Transactions of the Nigerian Association of Mathematical Physics
Volume 17, (October – December, 2021 Issue), pp179 –182

TORSION POINTS OF ELLIPTIC CURVES OVER QUADRATIC FIELD

N. Mukhtar[1] and A. T. Imam[2]

[1]Department of Mathematics and Statistics, Nuhu Bamalli Polytechnic, Zaria, Nigeria
[2]Department of Mathematics, Ahmadu Bello University, Zaria, Nigeria

Abstract

An elliptic curve is a cubic polynomial in two variables in which there is at least one rational solution. The set of all rational solutions to an elliptic curve is known to be an abelian group which is finitely generated. In this paper, we obtained the 2 – torsion and 3 – torsion points for the family of elliptic curves of the forms $y^2 = x^3 + ax$ and $y^2 = x^3 + ax^2 + bx$ over quadratic field.

Keywords: Elliptic Curve, torsion points, Quadratic Field.

1. Introduction

An elliptic curve is a cubic polynomial in two variables in which there is at least one rational solution. An essential tool in the study of an elliptic curve E is the fact that there exists a composition law on the set $E(\mathbb{Q})$ of rational points on E, which gives $E(\mathbb{Q})$ a group structure. This was first noted in [1]. The necessary conditions for a point on an elliptic curve over the rational field $\mathbb{Q}$ to be a torsion point was established by [2, 3], the work of [4] determined a complete list of 15 possible torsion subgroups for all elliptic curves over $\mathbb{Q}$. It has shown by [5, 6] that, for a quadratic field K, the torsion subgroup $E(K)_{tors}$ of $E(K)$ is isomorphic to one of a list of 26 groups. Characterization of $(K)_{tors}$ for certain families of elliptic curves over a quadratic field K where considered by [7] and also the 2-torsion and 3-torsion of elliptic curves of the form $y^2 = x^3 + bx + a$. In particular, they pare down the list of 26 possibilities to at most seven for a curves of the form $y^2 = x^3 + a$, where a is a square of an integer. In this paper, we obtained the 2 – torsion and 3 – torsion points of an elliptic curve of the form $y^2 = x^3 + ax^2 + bx$ over a quadratic field K, by adopting the approach of [7].
In section 2, we gave the preliminaries and some basic definitions to explain the points of order 2 and order 3, while in section 3, we present our main results.

2. Preliminaries and Basic Definitions

2.1 Elliptic Curve

An elliptic curve E is a cubic curve $f(x, y) = 0$ over a field K, with at least one K-rational point (i.e., there is at least one point P on E with coordinates in K).

2.2 Torsion Points

Every point on an elliptic curve E over $\mathbb{Q}$ is one of two kinds: a point of finite order or a point of infinite order in $E(\mathbb{Q})$ [8]. For a point P to be a point of finite order means there exist a smallest positive integer n such that $nP = P + P + P + \ldots + P = \mathcal{O}$. The point $\mathcal{O}$ is at infinity which is called zero and is always counted to be relational on E. If no such n exists then P is of infinite order. In other words, P being of infinite order means you can never get the point at infinity by adding P to itself, no matter how many times you do it. This distinction between finite and infinite points leads to the following definition:

Definition 2.3 A point $P \in E(\mathbb{Q})$ is called a torsion point (or n – torsion point) if $P$is of finite order n.

The set of all torsion points of a an elliptic curve E formed a finite subgroup of $E(\mathbb{Q})$ denoted by $E(\mathbb{Q})_{tors}$, that is, $E(\mathbb{Q})_{tors} = \{P \in E(\mathbb{Q}) | \text{P has finite order}\} \subseteq E(\mathbb{Q})$. The subset $E(\mathbb{Q})_{tors}$ is a subgroup of $E(\mathbb{Q})$ called the torsion subgroup of E.

Definition 2.4: Point of Order 2

A point $P \neq \mathcal{O}$ is said to be of order 2 if $2P = \mathcal{O}$. If we write $P = (x, y)$, then $-P = (x, -y)$. The condition $2P = \mathcal{O}$ is

Corresponding Author**:** Makhtar N., Email: nuraddeenm14@gmail.com, Tel: +2348034987045, +2348061299119 (ATI)

equivalent to $P = -P$. This implies $(x, y) = (x, -y)$, which can only happen when $y = 0$. So all the points of order two must have $y = 0$.

Definition 2.5. Point of Order 3

Torsion points of order 3 are the points that satisfy $3P = \mathcal{O}$, which implies that we are looking for points satisfying $2P = -P$. This is obtained by the equation, $\Psi_3(x) = 3x^4 + 4ax^3 + 6bx^2 + 12cx + (4ac - b^2)$. This was achieved by the used of duplication formula [9].

2.4 Lutz – Nagell Theorem

The problem of finding torsion points (points of finite order) on elliptic curve E was addressed by [3] and independently by [2].

Theorem 2.4.1: (Lutz – Nagell Theorem)

Let $E: y^2 = x^3 + bx + a$ be an elliptic curve with $a, b \in \mathbb{Q}$. Then

i. Both x and y are integers, and

ii. Either $y = 0$ or $y^2 | (4a^3 + 27b^2)$.

This theorem provides us with necessary conditions for a point $P = (x, y)$ on an elliptic curve E with integer coefficient to be a torsion point in $E(\mathbb{Q})$. The theorem can also be used to obtain a complete list of all possible torsion points.

3. Main Results

3.1 Points of Order 2

Let $E: y^2 = x^3 + ax^2 + bx + c$ be an elliptic curve in Weierstrass form and that the point at infinity $\mathcal{O}$ is taken to be the zero element for the group law. Which point in our group satisfy

$2P = \mathcal{O}$, with $P \neq \mathcal{O}$?

Instead of $2P = \mathcal{O}$, it is easier to look at the equivalent condition $P = -P$. Since $-(x, y)$ is just $(x, -y)$, these are the points with $y = 0$, that is

$$P_1 = (\alpha_1, 0)\ , P_2 = (\alpha_2, 0),\ P_3 = (\alpha_3, 0)$$

where α_1, α_2 and α_3 are the roots of the cubic polynomial $f(x) = x^3 + ax^2 + bx + c$. Thus, there are at most three points of order 2. If all the three roots of $f(x)$ are real, then the graph of $f(x)$ as in figure 1

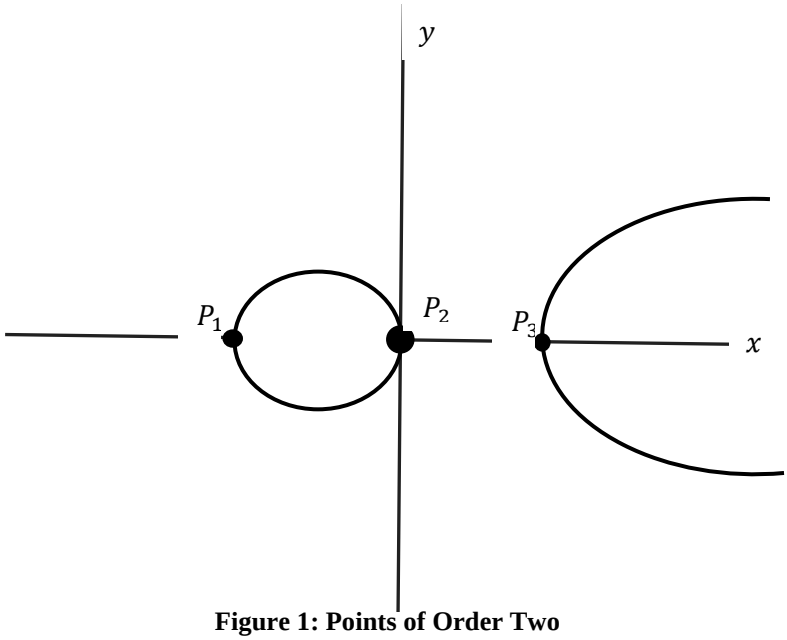

Figure 1: Points of Order Two

If we take all the points satisfying $2P = \mathcal{O}$, including $P = \mathcal{O}$, then we get the set $G = \{\mathcal{O},\ P_1,\ P_2,\ P_3\}$. It turns out that G is a group of order four, where every non-zero element is of order two. Thurs, this group G is the Klein Four Group, which is the direct product of two cyclic groups of order 2. This means that the sum of any two points $P_1,\ P_2,\ P_3$ should equal the third, which is obvious from the fact that the three points $P_1,\ P_2,$ and P_3 are collinear.

Lemma 3.1.1: A non – trivial point (x, y) on a curve $E(K): y^2 = x^3 + bx + a$, where $a, b \in K$, is a point of order two if and only if $x \in K$ satisfies $x^3 + bx + a = 0$.

i.e. $x^3 + bx + a$ was factor to identify the field over which E has 2 – torsion. In order for $E(K)_{tors}$ to contain a 2 – torsion point, there would necessarily be an element $x \in K$ such that x satisfies $x^3 + bx + a = 0$.

Theorem 3.1.2: Let $E(K)$: $y^2 = x^3 + ax^2 + bx$ be an elliptic curve. A point $(x, y) \in E(K)$ is 2 –torsion if and only if $x = 0$ or $x$is a point in K satisfying the monic polynomial $x^2 + ax + b = 0$.

Proof:

But we know that a point $(x, y) \neq \mathcal{O}$ on E is a point of order 2 $if\ and\ only\ if y = 0$

See [9]. That is, $x^3 + ax^2 + bx = 0$ if and only if $x(x^2 + ax + b) = 0$

$iff\ x = 0$ or $x^2 + ax + b = 0$.

$iff\ x = 0$ or $\frac{-a \pm \sqrt{a^2 - 4b}}{2}$

3.2 Points of Order 3

Torsion points of order 3 are the points P on an elliptic curve that satisfy $3P = \mathcal{O}$, which implies that we are looking for the points such that $2P = -P$. To find the points satisfying this condition, we use the duplication formula and set x coordinate of $2P$ equal to the x coordinate of P. This formula gives us the x value of $2P$ based on the x value of $P = (x,\ y)$. We want $2P = -P = (x, -y)$, which means the x value of $2P$ must equal to the x value of $(-P)$. We therefore have the equation

$$x = \frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4x^3 + 4ax^2 + 4bx + 4c},$$

Working out the algebra we get a simplified equation in term of x as $\psi_3(x) = 3x^4 + 4ax^3 + 6bx^2 + 12cx + (4ac - b^2) = 0$. The roots of this equation will be the x values for our points of order 3.

If $x \in \mathbb{C}$ we have 4 disticnt roots. We know they are distinct because $\psi_3(x)$ and $\psi'_3(x)$ have no common roots. If it happens that $\psi_3(x)$ and $\psi'_3(x)$ have a common root, then $f(x)$ and $f'(x)$ would have a common root, which contradict the fact that $f(x)$ is non-singular. Plugging in these 4 roots of $\psi_3(x)$ into our elliptic curve will yield a total of 8 distinct points. All together we get 9 points of order 3, the above mentioned 8 together with the point at infinity $\mathcal{O}$. There is only one commutative group of order 9 with every element having order 3, and that is the product of two cyclic groups of order 3. If we restrict $x \in \mathbb{R}$, we will always get a cyclic group of order 3. If we restrict x to being in $\mathbb{Q}$, we will either get a cyclic group of order 3 or the trivial group $\{\mathcal{O}\}$.

The same procedure that is used for torsion points of order 3 can be used to find torsion points of order higher than three. We simply need to find a way of re-writing $nP = \mathcal{O}$ that will utilize what we already know.

Lemma 3.2.1:

i. Let $E(K)$: $y^2 = x^3 + bx + a$, where $a, b \in K$. A point $(x, y) \in E(K)$ is a point of order three if and only if $x \in K$ is satisfies $3x^4 + 6bx^2 + 12ax - b^2 = 0$.

ii. Let $E(K)$: $y^2 = x^3 + a$, where $a \in K$. A point $(x, y) \in E(K)$ is a point of order three if and only if $x \in K$ is satisfies $3x^4 + 12ax = 0$. When a is a square, there will always be a point of order three on $E(\mathbb{Q})$.

Theorem 3.2.2:

(i) Let $E(K)$: $y^2 = x^3 + ax^2 + bx$, where $a, b \in K$. A point $(x, y) \in E(K)$ is a point of order three if and only if $x \in K$ satisfies $3x^4 + 4ax^3 + 6bx^2 - b^2 = 0$.

(ii) Let $E(K)$: $y^2 = x^3 + ax$, where $a \in K$. A point $(x, y) \in E(K)$ is a point of order three if and only if $x = 0$ or $x = -4a/3$.

Proof:

(i) From [9] pp 40, a point $P = (x, y) \neq \mathcal{O}$,
E: $y^2 = x^3 + ax^2 + bx + c$ is of order three if and only if x satisfies the polynomial $3x^4 + 4ax^3 + 6bx^2 + 12cx + (4ac - b^2) = 0$.
In the case of our elliptic curve $c = 0$ and so we have (x, y) is a point of order three if and only if x satisfies $3x^4 + 4ax^3 + 6bx^2 - b^2 = 0$.

(ii) If we let b and c to be all zeros from [9] we obtained that point (x, y) is a point of order three if and only if x satisfies $3x^4 + 4ax^3 = 0$. The solution to this equation are $x = 0$ and $x = -4a/3$.

Theorem 3.1.2 and 3.2.2 extends the results of [7] for the method of obtaining the 2 – torsion and 3 – torsion points of an elliptic curve quadratic field, from the family of curves of the form $y^2 = x^3 + a$ and $y^2 = x^3 + bx + a$ to that of form $y^2 = x^3 + ax$ and $y^2 = x^3 + ax^2 + bx$.

Conclusion

The results obtained from theorem 3.1.2 showed that, the 2- torsion for a family of elliptic curve of the form $y^2 = x^3 + ax^2 + bx$ occurs at $x = 0$ or $x = \frac{-a \pm \sqrt{a^2-4b}}{2}$ while theorem 3.2.2 present the method for obtaining the 3 – torsion point for the two families of elliptic curves over quadratic field.

Acknowledgement

The research term wish to thank Prof. G. U. Garba for his advice and encouragement during the research.

References

[1] Poincare, H. (1901). Sur les proprieties arithmetique des courbes algebrique. *Journal mathematics pure and applied 7*.

[2] Nagell, T. (1935). Solution de quelque problemes dans la theorie arithmetique des cubiques planes du premier genre. Wid. Akad. Skrifter Oslo I. Nr.1.(Springer).

[3] Lutz, E. (1937). Sur l'equation $y^2 = x^3 - Ax - B$ dans les corps p-adic. *Journal of Reine Angewandte Mathematik.* 177:431–466.

[4] Mazur, B. (1978). Rational isogenies of prime degree. *Inventiones Mathematicae.* 44, 129–162.

[5] Kenku, M. A. and Momose, F. (1988). Torsion points on elliptic curves defined over quadratic fields. *Nagoya mathematics Journal*, 125 – 149.

[6] Kamienny, S. (1992). Torsion points on elliptic curves and q – coefficient of modular form. *Inventiones Mathematicae Journal*, 109, 221 – 229.

[7] Jody, R. and Sophie, D. (2014). Torsion of elliptic curves over quadratic fields. *OAlib Journal*.

[8] Christian, C. (2006). Torsion points of elliptic curves over number fields. Honors thesis University of Massachusetts.

[9] Silverman, H. J. and Tate, J. (1992). Rational Points on elliptic curves (2nd. ed.). Springer – Verlag, New York.