(E_2) = 1$.

Dans la suite nous nous intéresserons à des cubiques particulières : **les cubiques de Weierstrass**.

2- Cubiques de Weierstrass :

Les cubiques de Weierstrass sont des courbes algébriques planes.

Définition 4 : *Une cubique de Weierstrass est une courbe algébrique plane C, irréductible, d'équation de Weierstrass :*

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

Les 5 coefficients $a_1,\ldots,a_6$ sont des éléments d'un corps commutatif K, global, local ou fini, les deux variables x et y sont des éléments d'une clôture algébrique K_{alg} de K .

D'après ce qui précède, les cubiques de Weierstrass sont classifiées en deux classes : classe des cubiques singulières de genre égal à zéro et classe des cubiques non singulières de genre égal à un.

Définition 5 : *une courbe elliptique est une cubique de Weierstrass non singulière.*

Pour l'étude des cubiques de Weierstrass, il est utile de diminuer le nombre de coefficients a_i. Pour cela nous utilisons des changements de variables linéaires. L'élimination des monômes en xy et en y dans l'équation (1) s'obtient avec le changement de variables :

$$x = X \text{ et } y = (Y - a_1X - a_3)/2 \text{ pour carac(K)} \neq 2 \qquad (2).$$

Tout calcul fait nous obtenons l'équation de Weierstrass :

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

Les coefficients b_{2i} sont des polynômes "homogènes" de degré 2i de l'anneau $Z[a_1,\ldots,a_6]$

$$b_2 = a_1^2 + 4a_2; \quad b_4 = a_1a_3 + 2a_4 \text{ et } \quad b_6 = a_3^2 + 4a_6 \qquad (4).$$

L'élimination, dans l'équation (3), du coefficient 4 et du monôme en x^2 s'obtient avec le changement de variables :

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

Après calcul, nous obtenons l'équation de Weierstrass :

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

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

$$c_4 = b_2^2 - 24b_4 \text{ et } c_6 = -b_2^3 + 36b_2b_4 - 216b_6 \; ; \qquad (7)$$

Il existe d'autres équations de Weierstrass :

La cubique de Weierstrass :

$$E_3 : y^2 = x^3 + A\, x + B \in K[x,y] \qquad (8\text{-}1)$$

Elle est utilisée en cryptographie et codage.

La courbe elliptique de Legendre *:*

$$E_4 : y^2 = x(x-1)(x-t) \in K[x,y] \text{ avec } t \neq 0,1 \; ; \qquad (8\text{-}2)$$

La courbe elliptique de Tate *:*

$$E_5 : y^2 + xy = x^3 + a_4x + a_6 \in ℂ[x,y] \qquad (8\text{-}3)$$

Les coefficients a_4 et a_6 sont des séries infinies complexes :

$$a_4 = -5\sum_{n\geq 1} n^3q^n/(1-q^n) \quad \text{et } a_6 = -\frac{1}{12}\sum_{n\geq 1}(7n^5+5n^3)q^n/(1-q^n)$$

où $q = \exp(2i\pi z)$ et $z = x + i\,y; \quad y > 0.$

La courbe elliptique de Deuring *:*

$$E_6 : y^2 + Axy + y = x^3 \in K[x,y] \qquad (8\text{-}5)$$

3- Invariants des cubiques de Weierstrass :[2],[13],[14]

Avec les coefficients b_{2i}, nous obtenons le discriminant.

Définition 6 : Le *discriminant d'une cubique de Weierstrass E est le polynôme "homogène" de degré 12, égal à :*

$$\Delta(E) = 9b_2b_4b_6 - 8b_4^3 - 27b_6^2 - b_2^2b_8 \in Z/[b_2, b_4, b_6, b_8] \qquad (9)$$

$$Où \quad 4b_8 = b_2b_6 - b_4^2 \qquad et\ carac(K) \neq 2,3$$

Avec le coefficient c_4 et le discriminant, nous obtenons l'invariant modulaire.

Définition 7: a) *l'invariant modulaire d'une cubique de Weierstrass E est l'élément du corps K égal à :*

$$j(E) = c_4^3/\Delta(E);\ pour\ caract(K) \neq 2,3$$

b) *l'invariant différentiel d'une cubique de Weierstrass d'équation :*

$$f(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 \in K[x,y],$$

est égal à :

$$\omega(E) = dx/(2y + a_1y + a_3) = dy/(3x^2 + 2a_2x + a_4 - a_1y),\ carac(K) \neq 2,3$$

Il y a d'autres invariants dans la théorie des courbes elliptiques : le conducteur, l'invariant de Hasse, le régulateur, la série L(E,s) de Dirichlet-Hasse, la fonction Zéta, etc …

Exemples de calcul d'invariants :

(1) Cubique de Weierstrass $E_1 : y^2 = x^3 + Ax + B \in IR[x,y]$

$b_2 = 0$; $b_4 = 2A$; $b_6 = 4B$; $b_8 = - A^2$; $c_4 = - 48A$;

$$\Delta(E_1) = - 16(4A^3 + 27B^2) \quad \text{et} \quad j(E_1) = \frac{1728 \times 4A^3}{4A^3 + 27B^2}$$

(2) Courbe elliptique de Legendre : E_2: $y^2 = x(x - 1)(x - t)$; $t \neq 0,1$

$b_2 = - 4(1 + t)$; $b_4 = 2t$; $b_6 = 0$; $b_8 = - t^2$; $c_4 = 16(t^2 - t + 1)$;

$j(E_2) = 2^8(t^2 - t + 1)^3/t^2(t - 1)^2$; $\Delta(E_2) = 16t^2(t - 1)^2$

(3) courbe elliptique de Tate : $E_3 : y^2 + xy = x^3 + a_4x + a_6 \in K[x,y]$;

$b_2 = 1$; $b_4 = 2a_4$; $b_6 = 4a_6$; $b_8 = a_6 - a_4^2$; $c_4 = 1 - 48a_4$;

$$\Delta(E_3) = 72a_4a_6 - 64a_4^3 - 432.a_6^2 - a_4^2 - a_6; \qquad j(E_3) = \frac{(1 - 48a_4)^3}{\Delta(E_3)}$$

(4) courbe elliptique de Deuring:

$E_4 : y^2 + Axy + y = x^3 \in K[x,y]$ pour $A \neq 3$;
$b_2 = A^2$; $b_4 = A$; $b_6 = 1$; $b_8 = 0$; $c_4 = A^4 - 24A$;

$$\Delta(E_4) = A^3 - 27; \quad j(E_4) = \frac{A^3(A^3 - 24)}{A^3 - 27}$$

4-Groupe de Mordell-Weil d'une courbe elliptique:[3],[13],[14]

L'ensemble E(K) des points K rationnels d'une courbe elliptique E de corps de base K peut être muni d'une structure de groupe abélien.

Définition 8 : *Le point à l'infini d'une cubique de Weierstrass est le point $0_E = (\infty, \infty)$ dans le plan affine et $0_E = (0, 1, 0)$ dans le plan projectif $IP^2(K)$.*
Il est déterminé de façon unique par la direction de l'axe Oy.

Proposition 1 : *Le point à l'infini 0_E est un point non singulier de toute cubique de Weierstrass E.*

Preuve :
Soit une cubique de Weierstrass E,

$$E : f(x,y,z) = y^2z + a_1xyz + a_3yz^2 - x^3 - a_2x^2z - a_4xz^2 - a_6z^3,$$ dans le plan

projectif $IP^2(K)$. La valeur : $f(0_E) = f(0,1,0) = 0$ implique que le point à l'infini 0_E appartient à la cubique.
La dérivée partielle $f'_z = y^2 + a_1xy + 2a_3yz - a_2x^2 - 2a_4xz - 3z^2$ prend la valeur :

$$f'_z(0_E) = 1 \neq 0$$

il en résulte que le point à l'infini 0_E n'est pas singulier sur la cubique E.

€

Proposition 2 : *Soit l'ensemble E(K) des points K-rationnels d'une courbe elliptique E de corps de base K, et le point à l'infini 0_E. Alors, l'application f :*

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

de valeurs : $f(P_1,P_2) = P_1 + P_2$ et $f(0_E) = 0_E$.

munie de la règle géométrique de trois points colinéaires de la courbe elliptique E:

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

est une loi de groupe abélien d'élément neutre le point 0_E.

Preuve :

Description de la loi de composition :

a) P et Q deux points d'une courbe elliptique E

b) La sécante (L) qui passe par ces points coupe E en un troisième point R (la sécante L est tangente à la courbe elliptique E si P = Q);

Soit (L') la droite qui joint le point R et le point 0_E celle-ci coupe la courbe E en un troisième point P+Q.

Vérifions les 4 axiomes du groupe abélien :

1) Axiome de l'élément neutre :

Il suffit de poser Q= 0_E dans (a) ceci implique que les sécantes (L) et (L') vont coïncider d'où le résultat.

2) Axiome de commutativité :

Les sécantes (PQ) et (QP) sont confondues.

3)Axiome du symétrique :

obtenu par la règle géométrique (3 points colinéaires ont une somme égale à l'élément neutre).

4) Axiome d'associativité ; il est vérifié par le calcul des coordonnées des points (P + Q) + R et P + (Q + R) :

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

$Q + R = T$ et $P + (Q + R) = P + T$.

€

1) Coordonnées du symétrique – P d'un point P:

La parallèle à l'axe Oy passant par le point P coupe la courbe en un point R :

$$P + R + 0_E = 0_E$$

Cette relation implique le symétrique de P ; R = - P, figure1 ;
Avec le calcul j'obtiens les coordonnées du symétrique:

$$R = - P = (x_R = x_P,\ y_R = - y_P - a_1 x_P - a_3)$$

Il en résulte la :

Proposition 3: *Soit une courbe elliptique E d'équation de Weierstrass:*

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

Les coordonnées du symétrique – P d'un point $P = (x_P,y_P)$ de la courbe E sont égales à :

$$- P = R \; ; \; x_R = x_P \;\; et \;\; y_R = - y_P - a_1x_P - a_3$$

2) **Coordonnées de la somme $P_1 + P_2 = M = (x_M, y_M)$** pour $P_1 \neq \pm P_2$
(Figure 2)

L'équation de la sécante P_1P_2 est égale à:

$$y = \lambda(x - x_1) + y_1 \quad \text{où} \quad \lambda = \frac{y_1 - y_2}{x_1 - x_2}$$

en remplaçant la valeur de y dans E j'obtiens une équation du troisième degré en x. Cette équation admet trois racines x_1,x_2 et x_3. Avec la fonction symétrique élémentaire ″somme des racines d'un polynôme″ j'obtiens les coordonnées:

$$M = P_1 + P_2 = \begin{cases} x_M = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2 \text{ et } \lambda = (y_1 - y_2)/(x_1 - x_2) \\ y_M = -\lambda^3 - 2a_1\lambda^2 + (a_2 - a_1^2 + 2x_1 + x_2)\lambda - a_3 + a_1(a_2 + x_1 + x_2) - y_1 \end{cases}$$

Proposition 4: *Soit une cubique de Weierstrass E:*

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

Soient 2 points P_1 et P_2 de la courbe E, $P_1 \neq \pm P_2$; $P_i = (x_i,y_i)$.

Alors les coordonnées de la somme $P_1 + P_2 = M$ sont égales à :

$$P_1+P_2= M =(x_M,y_M)= \begin{cases} x_M = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2, \ \ \lambda= (y_1 - y_2)/(x_1 - x_2) \\ y_M= -\lambda^3-2a_1\lambda^2+(a_2 - a_1^2+2x_1+ x_2)\lambda+a_1a_2 - a_3+ a_1(x_1 + x_2)- y_1 \end{cases}$$

.

3) Coordonnées de la somme P + P= 2P :

La sécante P_1P_2 devient la tangente à la cubique au point $P = (x_P, y_P)$, (Figure 3)
La pente de la tangente en ce point est égale à la dérivée y′ de y:

$$y' = (3x^2 + 2a_2x + a_4 - a_1y)/(2y + a_1x + a_3) \qquad (1')$$

cette tangente coupe la courbe E en un point double P et en un point simple R.

Les abscisses du point double P et du point simple R, sont les 3 racines de l'équation cubique :

$$[y'(x - x_P) + y_P]^2 + (a_1x +a_3)[y'(x - x_P) + y_P]= x^3 + a_2x^2 + a_4x +a_6; \qquad (2')$$

La somme des racines est une fonction symétrique élémentaire des 3 racines :

$$2x_P + x_R = -a_2 + y'^2 + a_1y' ; \qquad (3')$$

Nous en déduisons l'abscisse du point R :

$$x_R = y'^2 + a_1 y' - a_2 - 2\,x_P \; ; \qquad (4')$$

(1′) et (4′) impliquent l'ordonnée du point R :

$$y_R = y'(x_R - x_P) + y_P \qquad (5')$$

Avec les formules du symétrique du point R, nous obtenons les coordonnées du point 2P

Ces résultats impliquent la :

Proposition 5 : *Soit une courbe elliptique E d'équation de Weierstrass :*

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

Alors les coordonnées du point $P + P = 2P$ sont égales à :

$$\begin{cases} x_{2P} = y'^2 + a_1y' - a_2 - 2x_P \; ; \;\; y' = (3x^2 + 2a_2x + a_4 - a_1y)/(2y + a_1x + a_3) \; ; \\ y_{2P} = -\,y'^3 - 2a_1y'^2 + (a_2 - a_1^2 + 3x_P)y' + a_1a_2 - a_3 + 2a_1x_P - y_P \; ; \end{cases}$$

Exemple :

Soit la cubique de Weierstrass :

$$E : y^2 - xy + 2y = x^3 - x^2 - 2x \in IR[x,y].$$

Avec le calcul j'obtiens les valeurs:

$$b_2 = -3;\ b_4 = -6;\ b_6 = 4;\ b_8 = -12 \quad \text{et} \quad \Delta(E) = 25\times 81.$$

Les points $P_1=(0,0)$; $P_2 = (-1,-3)$; $P_3 = (2,0)$ sont sur la courbe.

Calcul des coordonnées de points $2P_1$; $P_1 + P_2$; $P_1 + P_3$; $- P_2$

En appliquant la proposition 5 j'obtiens les coordonnées du point $2P_1 = (3,4)$.

En appliquant la proposition 4 j'obtiens les résultats:

$$P_1 + P_2 = (8,15) ;$$

$$P_2 + P_3 = (0,0) ;$$

$$P_1 + P_3 = (-1,-3);$$

En appliquant la proposition 3, j'obtiens le symétrique:

- $P_2 = (-1, 0)$.

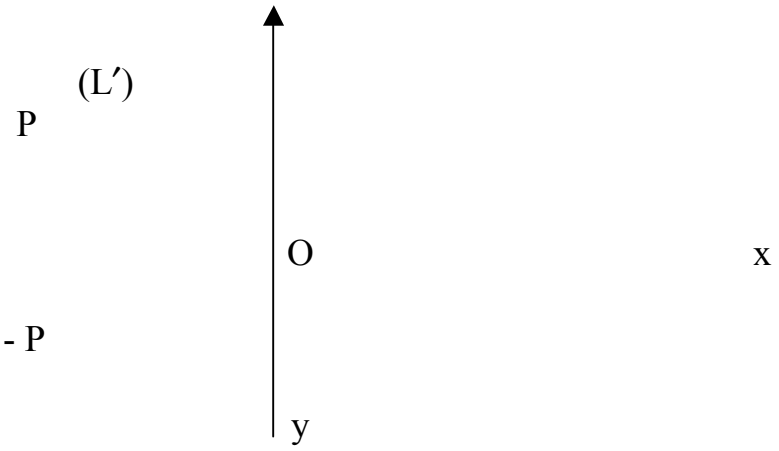


Figure 1

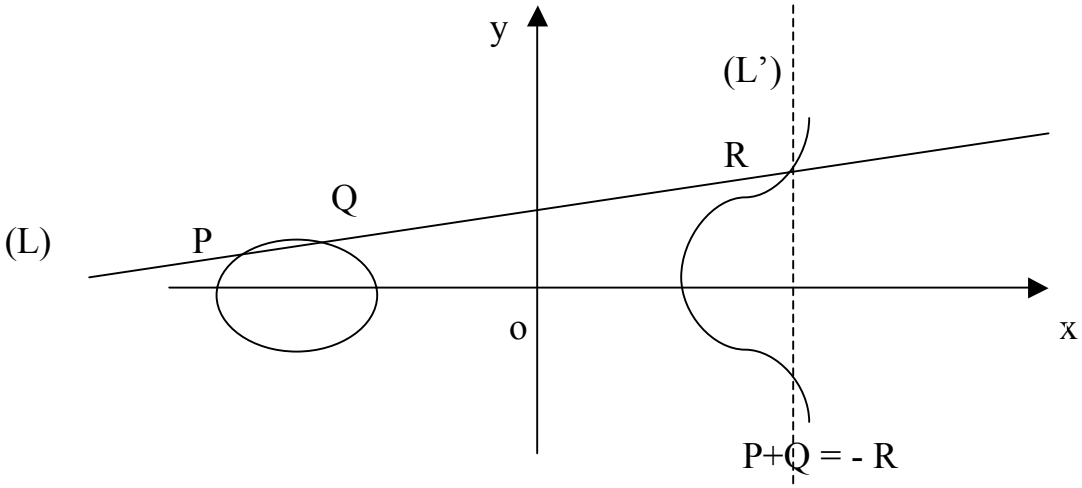
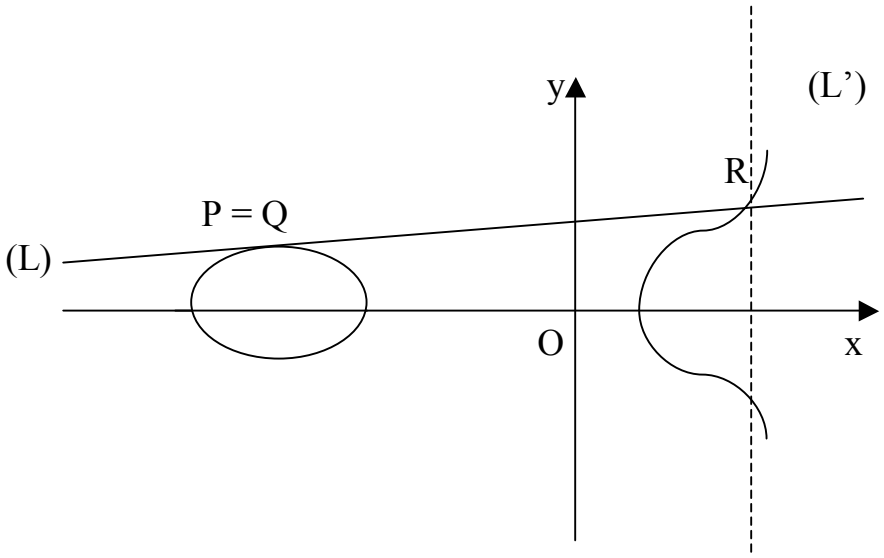


Figure 2



$$2P = - R$$

Figure 3

Avec les propositions 4 et 5, nous pouvons calculer les coordonnées des points mP, m = 3, 4, …

$$3P = P + 2P \; ; \; 4P = 2(2P) \; ; \; 5P = 2P + 3P \; ; \; \ldots$$

Le symbole mP pour $m \in Z$ est un point du groupe E(K) tel que :

$$mP = P + \ldots + P \; ; \; \text{m fois P}, \qquad \text{si } m > 0 \; ;$$

$$= (- P) + \ldots + (- P) \; ; \; \text{- m fois (-P)} \; ; \; \text{si } m < 0$$

$$= 0_E \; ; \quad \text{si } m = 0$$

Cassels [1], a obtenu les formules des coordonnées du point mP

Proposition 6 :

Soit une courbe elliptique E d'équation de Weierstrass:

$$E : y^2 = x^3 + Ax + B \in Q[x,y] \; ; \quad 4A^3 + 27B^2 \neq 0 \; ;$$

Alors les coordonnées d'un point mP de la cubique E sont égales à

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

Ψ_m, Φ_m *et* ω_m *sont des polynômes de l'anneau Z[x,y,A,B] qui satisfont les relations pour* $m \geq 2$*:*

$$\Psi_{-1} = -1 \; ; \; \Psi_0 = 0 \; ; \; \Psi_1 = 1 \; ; \; \Psi_2 = 2y \; ;$$
$$\Psi_3 = 3x^4 + 6Ax^2 + 12x - A^2 \; ;$$
$$\Psi_4 = 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3) \; ;$$
$$\Psi_{2m} = 2\Psi_m(\Psi_{m-2}\Psi_{m-1}^2 - \Psi_{m+2}\Psi_{m+1}^2) \; ;$$
$$\Psi_{2m+1} = \Psi_{m+2}\Psi_m^3 - \Psi_{m-1}\Psi_{m+1}^3 \; ;$$

$$\Phi_m = x\Psi_m^2 - \Psi_{m-1}\Psi_{m+1} \; ;$$
$$4\omega_m = \Psi_{m+2}\Psi_{m-1}^2 - \Psi_{m-2}\Psi_{m+1}^2 ;$$

Preuve :
La formule du symétrique :

$$-(x,y) = (x,-y-a_1x-a_3) = (x,-y) \; ; \quad \text{implique} \quad \Psi_{-1} = -1 \; ;$$

La formule $0_E = (\infty, \infty) = (x/0, y/0)$ implique $\Psi_0 = 0$.

La formule $1(x, y) = (x, y)$ de l'application identique implique : $\Psi_1 = 1$;

La formule $2(x, y) = (x_2, y_2)$ et la proposition 5 impliquent : $\Psi_2 = 2y$;

Avec les propositions 4 et 5, nous calculons les coordonnées des points $3P = 2P + P$ et $4P = 2(2P)$; on obtient ainsi les valeurs Ψ_3 et Ψ_4.

Pour les autres valeurs Ψ_m, nous utilisons une récurrence sur m.

€

Selon Lang, [6-1], Poincaré a conjecturé que le groupe E(K) des points K- rationnels d'une courbe elliptique E est un groupe abélien de type fini. En 1922, c'est Mordell qui démontre cette conjecture.
En 1930, Weil a étendu ce résultat aux variétés Abéliennes.

Définition 9 : *Le groupe abélien E(K) d'une courbe elliptique E est le groupe de Mordell-Weil de la courbe elliptique E.*

5-**Groupe de torsion d'une courbe elliptique [7], [13]:**

Les sous groupes du groupe de Mordell-Weil E(K) sont abéliens ou cycliques.

Définition 10: a)*Un point P du groupe E(K) d'ordre m est un point qui satisfait la relation : $mP = 0_E$.*

b) *Un sous groupe de m-torsion d'une cubique E de Weierstrass est l'ensemble des points P d'ordre m :*

$$E(K)[m] = \left\{ P \in E(K) \; ; \; mP = 0_E \right\}.$$

c) *La réunion infinie des sous groupes de torsion du groupe E(K) est un groupe de torsion :* $T(E/K) = \bigcup_{m \in Z} E(K)[m]$.

Le groupe de torsion T(E/K) est un sous groupe du groupe de Mordell-Weil.

Proposition 7 : *Le groupe de Mordell-Weil d'une courbe elliptique E est isomorphe à un produit de deux groupes abéliens*

$$E(K) \cong T(E/K) \times Z^r \text{ où } r = r(E) \geq 0.$$

T(E/K) = groupe de torsion de la courbe E ;
$Z/^r$ = r copies du groupe abélien Z/.

Définition11 : *l'entier $r = r(E) \geq 0$ est le rang de la courbe elliptique,il est égal au nombre de points indépendants qui engendrent la partie infinie du groupe abélien E(K)*

Les groupes de torsion des courbes elliptiques ont été déterminés pour le corps des nombres rationnels, pour les corps de nombres de degré 2, 3, 4. Ces groupes T(E/K) sont finis.

Proposition 8: *Les groupes de torsion T(E/Q) sont isomorphes à l'un des 15 groupes abéliens finis :*

Z/mZ pour $1 \leq m \leq 10$ et $m = 12$;

$Z/2Z \times Z/2dZ$ pour $d = 1, 2, 3, 4$.

Preuve : Mazur [8]

Les coordonnées des points de m-torsion d'une courbe elliptique E/Q peuvent être calculées par la:

Proposition 9(Théorème de Lutz):

Soit une courbe elliptique E/Q d'équation de Weierstrass :

$$E : y^2 = x^3 + Ax + B \in Z[x], \quad 4A^3 + 27B^2 \neq 0 ;$$

Les coordonnées (x_P, y_P) d'un point P de torsion satisfont les relations :

1) *x_P et y_P sont des entiers relatifs ;*

2) *Lorsque $2P \neq 0_E$, y_P^2 divise $4A^3 + 27B^2$.*

Preuve :

C'est un théorème démontré par Lutz(1937) et Nagell(1935) **[10]**.

€

Application :

Soit la courbe elliptique E d'équation de Weierstrass :

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

Le discriminant de la courbe E est égal à $\Delta(E) = -16(2^5.19)$;

Alors $4A^3 + 27B^2 = 2^5.19$

Algorithme :

1) Décomposition de $4A^3 + 27B^2 = 2^5.19$;
2) Recherche des carrés qui divisent $4A^3 + 27B^2$: $y^2 = 2^2$ et $y^2 = 2^4$;
2) Calcul des points P = (x,y) correspondants.

Pour $y^2 = 4$, l'équation (1) implique l'équation diophantienne :

$$x^3 + 5x - 6 = 0;$$

Cette équation admet la solution x = 1, il en résulte le point P = (1,2).

Pour $y^2 = 16$, l'équation (1) implique l'équation diophantienne :

$$x^3 + 5x - 18 = 0;$$

Cette équation admet la solution x = 2, il en résulte le point R = (2,4).

Calcul des points 2P et 2R avec la proposition 5:

$2P = (2,-4) \neq 0_E$ et $2R = \left(\frac{33}{8^2}, \frac{-433}{8^3}\right) \neq 0_E$.

D'après la proposition 9 les deux points P et R ne sont pas des 2-torsion,(mais ce sont des points de torsions).

6- Isogénies et isomorphismes de courbes elliptiques :

Ces notions se trouvent dans [2], [7], [11], [13]

1)-Isogénies de courbes elliptiques :

Définition 12 : *Une isogénie de deux courbes elliptiques E/K et E′/K est un homomorphisme surjectif de groupes abéliens :*

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

Les isogénies de courbes elliptiques possèdent deux invariants :

Définition 13 :

a) *le degré de l'isogénie f est égal à l'ordre de son noyau.*

b) *l'isogénie duale de l'isogénie $f : E(K) \longrightarrow E'(K)$ est l'homomorphisme :*

$$\hat{f} : E'(K) \longrightarrow E(K) \quad \text{tel que les composées :}$$

$$f o \hat{f} : E'(K) \longrightarrow E'(K) ;$$

$$\hat{f} o f : E(K) \longrightarrow E(K) ;$$

soient des multiplications par le degré de l'isogénie f.

Preuve : [13-III].

La multiplication sur le groupe E(K) par un entier $m \in Z$ est l'application:

$$t_m : E(K) \longrightarrow E(K) ; \text{ de valeur, } t_m(P) = mP$$

Cette multiplication a pour noyau le sous groupe E(K)[m] de m - torsion de E, c'est donc une isogénie du groupe E(K).

Proposition 10: *La multiplication par un entier m sur le groupe de Mordell-Weil E(K) ;*

$$t_m : E(K) \longrightarrow E(K) ; \; t_m(P) = mP,$$

est une isogenie de degré m^2 .

Preuve :

Soit Φ une isogénie de courbes elliptiques E_1 et E_2 de degré m et $\hat{\Phi}$ son dual.
Posons $\Phi = t_m$ et $\Psi = t_1$, par l'addition des applications duales on a :

$\hat{t}_{m+1} = \hat{t}_m + \hat{t}_1$, posons d = degré t_m , la multiplication par d donne :

$t_d = \hat{t}_m \circ t_m$ (par définition du dual)

$= t_{m^2}$, comme l'anneau d'endomorphisme des courbes elliptiques est un Z module de torsion libre on a : $d = m^2$.

pour les détails, consulter [13-III 6.2].

€

Proposition 11: *l'ensemble des multiplications t_m est un anneau isomorphe à l'anneau **Z**.*

Preuve :

Soient deux multiplications $t_m, t_{m'} : E(K) \longrightarrow E(K)$ (1) ;

Alors $(t_m + t_{m'})(P) = t_m(P) + t_{m'}(P) \quad \forall P \in E(K)$

$= mP + m'P = (m + m')P = t_{m+m'}(P)$ (2);

La relation $m + m' = m' + m$ implique la commutativité de l'addition.

Pour $m = 0$, la multiplication $t_0(P) = 0P = 0_E \in E(K)$ (3);
implique que t_0 est l'élément neutre de l'addition

Pour $m + m' = 0$, la multiplication $t_{m+m'}$ a pour valeur $t_{m+m'}(P) = (m + m')P = 0P = 0_E$.
Nous avons obtenu un groupe additif abélien.

Soit l'application f : **Z** $\longrightarrow \{t_m\}$, de valeur $f(m) = t_m$;

Au produit mm' correspond, $f(mm') = t_{mm'} : E(K) \longrightarrow E(K)$.

Par définition, $t_{mm'}(P) = mm'P = mt_{m'}(P) = t_m \text{ o } t_{m'}(P)$;
Il en résulte la formule :

$t_{mm'} = t_m \text{ o } t_{m'} = t_m t_{m'}$ (4) ;

Avec les formules (2) et (4) j'obtiens les relations :

$t_m(t_n + t_r) = t_m t_n + t_m t_r$.

Ce qui prouve que l'ensemble $\{t_m\}$ des multiplications t_m est un anneau isomorphe à l'anneau Z/ ; ses éléments neutres sont $t_0(P) = 0P = 0_E$ pour l'addition et $t_1(P) = 1P = Id_E$ pour la multiplication.

2)-Isomorphismes de courbes elliptiques :

Ce sont des homomorphismes bijectifs de groupes, ils sont déterminés par des formules spécifiques.

Proposition 12 : *Soit une courbe elliptique E/K d'équation de Weierstrass :*

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

Le changement de variables : $x = u^2X + r$ *et* $y = u^3Y + u^2sX + t$

où $u, r, s, t \in K$; $u \neq 0$;
est un isomorphisme de groupes de Mordell-Weil

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

la transformée E′(K) a pour équation de Weierstrass :

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

Preuve :
Calcul des variables X et Y,

$$X = (x - r)/u^2 \quad \text{et} \quad Y = (y - sx + sr - t)/u^3,$$

La condition $u \neq 0$ implique une seule solution X,Y, donc l'application f est injective.
L'image du point à l'infini est égale à :

$$X = \infty, \quad Y = \infty.$$

Avec le calcul, je vérifie la formule : $f(P + Q) = f(P) + f(Q)$,

f est surjective [2-II.6.8]

Donc f est un isomorphisme de groupes abéliens

Cette proposition admet le :

Corollaire :
Soit les hypothèses de la Proposition 12. Alors les coefficients et les invariants des deux courbes elliptiques E et E´sont liés par les relations :

$$\begin{cases} ua_1' = a_1 + 2s; \\ u^2a_2' = a_2 - sa_1 + 3r - s^2; \\ u^3a_3' = a_3 + ra_1 + 2t\ ; \\ u^4a_4' = a_4 - sa_3 + 2ra_2 - (t+rs)a_1 + 3r^2 - 2st\ ; \\ u_6a_6' = a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1\ ; \end{cases} \qquad (I\text{-}1)$$

$$\begin{cases} u^2b'_2 = b_2 + 12r; \\ u^4b_4' = b_4 + rb_2 + 6r^2; \\ u^6b_6' = b_6 + 2rb_4 + r^2b_2 + 4\,r^3\ ; \\ u^8b_8' = b_8 + 3rb_6 + 3r^2b_4 + r^3b_2 + 3r^4\ ; \end{cases} \qquad (I\text{-}2)$$

$$u^4c_4' = c_4 \ \ et \ \ u^6\,c_6' = c_6 \qquad (I\text{-}3)$$

$$u^{12}\Delta(E') = \Delta(E) \quad et \ \ j(E') = j(E) \qquad (I\text{-}4)$$

Preuve :
En remplaçant x par u^2X+r et y par u^3Y+su^2X+t, j'obtiens les formules (I-1) à (I-4).

La relation j(E) = j(E ′) permet de classifier les courbes elliptiques en classes de courbes isomorphes :

Proposition13 : *Deux courbes elliptiques E(K) et E′(K) sont isomorphes si et seulement elles ont le même invariant modulaire j(E) = j(E′).*

1) Preuve de ″ E et E′ isomorphes ″ implique ″ j(E) = j(E′)″ :
La formule (1 – 4) du corollaire est précisément l'égalité j(E) = j(E′).

2) Preuve de ″ j(E) = j(E′) ″ implique ″E et E′ isomorphes ″ :
Nous prenons l'équation de Weierstrass de la forme:

$E : y^2 = x^3 + Ax + B \in K[x,y]$ et $E' : y'^2 = x'^3 + A'x' + B' \in K[x,y]$;

Les invariants modulaires sont égaux à :

$$j(E) = 1728\frac{4A^3}{4A^3 + 27B^2} \quad \text{avec} \quad 4A^3 + 27B^2 \neq 0$$

$$j(E') = 1728\ \frac{4A'^3}{4A'^3 + 27B'^2} \quad \text{avec} \quad 4A'^3 + 27B'^2 \neq 0$$

Nous distinguons 3 cas suivant les valeurs j(E) :

j(E) = 0, j(E) = 1728 et j(E) ≠ 0, 1728.

a) Cas de j(E) = 0 cela implique A = 0 et B ≠ 0
L'isomorphisme d'équation $x = u^2X$, $y = u^3Y$ implique la relation $B = u^6B'$, cette équation admet 6 racines u, il en résulte 6 isomorphismes.

b) Cas de j(E) = 1728 implique A ≠ 0 et B = 0 ;
La relation d'isomorphisme $A = u^4A'$ implique 4 racines u , d'où 4 isomorphismes.

c) Cas de j(E) = t ≠ 0, 1728 avec le calcul nous obtenons la courbe elliptique isomorphe :

$$E' : Y^2 = X^3 + \frac{3tx}{1728 - t} + \frac{t}{1728 - t}.$$

€

Exemple de courbes elliptiques isomorphes :

Soit une courbe elliptique E d'équation de Weierstrass:

$$E : y^2 - 2xy + 8y = x^3 + 5x^2 + 8x - 10 \in Q[x,y] ;$$

Calcul des invariants de E :

$b_2 = 24$, $b_4 = 0$, $b_6 = 24$ et $b_8 = 144$;
$\Delta(E) = -24^2 \times 171$ et $j(E) = -24^4/171$.

Soit l'isomorphisme $f : E(Q) \longrightarrow E(Q)$ d'équations :

$$x = 4X + 3, \quad y = 8Y - 4X - 5.$$

Alors nous obtenons la courbe elliptique isomorphe :

$$E' : Y^2 - Y = X^3 + \frac{15}{4}X^2 - \frac{1}{16}X + 1/4.$$

Ses invariants s'obtiennent avec les formules (I – 4) du corollaire :

$$2^{12}\,\Delta(E') = \Delta(E) \quad \text{et} \quad j(E') = j(E).$$

CHAPITRE II

CORPS FINIS

1- Structure algébrique d'un corps fini

2 - Automorphismes d'un corps fini

Pour étudier les propriétés des courbes elliptiques sur les corps finis, il faut connaître la structure de ces corps. La description de ces corps se trouve dans des ouvrages de Théorie des nombres comme [6], [7].

1- Structure algébrique d'un corps fini :

Soit un corps fini $\mathbf{F_q}$ à q éléments. La structure de corps implique une addition d'élément neutre 0 et une multiplication d'élément neutre 1.
Tout corps contient un sous corps premier que nous déterminons avec l'homomorphisme d'anneaux,

$$u : Z/ \longrightarrow \mathbf{IF_q}$$

Le noyau de u est un idéal I de l'anneau Z/ ;
l'anneau Z/ étant principal, l'idéal I est principal , il est engendré par un nombre premier p (théorie des idéaux).
Il en résulte que le corps fini IF_q à q éléments contient le corps premier $Z/pZ= IF_p$.

Proposition 14:
Tout corps fini IF_q à q éléments contient un corps premier IF_p isomorphe au corps Z/pZ. Les corps IF_q et IF_p ont même caractéristique p premier.

Le corps fini IF_q a une structure de IF_p- espace vectoriel de dimension finie n.
Donc dans toute base $e_1,e_2 ;\ldots,e_n$ de l'espace vectoriel, le corps fini IF_q est l'ensemble des combinaisons linéaires : $x = r_1e_1 + r_2e_2 + \ldots + r_ne_n$ et $r_i \in Z/pZ$.
Il en résulte la proposition :

Proposition 15 :*Tout corps fini IF_q à q éléments est un espace vectoriel de dimension n sur un corps premier IF_p isomorphe au corps Z/pZ ; q est une puissance d'un nombre premier p, $q = p^n$.*

Dans la Théorie des Nombres Algébriques, toute extension finie L d'un corps K est le corps de décomposition d'un polynôme minimal $g(x) \in K[x]$.
Un corps fini IF_q est donc le corps de décomposition du polynôme
$g(x) = x^q - x \in IF_p[x]$.

La dérivée $g'(x) = qx^{q-1} = -1 \neq 0$ implique que le polynôme g(x) admet q racines simples :

$$x = 0, a_1, a_2, \ldots, a_{q-1}$$

Les racines du polynôme $g(x) / x = x^{q-1} - 1$ forment un groupe multiplicatif cyclique d'ordre q – 1.

Cela implique la :

Proposition16 : *l'ensemble IF_q^* des éléments non nuls d'un corps fini à q éléments forme un groupe multiplicatif d'ordre q – 1.*

Il en résulte les éléments du corps fini IF_q :

$$IF_q = \{0, a, a^2, \ldots, a^{q-1} = 1\}.$$

Tout générateur a du groupe cyclique IF_q^* est une racine primitive du polynôme $h(x) = x^{q-1} - 1$.
Une telle racine primitive peut être déterminée soit en calculant les puissances des entiers n = 2, 3,…, soit avec la :

Proposition 17: *Soit un groupe fini IF_q à $q = p^n$ éléments, tout générateur a du groupe cyclique IF_q^* satisfait la congruence :*

$$a^{(q-1)/d} \not\equiv 1 \bmod q \text{ pour tout diviseur } d \text{ de } q - 1.$$

Exemple:
Soit le corps IF_q , q = 7, alors q – 1 = 6 et d = 2,3.
Testons a = 2, 3, 4, 5, 6.
$2^2 = 4 \equiv 1 \bmod 7$; $2^3 \equiv 1 \bmod 7$, donc 2 n'est pas un générateur.
$32 = 9 \equiv 2 \bmod 7$, $33 \equiv 6 \bmod 7$, donc 3 est un générateur.
Vérification :
$3, 3^2 = 2, 3^3 = 6, 3^4 = 4, 3^5 = 5$ et $3^6 = 1$.
Test de a = 5
$5^2 \equiv 4 \bmod 7$, $5^3 \equiv 6 \bmod 7$, $5^4 \equiv 2 \bmod 7$, $5^5 \equiv 3 \bmod 7$, $5^6 \equiv 1 \bmod 7$.

Nous avons trouvé 2 générateurs du groupe cyclique IF_7.

Proposition18 : *Un corps fini IF_q à $q=p^n$ éléments admet une seule extension de degré s dans une clôture algébrique de IF_q. Cette extension est le corps fini à q^s éléments.*

Preuve :
Un corps fini IF_q est de degré n sur le corps IF_p lorsque $q = p^n$: $[IF_q : IF_p] = n$,
Une extension $IF_{q'}$ de IF_q est de degré $[IF_{q'} : IF_q] = s$, $q' = q^s = p^{ns}$.

Exemples :

1) le corps fini IF_q, pour $q = 5^4$ est une extension de degré 4 de IF_5 , une extension de degré 2 de IF_{25}.

2) suite d'extensions du corps premier IF_7 :

   $IF_7 \subset IF_{7^2} \subset IF_{7^6} \subset IF_{7^{12}} \subset IF_{7^{36}}$

2 – Automorphismes d'un corps fini :[3],[13]

Déterminons l'ensemble des automorphismes d'un corps fini IF_q pour $q = p^n$ et p premier.

Considérons l'endomorphisme de Frobenius de IF_q

$$Frob : IF_q \longrightarrow IF_q, \text{ de valeurs } Frob(x) = x^p,$$

Cette application est un homomorphisme et son noyau est trivial. Comme IF_q est fini, il en résulte que l'endomorphisme est surjectif ; par suite l'application Frob est un automorphisme du corps fini IF_q.

Proposition19:
L'ensemble $Aut(IF_q)$ des automorphismes d'un corps fini IF_q, $q = p^n$, p premier est un groupe cyclique d'ordre n. Il est engendré par l'application Frobenius.

Aut(IF_q) = { Frob, $Frob^2$,…, $Frob^n$ = Id }

Preuve :
Les n images $Frob^t(x)$ des puissances de Frob sont égales à :

$Frob(x) = x^p$, $Frob^2(x) = x^{p^2}$,…$Frob^{n-1}(x) = x^{p^{n-1}}$ et $Frob^n(x) = x^{p^n} = x$.
Donc le groupe $Aut(IF_q)$ des automorphismes du corps fini IF_q est :

$$Aut(IF_q) = \{Frob, Frob^2, \ldots, Frob^{q-1}, Frob^q = Id_{IFq}\}.$$

Une relation entre les corps finis $IF_p{}^d$ et $IF_p{}^n$ est précisée par :

Proposition 20 :
Soit un nombre premier p et les corps finis $IF_p{}^d$ et $IF_p{}^n$. Alors $IF_p{}^d$ est un sous corps de $IF_p{}^n$ si et seulement si d divise n. Alors $IF_p{}^n$ est une extension normale et séparable sur $IF_p{}^d$ de degré $[IF_p{}^n : IF_p{}^d] = n/d$.

Preuve :
Le corps fini *$F_p{}^n$ est le corps de décomposition du polynôme $f(x) = x^{pn} - x$.*
Pour $n = dn'$, $f(x) = (x^d)^{n'} - x$.
L'automorphisme de Frobenius du corps $IF_p{}^n$ a pour valeur : $Frob(x) = x^p$.
Il en résulte le groupe :

$$Aut(IF_p{}^n) = \{ Frob, Frob^2, \ldots, Frob^n = I_{dIFp^n} \}.$$

Ce groupe contient le sous groupe engendré par la puissance $Frob^{n'}$ qui est d'ordre $n/n' = d$; c'est le groupe $Aut(IF_p{}^d)$.

CHAPITRE III

COURBES ELLIPTIQUES SUR LES CORPS FINIS

1 - Groupe de Mordell-Weill E(IFq)

2 – Groupe formel d'une courbe elliptique

3 – Classification des courbes elliptiques E/IF_q par Hasse(E)

Nous examinerons dans ce chapitre la structure du groupe de Mordell-Weil, , $E(IF_q)$ sur les corps finis, le groupe formel d'une courbe elliptique E ainsi que l'invariant de Hasse Hasse(E).[2],[3],[13],[14]

1-Groupe de Mordell-Weil $E(IF_q)$:

Soit une courbe elliptique E d'équation de Weierstrass :

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

IF_q est un corps fini à $q = p^n$ éléments, p premier,
A chaque valeur x de IF_q il correspond 0 ou 2 racines y de l'équation (1) du $2^{ème}$ degré en y.
L'ordre du groupe abélien $E(IF_q)$ a été conjecturé par Hasse puis démontré par Hasse en 1930.

Proposition 21*(Théorème de Hasse): L'ordre du groupe $E(IF_q)$ de Mordell-Weil d'une courbe elliptique E sur un corps fini IF_q à $q = p^n$ éléments satisfait l'inégalité :*

$$/ card(E(IF_q) - q - 1/ \leq 2\sqrt{q}\,.$$

Preuve :
soit g l'homomorphisme qème du Frobenius:

$$g: E(IFq) \longrightarrow E(IFq)$$
$$(x,y) \qquad\qquad (x^q,y^q);$$

$\forall P \in E(IFq)$, $g(P) = P$ implique $P \in \ker(1 - g)$,

d'où $cardE(IFq) = card\ \ker(1 - g) = deg(1 - g)$,

Comme l'application degré est une forme quadratique définie positive alors:

$$|cardE(IFq) - q - 1| \leq 2\sqrt{q}$$

Dans la théorie des groupes de Mordell-Weil $E(IF_q)$, l'équation de Weierstrass

$$y^2 = x^3 + a_2x^2 + a_4x + a_6 = f(x) \in IF_q[x] \qquad (1)$$

est une équation Diophantienne sur le corps fini IF_q .

Pour déterminer le nombre de points P = (x,y) du groupe $E(IF_q)$ nous pouvons utiliser l'algorithme :

1) prendre x = k pour k = 1, 2, …,q.
2) résoudre les équations diophantiennes (1) qui sont de degré 2.

Il y a une autre procédure précisée par la:

Proposition22 :
Soit une courbe elliptique E d'équation de Weierstrass :

$$y^2 = x^3 + ax^2 + bx + c \in IF_q[x] \ , \ q = p^n \ ; \ p \text{ premier.}$$

Alors :

1) $card\ E(IF_q) = 1 + q + \sum_{x \in F_q} \chi(f(x))$.

2) le caractère quadratique $\chi : IF_q^* \longrightarrow \{\pm 1\}$ *satisfait l'inégalité :*

$$\left| \sum_{x \in F_q} \chi(f(x)) \right| \leq 2\sqrt{q} \ .$$

Par convention on pose $\chi(0) = 0$ *dans le corps* IF_q.

Preuve :
Lorsque $f(k) = n^2$ est un carré dans IF_q^*, alors $\chi(f(k)) = 1$

Lorsque $f(k)$ n'est pas un carré , alors $\chi(f(k)) = -1$

Dans la formule du card $E(IF_q)$, 1 correspond au point à l'infini et q est le nombre d'éléments x de IF_q .

Applications:

1) Soit la courbe elliptique E d'équation de Weierstrass:

$$E : y^2 = x^3 + 2x + 1 = f(x) \in IF_3[x] ;$$

Calcul des invariants de la courbe E :

$b_2 = 0$, $b_4 = 1$, $b_6 = 1$ et $\Delta(E) = 1 \neq 0 \in IF_3 = \{0, 1, 2\}$;

Algorithme de calcul des points (x,y) de E :

Pour x = 0, $f(0) = y^2 = 1$; donc 2 points (0,1) et (0,2);
Pour x = 1, $f(1) = 1$; donc 2 points (1,1) et (1,2) ;
Pour x = 2, $f(2) = 1$; donc 2 points (2,1) et (2,2);

Il en résulte que le groupe de Mordell-Weil est d'ordre 7:

$$E(IF_3) = \{0_E, (0,1), ((0,2), (1,1), (1,2), (2,1), (2,2)\}$$

Vérifions la formule du théorème de Hasse :

$$| \text{card } E(IF_q) - q - 1 | = | 7 - 3 - 1 | = 3 < 2\sqrt{q} = 2\sqrt{3} .$$

2) Soit la courbe elliptique E d'équation de Weierstrass :

$$E : y^2 = x^3 + 3x^2 + 2x + 4 = f(x) \in IF_7[x],$$

Calcul des invariants de E :
$b_2 = 5$, $b_4 = 4$, $b_6 = 2$, $b_8 = 2$ et $\Delta(E) = 2$;
Dans le corps fini IF_7 il y a 3 carrés qui sont $1^2 = 1$, $2^2 = 4$ et $3^2 = 2$;
Calcul des valeurs $f(x)$ et du caractère $\chi(f(x))$:

x	0	1	2	3	4	5	6
$f(x)$	4	3	0	1	5	4	4
$\chi(f(x))$	1	-1	0	1	-1	1	1

$$\text{Card}(IF_7) = 1 + q + \sum_{x \in F_q} \chi(f(x)) = 1 + 7 + 2 = 10$$

Il en résulte $E(IF_7) = \{(0,5),(0,2),(2,0),(3,6),(3,1),(5,5),(5,2),(6,2),(6,5),0_E\}$,

Vérifions la formule de Hasse :

$$| \text{card } E(IF_q) - q - 1 | = | 10\text{-}7\text{-}1 | = 2 < 2\sqrt{7}\,.$$

3) soit la courbe elliptique E d'équation :

$$E : y^2 = x^3 + 7x^2 + 4x + 1 = f(x) \in IF_{25}[x] ;$$

Calcul des invariants de E:

$b_2 = 3$, $b_4 = 8$, $b_6 = 4$ et $b_8 = 12$ et $\Delta(E) = 3$.

Les carrés dans le groupe IF_{25}^* sont :
$1 = 1^2$, $4 = 2^2$, $9 = 3^2$, $6 = 9^2 = 16^2$, $11 = 6^2 = 19^2$, $14 = 8^2 = 17^2$, $16 = 4^2$,
$19 = 12^2 = 13^2$, $21 = 11^2 = 14^2$, $24 = 7^2 = 18^2$.
Il y a 10 carrés et 14 non carrés ;

Tableau des valeurs $f(x)$ et $\chi(f(x))$:

x	0	1	2	3	4	5	6	7	8	9	10	11
$f(x)$	1	3	0	3	3	1	3	0	3	3	1	3
$\chi(f(x))$	1	-1	0	-1	-1	1	-1	0	-1	-1	1	-1

12	13	14	15	16	17	18	19	20	21	22	23	24
0	3	3	1	3	0	3	3	1	3	0	3	3
0	-1	-1	1	-1	0	-1	-1	1	-1	0	-1	-1

Card $(IF_{5^2}) = 1 + q + \sum_{x \in F_q} \chi(f(x)) = 1 + 25 - 10 = 16$ points

Vérifions le théorème de Hasse :

$$| \text{card } E(IF_q) - q - 1 | = | 16 - 25 - 1 | = 10 \leq 2\sqrt{25} = 10.$$

2-Groupe Formel d'une Courbe Elliptique :

Ce groupe est décrit par Tate dans [**14**], par Silverman dans [**13**], par Velu dans [**16**],…

Soit une courbe elliptique d'équation de Weierstrass :

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

Effectuons le changement de variables :

$$(x,y) \longrightarrow (z,w)$$

avec les formules $x = z/w$ et $y = -1/w$ (2)

L'équation (1) devient dans le plan affine (z,w) :

$$w = z^3 + a_1zw + a_2z^2w + a_3w^2 + a_4zw^2 + a_6w^3 \qquad (3)$$

C'est une fonction implicite $f(z, w(z))$.

Le point à l'infini 0_E de la courbe E est transformé au point $(z,w)= (0,0)$ (4)
Avec un algorithme de calcul dans (3) nous obtenons un développement formel au voisinage du point (0,0) :

$$w = z^3(1 + A_1z + A_2z^2 + A_3z^3 + \ldots); \qquad (5)$$

Les coefficients A_n, sont des polynômes " homogènes" de degré n de l'anneau $Z[a_1,\ldots a_6]$;

$$A_1 = a_1,\ A_2 = a_1^2 + a_2,\ A_3 = a_1^3 + 2a_1a_2 + a_3;\ A_4 = (a_1^4 + 3a_1^2a_2 + 3a_1a_3 + a_2^2 + a_4) ;\ldots$$

z est un paramètre local au point (0,0) du plan Ozw.
Avec le calcul nous obtenons les développements formels :

$$x = z/w(z) = 1/z^2 - a_1/z - a_2 - a_3z - (a_4+a_1a_3)z^2 + \ldots$$

$$y = y(z) = -1/w(z) = -1/z^3 + a_1/z^2 + a_2/z + a_3 + (a_4+a_1a_3)z + \ldots$$

Nous en déduisons l'invariant différentiel :

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

$$= dz[1 + a_1 z + (a_1^2 + a_2)z^2 + (a_1^3 + 2a_1 a_2 + 2a_3)z^3 + (a_1^4 + 3a_1^2 a_2 + 6a_1 a_3 + a_2^2 + 2a_4)z4 + \ldots]$$

La notion de groupe formel apparaît dans la formule d'addition dans le plan $\mathbf{0}_{z,w}$. À deux points (z_1,w_1) et (z_2,w_2), correspond le troisième point (z_3,w_3), colinéaire. Avec le calcul nous obtenons une fonction :

$$F(z_1,z_2) = z_3$$
$$= z_1 + z_2 - a_1 z_1 z_2 - a_2(z_1^2 z_2 + z_1 z_2^2) - 2a_3(z_1^3 z_2 + z_1 z_2^3) + (a_1 a_2 - 3a_3)z_1^2 z_2^2 + \ldots \in Z[a_1,..,a_6][[z_1,z_2]].$$

Cette fonction satisfait les 3 conditions :

a) la commutativité, $F(z_1,z_2) = F(z_2,z_1)$;
b) l'associativité, $F(z_1,F(z_2,z)) = F(F(z_1,z_2),z)$;
c) l'inverse, $F(z,i(z)) = 0$;

Une telle fonction est un groupe formel ; la structure de groupe formel à un paramètre est précisée par les formules :

1) $F(x,y) = x + y +$ termes de degré ≥ 2 ;
2) $F(x,(y,z)) = F(F(x,y),z)$;
3) $F(x,y) = F(y,x)$;
4) Il existe une série unique $i(T)$ telle que $F(T,i(T))=0$;
5) $F(x,0)=x$ et $F(0,y) = y$;

Pour un point P = (z,w), le point nP a une abscisse égale à z(nP).

Ces abscisses sont des séries $\psi_n(z)$ déterminées par la récurrence:

$$\psi_1(z) = z \text{ et } \psi_{n+1}(z) = F(z,\psi_n(z)) \text{ pour } n \geq 1.$$

Avec ces formules de récurrence, il est possible de calculer toutes les séries ψ_2, ψ_3,…

$$\psi_2(z) = 2z - a_1z^2 - 2a_2z^3 + (a_1a_2 - 7a_3)z^4 + \ldots$$

$$\psi_3(z) = 3z - 3a_1z^2 + (a_1^2 - 8a_2)z^3 + 3(4a_1a_2 - 13a_3)z^4 + \ldots$$

En caractéristique $p > 0$, la série formelle ψ_p du groupe formel à un paramètre $F(z,\psi_n(z))$ est de la forme :

$$\psi_p(z) = c_1z^{p^h} + c_2z^{2p^h} + c_3z^{3p^h} + \ldots, \quad \text{avec } c_1 \neq 0,$$

Définition 13: *La hauteur du groupe formel d'une courbe elliptique E est la puissance h de p de la série formelle $\psi_p(z)$, h satisfait :*

a)

1) $h \in N^*$

2) $h = \infty$ pour $\psi_p(z) = 0$.

b) *La hauteur du groupe formel d'une courbe elliptique E définie sur un corps fini IF_q est la hauteur de la multiplication t_p : $\hat{E} \longrightarrow \hat{E}$*

Proposition 25 :

Soit E une courbe elliptique sur IF_q , soit

$f : E \longrightarrow E^{pn}$ l'homomorphisme $q^{ème}$ du Frobenius, g l'homomorphisme de groupes formels induit par f . Alors :

$$deg_i(f) = p^{h(g)}.$$

Preuve : [13.IV.7-4]

□

Corollaire *: La hauteur $h(\hat{E})$ du groupe formel $\hat{E}$ d'une courbe elliptique E définie sur un corps fini IF_q, $q= p^n$, p premier est :*

$$h(\hat{E})= 1 \text{ ou } 2.$$

Preuve :

En remplaçant dans la proposition 25 *f* par la multiplication t_p .

□

3- Classification des courbes elliptiques E/IF_q par Hasse(E):

La hauteur du groupe formel d'une courbe elliptique E permet d'introduire l'invariant de Hasse, Hasse(E) de la courbe elliptique.

Définition 14 : *Soit une courbe elliptique E sur un corps fini IF_q à $q = p^n$ éléments ; L'invariant de Hasse de E est égal à Hasse(E) = 1 lorsque la hauteur h est égale à 1 et Hasse(E) = 0 lorsque la hauteur h = 2.*

Cet invariant Hasse(E) classifie les courbes elliptiques sur les corps finis en 2 classes, les courbes elliptiques ordinaires et les courbes elliptiques supersingulières.

Définition 15 :

1) *Une courbe elliptique ordinaire est une courbe elliptique sur un corps fini IF_q qui a un invariant de Hasse, Hasse(E) = 1.*

2) *Une courbe elliptique supersingulière est une courbe elliptique sur un corps fini IF_q qui a un invariant de Hasse, Hasse(E) = 0.*

Les courbes elliptiques des deux classes ne sont pas singulières, donc leur discriminant n'est pas nul.

CHAPITRE IV

COURBES ELLIPTIQUES SUPERSINGULIÈRES

1-Critères pour les courbes elliptiques supersingulières

2-Sous groupes de torsion des courbes elliptiques supersingulières

3-Invariants modulaires des courbes elliptiques supersingulières

Dans le chapitre précédent nous avons étudié le groupe formel d'une courbe elliptique et défini l'invariant de Hasse d'une courbe elliptique E/IF_q, $q=p^n$.

1 - Critères pour les courbes elliptiques supersingulières

Il y a une autre méthode de détermination des courbes elliptiques supersingulières basée sur la forme de l'équation de Weierstrass :

Pour la forme $y^2 = f(x)$ c'est la :

Proposition 26 : *soit une courbe elliptique E d'équation de Weierstrass :*

$$E : y^2 = x^3 + a_2x^2 + a_4x + a_6 = f(x) \in IF_q[x,y] ;$$

$q = p^n$ et p premier, $p>2$;

Alors, E est supersingulière si et seulement si le coefficient du monôme x^{p-1}

du polynôme $(f(x))^{\frac{p-1}{2}}$ est nul.

Preuve :

$$\text{card}(E(IFq) = 1 + q + \sum_{x \in IFq} \chi(f(x)).$$

en utilisant les propriétés des corps finis on a:

card(IFq) = q, IFq* est cyclique d'ordre q – 1, implique:

$\forall x \in IFq$, $\chi(f(x)) = x^{\frac{q-1}{2}}$ d'où :

$$\text{Card}(E(IFq)) = 1 + q + \sum_{x \in IF_q} (f(x)^{\frac{q-1}{2}} \quad \text{sur IFq ;}$$

Le corps IFq* étant cyclique, implique:

$$\sum_{x \in IF_q} x^i = \begin{cases} -1 \text{ si } q-1 \text{ divise } i \\ 0 \quad \text{sinon} \end{cases}$$

$f(x)$ est de degré 3; l'unique terme non nul est celui du monôme x^{q-1}, posons A_q son coefficient, alors:

$\text{card}(E(IFq)) = 1 + q + A_q$ (2)

or, $\text{card}(E(IFq)) = \deg(1 - \Phi) = 1 + q - \alpha$ (3)

(2) et (3) impliquent $A_q = - \alpha \in IFq$.
$A_q = 0$ implique $\alpha \equiv 0$ (modulo p),
la multiplication par α est $t_\alpha = \Phi \circ \hat{\Phi}$ d'où,

$\hat{\Phi} = t_\alpha - \Phi$, pour $\alpha = 0$, $\hat{\Phi}$ est inséparable implique E supersingulière.

$A_q = 0$ implique $A_p = 0$, pour cela il suffit de poser:

$p^{n+1} - 1 = p^n (p - 1) + p^n - 1$:

$$f(x)^{\frac{p^{n+1}-1}{2}} = \left(f(x)^{\frac{p-1}{2}} \right)^{p^n} + f(x)^{\frac{p^n-1}{2}}$$

D'où $A_{n+1} = A_p{}^{pn} A_p{}^n$ (4)
une récurrence sur $n \geq 0$ donne le résultat

Appliquons ce critère à quelques exemples :

1) soit une cubique de Weierstrass E_1 d'équation:

$E_1 : y^2 = x^3 - 4x^2 - 9x + 12 = f(x) \in IF_{13}[x,y]$,

Calcul des coefficients b_{2i} et du discriminant $\Delta(E_1)$:

$b_2 = 10, b_4 = 8, b_6 = 9, b_8 = 0$ et $\Delta(E_1) = 2$,

Calcul de $(f(x))^{\frac{p-1}{2}} = (f(x))^6$

Nous utilisons la formule du binôme :

$(A + B)^n = A^n + \binom{n}{1}A^{n-1}B + \binom{n}{2}A^{n-2}B^2 + \ldots + B^n$,

Alors nous obtenons pour $A = x^3 + 12$, $B = 9x^2 + 4x$ le coefficient D de x^{12} dans $f(x)^6$:

D = 2, il en résulte que la courbe elliptique E_1 est ordinaire.

2) Soit une courbe elliptique E_2 d'équation de Weierstrass :

$E_2 : y^2 = x^3 + x + 1 = f(x) \in IF_5[x,y]$,

Calcul des coefficients b_{2i} et du discriminant $\Delta(E_2)$:

$b_2 = 0$, $b_4 = 2$, $b_6 = 4$, $b_8 = 4$ et $\Delta(E_2) = 4$;

Appliquons le critère $f(x)^{\frac{p-1}{2}}$:

$f(x)^{\frac{p-1}{2}} = f(x)^2 = (x^3 + x + 1)^2 \in IF_5[x,y]$,
Calcul du coefficient $x^{p-1} = x^4$, en appliquant la formule du binôme , j'obtiens la valeur du coefficient D de x^4, $D = 2 \neq 0$, il en résulte que E_2 est ordinaire sur IF_5.

3) Soit la courbe elliptique E_3 d'équation de Weierstrass :

$E_3 : y^2 = x^3 + 3x^2 + 4x + 2 = f(x) \in IF_7[x,y]$,

$b_2 = 5$, $b_4 = 1$, $b_6 = 1$, $b_8 = 1$ et $\Delta(E_3) = 6$

Calcul du coefficient D du monôme x^6 dans le polynôme $f(x)^3$:

J'obtiens D = 0, il en résulte que la courbe elliptique E_3 est supersingulière sur IF_7.

4) Soit une courbe elliptique E_4 d'équation de Weierstrass :

$$E_4 : y^2 = x^3 + 6x + 6 = f(x) \in IF_{23}\,[x,y] ;$$

Calcul des coefficients b_{2i} ,(i = 1,2,3,4) et du discriminant $\Delta(E_4)$:

$b_2 = 0$, $b_4 = 12$, $b_6 = 1$, $b_8 = 10$ et $\Delta(E_4) = 18$.

Le coefficient D de x^{22} dans le polynôme $f(x)^{11}$ est égal à :

D = 0, donc E_4 est une courbe elliptique supersingulière sur IF_{23}

Pour la forme de Legendre c'est la :

Proposition 27 :

Soit une courbe elliptique E d'équation de Legendre :

$$E : y^2 = x(x-1)(x-t) \in IF_q\,[x,y] \text{ , } p>2 \text{ et premier}, q = p^n,\ t \neq 0,1.$$

a) *Soit le polynôme :*

$$g_p(u) = \sum_{0 \le i \le m} \binom{m}{i}^2 u^i \quad , \quad \text{pour } m = (p-1)/2.$$

Alors la courbe elliptique E est supersingulière si et seulement si u est racine du polynôme $g_p(u)$.

b) *Le polynôme $g_p(u)$ admet des racines distinctes. A isomorphisme près, le nombre de courbes supersingulières dans la clôture algébrique du corps fini IF_q est égal à:*

$$N_p = [p/12] + e_p,$$

où [p/12] = partie entière de p/12 et

$e_3 = 1$ *et pour* $p \geq 5$ $e_p = 0,1,\ 1,\ 2$ *si* $p \equiv 1, 5, 7, 11 \pmod{12}$.

Preuve :

La courbe elliptique E est supersingulière si le coefficient du monôme x^{p-1} dans $f(x)^{\frac{p-1}{2}}$ est nul,

Posons $m = \frac{p-1}{2}$

$f(x)^{\frac{P-1}{2}} = x^m(x-1)^m(x-\lambda)^m$, le coefficient x^m dans

$(x-1)^m(x-\lambda)^m$ est égal à :

$(-1)^m \sum_{i=0}^{m} \binom{m}{i}^2 \lambda^i$ le coefficient de x^{2m} est : $\sum_{i=0}^{m} \binom{m}{i}^2 \lambda^i$

b) l'application de l'opérateur différentiel (Picard-Fuchs) montre que les racines sont distinctes.

Pour p = 3 $g_p(\lambda) = 1 + \lambda$ implique une unique courbe elliptique supersingulière d'invariant modulaire
$j(E) = 0 = 1728$.
Pour $p \geq 5$
$j(E_\lambda) = 0$, $\lambda \in \{-\beta, \beta\}$ avec β racine primitive troisième de l'unité,
$j(E_\lambda) = 1728$ $\lambda \in \{ 1/2 , -1 , 2 \}$,

$j(E_\lambda) \neq 0, 1728$ $\lambda \in \{ \lambda, 1-\lambda, \frac{1}{\lambda}, \frac{1}{1-\lambda}, \frac{\lambda-1}{\lambda}, \frac{\lambda}{\lambda-1} \}$.

Soit :
N le nombre de courbes elliptiques supersingulières d'invariants modulaires $j(E_\lambda) \neq 0,1728$
N′ le nombre de courbes elliptiques supersingulières d'invariants modulaires $j(E_\lambda) = 0$ et $j(E_\lambda) = 1728$,
posons: $\varepsilon p(j) = 1$ si la courbe elliptique est supersingulière et $\varepsilon p(j) = 0$ si la courbe elliptique est ordinaire, alors:

$$Np = N + N'$$

$$Np = \frac{1}{6}\left[\frac{p-1}{2} - 2\varepsilon_p(0) - 3\varepsilon_p(1728) \right] + \varepsilon_p(0) + \varepsilon_p(1728)$$

Application de la proposition 27 :

Pour p = 3 , m = 1 j'obtiens le polynôme**:** $g_3(u) = 1 + u$.

Ce polynôme admet la racine u = 2, il en résulte que la courbe E d'équation de Legendre:

$$E : y^2 = x(x - 1)(x - u) \in IF_3[x,y]$$

est supersingulière pour $u \equiv 2 \bmod 3$.

Pour p = 5 , m = 2 j'obtiens le polynôme**:**

$g_5(u) = 1 + 4u + u^2$;

Ce polynôme admet ρ comme racine primitive troisième de l'unité.

Il en résulte que la courbe elliptique d'équation de Legendre :

$$E : y^2 = x(x - 1)(x - \rho) \in IF_{5\ alg}[x,y]$$

est supersingulière sur $IF_{5\ alg}$.

Pour p = 7 , m = 3 j'obtiens le polynôme cubique**:**

$g_7(u) = (1 + u)(1 + u + u^2)$;

Ce polynôme admet 3 racines u = 2, 4 et 6 modulo 7.

Il en résulte que la courbe elliptique de Legendre :

$$E : y^2 = x(x - 1)(x - u) \in IF_7[x,y]$$

est supersingulière les valeurs : $u \equiv 2, 4, 6 \bmod 7$.

Pour p = 11, m = 5 j'obtiens le polynôme de degré 5**:**

$g_{11}(u) = (1 + u)(1 – u + u^2)(1 + 3u + u^2)$

ce polynôme admet 3 racines u =2, 5 et 10 modulo 11.

Il en résulte que la courbe elliptique E de la forme de Legendre :

$$E : y^2 = x(x – 1)(x – u) \in IF_{11}[x,y]$$

est supersingulière pour les valeurs $u \equiv 2,5,10 \bmod 11$.

Exemples :
1)Soit une courbe elliptique E d'équation:

$$E: y^2 = x^3 – x = x(x – 1)(x + 1)$$

si E est définie sur IF_5^n , le polynôme:
$g_5(u) = 1 + 4u + u^2$, admet une solution primitive 3ème de l'unité d'où :
$g_5(-1) \neq 0$ implique que la courbe E est ordinaire sur IF_5.
2) Soit E une courbe elliptique d'équation de Weierstrass:

$E : y^2 = x^3 – 1$, $\Delta(E) = 1$, $j(E) = 0$,
pour p = 5, 7, 11, 13, 17

p	5	7	11	13	17
m	2	3	5	6	8
Coeff x^{p-1}	0	- 3	0	2	0
Classe de la courbe	Supersing	Ordinai	Supersing	Ordinai	Supersing

Développons les calculs pour p = 11:
$g_{11}(u) = (u^2 – u + 1)(u + 1)(u – 2)(u + 5)$

Les racines de $g_{11}(u)$ sont u = - 5, - 1, 2 ,

$\beta =$ et son conjugué

E est isomorphe sur IF11 alg à la courbe elliptique de Legendre:

$E\lambda : y2 = x (x – 1)(x – \lambda)$, $\lambda = \beta + 1$

et $g_{11}(\lambda) = 0$ implique

la courbe elliptique E est supersingulière pour p = 11.

- Signalons que pour p = 2, il n'y a qu'une seule courbe elliptique supersingulière :

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

2 - Sous groupes de torsion des courbes elliptiques supersingulières :

Le sous-groupe de p^r - torsion des courbes elliptiques supersingulières satisfait la proposition :

Proposition 28 : *Soit une courbe elliptique supersingulière E sur un corps fini IF_q à $q = p^n$ Alors le sous groupe de torsion $E(IF_q)[p^r]$ de E est trivial pour les entiers $r \geq 1$.*

Preuve :

L'ordre du groupe de Mordell-Weil E(IFq) d'une courbe elliptique supersingulière est:

$$Card(E(IFq)) = 1 + q,$$

Le p^r sous groupe de E(IFq) est: $\{P \in E(IFq) , pr\ P = 0E\}$

La multiplication $t_p{}^r : E(IFq) \longrightarrow E(IFq)$ à valeurs p^rP est une isogénie de degré p^{2r};

($t_p^r = (\hat{\Phi} \circ \Phi)^r$, qui est la composée de l'homomorphisme qème du Frobenius Φ et son dual.
L'ordre du $\ker(t_p^r) = (\deg(\Phi \circ \hat{\Phi}))r$, $r \geq 1$
$(\deg(\hat{\Phi}))r$,

E est supersingulière implique $\hat{\Phi}$ est inséparable

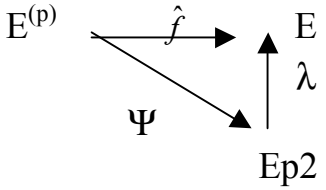
d'où $\#(\ker(t_p^r)) = 1$

3 - Invariant modulaire des courbes elliptiques supersingulières

Parmi les critères de reconnaissance des courbes elliptiques supersingulières il y a le critère basé sur l'invariant modulaire j(E) :

Proposition 29 :*L'invariant modulaire j(E) des courbes elliptiques supersingulières sur un corps fini IF_q, $q = p^n$, p premier est un élément du corps fini IF_{p^2}.*

Preuve :
Soit le factorisation :



λ o $\Psi = \hat{f}$ d'où $\deg(\lambda)\deg(\Psi) = \deg(\hat{f})$;
p $\deg(\lambda) = p$ implique $\deg(\lambda) = 1$, λ est un isomorphisme d'après **[13(II.2.4.1)] ;** alors :

$$j(E) = j(E^{(p^2)}) = j(E)^{p^2}$$

Les sujets d'étude des courbes elliptiques supersingulières sont nombreux : conducteurs, régulateurs, groupes de Châtelet-Weil, ″ formule de masse″, etc…

Références :

[1] J.W.CASSELS ″ Diophantine Equation with Special References to Elliptic Curves″ ; J. London Math. Soc. 41 (1966) 193/ 291.

[2] R.HARTSHORNE ″Algebraic Geometry″; Graduate Text in Mathematics- Springer- N° 52.

[3] D. HUSEMÖLLER ″ Elliptic Curves ″ ; 2nd Ed (2004).Graduate Text in Mathematics N° 111.

[4] N. KOBLITZ ″ Introduction to Elliptic Curves and Modular Forms ″; 2nd. Ed. Graduate Text in Mathematics - Springer- N° 95.

[5] KOSTRIKIN ″ Introduction à l'Algèbre ″ ; Ed. Mir- Moscou- 2nd. Ed.(1986).

[6] S. LANG ″ Algebra ″ 2nd. Ed – Addison Wesley- New York (1984).

[6-1] S. LANG ″ Elliptic Curves- Diophantine Analysis ″ Springer (1978).

[**7**] R. LERCIER ″Algorithmique des Courbes Elliptiques dans les Corps Finis″ Thèse de Doctorat- Ecole Polytechnique (1997).

[8] B. MAZUR ″ Rational Isogenies of Prime Degree ″ Inv. Math.44 (1978). 129/162.

[**9**] F. MORAIN ″ Calcul du nombre de points sur une courbe elliptique dans un corps fini : aspects algorithmiques″ Jour.Théorie.Nombres - Bordeaux7 (1995)255/282.

[10] T.NAGELL″Solution de quelques problèmes dans la théorie arithmétique des cubiques planes du premier genre″ Wid.Akad.Skrifter Oslo I, (1935).

[11] SHIMURA ″ Introduction to the Arithmetic Theory of Automorphic Functions ″ ; Princeton Univ.Press(1971).

[**12**] R.SCHOOF ″ Counting points on Elliptic Curves over finite fields″. Jour. Théorie Nombres- Bordeaux7 (1995)219/254.

[13] J. H. SILVERMAN ″ The Arithmetic of Elliptic Curves ″ ; Graduate Text in Mathematics N° 106.(1986).

[14] J. T. TATE ″ The Arithmetic of Elliptic Curves ″ ; Inv. Math.23 (1974). 179/209.

[**15**] J. TUNNELL ″ A Classical Diophantine problem and Modular Forms of weight 3/2 ″ Invent. Math. 72 (1983) 323 – 334.

[16] J. VELU ″ Isogénies entre Courbes Elliptiques ″ CRAS. Paris.Ser.A 273 (26 Juillet 1971) 238/241.

[**17**] WILES ″ Modular Elliptic Curves and Fermat's Théorèm″ Ann.of Math. 142 (1995) 443/551.