N° d'ordre : 05/2007= M/MT

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE
UNIVERSITE DES SCIENCES ET DE LA TECHNOLOGIE « HOUARI BOUMEDIENE»

Faculté des Mathématiques

MEMOIRE

Présenté pour l'obtention du diplôme de MAGISTER

En : MATHEMATIQUES
Spécialité : Algèbre et Théorie des Nombres

Par : **M^{elle} SABRI Farida**

SUJET

Calcul des points entiers sur une Courbe Elliptique

Soutenue le : **12 – 02 – 2007.** **devant le jury composé de :**

Mr M. AIDER	**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. KHELLADI	**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 M. O. HERNANE	**Maître de conférence à L'U. S. T. H. B**	**Examinateur.**

Remerciements

Je remercie Monsieur Mohamed ***ZITOUNI,*** *professeur à l'USTHB de m'avoir proposé ce sujet et de m'avoir guidé tout le long de la réalisation de cette thèse.*

Je remercie spécialement Monsieur M. AIDER, Professeur à l'USTHB d'avoir accepté de présider le jury et d'avoir apprécié ce présent travail.

Je remercie également Messieurs A. KHELLADI, professeur à l'USTHB, M. O. HERNANE, Maître de conférence à l'USTHB et M. S. HACHAICHI, Maître de Conférence à l'USTHB pour leur participation au jury.

SOMMAIRE

Introduction

Le point de départ de ma thèse est un article de Gebel, Petho et Zimmer, intitulé "Computing integral points on elliptic curves" et publié dans la revue Acta Arithmetica LXIII 2 (1994) -171-192.

Il s'agit de calculer les coordonnées de points d'une courbe elliptique E sur le corps Q des nombres rationnels. Les calculs des coordonnées x et y de grandes valeurs ne sont possibles qu'au moyen d'un ordinateur. Les méthodes utilisées exigent la connaissance de la structure du groupe de Mordell-Weil E(K) de la courbe E.

Ma thèse se compose de trois chapitres :

Dans le chapitre I, j'ai indiqué des notions indispensables de la théorie arithmétique des courbes elliptiques : équations de Weierstrass, invariant discriminant $\Delta(E)$, invariant modulaire $j(E)$, invariant différentiel $\omega(E)$ et classification des cubiques de Weierstrass par leurs invariants $\Delta(E)$ et C_4 (E).

J'ai traité des exemples d'application de cette classification.

Dans le chapitre II j'ai établi la structure algébrique de l'ensemble E(K) des points K- rationnels de la courbe elliptique. C'est un groupe abélien additif de type fini d'élément neutre le point a l'infini : E(K) est le groupe de Mordell-Weil de la courbe E.

Dans le chapitre III, j'ai étudié les points entiers de courbes elliptiques. J'ai utilisé les équations diophantiennes, les entiers algébriques de corps de nombres, des courbes elliptiques ayant un seul point de 2-torsion et l'équation des S-unités.

Chapitre - I - ARITHMETIQUE DES COURBES ELLIPTIQUES

1- Courbes algébriques planes

La théorie des courbes algébriques se trouve dans plusieurs ouvrages :

" Basic Algebraic Geometry" [16 -1]; "Algebraic Geometry" [6]

Définition 1 *Une courbe algébrique plane est l'ensemble des points* (x, y) *du plan* R^2 *qui satisfont une équation algébrique* $f(x, y) = 0$, $f(x, y) \in R[x, y]$, $\deg(f) = n = 1,2,...$

Le degré du polynôme $f(x, y)$ permet de classifier les courbes suivant leur degré.

Pour n = 1, $f(x, y) = r_1 x + r_2 y + r_3 = 0$ est l'équation d'une droite

Pour n = 2, $f(x, y) = (r_1 x^2 + r_2 xy + r_3 y^2) + (r_4 x + r_5 y) + r_6$ est l'équation d'un cercle, d'une ellipse, d'une hyperbole, d'une parabole ou du produit de deux droites.

Pour n = 3, $f(x, y) = (r_1 x^3 + r_2 x^2 y + r_3 xy^2 + r_4 y^3) + (r_5 x^2 + r_6 xy + r_7 y^2) + (r_8 x + r_9 y) + r_{10}$ est l'équation d'une cubique algébrique plane irréductible ou du produit de trois droites ou le produit d'une droite par une conique.

Pour n = 4, $f(x, y) = g_4(x, y) + g_3(x, y) + g_2(x, y) + g_1(x, y) + g_0(x, y)$, où $g_t(x, y)$ est un polynôme homogène de degré t, est l'équation d'une quartique algébrique plane.

Pour n = 5, $f(x, y) = g_5(x, y) + g_4(x, y) + g_3(x, y) + g_2(x, y) + g_1(x, y) + g_0(x, y)$ est l'équation d'une quintique algébrique plane.

Le polynôme $f(x, y)$ peut être irréductible ou réductible.
Cette propriété implique une classification des courbes en classe des courbes irréductibles et classe des courbes dégénéreés en produit de courbes degré inférieur.

Ainsi $f(x, y) = (r_1 x + r_2 y + r_3)(r_4 x + r_5 y + r_6)$ est le produit de deux polynômes de degré un, c'est l'équation du produit de deux droites

Un polynôme cubique admet deux décompositions :

Cubiques de Weierstrass

$f(x,y) = f_1(x,y) f_2(x,y) f_3(x,y)$, produit de trois polynômes de degré un est l'équation du produit de trois droites,

$f(x,y) = f_1(x,y) f_2(x,y)$, produit d'un polynôme f_1 de degré un par un polynôme irréductible f_2 de degré deux, est l'équation du produit d'une droite par une conique.

Un polynôme $f(x,y)$ irréductible peut être non singulier ou admettre des points singuliers. Cette propriété implique une classification des courbes algébriques planes irréductibles en classe des courbes irréductibles non singulières et classe des courbes irréductibles singulières

Le nombre s de points singuliers et le degré n d'une courbe algébrique permettent de définir l'invariant genre

Définition 2 *Le genre d'une courbe algébrique plane C, irréductible de degré n, ayant s points singuliers, est l'entier positif ou nul*

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

Les courbes algébriques irréductibles peuvent être classifiées par leur genre en classes de courbes de genre 0,1,…

L'équation $f(x,y) = 0$ de degré n, dans le plan affine $A^2(K)$, est transformée en équation projective dans le plan projectif $P^2(K)$ par deux opérations

$$f(x,y) \to f(\frac{x}{z}, \frac{y}{z}) \qquad \text{et} \qquad f(\frac{x}{z}, \frac{y}{z}) \to z^n f(\frac{x}{z}, \frac{y}{z}) = \text{g(x,y,z)}$$

Dans la suite, nous considérons seulement les cubiques planes irréductibles.

2 Cubiques de Weierstrass

Dans l'ensemble des polynômes $f(x,y)$ cubiques irréductibles, nous considérons la classe des équations particulières de Weierstrass

$$f(x,y) = y^2 + (a_1 x + a_3) y - x^3 - a_2 x^2 - a_4 x - a_6 = 0 \qquad (1)$$

Cubiques de Weierstrass

Définition 3 *Soit K* un *corps commutatif global, local ou fini. Une courbe elliptique est une cubique plane E, irréductible, non singulière, d'équation spécifique de Weierstrass :*

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

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

La nature du corps K permet de choisir les outils mathématiques pour étudier la courbe elliptique. Lorsque K est un corps de nombres algébriques, nous utilisons la Théorie des Nombres Algébriques :(avec les idéaux, les ramification, les valuations ...), analytique (avec les équations diophantiennes, les fonctions arithmétiques,...)

Lorsque K est le corps des nombres complexes, nous utilisons l'Analyse Complexe (fonctions elliptiques, fonctions modulaires ...), la Géométrie Algébrique (variétés, cohmologie, diviseurs...) Lorsque K est un corps fini, nous utilisons la théorie des corps finis

L'équation de Weierstrass (1) peut être transformée au moyen de changement de variables appropriés pour éliminer les monômes en xy, en y, en x^2

Le changement de variables

$$x = X, y = \frac{1}{2}(Y - a_1 X - a_3) \quad \text{pour car (K)} \neq 2 \qquad (2)$$

transforme (1) en l'équation de Weierstrass

$$E_1 : Y^2 = 4X^3 + b_2 X^2 + 2b_4 X + b_6 \in \text{K [x , y]} \qquad (3)$$

Les cœfficients b_{2i} sont des polynômes homogènes de degré $2i$ de l'anneau $Z[a_1, a_2, a_3, a_4, a_6]$

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

Le changement de variables

Invariants

$$X = \frac{(x - 3b_2)}{36}; Y = \frac{y}{108} \qquad \text{pour car (K)} \neq 2, 3 \tag{5}$$

transforme (3) en l'équation de Weierstrass

$$E_2 : y^2 = x^3 - 27c_4x - 54c_6 \quad \in \text{ K [x , y]} \tag{6}$$

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

$$c_4 = b_2^2 - 24b_4 \quad \text{et} \quad c_6 = -b_2^3 + 36b_2b_4 - 216b_6 \tag{7}$$

Exemple de courbes elliptiques

$$E_3 : y^2 = x^3 + Ax + B \in K[x, y] \qquad \text{avec } 4A^3 + 27B^2 \neq 0 \tag{8}$$

Equation de Legendre

$$E_4 : y^2 = x(x - 1)(x - t) \ , \ t \neq 0,1 \tag{9}$$

Equation de Deuring

$$E_5 : y^2 + Axy + y = x^3 \ ; \ A^3 \neq 27, \tag{10}$$

Equation avec $a_6 = D \neq 0$

$$E_6 = y^2 = x^3 + D, \tag{11}$$

Equation avec $a_4 = d^2 \neq 0$

$$E_7 : y^2 = x^3 - d^2x \ , \qquad d \neq 0 \tag{12}$$

3- Invariants des cubiques de Weierstrass

Une cubique de Weierstrass est une cubique irréductible d'équation (1).

Elle possède plusieurs invariants : un discriminant, un invariant modulaire, un invariant différentiel, un régulateur, une fonction Zêta, une fonction de Dirichlet –Hasse, un conducteur ...

Nous commençons par le discriminant, l'invariant modulaire et l'invariant différentiel

Invariants j (E) et ω(E)

Définition 4 *Le discriminant d'une cubique de Weierstrass E est un polynôme homogène de degré 12 de l'anneau IZ* $[b_2, b_4, b_6]$ *égal à :*

$\Delta(E) = 9b_2b_4b_6 - 8b_4^3 - 27b_6^2 - b_2^2b_8$ où $4b_8 = b_2b_6 - b_4^2$ pour car(K) $\neq$ 2 , 3

Exemple de la cubique de Weierstrass :

$E : y^2 - 5xy + 4y = x^3 + 6x^2 - 7x + 11 \in$ IQ[x, y]

Avec le calcul nous trouvons :

$b_2 = 49$; $b_4 = -34$; $b_6 = 60$; $b_8 = 446$ et $\Delta(E) = 1.774.254 = 6 \times 31 \times 9539$

Définition 5 *L'invariant modulaire d'une courbe elliptique E est l'élément* $j(E)$ *du corps K égal à* $j(E) = \dfrac{c_4^3}{\Delta(E)}$

Exemple précèdent

Avec le calcul nous obtenons les valeurs des invariants de la cubique E

$c_4 = 3197 = 23 \times 139$ et $j(E) = \dfrac{-3197^3}{1.774254}$

Définition 6 *L'invariant différentiel d'une courbe elliptique E est l'élément différentiel :*

$$\omega(E) = \frac{dx}{2y + a_1x + a_3} = \frac{dy}{3x^2 + 2a_2x + a_4 - a_1y}$$

Exemple précédent :

$$\omega(E) = \frac{dx}{2y - 5x + 4} = \frac{dy}{3x^2 + 12x - 7 + 5y}$$

Les invariants de la cubique de Weierstrass

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

sont égaux à

Discriminants de polynômes f(x)

$\Delta(E) = -16(4A^3 + 27B^2)$, $j(E) = \dfrac{1728(4A)^3}{\Delta(E)}$ et $\omega(E) = \dfrac{dx}{2y} = \dfrac{dy}{3x^2 + A}$.

4- Discriminant d'un polynôme f(x) $\in$ K[x]

La théorie du discriminant d'un polynôme se trouve dans "Algebra "de Lang [10 – 1] et dans " Introduction à l'Algèbre "de Kostrikine [9]

L'équation de Weierstrass d'une cubique peut se mettre sous la forme $y^2 = f(x)$ pour des polynômes cubiques de cinq types :

$f(x) = 4x^3 + b_2x^2 + 2b_4x + b_6$, $f(x) = x^3 - 27c_4x - 54c_6$,

$f(x) = (x - e_1)(x - e_2)(x - e_3)$, $f(x) = x^3 + Ax + B$; $f(x) = x^3 + a_2x^2 + a_4x + a_6$

Le discriminant $\Delta(E)$ d'une cubique de Weierstrass est lié au discriminant $dis(f)$ du polynôme $f(x) \in K[x]$ de l'équation $y^2 = f(x)$

Tout polynôme $f(x) = d_0x^n + d_1x^{n-1} + ... + d_n \in K[x]$ de degré n se factorise sous la forme

$f(x) = d_0(x - \alpha_1)(x - \alpha_2)...(x - \alpha_n) \in K[x]$

Définition 7 *Le discriminant d'un polynôme* $f(x)$, *est l'élément* $dis(f)$ *du corps K égal à*

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

C'est une fonction symétrique quadratique de ses racines α_i.

Les fonctions symétriques élémentaires de ces racines sont des sommes S_t de produits de t racines, t = 1,…,n

$S_1 = \sum_i \alpha_i = \dfrac{-d_1}{d_0}$; $S_2 = \alpha_1\alpha_2 + ... + \alpha_{n-1}\alpha_n = \dfrac{d_2}{d_0}$, ..., produit des racines $S_n = \prod_i \alpha_i = (-1)^n \dfrac{d_n}{d_0}$

La formule de la définition 7 implique la

Proposition 1 *Le discriminant d'un polynôme* $f(x)$ *de degré* $n > 1$ *est nul si et seulement si il admet deux racines égales*.

Discriminants de polynômes f(x)

Preuve de "discriminant du polynôme f(x) est nul "implique "il admet deux racines égales "

La formule $dis(f) = d_0^{2n-2} \prod_{1 \le i \pi j \le n} (\alpha_i - \alpha_j)^2 = 0$ implique $\alpha_i - \alpha_j = 0$ pour un certain facteur $\alpha_i - \alpha_j$

Il en résulte que f(x) admet deux racines égales $\alpha_i = \alpha_j$

□

Selon H-Cohn [3] le calcul du discriminant *dis (f)* s'obtient au moyen d'un déterminant

Proposition 2 *Soit un polynôme unitaire* $f(x)$ *de degré* $n > 1$

$$f(x) = x^n + d_1 x^{n-1} + \ldots + d_n = (x - \alpha_0)\ldots(x - \alpha_{n-1}).$$

$\alpha_1, \ldots, \alpha_{n-1}$ *sont dans une clôture algébrique*

Alors son discriminant $\mathrm{dis}(f)$ *est égal au déterminant symétrique d'ordre* n

$$\mathrm{dis}(f) = \begin{vmatrix} \sigma_0 & \sigma_1 & \Lambda & \sigma_{n-1} \\ \sigma_1 & \sigma_2 & \Lambda & \sigma_n \\ M & M & & M \\ M & M & & M \\ \sigma_{n-1} & \sigma_n & \Lambda & \sigma_{2n-2} \end{vmatrix}$$

Les éléments $\sigma_m = \sum_0^{n-1} \alpha_i^m$ *sont des sommes de puissances des racines ; ce sont donc des fonctions symétriques non élémentaires des racines qui sont des polynômes de l'anneau* $IZ[d_1, \ldots, d_i]$ *:*

$\sigma_0 = n$, $\sigma_1 = -d_1$, $\sigma_2 = d_1^2 - 2d_2$, $\sigma_3 = 3d_1d_2 - d_1^3 - 3d_3$ *et* $\sigma_m = -md_m - \sigma_1 d_{m-1} - \ldots - \sigma_{m-1} d_1$

et $\sigma_m = 0$ *lorsque* $m > n$

Preuve :

Méthode de Girard ("A classical to Initiation Algebraic Number " , Partie I - 7 – H –COHN)

□

Relation Δ(E) – dis (f)

Une relation entre le discriminant de f(x) et le discriminant $\Delta(E)$ de la courbe elliptique d'équation $y^2 = f(x)$ est obtenue avec la

Proposition 3 *Soit une cubique E de Weierstrass :*

$$E : y^2 = x^3 + Ax + B = f(x) \in K[x] \ , \quad 4B^3+27A^2 \neq 0$$

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

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

Preuve

Soit f(x)= $x^3 + Ax + B$, avec la formule de la page 11 de Lang [10] j'obtiens le discriminant dis(f) = $-(4A^3 + 27B^2)$

Avec le calcul j'obtiens les valeurs :

$b_2 = 0$; $b_4 = 2A$; $b_6 = 4B$; $b_8 = -A^2$ et $\Delta(E) = -16(4A^3 + 27B^2)$

Il en résulte la relation $\Delta(E) = 16 dis(f)$

□

Lorsque le polynôme f(x) change, la relation entre dis (f) et $\Delta(E)$ change aussi

Proposition 4 *Soit une cubique de Weierstrass :*

$$E : y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6 = f(x) \in K[x] \quad et \quad \Delta(E) \neq 0 \qquad (1)$$

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

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

Preuve

Soit le polynôme cubique $f(x) = d_0x^3 + d_1x^2 + d_2x + d_3$ alors

son discriminant est égal à :

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

Résultant de deux polynômes

(formule de Lang dans "Algèbra " [10 - 1]).

En appliquant cette formule au polynôme (1) j'obtiens la valeur :

$dis(f) = 16(9b_2b_4b_6 - 8b_4^3 - 27b_6^2 - b_2^2b_8)$

Il en résulte la relation $dis(f) = 16\Delta(E)$

□

5 - Résultant de deux polynômes

La théorie des résultants Res (f, g) se trouve dans plusieurs ouvrages :

" Algèbra" de Lang [10 - 1] "Introduction à l'algèbre " de Kostrikin [9] etc…

Soient deux polynômes :

$f(x) = d_0x^n + d_1x^{n-1} + ... + d_n \in K[x]$ de degré $n>0$ *et*

$g(x) = r_0x^t + r_1x^{t-1} + ... + r_t \in$ K[x] de degré $t>0$

Définition 8 *Le résultant de deux polynômes f et g est le déterminant d'ordre n+t égal à :*

$$\mathrm{Re}\,s(f,g) = \begin{vmatrix} d_0 & d_1 & \mathrm{K} & d_n & 0 & \mathrm{K} & 0 \\ 0 & d_0 & d_1 & \mathrm{K} & d_n & 0 & 0 \\ 0 & & \mathrm{O} & & & & 0 \\ 0 & \mathrm{K} & & d_0 & d_1 & \mathrm{K} & d_n \\ r_0 & r_1 & \mathrm{K} & & r_t & \mathrm{K} & 0 \\ 0 & r_0 & r_1 & \mathrm{K} & & r_t & 0 \\ 0 & \mathrm{K} & \mathrm{K} & \mathrm{K} & \mathrm{K} & \mathrm{K} & r_t \end{vmatrix}$$

formé de t lignes ($d_0 ... d_n$) et n lignes ($r_0 ... r_t$), les termes manquant sont remplacés par des zéros la diagonale principale est formée de t nombres d_0 et n nombres r_t

Proposition 5 *Soient deux polynômes : $f(x) = d_0 \prod_{1\le i\le n}(x-\alpha_i)$ de degré $n \ge 1$ et $g(x) = r_0 \prod_{1\le j\le t}(x-\theta_j)$ de degré $t \ge 1$; leur résultant satisfait les relations :*

Résultant de deux polynômes

$$\mathrm{Re}\, s(f,g) = d_0^t \prod_{i=1}^{n} g(\alpha_i) = (-1)^{mt} \prod_{j=1}^{t} f(\theta_j) = d_0^t r_0^n \prod_{i,j} (\alpha_i - \theta_j)$$

Preuve : dans les ouvrages cités en références

□

Cette proposition implique un critère pour que le résultant soit nul

Proposition 6 *Le résultant* $R(f,g)$ *de deux polynômes* $f(x)$ *et* $g(x)$ *est nul si et seulement si les deux polynômes ont une racine commune*.

Preuve

Res (f , g) = 0 et la relation de la proposition (5) impliquent α_i est racine du polynôme g(x) et $\alpha_{\mathrm{i}} = \theta_{\mathrm{j}}$ pour certains indices i , j

Donc les deux polynômes f(x) et g(x) ont une racine commune

□

Le résultant d'un polynôme f(x) et de sa dérivée f '(x) satisfait le

Corollaire *le résultant* $\mathrm{Re}\, s(f,f')$ *d'un polynôme* $f(x)$ *et de sa dérivée* $f'(x)$ *est égal à*

$$\mathrm{Re}\, s(f,f') = d_0^{n-1} \prod_{i=1}^{n} f'(\alpha_i) \quad , \quad \text{pour} \quad f(x) = d_0 (x-\alpha_1)...(x-\alpha_n)$$

□

Exemple : polynôme cubique f(x) = $x^3 + 2\,x^2 - 3\,x + 6$,

Alors f '(x) = $3\,x^2 + 4\,x - 3$, le résultant Res (f, f ') est égal au déterminant d'ordre 5

$$D = \begin{vmatrix} 1 & 2 & -3 & 6 & 0 \\ 0 & 1 & 2 & -3 & 6 \\ 3 & 4 & -3 & 0 & 0 \\ 0 & 3 & 4 & -3 & 0 \\ 0 & 0 & 3 & 4 & -3 \end{vmatrix}$$

J'obtiens la valeur Res (f , f ') =1848

Cubiques de Weierstrass singulières

6- Classification des cubiques de Weierstrass par leur discriminant $\Delta(E)$ et leur invariant $c_4(E)$

Les cubiques singulières sont classifiées par la

Proposition 7 *Soit une cubique de Weierstrass E, d'invariants* $\Delta(E)$ *et* $c_4(E)$.

1) la cubique est singulière si et seulement si $\Delta(E)=0$

2) elle admet un nœud si et seulement si $\Delta(E)=0$ *et* $c_4(E)\neq 0$

3) elle admet un point de rebroussement si et seulement si $\Delta(E)=0$ *et* $c_4(E)=0$.

Preuve de " E singulière " implique " $\Delta(E)=0$ "

Une cubique singulière est une cubique ayant un point singulier.

Prenons une équation de Weierstrass $y^2 = f(x)$

Le point singulier est un point multiple d'ordre s ≥ 2

D'après la théorie des discriminants des polynômes

$dis(f)=0$ si et seulement si f a une racine multiple d'ordre s ≥ 2 (1)

Les relations $\Delta(E)=16dis(f)$ et (1) impliquent la valeur

$\Delta(E)=0$

□

Preuve de" $\Delta(E)=0$ " implique "E singulière "

L'hypothèse $\Delta(E)=0$, la relation $\Delta(E)=d\times dis(f)$ et (4), impliquent la valeur

$dis(f)=0$ (2)

La relation (2) et la formule $dis(f)=\prod_{1\leq i\pi j\leq n}(\alpha_i-\alpha_j)^2$ impliquent

La cubique admet un point multiple d'ordre s ≥ 2, donc elle est singulière.

□

Cubiques de Weierstrass singulières

Preuve de " $\Delta(E)=0$ " et " $c_4(E) \neq 0$ " implique la cubique E admet un nœud :

L'hypothèse $\Delta(E)=0$ implique E admet un point singulier

Soit S ce point singulier ; en ce point la courbe admet deux tangentes distinctes ou confondues.

Les pentes de ces tangentes sont égales à la dérivée y' de y.

Je choisis une équation de Weierstrass $y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6$

Le calcul de la dérivée fournit la valeur

$$y' = \frac{6x^2 + b_2x + b_4}{y} = \frac{g(x)}{y} \ ;$$

g(x) est un polynôme de degré deux, de discriminant égal à $dis(g) = b_2^2 - 24b_4 = c_4(E)$ (3)

l'hypothèse $c_4(E) \neq 0$ implique la courbe E admet deux tangentes distinctes.

Il en résulte que la courbe E admet un nœud au point S.

□

Preuve de " $\Delta(E)=0$ "et " $c_4(E)=0$" impliquent le point S est un point de rebroussement.

La relation (6) et l'hypothèse $c_4(E)=0$ impliquent une racine double, donc deux tangentes confondues.

Par suite la cubique admet un point de rebroussement S.

□

Illustrons cette classification par un exemple de chacune des deux classes :

Exemple 1 : cubique qui a un nœud

Soit la cubique de Weierstrass :

$E_1 : y^2 + 4xy + 8y = x^3 - 4x^2 - 19x - 14$

Avec le calcul j'obtiens les invariants :

Cubiques de Weierstrass singulières

$b_2 = 0$; $b_4 = -6$; $b_6 = 8$; $b_8 = -9$; $\Delta(E_1) = 0$ et $c_4(E_1) = 144$

$\Delta(E_1) = 0$ et $c_4(E_1) \neq 0$ impliquent que la cubique E_1 admet un nœud

Tableau des coordonnées de quelques points de la cubique E_1

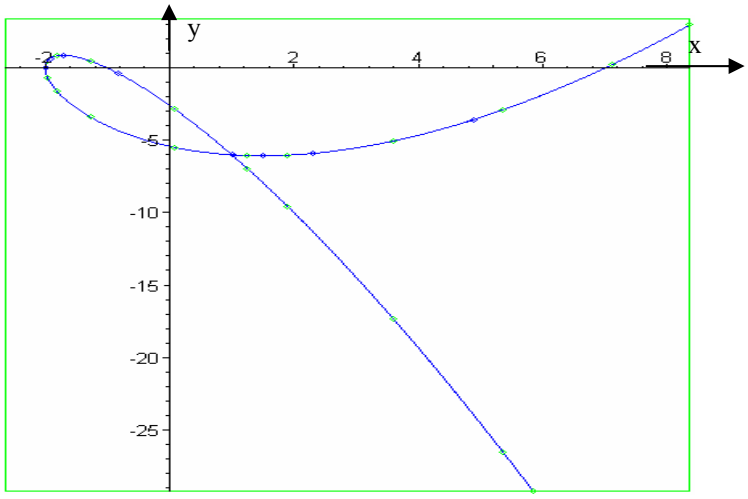
x	-3	-2	0	1	4	6
y	Pas de y réel	0	$-4 \pm \sqrt{2}$	-6 double	$-12 \pm 3\sqrt{6}$	$-16 \pm \sqrt{2}$

Le tableau indique que le nœud est le point de coordonnée (1, -6)

Pour x = -2 on trouve y = 0 est une racine double.

Pour trouver la nature de ce point singulier je calcule la valeur de la dérivée $y'(-2 , 0)$

$y'(-2 , 0) = -\infty$ donc la courbe admet une tangente parallèle à l'axe Oy en ce point.



Courbe tracée avec le logiciel « MAPLE 9

Exemple 2 Cubique de Weierstrass avec un point de rebroussement

Soit la cubique de Weierstrass

Cubiques de Weierstrass singulières

$E_2 : y^2 + 2xy + 10y = x^3 - x^2 - 10x - 25 \in$ IR [x, y]

Avec le calcul j'obtiens les invariants $b_{2i} = 0$ pour $i = 1,2,3,4$, $\Delta(E_2) = 0$ et $c_4(E_2) = 0$

La proposition 6 implique que cette cubique admet un point de rebroussement

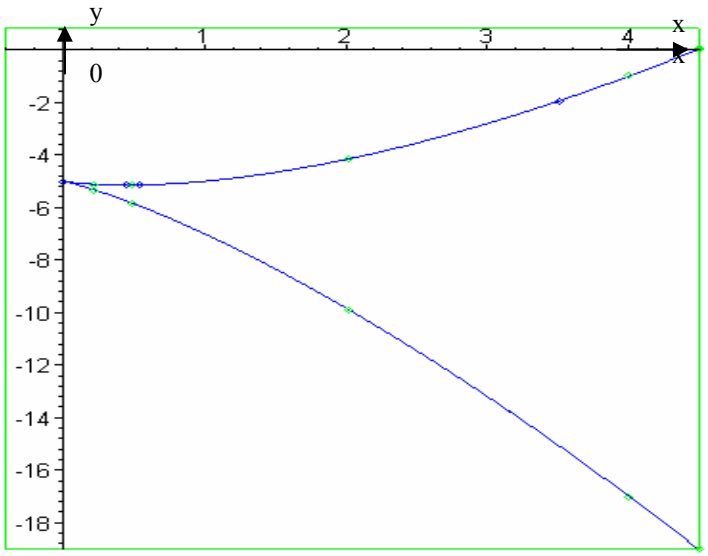
Tableau des coordonnées de quelques points de la cubique

x	-1	0	1	2	3
y	pas de solutions réelles	-5 double	-7 et -5	-10 et -4	$-8 \pm \sqrt{24}$

D'après le tableau, le point (0, -5) est le point de rebroussement de la cubique

La valeur $y'(0, 5) = \frac{0}{0}$ est indéterminée .

Pour obtenir l'équation de la tangente en ce point, je prends une droite $y = tx + 5$, je porte y dans l'équation de E_2, j'obtiens une équation en x qui admet une racine double.



Courbe tracée avec Logiciel MAPLE 9

Etudions maintenant les cubiques de Weierstrass non singulières

Courbes elliptiques

Proposition 8 *Soit une cubique de Weierstrass E de discriminant* $\Delta(E)$

$$E : \ y^2 = f(x) \in IR\,[\,x\,]$$

1) la cubique E est une courbe elliptique si et seulement si $\Delta(E) \neq 0$

2) la courbe elliptique E coupe l'axe 0x en trois points simples si et seulement si $\Delta(E) > 0$

3) la courbe elliptique E coupe l'axe 0x en un seul point qui est simple si et seulement si $\Delta(E) < 0$

1) Preuve de" $\Delta(E) \neq 0$ " implique " la cubique E est une courbe elliptique "

Soit une cubique de Weierstrass E : $y^2 = f(x) \in \mathrm{IR}\,[\,\mathrm{x}\,]$, de discriminant $\Delta(\mathrm{E})$.

L'hypothèse $\Delta(E) \neq 0$ et la relation entre les discriminants de E et de f impliquent

$\mathrm{Res}(f, f') \neq 0$,

par suite le polynôme cubique admet trois racines distinctes ; la cubique E n'est pas singulière ; c'est une courbe elliptique.

2) Preuve de" la courbe elliptique E coupe l'axe Ox en trois points simples " implique" $\Delta(E) > 0$"

Soit une courbe elliptique E qui coupe l'axe Ox en trois points distincts

$$P_i = (e_i, 0) \ ; \text{ pour } i = 1,2,3 \qquad (1)$$

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

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

La relation (1) implique que f(x) et $f'(x)$ n'ont pas de racine commune

Il en résulte que le résultant $\mathrm{Res}(f, f') \neq 0$.

Classification de courbes elliptiques

Par définition du discriminant d'un polynôme f(x) = $\prod_i (x - x_i)$, Le discriminant de f est égal à : dis(f) = $\prod_{i \pi j} (e_i - e_j)^2$;

Par hypothèse, les trois racines e_i sont réelles,

Donc les carrés $(e_i - e_j)^2$ sont positifs et dis(f) >0

La relation entre Res(f , f') et discriminants dis(f) de f et $\Delta(E)$ de E implique l'inégalité $\Delta(E)$>0.

3) Preuve de "E coupe l'axe Ox en un point simple" implique " $\Delta(E) < 0$ " :

L'hypothèse " la courbe elliptique E coupe l'axe Ox en un point simple " implique une équation de la forme :

E : $y^2 = (x-e)(x^2 + rx + s) = f(x) \in$ IR [x] avec $r^2 - 4s < 0$ (3)

Donc le polynôme x^2+rx+s admet deux racines complexes conjuguées

$e_j = -\frac{1}{2}(r \pm i\sqrt{4s - r^2})$ avec j=2,3

Le discriminant du polynôme f (x) est égal à :

$dis(f) = (e-e_1)^2(e-e_2)^2(e_1-e_2)^2 = -4(4s-r^2)^2\left[(e-\frac{1}{2}r)^2 + (4s-r^2)^2\right]^2 < 0$

La relation entre résultant Res(f, f '), discriminant dis (f) de f et $\Delta(E)$ de E, impliquent $\Delta(E) < 0$

□

7- Exemples illustrant la classification des courbes elliptiques

Exemple 1 : courbe elliptique qui coupe l'axe Ox en un point simple

Soit la cubique de Weierstrass d'équation :

$E_3 : y^2 + xy + 6y = x^3 + 4x^2 + x + 4$

Avec le calcul j'obtiens les invariants : $b_2 = 5$; $b_4 = 14$; $b_6 = 52$; $b_8 = 16$ et $\Delta(E) = -6200$

La valeur $\Delta(E) < 0$ implique que la courbe elliptique E_3 coupe l'axe Ox en un seul point qui est simple

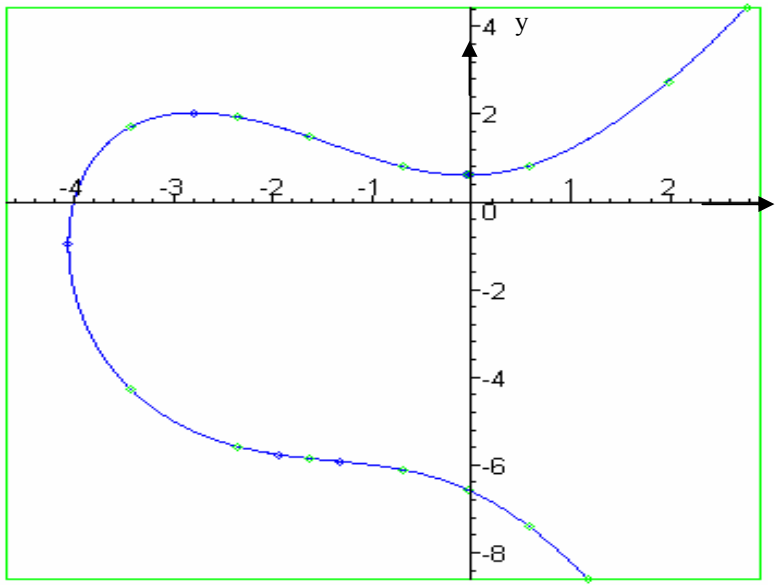
Exemple de courbe elliptique de type 2

Tableau des coordonnées de quelques points de la courbe

x	-5	-4	-3	-1	0
y	Pas de solutions réelles	0 et -2	$\frac{-3 \pm \sqrt{45}}{2}$	$\frac{-5 \pm \sqrt{41}}{2}$	$-3 \pm \sqrt{16}$

x	2
y	$-8 \pm \sqrt{46}$

Le tableau indique que le point d'intersection de courbe avec l'axe Ox est le point (-4 , 0)



Courbe tracée avec le logiciel Maple 9

Exemple 2 : courbe elliptique qui coupe l'axe Ox en trois points simples

Soit la Cubique de Weierstrass

Exemple de courbe elliptique de type 1

$E_4 : y^2 - xy + y = x^3 - 5x^2 - 56x + 60 \in \mathrm{IR}[x, y]$

Avec le calcul j'obtiens les invariants : $b_2 = -19$; $b_4 = -113$; $b_6 = 265$; $b_8 = -4451$

et $\Delta(E_4) = 16374507 > 0$

La valeur $\Delta(E_4) > 0$ implique trois points d'intersection simples de la courbe elliptique et l'axe Ox.

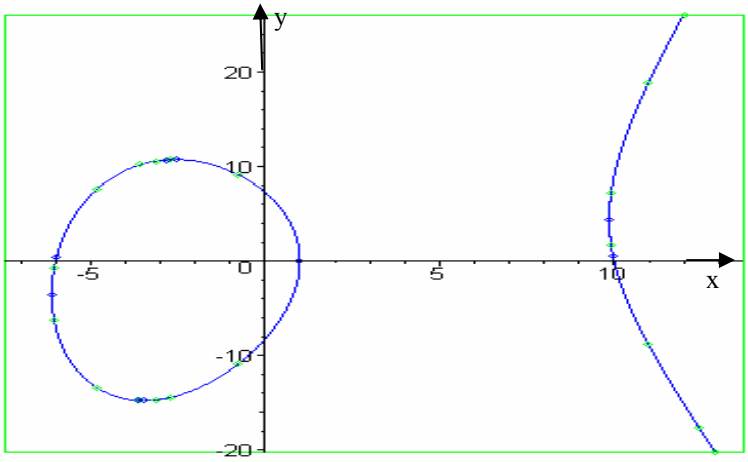
Tableau des coordonnées de quelques points de la courbe E_4

x	-6	-5	0	1	10	11	12
y	0 et - 7	$\frac{-5 \pm 2\sqrt{309}}{2}$	$\frac{1 \pm \sqrt{241}}{2}$	0 double	0 et 9	$\frac{11 \pm 2\sqrt{195}}{2}$	$\frac{11 \pm \sqrt{1705}}{2}$

Le tableau indique que les trois points d'intersection de la courbe avec l'axe Ox sont les points $P_1 = (-6, 0)$, $P_2 = (1, 0)$ et $P_3 = (10, 0)$

La courbe se trouve dans l'intervalle : $[-6, 1] \cup [10, \infty]$

La valeur de la dérivée $y'(1, 0) = \infty$ implique que la courbe admet une tangente en ce point parallèle a l'axe Oy.



Courbe tracée avec le logiciel Maple 9

Chapitre II GROUPE DE MORDELL-WEIL DES COURBES ELLIPTIQUES

Dans ce chapitre j'étudie la structure algébrique de l'ensemble E (K) des points K-rationnels d'une courbe elliptique.

1- Loi de groupe abélien sur une courbe elliptique

Soit une cubique de Weierstrass E d'équation

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

L'ensemble des points K-rationnels d'une cubique de Weierstrass peut être muni d'une structure de groupe abélien. Pour cela il faut un élément neutre et une loi de composition.

Proposition 1 *L'ensemble E(K) des points K-rationnels d'une cubique de Weierstrass E est un groupe abélien, d'élément neutre le point à l'infini* $O_E = (\infty, \infty) \in IA^2$ et $O_E = (0, 1, 0) \in IP^2$ *et de loi de composition*

$$E(K) \times E(K) \to E(K) \qquad (P_1, P_2) \to P_1 + P_2$$

basée sur la règle géométrique

"Trois points P_i colinéaires de la cubique E ont une somme nulle

$$P_1 + P_2 + P_3 = 0_E \text{ "}$$

Preuve :

Vérifions les quatre axiomes d'un groupe abélien.

Axiome de l'élément neutre :

Par définition le point à l'infini

$O_E = (\infty, \infty) \in IA^2$ et $O_E = (0, 1, 0) \in IP^2$

est déterminé par la direction de l'axe Oy

Coordonnées des points –P et P_1+P_2

Appliquons la règle géométrique des trois points colinéaires à un point P

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

Axiome du symétrique :

$P + R + O_E = O_E$ implique que la sécante PR est parallèle à l'axe Oy

Il en résulte que le symétrique est le point $-P = R$

Axiome de commutativité

Les sécantes P_1P_2 et P_2P_1 sont confondues ;

$P_1+P_2 = P_2+P_1$

Axiome d'associativité

Il se vérifie par le calcul des coordonnées des points

$(P_1+P_2) +P_3 = P_1+(P_2+P_3)$ pour des points $P_i \neq P_j$

□

2- Coordonnées des points –P, P_1+P_2, et 2P

Le symétrique -P d'un point $P = (x_1, y_1)$ est l'intersection de la cubique E par une parallèle à l'axe Oy passant par le point P (fig. 1).

Cette droite a pour équation $x = x_1$

Pour $x = x_1$ l'équation (1) devient une équation du deuxième degré en y, paramétrique en x_1. Donc elle admet deux racines y_1, y_2.

La fonction symétrique" somme des racines"d'un polynôme f(x) implique la relation :

$y_1 + y_2 = -a_1x_1 - a_3$

Il en résulte que le symétrique –P du point P est le point $-P = (x_1, -y_1 - a_1x_1 - a_3)$

Coordonnées des points –P et P_1+P_2

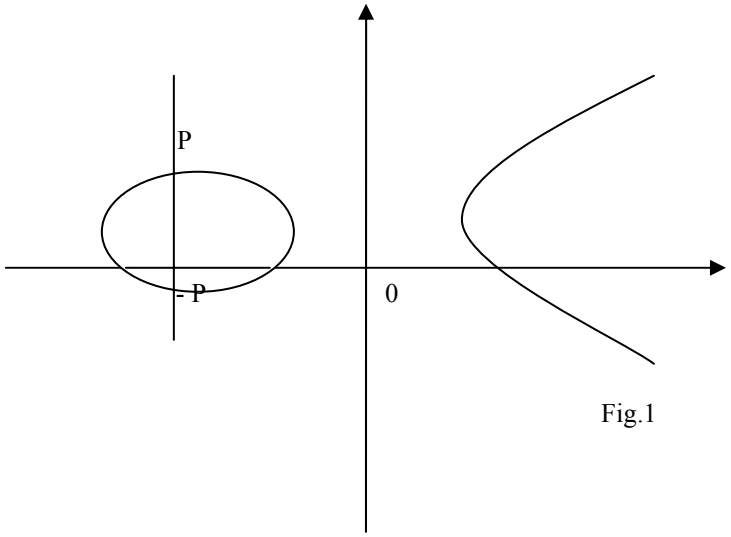


Fig.1

Les coordonnées de la somme P_1+P_2 de deux points $P_i = (x_i, y_i)$ de la cubique E, pour $P_1 \neq \pm P_2$ est déterminée par la règle géométrique des trois points colinéaires (Fig. 2)

$P_1 + P_2 + P_3 = 0_E$

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

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

Équation de la droite P_1P_2 :

$y = \lambda\ (x-x_1) + y_1$ de pente $\lambda = \frac{y_1 - y_2}{x_1 - x_2}$;

cette droite coupe la courbe en trois points P_1, P_2 et P_3

les abscisses de ces trois points sont les racines de l'équation (1)

J'utilise la fonction symétrique " somme de racines " d'un polynôme f(x) :

J'obtiens les coordonnées du point $P_1 + P_2 = M$

Coordonnées du point 2P

$$x_M = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2 \quad , \quad \text{où} \quad \lambda = \frac{y_1 - y_2}{x_1 - x_2} \quad \text{et} \quad x_1 \neq x_2$$

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

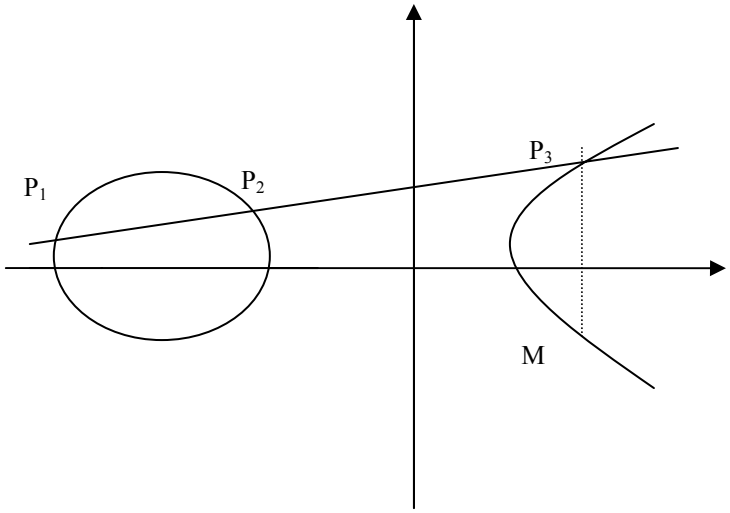


Fig. 2

Lorsque $P_1 = P_2 = P$ la droite P_1P_2 devient tangente à la courbe E au point P,

Cette tangente recoupe la courbe E en un point simple T. (Fig. 3)

La règle géométrique des trois points colinéaires implique la relation :

$P+P+T = 0_E = 2P + T$

L'équation de la tangente à la courbe E en un point P est égale à :

$$y = y'_P(x - x_P) + y_P \quad \text{avec} \quad y'_P = \frac{3x_P^2 + 2a_2x_P + a_4 - a_1y_P}{2yP + a_1x_P + a_3} \quad ,$$

y'_P est la pente de la tangente à la courbe E au point P

Pour $y = y'_P(x - x_P) + y_P$ l'équation (1) devient une équation du troisième degré en x

Elle admet une racine x_P double et une racine x_T simple.

Coordonnées du point 2P

Avec la fonction symétrique" somme des racines" j'obtiens l'abscisse x_{2P} :

$$x_{2P} = y_p'^2 + a_1 y_P' - a_2 - 2x_P$$

Avec la formule du symétrique, j'obtiens l'ordonnée du point 2P

$$y_{2P} = -y'^3_P + 2a_1 y_P'^2 + (a_2 - a_1^2 - 3x_P) y_P' + a_1 a_2 - a_3 + 2a_1 x_P - y_P$$

J'ai démontré la

Proposition 2 *Soit une courbe elliptique E d'équation de Weierstrass*

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

1) le symétrique –P d'un point P = (x_P , y_P) de la courbe E a pour coordonnées

$$x_{(-P)} = x_P \qquad et \qquad y_{(-P)} = -a_1 x_P - a_3 - y_p$$

2) la somme P_1+P_2 de deux points $P_1= (x_1 , y_1)$, $P_2 = (x_2 , y_2)$, $P_1 \neq \pm P_2$ de la courbe

E est le point M de coordonnées *:*

$$x_M = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2 \quad , \quad où \quad \lambda = \frac{y_1 - y_2}{x_1 - x_2} \quad et \quad x_1 \neq x_2$$

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

3) le point P +P =2P a pour coordonnées

$$x_{2P} = y_p'^2 + a_1 y_P' - a_2 - 2x_P \quad et \quad y_P' = \frac{3x_P^2 + 2a_2 x_P + a_4 - a_1 y_P}{2y_p + a_1 x_P + a_3}$$

$$y_{2P} = -y'^3_P + 2a_1 y_P'^2 + (a_2 - a_1^2 - 3x_P) y_P' + a_1 a_2 - a_3 + 2a_1 x_P - y_P$$

□

Exemple : courbe elliptique E d'équation de Weierstrass

$$E : y^2 = x^3 + 2x^2 - 15x \in IR[x]$$

Coordonnées des points mP ; formule de Cassels

Calcul des invariants : $b_2 = 8$; $b_4 = -30$; $b_6 = 0$; $\Delta(E) = 230400$; $C_4(E) = 784$

$\Delta(E) > 0$ implique trois points d'intersections avec l'axe Ox

P = (0, 0), R = (-5, 0) et T = (3 , 0)

Calcul des coordonnées des points –P, -R, -T, P+R, R+T, P+R+T, P-R, 2P, 2R, 2T.

-P = (0,0), -R = (-5,0), -T = (3,0).

P+R = (3,0), R+T = (0,0).

P+R+T = (∞, ∞), P-R = (3,0).

2P = (∞, ∞), 2R = (∞, ∞), 2T = (∞, ∞).

3-Points d'ordre fini d'une cubique de Weierstrass et formules de Cassels

Les coordonnées d'un point 2P sont des fonctions rationnelles en x et y.

La dérivée y' de y est la fonction rationnelle :

$$y' = \frac{3x^2 + 2a_2x + a_4 - a_1y}{2y + a_1x + a_3}$$

J'obtiens les coordonnées du point 2P avec la proposition 2 :

$$x_{2P} = \frac{\phi_2}{\psi_2^2} \quad \text{et} \quad y_{2P} = \frac{\omega_2}{\psi_2^3}$$

avec les polynômes : $\psi_2 = 2y + a_1x + a_3$ et

$$\phi_2 = 9x^4 + Ax^3 + Bx^2 + Cx + Dy^2 + Ey + Fx^2y + Gxy - 8xy^2 + H$$

où

$A = 12a_2 + a_1$, $B = 4a_2^2 + 6a_4 - a_1a_3 + a_1^2a_2$, $C = 4a_2a_4 + a_1^2a_4 - 2a_3^2$

$D = -a_1^2 - 4a_2$, $E = -a_1^2a_3 - 4a_2a_4$, $F = -8a_1$, $G = -a_1^3 - 4a_1a_2 - 8a_3$

Coordonnées des points mP ; formule de Cassels

$H = a_1 a_3 a_4 - a_2 a_3^2$ et $\psi_2 = 2y + a_1 x + a_3$,

$y_{2p} = \dfrac{\phi_2}{\psi_2^3}$ où ϕ_2 est un polynôme de degré 6 en x et y

Les coordonnées des points 3P = 2P+P, 4P=2(2P) et mP de courbes particulières peuvent être obtenues avec la

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

$$E : y^2 = x^3 + Ax + B \in \mathrm{IQ}[x, y] \quad \text{et} \quad 4A^3 + 27B^2 \neq 0$$

Les coordonnées des points mP, pour m >2, sont égales à :

$$(x_{mP}, y_{mP}) = \left(\frac{\phi_m(x,y)}{\psi_m^2(x,y)}, \frac{\omega_m(x,y)}{\psi_m^3(x,y)} \right)$$

Les polynômes ψ_m satisfont les relations de récurrence :

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

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

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

$$\psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_{m-1}^3\psi_{m+1}^3 \quad \textit{pour} \quad m \geq 2$$

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

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

Preuve :

La formule –P = (x , -y) implique

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

Groupe de Torsion T(E(K))

La relation OP = $(\infty,\infty) = (\frac{x}{0},\frac{y}{0})$ implique $\psi_0 = 0$

La relation 1. P = (x ,y) = ($\frac{x}{1^2},\frac{y}{1^3}$) implique $\psi_1 = 1$

Pour m ≥ 2 on utilise un raisonnement par récurrence sur m.

Selon Cassels [2], lorsque K= C = corps des nombres complexes,

ce sont les formules de la fonction P(z ; L) de Weierstrass qui sont utilisées

C'est le lemme 7-2 dans [2] de Cassels.

□

4-Groupe de torsion T(E(K)) d'une cubique de Weierstrass

Dans la théorie des groupes il y a la notion de points d'ordre fini et de sous groupes de torsion

Appliquons ces notions au groupe de Mordell –Weil E (K) des courbes elliptiques.

Définition 1 *1) Un point de m-tortion d'une courbe elliptique E est un point P d'ordre m dans le groupe de Mordell-Weil E(K) : $mP = 0_E$*

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

4) le groupe de torsion de la courbe E est la réunion infinie des sous groupes de

m- torsion $T(E) = \bigcup_m E[m] = \{P \in E(k) : mP = 0_E \; m \in Z\}$

La structure de ce groupe dépend du corps K

Conjecture : le groupe de torsion T(E(K)) est un groupe abélien fini

Hauteurs et descente sur un groupe abélien

La structure du groupe de torsion du groupe abélien E(IQ) est déterminée par la :

Proposition 4 *le groupe de torsion T(E)(IQ) d'une courbe elliptique E est isomorphe à l'un des quinze groupes additifs finis :*

IZ/dIZ avec $1 \le d \le 10$ et $d = 12;$

$IZ/2IZ \times IZ/2dIZ$ avec $1 \le d \le 4;$

Preuve : Mazur montre qu'il n'y a pas de groupe de m-torsion pour m =11 et $m \ge 13$.

Il utilise la théorie des isogenies, les Courbes Modulaires de niveau 13, la théorie de Neron-Tate relative aux homomorphismes d'un corps fini IF_p

(Invention Mathématique. 44 - (1978). 129-162.)

□

Ainsi le groupe de torsion T(E(Q)) est d'ordre inférieur à 11 ou égal à 12.

L'existence d'un point non nul de torsion sur une courbe elliptique E sur l'anneau IZ peut être étudiée avec la :

Proposition 5 *Soit la famille de courbes elliptiques E = E(A,B) d'équation de Weierstrass :*

$E : y^2 = x^3 + Ax + B \in IQ[x,y]$ avec $A, B \in IZ$ *et* $4A^3 + 27B^2 \neq 0.$

Alors tout point $P \in E(IQ)$ *de torsion a des coordonnées,* $x_p , y_p \in IZ$

Lorsque $2P \neq 0_E$, *alors* y_p^2 divise $4A^3 + 27B^2$

Preuve :

Lutz : "sur les équations $y^2 = x^3$-Ax –B " Jon R. Angew. n^0 177 (1937) – 237- 247

Nagell : " Théorie Arithmétique des cubiques planes Wid- Akad- Oslo (1935)

□

Hauteurs et descente sur un groupe abélien

5 Hauteurs sur un groupe abélien et descente sur E(K)

Selon Lang [10 -2] , Poincaré a conjecturé que le groupe E(K) des points K rationnels d'une courbe elliptique E est de type fini.

Mordell a prouvé cette conjecture dans ″on the rational solutions of the indeterminate equations of the third and fourth degrees ″- Proc. Camb. Philos. Soc. 21(1922) 179-192.

Weil a étendu ce résultat aux variétés abéliennes.

La preuve est formée de deux parties.

Dans l'une l'auteur montre que le groupe quotient $E(K)/2E(K)$ est fini.

Dans l'autre partie il utilise des fonctions spéciales « hauteurs sur un groupe abélien » et la procédure de « descente infinie ».

□

Proposition 6 *soit le groupe de Mordell-Weil E (K) d'une courbe elliptique E, alors le groupe quotient* $E(K)/2E(K)$ *est fini.*

Preuve : selon Lang [10]

Soit une courbe elliptique d'équation de Weierstrass

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

Alors les trois points $P_i = (e_i, 0)$ sont d'ordre deux

Considérons les trois homomorphismes de groupes $f_i : E(K) \to K^*/(K^*)^2$, i=1, 2, 3 dont les noyaux satisfont $\bigcap_i \ker f_i \subset 2E(K)$

Prenons les valeurs $f_i(0_E) = 1$, $f_i(x, y) = x - e_i \mod (K^*)^2$ si $x \neq e_i$

et $f_i(e_i, 0) = (e_i - e_j)(e_i - e_k) \mod (K^*)^2$

Ces valeurs des homomorphismes f_i sont choisies pour que le groupe quotient $E(K)/2E(K)$ soit fini.

□

Hauteurs et descente sur un groupe abélien

Les fonctions hauteurs sur un groupe abélien sont précisées dans la

Définition 2 **(** selon Silverman [17 – 1]) *une hauteur sur un groupe abélien A est une fonction* $h : A \rightarrow IR$

qui satisfait les trois conditions :

h_1) pour tout point $Q \in A$ il existe une constante $c_1(A, IQ)=c_1$ telle que

$$h(P+Q) \leq 2h(P) + c_1 \qquad \textit{pour tout point } P \in A$$

h_2) il existe un entier $m \geq 2$ et une constante $c_2(A) =c_2$ tels que :

$$h(mP) \geq m^2 h(P) - c_2 \qquad \text{pour tout point } P \in A$$

h_3) pour tout nombre réel c_3, l'ensemble : $\{P \in A : h(P) \leq c_3\}$ *est fini*

Utilisons un résultat de [17 -1]

Proposition 7 *soit un groupe abélien A tel que le groupe quotient* A/mA *est fini et une fonction hauteur* $h : A \rightarrow IR$. *Alors le groupe abélien A est de type fini*

Preuve

Soit un groupe abélien A, des représentants $R_1,\ldots,R_t$ des classes du groupe quotient A/mA

Construisons une suite infinie de points $P_1,\ldots,P_n$ à partir d'un point P :

$P=mP_1+R_{i_1}$; $P_1 =mP_2+R_{i_2}$; $P_j =mP_{j+1} + R_{i_{j+1}}$; $P_{n-1} =mP_n+R_{i_n}$ avec $1 \leq i_1, \ldots, i_n \leq t$. (1)

la relation $P_{j-1}=mPj+Ri_{-j}$ implique

$$mP_j = P_{j-1} - R_{i-j}$$

en appliquant l'axiome (h_2) et (h_1) au premier et au deuxième membre de l'égalité j'obtiens l'inégalité :

$$h(P_j) \le \frac{2}{m^2}(h(P_{j-1} - R_{i_{j-1}}) + c'_j) \qquad (2)$$

En additionnant membre à membre les inégalités (2) pour j = 1,…, n j'obtiens l'inégalité :

$$h(P_n) \le (\frac{2}{m^2})^n h(P) + \left(\frac{1}{m^2} + \frac{2}{m^4} + \frac{2^{n-1}}{m^{2n}}\right) c' \qquad (3)$$

La série en $\frac{1}{m^2}$ du deuxième membre provient du développement limité de

$$\frac{1}{1-u} = 1 + u + u^2 + ... + u^N + .. \qquad \text{pour } u^t = \frac{2^{t-1}}{m^{2t}} \qquad (4)$$

Les relations (3) et (4) impliquent les inégalités :

$$h(P_n)\ \pi\ (\frac{1}{m^2})^n h(P) - \frac{c}{m} \le \frac{1}{2^n} h(P) + \frac{c}{2} \qquad \text{pour } m \ge 2 \text{ et } c = \frac{c'}{2} \qquad (5)$$

Pour un entier n assez grand, $\lim_{n \to \infty} (\frac{2}{m^2})^n = 1.$ (6)

Il en résulte la borne de $h(P_n) \le 1+c_2$ (7)

L'axiome (h_3) et la relation (7) impliquent que l'ensemble :

$\{ P_n \in A ; h(P_n) \le 1+c_5 \}$ est fini .

Il en résulte que tout point P du groupe abélien A est une combinaison linéaire

$$P = n_1 R_1 + ... + n_t R_t + n_{t+1} P_1 + ... + n_{t+r} P_u \ ; \quad ; n_1,...,n_{t+r} \in IZ$$

□

Citons quelques types des hauteurs sur les courbes elliptiques : la hauteur logarithmique (hauteur de Weill), la hauteur canonique (hauteur de Neron-Tate) et les hauteurs locales .

Hauteur de Weil

Définition 3 *la hauteur de Weil sur une courbe elliptique E est la fonction*

h : E(IO) $\to$ *IR de valeur h(P) = log{max (* $|a|, |b|$ *) } pour P=(x , y)*

d'abscisse $x = \frac{a}{b}$

Exemple : soit la courbe elliptique E d'équation de Weierstrass :

$$E : y^2 + \frac{3}{4}y = x^3 - \frac{5}{3}x^2 + \frac{2}{3}x \quad \in IQ[x, y]$$

Son discriminant est égal à $\Delta(E) = \frac{3634693}{20736} > 0$. Le point P= $(\frac{2}{3}, -\frac{3}{4})$ est un point de la courbe E(IQ) sa hauteur de Weill est égale à h(P) = log{ max($|2|, |3|$) } = log 3 .

Définition 4 *la hauteur canonique (hauteur de Néron -Tate) sur une courbe elliptique E est la fonction* $\hat{h} : E(K_{alg}) \to IR$ *de valeur :*

$$\hat{h}(P) = \lim_{n \to \infty} 4^{-n} h(2^n P) .$$

La hauteur canonique $\hat{h}_f$ relative à une fonction f (paire, non constante, du corps des fonctions K(E)) est obtenue par la :

Proposition 8 *la hauteur canonique* $\hat{h}_f$ *relative à une fonction f à pour valeur :*

$\hat{h}_f(P) = \frac{1}{\deg(f)} \hat{h}(P) = \frac{1}{\deg(f)} \lim 4^{-n} h_f(2^n P)$. *Alors , la limite existe ; elle est indépendante de f*

Preuve : selon [9-2] chapitre VIII paragraphe 9 proposition 9.1

□

La structure du type du groupe de Mordel-Weil est précisée par la

Proposition 9 *le groupe de Mordell-Weil E (K) d'une courbe elliptique E est un groupe*

abélien de type fini isomorphe à un produit de deux groupes abéliens.

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

T(E) = groupe de torsion de E qui est fini.

IZ^{r} = r copies du groupe abélien IZ des entiers rationnels

□

Définition 3 *l'entier r = r(E) ≥ 0 de la formule de la proposition (5) est le rang de la courbe elliptique ,il est égal au nombre de points indépendants qui engendrent la partie infini E(K)-T(E)*

Cette structure $T(E) \times IZ^{r}$ est semblable à celle du groupe des unités d'un corps de nombres

Théorème (Dirichlet**)** *soit un corps de nombres L de degré fini [L : Q] = n =r_1+2r_2. r_1 conjugués réels et 2r_2 conjugués complexes*

Les unités du corps forment un groupe abélien U (L) isomorphe à un produit de groupes abéliens $U(L) \approx C(L) \times IZ^{t}$

où C(L)=groupe des racines de l'unité contenues dans L,

$t = r_1 + r_2 - 1$ = rang du groupe des unités

□

6- Rang de courbes elliptiques

Le rang r (E) d'une courbe elliptique E est donc le nombre de points d'ordre infini qui sont linéairement indépendants et qui engendrent la partie infinie du groupe de Mordell-Weil E (K).

Rang de courbes elliptiques

Dans la formule d'isomorphisme $T(E) \times IZ^r$, il n' y a pas de formule de calcul de ce rang comme la formule du rang du groupe des unités d'un corps de nombres.

Les procédés de calcul de ce rang sont basés sur les propriétés des courbes elliptiques

Il existe des courbes elliptiques de rang r(E) =0, 1, 2,…

Plusieurs auteurs se sont intéressés à la détermination du rang des courbes elliptiques

Citons quelques résultats.

(1) WIMAN a trouvé des courbes elliptiques de ranq $r(E) \geq 4$,

d'équation de Weierstrass : E : $y^2 + 351y = x^3 - 63x^2 + 56x + 22$ et r(E) =6.

Dans Ada Aushética 77 (1948) 281-320

(2) PENNEY et POMERANCE ont trouvé trois courbes elliptiques de rang $r(E) \geq 7$

Ce sont les courbes d'équation de Weierstrass

$y^2 = x^3 + ax + bx \in IQ[x]$ avec $a^2 - 4b$ non carré

pour $a = 1692602,\ a = 2843738$ et $a = 2877338$

$b = -3 \times 5 \times 11 \times 13 \times 17 \times 19 \times 23 \times 31 \times 37$

Math Comp, 29 (1975) 968-967 , classification AMS =10 B 10, 14G25 et 14H30

(3) MESTRE a trouvé une courbe elliptique de rang $r(E) \geq 12$,

d'équation de Weierstrass

$E : y^2 - 246xy + 36599029y = x^3 - 89199x^2 - 19339780x - 36239244$

CRAS n^0 295 – (1982) 643 – 644

(4) BRUMER et KAMMER ont décrit des algorithmes pour obtenir des bornes de rang de courbes elliptiques E (IQ) dans "the rank of Elliptic Curves " Invention- Math. J. 44 (1977) 715 – 743.

Rang de courbes elliptiques

Ils ont obtenu trois courbes elliptiques d'équations de Weierstrass

$E_1 : y^2 + y = x^3 - 7x + 6,\ \Delta(E_1) = 5077,$ et $r(E_1) \geq 4$

$E_2 : y^2 + 8xy + 11y = x^3 + 2x^2 - 3x;\ \Delta(E_2) = -953243$ et $r(E_2) \geq 4$

$E_3 : y^2 + 14xy + 29y = x^3 + 2x^2 - 15x;\ \Delta(E_3) = 17785971$ et $r(E_3) = 5$

(5) RUBIN et SILVERBERG ont étudié les rangs de la famille de courbes elliptiques d'équation de Weierstrass :

$E(a,b) : y^2 = x^3 + ax + b \in Q[x,y],\ \Delta(E) = -16(4a^3 + 27b^2) \neq 0$

Ils ont utilisé la fonction L(E,s) de Hasse – Weil et la conjecture de Birch et Swinnerton-Dyer :

Dans Bulletin of the American Math – Soc-39- (2002) - 455-474.

La série L(E,s) de Hasse-Weil d'une courbe elliptique E admet en s = 1 un zéro d'ordre égal au rang r(E) de la courbe elliptique E ; cette série est égale au produit eulérien :

$$L_E(s) = \prod_{p \text{ divise } \Delta(E)} (1 - t_p p^{-s})^{-1} \prod_{p \text{ ne divise pas } \Delta(E)} (1 - t_p p^{-s} + p^{1-2s})^{-1}$$

où $t_p = 1+p-A_p$, A_p est le nombre de points de la courbe E modulo p et $t_p = 0$, 1 ou -1 selon [18 -1] VIII -8-9

L'ordre r est le rang analytique $r_{ana}(E)$

(6) WADA a étudié le rang r(E) de la courbe elliptique E : $y^2 = x^3 - (1513)^2 x$ dans ″Proc. Jap. Acad. 72 série A (1996) 34-35.

En utilisant la méthode exposée par Tate – Silverman dans ″Rational Points on elliptic curves – Springer (1992) , WADA considère des équations diophantiennes liées à la

Rang de courbes elliptiques

décomposition $1513=17 \times 89$ de la forme $dX^4 + d'X^4 = Z^2$ pour d = 1513, 17, 89 et $d'=4, 4\times17, 4\times89$.

Il a montré que le rang r(E) = 2

(7) BUHLER, GROSS ET ZAGIER ont montré que la courbe elliptique d'équation :

$$E : y^2 = 4x^3 - 28x + 25$$

a un rang égal à r(E) = 3

Pour cela ils ont utilisé la conjecture Birch-Swinnerton-Dyer et calculé la valeur L(E, 1)

Math. Comp. Vol 44 (avril 1985) p 473-481. Classification -AMS =14K07, 14G10.

Chapitre III Calcul des points entiers sur une courbe elliptique

1- Entiers algébriques d'un corps de nombres

Les points entiers sur une courbe elliptique E sur le corps Q sont les points P = (x, y) du groupe de Mordell-Weil E (IQ) de coordonnées x, y dans l'anneau IZ.

$$y^2 + a_1 x y + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \in \text{IZ}[\text{x}, \text{y}] \qquad (1)$$

Ces coordonnées sont les racines de l'équation diophantienne à deux inconnues :

$$y^2 + a_1 x y + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \in \text{IZ}[\text{x}, \text{y}] \qquad (1)$$

Les solutions de l'équation diophantienne

$$f(x) = x^n + a_1 x^{n-1} + \ldots + a_n \in IZ[x]$$

s'obtiennent avec le :

Théorème 1 : *Toute solution de l'équation diophantienne f(x) = 0 est un diviseur du terme constant* a_n

□

Il en résulte une méthode de calcul des points entiers $P = (x, y) \in E(Q)$

L'équation de Weierstrass (1) est mise sous la forme

$$f(x, y) = x^3 + a_2 x^2 + a_4 x + a_6 - y^2 - a_1 x y - a_3 y \in IZ[x, y].$$

A chaque valeur $y = t \in$ IZ correspond le polynôme f (x, t) = g (x) cubique en x, paramétrique en t

$$g(x) = x^3 + a_2 x^2 + (a_4 - a_1 t) x + a_6 - t^2 - a_3 t ;$$

le cœfficient $a_6 - t^2 - a_3 t$ admet un nombre fini de diviseurs $d_1, d_2, \ldots, d_s$.

On teste les valeurs $g(d_1), \ldots, g(d_s)$ pour obtenir les solutions de l'équation diophantienne g (x) = 0. Il en résulte un nombre fini de solutions x.

Exemple 1

$$E : y^2 + 5 x y - 2 y = x^3 - 4 x^2 + 7 \in IZ[x, y]$$

Entiers algébriques d'un corps de nombres

Alors $g(x) = x^3 - 4x^2 - 5tx + 7 + 2t - t^2 \in IZ[x]$

Pour t = 0, $g(x) = x^3 - 4x^2 + 7$

les diviseurs de 7 sont $d = \pm 1, \pm 7$

Parmi les valeurs g (d) il n'y a pas g (d) = 0. Donc pas de points entiers

Pour t = 1, $g(x) = x^3 - 4x^2 - 5x + 8 \in IZ[x]$,

les diviseurs du terme constant sont $d = \pm 1, \pm 2, \pm 4$ et ± 8.

Après calcul j'obtiens g (d) = 0 pour d = 1 et g (d) $\neq 0$ pour les autres diviseurs d,

il en résulte le point entier P = (1 , 1).

Pour les grandes valeurs de t > 1000 il faut l'aide d'un logiciel de calcul.

Lorsque le corps de base de la courbe elliptique E est un corps de nombres, les entiers de K sont les entiers algébriques de K. C'est la théorie Algébrique des Nombres qui fournit les propriétés de ces entiers.

Références : Samuel, Weil, Lang.

Par définition, un entier algébrique est une racine d'un polynôme unitaire

$$f(x) = x^n + a_1 x^{n-1} + \ldots + a_n \in IZ[x]$$

Les entiers algébriques forment un IZ-module A (K) libre de type fini selon Dedekind, ce IZ-module a une structure d'anneau.

Les entiers des corps quadratiques $K = Q(\sqrt{d})$, d entier rationnel sans facteur carré : $d = \pm 1, \pm 2, \pm 3$ et ± 5,.....sont selon

Borevich et Shafarevich (Théorie des Nombres – Edition- Gautier Villard Paris), décrit par le

Calcul des points entiers des courbes elliptiques sur un corps quadratique

Théorème 2 : *Les entiers d'un corps quadratique K = Q ($\sqrt{d}$) forment un IZ-module libre de rang 2 et de base {1, $\sqrt{d}$ } pour d ≡ 2, 3 mod 4 et { 1, $\frac{1}{2}(1 \pm \sqrt{d})$ } pour d ≡1 mod 4*

□

Les entiers algébriques quadratiques sont de la forme x =a + b $\sqrt{d}$ avec a, b ∈ IZ pour d ≡ 2, 3 mod 4 et x = $\frac{a+b\sqrt{d}}{2}$ avec a, b ∈ IZ de même parité pour d ≡1 mod 4

2 Calcul des points entiers des courbes elliptiques sur un corps quadratique

La détermination des points entiers des courbes elliptiques E sur le corps quadratique K = Q ($\sqrt{d}$) nécessite un logiciel particulier mis au point par des théoriciens des nombres

Les points entiers du groupe E(Q) sont determinés par la proposition 5.

Exemple 1 : soit la courbe elliptique E_1 d'équation de Weierstrass

E_1: $y^2 = x^3 - 3x + 8 \in Q[x, y]$

Alors $4A^3 + 27B^2 = 60 \times 27$

Cette courbe admet l'axe Ox comme axe de symétrie.

Soit un point P = (x, y) qui n'est pas de 2-torsion.

Alors y^2 divise 60×27

Les valeurs possibles sont $y^2 = 4, 9$ et 4×9.

Il en résulte les ordonnées entières possibles $y = \pm 2, \pm 3, \pm 6$

Pour $y^2 = 4$, j'obtiens l'équation diophantienne $x^3 - 3x + 4 = 0$, elle n'admet pas de solution.

Pour $y^2 = 9$, j'obtiens l'équation diophantienne $x^3 - 3x - 1 = 0$ elle n'admet pas de solution.

Calcul des points entiers des courbes elliptiques sur un corps quadratique

Pour $y^2 = 36$ j'obtiens l'équation diophantienne $x^3 - 3x - 28 = 0$ elle n'admet pas de solution.

Donc cette courbe n'a pas de points entiers.

Exemple 2 : soit la courbe elliptique E_2 d'équation de Weierstrass

$E_2: y^2 = x^3 - 6x + 4 \in Q[x, y]$

Alors $4A^3 + 27B^2 = -432 = -3^3 \times 2^4$

Soit un point P = (x , y) qui n'est pas de 2-torsion

Alors y^2 divise $3^2 \times 2^4$

Les valeurs possibles sont $y^2 = 4, 9, 16, 4\times9$ et 12^2

Il en résulte les ordonnées entières possibles $y = \pm 2, \pm 3, \pm 4, \pm 6, \pm 12$.

Pour $y^2 = 4$, j'obtiens l'équation diophantienne $x^3 - 6x = 0$, x = 0 est une solution entière.

Il y a deux points entiers $(0, \pm 2)$.

Pour $y^2 = 9$, j'obtiens l'équation diophantienne $x^3 - 6x - 5 = 0$, x = -1 est une solution entière. Cela implique deux points entiers $(-1, \pm 3)$.

Pour $y^2 = 16$, j'obtiens l'équation diophantienne $x^3 - 6x - 12 = 0$, elle n'admet pas de solution.

Pour $y^2 = 36$, j'obtiens l'équation diophantienne $x^3 - 6x - 32 = 0$, elle n'admet pas de solution.

Pour $y^2 = 24$, j'obtiens l'équation diophantienne $x^3 - 6x - 20 = 0$, elle n'admet pas de solution

Cette courbe admet quatre points entiers $(0 , \pm 2)$ et $(-1, \pm 3)$.

Il existe d'autres méthodes de calcul des points entiers d'une courbe elliptique.

Calcul des points entiers des courbes elliptiques sur un corps quadratique

Je choisis celle de Don-Zagier [23] qui traite des courbes elliptiques ayant un seul point de 2-torsion

Exemple 1 : Soit la courbe elliptique d'équation de Weierstrass :

$$E_1 : \quad y^2 = x^3 + 96\ x + 605 = f(x) \qquad (1)$$

Cette courbe admet l'axe Ox comme axe de symétrie.

Je calcule les invariants de E_1

$b_2 = 0$; $b_4 = 192$; $b_6 = 2420$; $b_8 = -9216$; $\Delta(E_1) = -16\,(4A^3 + 27B^2) = -16 \times 3^7 \times 17 \times 19^2$

Donc la courbe E_1 coupe l'axe Ox en un seul point (d'après la théorie de classification des courbes elliptiques).

Dans le corps Q, l'équation diophantienne f (x) = 0 admet une solution x = -5

Il en résulte la factorisation

$$f(x) = (x+5)(x^2 - 5x + 121) = (x+5)\left(x - \frac{5+3\sqrt{-51}}{2}\right)\left(x - \frac{5-3\sqrt{-51}}{2}\right) \in Q(\sqrt{-51})[x]$$

En utilisant les formules de Cassels j'obtiens les coordonnées du point $2P = (x_{2P}, y_{2P})$

$$\begin{cases} x_{2P} = \dfrac{x^4 - 192x^2 - 464640x + 9216}{(2y)^2} \\ y_{2P} = \dfrac{x^6 + 480x^5 + 12100x^3 - 46080x^2 - 232320x - 3812936}{(2y)^3} \end{cases} \qquad (2)$$

pour le point P de coordonnées P = (x, y)

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

$$2P = 0_E = (\infty, \infty) \qquad (3)$$

Calcul des points entiers des courbes elliptiques

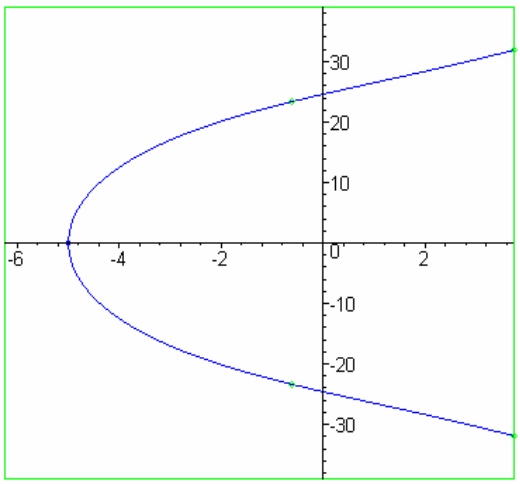
sur un corps quadratique

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

$$y = 0 \qquad (4)$$

Les égalités (1) et (4) impliquent trois points de 2-torsion, $T_1 = (-5, 0)$,

$T_2 = (\frac{5+3\sqrt{-51}}{2}, 0)$ et $T_3 = (\frac{5-3\sqrt{-51}}{2}, 0)$. Le point T_1 à coordonnées dans IZ et les points T_2 et T_3 à coordonnées entières dans le corps quadratique $Q(\sqrt{-51})$. La congruence $-51 \equiv 1 \bmod 4$ implique que les nombres $\frac{5 \pm 3\sqrt{-51}}{2}$ sont des entiers dans le corps quadratique $Q(\sqrt{-51})$.



Courbe tracée avec le logiciel « MAPLE 9

Exemple 2

$E_2 : y^2 = x^3 - 15x - 18 = f(x)$

Cette courbe admet l'axe Ox comme axe de symétrie.

Calcul des points entiers des courbes elliptiques

sur un corps quadratique

Je calcule les invariants de E_2

$b_2 = 0$; $b_4 = -30$; $b_6 = -72$; $b_8 = -225$; $\Delta(E_2) = -16\,(4A^3 + 27B^2) = 11 \times 16^2 \times 27$

Donc la courbe E_2 coupe l'axe Ox en trois points (d'après la théorie de classification des courbes elliptiques).

Dans le corps Q, l'équation diophantienne f (x) = 0 admet une solution x = -3

Il en résulte la factorisation

$$y^2 = f(x) = (x+3)(x^2-3x-6)$$
$$= (x+3)\left(x - \frac{3-\sqrt{33}}{2}\right)\left(x - \frac{3+\sqrt{33}}{2}\right) \in Q(\sqrt{33})[x] \qquad (5)$$

En utilisant les formules de Cassels j'obtiens les coordonnées du point $2P = (x_{2P}, y_{2P})$

$$\begin{cases} x_{2P} = \dfrac{x^4 + 30x^2 - 4860x + 225}{(2y)^2} \\ y_{2P} = \dfrac{x^6 - 75x^5 - 360x^3 - 1125x^2 - 1080x + 783}{(2y)^3} \end{cases} \qquad (6)$$

Pour le point P de coordonnées P = (x, y)

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

$$2P = 0_E = (\infty, \infty) \qquad (7)$$

Les formules (6) et (7) impliquent l'ordonnée du point P est

$$y = 0$$

Les égalités (5) et (7) impliquent trois points de 2-torsion, $T_1 = (-3, 0)$, $T_2 = \left(\frac{3+\sqrt{33}}{2}, 0\right)$ et $T_3 = \left(\frac{3-\sqrt{33}}{2}, 0\right)$. Le point T_1 à coordonnées dans IZ et les points T_2 et T_3 à coordonnées entières dans le corps quadratique $Q(\sqrt{33})$. La congruence $33 \equiv 1 \bmod 4$ implique que les nombres $\frac{3 \pm \sqrt{33}}{2}$ sont des entiers dans le corps quadratique $Q(\sqrt{33})$.

Calcul des points entiers des courbes elliptiques sur un corps quadratique

avec la proposition 5, j'obtiens y^2 divise $11 \times 27 \times 11$

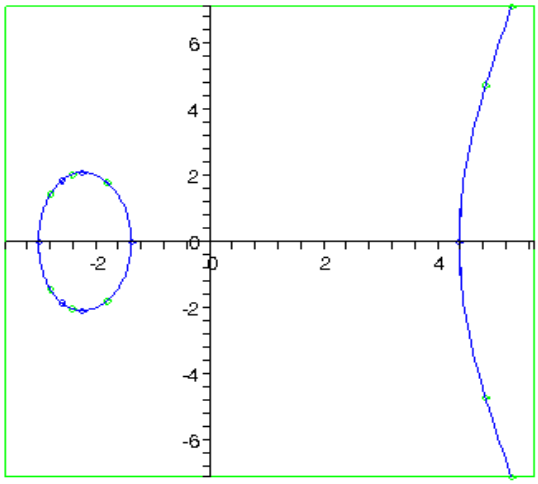
il en résulte une solution x = - 2 pour $y^2 = 4$

J'obtiens deux points de la courbe E_2 $R_{1,2} = (-2, \pm 2)$

Avec la règle géométrique des trois points colinéaires j'obtiens $2R_1 = (\frac{-55}{16}, \frac{187}{64})$

et $2R_2 = (\frac{73}{16}, \frac{-133}{64})$

ce qui implique que les deux points R_1 et R_2 ne sont pas de 2-torsion



Courbe tracée avec le logiciel « MAPLE 9

Exemple 3

$E_3 : y^2 = x^3 + 7x^2 + 17x + 14 = f(x)$

Cette courbe admet l'axe Ox comme axe de symétrie.

Je calcule les invariants de E_3

$b_2 = 28$; $b_4 = 34$; $b_6 = 56$; $b_8 = 103$; $\Delta(E_3) = -48$

Calcul des points entiers des courbes elliptiques

sur un corps quadratique

Donc la courbe E_3 coupe l'axe Ox en un seul point (d'après la théorie de classification des courbes elliptiques).

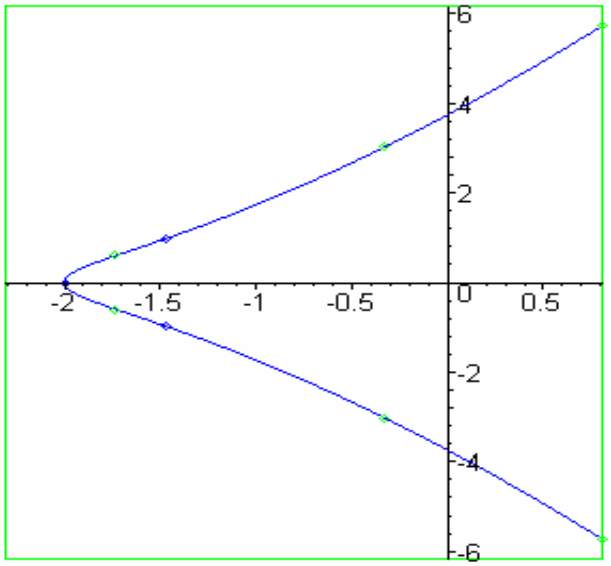
Dans le corps Q, l'équation diophantienne f (x) = 0 admet une solution x = -2

Il en résulte la factorisation

$y^2 = f(x) = (x+2)(x^2+5x+7)$

$= (x + 2)\left(x - \frac{-5-\sqrt{-3}}{2}\right)\left(x - \frac{-5+\sqrt{-3}}{2}\right) \in Q(\sqrt{-3})[x]$

La courbe E_3 coupe l'axe Ox en trois points de 2-torsion $T_1 = (-2, 0)$, $T_2 = \left(\frac{-5-\sqrt{-3}}{2}, 0\right)$ et $T_3 = \left(\frac{-5+\sqrt{-3}}{2}, 0\right)$, le point T_1 à coordonnées dans IZ et les points T_2 et T_3 à coordonnées entières dans le corps quadratique $Q(\sqrt{-3})$. La congruence $-3 \equiv 1 \bmod 4$ implique que les nombres $\frac{-5 \pm \sqrt{-3}}{2}$ sont des entiers dans le corps quadratique $Q(\sqrt{-3})$.



Courbe tracée avec le logiciel « MAPLE 9

3 - Equation des S-unités [17]

Les points entiers d'une courbe elliptique E sur le corps Q sont déterminés avec les équations diophantiennes.

La résolution de ces équations a été obtenue pour les équations de Pythagore et les équations $x^n + y^n = z^n$ de Fermat.

Pour les autres types, il y a des théorèmes d'approximation du nombre de solutions.

Un corps de nombres K possède des valuations. La théorie des valuations se trouve dans les ouvrages de théorie des nombres (Lang, Artin, Hasse,…)

Définition 1 *Une valuation d'un corps K est une fonction* $v : K \to IR^+$

qui satisfait les axiomes

(Val 1) $v(x) \geq 0$ *pour tout* $x \in K$ *et* $v(x) = 0$ *si et seulement si* $x = 0$

(Val 2) $v(x\,y) = v(x)\,v(y)$ *pour tous* $x, y \in K$

(Val 3) $v(x+y) \leq v(x) + v(y)$ *pour tous* $x, y \in K$

Exemples

1) Valeur absolue sur le corps IR des nombres réels

$|x| = x$ si $x > 0$ et $|x| = -x$ si $x < 0$

2) Valuation p-adique associée à un nombre premier p du corps Q

Pour $x = p^r \frac{a}{b}$ a, b $\in$ IZ et ab premier à p, $v_p(x) = \frac{1}{p^r}$

Les valuations du corps K sont classifiées en deux classes, les valuations archimédiennes et les valuations non archimédiennes suivant l'axiome (Val 3)

Définition 2 *une valuation* $v : K \to IR^+$ *est non archimédienne si elle satisfait*

$v(x+y) \leq max\,(v(x), v(y))$

Equation des S-unités

Les valuations non archimédiennes possèdent d'autres propriétés :

Anneaux de valuations v-idéal maximal, groupe des v-unités, corps résiduel.

Pour la recherche des entiers il y a la méthode des S- unités pour toute partie S de l'ensemble M des valuations d'un corps K avec la théorie des valuations d'une partie S de l'ensemble M des valuations de K. On lui associe des S-entiers et des S-unités.

Selon Silverman (IX –paragraphe 4) l'équation des S-unités d'une courbe algébrique plane est de la forme ax + by = 1. Ses solutions sont précisées par la :

Proposition 1 (Théorème IX - 4 -1 – [17])

Soit une partie S de l'ensemble M_K *des valuations d'un corps K et deux nombres non nuls a et b du corps K. Alors l'équation ax + by = 1 admet seulement un nombre fini de solutions x, y telles que*

v(x) = v(y) = 1 pour toute valuation v dans l'ensemble S.

□

L'application de cette proposition nécessite la connaissance des nombres transcendants (exemple de Gelfond : $2^{\sqrt{2}}$ est transcendant), d'équations logarithmiques de la forme $a_1 \log b_1 + a_2 \log b_2 + \ldots + a_n \log b_n \neq 0$ et de résultat de Baker, Evertse, Siegel .

L'étude des S-unités d'un corps sera développée dans une recherche ultérieure.

REFERENCES

[1] ARTIN: « Algebraic Number and Algebraic Functions » -Gordon and Breach - sciences Publishers; New York; (1960).

[2] CASSELS: « Diophantine Equations with Special Reference to Elliptic Curves »- Journal London Mathematical Society - 41 (1966) 193-291.

[3] HARVEY COHN: « A classical invitation to Algebraic Numbers and class Fields » -Springer Verlag -(1978)

[4] FULTON: « Algebraic Curves »- Benjamin- New York (1969).

[5] J. GEBEL, A. PETHO and H. G. ZIMMER: «Computing integral points on elliptic curves» - Acta Arethmetica LXVIII. 2 (1994) 171-192

[6] HARTSHORNE: « Algebraic Geometry »- GTM 52-Springer (1983).
Classification: 14 A 10 – 14 Fxx – 14Hxx – 14 Ixx.

[7] HUSEMOLLER: « Elliptic Curves » -G.T.M 111 Springer (1987).

[8] IYANAGA: « The Theory of Numbers » -North Holland Pub. Company-Amsterdam (1975).

[9] KOSTRIKIN: « Introduction à l'Algèbre » - Ed. Mir- Moscou- 2eme édition (1986).

[10] LANG: (1) « Algebra » - 2eme édition, Addison Wesley Publishing Company, Inc, Reading, Massachusetts, New York (1984).
(2) « Elliptic Curves – Diophantine Analysis » - Springer Verlag (1978) - Classification AMS = 10 B 45 – 10 F 99 -14 G 25 – 14 H 25.
(3) « Algebraic Number Theory » - Addition – Wesley (1970).
(4) « Cyclotomic Fields »- GTM 59 – Springer.

[11] KOBLITZ: (1) « Introduction to Elliptic Curves and Modular Forms » -2eme édition GTM97. Springer (1984)
(2) « A course in Number Theory and Cryptographiy » - 2eme édition GTM 114-Springer.

[12] MAZUR: (1) "Modular curves and the Eisenstein ideal " - IHES Publ. Math. 47. (1977), 33-186
(2) « Rational points on Modular Curves » - LNM. n 601 (1977) 107 – 147.

[13] NERON: « Quasi Fonctions et Hauteurs sur les Variétés Abéliennes » - Annals of Mathematics 82 (1965), 249-331.

[14] RUBIN: « Elliptic Curves with Complex Multiplication and the Conjecture of Birch and Swinnerton » – Dyer – Inventions Mathématique. 64 (1981) 455 – 470.

[15] SERRE: (1) « Géométrie Algébrique et Géométrie Analytique »- Ann. Inst. Fourier 6 (1956) – 1 – 42.
(2) « Propriétés galoisiennes des points d'ordre fini des courbes elliptiques »

- Inventions Mathématiques 15 (1972), 259-331.

[16] SHAFAREVICH: (1) « Basic Algebraic Geometry » - Springer Verlag (1977).
(2) « Algebraic I»- Mir (1986)-Springer (1987).
Classification AMS = 12 – xx, 20 – xx.

[17] SILVERMAN: (1) « The Arithmetic of Elliptic Curves »- GTM 106 – Springer (1986).
Classification AMS = 1401, 14G 99, 14H 05, 14 K 15.
(2) « Lower Bounds for the canonical height on Elliptic Curves » - Duke Math- J .48 (1981). 633-648.
(3) « The Difference between the Weil Height and the Canonical Height on Elliptic Curves » - Math. Comp. 35 (1990) 723-743.
Classification = 11G 05, 11 Y 50

[18] SHIMURA: « Introduction to the Arithmetic Theory of Automorphic Functions »
- Princeton University Press -(1971).

[19] TATE: « The Arithmetic of Elliptic Curves »- Invention- Mathematique 23 (1974) 179-206.

[20] VELU: « Isogénies entre Courbes Elliptiques »- C.R.A.S. Paris (1971) 238-241.

[21] WEIL : (1) « Sur un théorème de Mordell »- Bull. Sci. Math. 54 (1930).

[22] WEISS: « Algebraic Number Theory » - Mc Graw – Hill - New York (1964).

[23] – D. ZAGIER: « Large integral points on elliptic curves» -Math. Comp. 48 (1987), 425-436.

[24] ZIMMER: (1) « On the Difference of the Weil Height and the Neron-Tate Height»- Math. Zeit 147 (1976) 35-51.
(2) « **On Manin's conditional algorithm**»- Bull. Soc. Math. France Mém.49-50 (1977), 211-224 **.**

Université des Sciences et de la Technologie
Houari Boumediene

Faculté de Mathématiques
Laboratoire d'Algèbre et Théorie des Nombres

Calcul des points entiers sur une Courbe Elliptique *

Présentée par :

M^elle SABRI Farida **

Résumé :

Ma thèse a pour objectif les méthodes de calcul des points entiers sur une courbe elliptique. Elle est basée sur un article de Gebel et Zimmer.

J'ai indiqué des notions indispensables de la théorie arithmétique des courbes elliptiques.

J'ai établi la structure algébrique de l'ensemble E(K) des points K-rationnels des courbes elliptiques : c'est le groupe de Mordell-Weil.

J'ai choisi la méthode de Don-Zagier qui traite des courbes elliptiques ayant un seul point de 2-torsion pour les points entiers.

J'ai utilisé les équations diophantiennes, les entiers algébriques des corps quadratiques et l'équation des S-unités.

*thèse de Magister
**Directeur de thèse : Mr M.ZITOUNI Professeur à l'U.S.T.H.B