N° d'ordre : 15 / 2004 – M / MT.

Ministère de l'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 M^elle HASSEN F. ZOHRA

sujet

Courbes Elliptiques sur un Corps Fini

Soutenu publiquement le : 15/07/2004, devant le jury composé de :

Mr K .BETINA	Professeur à L'U.S.T.H.B	Président.
Mr M .ZITOUNI	Professeur à L'U.S.T.H.B	Directeur de thèse.
Mr A .KESSI	Professeur à L'U.S.T.H.B	Examinateur.
Mr M.S.HACHAICHI	Maître de conférences à L'U.S.T.H.B	Examinateur.
Mr B .BENSEBAA	Chargé de cours à L'U.S.T.H.B	Examinateur.

Sommaire :

INTRODUCTION :

Dans cette thèse, nous nous sommes intéressés aux courbes elliptiques : arithmétique, géométrie et structures.

Dans le chapitre I, nous avons examiné les transformations linéaires de l'équation de Weierstrass d'une courbe elliptique.

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

L'invariant discriminant a permis une classification des cubiques ; l'invariant modulaire a donné une classification des courbes elliptiques isomorphes. Nous avons déterminé la structure du groupe de Mordell –Weil E (K) et les sous groupes de m – torsion.

Dans le chapitre II, nous avons fait un bref exposé sur les valuations d'un corps. Ces valuations entraînent des opérations de réductions de courbes elliptiques : bonnes réductions, réductions multiplicatives, réductions additives. La détermination du rang d'une courbe elliptique nécessite des fonctions particulières : les fonctions hauteurs. Une procédure de descente infinie intervient. Nous avons étudié quelques types de hauteurs : hauteurs de Weil, hauteurs de Néron – Tate, hauteurs locales.

Le 3ème chapitre est consacré au cas particulier des courbes elliptiques sur un corps fini. Nous avons montré qu'un corps fini IF_q, à q éléments, contient le sous corps fini premier $IF_p = IZ / p\,IZ$, qui est de caractéristique égale à un nombre premier $p \geq 2$; Il a une structure de IF_p - espace vectoriel de dimension fini n. Nous avons étudié le groupe de Mordell –Weil E (IF_q) ; ce groupe est d'ordre fini A_q, cet ordre satisfait un théorème de Hasse :

$$q + 1 - 2\sqrt{q} \leq A_q \leq q + 1 + 2\sqrt{q}$$

Nous avons examiné les groupes de q – torsion de ces courbes.
Ils sont de 2 types :

Le type E [q] = 0_E pour les courbes elliptiques supersingulières, et le type E [q] = $IZ / q\,IZ$ pour les courbes elliptiques ordinaires.

Il y a plusieurs critères de reconnaissance de ces 2 types :

1) Par l'invariant de Hasse,
2) Par le groupe formel $z_3 = F(z_1, z_2)$
3) Par le polynôme $H_p(t) = \sum_{i=0}^{m} \binom{m}{i}^2 t^i$

Nous avons illustré chaque chapitre par des exemples.

CHAPITRE I
THEORIE ALGEBRIQUE DES COURBES ELLIPTIQUES

Selon les spécialistes, la théorie des courbes elliptiques a des liens avec la théorie des nombres, la géométrie algébrique, l'analyse complexe.

1. *Structures algébriques*

Une courbe elliptique possède plusieurs structures algébriques :

1) Variété abélienne de dimension un;
2) Courbe algébrique projective lisse de genre un ;
3) Cubique plane non singulière d'équation spécifique de Weierstrass ;
4) Schéma séparé, intègre, de dimension un ;

chacune d'elles peut servir de définition .Nous choisissons la structure (3)

Définition 1:

Une courbe elliptique est une cubique plane, E, non singulière, irréductible, d'équation particulière de la forme :

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \qquad (1)$$

Définition 2 :

L'équation algébrique (1) est l'équation de Weierstrass de la courbe E

Dans l'équation (1), les cinq coefficients $a_1,\ldots a_6$ sont des éléments d'un corps commutatif K, global ou local ou fini.

Les deux variables x et y sont racines de l'équation algébrique (1).

Donc x et y sont des éléments d'une clôture algébrique K_{Alg} du corps K.

Ainsi, toute clôture algébrique du corps Q des nombres rationnels est un sous corps du corps C des nombres complexes.

La nature du corps de base K influe sur les propriétés de la courbe elliptique E.

Lorsque K est un corps de nombres algébriques, il s'applique à la courbe elliptique E la théorie des nombres (entiers, discriminants, idéaux, valuations, analyse p -adique, groupe de Galois, ramifications, fonctions arithmétiques, nombres premiers, équations diophantiennes …).

Lorsque K est le corps de nombres complexes, il s'applique à la courbe elliptique E l'analyse complexe (réseaux, tores, isomorphismes analytiques complexes, groupes de Lie, formes automorphes, formes modulaires …) et la géométrie algébrique (diviseurs, variétés, schémas ; courbes algébriques, homologie, cohomologie).

Lorsque K est un corps fini, il s'applique à la courbe elliptique E la théorie des corps finis.

Lorsque K est un corps de fonctions, il s'applique à la courbe elliptique E la théorie des corps de fonctions.

Lorsque K est un corps local, il s'applique à la courbe elliptique E la théorie des corps locaux.

2. Equations d'une courbe elliptique :

L'équation de Weierstrass (1) peut être transformée par des changements linéaires des variables et par des changements rationnels des variables.

Dans la suite, le symbole ZI désigne l'anneau des entiers rationnels.

Dans l'équation de Weierstrass

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \qquad (1)$$

Eliminons les monômes en y, lorsque caractéristique de K 2, par le changement de variables linéaire :

$$(x, y) \longmapsto (x, \frac{1}{2}(y - a_1 x - a_3)) \qquad (2)$$

Avec le calcul, nous obtenons l'équation de Weierstrass :

$$E_1 : y^2 = 4x^3 + b_2 x^2 + 2 b_4 x + b_6 \qquad (3)$$

Les 3 coefficients b_{2i} sont des polynômes « homogènes de degré 2 i » dans l'anneau de polynômes ZI $[a_1, a_2, a_3, a_4, a_6]$.

$b_2 = 4 a_2 + a_1^2$;

$b_4=2\,a_4 + a_1a_3$; (4)

$b_6=4\,a_6 + a_3^2$;

Eliminons les monômes en x^2 et le coefficient 4 dans (3), lorsque caractéristique de K 2, 3, par le changement de variables :

$$(x, y) \longmapsto \left(\frac{x-3b_2}{36}, \frac{y}{108}\right) \quad (5)$$

Par le calcul, nous obtenons l'équation de Weierstrass :

E_2: $y^2 = x^3 - 27c_4\,x - 54\,c_6$ (6)

Ces 2 coefficients c_{2i} sont des polynômes « homogènes de degré 2i » dans l'anneau de polynômes ZI $[b_2, b_4, b_6]$.

$c_4 = b_2^2 - 24\,b_4$;

$c_6 = -\,b_2^3 + 36\,b_2b_4 - 216\,b_6$; (7)

Dans la littérature, nous pouvons trouver d'autres formes d'équations de courbes elliptiques

1) Le modèle de Cassels :

E : $y^2=x^3 +Ax +B$, A, B∈ ZI (8)

2) Le modèle de Legendre :

E : $y^2= x(x-1)\,(x-\lambda)$; λ 1,0 (9)

3) La forme normale de Deuring :

E : $y^2+axy+y=x^3$; a^3 27, sur un corps K de caractéristique 3. (10)

4) L'équation de Tate :

E : $y^2+xy=x^3+ax+b$, à coefficients modulaires

$$a = -5\sum_{n\geq 1} n^3 q^n (1-q^n)^{-1}; b = -\frac{1}{12}\sum_{n\geq 1} q^n (7n^5 + 5n^3)(1-q^n)^{-1};$$

où q =exp (2π i z) et z = x + i y , y > 0 (11)

3. *Invariants d'une courbe elliptique :*

Toute courbe elliptique E possède plusieurs invariants, dont le discriminant Δ(E) l'invariant modulaire j(E), l'invariant différentiel ω(E),le conducteur N(E),le régulateur R(E),…

Définition 3 :

a) *Le discriminant d'une courbe elliptique E est le polynôme « homogène de degré 12 » de l'anneau ZI $[b_2, b_4, b_6, b_8]$*

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

où l'on a posé:

$$4b_8 = b_2 b_6 - b_4^2$$

et caractéristique (K)≠ 2 , 3

b) *L'invariant modulaire d'une courbe elliptique E est 1'élément :*

$$j(E) = c_4^3 / \Delta(E) = 1728\, c_4^3 / [c_4^3 - c_6^2] \qquad (13)$$

c) *L'invariant différentiel d'une courbe elliptique est l'élément différentiel*

$$\omega(E) = \frac{dx}{2y + a_1 x + a_3} = \frac{dy}{3x^2 + 2a_2 x + a_4 - a_1 y} \qquad (14)$$

4. Résultant de polynômes et classification des cubiques planes :

L'équation de Weierstrass d'une courbe elliptique E se met sous la forme :

$$y^2 = f(x)$$

L'étude des points singuliers et du discriminant de $f(x)$ peut être menée avec la théorie du résultant de 2 polynômes.

Définition 4 :

Le résultant de 2 polynômes de l'anneau K[x],

$f(x) = d_0 x^n + d_1 x^{n-1} + \ldots + d_n$ de degré n et

$g(x) = r_0 x^s + r_1 x^{s-1} + \ldots + r_s$ de degré s

est le déterminant d'ordre n + s

$$Res(f,g)=\begin{vmatrix} d_0 & d_1 & . & . & . & d_n & 0 & . & . & . \\ 0 & d_0 & d_1 & . & . & . & d_n & 0 & . & . \\ . & . & . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & 0 & d_n & . \\ 0 & . & . & . & . & 0. & d_0 & . & . & d_n \\ r_0 & r_1 & . & r_s & 0 & . & . & . & . & . \\ 0 & r_0 & r_1 & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . & . & . \\ 0 & . & . & . & . & 0 & r_0 & r_1 & . & r_s \end{vmatrix}$$

Avec n lignes de $(d_0, \ldots, d_n)$ *et s lignes de* $(r_0, \ldots, r_s)$.

Ce résultant possède plusieurs propriétés (« Algebra » de S .Lang ; « Introduction à l'algèbre » de Kostrikin) que nous énonçons sans démonstration.

Proposition 1 :

L e résultant des 2 polynômes f(x) et g(x) est une fonction polynomiale homogène des racines $\theta_1, \theta_2, \ldots, \theta_n$ *de f(x) et* $\alpha_1, \alpha_2, \ldots, \alpha_s$ *de g(x) :*

$$Res(f,g) = d_0^s r_0^n \prod_{1\le i\le n;\, 1\le j\le s} (\theta_i - \alpha_j) = d_0^s \prod_{i=1}^{n} g(\alpha_i)$$

$$= (-1)^{ns} r_0^n \prod_{j=1}^{s} f(\theta_j)$$

Il en résulte la relation :

Res (f , g) = (- 1)$^{n\,s}$ Res (g , f).

Pour un polynôme fg et un polynôme u, leurs résultants sont déterminés par :

Proposition 2 :

Soient 3 polynômes f(x), g(x) et u(x).Alors les résultants satisfont la relation :

Res (f g , u) = Res (f , u) Res (g , u).

La proposition 1 donne un moyen de reconnaître 2 polynômes de résultant nul.

Proposition 3 :

Soit les 2 polynômes $f(x)$ et g(x) ci-dessus.
Leur résultant Res (f, g) est nul si et seulement si ces 2 polynômes ont une racine commune.

Dans le cas particulier d'un polynôme f(x) et de sa dérivée f`(x), le résultant de ces 2 polynômes est déterminé par la :

Proposition 4 :

Le résultant d'un polynôme de degré n

$$f(x) = d_0 x^n + d_1 x^{n-1} + \ldots + d_n$$

et de sa dérivée f `(x) est égal à :

$$Res\ (f, f\ `) = d_0^{n-1} \prod_{1 \le i \le n} f'(\theta_i)$$

Le discriminant d'un polynôme f(x) est une fonction polynomiale de ses racines.

Définition 5 :

Le discriminant d'un polynôme de degré n

$$f(x) = d_0 (x - \theta_1)\ldots(x - \theta_n)$$

est égal à :

$$dis\ (f) = d_0^{2n-2} \prod_{1 \le i \pi\, j \le n} (\theta_i - \theta_j)^2$$

Le discriminant de f et le résultant de f sont liés par la :

Proposition 5 :

Soit un polynôme f(x) de degré n, son discriminant dis (f) et son résultant Res (f,f `).Alors :

$$Res\ (f, f\ `) = dis(f).d_0.(-1)^{\frac{n(n-1)}{2}}$$

Exemples:

1) Soit une courbe elliptique E d'équation de Weierstrass

$y^2 = f(x) = x^3 + A\,x + B$; avec $4A^3 + 27B^2 \neq 0$

le discriminant de f est égal à :

$dis\,(f) = -(4A^3 + 27B^2)$

2) Le discriminant d'un polynôme cubique

$f(x) = d_0 x^3 + d_1 x^2 + d_2 x + d_3$

est égal à :

$$dis\,(f) = 18\,d_0d_1d_2d_3 + d_1^2d_2^2 - 4\,d_0d_2^3 - 4\,d_1^3d_3 - 27\,d_0^2d_3^2 \qquad (2)$$

3) Le discriminant d'un polynôme cubique

$f(x) = 4x^3 + b_2 x^2 + 2b_4 x + b_6$

est égal à :

$dis\,(f) = 16(9\,b_2b_4\,b_6 - 8\,b_4^3 - 27b_6^2 - b_2^2b_8)$.

Il en résulte une relation entre les discriminants $dis\,(f)$ du polynôme f et le discriminant $\Delta(E)$ de la courbe elliptique

Proposition 6 :

Soit une courbe elliptique E d'équation de Weierstrass :

$E : y^2 = 4x^3 + b_2 x^2 + 2b_4 x + b_6 = f(x)$.

Alors les discriminants $dis\,(f)$ de f et $\Delta(E)$ de E satisfont la relation :

$dis\,(f) = 16\,\Delta(E)$

Grâce aux propositions 3,5et 6 nous pouvons déterminer les cubiques singulières, les cubiques non singulières et le signe des discriminants de f et de la cubique.

Lorsque $Res\,(f, f`) = 0$, le polynôme $f(x)$ admet une racine double ou triple ; donc la cubique est singulière.

Lorsque $Res\,(f, f`) \neq 0$, le polynôme $f(x)$ admet 3 racines simples ; il en résulte que la cubique est une courbe elliptique.

Proposition 7:

Soit une cubique plane C d'équation $y^2 = f(x)$, de discriminant $\Delta(C)$.
Alors :

1) *La cubique C est singulière si et seulement si $\Delta(C) = 0$,*
2) *La cubique C est une courbe elliptique si et seulement si $\Delta(C)$ 0,*

Preuve de « $\Delta(C) = 0$ » implique « la cubique C est singulière » :

Soit une cubique C d'équation $y^2 = f(x)$ et discriminant $\Delta(C)=0$;
La théorie du résultant d'un polynôme et de sa dérivée implique Res $(f, f`)=0$.

Il en résulte que le polynôme f admet une racine double.
Donc la cubique C est singulière ; ce n'est pas une courbe elliptique.

Preuve de « $\Delta(C)$ 0 » implique « la cubique C est une courbe elliptique » :

L'hypothèse « $\Delta(C)$ 0 » implique un résultant Res $(f, f`)$ 0.
Donc le polynôme cubique f admet 3 racines simples ; la cubique C n'est pas singulière ; c'est une courbe elliptique.

Nous ne ferons pas les 2 autres preuves.

Lorsque la cubique C est singulière, elle admet un point singulier ; ce point est soit un nœud, soit un point de rebroussement .La nature du point singulier est déterminée par l'invariant $c_4(C) = b_2^2 - 24\, b_4$,

Proposition 8:

Soit une cubique C d'équation de Weierstrass
$$y^2 = 4x^3 + b_2 x^2 + 2 b_4 x + b_6 = f(x)$$
et d'invariants $c_4(C)$ et $\Delta(C)$.

1) *Cette cubique C admet un nœud si et seulement si $c_4(C)$ 0 et $\Delta(C) = 0$.*
2) *La cubique C admet un point de rebroussement si et seulement si $c_4(C) = 0 = \Delta(C)$.*

Preuve de « $\Delta(C) = 0$ et $c_4(C)$ 0 » implique « la cubique C admet un nœud » :

Par la proposition 7 précédente, l'hypothèse « $\Delta(C)= 0$ » implique que la cubique est singulière ; soit S son point singulier ; (1)
En ce point S, la cubique C admet 2 tangentes, distinctes ou confondues.
Les pentes de ces tangentes sont égales à la dérivée y`de y. (2)

Le calcul de la dérivée donne :

$$y` = \frac{6x^2 + b_2x + b_4}{y} = \frac{g(x)}{y} \qquad (3)$$

Le numérateur g(x) est un polynôme de degré 2.Son discriminant est égal à

$$dis\ (g) = b_2^2 - 24\, b_4 = c_4(C). \qquad (4)$$

L'hypothèse « $c_4(C)$ 0 » implique 2 tangentes distinctes.

Il en résulte que la cubique C admet un nœud. (5)

Preuve de « $\Delta(C) = c_4(C) = 0$ » implique « le point S est un point de rebroussement » :

Reprenons les formules de (1) à (4) ci-dessus

L'hypothèse « $c_4(C) = 0$ » implique une racine double, donc 2 tangentes confondues. (6)

Il en résulte que la cubique C admet un point de rebroussement.

Nous ne ferons pas les preuves des réciproques.

Le nombre de points d'intersection d'une courbe elliptique par l'axe Ox est déterminé par le signe du discriminant.

Proposition 9 :

Soit une courbe elliptique E, de discriminant $\Delta(E)$ .Alors :

1) *E coupe Ox en 3 points, simples, si et seulement si $\Delta(E) > 0$.*
2) *E coupe Ox en 1 seul point, simple, si et seulement si $\Delta(E) < 0$.*

Preuve de «E coupe Ox en 3 points simples » implique « $\Delta(E) > 0$ » :

Soit une courbe elliptique E qui coupe l'axe Ox en 3 points simples

$P_i = (e_i, 0)$, pour i = 1, 2, 3 (1)

L'équation de Weierstrass de E se met sous la forme :

$$E : y^2 = (x-e_1)(x-e_2)(x-e_3) = f(x) \qquad (2)$$

Par la théorie des multiplicités des racines d'un polynôme, $f(x)$ et sa dérivée $f`(x)$ n'ont pas de racine commune. (3)

Il en résulte que le résultant Res (f, $f`$) 0 n'est pas nul.

Par définition du discriminant d'un polynôme $f(x) = \prod_i (x - e_i)$, le discriminant de f est égal à :

$$dis\ (f) = \prod_{i \pi j} (e_i - e_j)^2 \ ; \qquad (4)$$

Par hypothèse, les 3 racines sont des nombres réels, cela implique que les carrés sont positifs et dis (f) >0 (5)

La relation entre Res (f, f`) et discriminants dis (f) de f et Δ(E) de E implique Δ(E) >0. (6)

Preuve de «E coupe Ox en 1 point simple » implique « Δ(E) <0 » :

L'équation de Weierstrass d'une telle courbe elliptique E est de la forme :

$E : y^2=(x-e)(x^2+rx+s) = f(x)$ avec $r^2-4s<0$ (7)

La condition (7) implique 2 racines complexes de $f(x)$

$$x_j = -\frac{1}{2}(r \pm i\sqrt{4s - r^2}) \text{ avec } j = 1,2 \text{ et } 4s - r^2 >0. \quad (8)$$

La formule (4) du discriminant d'un polynôme f donne :

$$\text{dis}(f) = (e - x_1)^2(e - x_2)^2(x_1 - x_2)^2$$

$$\text{dis}(f) = -4(4s - r^2)^2[(e - \frac{1}{2}r)^2 + (4s - r^2)^2]^2 <0 \quad (9)$$

La relation entre Res (f, f`) et discriminants dis (f) de f et Δ(E) de E implique Δ(E) <0. (10)

Les propositions 7, 8 et 9 impliquent la classification des cubiques planes :

Corollaire :

Les cubiques planes E sont classifiées en 4 classes selon leur discriminant Δ(E) et leur invariant $c_4(E)$:

1) Classe (Cl1) des cubiques planes singulières qui ont un nœud :

Δ(E) =0 et $c_4(E) \neq 0$.

2) Classe (Cl2) des cubiques planes singulières qui ont un point de rebroussement :

Δ(E) = $c_4(E) = 0$.

3) Classe (Cl3) des courbes elliptiques qui coupent l'axe Ox en un seul point :

Δ(E)< 0.

4) Classe (Cl4) des courbes elliptiques qui coupent l'axe Ox en 3 points :

Δ(E)> 0.

Exemples :

1) courbe elliptique qui coupe l'axe Ox en un seul point :

Soit la cubique E_1 d'équation de Weierstrass :

$E_1 : y^2 = x^3 - x^2 + 17x + 87$

Calcul des invariants :

$b_2 = -4$; $b_4 = 34$; $c_4 = -800$; $b_6 = 348$; $\Delta(E_1) = -2^4 \times 3^3 \times 5 < 0$

Le discriminant $\Delta(E_1) < 0$ implique que la cubique E_1 est une courbe elliptique qui coupe l'axe Ox en 1 seul point, R.

Si ce point R a une abscisse x_R entière, alors l'équation diophantienne :

$x^3 - x^2 + 17x + 87 = 0$

admet une solution x_R qui divise le coefficient constant 87.

Par le calcul nous obtenons la valeur $x_R = -3$.

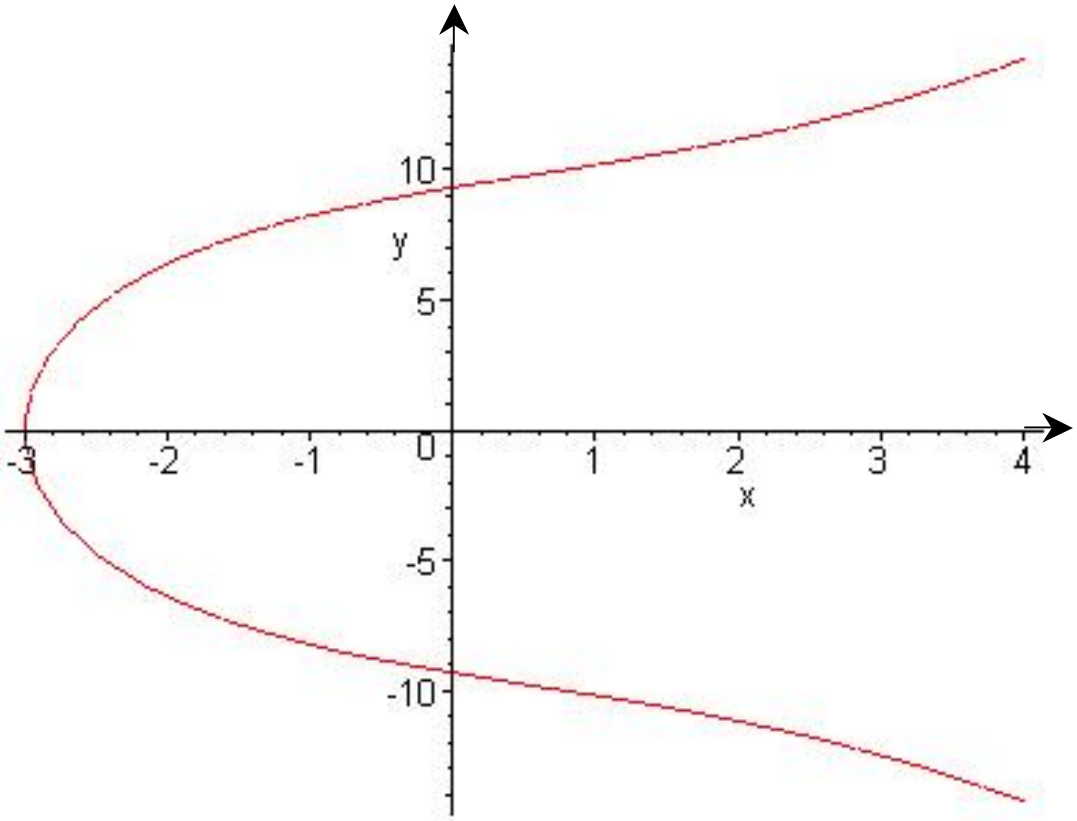
L'équation de E_1 se met sous la forme :

$y^2 = (x+3)(x^2 - 4x + 29)$.

Tableau de coordonnées de quelques points de E_1 :

x	-4	-3	-2	-1	0	1	2	3
y^2	-61	0	41	68	87	104	125	180
y	Non	0	$\pm\sqrt{41}$	$\pm 2\sqrt{17}$	$\pm\sqrt{87}$	$\pm 2\sqrt{26}$	$\pm 5\sqrt{5}$	$\pm 6\sqrt{5}$

.



2) courbe elliptique qui coupe l'axe Ox en 3 points :

cubique E_2 d'équation de Weierstrass :

$E_2 : y^2 = x^3 + 3x^2 - 13x - 15 = f(x)$

Calcul des invariants :

$b_2 = 12$; $b_4 = -26$; $b_6 = -60$; $c_4 = 768^2$; $\Delta(E) = 2^4 \times 3^3 \times 7 > 0$

Le discriminant $\Delta(E) > 0$ implique que la cubique E_2 est une courbe elliptique qui coupe l'axe Ox en 3 points simples.

Pour trouver des racines entières de l'équation diophantienne

$f(x) = 0$;

Nous testons les diviseurs de 15 :

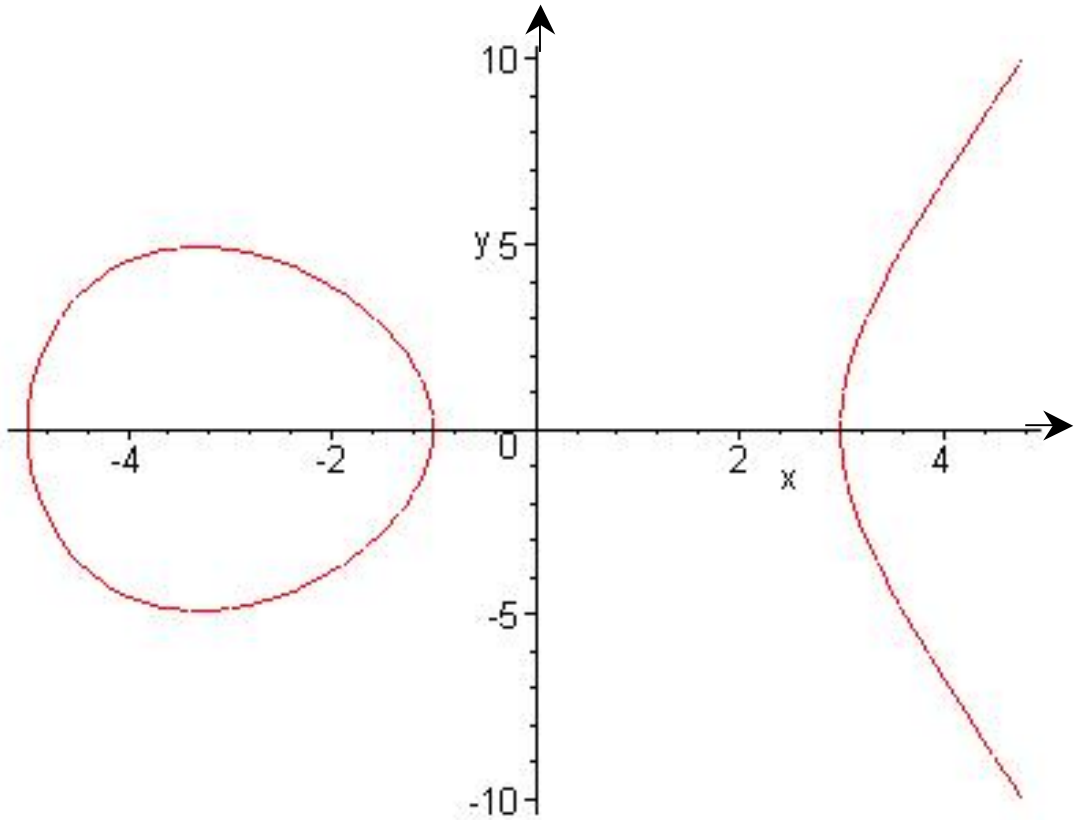
$d = \pm 1, \pm 3, \pm 5$ et ± 15

Le calcul donne 3 racines entières :

$e_1 = -5$, $e_2 = -1$ et $e_3 = 3$

Tableau de coordonnées de quelques points de E_2 :

x	-5	-4	-3	-2	-1	0	1	2	3	4	5
y^2	0	21	24	15	0	-15	-24	-21	0	45	120
y	0	$\pm\sqrt{21}$	$\pm 2\sqrt{6}$	$\pm\sqrt{15}$	0	Non	Non	Non	0	$\pm 3\sqrt{5}$	$\pm 2\sqrt{30}$



3) cubique avec un nœud :

cubique E_3 d'équation de Weierstrass :

$E_3 : y^2 = x^3 - 3x + 2$

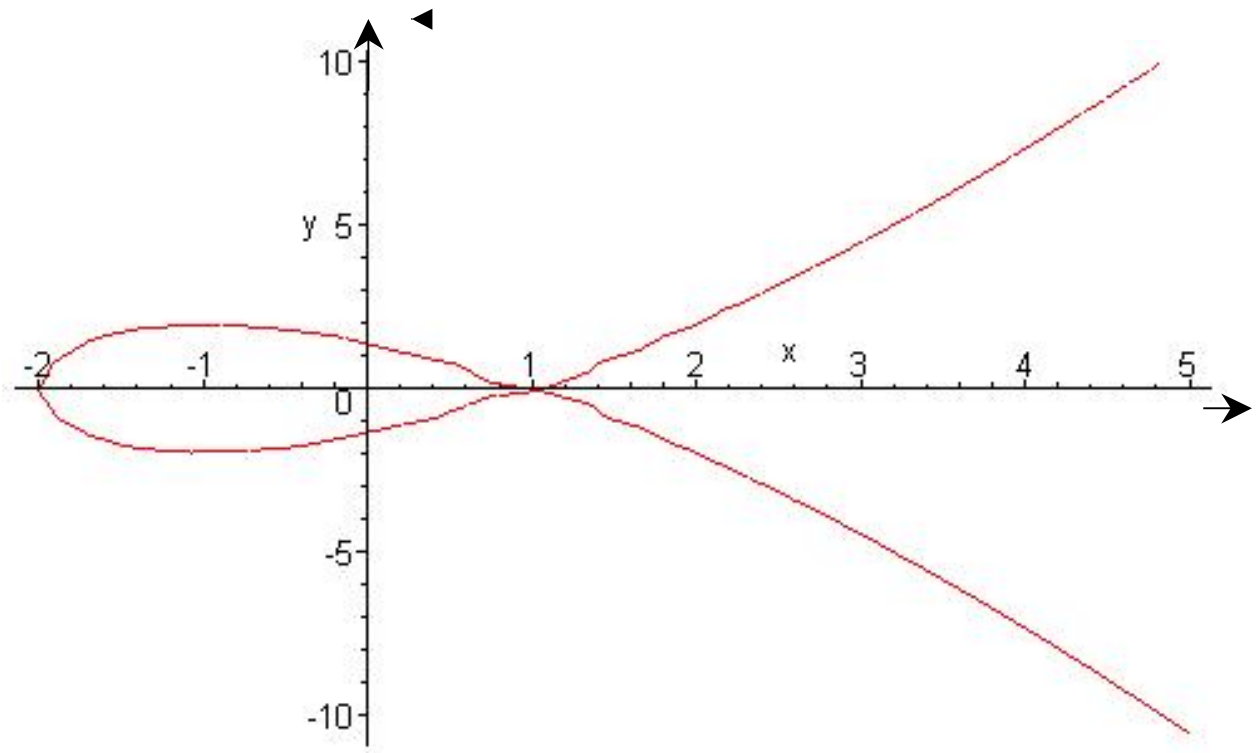
Calcul des invariants :

$b_2 = 0$; $b_4 = -6$; $b_6 = 8$; $c_4 = 144$; $\Delta(E) = 0$.

Les valeurs $c_4 \neq 0$ et $\Delta(E) = 0$ impliquent que cette cubique singulière admet un nœud au point (1,0).

Tableau de coordonnées de quelques points de E_3:

x	-2	-1	0	1	2	3	4
y^2	0	4	2	0	4	20	54
y	0	± 2	$\pm\sqrt{2}$	0	± 2	$\pm\sqrt{20}$	$\pm\sqrt{54}$



4) cubique avec un point de rebroussement :

cubique E_4 d'équation de Weierstrass :

$E_4 : y^2 + 2xy + 2y = x^3 - x^2 - 2x - 1$

Le calcul des invariants donne :

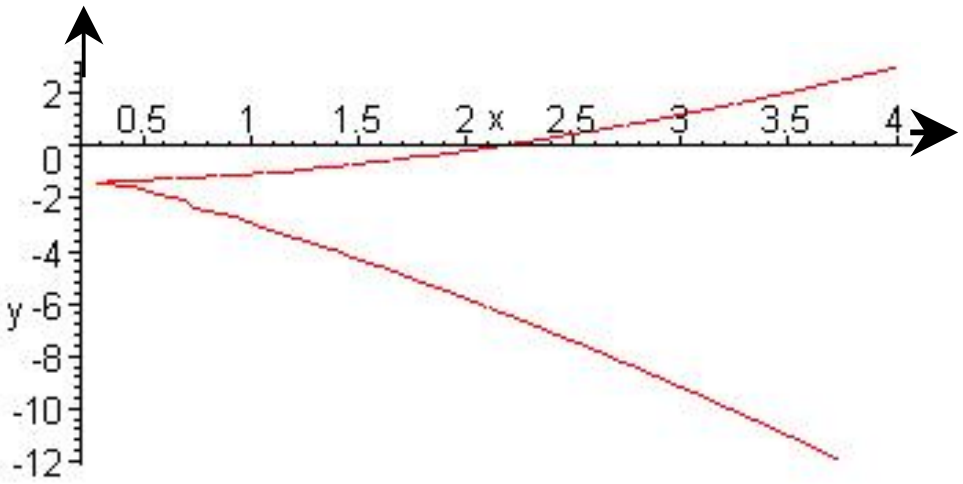
$b_2 = b_4 = b_6 = 0$; $c_4 = 0$; $\Delta(E_4) = 0$.

$c_4 = \Delta(E_4) = 0$ implique que cette cubique admet un point de rebroussement S.

Tableau de coordonnées de quelques points de la cubique :

x	-1	0	1	2	3	4
y	Non	-1 racine double	-1 et -3	$-3 \pm \sqrt{8}$	$-4 \pm \sqrt{27}$	3 et -13

Le tableau indique que le point de rebroussement est S = (0,-1).



5. Plans affines, plans projectifs, variétés abéliennes :

Une cubique plane X a une équation algébrique de la forme :

$$d_1y^3 + d_2x^3 + d_3y^2x + d_4yx^2 + d_5y^2 + d_6x^2 + d_7xy + d_8y + d_9x + d_{10} = 0 \quad (1)$$

son équation de Weierstrass est égale à :

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad (2)$$

Les 10 coefficients $d_1, \ldots, d_{10}$ et les 5 coefficients $a_1, \ldots, a_6$ sont des éléments d'un corps commutatif K.

Les deux variables x et y sont des éléments d'une clôture algébrique du corps K ; ce sont les coordonnées affines d'un point P = (x, y) du plan affine de dimension 2.

Définition 6 :

Un plan affine, de dimension n sur un corps algébriquement clos k, est l'espace $IA^n(k)$ des n – uplets $t = (t_1, \ldots, t_n)$, d'éléments $t_1, \ldots, t_n$ de k.

Avec l'addition

$$(t_1, \ldots, t_n) + (t`_1, \ldots, t`_n) = (t_1+t`_1, \ldots, t_n+t`_n) \quad (3)$$

et la multiplication par les scalaires

$$\lambda\,(t_1, \ldots, t_n) = (\lambda t_1, \ldots, \lambda t_n) \quad (4)$$

Le plan affine IA^n (k) est muni d'une structure de variété algébrique affine de dimension n sur un corps k avec la topologie de Zariski.

Exemples :

Variétés affines IA^1 (IR), IA^2 (IR), IA^1(C), IA^2 (C), IA^3 (C),…

Dans une variété affine IA^n (k), la relation $\Re$

$(t_1, \ldots, t_n)\ \Re\ (t`_1, \ldots, t`_n)$ si et seulement si

$(t`_1, \ldots, t`_n) = \lambda\,(t_1, \ldots, t_n)$ pour un scalaire λ non nul, (5)

est une relation d'équivalence ;cette relation $\Re$ détermine donc des classes d'équivalence dans l'espace quotient .

Définition 7 :

Le plan projectif, de dimension n sur un corps k, est l'espace quotient

$IP^n(k) = IA^{n+1}(k) - \{0\} / \Re$

par la relation $\Re$ d'équivalence .

C'est donc un ensemble de classes.

Avec les opérations sur les classes d'équivalence, le plan projectif $IP^n(k)$ devient la variété projective $IP^n(k)$.

Donc tout point P de $IP^n(k)$ admet n + 1 coordonnées homogènes.

Exemples :

La variété projective $IP^1(IR) = \{cl(a, b) ; (a, b) \neq (0, 0)\}$

La variété projective $IP^2(IR) = \{cl(a, b, c) ; (a, b, c) \neq (0, 0, 0)\}$

L'équation de Weierstrass d'une cubique C dans le plan projectif $IP^2(k)$ est un polynôme homogène,de degré 3,en x , y , z :

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3 \qquad (6)$$

Une variété projective X peut être munie d'une structure de variété abélienne de dimension n.

Pour cela il faut que X soit non singulière, irréductible et admet une loi de groupe abélien

$X \times X \to X$ de valeur $(a, b) \to a+b$

et une loi :

$X \to X$ de valeur $a \to a^{-1}$

Ces notions de variétés algébriques se trouvent dans des ouvrages de géométrie algébrique (« Algebraic Geometry » de HARTSORNE, « Basic Algebraic Geometry » de SHAFAREVICH, etc. …)

Il en résulte qu'une courbe elliptique a une structure de variété abélienne de dimension 1. La théorie des diviseurs est un outil mathématique employé pour étudier certains aspects géométriques, algébriques des courbes elliptiques.

6. Groupe de Mordell-Weil d'une courbe elliptique:

6.1. Soit une courbe elliptique E, sur un corps K, d'équation de Weierstrass :

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

Proposition 10 :

Le point à l'infini $O_E = (0, 1, 0)$ est un point non singulier sur la courbe elliptique E.

Preuve :

Considérons l'équation projective de E :

$$f(x, y, z) = y^2z + a_1xyz + a_3yz^2 - x^3 - a_2x^2z - a_4xz^2 - a_6z^3 \in K[x, y, z] \quad (1)$$

Au point O_E, la fonction prend la valeur

$$f(O_E) = f(0, 1, 0) = 0 ; \quad (2)$$

Cela implique les coordonnées du point $O_E = (0, 1, 0)$ satisfont l'équation projective de E

Il en résulte que le point à l'infini O_E est sur la courbe E.

La dérivée partielle

$$f'_z = y^2 + a_1xy + 2a_3yz - a_2x^2 - 2a_4xz - 3a_6z^2 \quad (3)$$

ne s'annule pas au point $O_E = (0, 1, 0)$;donc le point O_E n'est pas singulier.

Construisons un groupe abélien additif avec la :

Proposition 11 :

Soit une courbe elliptique E, et le point à l'infini $O_E = (\infty, \infty) = (0, 1,0)$.

Alors, 1 'ensemble E (K) des points K rationnels de E, muni de l'application :

$$f : E(K) \times E(K) \longrightarrow E(K) \text{ ,avec}$$

$$(P_1, P_2) \longrightarrow P_1 + P_2$$

basée sur « la règle géométrique de 3 points colinéaires $P + Q + R = O_E$ »,

est un groupe additif abélien d'élément neutre le point O_E.

Preuve :

Soit l'ensemble E (K) des points K - rationnels de la courbe E.

Le point O_E, unique par ses coordonnées projectives, est déterminé par la direction de l'axe Oy.

Considérons l'application :

$$T : E(K) \times E(K) \longrightarrow E(K),$$

de valeur $T(P_1, P_2) = P_1 + P_2$

Le point $P_1 + P_2$ est déterminé par la règle géométrique :

« Trois points colinéaires P_1, P_2, P_3 d'une courbe elliptique E ont une somme nulle »:

$$P_1 + P_2 + P_3 = O_E$$

Vérifions que cette application T satisfait les 4 axiomes d'un groupe abélien :

Axiome de l'élément neutre :

C'est le point O_E à 1'infini qui joue le rôle d'élément neutre.

Pour tout point P de E (K), la sécante PO_E est parallèle à l'axe Oy.

La règle des 3 points colinéaire implique :

$$P + O_E = O_E + P = P \qquad (1)$$

Axiome du symétrique

Soit une sécante parallèle à l'axe Oy qui coupe la courbe C en 3 points P_1, P_2 et O_E

Il en résulte la relation :

$$P_1 + P_2 + O_E = O_E \qquad (2)$$

Nous en déduisons le symétrique :

$$P_1 = - P_2 \qquad (3)$$

Axiome de commutativité

Les sécantes P_1P_2 et P_2P_1 sont confondues ;

$$P_1 + P_2 = P_2 + P_1 \qquad (4)$$

Axiome d'associativité

Il se vérifie par les calculs des coordonnées des points

$(P_1 + P_2) + P_3$ et $P_1 + (P_2 + P_3)$, pour des points $P_i \neq \pm P_j$.

Définition 8:

Le groupe E (K) des points K -rationnels d'une courbe elliptique E est le groupe de Mordell-Weil de la courbe elliptique E.

6.2. Coordonnées du symétrique et de la somme dans le groupe E (K) :

Soit une courbe elliptique E d'équation de Weierstrass :

$$E : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \qquad (1)$$

Déterminons les coordonnées des points - P et P_1+P_2

Calcul des coordonnées du symétrique - P d'un point P (fig. 1):

Le point -P satisfait la relation $P + (-P) = O_E$

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

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

Il en résulte que l'équation (1) est de degré 2 en y ;

Les calculs donnent les coordonnées du symétrique -P de P

$$- P = - (x, y) = (x, - y - a_1 x - a_3) \qquad (2)$$

Calcul des coordonnées, du point somme $P_1 + P_2$ où $P_1 \neq \pm P_2$: (fig2)

Soit les points $P_1 = (x_1, y_1)$ et $P_2 = (x_2, y_2)$

La somme est déterminée par la règle géométrique :

$P_1 + P_2 + P_3 = O_E$

Cela implique $P_1 + P_2 = - P_3 = M$

Les coordonnées du point P_3 sont calculées avec la théorie analytique de l'intersection de 2 courbes planes.

Equation de la sécante P_1P_2 :

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

Cette sécante P_1P_2 coupe la courbe en trois points simples P_1, P_2 et P_3

Les abscisses de ces 3 points sont les zéros de l'équation du 3ème degré en x ;

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

La somme de ces zéros est une fonction symétrique élémentaire des zéros du polynôme :

$$x_1 + x_2 + x_3 = \lambda^2 + a_1\lambda - a_2$$

Les calculs donnent les coordonnées de la somme $P_1 + P_2 = - P_3 = M$

$$\begin{cases} x_M = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2 \\ y_M = -\lambda^3 - 2a_1\lambda^2 + \lambda(a_2 + 2x_1 + x_2 - a_1^2) + a_1a_2 - a_3 - y_1 + a_1(x_1 + x_2) \end{cases} \quad (3)$$

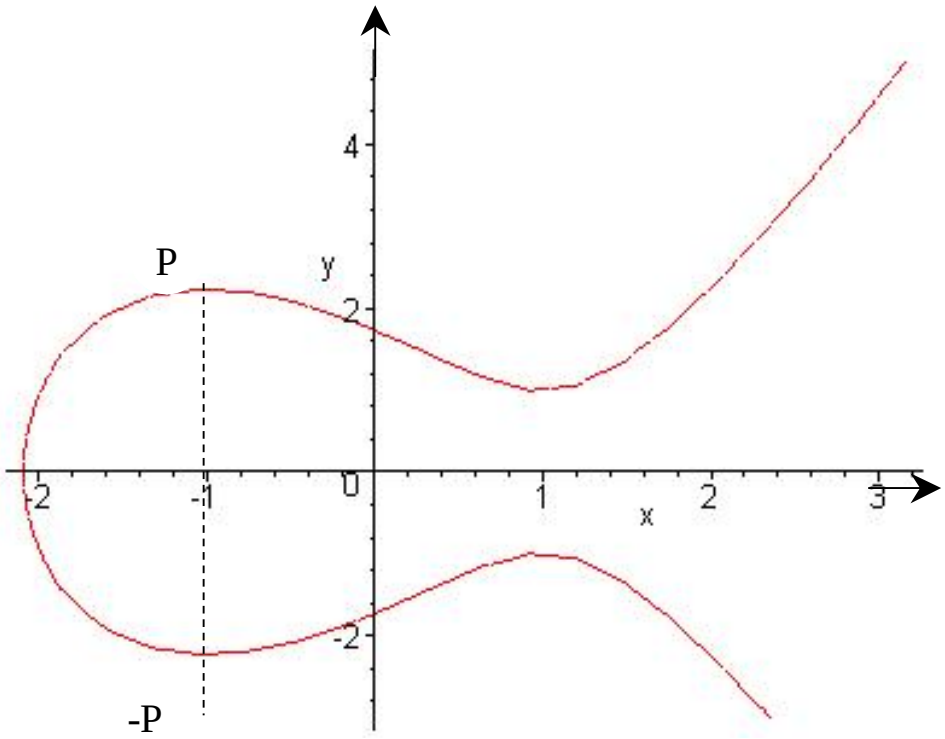


Figure 1

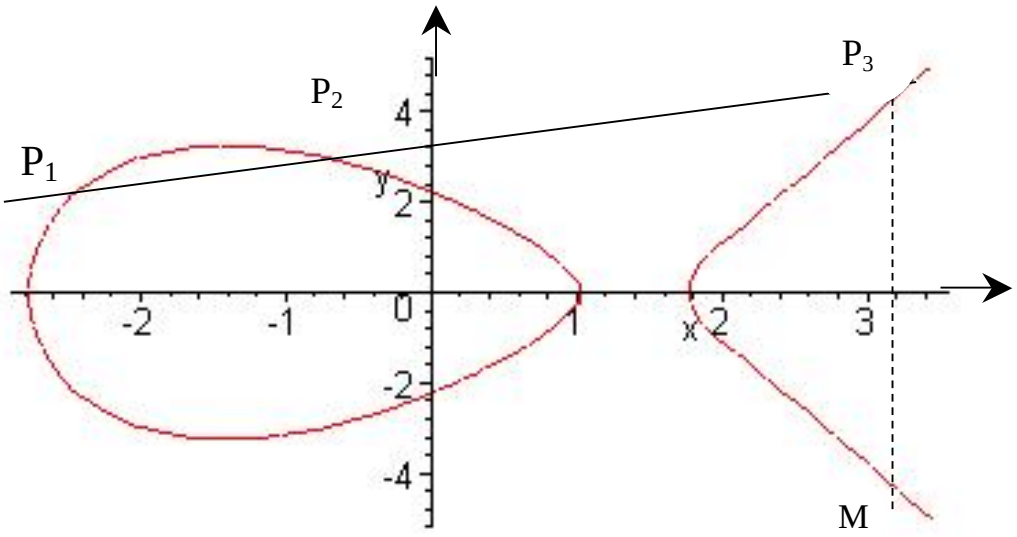


Figure 2

Nous avons démontré la

Proposition 12 :

Soit une courbe elliptique E d'équation de Weierstrass :

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

1) le symétrique – P d'un point P = (x_p, y_p) de E a pour coordonnées

$$- P = (x, y) \text{ avec } x = x_p,\ y = - y_p - a_1 x_p - a_3$$

2) la somme $P_1 + P_2 = M$ de 2 points $P = (x_i, y_i)$ de E, $P_1 \pm P_2$ a pour coordonnées :

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

6.3. Coordonnées des points mP et sous groupe de m - torsion :

Lorsque $P_1 = P_2 = P$ la sécante P_1P_2 devient une tangente à la courbe au point P, cette tangente recoupe E en un point simple R.

La règle des 3 points colinéaires implique la relation :

$$P + P + R = 2P + R = 0_E \qquad \text{(sur la figure 2)} \qquad (1)$$

Pour obtenir les coordonnées du point 2P, nous utilisons la théorie analytique de l'intersection d'une courbe par une tangente.

Pente de la tangente à E en un point P = (x_p, y_p) :

$$y'_p = \frac{3x_p^2 + 2a_2x_p + a_4 - a_1y_p}{2y_p + a_1x_p + a_3} \qquad (2)$$

Equation de la tangente :

$$y = y'_p(x - x_p) + y_p \quad ; \qquad (3)$$

L'équation algébrique de E et la relation (3) impliquent une équation algébrique du 3ème degré en x, dont les racines sont x_p , double, et x_R simple.

La fonction symétrique élémentaire des racines donne l'abscisse :

$$x_{2P} = y'^2_p + a_1y'_p - a_2 - 2x_p \quad ;$$

Avec la formule du symétrique, nous obtenons l'ordonnée.

$$y_{2P} = -y'^3_p + 2a_1y'^2_p + (a_2 - a_1^2 - 3x_p)y'_p + a_1a_2 - a_3 + 2a_1x_p - y_p \qquad (4)$$

Nous avons démontré la

Proposition13 :

Soit une courbe elliptique E d'équation de Weierstrass :

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

Les coordonnées du point P + P= 2P de E sont :

$$\begin{cases} x_{2P} = y'^2_p + a_1y'_p - a_2 - 2x_p \\ y_{2P} = -y'^3_P + a_1y'^2_P + (a_2 - a_1^2 - 3x_P)y'_P + a_1a_2 - a_3 + 2a_1x_P - y_P \\ y'_P = \dfrac{3x_P^2 + 2a_2x_P + a_4 - a_1y_P}{2y_P + a_1x_P + a_3} \end{cases}$$

Pour tout entier rationnel m, et pour tout point P de la courbe E, le symbole mP signifie :

mP = P + P + . . .+ P , m fois P lorsque m>0 ;

mP = (-m)(-P) = (-P) + (-P) + . . . + (-P),(-m) fois –P ,lorsque m<0

et $0P = 0_E$ lorsque m = 0.

Les coordonnées d'un point mP peuvent être obtenues par application des formules de la somme $P_1 + P_2$ et du point 2P.

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

Il existe des formules de récurrence que l'on trouve dans l'article de « Cassels » : « Diophantine Equations with special references to elliptic cruves, Jour.London Math.Soc 41(1966)193-291»

Proposition 14 :

Soit une courbe elliptique E sur le corps Q des rationnels, d'équation de Weierstrass :

$E: y^2 = x^3 + A\,x + B$ *avec* $4A^3 + 27\,B^2 \neq 0$

Les coordonnées des points m P, pour m>2, sont déterminées par les formules :

$$m\,P = \left(\frac{\phi_m(x,y)}{\psi_m^2(x,y)}, \frac{\omega_m(x,y)}{\psi_m^3(x,y)} \right);$$

Les polynômes ψ_m *satisfont les relations de récurrence :*

$\psi_{-1} = -1,\ \psi_0 = 0,\ \ \psi_1 = 1,\ \psi_2 = 2\,y,\ \ \psi_3 = 3x^4 + 6Ax^2 + 12Bx - A^2$

$\psi_4 = 4y\,(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3)$

$$\psi_{2m} = 2\psi_m\,(\psi_{m+2}\ \psi_{m-1} - \psi^2_{m-2}\ \psi^2_{m+1})$$

$$\psi_{2m+1} = \psi_{m+2}\,\psi^3_m - \psi^3_{m-1}\psi^3_{m+1} \qquad \text{pour } m \geq 2$$

Les polynômes numérateurs ϕ_m et ψ_m satisfont les relations de récurrence :

$$\phi_m = x\psi m^2 - \psi_{m-1}\,\psi_{m+1}$$

$$4\,y\omega_m = \psi_{m+2}\,\psi^2_{m-1} - \psi_{m-2}\,\psi^2_{m+1}$$

Preuve :

La formule – P = (x,-y) implique

$-\,y = \frac{y}{(-1)^3}$ et $x = \frac{x}{(-1)^2}$; donc $\psi_{-1} = -1$

La formule 0P = (∞,∞) implique

$x = \frac{x}{0}$ et $y = \frac{y}{0}$; donc $\psi_0 = 0$

La formule 1P = (x, y) implique

$x = \frac{x}{(1)^2}$ et $y = \frac{y}{(1)^2}$; donc $\psi_1 = 1$

La formule 2 P = (x_{2P}, y_{2P}) avec $y` = \frac{3\,x^2 + A}{2\,y}$ implique

$\psi_2 = 2\,y$

Un raisonnement par récurrence permet de démontrer cette proposition.

Lemme 7.2.Cassels.

Définition 9 :

1) Un point de m -torsion d'une courbe elliptique E est un point P d'ordre m dans le groupe de Mordell -Weil de E.

$$m\,P = 0_E\,.$$

2) Un sous groupe de m -torsion de E est l'ensemble E (K) [m]=E[m] des points d'ordre m.

3) Le groupe de torsion de la courbe E est la réunion infinie des sous groupes de m -torsion de E :

$$T(E) = \bigcup_m E[m] = \{P \in E\,(K)\ ; m\,P = 0_E \text{ pour } m \in Z\}$$

La structure du groupe de Mordell -Weil est précisée par la:

Proposition 15:

Le groupe E (K) de Mordell - Weil d'une courbe elliptique E, est un groupe abélien de type fini.

Preuve :

Elle se décompose en 2 parties : dans l'une il faut prouver que le groupe quotient E (K)/m E (K) est fini pour m = 2 ; dans l'autre il faut appliquer une «descente infinie » au moyen de fonctions particulières : fonctions hauteurs $E(K) \rightarrow IR$

Corollaire:

Soit les hypothèses de la proposition 5.

Le groupe E (K) de Mordell - Weil d'une courbe elliptique E, est isomorphe à un produit de groupes abéliens

$$E(K) \approx T(E) \times ZI^{r}$$

où T(E) désigne le groupe de torsion de la courbe elliptique E , ZI^{r} désigne r copies du groupe abélien ZI, r = r (E) est un entier naturel non négatif.

Définition 10 :

L'entier r = r (E) est le rang de la courbe elliptique E.

Le groupe T(E) de torsion d'une courbe elliptique est fini, selon les spécialistes (Mazur, Cassels, Tate,…)

Citons le cas particulier de torsion sur le corps Q des rationnels :

Proposition 16 :

Le groupe de torsion d'une courbe elliptique, sur le corps Q des nombres rationnels, est isomorphe à l'un des 15 groupes abéliens additifs :

$ZI / m\,ZI$ *pour* $1 \le m \le 10$ *et* $m = 12$.

$ZI/2ZI \times ZI/dZI$ *pour* $d = 1, 2, 3, 4$.

C'est un théorème conjecturé par OGC et démontré par MAZUR.

7. Homomorphismes de courbes elliptiques :

Le groupe E (K) de Mordell –Weil est abélien, donc il y a des homomorphismes et des isomorphismes de groupes $E(K) \longrightarrow E`(K)$, des endomorphismes et des automorphismes de groupes $E(K) \longrightarrow E(K)$ , et des isogénies de groupes $E(K) \longrightarrow E`(K)$.

7.1. Isomorphismes de courbes elliptiques :

Soient deux courbes elliptiques, d'équations de Weierstrass respectives :

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

$E' : y^2 + a'_1xy + a'_3y = x^3 + a'_2x^2 + a'_4x + a'_6$

Définition 11 :

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 :

$f(P+Q) = f(P) + f(Q)$, $f(O_E) = O_E$

Proposition 17 :

Un isomorphisme de 2 courbes elliptiques est défini par le changement de variables linéaire :

$$x = u^2x' + r$$
$$y = u^3y' + u^2x's + t \qquad (1)$$

avec u , r, s, t dans le corps K et u 0.

Preuve :

Soit un isomorphisme

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

déterminé par les formules (1).Alors l'isomorphisme réciproque

$$\psi : E`(K) \longrightarrow E(K)$$

est déterminé par les relations :

$$x` = (x - r)\, u^{-2}$$

$$y` = (y - s\,x - t + s\,r)\, u^{-3}$$

La relation (1) et les calculs impliquent des relations entre les coefficients et les invariants des 2 courbes :

Relations entre les coefficients a_i *et* a_i' *:*

$$\begin{aligned} u\,a'_1 &= a_1 + 2s \\ u^2\,a'_2 &= a_2 - s a_1 + 3r - s^2 \\ u^3\,a'_3 &= a_3 + r a_1 + 2t \\ u^4\,a'_4 &= a_4 - s a_3 - r s a_1 + 2r a_2 - t a_1 + 3r^2 - 2ts \\ u^6\,a'_6 &= a_6 + r a_4 + r^2 a_2 - t a_3 - t a_1 + 3r^2 - 2ts \end{aligned} \qquad (2)$$

Relations entre les invariants b_{2i} *et* b_{2i}' *:*

$$\begin{aligned} u\,b'_2 &= b_1 + 12r \\ u^4 b'_4 &= b_4 + 2b_2 + 6r^2 \\ u^6\,b'_6 &= b_6 + 2r\,b_4 + r^2\,b_2 + 4r^3 \\ u^8\,b'_8 &= b_8 + 3\,r\,b_6 + 3r^2 b_4 + r^3 b_2 + 3r^4 \end{aligned} \qquad (3)$$

Relations entre les invariants c_{2i} *et* c_{2i}' *:*

$$\begin{aligned} u^4 c'_4 &= c_4 \\ u^6 c'_6 &= c_6 \end{aligned} \qquad (4)$$

Relation entre les discriminants :

$$u^{12}(E) = \Delta(E) \qquad (5)$$

Relations entre les invariants modulaires j(E) et différentiels ω (E) :

$$j(E') = j(E) \text{ et } u^{-1}\omega(E') = \omega(E) \qquad (6)$$

La relation (5) implique le signe de $\Delta(E')$ 0, donc E' est une courbe elliptique.

La relation (6) est une relation d'équivalence dans l'ensemble des courbes elliptiques qui ont des invariants modulaires égaux.

Proposition 18:

Deux courbes elliptiques E et E , sont isomorphes si et seulement si elles ont des invariants modulaires égaux

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

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

Soit 2 courbes elliptiques E et E' isomorphes ; alors les coordonnées, d'un point du groupe de Mordell - Weil E (K) sontliées à celles du point de E'(K) correspondant par les formules d'isomorphismes :

$$(x,y) \longrightarrow (u^2 x' + r\ ,\ u^3 y' + u^2 x' s + t)$$

Les relations (6) impliquent :

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

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

L'invariant modulaire j(E) d'une courbe elliptique E peut prendre trois valeurs : j(E) = 0, j(E) = 1728, j(E) = t 0, 1728 sur un corps K de caractéristique 2,3.

Examinons les 3 cas possibles pour j(E)

Prenons une équation de la courbe elliptique E sous la forme

$$E : y^2 = x^3 - 27c_4 x - 54\, c_6 \qquad (1)$$

$$\text{Alors } j(E) = 1728\, c_4^3/[c_4^3 - c_6^2] \qquad (2)$$

1er cas : Soit une courbe elliptique E d'invariant j(E)=0

ceci implique : $c_4 = 0$ et $c_6 \neq 0$ (3)

L'équation (1) devient l'équation :

$$E : y^2 = x - 54c_6 \quad (4)$$

La relation d'isomorphisme entre les invariants c_i et c_i' des 2 courbes elliptiques :

$$u^6 c'_6 = c_6 \quad (5)$$

C'est une équation algébrique de degré 6en u qui admet donc 6 racines dans une clôture algébrique K_{Alg} du corps K.

$$u = [c_6 / c'_6]^{1/6}$$

Cela implique 6 isomorphismes :

$$E(K) \longrightarrow E'(K) \quad \text{avec} \quad (x, y) \longrightarrow (u^2x, u^3y)$$

2ème cas : Soit une courbe elliptique d'invariant j(E) =1728

Cette hypothèse implique les 2 conditions $c_4 \neq 0$, $c_6 = 0$.

L'équation (1) devient l'équation :

$$E : y' = x^3 - 27 c_4 x$$

Relations d'isomorphismes entre les invariants c_i et c_i' :

$$u^4 c'_4 = c_4$$

Cette égalité est une équation du 4ème degré en u ; elle admet 4 racines dans une clôture algébrique K_{Alg} de K.

$$u = [c_4 / c'_4]^{1/4}$$

Il en résulte les 4 isomorphismes :

$$E(K) \longrightarrow E'(K) \quad \text{avec} \quad (x, y) \longrightarrow (u^2x, u^3y)$$

3ème cas : Soit une courbe elliptique d'invariant j(E) = t ≠1728

La formule (2) de j(E) implique l'équation :

$$tc^2_6 = c^3_4 (t - 1728)$$

Cette équation admet la solution :

$c_4 = t / (t - 1728)$, $c_6 = \pm t / (t - 1728)$

Relations d'isomorphismes entre les invariants c_i et c_i' :

$$u^4 c'_4 = c_4 \text{ et } u^6 c'_6 = c_6$$

Ce sont 2 équations algébriques en u de degrés 4 et 6.

Elles admettent, dans un corps algébriquement clos les solutions :

$$u = [c_4 / c'_4]^{1/4} = [c_6 / c'_6]^{1/6}$$

Il en résulte les 24 isomorphismes :

$$E(K) \longrightarrow E'(K) \quad \text{avec} \quad (x, y) \longrightarrow (u^2 x, u^3 y)$$

7.2. Automorphismes d'une courbe elliptique :

Les automorphismes d'une courbe elliptique dépendent de son invariant modulaire j (E) et de la carac (K).

Proposition19 :

Soit une courbe elliptique E. Alors le groupe Aut (E) des automorphismes de E est un groupe d'ordre un diviseur de 24 :

1) *Aut(E) est d'ordre 2 si j(E) ≠ 0,1728*
2) *Aut(E) est d'ordre 4 si j(E) = 1728 et caractéristique de K différente de 2,3*
3) *Aut(E) est d'ordre 6 si j(E) = 0 et caractéristique de K différente de 2,3*
4) *Aut(E) est d'ordre 12 si j(E) = 0 = 1728 et caractéristique de K égale à 3*
5) *Aut(E) est d'ordre 24 si j(E) = 0 = j (E) = 1728 et caractéristique de K égale à 2*

Preuve de (1) :

Soit une courbe elliptique E, d'invariant modulaire j(E) ≠ 0,1728 (1)

Nous prenons une équation de E de la forme

$$y^2 = x^3 + Ax + B \quad \text{avec } 4A^3 + 27B^2 \neq 0 \qquad (2)$$

Son invariant modulaire vaut :

$$j(E) = 4.1728.\ A^3/\ (4A^3 + 27\ B^2) \text{ pour carac } (K) \neq 2,3 \qquad (3)$$

Considérons un automorphisme du groupe E (K) de la forme:

$$x = u^2\ x'\ ;\ y = u^3 y' \qquad (4)$$

Les formules (1) et (3) impliquent les 2 conditions :

$$A \neq 0 \text{ et } B \neq 0 \qquad (5)$$

Les relations d'isomorphismes entre les coefficients 2 courbes elliptiques isomorphes sont :

$$u^4 A = A \text{ et } u^6 B = B \qquad (6)$$

Ce sont 2 équations algébriques de degrés 4 et 2 en u :

$$u^4 = 1 \text{ et } u^6 = 1$$

soit $u^2 = 1$

Cette équation admet 2 racines dans K :

$$u = 1,\ u = -\ 1$$

Il en résulte 2 automorphismes de E :

E (K) $\longleftrightarrow$ E (K) de valeur $(x = x', y = y')$ et $(x = x', y = -\ y')$

Le groupe Aut (E) est d'ordre 2.

Preuve de (2) :

Soit une courbe elliptique E, d'invariant modulaire j(E) = 1728 sur un corps K de caractéristique $\neq 2,3$ (7)

La formule de l'invariant modulaire j(E) et (7) impliquent les 2 conditions :

$$A \neq 0 \text{ et } B = 0 \qquad (8)$$

Les formules (6) impliquent l'équation :

$$u^4 A = A$$

soit $u^4 = 1$

Cette équation admet 4 racines dans le corps K (i)

Il en résulte 4 automorphismes :

$$E(K) \longrightarrow E(K) \text{ de valeur}$$

$(x = x', y = y')$, $(x = x', y = - y')$, $(x = - x', y = -i\, y')$ et $(x = - x', y = i\, y')$

Preuve de (3)

Soit une courbe elliptique E, d'invariant modulaire $j(E) = 0$ sur un corps K de caractéristique $\neq 2,3$ (9)

La formule (3) de l'invariant modulaire j(E) et (9) impliquent les 2 conditions :

$$A = 0 \text{ et } B \neq 0 \qquad (10)$$

Les formules (6) impliquent l'équation :

$$u^6 B = B \text{ soit } u^6 = 1$$

Cette équation admet 6 racines dans le corps K (u)

$$u = \pm 1,\ u = \pm j,\ u = \pm j^2 \text{ où } j = \frac{1}{2}(1+\sqrt{3})$$

Il en résulte 6 automorphismes:

$$E(K) \longrightarrow E(K) \text{ de valeur}$$

$(x = x', y = y')$, $(x = x', y = - y')$, $(x = j^2 x', y = j^3 y')$,

$(x = j^2 x', y = - j^3 y')$, $(x = j\, x`, y = j\, y')$ et $(x = j\, x', y = - j\, y')$

Preuve de (4) :

Soit une courbe elliptique E, d'invariant modulaire $j(E) = 0$ sur un corps K de caractéristique égale à 3.

Nous prenons un automorphisme de la courbe de la forme :

$$x = u^2 x' + r\ ;\ y = u^3 y'$$

Les relations entre les coefficients isomorphes des courbes elliptiques sont:

$$u^4 A = A \text{ et } u^6 B = B + rA + r^3 \qquad (12)$$

Les automorphismes sont déterminés par les couples (u, r)

chaque couple (u, r) est solution du système :

$$u^4 = 1 \text{ et } r^3 + rA + B(1 - u^2) = 0 \qquad (13)$$

Sur une clôture algébrique de K, u engendre un sous groupe C_4 d'ordre 4 et r engendre un sous groupe C_3 d'ordre 3.

Le groupe Aut(E) est isomorphe au groupe produit C_4 x C_3, qui est donc d'ordre 12.

Preuve de (5) :

Soit une courbe elliptique E, d'invariant modulaire j(E) = 0 sur un corps K de caractéristique égale à 2. (14)

Prenons l'équation de la courbe sous la forme :

$$y^2 + a_3x = x^3 + a_4x + a_6 \quad (15)$$

L'équation (15) est préservée par l'automorphisme :

$$x = u^2 x' + s^2 \; ; \; y = u^3y' + u^2s\, x' + t, \quad u, s, t \in K^* \quad (16)$$

Les relations entre les coefficients des courbes isomorphes impliquent:

$$u^3a'_3 = a_3$$

$$u^4a'_4 = a_4 + sa_3 + s_4 \quad (17)$$

$$u^6a'_6 = a_6 + s^2a_4 + ta_3 + s_6 + t_2$$

Le groupe Aut (E) de la courbe E est déterminé par les triplets (u, s, t) dans une clôture algébrique de K :

$$u^3 = 1,\ s^4 + sa_3 + a_4 (1-u) = 0 \text{ et } t^2 + ta_3 + s^2a_4 + s^6 = 0 \quad (18)$$

u engendre un groupe cyclique C_3 d'ordre 3 ; s engendre un groupe cyclique C_4 d'ordre 4 et t engendre un groupe cyclique C_2 d'ordre 2 .

Les relations (18) entre s et t impliquent que le groupe C_4 est twisté par le groupe C_2 ; le produit C_2C_4 est un groupe d'ordre 8 isomorphe au groupe Q (8) des quaternions.

Les automorphismes (15) sont liés aux triplets (u, s, t).

Donc le groupe Aut (E) est d'ordre égal au nombre de triplets (u, s, t), soit 24.

Le groupe Aut (E) est isomorphe au produit de groupes C_3 x Q (8).

7.3. Isogénies et endomorphismes de courbes elliptiques :

Un exemple d'isogénie de courbes elliptiques est constitué par la multiplication Ψ_m par un entier rationnel m :

$$\Psi_m : E(K) \longrightarrow E(K)$$

de valeur $\Psi_m(P) = m\,P$

Cette application satisfait les formules d'homomorphisme de groupe :

$$\Psi_m(P+R) = m(P+R) = mP + mP = \Psi_m(P) + \Psi_m(R)$$

et $\Psi_m(0_E) = m\,0_E = 0_E$.

Donc Ψ_m est un endomorphisme du groupe E (K).

Selon Shimura (Introduction to the Arithmetic of Automorphic functions), le noyau de cette application Ψ_m est le sous groupe de m -torsion de E :

$$\psi_m^{-1}(0_E) = \{P \in E(K) \text{ avec } mP = 0_E\}$$

Ce groupe est isomorphe à $(ZI / mZI)^2$, produit de deux copies de (ZI / mZI) si carac (K)=0 ou si carac (K)=p ne divise pas m.

L'ensemble de ces multiplications Ψ_m a une structure d'anneau.

Proposition 20 :

Soit une courbe elliptique E .L'ensemble $End_{ZI}(E)$ des multiplications Ψ_m, dans le groupe E (K) par les entiers rationnels m forme un anneau isomorphe à l'anneau ZI :

$$End_{ZI}(E) \approx Z.$$

Preuve :

Soient 2 entiers rationnels m et n ; les endomorphismes associés :

$$\Psi_m , \Psi_n : E(K) \longrightarrow E(K) \qquad (1)$$

satisfont les formules des endomorphismes d'anneaux :

$$\Psi_{m+n}(P) = (m+n)P = mP + nP = \Psi_m(P) + \Psi_n(P) ; \qquad (2)$$

$$\Psi_{m\,n}(P) = (m\,n)P = m(nP) = m\Psi_n(P) = \Psi_m(\Psi_n(P)) \qquad (3)$$

$$\Psi_0(P) = 0 \; P=0_E \text{ et } \Psi_m(0_E) = m\; 0_E = 0_E \qquad (4)$$

Considérons l'application:

$$f: ZI \longrightarrow \text{End}_{ZI}(E)$$

de valeur $f(m) = \Psi_m : E(K) \longrightarrow E(K)$

Les formules (2), (3) et (4) impliquent que l'application f est un isomorphisme d'anneaux :

$$\text{End}_{ZI}(E) \approx ZI.$$

Il existe d'autres formes d'isogonies $E(K) \longrightarrow E(K)$ et $E(K) \longrightarrow E`(K)$.

Avec Shimura, nous posons la :

Définition 12 :

Une isogénie de courbes elliptiques E et E' est un homomorphisme

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

qui satisfait les conditions:

1) *λ n'est pas nul ;*
2) *le noyau de λ est fini ;*
3) *λ est un homomorphisme surjectif.*

Les coordonnées des points m P d'une courbe elliptique E sont des fractions rationnelles du corps K (x, y) :

$$m\,P = (x_m, y_m) \quad \text{avec } x_m = \frac{\varphi_m}{\theta_m^2} \quad \text{et } y_m = \frac{\omega_m}{\theta_m^3},$$

où φ_m , θ_m et ω_m sont des polynômes de l'anneau K [x , y] .

Il en est de même pour toute isogénie $\lambda : E(K) \longrightarrow E`(K)$:

$\lambda(P) = (x_\lambda , y_\lambda)$, où $x_\lambda = \frac{A_\lambda}{D_\lambda^2}$, $y_\lambda = \frac{B_\lambda}{D_\lambda^3}$, A_λ , B_λ et D_λ étant des polynômes de l'anneau K [x, y] .

Citons un exemple (Velu dans « isogénies de courbes elliptiques », CRAS, Paris t 273 A (26 juillet 1971) 238-240)

Soit la courbe elliptique A d'équation de Weierstrass :

$A : y^2 + y = x^3 - x^2$;

Invariants : $c_4 = 2^4$; $\Delta = -11$; $j = -2^{12} / 11$

Le point P = (0, 0) engendre dans le groupe A (IQ) un sous groupe F d'ordre 5 :

{P, 2P = (1, -1), 3P = (1, 0), 4P = (0, -1) et $5P = 0_E$}

Ce groupe F permet de construire une 5- isogénie λ d'équations :

$$x_\lambda = x + \frac{1}{x^2} + \frac{2x-1}{(x-1)^2} \quad ;$$

$$y_\lambda = y - \frac{2y + xy + 1}{x^3} - \frac{2y + y(x-1) + x}{(x-1)^3}.$$

Alors, l'équation de la courbe B par l'isogénie $\lambda : A \rightarrow B$ est :

$B : y^2 + y = x^3 - x^2 - 10x - 20;$

d'invariants : $c_4 = 2^3 \times 31$; $\Delta = -11^5$; $j = -2^{12} \times 31^3 / 11$

Cette isogénie λ a un noyau qui est un sous groupe d'ordre 5 du groupe E (K).

Toute isogénie λ possède 2 invariants spécifiques : un degré et une isogénie duale.

Définition 13 :

Le degré d'une isogénie

$\lambda : E(K) \longrightarrow E`(K)$,

de 2 courbes elliptiques E et E` est égal à l'ordre du sous groupe noyau de λ *:*

$\deg\lambda = \text{card.}(\ker\lambda)$

Définition 14:

Soit une isogénie de courbes elliptiques de degré d :

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

L'isogénie duale de λ *est l'homomorphisme*

$\hat{\lambda} : E`(K) \longrightarrow E(K)$.

dont les composés satisfont:

$\lambda \circ \hat{\lambda}$ *est la multiplication sur E` (K) par d ;*

$\hat{\lambda} \circ \lambda$ *est la multiplication sur E (K) par d .*

La structure de l'anneau End $_K$(E) des endomorphismes d'une courbe elliptique E est précisée par la :

Proposition 21:

L'anneau End $_K$(E) des endomorphismes d'une courbe elliptique E est isomorphe:

1) *soit à l'anneau ZI des entiers rationnels ;*
2) *soit à l'anneau A_L des entiers d'un corps quadratique imaginaire L ou à un ordre de cet anneau ;*
3) *soit à un ordre de l'algèbre des quaternions sur le corps IR des nombres réels.*

Ce 3ème cas se présente seulement pour carac (K) = p> 0

Preuve :

C'est un théorème de Deuring.

Les courbes elliptiques E dont l'anneau des endomorphismes est isomorphe à un ordre d'un corps quadratique imaginaire, forment une classe particulière.

Définition 15 :

Une courbe elliptique à Multiplication Complexe _ « C M curve » en anglais _ est une courbe elliptique E, sur un corps K de carac (K)=0, dont l'anneau End (E) est isomorphe à un ordre d'un corps quadratique imaginaire.

Exemple :

Le changement de variables $(x, y) \to (-x, iy)$ transforme une courbe elliptique E en une courbe elliptique E`à Multiplication Complexe par l'anneau Z[i] du corps quadratique imaginaire Q ($\sqrt{-1}$).

CHAPITRE II

GEOMETRIE DES COURBES ELLIPTIQUES

1. Valuations d'un corps :

Les valuations d'un corps de nombres s'appliquent aux corps de définition des courbes elliptiques.

Ce sont des ouvrages de *Théorie des nombres* qui traitent la théorie des valuations, comme :

«Number theory » de H .Hasse

«Algebraic Number Theory, chapitres I et II » de E .Weiss

« The Theory of numbers, chapitre II » de S.Iyanaga

« Theory of Number » de E. Artin

qui ont inspiré ce bref exposé :

Définition 1 :

Une valuation d'un corps K est une fonction sur K à valeurs réelles positives :

$$v : K \longrightarrow IR_+$$

qui satisfait les 3 axiomes :

(Val 1) $v(x) \geq 0$ et $v(x) = 0$ équivaut à $x = 0$ pour tout élément x du corps K

(Val 2) $v(xy) = v(x)\,v(y)$ pour tous les éléments x et y du corps K

(Val 3) il existe une constante réelle $c \geq 1$ telle que :

$v(x) \leq 1$ implique $v(x + 1) \leq c$ pour tout élément x de K

L'axiome (Val 2) implique qu'une valuation v est un homomorphisme du groupe multiplicatif K^* des éléments non nuls du corps K dans le groupe multiplicatif des nombres réels positifs IR_+^*

L'axiome (Val 3) de la définition peut être remplacé par l'inégalité triangulaire :

(Val 3′) $v(x+y) \leq c \max\{ v(x), v(y) \}$ pour tous les éléments x et y du corps K

Exemples :

1) La valuation triviale sur un corps K :

L'application $v : K \longrightarrow IR_+$ de valeurs :

$v(0) = 0$ et $v(x) = 1$ pour $x \neq 0$

est la valuation triviale du corps K ; et c = 2.

2) La valeur absolue ordinaire du corps des nombres réels IR est la fonction v de valeur :

$v(x) = \max\{ x , -x \}$

Pour le 3ème axiome, nous prenons la constante c = 2.

3) Soit le corps C des nombres complexes et la fonction v de valeur :

$v(x) = (a^2 + b^2)^{1/2}$ pour $x = a + i\,b$

Le 3ème axiome est vérifié pour c = 2.

4) La valuation p -adique du corps IQ des nombres rationnels :

pour p premier, soit l'application :

$v_p : Q \longrightarrow IR^+$ de valeur :

$v_p(p) = 1/p$ et $v_p(q) = 1$ pour tout nombre premier $q \in IZ$ différent de p

Alors la valuation d'un nombre rationnel $x = y\,p^n$ tel que y premier à p est égale à :

$v_p(x) = p^{-n}$

v_p est la valuation p -adique du corps Q

Pour le 3ème axiome, nous prenons la constante c = 1.

Toute valuation v non triviale d'un corps K, permet de définir une topologie de « HAUSDORFF » qui est caractérisée par la propriété :

Deux points séparés admettent des voisinages disjoints.

Un système fondamental de voisinages d'un élément $x \in K$ est l'ensemble :

$$U(x, \zeta) = \{ y \in K ; v(x - y) < \zeta \}$$

pour une famille de nombres réels ζ positifs .

Proposition 1 :

Soit une valuation d'un corps K

$v : K \longrightarrow IR_+$.

Alors :

v détermine sur ce corps K une topologie de Hausdorff .

Cette topologie permet de définir des valuations équivalentes, des suites de Cauchy et des corps complets.

Définition 2 :

Deux valuations $v_i : K \longrightarrow IR_+$; $i = 1, 2$ d'un corps K sont équivalentes lorsqu'elles déterminent la même topologie sur le corps K.

Deux valuations équivalentes d'un corps K sont liées par la :

Proposition 2 :

Soit une valuation non triviale v_1 d'un corps K :

$K \longrightarrow IR_+$.

Alors :

toute valuation $v_2 : K \longrightarrow IR_+$ équivalente à v_1 est de la forme :

$v_2 = v_1^c$ *où c et une constante positive* $c > 0$

qui satisfait la relation :

$v_2(x) = v_1(x)^c$ *pour tout élément* $x \in K$

Diviseurs premiers d'un corps :

Les valuations équivalentes d'un corps K permettent de définir les diviseurs premiers de K par la :

Définition 3 :

Chaque classe d'équivalence dans l'ensemble V_K des valuations d'un corps K est un diviseur premier D de K pour la valuation v :

$$D = \{v^{c} \quad ; \quad c > 0\}$$

La classe d'une valuation non triviale est un diviseur premier ordinaire de K

Dans l'ensemble V_K des valuations d'un corps K, on ne considère que les valuations non équivalentes qui, sont donc des représentants des diviseurs premiers du corps K

Dans l'ensemble V_K des valuations du corps K, les valuations non triviales et non équivalentes impliquent la :

Proposition 3 :

Soient n valuations non triviales $v_1,\ldots\ldots,v_n$ et non équivalentes d'un corps K. Alors :

1) il existe un élément $x \in K$ de valuation $v_1(x) > 1$ tel que :

et $v_i(x) < 1$ pour $i = 2, 3, \ldots,n$

2) il existe un élément $x \in K$ et un nombre réel $\zeta > 0$ tels que :

$v_1(1 - x) < \zeta$ et $v_i(x) < \zeta$ pour tout $i = 2, 3, \ldots\ldots, n$

Valuations archimédiennes et non archimédiennes :

Dans l'ensemble V_K des valuations d'un corps K, nous distinguons deux types de valuations suivant la valeur de la constante c dans l'axiome (Val 3) de la définition d'une valuation

Définition 4 :

Une valuation $v \in V_K$ est archimédienne si elle satisfait l'inégalité :

$v(x) \leq 1$ implique $v(x + 1) \leq 2$

Dans l'axiome (Val 3), la constante c vaut $c = 2$

Une valuation $v \in V_K$ est non archimédienne si elle satisfait l'inégalité :

$v(x) \leq 1$ implique $v(x + 1) \leq 1$

Ce qui donne la valeur $c = 1$

Il en résulte que les valuations V_K d'un corps K sont classées dans deux classes disjointes :

Classe des valuations archimédiennes et classe des valuations non archimédiennes

Exemples :

1) La valuation triviale sur un corps K est non archimédienne.
2) Les valeurs absolues sur les corps IR et CI sont des valuations archimédiennes.
3) L'ensemble V_Q des valuations non équivalentes du corps Q est la réunion disjointe du sous ensemble V_0 de valuations non archimédiennes et du sous ensemble V_∞ des valuations archimédiennes.
4) Les valuations archimédiennes du corps Q sont équivalentes à la valeur absolue

$$| x | = \max \{ x , – x \}$$

5) Les valuations non archimédiennes sont équivalentes aux valuations p -adiques

Une valuation non archimédienne est caractérisée par les 2 propositions :

Proposition 4 :

Soit une valuation non archimédienne $v \in V_K$ d'un corps K, alors :

1) $v (x) \neq v (y)$ implique $v (x + y) = \max \{ v (x) , v (y) \}$

2) Soient n éléments $x_1 , \ldots\ldots , x_n$ qui satisfont la condition :

$v (x_1) \geq v (x_i)$ pour $i = 2, \ldots\ldots , n$

Alors v satisfait la relation :

$v (x_1 + x_2 + \ldots\ldots + x_n) = v (x_1)$

Preuve :

Ce théorème se démontre en utilisant les axiomes d'une valuation non archimédienne

Proposition 5 :

Soit une valuation non archimédienne v d'un corps K. Alors elle satisfait les propriétés :

1) $v(x+y) \leq \max\{ v(x), v(y) \}$ pour tout élément $x, y \in K$

2) L'ensemble $\{ v(n.1) ; 1$ unité de K et $n \in IZ \}$ est borné

Preuve :

E.Weiss : Algebraic number theory

Valuations non archimédiennes discrètes :

Définition 5:

Une valuation non triviale $v : K \longrightarrow IR \cup \{\infty\}$ est discrète lorsque son groupe de valuation $v(K)$ est discret dans le corps IR des nombres réels .

$$v(K) = ZI \cup \{\infty\}$$

A une valuation non archimédienne discrète v sont associés les sous ensembles suivants du corps K :

$A_v = \{ x \in K ; v(x) \geq 1 \}$ = l'anneau des v-entiers de K

$M_v = \{ x \in K ; v(x) > 1 \}$ = l'idéal maximal en v

$U_v = \{ x \in K ; v(x) = 1 \}$ = le groupe des v-unités

Le corps quotient $k = A_v / M_v$ = le corps de classes résiduelles en v

L'idéal maximal M_v possède un élément π de valuation $v(\pi) = 1$

L'élément π est une uniformisante en v

Dans ce cas l'anneau de valuation A_v est un anneau de valuation discrète, il en résulte que tout élément a de l 'anneau A_v se met sous la forme :

$$a = \pi^r u \quad ;$$

où r est un entier naturel et u une unité .

Exemples :

Soit le corps IQ des nombres rationnels, et un nombre premier p.

La valuation p -adique est la fonction :

$v_p : IQ \longrightarrow IR_+$ de valeurs :

$v_p(p) = 1/p$ et $v_p(q) = 1$ pour tout nombre premier $q \neq p$

La valuation p -adique est discrète lorsqu'elle satisfait :

$v_p(p^r) = r$ et $v_p(q) = 0$ pour tout nombre premier $q \neq p$

La structure multiplicative de la propriété (Val 2) d'une valuation d'un corps K montre que ces valuations sont multiplicatives .

Valuations additives :

Soit une valuation non archimédienne discrète :

$v : K \longrightarrow IR \cup \{\infty\}$

multiplicative

A cette valuation v nous associons une valuation additive par l'application logarithme : c'est la valuation exponentielle :

$\varphi : K \longrightarrow IR \cup \{\infty\}$ de valeur :

$\varphi(x) = -\ \mathrm{Log}\ |\, v(x)\,|$

où :

$|a|$ désigne la valeur absolue de a

Les axiomes de cette valuation exponentielle proviennent des axiomes de la définition d'une valuation :

(Val1) $\varphi(x)$ réel et $\varphi(x) = +\infty$ équivaut à $x = 0$

(Val2) $\varphi(x\,y) = \varphi(x) + \varphi(y)$ pour tous x , y du corps K

(Val3) $\varphi(x + y) \geq \min\{\varphi(x), \varphi(y)\}$ pour tous $x , y \in K$

Les 3 objets mathématiques associés à cette valuation exponentielle φ sont :

$A_\varphi = \{ x \in K ;\ \varphi(x) \geq 0 \}$ = l'anneau des φ-entiers de K

$M_\varphi = \{ x \in K ;\ \varphi(x) > 0 \}$ = l'idéal maximal en φ

$U_\varphi = \{ x \in K ;\ \varphi(x) = 0 \}$ = le groupe des φ-unités

La valuation φ est discrète lorsque son groupe de valeurs est discret :

$$\varphi(K) = ZI \cup \{\infty\}$$

L'ensemble V_K des valuations non équivalentes d'un corps K est une partition :

$$V_K = V_0 \cup V_\infty$$

où : V_0 est le sous ensemble des valuations non archimédiennes discrètes et V_∞ l'ensemble formé des valuations archimédiennes .

Les valuations non archimédiennes discrètes permettent d'obtenir les notions de discriminant minimal et de réduction d'une courbe elliptique sur un corps K. Ceci est l'objet de la partie qui suit.

Equation minimale :

Soit une courbe elliptique E d'équation de Weierstrass :

$$E : y^2 + a_1 x y + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \qquad (1)$$

Définition 6 :

L'équation (1) de Weierstrass est minimale en v si ses coefficients a_i sont v -entiers $v(a_i) \geq 0$ et si son discriminant $\Delta(E)$ est de valuation $v(Ä(E))$ minimale.

L'équation minimale d'une courbe elliptique E n'est pas unique à cause de ses transformées en une courbe E` par l'isomorphisme :

$$(x, y) \longrightarrow (u^2 x + r \ , \ u^3 y + s u^2 x + t) \text{ où } r, s, t \in K \ , \ u \neq 0$$

Les relations entre les coefficients de deux courbes elliptiques E et E` isomorphes :

$$u^4 c`_4 = c_4 \ , \ u^6 c`_6 = c_6 \text{ et } u^{12} Ä(E`) = Ä(E)$$

impliquent que l'équation (1) est minimale en v dans les 3 cas :

1. Les cinq coefficients a_i sont v- entiers et $v(Ä(E)) < 12$;
2. Les cinq coefficients a_i sont v- entiers et $v(c_4(E)) < 4$;
3. Les cinq coefficients a_i sont v- entiers et $v(c_6(E)) < 6$;

Lorsque l'équation (1) n'est pas minimale, le changement :

$(x, y) \longrightarrow (u^{-2} x , u^{-3} y)$ la rend minimale

Exemple d'une courbe elliptique d'équation minimale :

Soit un nombre premier p et une courbe elliptique E d'équation de Weierstrass :

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

Le calcul donne les invariants :

$c_4(E) = 129 = 3 \times 43$; $c_6(E) = -2241 = -3^3 \times 83$; $\Ä(E) = -1664 = -2^7 \times 13$

Les valuations considérées sont :

v_2 , v_3 , v_{13} , v_{43}

Nous obtenons les valeurs :

$v_2(c_4) = 0 < 4$, $v_2(\Ä(E)) = 7 < 12$

$v_p(c_4(E)) < 4$ et $v_p(\Ä(E)) < 12$ pour tout nombre premier $p \neq 2$

Il en résulte que l'équation de la courbe E est minimale en la valuation NAD v_p pour tout nombre premier $p \in$ ZI.

2. Réduction d'une courbe elliptique :

La réduction d'une courbe elliptique consiste à réduire le corps de base K à un corps « local » possédant un seul idéal premier ; alors les coefficients a_i et les variables x et y de la courbe E sont « réduits » modulo cet idéal premier .

Réduction modulo une uniformisante :

Pour toute VNAD v du corps K, la réduction en v (réduction modulo π) est l'application canonique :

$$\varphi : A_v \longrightarrow k = A_v / \pi A_V$$
$$t \longrightarrow t$$

φ induit l'application réduction :

$$E(K) \longrightarrow \tilde{E}(K)$$
$$P \longrightarrow \tilde{P}$$

La courbe $\tilde{E}$ est la courbe réduite en v.

Si E est une courbe elliptique sur K d'équation de Weierstrass minimale en v, alors pour obtenir l'équation de la courbe réduite $\tilde{E}$ sur le corps résiduel k ; il suffit de réduire modulo π les coefficients a_i et les nombres x et y :

$\varphi(a_{i)} = \tilde{a}_i$, $\varphi(x) = \tilde{x}$, $\varphi(y) = \tilde{y}$

donc la courbe réduite $\tilde{\tilde{E}}$ a pour équation :

$\tilde{E} : y^2 + \tilde{a}_1 x y + \tilde{a}_3 y = x^3 + \tilde{a}_2 x^2 + \tilde{a}_4 x + \tilde{a}_6$, avec $\tilde{x} = x$ et $\tilde{y} = y$.

Les réductions sont classifiées par la nature de la cubique réduite $\tilde{\tilde{E}}$; selon que $\tilde{E}$ est elliptique possède un nœud ou un point de rebroussement.

Bonne et mauvaise réduction :

Définition 8 :

Soit une courbe elliptique E, sur un corps K muni d'une valuation v, d'équation de Weierstrass minimale en v et la courbe réduite $\tilde{E}$ de E modulo π

Alors nous distinguons 3 types de réductions de la courbe E :

1) *La courbe E a une bonne réduction en v si la courbe réduite $\tilde{E}$ est non singulière .*

Il en résulte que $\tilde{E}$ est une courbe elliptique sur le corps résiduel k.

2) *La courbe E a une mauvaise réduction sur K si la courbe réduite $\tilde{E}$ est singulière .*

Cette mauvaise réduction est :

a) multiplicative en v si la courbe réduite $\tilde{\tilde{E}}$ possède un nœud :

multiplicative décomposée si les deux équations des tangentes à $\tilde{E}$ au nœud sont rationnelles (à coefficients dans le corps résiduel k) .

b) additive sur K si $\tilde{E}$ possède un point de rebroussement

Vocabulaire :

Une bonne réduction est une réduction stable.

Une réduction multiplicative est une réduction semi stable.

Une réduction additive est une réduction instable.

La nature de la réduction d'une courbe elliptique E se détermine à partir d'une équation de Weierstrass minimale par la :

Proposition 6 :

Soit un corps K muni d'une valuation v et une courbe elliptique E d'équation de Weierstrass minimale en v :

$$E : y^2 + a_1 x y + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$$

Soit son discriminant Ä (E) et son invariant usuel c_4 (E). Alors :

a) La courbe E a une bonne réduction en v si et seulement si

$$v (Ä (E)) = 0 ;$$

donc Ä (E) est une v- unité.

b) La courbe E a une réduction multiplicative en v si et seulement si :

$$v (Ä (E)) > 0 \text{ et } v (c_4 (E)) = 0;$$

donc Ä (E) est un élément du v – idéal M_v et c_4 (E) est une v –unité.

c) La courbe E a une réduction additive en v si et seulement si :

$$v (Ä (E)) > 0 \text{ et } v (c_4 (E)) > 0 ;$$

donc Ä (E) et c_4 (E) sont des éléments du v – idéal maximal.

Cette proposition se démontre en utilisant la proposition 9 du chapitre I

Preuve de « E a une bonne réduction en v » implique « v (Ä (E)) = 0 » :

L'hypothèse E a une bonne réduction en v implique que la réduite $\tilde{E}$ est non singulière.

Ceci implique que son discriminant $Ä(\tilde{E}) \neq 0$ dans le corps résiduel k

D'où $v(Ä(E)) = 0$

Preuve de «E a une réduction multiplicative en v» implique «v (Ä (E)) > 0 et v (c_4 (E)) = 0 » :

L'hypothèse « la courbe E a une réduction multiplicative » implique que la courbe réduite $\tilde{E}$ admet un nœud.

Le proposition 9 du chapitre I implique que la courbe réduite $\tilde{E}$ a un discriminant $\Delta(\tilde{E}) = 0$ et l'invariant usuel $c_4(\tilde{E}) \neq 0$

L'hypothèse $Ä(\tilde{E}) = 0$ implique l'inégalité $v(Ä(E)) > 0$

L'invariant $\tilde{c_4} \neq 0$ implique la valuation :

$v(c_4) = 0$

Preuve de « E a une réduction additive en v » implique «v (Ä (E)) > 0 et v (c_4 (E)) > 0 » :

L'hypothèse la courbe E a une réduction additive implique que la courbe E admet un point de rebroussement

La proposition du chapitre I implique les valeurs :

Ä ($\tilde{E}$) = 0 et c_4 ($\tilde{E}$) = 0

Ä (E) = 0 implique que v (Ä (E)) = 0

c_4 ($\tilde{E}$) = 0 implique que v (c_4 (E)) = 0

Nous ne ferons pas les 3 autres preuves.

Application à la réduction d'une courbe elliptique :

Exemple : *figure 3*

Soit la courbe elliptique E sur IQ d'équation de Weierstrass :

E : $y^2 = x^3 + 5x^2 + 1$

Calcul des invariants :

$b_2 = 2^2.5$; $b_4 = 0$; $b_6 = 2^2$; $b_8 = 2^2.5$; Ä (E) = $-2^4.17.31$; c_4 (E) = $2^4.5^2$

Nous appliquons la proposition à cette courbe :

La courbe elliptique E a une bonne réduction en tout nombre premier p qui ne divise pas Ä (E) ; soit $p \neq 2$, 17 et 31

Pour p = 17, 31, la valuation p -adique v implique les inégalités :

v_p (Ä (E)) > 0 et v_p (c_4 (E)) = 0 ;

C'est une réduction multiplicative en v_p.

Pour p = 2, la valuation 2 -adique v implique les inégalités

v_2 (Ä (E)) > 0 et v_2 (c_4 (E)) > 0 ;

C'est une réduction additive en v_2.

Tableau de coordonnées de quelques points de la courbe E :

x	-6	-5	-4	-3	-2	-1	0	1	2
y^2	-35	1	17	19	13	5	1	7	29
y	Non	± 1	$\pm\sqrt{17}$	$\pm\sqrt{19}$	$\pm\sqrt{13}$	$\pm\sqrt{5}$	± 1	$\pm\sqrt{7}$	$\pm\sqrt{29}$

Pour p = 5, la courbe E admet une bonne réduction modulo 5 . Donc la courbe réduite $\tilde{E}$ est une courbe non singulière d'équation de Weierstrass :

$$y^2 = x^3 + 1 \in IF_5[x, y].$$

Elle admet 6 points rationnels :

$$\tilde{E}(IF_5) = \{ 0_E, (0,1), (0,4), (4,0), (2,3), (2,2) \}$$

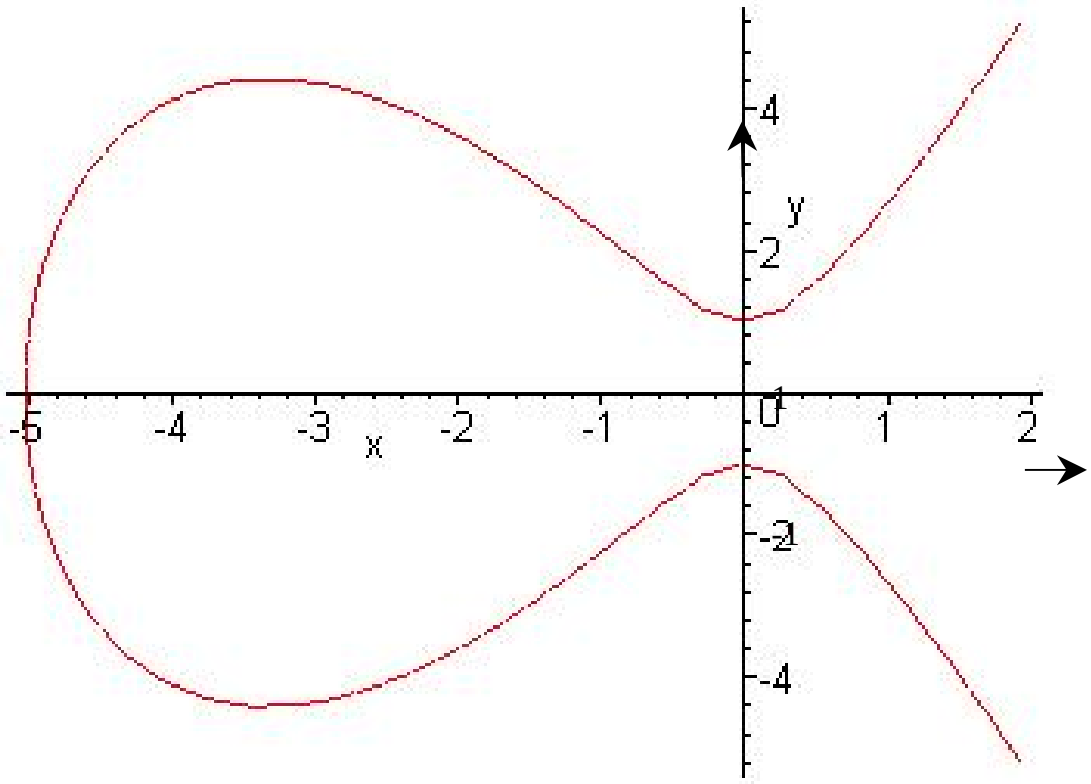


Figure 3

3. Hauteurs sur les courbes elliptiques:

Pour l'étude du groupe abélien de Mordell -Weil d'une courbe elliptique, la fonction hauteur est un outil efficace.

Proposition 7 :

Soit un groupe abélien G et la fonction h à valeurs réelles :

$h : G \longrightarrow IR$

qui satisfait les 3 conditions :

1. Pour tout point $Q \in G$, il existe une constante $c_1 = c_1 (G, Q)$ telle que:

$h (P+Q) \leq 2h(p)+c_1$ *pour tout élément* $P \in G$

2. Il existe un entier $m \geq 2$ et une constante $c_2 = c_2 (G)$ tels que :

$h (m P) \geq m^2 h(P) - c_2$ *,pour tout élément* $P \in G$

3. Pour tout nombre réel c_3, l'ensemble :

$\{P \in G : h (P) \leq c_3\}$

est fini.

Preuve :

Dans S. Lang « Elliptic Curves ; Diophantine Analysis », chapitre III _ Heights_ théorème 1.2 et 2.1

C'est le « théorème de descente infinie » ; parce que la preuve utilise une suite $P_1, P_2, \ldots, P_n$ de points ; cette méthode est semblable à l'algorithme « descente » de Fermat.

Définition 9:

La fonction

$h : G \longrightarrow IR$

est une hauteur sur le groupe G.

Une fonction hauteur h sur le groupe de Mordell -Weil E (K) satisfait d'autres propriétés comme celle de la « loi du parallélogramme »

4. Exemples de hauteurs :

Comme toute fonction $f : A \to B$, la hauteur peut prendre plusieurs valeurs, il en résulte plusieurs types de hauteurs.

1) *Hauteur sur un espace projectif IP^n (Q) :*

$$h(P) = \prod_{v \in M_Q} \max v(a_N) \quad , \text{P} = (a_0, a_1, \ldots, a_N)$$

2) *Hauteur sur le corps IQ des nombres rationnels ;* $h : IQ \to IR$

$$h(x = a/b) = \max\{|a|, |b|\}$$

3) *Hauteur sur le groupe E (IQ) d'une courbe elliptique E;* $h : E(IQ) \to IR$

$$h(P) = \log(\max\{|a|, |b|\}) \ ;$$

si P= (x, y), x = a/b et $h(0_E) = 0$

c'est la hauteur logarithmique (ou de Weil)

4) *Hauteur canonique (ou de Néron – Tate) ;* $h : E(K) \to IR$

$$h(P) = \frac{1}{\deg f} \lim_{N \to +\infty} 4^{-N} h_f(2^N.P), \text{ h } (0_E) = 0$$

où $f \in$ K(E) est une fonction paire non constante (deg f >0)

et $h_f(P) = \log|f(P)|$

Cette hauteur canonique est associée à une fonction f.

5) *Hauteur canonique;* $\hat{h} : E(K) \to IR$

$$\hat{h}(P) = \frac{1}{[K : Q]} \sum_{v \in M_K} n_v \lambda_v(P) \ ; \ \hat{h}(0_E) = 0$$

où V K= ensemble des valuations inéquivalentes de K

n_v = [K_v : IQ_v] = degré local de K sur IQ en v.

λ_v : $E(K_v) \to IR$ hauteur locale en v, qui est continue pour les topologies sur E(K_v)et sur IR, qui satisfait :

(1) $\lambda_v(2P) = 4\lambda_v(P) + v(2y_P + a_1 x_P + a_3) - \frac{1}{4} v(\Delta(E))$

(2) $\lambda_v(P+Q) + \lambda_v(P-Q) = 2\lambda_v(P) + 2\lambda_v(Q) + v(x_P - x_Q) - \frac{1}{6} v(\Delta(E))$.

$\lambda_v(0_E)$=1

Cette hauteur canonique est associée aux « hauteurs locales » λ_v.

Un procédé de détermination du rang d'une courbe elliptique est basé sur le choix d'une hauteur h sur le groupe E (K) d'une courbe elliptique E et sur les valeurs minimales h (P) sur des générateurs P du groupe E (K).

Il existe un logiciel de calcul des points rationnels sur les courbes elliptiques E d'équations de Weierstrass :

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

Pour des grandes valeurs de A et B.

CHAPITRE III
COURBES ELLIPTIQUES SUR UN CORPS FINI

Dans la description des anneaux $\mathbb{Z}/n\mathbb{Z}$ des classes d'entiers rationnels modulo n, nous trouvons des anneaux intègres $\mathbb{Z}/p\mathbb{Z}$ lorsque p est premier, cela provient de la propriété de l'idéal $p\,\mathbb{Z}$ d'être à la fois premier et maximal. Il en résulte que $\mathbb{Z}/p\mathbb{Z}$ est un corps fini à p éléments et un corps premier. Il est de caractéristique p.

Soit un corps fini $\mathbb{F}_q$ à q éléments et l'homomorphisme d'anneaux :

$$\mathbb{Z} \longrightarrow \mathbb{F}_q.$$

Puisque $\mathbb{Z}$ est infini, cet homomorphisme n'est pas injectif. Donc son noyau est un idéal $p\,\mathbb{Z} \neq 0$ de l'anneau $\mathbb{Z}$.

Il en résulte que l'anneau quotient $\mathbb{Z}/p\mathbb{Z}$ est isomorphe à un sous corps du corps $\mathbb{F}_q$.

Ainsi tout corps fini $\mathbb{F}_q$ contient un sous corps isomorphe au corps premier $\mathbb{Z}/p\mathbb{Z}$.

Donc tout corps fini $\mathbb{F}_q$, à q éléments, est de caractéristique p et $q = p^n$.

L'anneau $\mathbb{Z}/q\mathbb{Z}$ des classes résiduelles des entiers modulo $q = p^n$ admet des diviseurs de zéros comme :

$$p^2 = p.p \quad , \quad p^3 = p^2.p$$

Donc l'anneau $\mathbb{Z}/q\mathbb{Z}$ n'est pas un corps pour toute puissances $q = p^n$.

Ses éléments inversibles forment le groupe cyclique $(\mathbb{Z}/q\mathbb{Z})^*$ qui est d'ordre :

$$\varphi(q) = p^n - p^{n-1} \neq q - 1.$$

Certains auteurs désignent un corps fini à q éléments par le symbole GF (q), « Galois Field » à q éléments.

1. Structures d'un corps fini :

1.1. Un corps $\mathbb{F}_q$ fini de $q = p^n$ éléments est un corps dont les éléments sont les racines du polynôme

$$f(x) = x^q - x \in \mathbb{Z}[x]$$

Par définition, $\mathbb{F}_q$ est le corps de décomposition de ce polynôme $f(x)$.

Ce polynôme $f(x)$ se décompose sous la forme

$$f(x) = x(x^{q-1} - 1)$$

Ses racines sont

$$x = 0, a, a^2, ..., a^{q-1} = 1.$$

Elles sont simples parce que la dérivée ne s'annule pas

$$f'(x) = qx^{q-1} - 1 \; ; \; f'(0) = -1 \neq f(0) = 0$$

$f'(x)$ n'a pas de racines communes avec f (x).

Il en résulte que l'ensemble IF^*_q des éléments inversibles du corps fini IF_q est un groupe multiplicatif, cyclique, d'ordre q – 1.

Le corps fini IF_q pour $q = p^n$, a une structure de IF_p – espace vectoriel, de dimension n :

Tout élément b du corps IF_q est donc une IF_p – combinaison linéaire d'une base $e_1,\ldots, e_n$:

$b = r_1e_1 + r_2e_2 + \ldots + r_n e_n$, avec $r_1,\ldots, r_n$ dans IF_p

L'inclusion de corps finis est précisée par la :

Proposition 1 :

Soit un corps fini IF_q à $q = p^n$ éléments, p premier. Alors :

IF_q est inclus dans tout corps fini IF_{q^d} pour tout entier d = 2,3,…

Preuve :

Pour $q = p^n$, $q^d = p^{nd}$, le corps IF_{q^d} est une extension finie du corps IF_q de degré $[IF_{q^d} : IF_q] = d$.

Donc, tout corps fini K est isomorphe à corps fini IF_q, $q = p^n$ où p premier.

Il contient le sous corps premier IF_p.

1.2. Automorphisme de Frobenius :

Le petit théorème de Fermat :

$$a^{p} \equiv a \ mod.\ p,$$

pour tout nombre premier p et pour tout entier a,a = 1,2,…,p-1 ;

est utilisé pour construire l'automorphisme de Frobenius :

$$Fro : IF_q \longrightarrow IF_q$$

de valeur $Fro(x) = x^{p}$

Proposition 2 :

Le groupe des automorphismes du corps fini IF_q, à $q = p^{n}$ éléments est cyclique, d'ordre n, engendré par l'automorphisme de Frobenius.

Preuve :

Soit l'automorphisme de Frobenius de IF_q ; $q = p^{n}$:

$$Fro : IF_q \longrightarrow IF_q \ ; \ Fro(x) = x^{p} \qquad (1)$$

Cet automorphisme engendre un groupe cyclique :

$$Fro, Fro^{2}, Fro^{3}, ..., Fro^{n} = Id_{IF_q} \qquad (2)$$

La formule (1) donne les images :

$$Fro(x) = x^{p}, Fro^{2}(x) = x^{p^{2}}, Fro^{3}(x) = x^{p^{3}}, ..., Fro^{n}(x) = x^{p^{n}} = x^{q} \qquad (3)$$

Par définition, IF_q est le corps de décomposition de :

$$x^{q} - x = 0 \qquad (4)$$

Ceci implique l'égalité :

$$x^{q} = x \qquad (5)$$

Les formules (2) et (5) impliquent que le Fro est d'ordre n.

1.3. Relation entre les polynômes $f(x)$ et les polynômes cyclotomiques $f_n(x)$:

Dans la décomposition

$$f(x) = x^q - x = x(x^{q-1} - 1),$$

il y a le polynôme

$$g(x) = x^{q-1} - 1.$$

Par la théorie des polynômes cyclotomiques, le polynôme g(x) est produit de polynômes cyclotomiques $g_d(x)$:

$$g(x) = x^{q-1} - 1 = \prod g_d(x) \ ;$$

pour tous les diviseurs d de q-1,d=1,…,q-1 .

Le d – ème polynôme cyclotomique $g_d(x)$ est de degré $\phi(d)$.

Exemple :

Le corps fini IF_q pour $q = 5^2$:

Alors $g(x) = x^{q-1} - 1 = x^{24} - 1$;

les diviseurs de 24 sont :

d = 1, 2, 3, 4, 6, 8,12 et 24

Il en résulte que le polynôme g (x) est produit de polynômes cyclotomiques g_d :

$$x^{q-1} - 1 = x^{24} - 1 = g_1(x)g_2(x)g_3(x)g_4(x)g_6(x)g_8(x)g_{12}(x)g_{24}(x)$$

Ce calcul donne les polynômes cyclotomiques :

$$g_1(x) = x - 1, g_2(x) = x + 1, g_3(x) = x^2 + x + 1, g_4(x) = x^2 + 1, g_6(x) = x^2 - x + 1,$$
$$g_8(x) = x^4 + 1 \ , \ g_{12}(x) = x^4 - x^2 + 1 \ \text{ et } \ g_{24} = x^8 - x^4 + 1$$

Anneau $IF_q[x]$ des polynômes à une indéterminée.

Les corps finis IF_q et les anneaux $IF_q[x]$ sont utilisés en cryptographie.

Les racines primitives modulo q sont calculées avec la :

Proposition 3 :

Un élément g dans le groupe cyclique IF^*_q est une racine primitive si et seulement si g satisfait la congruence :

$$g^{(q-1)/d} \not\equiv 1 \bmod q$$

pour tout diviseur premier d de q – 1

C'est par un algorithme de calcul que l'ont trouve g.

Cet algorithme, mis sous forme de programme, peut être exécuté par ordinateur.

Les polynômes irréductibles dans $IF_q[x]$ peuvent être reconnus avec la :

Proposition 4 :

Un polynôme h (x) dans l'anneau $IF_p[x]$, de degré k, est irréductible si et seulement si il satisfait :

$$p \gcd(h(x), x^{p^t} - x) = 1 \quad \text{pour } t = 1,2,\ldots,[k/2].$$

R .CARANDALL et C .POMERANCE, « Prime Numbers ; A computational Perspective », Springer (2002).

Le calcul des pgcd de 2 polynômes peut être fait par un algorithme, traduit en programme exécutable par ordinateur.

Exemple :

Soit le polynôme

$h(x) = 2x^{10} + 3x^8 + 4x^6 + x^5 + 2x^3 + 3x + 4$

dans le corps IF_q pour q = 3.

Appliquons la proposition 4 pour t = 1, 2, …, 5.

Nous obtenons les polynômes :

$x^3 - x,\ x^9 - x,\ x^{27} - x,\ x^{81} - x,\ x^{243} - x$

Il en résulte que le polynôme h (x) est irréductible dans l'anneau $IF_3[x]$.

Il y a un autre algorithme basé sur les calculs des valeurs h (1), h (2), h (3),…

2. Groupe de Mordell -Weil d'une courbe elliptique sur un corps fini IF $_q$:

Le groupe de Mordell –Weil E (K), d'une courbe elliptique E sur un corps fini K, est fini. Il a fait l'objet de plusieurs publications :

1). « The Arithmetic of Elliptic Curves », Inv.Math.23 (1974) p 197- 206 par Tate.

2). «Counting points on Elliptic Curves over finite fields», Journal de théorie des nombres de Bordeaux (1995) p 219- 254 par SCHOOF.

3). « On Waring's problem in finite fields »,Acta Auth.87 (1998) p 171- 177 par Winterhof.

4). «Elliptic Curves in Cryptography » , volume 265 of London Math Soc.(1999) par Seroussi,Smartand Blake.

5). «Searching for primitives roots in finite fields » ,Math.Comp.58(1992) p 369-380,par Shoup.

6). «Discrete logarithms in finite fields and their cryptographic significance », Lecture Notes in Computer Science 209(1985) p 224 – 313 par Odlyzko.

7). « Calcul du nombre de points sur une courbe elliptique sur un corps fini:aspects algorithmiques », J. Th. Nombres, de Bordeaux 7(1995) p 255 – 282 par Morain.

8). « Redicing elliptic curve logarithms to a finite Field », Trans. Inform.Theory 39(1993) p 1639 – 1446 par Menezes, Okamoto and Vanstne.

9). « Elliptic Curve cryptosystems», Math Comp 48(1987) p 203 – 209 par Koblitz.

Nous pouvons estimer le nombre de points K -rationnels par un théorème de Hasse (1930) :

Proposition 5 :

Soit une courbe elliptique E sur un corps fini K à q éléments.

Alors l'ordre de son groupe de Mordell -Weil satisfait l'inégalité :

$$\left| card E(K) - q - 1 \right| \leq 2\sqrt{q}$$

Preuve :

Soit l'endomorphisme de Frobenius :

$$\varphi : E(IF_q) \rightarrow E(IF_q)$$

de valeur $\varphi(x, y) = (x^q, y^q)$.

Alors, le noyau de l'endomorphisme 1 -φ et légalité $x^q = x$ impliquent :

E (K) = ker (Id -φ)

Ceci implique :

card E(K)= card (ker (Id -φ))

La propriété d'isogénie implique:

degré (Id -φ)= card. (ker (Id -φ))

Les propriétés des degrés des isogénies séparables impliquent :

degré (Id -φ)= deg (φ) – trace (φ) + 1

Plus de détails dans « The Arithmetic of Elliptic Curves » par J. H .Silvermann.

3. Groupe formel et invariant de Hasse :

Introduisons un groupe formel pour étudier une courbe elliptique E d'équation de Weierstrass :

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

L'équation de Weierstrass (1) est transformée par le changement rationnel de variables :

$$(x, y) \longmapsto (\frac{z}{w}, -\frac{1}{w}) \qquad (2)$$

d'où :

$$z = -\frac{x}{y} \quad , \quad w = -\frac{1}{y} \quad , \qquad (3)$$

Avec le calcul, nous obtenons une nouvelle équation implicite :

$$w = z^3 + (a_1z + a_2z^2)w + (a_3 + a_4z)w^2 + a_6w^3 \qquad (4)$$

Le point à l'infini $O_E = (\infty, \infty)$ dans le plan x O y devient, dans le plan (z, w) le point

$O_E = (0, 0)$. (5)

En remplaçant dans (4), w dans le deuxième membre, nous obtenons une fonction w (z):

$$w = z^3 + a_1 z^4 + (a_1^2 + a_2) z^5 + (a_1^3 + 2a_1 a_2 + a_3) z^6 + \qquad (6)$$

$$(a_1^4 + 3a_1^2 a_2 + 3a_1 a_3 + a_2^2 + a_4) z^7 + \ldots \in \mathrm{ZI}\,[[a_1, a_2, a_3, a_4, a_6]]$$

Ce développement formel se met sous la forme :

$$w = z^3 (1 + A_1 z + A_2 z^2 + A_3 z^3 + \ldots) \qquad (7)$$

où les coefficients A_n sont des polynômes « homogènes de degré n» dans l'anneau de polynômes ZI $[a_1, a_2, a_3, a_4, a_6]$.

En utilisant l'équation (6) et le changement de variables (2), nous obtenons les séries de Laurent pour x et y :

$$x = z^{-2} - a_1 z^{-1} - a_2 - a_3 z - (a_4 + a_1 a_3) z^2 + \ldots$$

$$y = -z^{-1} x = z^{-3} + a_1 z^{-2} + \ldots \qquad (8)$$

La formule de l'invariant différentiel ω et les formules (6) et (8) impliquent le développement formel :

$$\omega = (1 + a_1 z + (a_1^2 + a_2) z^2 + (a_1^3 + 2a_1 a_2 + a_3) z^3 +$$

$$(a_1^4 + 3a_1^2 a_2 + 3a_1 a_3 + a_2^2 + a_4) z^4 + \ldots)\, dz. \qquad (9)$$

Pour trois points P_1, P_2, P_3 de la courbe elliptique E tels que

$$P_1 + P_2 = P_3 \text{ , avec } P_i = (z_i, w_i) \qquad (10)$$

nous posons $z_3 = F(z_1, z_2)$ .C'est une série formelle en $z_1$et z_2 :

$$F(z_1, z_2) = z_1 + z_2 - a_1 z_1 z_2 - a_2 (z_1^2 z_2 + z_1 z_2^2)$$

$$- 2a_3 z_1^3 z_2 - (a_1 a_2 - 3a_3) z_1^2 z_2^2 + 2a_3 z_1 z_2^3 + \ldots \qquad (11)$$

Ainsi nous avons obtenu le groupe formel $F(z_1, z_2)$ à un paramètre z.

Pour les sommes 2P, 3P, …, n P, l'abscisse z (n P) est une fonction de l'abscisse z (P).

Proposition 6 :

Pour tout entier $n \geq 1$ et pour une courbe elliptique E sur IF_q, les coordonnées d'un point n P de E satisfont la relation :

$$z\,(n\,P) = z\,\psi_n\,(z\,(P))$$

où les fonctions ψ_n sont déterminées par les formules de récurrence :

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

D'après « Arithmetic of Elliptic Curves »de Tate.

3.1. Hauteur du groupe formel d'une courbe elliptique :

Dans le groupe formel à un paramètre en caractéristique p > 0, les séries ψ_p sont de la forme :

$$\psi_p = c_1 z^{p^h} + c_2 z^{2p^h} + c_3 z^{3p^h} + \ldots, \quad \text{avec } c_1 \neq 0 \qquad (12)$$

où h est un entier ≥ 1

Pour h = ∞, on pose $\psi_p(z) = 0$.

Définition 1 :

L'entier h est la hauteur du groupe formel de la courbe elliptique E sur un corps fini IF_q à $q = p^n$ éléments.

La hauteur du groupe formel associé à une courbe elliptique sur un corps fini est déterminée par la :

Proposition 7 :

Soit une courbe elliptique E, sur un corps fini de caractéristique p. Alors ;

la hauteur h du groupe formel associé à la courbe elliptique E est égale à 1 ou 2.

Preuve :

La multiplication par p :

$$E(IF_q) \rightarrow E(IF_q), \qquad R \rightarrow pR$$

est une isogénie de degré p^2.

Alors, p^h est la partie inséparable de p^2 ; donc h = 1 ou 2.

3.2. Invariant de Hasse d'une courbe elliptique:

Cette hauteur permet de définir l'invariant de Hasse.

Définition 2 :

Lorsque la hauteur h du groupe formel associé à la courbe elliptique E est égale à 2, l'invariant de Hasse est égal à Hasse (E)= 0.

Lorsque la hauteur h du groupe formel associé à la courbe elliptique E est égale à 1, l'invariant de Hasse est égal à Hasse (E)= 1.

Cet invariant de Hasse classifie les courbes elliptiques en 2 classes :

1) Les courbes elliptiques ordinaires qui ont un invariant *Hasse (E)= 1*.
2) Les courbes elliptiques supersingulières qui ont un invariant *Hasse (E)*= 0.

4. Courbes elliptiques supersingulières :

Ces courbes elliptiques E (IF_q) ont un discriminant $\Delta(E) \neq 0$, donc elles ne sont pas singulières.

Pour les déterminer, nous pouvons utiliser la définition de l'invariant Hasse (E). L'algorithme de calcul repose sur le groupe formel F (z_1, z_2) et les séries ψ_p.

Il existe un autre moyen de trouver des courbes elliptiques E (IF_q) supersingulières.

Proposition 8 :

Une courbe elliptique E sur un corps fini K de caractéristique p≠ 2, d'équation de Weierstrass

$$y^2 = f(x) \in K[x, y]$$

est supersingulière si et seulement si le coefficient de $x^{(p-1)}$ *dans le développement de la puissance* $(f(x))^{(p-1)/2}$ *est nul.*

Exemple:

La courbe elliptique E d'équation de Weierstrass :

$$E : y^2 = x^3 + 1 \in IF_q[x, y]$$

Sur un corps fini IF_q de caractéristique $p \equiv 2 \bmod 3$, le coefficient de x^{p-1} dans le développement $(f(x))^{(p-1)/2}$ est nul.

Donc la courbe elliptique E est supersingulière.

Un nombre premier $p \equiv 1 \bmod 3$, est de la forme $p = 6s + 1$

Il en résulte $\frac{p-1}{2} = 3s$

Dans le développement $(f(x))^{3s}$ le coefficient de x^{6s} est égal à

$$\binom{3s}{2s} = \frac{(3s)!}{(2s)!s!} = \frac{(2s+1)(2s+2)...(3s)}{s(s-1)(s-2)...1} \neq 0.$$

Donc la courbe elliptique E est ordinaire.

Proposition 9 :

Soit un corps K de caractéristique p> 2, l'entier $m = (p-1)/2$, et le polynôme :

$$H_p(t) = \sum_{i=0}^{m} \binom{m}{i}^2 t^i$$

Alors, la courbe elliptique E

$$E : y^2 = x(x-1)(x-\lambda) \quad \text{où } \lambda \neq 0,1.$$

est supersingulière si et seulement si $H_p(\lambda)=0$

Preuve :

Nous utilisons la proposition 8.

Le coefficient de x^{p-1} dans le développement $(x(x-1)(x-\lambda))^m$ est alors le coefficient de x^m dans le développement $((x-1)(x-\lambda))^m$,qui est égal à :

$$\sum_{i=0}^{m}\binom{m}{i}(-\lambda)^{i}\binom{m}{m-i}(-1)^{m-i}$$

Cette formule est différente du polynôme $H_p(\lambda)$ par le facteur $(-1)^m$.

Il en résulte que la courbe est supersingulière si $H_p(\lambda) = 0$.

Plus de détails dans « The Arithmetic of Elliptic Curves » par J. H .Silvermann

Le polynôme $H_p(t)$ admet un nombre fini de zéros ; il en résulte un nombre fini de courbes elliptiques supersingulières sur un corps fini IF_q, $q = p^n$

Corollaire :

Sur un corps fini IF_q, $q = p^n$, il y a un nombre fini N_p de courbes elliptiques supersingulières :

$$N_p = [p / 12] + s_p, \text{ où } s_p = 1 \text{ pour } p \equiv 1, 5, 7, 11 (\text{mod}.12).$$

Exemple:

La courbe elliptique E d'équation de Weierstrass :

$$E : y^2 = x^3 + 15x - 4 \in IF_q[x, y]$$

Discriminant $\Delta(E) = -16 \times 12 \times 43 = -3 \times 64 \times 43$

condition $\Delta(E) \neq 0$ dans IF_p satisfaite pour $p \neq 2, 3$ et 43.

1) pour p =5, l'équation de la courbe :

$$E : y^2 = x^3 + 1 \in IF_5[x, y]$$

Calcul de $f(x)^{(p-1)/2} = f(x)^2$

$$f(x)^2 = x^6 + 2x^3 + 1$$

Il en résulte que coefficient de x^4 est égal à 0, donc la courbe elliptique E est supersingulière.

2) pour p =7, l'équation de la courbe :

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

Calcul de $f(x)^{(p-1)/2} = f(x)^3$

$$f(x)^3 = x^9 + 3x^7 + 6x^6 + 3x^5 + 18x^4 + 28x^3 + 9x^2 + 27$$

Il en résulte que coefficient de x^6 est égal à $6 \neq 0$, donc la courbe elliptique E est ordinaire.

3) pour p =11, l'équation de la courbe :

$$E : y^2 = x^3 + 4x + 7 \in IF_{11}[x, y]$$

Le calcul de $f(x)^{(p-1)/2} = f(x)^5$ implique que :

le coefficient de x^{10} est égal à $6 \pmod{11} \neq 0$.

Donc la courbe elliptique E est ordinaire.

4) pour p =13, l'équation de la courbe :

$$E : y^2 = x^3 + 2x + 9 \in IF_{13}[x, y]$$

Le calcul de $f(x)^{(p-1)/2} = f(x)^6$ implique que :

le coefficient de x^{12} est égal à $7 \pmod{13} \neq 0$.

Donc la courbe elliptique E est ordinaire.

5) pour p =17, l'équation de la courbe :

$$E : y^2 = x^3 + 15x - 4 \in IF_{17}[x, y]$$

Le calcul de $f(x)^{(p-1)/2} = f(x)^8$ implique que :

le coefficient de x^{16} est non nul (mod.17) .

Donc la courbe elliptique E est ordinaire.

Dans ces 5 cas il y a une courbe supersingulière et 4 courbes ordinaires.

Références

[1] *A .Frohlich* « Formal Groups », Lecture Notes in Mathematics 74 (1968)

[2] *A .Ogg* « Modular Forms and Dirichlet series », Benjamin, New-York (1968).

[3] *A .W .Knapp* « Elliptic Curves », Princeton University Press, New-Jersey (1992).

[4] *B .J .Birch and H .P .F .Swinnerton Deyer* « Notes on Elliptic Curves, I and II», Jour.Reine Ang.Math.212 (1963)7-25 et n° 218(1965)79-108.

[5] *B .Mazur* « Rational Isogenies of prime degree », Inv.Math.44 (1978), 129-162.

[6] *D .B .Zagier* « L –séries of elliptic curves », Amer.Math.Soc.31 (1984)739-743.

[7] *D .Husermoler* « Elliptic Curves», Springer Verlag, New-York (1987)

[8] *D .Weil* « Courbes algébriques et variétés abéliennes», Hermann (1971).

[9] *G .Shimura* «Introduction to the ArithmeticTheory of Automorphic Functions», Publi.Math.Soc Japan n° 11 (1971).

[10] *J .E .Cremona*« Algorithms for Modular Elliptic Curves », Cambridge University Press, (2 nd -1997).

[11] *J .H .Silvermann* « The Arithmetic of Elliptic curves », GTM 106(1986).

[12] *J. P. Serre* «Propriétés Galoisiennes des points d'ordre fini des courbes elliptiques », Invt.Math.15 (1972)259-331.

[13] *J. Tate* « The Arithmetic of Elliptic Curve » Ivent. Math 23(1974) ,179-206.

[14] *J. W. S Cassels* « Diophantine Equations with special reference to elliptic curves », J .London. Math.Soc41 (1966), 193-291.

[15] *N. Koblitz* « Introduction to Elliptic curves and Modular Forms », GTM 97(1984).

[16] *R . Hartshorne* « Algebraic Geometry » Springer Verlag (1977)

[17] *S .Lang* « Elliptic Curves, Diophantine Analysis » Springer Verlag (1978)

[18] *Schoof* « Elliptic Curves over Finite Fields and the Computation of Square Roots mod p » Mathematics of computation volume 44, number 170(April 1985), 483-494.