International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

COPY RIGHT

ELSEVIER SSRN

IJIEMR Transactions, online available on 26th Dec 2022. Link :http://www.ijiemr.org/downloads.php?vol=Volume-11&issue=Issue12

10.48047/IJIEMR/V11/ISSUE 12/231

TITLE: A STUDY OF TORSION GROUPS OF MORDELL CURVES OVER CUBIC AND SEXTIC FIELD

Volume 11, ISSUE 12, Pages: 1769-1777

Paper Authors **BANDEPPA GURUNATH, DR. HOSHIYAR**

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

A STUDY OF TORSION GROUPS OF MORDELL CURVES OVER CUBIC AND SEXTIC FIELD

BANDEPPA GURUNATH, DR. HOSHIYAR

DESIGNATION-RESEARCH SCHOLAR MONAD UNIVERSITY HAPUR U.P
DESIGNATION- (ASSISTANT PROFESSOR) MONAD UNIVERSITY HAPUR U.P

ABSTRACT

One prominent area of research involves the study of additive number theory within finite abelian groups. This branch delves into questions related to representations of integers as sums of group elements, exploring topics such as the Frobenius coin problem and Goldbach-type theorems in this setting. These problems not only deepen our understanding of number theory but also have practical applications in cryptography and coding theory. Combinatorial number theory also plays a pivotal role in understanding finite abelian groups. Researchers investigate questions concerning the distribution of elements with specific properties, such as primitive roots, quadratic residues, and primitive Pythagorean triples, within these groups. This combinatorial approach often involves exploring patterns and regularities in group elements' behavior, shedding light on the intrinsic connections between algebra and combinatorics. Addressing problems in algebraic and combinatorial number theory connected to finite abelian groups is a fascinating and intricate field of mathematics that uncovers the hidden relationships between algebraic structures and combinatorial phenomena. This multidisciplinary approach has far-reaching implications across various branches of mathematics and continues to inspire new discoveries and applications.

KEYWORDS:- Torsion Groups, Mordell Curves, Cubic And Sextic Field, abelian groups, combinatorial approach.

INTRODUCTION

Definition .1: A field K in C is called number field if the dimension of K as a vector space over Q is finite. The dimension is known as the degree of K over Q and it is denoted by [K : Q].

Definition 2. An Elliptic curve E over a field K is a curve of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

where a1,...,a6 ∈ K.

We consider the set E(K) = {P = (x, y) : x, y ∈ K and E(x, y)=0} ∪ {O}, where O is the point of infinity. This set E(K) turns out to be a group under binary operation, addition, and E(K) is called the set of all K-rational points of the elliptic curve E. The group E(K) is also called the Mordell-Weil group of E over K.

Theorem 1: Let E be an elliptic curve defined over K. Then E(K) is a finitely generated abelian group.

Hence, by the structure theorem of finitely generated abelian groups, we have E(K) ∼= T ⊕ Zr, for some non-negative integer r. We call r as the rank of the elliptic curve E and T is called the torsion subgroup of E(K). Sometimes we may write T = E(K)tors.

The next topic is about all possible groups appearing as E(K)tor.

Notation 1-For an integer d ≥ 1, we define Φ (d) = {E(K)tors : K/Q is a number field of degree d and E is an elliptic curve defined over K}. For any two element A, B ∈ Φ (d), we say A ∼ B if and only if A ∼= B. Then ∼ is an equivalence relation on Φ (d) and let Φ(d) := Φ (d)/ ∼. In short, for a fixed natural number d ≥ 1, the set of all possible torsion subgroups of elliptic curves defined over number field of degree d is denoted by Φ(d).

Theorem 2. Let d ≥ 1 be an integer. Then the number of elements in Φ(d) is finite.

When we restrict elliptic curves over Q, we define the following notation in a similar way

Notation 2. When K varies over any number field of degree d and E varies over any any rational elliptic curve, then the set of all possible torsion subgroups of E(K) (up-to isomorphism) is denoted by ΦQ(d).

Note that when K = Q, we see that Φ(1) = ΦQ(1).

When K = Q, in [60], Mazur proved that

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

$$\Phi(1) = \{\mathbb{Z}/m\mathbb{Z} : 1 \leq m \leq 12, m \neq 11\} \cup \{\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z} : 1 \leq m \leq 4\}.$$

By a result of Kamienny and by another result of Kenku and Momose, it is known that

$$\Phi(2) = \{\mathbb{Z}/m\mathbb{Z} : 1 \leq m \leq 18, m \neq 17\} \cup \{\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z} : 1 \leq m \leq 6\}$$

$$\cup \{\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3m\mathbb{Z} : 1 \leq m \leq 2\} \cup \{\mathbb{Z}/4\mathbb{Z}\}.$$

Also, it has been proved that if K varies over all cubic number fields and E varies over all elliptic curves over K, then the group structures which appear infinitely often as E(K)tors are exactly the following

$$\mathbb{Z}/m\mathbb{Z}; \qquad 1 \leq m \leq 20, m \neq 17, 19$$

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}; \qquad 1 \leq n \leq 7.$$

From the above information, we can say that the set of these 25 groups is a subset of Φ(3). Moreover, in the same paper, they proved that if E varies over all rational elliptic curves, then each elements of Φ(1) occurs infinitely often as E(Q)tors. They have also mentioned that all 26 groups in Φ(2) occur infinitely often as E(K)tors, when K varies over all quadratic number fields and E varies over all elliptic curves over K.

Moreover, it has been determined that which groups of the form Z/MZ ⊕ Z/NZ occur infinitely often as torsion groups E(K)tors when K varies over all quartic number fields and E varies over all elliptic curves over K. However in general it is still unknown about the set Φ(d) for d ≥ 3.

PRELIMINARIES

3. Basics on Number field

In this section, we shall state some basics results in algebraic number theory which are useful later

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

Proposition 2. Let K be a number field and OK be the ring of integers of K. For a prime number p ∈ Z, the principal ideal can be written uniquely as a product of prime ideals. That is, pOK = Pe1 1 ⋯Per r where P1,...,Pr are prime ideals in OK and r is some integer.

Here ei is called the ramification index of Pi.

Definition 2. Let p be a prime number in Z and P be a prime ideal in OK such that POK ∩ Z = pZ. Then OK/P is a finite dimensional vector space over Z/pZ and the dimension is f = [OK/P : Z/pZ]. The number f is called the residue degree of P.

Proposition 1.3.3 *Let K be a number field and p be a prime number in $\mathbb{Z}$ such that $p\mathcal{O}_K = \mathcal{P}_1^{e_1} \cdots \mathcal{P}_r^{e_r}$ and $f_i = [\mathcal{O}_K/\mathcal{P}_i : \mathbb{Z}/p\mathbb{Z}]$, for all $i = 1, \ldots, r$. Then we have $[K : \mathbb{Q}] = \sum_{i=1}^{r} e_i f_i$.*

Notation 2. For a number field K, we denote the algebraic closure of K by K. The Galois group of K over K is denoted by Gal(K/K), where Gal(K/K) is the inverse limit of Gal(L/K) as L varies over all finite Galois extensions of K.

Basics on elliptic curves over number field

Let K be a field. We consider elliptic curves as defined in Definition 2. If char $(\overline{K}) \neq 2,$ then the substitution $y \mapsto \frac{1}{2}(y - a_1x - a_3)$ transforms E to the form

$$E : y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6,$$

where $b_2 = a_1^2 + 4a_4$, $b_4 = 2a_4 + a_1a_3$ and $b_6 = a_3^2 + 4a_6$.

Again if $char(\overline{K}) \neq 2, 3$, then the substitution $(x, y) \mapsto \left(\frac{x-3b_2}{36}, \frac{y}{108}\right)$ eliminates the x^2 term and provides the simpler equation $y^2 = x^3 - 27c_4x - 54c_6$, where $c_4 = b_2^2 - 24b_4$ and $c_6 = -b_2^3 + 36b_2b_4 - 216b_6$.

If K is a number field, then char(K)=0 and hence we, now onwards, for an elliptic curve E defined over a number field K, consider E is of the form

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

$$y^2 = x^3 + ax + b, \qquad \text{for some } a, b \in K. \tag{2}$$

For any point Q = (x, y) on the curve (2), we denote its reflection as −Q = (−x, y). For any two points Q1 and Q2 on the curve, the line joining Q1 and Q2 cuts the curve E on the third point Q3 = Q1 +Q2. We define "addition" of Q1 and Q2 by Q1 ⊕ Q2 = −Q3 which is a point on the curve. Since E(K) forms a group under the binary operation ⊕, we want to describe duplication formula explicitly.

Addtion formula

Let Q1 = (x1, y1) and Q2 = (x2, y2) be two points on the curve (2.1) and Q3 = (x3, y3) be the point Q1 + Q2 as described above, where x3 and y3 can be computed as follows.

Case 1: (x1 $\neq$ x2)

Firstly, we consider the line joining Q_1 and Q_2 which is $y = \lambda x + \nu$ with $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$ and $\nu = y_1 - \lambda x_1 = y_2 - \lambda x_2$.

This line intersects the cubic E already in two points (x1, y1) and (x2, y2). For finding the third intersecting point, we substitute y = λx + ν in the curve (1) and get $y^2 = (\lambda x + \nu)^2 = x^3 + bx + c \Leftrightarrow x^3 - \lambda x^2 + (b - 2\lambda\nu)x + (c - \nu^2) = 0$ which we can write as

$$x^3 - \lambda x^2 + (b - 2\lambda\nu)x + (c - \nu^2) = (x - x_1)(x - x_2)(x - x_3). \tag{2}$$

After equating the coefficients of the x2 term on both side, we get λ2 − a = x1 + x2 + x3 and thus

$$x_3 = \lambda^2 - x_1 - x_2, \text{ and } y_3 = \lambda x_3 + \nu. \tag{3}$$

Case 2: (x1 = x2).

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

If y2 = −y1, then we get Q1 ⊕ Q2 = O, the point at infinity. If y2 = y1, then we calculate Q1 ⊕ Q1 = 2Q2. For the curve (1), we calculate the slope of the tangent which is given by

$$\lambda = \frac{dy}{dx} = \frac{3x^2 + b}{2y}.$$

Putting the value λ in the formula (3), we get the point 2Q2. Thus, we have

$$x \text{ coordinate of } 2Q_1 := x(2Q_1) = \frac{x^4 - 2bx^2 - 8cx + b^2}{4x^3 + 4bx + 4c}. \quad 4)$$

This formula is called as the duplication formula. Similarly one can calculate the y coordinate of 2Q1 := y(2Q1)

$$= \frac{2x^6 + 4ax^5 + 10ax^4 + 40bx^3 - 10a^2x^2 - (4a^3 + 8ab)x - (2a^3 + 16b^2)}{8y^3}. \quad (5)$$

In a similar way, for an integer n ≥ 2 and for any point P of an elliptic curve E, one can calculate x(nP) and y(nP). It turns out that they are rational functions in terms of x and y.

Now, for any elliptic curve E defined over a field K and for an positive integer n, we define

$$E(K)[n] := \{P = (x, y) \in E(K) : nP = \mathcal{O}\} \cup \{\mathcal{O}\}.$$

Any element of E(K)[n] is called an n-torsion point over K (or sometimes, n-division point).

We observe that

$$E(K)_{tors} = \bigcup_{n=1}^{\infty} E(K)[n]$$

and we define

$$E[n] := E(\overline{K})[n] = \{P = (x, y) \in E(\overline{K}) : nP = \mathcal{O}\} \cup \{\mathcal{O}\},$$

where E[n] is also called the full n-torsion of E.

CONCLUSION

In our exploration of problems within algebraic and combinatorial number theory connected to finite abelian groups, we have embarked on a journey that reveals the elegance and complexity of mathematics. Through this expedition, we have gained insights into the fundamental principles governing these groups and their interactions with various mathematical concepts. In this conclusion, we shall reflect on the strategies, techniques, and broader perspectives that are essential for dealing with such problems. A structured approach is paramount when tackling problems related to finite abelian groups. The first step is to develop a solid understanding of the foundational concepts and theorems that underlie these groups. The classification theorem for finite abelian groups, attributed to mathematicians like Carl Friedrich Gauss and Ernst Eduard Kummer, plays a pivotal role in this regard. This theorem establishes that every finite abelian group can be expressed as a direct sum of cyclic groups. Armed with this knowledge, mathematicians can categorize finite abelian groups and work with them systematically. Moreover, the isomorphism theorems, such as the Fundamental Theorem of Finite Abelian Groups, offer a powerful lens through which to analyze and understand these groups' structures. This theorem provides a clear and concise way to decompose a finite abelian group into its constituent cyclic subgroups, shedding light on its inherent properties. Consequently, understanding these theorems and their implications is crucial when approaching problems connected to finite abelian groups in algebraic and combinatorial number theory.

REFERENCES

1. Pirzada, Shariefuddin & Wani, Bilal & Somasundaram, A.. (2021). On the eigenvalues of zero-divisor graph associated to finite commutative ring Z p M q N. AKCE International Journal of Graphs and Combinatorics. 18. 1-6. 10.1080/09728600.2021.1873060.

2. Nadeem, Muhammed & Ahmad, Sarfraz & Siddiqui, Muhammad & Ali, Arfan & Farahani, Mohammad & Khalaf, Abdul Jalil M.. (2021). On some applications related with algebraic structures through different well known graphs. Journal of Discrete

Mathematical Sciences and Cryptography. 24. 451-471. 10.1080/09720529.2021.1885806.

3. Iga, Kevin. (2021). Adinkras: Graphs of Clifford Algebra Representations, Supersymmetry, and Codes. Advances in Applied Clifford Algebras. 31. 10.1007/s00006-021-01181-0.

4. Mönius, Katja. (2021). Algebraic and Arithmetic Properties of Graph Spectra. 10.25972/OPUS-23085.

5. Bose, Bedanta & Das, Angsuman. (2020). Graph theoretic representation of rings of continuous functions. Filomat. 34. 3417-3428. 10.2298/FIL2010417B.

6. Pirzada, Shariefuddin & Aijaz, M. & Bhat, Imran. (2020). On zero divisor graphs of the rings Zn. Afrika Matematika. 31. 1-11. 10.1007/s13370-019-00755-3.

7. Pirzada, Shariefuddin & Bhat, Imran. (2020). On graphs associated to ring of Guassian integers and ring of integers modulo n.

8. Ural, Alattin. (2019). Ninth graders' understanding the concept of function in a graphical representation.

9. Barman, Bikash & Rajkhowa, Kukil. (2019). Non-comaximal graph of ideals of a ring. Proceedings - Mathematical Sciences. 129. 10.1007/s12044-019-0504-x.

10. Shinavier, Joshua & Wisnesky, Ryan. (2019). Algebraic Property Graphs.

11. Nikmehr, M.J., & Hosseini, S.M. (2019). More on the annihilator-ideal graph of a commutative ring. *Journal of Algebra and Its Applications*.

12. Elahi, Kashif & Ahmad, Ali & Hasni, Roslan. (2018). Construction Algorithm for Zero Divisor Graphs of Finite Commutative Rings and Their Vertex-Based Eccentric Topological Indices. Mathematics. 6. 301. 10.3390/math6120301.

13. Đurić, Alen & Jevđenić, Sara & Stopar, Nik. (2018). Categorial properties of compressed zero-divisor graphs of finite commutative rings.

14. Anderson, D. & Weber, Darrin. (2018). The zero-divisor graph of a commutative ring without identity. International Electronic Journal of Algebra. 23. 176-202. 10.24330/ieja.373663.

15. Kimball, Candace & LaGrange, John. (2018). The idempotent-divisor graphs of a commutative ring. Communications in Algebra. 1-14. 10.1080/00927872.2018.1427245.

16. Đurić, Alen & Jevđenić, Sara & Oblak, Polona & Stopar, Nik. (2018). The total zero-divisor graph of commutative rings. Journal of Algebra and Its Applications. 18. 10.1142/S0219498819501901.