N° d'ordre : 32 / 2004 - M / MT .

Université des Sciences et de la Technologie
Houari Boumediene

جامعة هواري بومدين
للعلوم والتكنولوجيا
U S T H B

Faculté de Mathématiques

Mémoire présenté pour l'obtention du diplôme de Magister
En Mathématiques

Spécialité : Algèbre et Théorie des Nombres

Par : M^elle LAGHLIEL SAIDA

Sujet

Fonctions modulaires et courbes elliptiques

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

Soutenu publiquement le : 16 / 12 / 2004 , devant le jury composé de :

Mr Kamel BETINA	Professeur à l' U.S.T.H.B	Président .
Mr Mohamed ZITOUNI	Professeur à l' U.S.T.H.B	Directeur de thèse .
Mr M.S.HACHAICHI	Professeur à l' U.S.T.H.B	Examinateur .
Mr Rachid BEBBOUCHI	Professeur à l' U.S.T.H.B	Examinateur .
Mr Boualem BENSEBAA	Chargé de cours à l'U.S.T.H.B	Examinateur .

Sommaire

Introduction

La théorie des courbes elliptiques comporte des aspects variés : géométrique , algébrique , analytique , arithmétique , algorithmique .

Dans cette étude , nous nous somme inspirés pour les notions générales des ouvrages de J.H. Silvermann [12], S. Lang [7] , J.W. S. Cassels [4] pour l'arithmétique et la géométrie des courbes elliptiques et de Apostol [1] pour les formes modulaires .

Le chapitre I est consacré à l'arithmétique des courbes elliptiques : somme de 2 points , symétrique d'un point , conditions d'existence de points singulièrs a l'aide de la théorie du résultant de 2 polynômes , nous avons réussi à classifier les cubiques singulieres avec leur invariant $c_4(E)$, nous avons classifier les courbes elliptiques avec leurs discriminants et leurs invariants modulaire .

Dans le chapitre II , nous avons exposons les relations d'isomorphismes entre un réseau complexe L et la courbe elliptique E (L) paramétreé par la fonction P(L) de Weierstrass .

Pour obtenir une forme modulaire nous faisons agir des sous groupes de congruences modulaires sur le demi – plan supérieur $/H = \{z= x+iy \in ¢ ; y>0\}$.

En suivant une technique de Monsky **[8] ,** nous obtenons des abscisses de points rationnels de la courbe elliptique E_a de d'équation de Weierstrass :

$$E_a \ : \ y^2 = x^3 + a\,x$$

Chapitre I

Arithmétique des courbes elliptiques

L'ensemble des courbes algébrique planes se répartit dans plusieurs sous ensembles suivant leurs degrés :

Les courbes d'équations projectives f (x, y, z)=0, de degré 1, sont des droites.

Les courbes d'équations projectives f(x, y, z)=0, de degré 2, sont des cercles et des coniques.

Les courbes d'équations projectives f (x, y, z)=0, de degré 3, sont des cubiques.

1. *Structures algébriques*

Une courbe elliptique possède plusieurs structures :

Une structure de variété abélienne de dimension 1, une structure de courbe algébrique, projective , non singulière , de genre 1 ; une structure de groupe abélien fini ; une structure de schéma séparé , non singulier ,intègre , de dimension 1.

Définition 1 :

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

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

Dans l'équation (1), les cinq coefficients $a_1,...a_6$ 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.

Définition 2 :

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

2. Changement de variables et équations de Weierstrass :

Dans le plan projectif IP^2 (K), l'équation (1) devient un polynôme homogène de degré 3 :

$$E : y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3 ; \quad (2)$$

Le changement de variables pour un corps de carac (K) $\neq 2$:

$$(x, y) = \left(x, \frac{1}{2}(y - a_1x - a_3) \right)$$

élimine les monômes en y et en xy dans (1) ; l'équation (1) de la courbe devient l'équation :

$$E_1 : y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6 \quad (3)$$

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

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

Éliminons le monôme en x^2 et le coefficient 4 par le changement de variables :

$$(x, y) \to \left((x - 3b_2)/36, y/108 \right) \quad (5)$$

pour un corps de carac (K) $\neq 2,3$

Les calculs impliquent l'équation :

$$E_2 : y^2 = x^3 - 27c_4x - 54c_6 \quad (6)$$

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

$$c_4 = b_2^2 - 24\,b_4$$
$$c_6 = 36\,b_2b_4 - b_2^3 - 216\,b_6 \quad (7)$$

Il existe d'autres modèles d'équations de Weierstrass d'une courbe elliptique:

Le modèle de Legendre :

$$E : y^2 + x^3(x-1)(x-\partial) \text{ avec } \partial \neq 1,0 ; \quad (8)$$

Le modèle de Deuring :

$$E : y^2 + axy + y = x^3 \text{ ; avec } a^3 \neq 27 \text{ et pour carac (K)} \neq 3 \quad (9)$$

Equation de Weierstrass où $a_1 = a_2 = a_3 = 0$:

$$E : y^2 = x^3 + Ax + B \ . \quad (10)$$

3. Invariants d'une courbe elliptique :

Une courbe elliptique possède plusieurs invariants : un discriminant Δ(E), un invariant modulaire j (E), un invariant différentiel, un rang r (E),etc...

Définition 3:

Le discriminant d'une courbe elliptique E est un polynôme « homogène en b_{2i} de degré 12 », de l'anneau Z/ [b_2, b_4, b_6, b_8], pour carac(K) ≠2 et 3

$$\Delta(E) = 9b_2b_4b_6 - 8b_4^3 - 27b_6^2 - b_2^2b_8 \quad (11)$$

où on a posé . $b_8 = \frac{b_2b_6 - b_4^2}{4}$

Une courbe elliptique E d'équation de Weierstrass :

$$E : y^2 = x^3 - 27c_4x - 54c_6, \text{ carac (K) } \neq 2 \text{ et } 3$$

a un discriminant de la forme :

$$\Delta(E) = \frac{1}{1728}(c_4^3 - c_6^2) \quad (12)$$

Définition 4 :

L'invariant modulaire d'une courbe elliptique E d'équation de Weierstrass :

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

est l'élément du corps de base K de carac (K) ≠2 , 3 égal à :

$$j(E) = c_4^3 / \Delta(E) \quad (13)$$

L'invariant modulaire d'une courbe elliptique d'équation de Weierstrass :

$$E : y^2 = x^3 + Ax + B \text{ ; avec } 4A^3 + 27B^2 \neq 0$$

est de la forme :

$$j(E) = 4\times 1728\, A^3 / (4A^3+27B^2)\ ; \qquad (14)$$

Définition 5 :

L'invariant différentiel d'une courbe elliptique E d'équation de Weierstrass :

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

est la forme différentielle

$$\omega(E) = \frac{dx}{2y + a_1 x + a_3} = \frac{d\ y}{3x^2 + 2a_2 x + a_4 - a_1 y} \qquad (15)$$

Les dénominateurs sont les dérivées partielles d'ordre un de $f(x,y)$ *;*

$f'_x = a_1 y - 3x^2 - 2a_2 x - a_4$; et $f'_y = 2y + a_1 x + a_3$;

Chacun de ces invariants implique une classification des courbes elliptiques.

Exemple :

Soit une courbe elliptique E d'équation de Weiestrass :

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

Les coefficients a_i sont égaux à :

$a_1= a_2= a_3= a_6= 0$ et $a_4= a$

Le calcul implique les invariants b_{2i} :

$b_2=0$; $b_4=2a$; $b_6= 0$ et $b_8= - a^2$

Nous obtenons par le calcul les valeurs des invariants :

$c_4 = - 48a$; $\Delta(E) =-64a^3$; $j(E)=1728$, $a\neq 0$

$$\omega\ (E) = \frac{dx}{2y} = \frac{d\ y}{3x^2 + a}$$

4. Classification des cubiques planes :

Les cubiques planes sont classifiées, par leurs discriminants $\Delta(E)$ et leurs invariants $c_4(E)$ .Les cubiques non singulières , qui sont des courbes elliptiques sont classifiées par le signe de $\Delta(E)$.

L'existence de point singulier peut être établie à l'aide du résultant de deux polynômes .

4.1. Résultant de deux polynômes de l'anneau K [x] :

Le résultant de deux polynômes est une application de l'algèbre multilinéaire à un anneau de polynômes. Soit un anneau K[x] de polynômes sur un corps commutatif K et 2 polynômes f et g :

$$f(x) = c_0 x^r + c_1 x^{r-1} + c_2 x^{r-2} + \ldots + c_{r-1} x + c_r \text{ , de degré r}$$

$$g(x) = d_0 x^p + d_1 x^{p-1} + d_2 x^{p-2} + \ldots + d_{p-1} x + d_p \text{ , de degré p} \qquad (1)$$

Définition 6 :

L e résultant des 2 polynômes f et g est le déterminant d'ordre r + p :

$$Res(f, g) = \begin{vmatrix} c_0 & c_1 & . & . & . & c_r & 0 & . & . & . \\ 0 & c_0 & c_1 & . & . & . & cr & 0 & . & . \\ . & . & . & . & . & . & . & . & . & . \\ 0 & . & . & . & . & c_1 & c_2 . & & & c_r \\ d_0 & d_1 & . & . & d_p & & & . & . & \\ & & . & & & d_p . & . & . & . & . \\ & & & . & . & . & d_p & . & . & . \\ . & . & . & . & . & . & . & . & . & . \\ 0 & . & . & . & . & 0 & d_0 & d_1 & . & d_p \end{vmatrix}$$

p lignes ; *r lignes*

avec r lignes L'$_i$ de (d_0, . . ., dp) , et p lignes L_i de(c_0 , . . ., .c_r)

Res (f,g)=det (L_1,L_2...,L_p,$L`_1$,$L`_2$,...,$L`_r$) ;

les termes manquants sont remplacés par des zéros .

La théorie du résultant Res(f , g) se trouve dans plusieurs livres : " Algebra " de Lang "Introduction à l'algèbre" de Kostrikine , etc…

Les théorèmes suivants sont énoncés sans démonstration.

Théoreme1:

Soient deux polynômes :

$f(x) = c_0(x - \alpha_1)(x - \alpha_2) \ldots (x - \alpha_r)$ *, de degré r*

$g(x) = d_0(x - \beta_1)(x - \beta_2) \ldots (x - \beta_p)$ *, de degré p*

alors , leur résultant est égal à :

$$\mathrm{Res}(f,g)= c_0^{p} d_0^{r} \prod_{i,j}(\alpha_i-\beta_j)$$

□

Ce théorème implique une condition pour que Res (f , g) = 0

Corollaire :

Le résultant de deux polynômes est nul si et seulement si ces deux polynômes ont une racine commune .

□

Le résultant Res(f , f') d'un polynôme f et de sa dérivée f' a des liens avec les racines de f .

Définition7:

Soit un polynôme

$f(x) = c_0(x- \alpha_1) (x-\alpha_2) \dots (x-\alpha_r)$, de degré r

et le polynôme dérivée f'(x) . Son discriminant est égal à :

$$dis(f) = c_0^{2r-2} \prod_{1\le i\langle j\le r}(\alpha_i - \alpha_j)^2 \qquad (1)$$

Le résultant des polynômes f *et* f' est fonction des racines de f :

$$Res\ (f\ ,\ f') = c_0^{2r-1} \prod_{1\le i\le r} \prod_{j\ne i}(\alpha_i - \alpha_j) \qquad (2)$$

Les formules (1) et (2) impliquent la relation entre discriminant et résultant :

$$Res\ (f\ ,\ f') = c_0 (-1)^{\frac{r(r-1)}{2}} dis(f) \qquad (3)$$

Exemples :

1) le discriminant du produit $f g$ de deux polynômes est égal à :
dis(f g) = dis(f) dis (g) Res (f , g)^2 (d'après Kostrikine) (4)

2)Discriminant du polynôme :
f (x)= $x^n + x^{n-1} + \dots + x + 1$
Il est égal à :

$$dis\ (f) = (-1)^{\frac{n(n-1)}{2}} (n+1)^{n-1} \qquad (5)$$

d'après « Introduction à l'Algèbre » Kostrikine

3)Discriminant du polynôme cubique :

$$f(x) = a_0 x^3 + a_1 x^2 + a_2 x + a_3 \qquad (6)$$

Il est égal à :

$$dis\,(f) = 18\,a_0\,a_1\,a_2\,a_3 + a_1^2\,a_2^2 - 4\,a_0\,a_2^3 - 4\,a_3\,a_1^3 - 27\,a_0^2\,a_3^2$$

d'après « Algebra » , Lang

4)Discriminant du polynôme cubique :

$$f(x) = x^3 + A\,x + B$$

Il est égal à :

$$dis\,(f) = -(4A^3 + 27B^2) \qquad (7)$$

d'après « Algebra » , Lang

4)Discriminant du polynôme cubique:

$$f(x) = x^3 + N\,x$$

Il est égal à :

$$dis\,(f) = -4N^3 \qquad (8)$$

Le résultant Res (f , f') peut être obtenu avec le:

Théorème2 :

Soit un polynôme :

$$f(x) = c_0\,(x - \alpha_1)\,(x - \alpha_2)\,\ldots(x - \alpha_r)\ ,\ de\ degré\ r$$

et sa dérivée f' (x) , alors le résultant de f est égal à :

$$\mathrm{Res}\,(f, f') = c_0^{\,r-1} \prod_{i=1}^{r} f'(\alpha_i) \qquad (9)$$

□

Ce résultant est lié au discriminant dis (f) du polynôme f (x) par les formules :

$$dis\,(f) = c_0^{\,2r-2} \prod_{i \prec j} (\alpha_i - \alpha_j)^2 \quad et \quad \mathrm{Res}(f, f') = c_0\ dif\ (f). \qquad (10)$$

4.2. Cubiques singulières :

Considérons une cubique plane E d'équation de Weierstrass :

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

L'équation (1), mise sous la forme implicite $f(x, y) = 0$ admet des dérivées partielles f'_x et f'_y d'ordre un.

Lorsque le système $f'_x = f'_y = 0$ n'admet pas de solution, la courbe est non singulière, d'après la théorie des points singuliers d'une courbe plane.

Lorsque ce système admet une solution *(x, y)* = P , ce point P est un point singulier de E ; ce point est un nœud si E admet 2 tangentes distinctes en P ; P est un point de rebroussement si E admet 2 tangentes confondues en P.

Le discriminant et la nature de ces racines peuvent être déterminés avec la théorie du résultant de 2 polynômes.

Les cubiques singulières sont classifiées par le :

Théorème 3 :

Soit une cubique plane E d'équation de Weierstrass :

$$E : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4x + a_6 \in K[x,y]$$

son discriminant Δ (E) , son invariant $c_4(E)$ et son point à l'infini $O_E = (\infty, \infty)$

1) *Le point O_E = (0, 1,0) est un point non singulier sur E ;*
2) *La cubique E est singulière si et seulement si Δ (E) = 0*
3) *La cubique E possède un nœud si et seulement si Δ (E) = 0 et c_4 (E) $\neq$ 0*
4) *La cubique E possède un point de rebroussement si et seulement si*

Δ (E) =0 et $c_4(E) = b_2^2 - 24\, b_4 = 0$.

Preuve : *« O_E est un point non singulier de E »*

On utilise les propriétés du résultant Res (f, f') et la relation entre le discriminant dis(f) *de* f et le discriminant Δ *(E)* de E

Dans le plan projectif IP^2, l'équation de la courbe se met sous la forme :

$$f(x, y, z) = y^2z + a_1xyz + a_3yz^2 - x^3 - a_2x^2z - a_4xz^2 - a_6z^3 = 0 \quad (2)$$

Au point O_E, la fonction f prend la valeur :

$$f(0, 1,0) = 0. \quad (3)$$

Il en résulte que ce point O_E est sur la courbe E.

La dérivée partielle f'_z prend au point O_E la valeur $f'_z(0, 1,0) = 1 \neq 0$;

Cela implique que ce point n'est pas singulier sur la courbe E.

Preuve de « E est une cubique singulière » implique « son discriminant est nul »:

Nous prenons une équation de la forme :

$$E : y^2 = f(x) \quad (4)$$

L'hypothèse « E est singulière » implique que le polynôme $f(x)$ admet une racine multiple d'ordre 2 ou 3.

Par la théorie du résultant de deux polynômes

$$\text{Res}(f, f') = 0 \quad (5)$$

La relation entre Res (f, f') et discriminant dis (f) de f et (5) impliquent la valeur :

$$\text{dis}(f) = 0 \quad (6)$$

La relation entre les discriminants de f et de la courbe E implique :

$$\Delta(E) = 0 \quad (7)$$

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

Soit une cubique E de discriminant $\Delta(E) = 0$

La relation entre les discriminants de E et de f implique :

$$\text{dis}(f) = 0 \quad (8)$$

Par la théorie des points singuliers, cette relation implique que le polynôme $f(x)$ admet une racine multiple d'ordre 2 ou 3.

Il en résulte que la cubique E est singulière .

Preuve de « $\Delta(E) = 0$ et $c_4(E) \neq 0$ *» implique « la cubique E admet un nœud »*

L'hypothèse $\Delta(E) = 0$ implique que la cubique E est singulière

Considérons une équation de la cubique E de la forme :

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

Donc cette équation admet une racine double

Cette racine double détermine un point singulier de la cubique E

Les pentes des tangentes en ce point sont égales à la dérivée y' de y :

$$y' = \frac{6x^2 + b_2 x + b_4}{y} = \frac{N(x)}{y}$$

L'hypothèse $c_4 \neq 0$ et la formule (7) impliquent le discriminant du polynôme $N(x)$:

$$\text{dis}(N(x)) = b_2^2 - 24\, b_4 = c_4(E) \neq 0$$

Cela implique que le polynôme N(x) admet 2 racines simples

Donc E admet deux tangentes distinctes

Il en résulte que la cubique E admet un nœud.

Preuve de « la cubique E admet un point de rebroussement » implique *« $c_4 = 0$ »*

L'hypothèse *« la cubique E admet un point de rebroussement »* implique *« la cubique E est singulière »*

D'après le théorème (1), le discriminant de E est nul :

$$\Delta(E) = 0$$

La cubique E a une équation de Weiestrass de la forme *:*

$$y^2 = 4x^3 + b_2 x^2 + 2b_4 x + b_6$$

La dérivée y' de y est égale à :

$$y' = \frac{6x^2 + b_2 x + b_4}{y} = \frac{N(x)}{y}$$

L'hypothèse *« deux tangentes confondues »* implique que le polynôme N(x) admet une racine double.

Cela implique que son discriminant dis(N(x)) = c_4(E) est nul .

□

Les cubiques non singulières , qui sont donc des courbes elliptiques , sont classifiées par le **:**

Théorème 4 :

Soit une courbe elliptique E d'équation de Weierstrass :

$$E : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \in /R[x,y]$$

et de discriminant $\Delta(E)$

1) *La courbe elliptique E coupe l'axe Ox en 3 points, simples, si et seulement si* $\Delta(E) > 0$ *;*

2) *La courbe elliptique E coupe l'axe Ox en un seul point, simple, si et seulement si* $\Delta(E) < 0$

Preuve de «E coupe Ox en 3 points simples » implique *« Δ(E) >0 » :*

Soit une courbe elliptique E d'équation de Weierstrass :

$$E : y^2 = x^3 + a_2x^2 + a_4x + a_6 = f(x) \in /R[x,y] \quad (1)$$

D'après le théorème 2 :

$$\Delta(E) \neq 0 \quad (2)$$

Soient $(e_i, 0)$; i=1, 2, 3, les trois points d'intersection de l'axe Ox par la courbe E.

Alors, E a une équation de Weierstrass :

$$y^2 = (x-e_1)(x-e_2)(x-e_3) = f(x) \text{ , avec } e_i \neq e_j \quad (3)$$

Par définition du discriminant d'un polynôme, celui de $f(x)$ est égal à :

$$dis(f) = \prod_{1 \le i \le j \le 3} (e_i - e_j)^2 \quad (4)$$

L'hpothése « 3 racines e_i réelles », implique que les carrés

$$(e_i - e_j)^2 > 0 \quad (5)$$

Il en résulte :

$$dis(f) > 0$$

Le discriminant d'une courbe elliptique E d'équation de Weierstrass

$$E : y^2 = x^3 + a_2x^2 + a_4x + a_6 = f(x) \text{ ;}$$

est lié au discriminant dis (f) par la relation :

$$\Delta(E) = 16 \, dis(f) \quad (6)$$

Les relations (5) et (6) impliquent $\Delta(E) > 0$

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

Soit une courbe elliptique E qui coupe l'axe Ox en un seul point (e,0), simple (7)

Donc E a une équation de la forme :

$$y^2 = (x - e)(x^2 + r\,x + s) = f(x) \text{ avec } r^2 - 4s < 0 \quad (8)$$

Le polynôme du 2ème degré, dans (8), admet 2 racines complexes de la forme :

$$e_i = \frac{1}{2}(-r \pm i\sqrt{4s - r^2}) \quad (9)$$

Il en résulte que le discriminant du polynôme $f(x)$ est égal à :

$$\text{dis}(f) = [e - \frac{r}{2} + \frac{i}{2}\sqrt{4s - r^2}\,][e - \frac{r}{2} - \frac{i}{2}\sqrt{4s - r^2}\,]^2\,[\,i\sqrt{4s - r^2}\,]^2$$

Le calcul implique que le discriminant du polynôme $f(x)$ est égal à :

$$\text{dis}(f) = -(4s - r^2)\,[\,(e - \frac{r}{2})^2 + \frac{4s - r^2}{4}\,] \prec 0 \quad (10)$$

Il en résulte le signe :

$$\text{dis}(f) < 0 \quad (11)$$

La relation entre les discriminants de E et de $f(x)$ et (11) impliquent :

$$\Delta(E) < 0 \quad (12)$$

□

Ces théorèmes (3) et (4) permettent une classification des cubiques .

Corollaire :

Les cubiques planes E sont classifiées par leur discriminant $\Delta(E)$ et leur invariant $c_4(E)$ en 4 ensembles .

1)l'ensemble ξ_1 des cubiques qui ont un nœud :

$$\Delta(E) = 0 \quad et\ c_4(E) \neq 0$$

2)l'ensemble ξ_2 des cubiques qui ont un point de rebroussement :

$$\Delta(E) = c_4(E) = 0$$

3)l'ensemble ξ_3 des courbes qui coupent l'axe 0x en 3 points simples :

$$\Delta(E) > 0$$

5) l'ensemble ξ_4 des courbes qui coupent l'axe 0x en un point simple :

$$\Delta(E) < 0$$

Preuve : avec les deux théorèmes 3 et 4 précédents.

□

Illustrons ce corollaire par un exemple de chaque ensemble .

Exemple1 :cubique E_1 qui admet un nœud .

Soit la cubique E_1 d'équation de Weierstrass :

$E_1 : y^2=x^3+4x^2+5x+2$

Avec le calcul nous obtenons les invariants :

$b_2=16$; $b_4=10$; $b_6=8$; $b_8=7$; $c_4=16$ et $\Delta(E_1) = 0$

L'invariant $c_4 \neq 0$ implique que la cubique plane E_1 admet un nœud.

Les coordonnées de ce nœud sont les solutions du système d'équations algébriques :

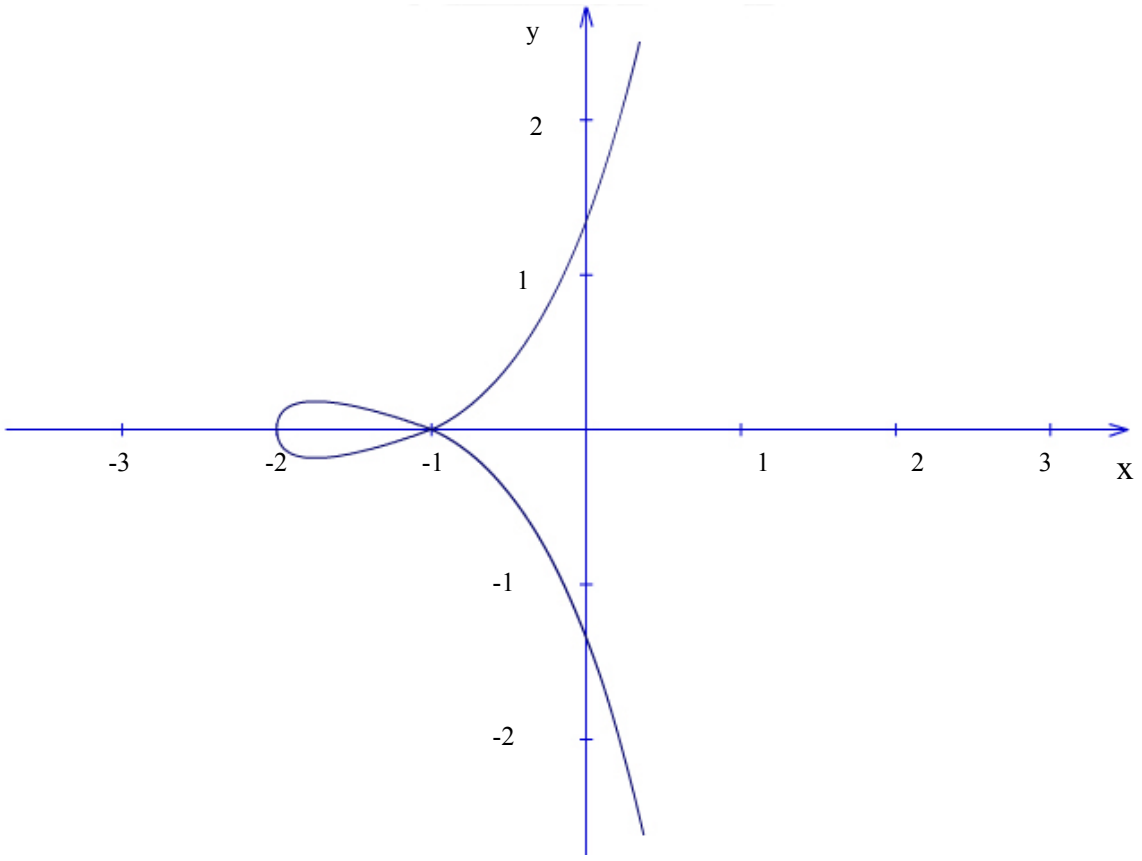
$$\begin{cases} f(x,y) = y^2 - x^3 - 4x^2 - 5x - 2 = 0 \ , \ f'_x(x, y) = -3x^2-8x-5=0 \\ f'_y(x, y) = 2y = 0 \end{cases}$$

Nous obtenons la solution (-1,0)

Donc le nœud de E_1 est le point (-1,0)

Tableau de valeurs des coordonnées de quelques points de la courbe E_1 :

x	-2	-1	0	1	2	3
y^2	0	0	2	12	36	80
y	0	0	$\pm\sqrt{2}$	$\pm 2\sqrt{3}$	± 6	$\pm 4\sqrt{5}$



Exemple 2 :Cubique E_2qui admet un point de rebroussement

Soit la cubique plane E_2 d'équation de Weierstrass :

$$E_2 : y^2=x^3-6x^2+12x-8$$

Nous obtenons les valeurs des invariants :

$b_2=-24$, $b_4=24$et $b_6=-32$; $b_8= 48$; $c_4(E_2)=0$; $\Delta(E_2)=0$

Les valeurs $\Delta(E_2) = c_4(E_2)=0$ impliquent que la cubique E_2 possède un point de rebroussement.

Les coordonnées de ce point sont les solutions du système :

$$\begin{cases} f(x,y) = y^2 - x^3 + 6x^2 - 12x + 8 = 0 \\ f'_X(x,y) = -3x^2+12x-12 = 0 \\ f'_Y(x,y) = 2y = 0 \end{cases}$$

Nous obtenons le système :

$$\begin{cases} x^3-6x^2+12x-8 = 0 \\ x^2 -4x+4 = 0 = (x-2)^2 \end{cases}$$

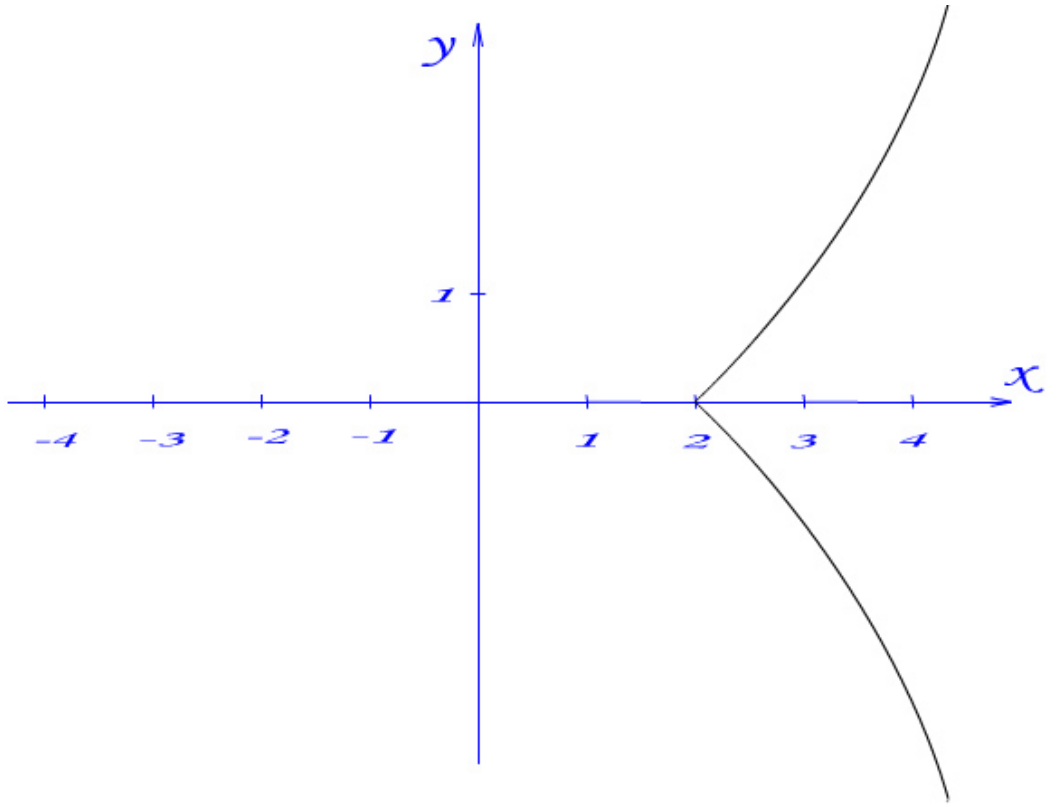
Ce système admet la solution $x=2$, $y = 0$

Donc le point de rebroussement est le point (2,0)

Tableau de valeurs des coordonnées de quelques points de la cubique E_2:

x	0	1	2	3	4	5	6
y^2	- 8	- 1	0	1	8	27	64
y	Non	Non	0	± 1	$\pm 2\sqrt{2}$	$3\sqrt{3}$	± 8

La cubique plane E_2 :



Exemple3 : courbe elliptique E_3 qui coupe l'axe Ox en 3 points :

Soit la courbe elliptique E_3 d'équation de Weierstrass :

$E_3 : y^2=x^3+ 7x^2+14x+8$

Le calcul implique les invariants :

$b_2=28, b_4=28, b_6=32$ et $b_8=28$; $c_4(E_3)=112$ et $\Delta(E_3)=576$

$\Delta(E_3)>0$ implique que cette courbe elliptique coupe Ox en 3 points simples.

Pour construire cette courbe elliptique E_3, déterminons ses trois points d'intersection avec l'axe Ox.

Les solutions rationnelles de l'équation :

$$f(x) = y^2= x^3+ 7x^2+14x+8 \qquad (16)$$

se calculent avec le:

Théorème 5 :

Soit une équation diophantienne :

$x^n+d_1x^{n-1}+\ldots+d_n=0$

Alors toute solution de cette équation est un diviseur du coefficient constant d_n.

□

Dans l'équation (16), le terme constant est $d_3=8$; donc toute solution de (16) est un diviseur de 8.

Les diviseurs de 8 sont $\pm 1, \pm 2, \pm 4, \pm 8$

Avec les tests $f(d)$ nous obtenons , les trois zéros du polynôme $f(x)$ qui sont :

-1 , -4 et –2

Il en résulte la factorisation du polynôme :

$x^3+7x^2+14x+8 =(x+1)(x+4)(x+2)$

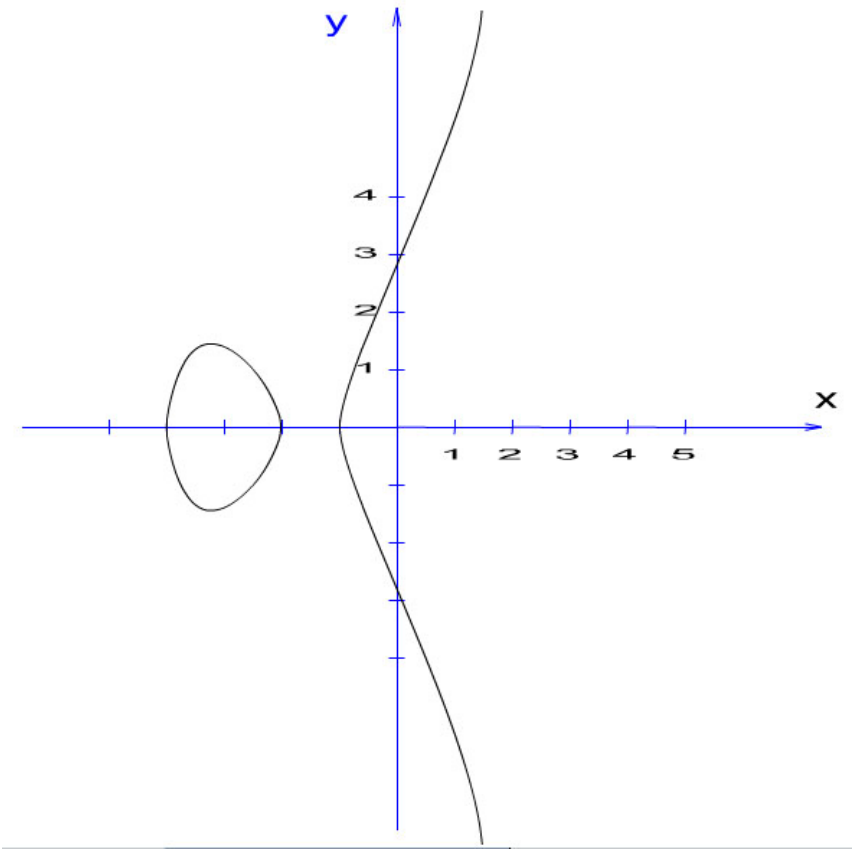
Donc la courbe E_1 coupe l'axe Ox aux 3 points :

$P_1= (-1,0)$; $P_2= (-4,0)$ et $P_3=(-2,0)$

Tableau de valeurs des coordonnées de quelques points de la cubique E_3

x	-4	-3	-2	-1	0	1	2
y^2	0	2	0	0	8	30	72
y	0	$\pm\sqrt{2}$	0	0	$\pm 2\sqrt{2}$	$\pm\sqrt{30}$	$\pm 6\sqrt{2}$

Courbe elliptique E_3



Exemple 4 : courbe elliptique E_4 qui coupe l'axe Ox en 1 seul point :

Soit la Courbe elliptique E_4 d'équation de Weierstrass :

$E_4 : y^2=x^3+4x^2-2x+1$

Nous obtenons par le calcul les valeurs des invariants de E_4 :

$c_4(E_4) = 352$ et $\Delta(E_4) = -9904$

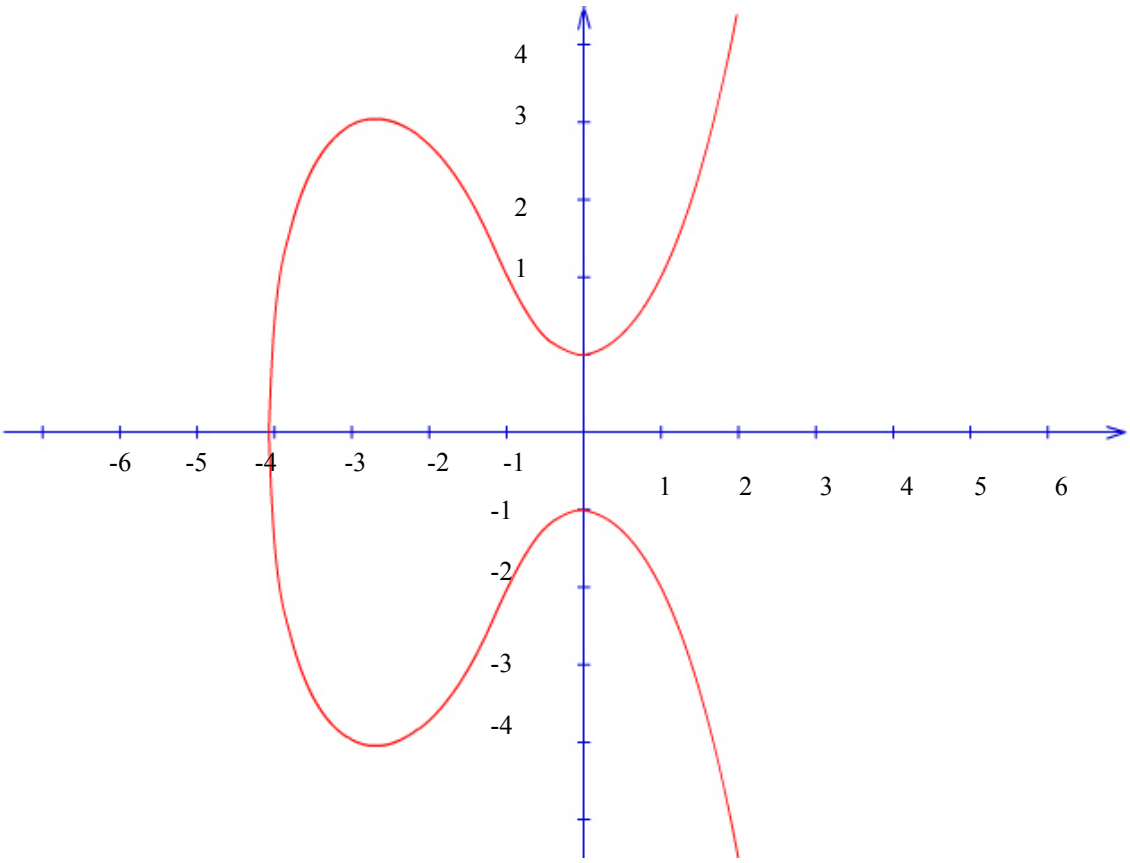
$\Delta(E_2) < 0$ implique que cette courbe elliptique coupe Ox en un seul point.

Le point d'intersection avec l'axe Ox a une abscisse a entre - 4,25 et – 4

Tableau de valeurs des coordonnées de quelques points :

x	-4	-3	-2	-1	0	1	2	3
y2	9	16	13	6	1	4	21	58
y	±3	±4	$\pm\sqrt{13}$	$\pm\sqrt{6}$	±1	±2	$\pm\sqrt{21}$	$\pm\sqrt{58}$

Courbe elliptique E_4



5- Structure de groupe abélien de Mordell - Weil:

Considérons l'ensemble E (K) des points K rationnels d'une courbe elliptique E et le point à l'infini $O_E = (\infty,\infty)$ dans le plan affine /A (K) ; $O_E = (0, 1,0)$ dans le plan projectif IP^2 (K).

Construisons un groupe additif abélien, d'élément neutre le point O_E , par l'application :

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

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

Cette somme s'obtient par la règle géométrique de 3 points colinéaires de la courbe E

« 3 points colinéaires d'une courbe elliptique E ont une somme nulle »

$$P_1+P_2+P_3=O_E$$

Vérifions les axiomes d'un groupe abélien :

1)Axiome de l'élément neutre :

L'élément neutre du groupe est le point à l'infini O_E ; ce point est déterminé par la direction de l'axe Oy.

$P+O_E = O_E+P = P$, pour tout point $P \in E$.

2)Axiome du symétrique :

Le symétrique d'un point P de la courbe est le point P`qui se trouve à l'intersection de la parallèle à Oy passant par P et de la courbe.

$P + P' = P' + P = O_E$; pour tout point $P \in E$.

(figure 1)

3)Axiome d'associativité : il est vérifié par les calculs des sommes.

$(P_1 + P_2) + P_3$ et $P_1 + (P_2 + P_3)$.

4)Axiome de commutativité : il est vérifié par la coïncidence des sécantes P Q et Q P qui implique l'égalité .

$P + Q = Q + P$

Calcul des coordonnées du symétrique d'un point P de la cubique E :

Considérons la parallèle à 0y passant par le point P . Elle recoupe la courbe E au point P' ; c'est le symétrique de P ; les abscisses de P et de P' sont égales :

$$x_P = x_{P'}$$

les ordonnées sont solutions de l'équation en y .

$$y^2 + y(a_1x+a_3) = x_p^3 - a_2x_p^2 - a_4x_p - a_6 \quad . \qquad (1)$$

La somme des 2 racines est une fonction symétrique élémentaire

$$y_p + y_{p'} = -a_1x_p - a_3 \quad . \qquad (2)$$

Il en résulte les coordonnées du point –P symétrique du point P :

$$-P = (x_p, -y_P - a_1x_p - a_3) \quad . \qquad (3)$$

Calcul des coordonnées de la somme de deux points

$P_1 + P_2 = M$; $P_1 \neq \pm P_2$.

La sécante $P_1 P_2$ a pour équation :

$$y = y_1 + t(x - x_1) \text{ ; avec } \quad t = \frac{y_1 - y_2}{x_1 - x_2} \tag{4}$$

La sécante $P_1 P_2$ coupe la courbe *E* en 3 points simples $P_i=(x_i , y_i)$ où $1 \leq i \leq 3$

(figure 2)

Les abscisses x_1, x_2, x_3 de ces 3 points P_i sont les zéros de l'équation cubique en x :

$$x^3 + a_2 x^2 + a_4 x + a_6 = \left[y_1 + t(x - x_1)\right]^2 + a_1 x\left[y_1 + t(x - x_1)\right] + a_3\left[y_1 + t(x - x_1)\right] \tag{5}$$

La fonction symétrique « somme des racines » est égale à :

$$x_1 + x_2 + x_3 = \frac{-coeff \quad x^2}{coeff \quad x^3} = t^2 + a_1 t - a_2 \tag{6}$$

Nous en déduisons le 3ème point d'intersection :

$$P_3=(t^2+a_1t-a_2-x_1-x_2 , y_1+t(x_3-x_1)) \ . \tag{7}$$

La relation géométrique $P_1 + P_2 + P_3 = 0$ implique que le point

$M = P_1 + P_2$ est le symétrique du point P_3

Il en résulte les coordonnées du point M :

$$\begin{cases} x_M = t^2 - a_1 t - a_2 - x_1 - x_2 & , \ t = \dfrac{y_1 - y_2}{x_1 - x_2} \\ y_M = -t^3 - 2a_1 t^2 + t(a_2 - a_1^2 + 2x_1 + x_2) + a_1(a_2 + x_1 + x_2) - y_1 - a_3 \end{cases} \tag{8}$$

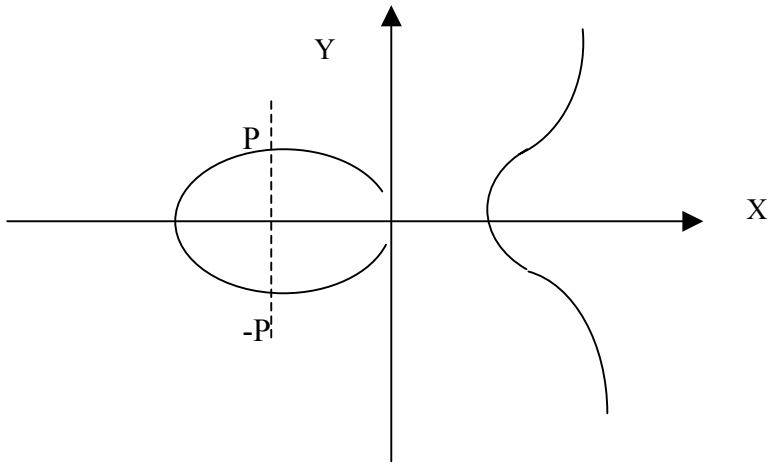


Figure 1

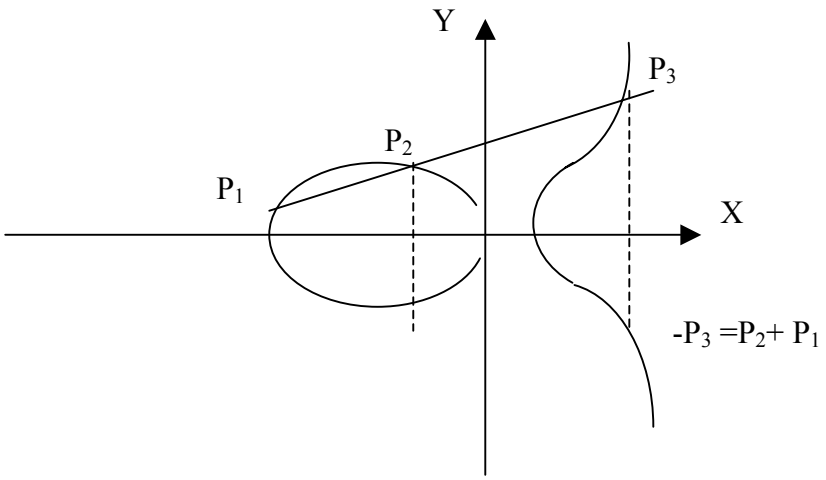


Figure 2

Nous avons démontré le :

Théorème 6:

1) L'ensemble E (K) des points K rationnels d'une courbe elliptique E est un groupe abélien d'élément neutre le point à l'infini O_E *avec la règle géométrique des 3 points colinéaires « $P_1 + P_2 + P_3 = 0_E$ ».*

2)Le symétrique d'un point P(x , y) est le point :

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

3) La somme $P_1 + P_2 = M$ de deux points $P_1 (x_1 , y_1) \neq \pm P_2 (x_2 , y_2)$

est le point de coordonnées :

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

avec $t = (y_1 - y_2)/(x_1 - x_2)$

□

Définition 8 :

Le groupe abélien E (K) est le groupe de Mordell - Weil de la courbe elliptique E sur un corps commutatif K.

6. Points d'ordre fini d'une courbe elliptique :

Soit une courbe elliptique E d'équation de Weiesrtrass :

$$E : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \ , \ a_i \in K\ [x, y]. \qquad (1)$$

Un point P du groupe de Mordell – Weil de la courbe E est d'ordre m s'il satisfait la relation :

$$mP = O_E \ ;$$

le symbole mP signifie :

$$mP = \begin{cases} P+P+\ldots+P, \text{ m fois P lorsque } m>0 \\ (-P)+(-P)+\ldots+(-P), \text{ (-m) fois } -P, \text{ lorsque } m<0 \\ O_E \text{ lorsque } m=0 \end{cases} \qquad (2)$$

Définitions 9 :

1) Le sous groupe de m torsion d'une courbe E est l'ensemble des points P d'ordre m du groupe de Mordell-Weil E (K) :

$$E(K)[m] = \{P \in E \ ; \ m P = O_E\}. \qquad (3)$$

2) Le groupe de torsion du groupe de Mordell- Weil E (K) est l'ensemble des points P du groupe E (K) d'ordre fini :

$T(E) = \{P \in E(K), m P = 0_E \text{ pour } m \geq 0\}$ (4)

Ce groupe est la réunion infinie des sous groupes de m torsion avec $m \in Z/$

Calcul des coordonnées du point P+P=2P

Nous obtenons les coordonnées du point 2P pour P = (x, y) avec la tangente à la courbe E au point P = (x, y) :

$$\begin{cases} x_{2p} = y'^2_p + a_1 y'_p - a_2 - 2x_p \\ y_{2p} = -y'^3_p - a_1 y'^2_p + (a_2 - a_1^2 + 3x_p)\, y'_p + a_1 a_2 - a_3 + 2 a_1 x_p - y_p \end{cases} \quad (5)$$

où $y'_p = \dfrac{3x_p^2 + 2a_2 x_p + a_4 - a_1 y_p}{2y_p + a_1 x_p + a_3}$ (6)

Exemple :

Soit la courbe elliptique E d'équation de Weierstrass :

$E : y^2 = x^3 + 7x^2 + 14x + 8$

Le calcul implique les invariants :

$b_2 = 28, b_4 = 28, b_6 = 32$ et $b_8 = 28$; $c_4(E) = 112$ et $\Delta(E) = 576$

$\Delta(E) > 0$ implique que cette courbe elliptique coupe Ox en 3 points simples.

$P_1 = (-1,0)$; $P_2 = (-4,0)$ et $P_3 = (-2,0)$

Le calcul implique les coordonnées des points :

$2P_1 = O_E$; $2P_2 = O_E$; $2P_3 = O_E$;

$P_1 + P_2 = (-9, 0)$; $P_1 + P_3 = (-11, 0)$; $P_2 + P_3 = (-8, 0)$

Selon Cassels « Diophantine Equation with Special Reference to Elliptic Curves » les coordonnées des points m P, pour m >2, sont déterminées par le:

Théorème 7 *:*

Soit une courbe elliptique E sur le corps Q des nombres rationels d'équation :

$$E: y^2=x^3+Ax+B \in Z/[x,y] \quad ;4A^3 + 27 B^2 \neq 0 \qquad (7)$$

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

$$m\,P = \left(\frac{\phi_m(x,y)}{\psi_m^2(x,y)}, \frac{\omega_m(x,y)}{\psi_m^3(x,y)} \right) ; \qquad (8)$$

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

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

Pour $m \geq 2$ *, les polynômes* ψ_m *satisfont les relations de récurrence :*

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

$$\psi_{2m+1} = \psi_{m+1}\ \psi^3_m - \psi^3_{m-1} \quad ; \qquad (9)$$

Les polynômes numérateurs ϕ_m *et* ω_m *sont égaux à:*

$$\phi_m = x\psi_m^2 - \psi_{m-1}\ \psi_{m+1} \quad ;$$

$$4y\omega_m = \psi_{m+2}\ \psi^2_{m-1} - \psi_{m-2}\ \psi^2_{m+1} \quad ; \qquad (10)$$

Preuve :

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

Pour m = 0 , 0(x , y) = (∞, ∞) =$(\frac{x}{0}, \frac{y}{0})$;donc $\psi_0 = 0$

Pour m = 1 , 1 (x , y) = (x , y) =$(\frac{x}{1^2}, \frac{y}{1^3})$;donc $\psi_1 =1$

Pour m = 2 , 2(x , y) = $(\frac{x}{(2y)^2}, \frac{y}{(2y)^3})$;donc $\psi_2 = 2y$

C'est le lemme 7.2 dans l'ouvrage cité de Cassels .

On peut aussi utiliser une preuve par récurrence sur l'entier m , avec les formules P_1+P_2 du théorème (6) et 2P de (5) .Ce sont des calculs très longs .

Exemple :

Soit la courbe elliptique d'équation de Weierstrass :

$E : y^2 = x^3 + 4x + 25$

La condition $4A^3+27B^2 = 4^4 + 27\,(25)^2 \neq 0$ est satisfaite

Le calcul implique les invariants :

$b_2 = 0$; $b_4 = 8$; $b_6 = 100$; $b_8 = -16$; $c_4(E) = -192$ et $j(E) = (4^7 \times 3^3)/17131$

Le groupe E(Q) contient les deux points P=(0,5) et R=(-2,3)

Le calcul implique les coordonnées du point 2P (appliquons les formules (5) et (6))

La valeur $y' = \frac{3x^2 + 4}{2y}$ au point p=(0 , 5) est égale à :

$$y'(P) = \frac{2}{5}$$

Nous obtenons le point $2P = \left(\frac{4}{25} , \frac{-633}{125} \right)$

Le calcul implique les coordonnées du point 3P=2P+P (appliquons les formules du théorème (6))

$$3P = \left(\frac{15825}{4} , \frac{398277}{8} \right)$$

Le calcul implique les coordonnées du point 4P=2(2P) (appliquons les formules (5) et (6) page 22)

$$4P = \left(-\frac{1582436}{10017225} , \frac{3047428493}{6340903425} \right)$$

Le calcul implique les coordonnées du point 5P (appliquons les formules de Cassels du théorème (7))

$$5P = \left(-\frac{10^3 \times 51945946213}{(25001)^2} , \frac{10^3 \times 65733289219}{(25001)^3} \right)$$

7 – Morphismes de groupes E (K)→ E' (K)

Il existe des homomorphismes entre les courbes elliptiques .Ces homomorphismes sont des isogènies , des isomorphismes , des endomorphismes , des automorphismes .

7-1 Isogénies de courbes elliptiques:

Définition 10 :

Une isogénie de 2 courbes elliptiques E_1 et E_2 est un morphisme de groupes abéliens

$g : \quad E_1(K) \to E_2(K)$

qui satisfait les conditions :

1) *g n'est pas nulle .*
2) *le noyau de l'isogénie est un sous groupe d'ordre fini du groupe* $E_1(K)$.
3) *l'isogénie est surjective .*
4) $g(P_1 + P_2) = g(P_1) + g(P_2)$ *et* $g(0_{E_1}) = 0_{E_2}$

Cette définition est empruntée à Shimura "Introduction to the Arithmetic Theory of Automorphic Forms" , Math . Soc . Japan 11(1971) .
Cette isogénie admet des invariants : le degré , l'isogénie duale .

Définition 11 :

L'ordre du sous- groupe « noyau d'une isogénie » est le « degré de l'isogénie »

Un exemple d'isogénie de courbes elliptiques est constitué par la multiplication par un entier rationnel m sur une courbe elliptique :

$$\lambda_m : E(K) \to E(K)$$

de valeur :

$$\lambda_m (P) = mP$$

Théorème 8 :

Soient deux courbes elliptiques E et E` et une isogènie

$f : E(K) \to E'(K)$, de degré m

Alors il existe une application unique

$$\hat{f} : E'(K) \to E(K)$$

dont les composées satisfont :

$\hat{f} \circ f$ = multiplication par m sur le groupe E(K)

$f \circ \hat{f}$ = multiplication par m sur le groupe E'(K)

Preuve : (cf. Silverman. Chapitre III théorème 1.6)

□

Définition 12 :

Cette application $\hat{f}$ est l'isogénie duale de l'isogénie f.

Les formules d'une isogénie de courbes elliptiques font intervenir des fractions rationnelles contenues dans les formules des coordonnées des points $P_1 + P_2$ et $2P$.

Nous utilisons la méthode de Velu de détermination des formules d'une isogénie de courbes elliptiques (C R A S Paris , série A 273 , 234)

Soit une courbe elliptique E d'équation de Weierstrass :

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

et un sous groupe fini F de E(Q)
Désignons par F_2 l'ensemble des points d'ordre 2 de l'ensemble $F - 0_E$:

$$F_2 = \{ P \in E(Q) ; 2P = 0_E, P \neq 0 \}$$

Soit une partie R de $F - 0_E - F_2$ telle que :

$$R \cup (-R) = F - F_2 - 0_E \quad \text{et} \quad R \cap (-R) = \phi$$

Soit la réunion $S = F_2 \cup R$

Soit une isogénie :

$$\Phi : E(Q) \rightarrow E'(Q) = E(Q)/F$$
$$(x, y) \rightarrow (X, Y)$$

Alors les coordonnées d'un point de la courbe isogéne E' sont des fonctions rationnelles de la forme :

$$X = x + \sum_{p \in S} \frac{t_p}{x - x_p} + \frac{u_p}{(x - x_p)^2}$$

$$Y = y - \sum_{p \in S} \left[u_p \frac{2y + a_1 + a_3}{(x - x_p)^3} + t_p \frac{a_1(x - x_p) + y - y_p}{(x - x_p)^2} + \frac{a_1 u_p - G'_x G'_y}{(x - x_p)^2} \right]$$

où $P = (x_p , y_p)$

$G'_x = 3x_p^2 + 2a_2 x_p + a_4 - a_1 y_p$ = dérivée partielle en x de $G(x,y) = 0$

et

$G'_y = -2 y_p - a_1 x_p - a_3$ = dérivée partielle en y de $G(x,y) = 0$

$$t_p = \begin{cases} G'_x(P) & \text{si } P \in F_2 \\ 6x_p^2 + 2x_p + b_4 & \text{si } P \notin F_2 \end{cases}$$

$$u_p = 4x_p^3 + b_2 x_p^2 + 2 b_4 x_p + b_6$$

On obtient l'équation de Wiestrass la courbe E' isogéne à E :

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

où $t = \sum_{p \in S} t_p$ et $w = \sum_{p \in S} (u_p + t_p x_p)$

Exemple de Velu :

Soit une courbe elliptique E d'équation :

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

Avec le calcul nous obtenons les invariants :

$b_2 = -3$; $b_4 = -5$; $b_6 = 13$; $b_8 = -16$; $c_4(E) = 129$ et $\Delta(E) = -1664$

Le groupe E (Q) contient le point M = (1 ,0) ; ce point engendre un sous groupe F

$$F = \{ M , 2M , 3M , 4M , 5M , 6M , 7M = 0_E \}$$

avec 2M =(-1,-2) , 3M =(3,-6) , 4M =(3,2) , 5M =(-1,2) , 6M =(1,-2).

F est un sous groupe cyclique de E (K) d'ordre 7.

Sous ensembles de F :

$$F - 0_E = \{ M , 2M , 3M , 4M , 5M , 6M \} = \{ \pm M , \pm 2M , \pm 3M \}$$

Dans le sous groupe F, il n'y a pas de point d'ordre 2 ; cela implique les parties :

$F_2 = \varnothing$, $R = \{ M , 2M , 3M \}$, $-R = \{ -M , -2M , -3M \}$; $S == F_2 \cup R = R$

Tableau des coordonnées des 3 points P =M, 2M et 3M

x_p	t_p	u_p	G'_x	G'_y
1	-2	4	-4	-2
-1	4	16	4	4
3	40	64	24	8

Le calcul implique les invariants :

b_2= -3 ;b_4= -5 ; b_6= 13 ; t = 42 et w =198

Il en résulte l'équation de Weierstrass de la courbe isogéne E':

$$E\text{ ' : } Y^2 + XY + Y = X^3 - X^2 - 213X - 1257$$

7-2 . Isomorphismes de courbes elliptiques:

Les isomorphismes de deux courbes elliptiques E sont déterminés par les changements de variables :

$$\begin{cases} x = u^2 X + r \\ y = u^3 Y + u^2 X\, s + t \end{cases} \qquad (1)$$

où $u \neq 0$, r, s, t sont des éléments d'un corps K.

Soit une courbe elliptique E d'équation de Weierstrass :

$$E: y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \in K\,[x,y] \qquad (2)$$

Une courbe elliptique E`isomorphe à E a une équation de Weierstrass

$$E' : Y^2 + a'_1 XY + a'_3 Y = X^3 + a'_2 X^2 + a'_4 X + a'_6 \in K\,[X,Y] \qquad (3)$$

Les calculs impliquent les relations entre les coefficients a_i, les invariants b_{2i}, c_{2i}, j(E),Δ(E) de E et les coefficients a`$_i$, les invariants b'$_{2i}$, c'$_{2i}$, j(E`),Δ(E`) de la courbe E' isomorphe à E .

Relations entre les coefficients a_i et a_i' :

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

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

$$\begin{aligned} u\, b'_2 &= b_1 + 12r \\ u^4 b'_4 &= b_4 + 2b_2 + 6r^2 \\ u^6 b'_6 &= b_6 + 2r\, b_4 + r^2\, b_2 + 4r^3 \\ u^8 b'_8 &= b_8 + 3\, r\, b_6 + 3r^2 b_4 + r^3 b_2 + 3r^4 \end{aligned} \qquad (5)$$

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

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

Relations entre les invariants :

$$u^{12}\Delta(E') = \Delta(E) \quad , \quad j(E') = j(E) \text{ et } u^{-1}\,\acute{\omega}(E') = \omega(E) \qquad (7)$$

L'invariant modulaire j (E) permet une classification des courbes elliptiques isomorphes .

Théorème 9:

Deux courbes elliptiques E et E' sont K isomorphes si et seulement si leurs invariants modulaires j(E) et j(E') sont égaux.

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

Soient deux courbes elliptiques E et E' isomorphes

Les formules d'isomorphismes (7) impliquent que les invariants modulaires j(E′) et j(E) sont égaux .

Preuve de «j (E′)= j(E) » implique que « les deux courbes E et E' son isomorphes ».

Soient 2 courbes elliptiques E et E` d'invariants modulaires égaux

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

Nous considérons des équations de Weierstrass :

$$E : y^2 = x^3 + Ax + B \qquad (8)$$

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

Avec les conditions :

$4A^3 + 27\,B^2 \neq 0$ et $4A'^3 + 27\,B'^2 \neq 0$

les invariants modulaires sont égaux à :

$$j(E)=\frac{(4A)^3}{4A^3+27B^2} \text{ et } j(E')=\frac{(4A')^3}{4A'^3+27B'^2}$$

L'égalité des invariants modulaires : $j(E') = j(E)$ implique l'égalité :

$$A^3B'^2 = A'^3B^2 \qquad (9)$$

Déterminons un isomorphisme

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

de valeur :

$$(x, y) \rightarrow (u^2x', u^3y') \quad , \; u \neq 0, 1 \qquad (10)$$

où u dans une clôture algébrique K_{alg} du corps K

Les formules d'isomorphismes impliquent les relations entre les invariants a_i et a'_i .

$$u^4A' = A \; ; \; u^6B' = B \qquad (11)$$

Ces deux équations impliquent trois cas possibles pour les valeurs de A et B :

1er cas : $A = 0$ et $B \neq 0$; alors $j(E) = 0$ et la condition $4A^3 + 27\,B^2 = 27\,B^2 \neq 0$ (12)

Les formules (11) impliquent l'équation en u de degré 6 :

$u^6B' = B$ admet 6 racines dans une clôture algébrique de K

$$u = (B/B')^{1/6} \qquad (13)$$

d'où 6 isomorphismes $E(K) \rightarrow E'(K)$

2ème cas : $B = 0$; $A \neq 0$; alors $j(E) = 1728$ et $B' = 0$

Les formules (11) impliquent une équation en u de degré 4 :

$u^4A' = A$ admet 4 racines dans une clôture algébrique de K

$$u = (A/A')^{1/4} \qquad (14)$$

d'où 4 isomorphismes $E(K) \rightarrow E'(K)$

3ème cas : $AB \neq 0$; cela implique $j(E) \neq 0$; 1728 et $A'B' \neq 0$

Les formules (11) impliquent deux équations en u :

$$u = (B/B')^{1/6} = (A/A')^{1/4} \; ;$$

Posons $B = d^{12}\,B'$, alors $u = d^2$ et $A = d^8\,A'$.

Il en résulte l'équation de la courbe elliptique isomorphe à E :

$E' : Y^2 = X^3 + A\,d^{-8}\,X + B\,d^{-12}$.

□

Exemple de courbes elliptiques isomorphes :

Soit une courbe elliptique E_1 d'équation de Weierstrass :

$$E_1 : y^2 = x^3 - 6x + 5$$

Nous obtenons par le calcul les valeurs des invariants :

$b_2 = 0$; $b_4 = -12$; $b_6 = 20$; $b_8 = -36$; $c_4(E_1) = 288$; $\Delta(E_1) = 3024$;

$$j(E_1) = (288)^3/3024 = (3^3 \times 2^{11}) / 7$$

Transformons E_1 par l'isomorphisme :

$$(x,y) \rightarrow (4X - 1,\ 8Y + 4X)$$

pour les éléments $u = 2$, $r = -1$, $s = 1$, et $t = 0$ du corps Q.

Nous obtenons par les calculs l'équation de la courbe elliptique isomorphe :

$$E' : Y^2 + XY = X^3 - X^2 - \frac{3}{16}X + \frac{5}{32}$$

Les valeurs des invariants de la courbe E' :

$$c_4(E') = 18 \ ; \Delta(E') = \frac{189}{256} \ ; \ j(E') = ((18)^3 \times 256) / 189$$

Le calcul implique les égalités :

$2^4 \ c'_4(E') = 288 = c_4(E_1)$

$2^{12} \Delta(E') = 3024 = \Delta(E_1)$

Une courbe elliptique a une structure de variété algébrique abélienne de dimension 1 Nous indiquons quelques notions sur les variétés algébriques.

8. Variétés algébriques :

Il existe plusieurs types de variétés algébriques: variétés affines, variétés projectives, variétés abéliennes, variétés de Picard, variétés de Véronèse, etc. ...

8-1 Variétés affines :

Définition 12 :

L'espace affine est le n – espace $/A^n(K)$ des n – uples d'éléments x de K.

$$IA^n = \{x = (x_1, \ldots, x_n), \text{ avec } x_1, \ldots, x_n \text{ dans } K\} \ ; \ n = 1, 2, \ldots$$

Dans le langage géométrique $(x_1, \ldots, x_n)$ est un point x de l'espace

Sur cet espace affine, les zéros d'une famille de polynômes $\{f_1, f_2 \ldots f_d\}$ de l'anneau de polynômes $K[x_1, \ldots, x_n]$ forment un ensemble algébrique .
Cet ensemble est considéré comme un ensemble fermé pour construire une topologie sur la variété .

Définition 13 :

Dans la topologie de ZARISKI sur l'espace affine IA^n les sous ensembles ouverts sont les complémentaires de sous ensembles algébriques.
Donc les sous ensembles fermés sont les ensembles algébriques.

Exemple :

1) Le polynôme $f(x, y) = x^2+3y^2+4 \in /R [x, y]$
n'a pas de racine dans l'espace affine $/A^2(/R)$.

2) Le polynôme :
$g(x, y) = x^2+y^2-1 \in /R [x, y]$

admet une infinité de zéros ; ces zéros sont représentés par les points du cercle de centre O et de rayon 1, ce cercle est donc un ensemble algébrique , c'est un fermé dans l'espace affine $/A^2(/R)$.

Une partie d'un espace affine devient une variété affine à certaines conditions

Définition 14 :

Une variété algébrique affine X est une partie irréductible et fermée d'un espace affine $/A^n$.
C'est donc l'ensemble des zéros d'une famille de polynômes $f_1, \ldots f_d \in K[x]$

Définition 15 :

Soit une variété algébrique affine X, alors l'idéal de cette variété X est l'ensemble :
$I(x) = \{ f \in \overline{K}[x] : f(P) = 0$ pour tout point $P \in X\}$

Définition 16 :

Une variété quasi- affine est une partie ouverte d'une variété affine /$A^n(K)$.

8-2Variétés projectives :

Considérons un ensemble affine /A^{n+1} (K), et la relation d'équivalence $\Re$ définie par la propriété :

$(a_0, a_1,\ldots, a_n)\ \Re\ (b_0, b_1,\ldots, b_n)$ si et seulement si :

$(a_0, a_1,\ldots, a_n) = \lambda\ (b_0, b_1,\ldots, b_n) = (\lambda b_0, \lambda\ b_1,\ldots, \lambda b_n)$

pour un élément non nul λ du corps K.

Vérifions que $\Re$ est une relation d'équivalence :

1) pour $\lambda = 1$:

$(a_0, a_1,\ldots, a_n) = 1\ (a_0, a_1,\ldots, a_n)$

donc $\Re$ est réflexive .

2) Soit la relation :

$(a_0, a_1,\ldots, a_n) = \lambda\ (b_0, b_1,\ldots, b_n)$, alors $\lambda \neq 0$, implique :

$(b_0, b_1,\ldots, b_n) = \lambda^{-1}\ (a_0, a_1,\ldots, a_n)$

donc $\Re$ est symétrique .

3) Soit deux relations :

$(a_0, a_1,\ldots, a_n) = \lambda\ (b_0, b_1,\ldots, b_n)$ et $(b_0, b_1,\ldots, b_n) = \beta\ (c_0, c_1,\ldots, c_n)$, $\lambda \neq 0$, $\beta \neq 0$

cela implique :

$(a_0, a_1,\ldots, a_n) = \lambda\beta\ (c_0, c_1,\ldots, c_n)$

donc $\Re$ est transitive .

Il en résulte que $\Re$ est une relation d'équivalence sur l'ensemble affine

$IA^{n+1}(K) - \{0\}$.

Définition 17 :

L'espace projectif $IP^n(K)$ est l'ensemble quotient de l'espace affine

$IA^{n+1}(K) - \{(0, 0,,...,0)\}$, par la relation d'équivalence $\Re$.

Les éléments de l'espace projectif $IP^n(K)$ sont des classes : la classe d'un n- uple a est représentée par une droite qui passe par l'origine.

cl a $=\{\lambda a , \lambda \neq 0 \}$

Donc le point à l'infini $O_E= (0,1,0)$ est un représentant de la classe des droites parallèles à l'axe Oy

Ces définitions sont précisées dans les ouvrages de Géométrie Algébrique : « Algébraic géométry » de Harsthorne , « Basic Algebraic géométry » de Shafarevich etc...

Définition 18 :

Une variété projective est un sous ensemble algébrique irréductible d'un espace projectif $IP^n(K)$ muni de la topologie de Zariski .

Définition 19 :

Une variété quasi- projective est une partie ouverte d'une variété projective .

8-3Variétés abéliennes :

Définitions 20 :

1) Une variété de groupe est une variété X munie de 2 lois :

une loi de groupe abélien :

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

et une loi :

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

2) Une variété abéliene est une variété projective de groupe, non singulière , munie d'une loi de groupe abélien .

Exemple :

Une variété abélienne de dimension 1 est une courbe elliptique .

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

Le groupe E(K) possède des points P =(x, y) rationnels , l'ensemble ces points rationnels est un fermé pour la topologie de Zariski .

E admet une équation projective dans le plan projectif $IP^2(K)$:

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

La dimension de la courbe E(K) est égale à :

dim $IP^2(K)$ - nombre de relations $f(x, y, z) = 2-1 = 1$.

Chapitre II

Fonctions modulaires et courbes elliptiques $y^2=x(x^2 + a)$

1-Introduction :

Soit la famille de courbes elliptiques:

$$E_a : y^2 = x (x^2 + a) \in Q[x , y]$$

paramétrées par un nombre rationnel a non nul .
Ces courbes elliptiques E_a ont des invariants égaux à:
$b_2 = 0$; $b_4 = 2a$; $b_6 = 0$; $b_8 = -a^2$; $c(E_a) = -48a$; $\Delta(E_a) = -64a^2$ et $j(E_a) = 1728$

Ces courbes ont intéressé plusieurs auteurs :
1)Bremner A. dans « On The Equation $\mathbf{y^2 = x (x^2 +a)}$ » ; Number Theory and Application , Dordrecht , Kluvert , Acadimic Press(1989)
2) Bremner A . et Cassels dans « On The Equation $\mathbf{y^2 = x (x^2 + p)}$ » Math. Comput. 42(1984)
3)Monsky P . dans « Mock Hegner Points and Congruents Numbers » ; Math . Zeit 204 (1990) 45-68 ; et dans « Three Constructions Of Rationals Points on $\mathbf{y^2 = x (x^2 \pm N)}$ » Math . Zeit. 209(1992)445-462 .

Selon Monsky, pour tout nombre premier $p \equiv 5 \bmod 8$, la courbe elliptique E_p d'équation de Weierstrass :

$$E_p : y^2 = x^3 + px \in Q[x , y]$$

contient au moins les deux points (0,0) et $0_E =(\infty,\infty)$
La méthode de 2-descente permet d'obtenir un isomorphisme de groupes abéliens :
$E_p(Q) \approx Z/ / 2 Z/ \times Z/$.
Dans cette relation Z/ / 2 Z/ est l'un des 15 groupes isomorphes au groupe de torsion T(E)(Q) prévus par le théorème de Mazur .
La 2-descente est exprimée dans l' énoncé suivant .

Théorème de 2-descente :
Soit une courbe elliptique E d'équation de Weierstrass :

$$E : y^2 = (x-e_1) (x-e_2) (x-e_3) \in K[x , y].$$

Soit un ensemble fini S de places du corps K contenant les places archimédiennes , les places qui divisent deux et toutes les places en lesquelles E a une mauvaise réduction. Soit le corps $K(S,2)= \{ b \in K^* /K^{*2}$; $ord_v (b) \equiv 0 \bmod 2$, pour toute place v hors de S $\}$

a) Alors, il y a un homomorphisme injectif de groupes :

$$\lambda : E(K)/2E(K) \rightarrow K(S,2) \times K(S,2)$$

de valeur :

$$\lambda(x,y) = \begin{cases} (x-e_1 , x-e_2) & si \quad x \neq e_1 , e_2 \\ ((e_1-e_3)/(e_1-e_2) , e_1-e_2) & si \quad x = e_1 \\ (e_2-e_1 , (e_2-e_3)/(e_2-e_1)) & si \quad x = e_2 \end{cases}$$

et $\lambda(0_E) = (1,1)$

b) Soit un couple $(d_1 , d_2) \in K(S,2)^2$ *différent des images* $\lambda(0_E)$, $\lambda(e_1,0)$ *et* $\lambda(e_2,0)$. *Alors* (d_1 , d_2) *est l'image d'un point* $P=(x, y)$ *du groupe* $E(K)/2E(K)$ *si et seulement si les deux équations en* z_i *:*

$$d_1 z_1^2 - d_2 z_2^2 = e_2 - e_1 \quad ;$$

$$d_1 z_1^2 - d_1 d_2 z_3^2 = e_3 - e_1 \ ;$$

admettent une solution $z_1, z_2 \in K^x$, $z_3 \in K$

Alors le point P est de la forme :

$$P = (d_1 z_1^2 + e_1 , d_1 d_2 z_1 z_2 z_3)$$

Preuve : (Silverman, chap. X .proposition 1-4).

□

Le groupe de torsion T(E) peut être déterminé par la .

Proposition 1 :

Soit un entier rationnel D sans facteur à la puissance 4 et une courbe elliptique :

$$E_D : y^2 = x^3 + Dx \in Q[x, y]$$

Alors son groupe de torsion T(E)(Q) est isomorphe à :

$$\begin{cases} Z/2Z/ & si\ D=4 \\ (Z/2Z/)^2 & si\ -D \text{ est un carré} \\ Z/2Z/ & pour\ les\ autres\ D \end{cases}$$

Le rang $r(E_D)$ *satisfait la relation :*

$$r(E_D) \leq 2\delta(2D) - 1 \ , \ \delta(2D) = \text{nombre de diviseurs premiers de } 2D.$$

Preuve : (Silverman, chap. X .proposition 6-1).

Soit une courbe elliptique E d'équation de Weierstrass :

$$E : y^2 = x^3 + Dx \qquad (1)$$

et l'isogénie :

$$\phi : E(Q) \rightarrow E'(Q)$$

de valeur :

$$\phi(x, y)= (y^2/ x^2 ,y(D- x^2)/ x^2). \quad (2)$$

L'équation de Weierstrass de la courbe isogéne E' :

$$E' : y^2 = x^3-4Dx \quad (3)$$

Considérons l'isogéne duale

$$\phi' : E'(Q) \rightarrow E(Q)$$

Soit $\delta(2D)$ nombre de diviseurs premiers de 2D , on obtient l'inégalité :

$$\dim E(Q)/ 2E(Q) \leq 2v(2D) - \dim E'(Q)[\phi'] + \dim \phi(E(Q)[2]) \quad (4)$$

La proposition (4-9) de Silverman permet d'obtenir un isomorphisme de groupes abéliens :

$$E'(Q)[\phi'] \cong Z/ / 2Z/ \quad (5)$$

1^{er} cas : $E(Q)[2] \cong Z/ / 2Z/$

donc $\dim E(Q)/ 2E(Q) =$rang $E(Q) +1$ (6)

les relations (6) et (8) impliquent l'inégalité:

$$\text{rang } E(Q) \leq 2v(2D) -1 \quad (7)$$

$2^{éme}$ cas : $E(Q)[2] \cong Z/ / 2Z/ \times Z/ / 2Z/$

donc $\phi(E(Q)[2]) \cong Z/ / 2Z/$ et $\dim E(Q)/ 2E(Q) =$rang $E(Q) +2$ (8)

les relations (6) et (10) impliquent l'inégalité:

$$\text{rang } E(Q) \leq 2v(2D) \quad (9)$$

□

Mordell a conjecturé que les courbes elliptiques E_p , pour p premier , possèdent un point d'ordre infini , donc un rang $r(E_p) \geq 1$.

Bremner a vérifié , par le calcul cette conjecture pour les nombres premiers $p \equiv 5 \mod 8$ et $p< 20000$.

Monsky a utilisé une technique particulière pour étudier les points rationnels des courbes elliptiques E_N d'équations de Weierstrass :

$$E_N : y^2 = x^3 \pm N \quad x \in Q[x , y] .$$

.

Cette technique est basée sur les fonctions modulaires.

2-Fonctions modulaires :

Nous commençons par décrire les fonctions modulaires d'après les ouvrages :

1) « Introduction to the Arithmetic Theory of Automorphic Functions » de Shimura ;

2) « Modular Functions and Dirichlet Series in Number Théory » de Apostol ;

3) « The Arithmetic of Elliptic Curves » de J.H.Silverman .

4) « Modular Forms and Dirichlet Series » de A. OGG.

Soit un réseau complexe $L= \omega_1 Z/ + \omega_2 Z/$, où ω_i sont deux nombres complexes de quotient ω_1 /ω_2 non réel ; ces deux nombres forment une base du réseau L .

Définition 1 :
la fonction elliptique de Weierstrass attachée à un réseau complexe *L est la série infinie:*

$$P(z ; L) = \frac{1}{z^2} + \sum_{\omega \in L-\{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right) \quad . \qquad (1)$$

Cette fonction est doublement périodique, de périodes formant une base du réseau L.
Elle admet un pôle double en z=0
Elle est paire : P(-z) = P(z)
Elle est dérivable. Sa dérivée est égale à :

$$P'(z ; L) = -2 \sum_{\omega \in L} \frac{1}{(z-\omega)^3} \qquad (1\text{-}2)$$

Dans cette série P(z) se trouve une autre série $\sum \frac{1}{\omega^2}$

Définition 2 :
La série d'Eisenstein de poids k attachée à un réseau L est la fonction complexe :

$$G_k = \sum_{\omega \in L-\{0\}} \frac{1}{\omega^k} \qquad (1\text{-}3)$$

Les séries d'Eisenstein admettent des développements de Fourier de type :

$$G_{2k}(z) = 2\,\xi(2k) + \frac{2(2\pi i)^{2k}}{(2k-1)!} \sum_{n \geq 1} \sigma_{2k-1}(n)\; q^n \text{ ; avec } q = exp(2i\pi z)$$

$\xi(2k)$= fonction Zéta de Riemann $= \sum_{n \geq 1} n^{-2k}$

$\sigma_t(n)$= somme des puissances d^t des diviseurs d de $n = \sum_{d/n} d^t$

La fonction P(z ; L) admet un développement de Laurent de type :

$$P(z ; L) = \frac{1}{z^2} + \sum_{k \geq 1} (2k+1)\; G_{2k+2}\; (z)\; z^{2k} \qquad (1\text{-}4)$$

Sa dérivée est égale à :

$$P'(z ; L) = \frac{-2}{z^3} + \sum_{k \geq 1} 2k\,(2k+1)\; G_{2k+2}\; (z)\; z^{2k-1} \qquad (1\text{-}5)$$

Les séries (1-4) et (1-5) satisfont l'équation :

$$P'(z)^2 = 4\ P(z)^3 - 60\ G_4\ P(z) - 140\ G_6 \qquad (1\text{-}6)$$

Cette relation (1-6) implique un isomorphisme analytique complexe entre le tore complexe $\mathbb{C}/L$ et la courbe elliptique :

$$E_L : y^2 = 4x^3 - g_2 x - g_3\ .\ \in \mathbb{C}[x, y] \qquad (1\text{-}7)$$

$$\mathbb{C}/L \rightarrow E_L/\mathbb{C}$$
$$z \rightarrow (x=P(z)\ ;\ y=P'(z)) \qquad (1\text{-}8)$$

Dans la relation (1-7) : $g_2 = 60\ G_4(z)$ et $g_3 = 140\ G_6(z)$ (1-9)

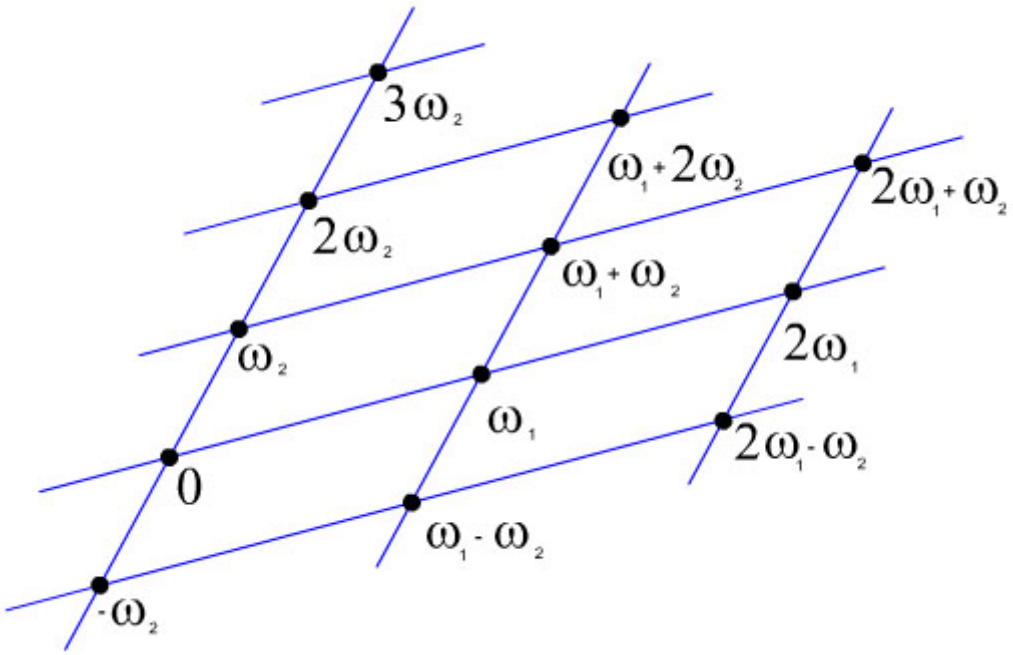
Cette courbe elliptique E_L a un discriminant égal à :

$$\Delta(E_L) = g_2(z)^3 - 27\ g_3(z)^2\ . \qquad (1\text{-}10)$$

L'invariant modulaire de E_L est égal à :

$$J(E_L) = 12^3\ g_2(z)^3 / \Delta(z)\ . \qquad (1\text{-}11)$$

Le réseau L de base (ω_1,ω_2) est représenté dans le plan complexe par la figure :



Pour obtenir des fonctions modulaires, il faut le demi plan supérieur :

$$IH = \{ z = x + i\, y \in \mathbb{C} \ , y > 0 \} \qquad (2)$$

et le groupe modulaire $SL(2 , Z/) = \Gamma$ des 2×2 matrices $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, à coefficients entiers rationnels et de déterminant égal à 1.

$$SL(2 , Z/) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \ ; \text{avec } a,b,c,d \in Z/ \ ; \ ad-bc = 1 \right\} = \Gamma \quad . \qquad (2\text{-}1)$$

Le groupe modulaire SL(2 , Z/) opère sur le demi plan supérieur *IH* par homographie :

$$Az = \frac{az + b}{cz + d} \qquad (2\text{-}2)$$

Le groupe modulaire Γ possède des sous groupes spécifiques :

les sous groupes *de congruence* .

Définition 3 : (Silverman)

Soit un entier $N \geq 1$, les sous groupes de congruence modulaires de niveau N sont :

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(Z/) \ ; \quad c \equiv 0 \bmod N \right\} \qquad (1)$$

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(Z/) \ ; \quad c \equiv 0 \ ; a \equiv d \equiv 1 \bmod N \right\} \qquad (2)$$

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(Z/) \ ; a \equiv d \equiv 1 \bmod N \ ; b \equiv c \equiv 0 \bmod N \right\} \qquad (3)$$

Γ(N) est le sous groupe de congruence modulaire principal de niveau N .

Tout sous groupe G de SL(2 ,Z/) qui contient Γ(N) est un sous groupe de congruence modulaire de niveau N .

Définition 4 : (Apostol)

Une fonction modulaire de poids k est une fonction méromorphe f sur le demi – plan /H ,qui satisfait les conditions :

1) $f(Az) = (cz + d)^k f(z)$; pour tout matrice $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(Z/)$ (1)

2) f admet un développement de Fourier de type :

$$f(z) = \sum_{n \geq -m} a(n) q^n \quad ; \; m>0 , \; q = exp (2i\pi z) \quad . \qquad (2\text{-}3)$$

Cette définition implique qu'une fonction modulaire est invariante par le groupe modulaire SL(2 , Z/) ; elle est analytique sur le demi plan supérieur /H , sauf aux pôles , qui existent lorsque m > 0 et a(-m) ≠0 . La fonction f a un pôle d'ordre m en z=i∞ .
Pour m<0 , la fonction f est analytique en z=i∞ .

Définition 5 : (Apostol)

Une forme modulaire de poids k pour le groupe modulaire Γ =SL(2 ,Z/) est une fonction f qui satisfait les 3 conditions :
1)f est analytique sur le demi plan supérieur IH .
.

2) $f(A z) = (c z + d)^k f(z)$, *pour toute matrice* $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ *de* Γ. (2-4)

3) f admet un développement de Fourier de type :

$$f(z) = \sum_{n \geq 0} c(n)\, q^n \qquad où \qquad q = exp (2i\pi z) \quad et \quad c(n) \in \mathbb{C} \; .$$

Dans le développement $f(z)$ de Fourier, le coefficient c(0) est égal à la valeur de f en z =i∞ *:*

$$f (i \infty)= c(0)$$

Les formes modulaires sont de deux types suivant le coefficient c(0).

Définition 6 : (Apostol)
Une forme modulaire f est parabolique lorsqu'elle prend la valeur :

$$c(0)= f (i \infty)=0 \qquad (2\text{-}5)$$

Alors elle a un développement de Laurent de la forme :

$$f(z)= c(n_0)\, q^{n_0} + 1 + \ldots + c(n)\, q^n \quad , \text{pour } n_0 > 0 \qquad (2\text{-}6)$$

Les formes modulaires de poids k sont classifiées par la

Proposition 1 (Apostol)

1) les formes modulaires de poids k=0 sont les constantes
2) les formes modulaires de poids k< 0, k = 2 et k impair sont nulles .
3) toute forme modulaire , non constante et non nulle , a un poids k pair et $k \geq 4$.
4) les formes paraboliques de poids k < 12 sont nulles .

Preuve : dans Apostol

Exemples:

1)L'invariant modulaire :

$$J(E) = 1728\ g_2^3 / \Delta \quad , \text{avec} \quad g_2 = 60\, G_4(z)$$

est une fonction modulaire:

$$J(z) = \frac{1}{q} + 744 + \sum_{n\geq 1} c(n)\, q^n \quad , \text{avec} \quad q = \exp(2i\pi z) \qquad (2\text{-}7)$$

2) Le discriminant Δ (E) est une forme modulaire parabolique de poids 12

$$\Delta(z) = (2\pi)^{12}\, q \prod_{n\geq 1} (1-q^n)^{24} \ , \ \textit{avec} \ \ q = \textit{exp}(2i\pi z) \qquad (2\text{-}9)$$

*3)*La fonction Eta de Dedekind est la forme modulaire :

$$\eta(z) = q^{1/24} \prod_{n\geq 1} (1- q^n) \ ; \textit{avec} \ \ q = \textit{exp}(2i\pi z) \qquad (2\text{-}10)$$

Elle est liée à la forme parabolique discriminant Δ (z) par la relation :

$$\Delta(z) = (2\pi)^{12}\, \eta(z)^{24}$$

4)Les séries d'Eisenstein G_{2k} (z) , k≥ 2 sont des formes modulaires de poids 2k pour le groupe modulaire SL (2 , Z/) .

Ces fonctions engendrent des formes modulaires.
L'ensemble M_k des formes modulaires de poids k a une structure de $\mathbb{C}$ espace vectoriel.
Sa dimension est précisée par la :

Proposition 3 :

1) Les formes modulaires de poids k pair ≥ 4, forment un $\mathbb{C}$ - espace vectoriel M_k de dimension :

$$\dim M_k = \begin{cases} [k/12] = \textit{partie entière de } k/12 & \textit{si} \quad k \equiv 2 \bmod 12 \ , \ k \geq 0 \\ [k/12] + 1 & \textit{si} \ \ k \equiv 2 \bmod 12, \ k \geq 0 \end{cases}$$

2) Toute forme modulaire de poids k pour le groupe Γ est un polynôme de type :

$$f(z) = \sum_{a,b} c(a,b)\, G_4^{\,a} G_6^{\,b} \qquad (1)$$

où a , b sont des entiers positifs qui satisfont :
$4a + 6b = 2k$.

c(a , b)= nombre complexe

G_4 et G_6 sont les séries d'Eisenstein G_{2k}

Preuve : Apostol, Théorème 6-4.

□

Exemple :
dim M_k=1 , pour k = 4,6,8,10 et 14 .

Corollaire :
Les formes modulaires paraboliques de poids k pair ≥ 12 , forment un ℂ - espace vectoriel $M_{k,0}$ de dimension :

$$\dim M_{k,0} = \dim M_k - 1 \ .$$

Preuve : Apostol, Théorème 6-3 et 6-4 .

□

Exemple :
dim $M_{k,0}$=1 , pour k =12,16,18,20 ,22 et 26

Monsky a construit des fonctions modulaires f_i *à partir* des formes modulaires paraboliques discriminant Δ (z) et P_L (z) de Weierstrass :

$$f^{24}(z) = -\Delta(z+1/2)/\Delta(z)$$
$$f_1^{24}(z) = -\Delta(z/2)/\Delta(z) \qquad (3)$$
$$f_2^{24}(z) = 2^{12}\ \Delta(2z)/\Delta(z)$$

Ces 3 fonctions modulaires sont holomorphes sur le demi plan supérieur *IH* , elles n'admettent pas de zéro dans *IH* . Elles sont de niveau 2 .
Elles prennent des valeurs réelles positives en $z = i\infty$ *;*

$$\lim_{z \to i\infty} q = 0 \quad \text{implique} \quad \lim_{z \to i\infty} \Delta(z) = (2\pi)^{12}$$

Monsky considère 3 autres fonctions modulaires qui prennent des valeurs réelles positives

$$T= 8^{-1/2} f^{6} \; ; \; T_1= 8^{-1/2} f_1^{12} \; ; \; T_2= 8^{-1/2} f_2^{12} \; . \qquad (3\text{-}1)$$

Elles sont holomorphes sur le demi plan supérieur IH *et* prennent des valeurs réelles positives en $z = i\infty$.

Monsky introduit des fonctions modulaires associées à la fonction $P_L(z)$ de Weierstrass :

$$e_{u,v}(z) = P_L((uz + v)/8) \; ; \quad u, v \in Z/8 \text{ , telle que } u \neq 0 \text{ et } v \neq 0 \qquad (3\text{-}2)$$

Ces fonctions modulaires $e_{u,v}(z)$ sont des formes modulaires de niveau 8 et de poids 2

Il existe des relations entre ces fonctions .

$$T= ((i-1) E_7E_8) /32 E_2E_3 \; ; \; T_1= 8^{1/2} E_3 / E_6 \; ; T_2= 8^{1/2} E_2 / E_9 \qquad (3\text{-}3)$$

avec :

$$E_2= e_{4,4} - e_{4,0} \; ; \quad E_7= e_{1,1} - e_{1,5} - e_{5,5} - e_{5,1} \; ;$$
$$E_3= e_{0,4} - e_{4,4} \; ; \quad E_8= e_{1,3} - e_{3,5} - e_{5,7} - e_{7,1} \; ; \qquad (3\text{-}4)$$
$$E_6= e_{2,4} - e_{2,0} \; ; \quad E_9= e_{0,2} - e_{4,2} \; ;$$

On pose :

$$U = T(T_1 + T_2) / (4 T^2 - 2)$$

et (3-5)

$$V = T(T_1 - T_2) / (4 T^2 + 2) .$$

Ces deux fonctions U et V sont modulaires de niveau 8 et holomorphes sur $/H$. Elles satisfont les relations :

$$2U^2 = T^2 + 1 \quad \text{et} \quad 2V^2 = T^2 - 1 \; ; \qquad (3\text{-}6)$$

Elles prennent les valeurs particulières :

$$U(i) = T(i) = 1 \quad et \quad V(i) = 0 \; .$$

3- Extensions abéliennes finies du corps quadratique imaginaire Q (i) :

Soit un entier positif D .
Soit L_D la plus grande extension abélienne du corps quadratique imaginaire Q(i) dont le conducteur cond (L_D/ Q(i)) divise D.

Le conducteur d'une extension abélienne M de Q est l'entier f tel que le $f^{éme}$ corps cyclotomique soit le plut petit qui contienne M .

Le groupe de Galois G_D de L_D/ Q(i) est isomorphe à un groupe quotient :

$$G_D \rightarrow (Z/[i]/D)^*/ \{\pm 1, \pm i\} \quad (4)$$

Soit K_D le corps de classe d'anneau de Z/[Di] .

$$Q(i) \subset K_D \subset L_D \quad (4\text{-}1)$$

Ces définitions se trouvent chez de H. Cohn « Théorie du corps de classes » .
Le corps de décomposition de (1 +i) est un sous corps K'_D tel que :

$$[K_D : K'_D] = 2 \quad (4\text{-}2)$$

Pour D impair > 1 , on obtient les inclusions de corps :

$$Q (i) \subset K'_D \subset K_D \subset K_{2D} . \quad (4\text{-}3)$$

et les degrés :

$$[K_{2D} : K_D] = [K_D : K'_D] = 2 \quad (4\text{-}4)$$

Proposition 4 :
1) Les nombres T(Di) , T_1(Di) et T_2(Di) sont dans le corps L_{2D}.
2) Les nombres T(Di) , U(Di) et V(Di) sont dans le corps K_{8D}.

Preuve : Monsky ,lemme 3-1 et théorème 3-2

□

4-Points rationnels sur $E_N : y^2 = x^3 \pm Nx$

On pose :

$$T (D i) = t ; U (D i) = u ; V (D i) = v ; \quad (5)$$

$$w = \sqrt{t} \quad \text{lorsque } D \equiv 1 \bmod 4 ;$$

et (5-1)

$$w = \sqrt{2t} \quad \text{lorsque } D \equiv 3 \bmod 4$$

N entier positif , tel que $N \equiv \pm 3, \pm 5 \bmod 8$ (5-2)

$$n = N \quad \text{si } N \equiv 1 \bmod 4$$

et (5-3)

$n = 4N$ si $N \equiv 3 \bmod 4$

$N \equiv \pm 5 \bmod 16$ si $D \equiv 1 \bmod 4$

et (5-4)

$N \equiv \pm 3 \bmod 16$ si $D \equiv 3 \bmod 4$

Proposition 5 :

Soit les entiers N et D satisfont (5-2) et (5-3) et tels que N divise une certaine puissance D^s .

Alors :

1) $n^{1/4}$ est un nombre de $K_{2D.}$

2)Lorsque $N \equiv 3, 5 \bmod 8$,alors $K_D = K'_D (n^{1/2})$ et $K_{2D} = K'_D (n^{1/4})$

Preuve : Monsky définition 2-7 ,lemme 2-10 et théorème 2-11

□

Par cette proposition 5 et la formule (5-1) , le nombre w est de la forme :

$w = a + b\sqrt{n} \in K_D$, *a et b dans* K'_D

Proposition 6 :

Soit un nombre $w = a + b\sqrt{n} \in K_D$ *. Alors :*

1*) a et b sont des nombres positifs du corps* K'_D

2) $a^2 - nb^2 = 1 , -2 , -1$ *ou* 2 *selon que* $D \equiv 1, 3 , 5$ *ou* $7 \bmod 8$ *;*

3) $a^2 + nb^2$ *et* $2ab$ *sont des carrés dans le corps* K'_D *;*

Preuve : Monsky ,lemme 5-10 et théorème 5-2

□

Ces nombres a et b interviennent dans les points rationnels des courbes elliptiques .

$$E_B : y^2 = x^3 + Bx \qquad (6)$$

Soit K_0 le sous corps réel maximal du corps K'_D (6-1)

Proposition 7 :

Soit les courbes elliptiques E_B et le corps K_0 , les formules (6) et (6-1).

1) Lorsque $D \equiv 1 \bmod 8$, la courbe elliptique E_{-4n} possède un point K_0 rationnel (x, y) d'abscisse $x = 2a / b$

2) Lorsque $D \equiv 3 \bmod 8$, la courbe elliptique E_{-n} possède un point K_0 rationnel (x , y) d'abscisse $x = -a / b$

3) Lorsque $D \equiv 5 \bmod 8$, la courbe elliptique E_{-4n} possède un point K_0 rationnel (x , y) d'abscisse $x = -2a / b$

4) Lorsque $D \equiv 7 \bmod 8$, la courbe elliptique E_{-n} possède un point K_0 rationnel (x , y) d'abscisse $x = a / b$

Preuve : Elle est basée sur la proposition 6 .
Monsky : Corollaire 5.3.1.

□

Lorsque D ≡3 mod 8 , la proposition 6 implique que :
-a/b =2 ; c'est le carré d'un nombre de K_0
l'inclusion $Q (i) \subset K_0$ implique la relation :
$-2 = (\sqrt{2i})^2$
Il en résulte que $(-a/b)^2 – n = -2/ b^2$ est le carré du nombre $((\sqrt{2i})/ b) \in K_0$.
Il en résulte la :

Proposition 8 :
Les courbes elliptiques E_{4n} d'équation de Weierstrass :
$E_{4n} : y^2 = x^3 + 4n\, x \in K_0 [x,y]$
contient un point K_0 rationnel $P=(2a / b , y)$.

Preuve :

Au point P=(2a / b , y) , le polynôme $x^3 + 4n x$ prend la valeur :
$(2a / b)^3 +4n (2a / b) = \frac{2a}{b^3} (4a^2 +4n b^2) = \frac{2ab}{b^4} 4(a^2 +n b^2)$
La proposition 6 , (3) implique que 2ab est un carré . Il en résulte que l'équation :

$$y^2 = \frac{2ab}{b^4} 4(a^2 +n b^2)$$

admet une solution K_0 rationnelle y .

□

Exemple :

Calcul de D avec la congruence D ≡1 mod 8
cette congruence admet une infinité de solutions :
D = 9,17,25,33,41,49,57,65,…
la formule (5-4) implique la congruence :
N ≡± 5 mod 16
cette congruence admet une infinité de solutions :
N = 5,11,21,27,37,43,…
Je choisis N divise D^s :
N = 5 et D = 65
$L_D = L_{65}$ est un sous corps du $65^{éme}$ corps cyclotomique $Q(z_{65})$ qui contient Q(i) .

$[Q(z_{65}) :Q] = \phi(65) = 48$

La racine $z = z_{65} = \cos(2\pi/65) + i \sin (2\pi/65)$
Le corps de classe d'anneau K_D satisfait :
$Q(i) \subset K'_{65} \subset K_{65} \subset L_{65}$

Donc les corps intermédiaires sont quadratiques :

$$[L_{65} : K_{65}] = [K_{65} : K'_{65}] = 2$$

La formule (5-3) implique que $n = N = 5$

Nombre $w = a + b\sqrt{n} = a + 2b\sqrt{5} \in K_{65}$

a et b sont des nombres positifs du corps K'_{65} .

Les nombres de ce corps sont de la forme :

$$u= u(i , z_{65}) = r_1 z + r_2 z^2 + \ldots + r_{64} z^{64} + s + it$$

Les nombres a et b satisfont la relation :

$$a^2 – nb^2 = 1 \text{ lorsque } D \equiv 1 \bmod 8$$

Les calculs sont très longs , nous ne les ferons pas .

Il en résulte que le point d'abscisse $x = 2a / b$ appartient à la courbe elliptique E d'équation :

$$E : y^2 = X^3 – 20x \in K'_{65}[x,y]$$

[1] ***T. Apostol*** « Modular Functions and Dirichlet and Series in Number Theory » GTM 41 .

[2] ***A.Bremner*** « On The Equation $y^2= x(x^2 +a)$, Number Theory and Application » Dordrecht , Kluvert , Acadimic . Press (1989) .

[3] ***A.Bremner et Cassels*** « On The Equation $y^2= x(x^2 +a)$ » Math . Comput .42(1984) .

[4] ***J . . S Cassels*** « Diophantine Equations with Special Reference To Elliptic Curves » J . London . Math . Soc 41 (1966), 193-291 .

[5] ***R . Hartshorne*** « Algebraic Geometry » Springer Verlag (1977) .

[6] ***N . Koblitz «*** Introduction To Elliptic curves and Modulair Forms » Springer Verlag (1977) GTM 97 .

[7] ***S . Lang*** «Elliptic Curves, Diophantine Analysis » Springer Verlag (1978) .

[8] ***P . Monsky*** « Three Constructions Of Rationals Points On $y^2= x(x^2\pm N)$ » Math . Zeit . 209(1992)445-462 .

[9] ***A.P.Ogg*** « Diophantine Equations and Modulair Forms » Bul. Amer. Math. Soc 81(1975) , 14-27 .

[10] ***R . Shafarevich*** «Basic Algebraic Geometry » Springer Verlag (1977) .

[11] ***G. Shimura*** **«** Introduction To The Arithmetic Theory Of Automorphic Functions » Publ. Math. Soc . Japan 11(1971) .

[12] ***J. H. Silverman*** «The Arithmetic of Elliptic Curves » Grad . Texts in Math .106 Springer (1986) .

[13] ***J . Tate*** « The Arithmetic of Elliptic Curves » Invent . Math 23 (1974), 179-206

[14] ***M.J. Velu*** « Isogenies entre courbes elliptiques »CR . Acad .Sci .Paris . Sér .A 273 (1971) , 238-241 .