REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE DES SCIENCES ET DE LA TECHNOLOGIE
U.S.T.H.B D'ALGER – BAB EZZOUAR

Faculté des sciences (Mathématiques)
Département d'Algèbre et Théorie des nombres

Thèse de magister

Conducteur de courbes elliptiques ayant un point d'ordre 2

Par :
M^me^ BOUDOUH LEILA

Soutenue le : / / 2001
Devant le Jury composé de :

M^r^ BEBBOUCHI Rachid , Professeur à l'USTHB	Président
M^r^ ZITOUNI Mohamed , Professeur à l'USTHB	Rapporteur
M^r^ BETINA Kamel , Professeur à l'USTHB	Examinateur
M^r^ KESSI Arezki , Maître de conférences à l'USTHB	Examinateur

A mes parents

A mon mari et ma fille : Ahle

A mes frères et mes soeurs

A Mohamed et mes copines

A mes enseignants

Remerciments

Ma gratitude

A monsieur Zitouni Mohamed mon encadreur pour l'aide , le soutien et les orientations qu'il m'a apporté afin d'arriver à ce résultat .

Mes remerciments

A monsieur Bebbouchi Rachid d'avoir accepter de présider le Jury .

A messieurs Betina Kamel , Kessi Arezki d'avoir accepter d'être membres du Jury .

Table des matières

Introduction

En géométrie algébrique , les courbes de genre 1 sont les cubiques planes et les intersections planes de surfaces quadriques dans l'espace à 3 dimensions .

Ces courbes algébriques sont appelées dans la littérature mathématique "courbes elliptiques" . Une courbe elliptique est une cubique plane munie d'une structure de courbe algébrique , projective , lisse , de genre 1 , irréductible et avec un point O_E de base qui est le point à l'infini .
Plusieurs auteurs (T.HADANO , A.P.OGG…) ont prouvé l'existence de courbes elliptiques ayant un point P d'ordre n pour n = 1,…10,12 .
Pour démontrer l'existence de courbes elliptiques E/Q ayant un point rationnel d'ordre 2 et de conducteur produit de deux nombres premiers , on utilise la méthode employée par A.P.OGG. Cette méthode est basée sur la résolution de certaines équations diophantiennes .

Dans le chapitre 1 , on rappelle quelques points de base pour l'étude des courbes elliptiques équations de WEIERSTRASS , invariants arithmétiques , points singuliers , loi de groupe abélien et groupe de MORDELL-WEIL , homomorphismes .

Dans le chapitre 2 , on rappelle certaines définitions et propriétés des valuations sur un corps , définitions et classification des réductions d'une courbe elliptique , et quelques aspects de la théorie du groupe modulaire SL(2,9) et des formes modulaires .

Dans le chapitre 3 , on donne la notion de conducteur , on montre qu'une courbe elliptique E/Q de conducteur $N(E) = 2^n \times 3$ possède un point d'ordre 2 , cela permet de déterminer une famille de courbes elliptiques E/Q de conducteur $N(E) = 2^n \times 3$ en utilisant la résolution d'équations diophantiennes . On termine la thèse par la démonstration de l'inexistence de courbe elliptique E/Q de conducteur $N(E) = 10$.

Chapitre 1

Quelques notions de base sur les courbes elliptiques

1-Introduction :

En géométrie algébrique , les courbes de genre 0 sont les lignes et les coniques du plan ; les courbes de genre 1 sont les cubiques planes lisses et les intersections planes de surfaces quadriques dans l'espace à 3 dimensions .

Ces courbes algébriques de genre 1 sont appelées "courbes elliptiques" dans la littérature mathématique .

Une courbe elliptique peut être munie d'autres structures algébriques :

Une structure de variété abélienne de dimension 1 ;

Une structure de courbe algébrique , projective , lisse , irréductible , de genre 1 et avec un point O_E de base qui est le point à l'infini .

Dans ce chapitre nous exposerons quelques points de base pour l'étude des courbes elliptiques : équations de WEIERSTRASS , invariants arithmétiques , points singuliers , loi de groupe abélien et groupe de MORDELL-WEIL , homomorphismes et réductions .

Ces courbes elliptiques sont définies sur un corps commutatif K , qui est global ou local.

Chapitre 2

Réduction des courbes elliptiques ; groupe modulaire

L'étude de certaines propriétés des courbes elliptiques comme les réductions , les hauteurs , le rang , nécéssite la connaissance d'une partie de la théorie des valuations . Chaque ouvrage de théorie des nombres contient un exposé partiel de cette théorie (cf. S. Lang , E.Weiss , H.Hasse , I.Iyanaga , E.Artin , J.T .Tate , N.Bourbaki , …).

1-Valuations sur un corps :

La valeur absolue ordinaire sur le corps 3 , notée $|\,.\,|$, égale à $|x|=\max\{x,-x\}$ satisfait aux 3 propriétés suivantes des valuations :

$|x|>0$ et $|x|=0$ équivaut à $x=0$;

$|xy|=|x||y|$ pour tous réèls x et y ;

$|x+y|<|x|+|y|$, dite inégalité triangulaire .

Cette notion de valeur absolue sur 3 est prolongée à un corps K par la :

Définition10 :

On appelle valeur absolue sur un corps K toute fonction réèlle :

Chapitre 3

Courbes elliptiques E/Q de conducteurs ayant deux facteurs premiers

1-Notion de conducteur :

Soit une courbe elliptique E/Θ d'équation de WEIERSTRASS :

E/Θ : $y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$;
(1)

et le point neutre $O_E = (\infty,\infty)$ du groupe de MORDELL-WEIL E(Θ) . (2)

Définition 28 :

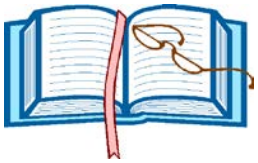
L'équation (1) est minimale en un nombre premier p si chaque coefficient a_i est entier en p et si l'ordre du discriminant Δ(E) en p est minimal dans l'ensemble des valeurs possibles Δ(E).

Puisque l'anneau 9 des entiers du corps Θ est principal , il existe une équation de forme (1) minimale en tout nombre premier du corps Θ.

C'est ce qu'on appelle une équation minimale globale de E/Θ .

On réduit la courbe E/Θ d'équation minimale modulo p ; soit ℵ la courbe réduite modulo p.

Bibliographie



[1] B.J.BIRCH and H.P.F.SWINNERTON-DYER ; Notes on elliptic curves , Crelles J .212 (1963) p 7-25.

[2] J.W.S.CASSELS : Diophantine equations with special references to Elliptic Curves, Jour. Lond.Math.Soc. 41 (1966) p 193-291.

[3] T.HADANO : On the conductor of an Elliptic Curve with a rational point of order two , Nagoya.Math.Jour.Vol 53 (1974) p 199-210.

[4] S.LANG : Variétés abéliennes , N.Y, 1959.

[5] B.MAZUR and H.P.F.SWINNERTON-DYER : Arithmetic of Weil curves, Inv .Math 25 (1974) p 1-61.

[6] I.MIYAKI : Elliptic curves of prime power conductor with Θ-rational points of finite order, Osaka Jour. Math. 10 (1973) p 309-323.

[7] L.J.MORDELL : Diophantine equations , Acad.Press.London and N.Y. (1969).

[8] R.NERON : Modèles minimaux des variétés abéliennes sur les corps locaux et globaux. Publi.Math.I.H.E.S.N°21 (1965) p 5-125.

[9] A.P.OGG : 1) Abelian curves of small conductor .Jour.Reine Angew 226 (1967) p 204-215.

2) Abelian curves of 2-power conductor, Proc. Camb.Phil.Soc. 62 (1966) p 143-168.

3) Elliptic curves and wild ramification, Amer.J.Math 89 (1967) p 1-21.

[10] SHAFAREVICH : Basic Algebraic Geometry , Springer (1977) .

[11] G.SHIMURA : 1) The Zeta-function of an algebraic variety and automorphic functions, AMS conference on algebraic geometry, Wovds Hole (1964).

2) Introduction to the arithmetic theory of automorphic functions , Princeton U.Press. (1971).

[12] J.S.SILVERMAN : 1) The Arithmetic of Elliptic Curves, GTM 106 (1986) Springer Verlag.

2)Advanced topics in the Arithmetic of Elliptic curves, GTM 151, Springer Verlag (1994).

[13] J.VELU : 1) Courbes elliptiques sur Θ ayant bonne réduction en dehors de 11, C.R.Acad Sc.Paris , 273 (1971) p 73-75.

2) Isogénies entre courbes elliptiques , p 238-241.

[14] A.WEIL : 1) Zeta-functions and Mellin transforms, Algebraic geometry, Fata Intitute of fondamenta Rearch, Bombay (1969) p 409-426.

2) Fondations of algebraic geometry, Amer. Math.Soc. 29 (1962) , Providence.

3) Variétés abéliennes et courbes algébriques, Paris, (1948).