Point of infinite order on an elliptic curve over a quadratic field

S. ABDELALIM, A. CHILLALI, S. ELHAJJI
Laboratory of Mathematics, Computing and Application
Department of Mathematical and computer
Faculty of sciences, University of Mohamed V Agdal
BP.1014 .Rabat
MOROCCO
seddikabd@hotmail.com, chil2015@yahoo.fr

Abstract: - Let $E_{A,B}$ an elliptic curve over the quadratic field $K = \mathbb{Q}(\sqrt{d})$ given by Weierstrass equation: $Y^2Z = X^3 + AXZ^2 + BZ^3$, where A, B in K. We introduce some fundamental results of the elliptic curve $E_{A,B}$. After we create an elliptic curve $E_{A',B}$, with an element of infinite order [2,3,4].

Key-Words: - Elliptic Curves, Quadratic Fields, Infinite Order...
Subject Classification: 14Gxx, 16Lxx, 16Zxx, 11Hxx, 11Txx

1 Introduction

Let E be an elliptic curve over $\mathbb{Q}$. By Mordell's theorem, $E(\mathbb{Q})$ is a finitely generated abelian group. This means that $E(\mathbb{Q}) = E(\mathbb{Q})_{tors} \times \mathbb{Z}^r$. By Mazur's theorem, we know that $E(\mathbb{Q})_{tors}$ is one of the following 15 groups:

- $\mathbb{Z}/n\mathbb{Z}$ with $1 \le n \le 10$ or n=12,
- $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$, with $1 \le m \le 4$.

On the other hand, it is not known what values of rank r are possible for elliptic curves over $\mathbb{Q}$.

The conjecture is that a rank can be arbitrary large.

The current record is an example of elliptic curve with rank≥ 28. We introduce some important results over the ring of integers of the quadratic fields.

Definition 1. The quadratic field is any extension of degree two over the rational field $\mathbb{Q}$.

Theorem 2. All quadratic field is of the form $\mathbb{Q}(\sqrt{d})$, where d is an integer without square factor.

Proposition 3. Let $K = \mathbb{Q}(\sqrt{d})$ is a quadratic field where d is an integer without square factor.
1. If $d \equiv 2 \mod 4$ or $d \equiv 3 \mod 4$ then the integer ring of K is the set of $a + b\sqrt{d}$ where $a, b \in \mathbb{Z}$.
2. If $d \equiv 1 \mod 4$ then the integer ring of K is the set of $\frac{1}{2}(a + b\sqrt{d})$ where $a, b \in \mathbb{Z}$ and $a \equiv b \mod 2$.

Definition 4. An elliptic curve over the quadratic field $K = \mathbb{Q}(\sqrt{d})$ is curve that is given by Weierstrass equation:

$$\boldsymbol{Y^2Z = X^3 + AXZ^2 + BZ^3},$$

where A, B in K and $27B^2 + 4A^3 \neq 0$.

2 Elliptic Curves over the quadratic field with an element of infinite order

In this section we introduce some lemmas for created an elliptic curves over quadratic field with an element of infinite order.

Let $\boldsymbol{E_{A,B}}$ an elliptic curve over the quadratic field K given by Weierstrass equation:

$Y^2Z = X^3 + AXZ^2 + BZ^3$, where A, B in K.

Lemma 1. Let $K = \mathbb{Q}(i)$, $A, B \in K$ and $P(x, y)$ an element of finite order in $E_{A,B}$.

If $(x, y) \in K^2$ then $y = 0$ or $y^2 \mid 4A^3 + 27B^2$.

Proof

Let $E_{A,B}$ an elliptic curve over the quadratic field $K = \mathbb{Q}(i)$ given by Weierstrass equation:

$y^2 = x^3 + Ax + B$, with $A, B \in \mathbb{Z}[i]$.

Let $P = (x, y) \in E_{A,B}$. Suppose that P has finite order.

If $x, y \in \mathbb{Z}[i]$, then by Lutz Nagelle Theorem [2], we have:

if $y \neq 0$ then $y^2 \mid 4A^3 + 27B^2$.

Lemma 2. Let $E_{A,B}$ an elliptic curve over the quadratic field $K = \mathbb{Q}[i]$ given by Weierstrass equation:

$y^2 = x^3 + Ax + B$, with $A, B \in \mathbb{Z}[i]$.

Then, there exists $A^{'}, B^{'} \in \mathbb{Z}[i]$ such that $|A^{'}| \geq |A|$ and $|B^{'}| \geq |B|$ which the elliptic curve $E_{A^{'},B^{'}}$ over K have a point of an infinite order.

Proof

Let $E_{A,B}$ an elliptic curve over the quadratic field $K = \mathbb{Q}[i]$ given by Weierstrass equation:

$y^2 = x^3 + Ax + B$, with $A, B \in \mathbb{Z}[i]$.

We pose:

$A^{'} = -(3|A|+1)^2$,

$B^{'} = (3|B|+3)^2$,

$x_1 = 3|A|+1$,

and $y_1 = 3|B|+3$.

We have:

$$\begin{aligned} x_1^3 + A^{'}x_1 + B^{'} &= (3|A|+1)^3 - (3|A|+1)^2 \times (3|A|+1) + (3|B|+3)^2 \\ &= (3|A|+1)^3 - (3|A|+1)^3 + (3|B|+3)^2 \\ &= (3|B|+3)^2 \\ &= y_1^2 \end{aligned}$$

It's clair that $Q = (x_1, y_1) \in E_{A^{'},B^{'}}$.

Suppose that Q has finite order, so by lemma2.1 we have:

$$y_1^2 \mid 4A^{'3} + 27B^{'2} \Rightarrow 3 \mid 4A^{'3} + 27B^{'2} \Rightarrow 3 \mid 4A^{'3} \Rightarrow 3 \mid A^{'}$$

Which is absurd because: $A^{'} = -(3|A|+1)^2$

Lemma 3. Let $K = \mathbb{Q}(\sqrt{d})$ and $E_{A,B}$ an elliptic curve over K given by Weierstrass equation:

$y^2 = x^3 + Ax + B$, with $A, B \in \mathbb{Z}[\sqrt{d}]$.

Then, there exists $A^{'}, B^{'} \in \mathbb{Z}[\sqrt{d}]$ such that $|A^{'}| \geq |A|$ and $|B^{'}| \geq |B|$ which the elliptic curve $E_{A^{'},B^{'}}$ over K have a point of an infinite order.

Proof

Let $K = \mathbb{Q}(\sqrt{d})$ and $E_{A,B}$ an elliptic curve over K given by Weierstrass equation:

$y^2 = x^3 + Ax + B$, with $A, B \in \mathbb{Z}[\sqrt{d}]$.

We suppose:

$T = sup\{|A|+1; |B|+1\}$,

$A^{'} = 2T$,

$B^{'} = 3^2T^2$,

$x_1 = \frac{1}{3}$,

and $y_1 = \frac{1+3^4T}{3^3}$.

We have:

$$\begin{aligned} x_1^3 + A^{'}x_1 + B^{'} &= \tfrac{1}{3^6} + \tfrac{2T}{3^2} + 3^2T^2 \\ &= \tfrac{1+2\times3^4\times T+3^8T^2}{3^6} \\ &= (\tfrac{1++3^4T}{3^3})^2 \\ &= y_1^2. \end{aligned}$$

Such that , $Q = (x_1, y_1) \in E_{A^{'},B^{'}}$, so by lemma2.1 we have: Q has an infinite order.

Acknowledgment

I would thank Laboratory of Mathematics, Computing and Application for his helpful comments and suggestions.

References:

[1] A. Chillali, Elliptic Curves of the Ring, International Mathematical Forum, Vol. 6, no. 31 (2011), 1501-1505.

[2] S. Abdelalim, A. Chillali, S. Elhajji, Elliptic Curve Over The Rational Filed Whit Element Of Infinite Order, International Journal of Algebra, vol. 7, no. 19, (2013), 929-933.

[3] N. Koblitz, Elliptic curve cryptosystems, Mathematics of Computation, vol. 48 (1987), 203-209.
[4] E. Lutz, Sur l'quation y2 = x3 dans les corps p-adic Math, J. Reine Angew, 1937.
[5] B. Mazur, Rational isogenies of prime degree, an appendix by D. Gold- feld,Invent. Math 1978.
[6] P. Samuel , Théorie Algébrique Des Nombres ISBN 2 7056 5589 1 deuxième Edition collection Hermann 1997.

This work was supported in part by the Laboratory of Mathematics, Computing and Application , Faculty of sciences University of Mohamed V Agdal, BP.1014 . Rabat, Morocco.

S. Abdelalim: Laboratory of Mathematics, Computing and Application, Department of Mathematical and computer, Faculty of sciences University of Mohamed V Agdal, BP.1014 . Rabat, Morocco. seddikabd@hotmail.com

A. Chillali: Department of Mathematics, USMBA, FST, FEZ, MOROCCO. chil2015@hotmail.fr

S. Elhajji: Laboratory of Mathematics, Computing and Application, Department of Mathematical and computer, Faculty of sciences University of Mohamed V Agdal, BP.1014 . Rabat, Morocco.elhajji@fsr.ac.ma