International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 October 2023*

Torsion Points and Torsion Subgroups of Elliptic Curves Over $\mathbb{Q}(i)$ And $\mathbb{Q}(3i)$

Swapnil Kalita[1*], Dr. Manmohan Das[2]

[1*]Department of Mathematics, Bhattadev University, Bajali, Assam, India, mail- kswapnil9234@gmail.com
[2]Department of Mathematics, Bhattadev University, Bajali, Assam, India, mail- mdas.bajali@gmail.com

Abstract
Within the realm of elliptic curve theory, the count of rational points residing on these curves and the intricate nature of their torsion subgroups hold paramount significance. A comprehensive exploration into the diverse torsion subgroups of elliptic curves across varying number fields not only enriches our comprehension of their inherent properties but also bestows us with tools applicable to intricate mathematical conundrums. This paper embarks on this journey by laying the foundation with Mazur's seminal theorem, which serves as a pivotal classification of these torsion subgroups within the rational number field. Subsequently, our investigation broadens to encompass a discussion of these subgroups across general number fields, including the complex number field. Finally, our exploration culminates with a meticulous examination of the distinct properties characterizing torsion points within quadratic number fields.

Keywords: Elliptic curves, torsion point, torsion subgroups, quadratic number field

Introduction

An elliptic curve is a unique type of smooth curve characterized by a genus of one and featuring a distinctive point known as the point at infinity. Now any cubic curve with a known rational point on the curve can be converted into a special form called Weirstrass Normal Form.

$$E: y^2 = f(x) = x^3 + Ax + B$$

Here, the discriminant of this curve takes the form:

$$D = 4A^3 + 27B^2 \neq 0$$

Understanding that having knowledge of two rational points on an elliptic curve allows us to connect these points through a straight line, resulting in their intersection at a third point on the curve. Subsequently, drawing a line through this third point and the point at infinity leads to yet another intersection with the curve, giving rise to a new point, inherently rational in nature. This resultant point denotes the addition of the initial two points in algebraic number theory. Furthermore, the third point serves as a mirror image in relation to the X-axis. By iterating these steps, an intriguing phenomenon emerges: the ability to discover an infinite set of rational points for any specified elliptic curve.

Now these group of rational points on an elliptic curve forms a finitely general abelian group having the point of infinity as the identity element and follows all the properties of group theory.

Mathematically we can state this as

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus E(\mathbb{Q})_{tors}$$

Where $E(\mathbb{Q})$ is the abelian group of rational points of the elliptic curve, $\mathbb{Z}$ is some cyclic subgroup, r is the number of copies of the cyclic subgroup $\mathbb{Z}$ and $E(\mathbb{Q})_{tors}$ is the torsion subgroup of the elliptic curves over the field of rational numbers. Now this $E(\mathbb{Q})_{tors}$ is bounded above and doesn't determine the size of the abelian group. However the r is alsoknown as the rank of the elliptic curve, it can be infinite though till now only elliptic curves of rank is known to us.

Torsion Subgroups and Computation of $E(\mathbb{Q})_{tors}$

When delving into the realm of elliptic curves and their associated abelian groups, two fundamental inquiries immediately surface. Firstly, the quest to determine the potential ranks achievable by elliptic curves presents a formidable challenge. While empirical observations reveal that 99% of these curves possess ranks of 0 or 1, the existence of an infinite collection within the remaining 1% opens the door to the possibility of elliptic curves with ranks stretching to infinity. The Birch and Swinnerton-Dyer conjecture, although yet unproven, offers a tantalizing link between the algebraic rank of an elliptic curve and its analytical counterpart through a specific L-function. This conjecture holds the promise of providing a calculable algorithm to ascertain the rank of these curves.

The second query pertains to the finite torsion subgroup $E(\mathbb{Q})_{tors}$. Mazur's celebrated theorem provides clarity by confining these torsion subgroups for elliptic curves over the field $\mathbb{Q}$ to a maximum of

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 October 2023*

16. This theorem serves as a pivotal boundary, shedding light on the potential sizes of these finite torsion subgroups inherent to such curves.

Theorem (Mazur,1977): Let E be an elliptic curve over the field $\mathbb{Q}$. Then

$$E(\mathbb{Q})_{tors} \cong \begin{cases} \mathbb{Z}/m\mathbb{Z} \\ for\ 1 \le m \le 10\ and\ m = 12 \\ \mathbb{Z}/2\mathbb{Z}\ for\ 1 \le m \le 4 \end{cases}$$

However these possible subgroups can appear infinitely many times for a given curve.

Now the nature of these torsion subgroups vary significantly once we change the field associated with the curve. For an elliptic curves defined over a quadratic field k are as follows

$$E(\mathbb{Q})_{tors} = \begin{cases} \mathbb{Z}/m\mathbb{Z}\ for\ 1 \le m \le 18,\ m \ne 17 \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z}\ for\ m = 1,2,3,4,5,6 \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3m\mathbb{Z} \\ for\ m = 1,2 \\ \{\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \end{cases}$$

Here if we define the quadratic field K and fixed it to some particular field then only a few of these subgroups from the above list can appear. (Kamienny, Kenku and Momose,)

These results can further be analyzed if we restrict the quadratic fields to some complex quadratic field. Such as for the quadratic cyclotomic field $\mathbb{Q}(i)$, $E(\mathbb{Q}(i))_{tors}$ is either one of the subgroups listed in Mazur's theorem or $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$. Similarly if we take the field $\mathbb{Q}(3i)$, $E(\mathbb{Q}(3i))_{tors}$ is again either one of the subgroups listed in Mazur's theorem or $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3m\mathbb{Z}$ $for\ m = 1,2$. (Filip Nazman,)

Torsion Point

Theorem 1: Let an elliptic curve E is defined over a quadratic cyclotomic field $\mathbb{Q}(i)$ or

$\mathbb{Q}(3i)$. Then E(K) has can not have a point of order 21.

Proof: Let us assume that, if possible E(K) has point of order 21.

Case 1- If the quadratic cyclotomic field is $\mathbb{Q}(i)$ and let us assume that W be an quadratic extension of K.

So here $E^{(d)}(K)_{2/} = \{P \in E^{(d)}(K): [7]P = 0\}$ for some d in $_{o}k$. Hence there will be a point of order 7 in $E^{(d)}(K)$.

Again as the field is quadratic cyclotomic field $\mathbb{Q}(i)$

$E(K)_{2/} = \{P \in E(K): [7]P = 0\}$

Now taking E as the quadratic twist of $E_t : y^2 + (1 - m)xy - ny = x^3 - bx^2$ we can easily show that there will be a point P of order 3 also in E in a quadratic extension of K and the point will generate a K-rational subgroup. So the curve given by the equation

$C : \phi(x, t) = 0$

will get satisfied by the point (E,P). Here it will be sufficient to show that K-points on C will be equal to rational points on C. Now using MAGMA computation Ozlem Ejder have shown that $C^*(K) = C^*(\mathbb{Q})$ where C^* is a hyperelliptic curve birational to C and they both isomorphic over K except the singularity points set {(0,0),(0,1)}. Therefore (E,P) on C(K) will have a corresponding point on the hyperelliptic curve C^* over rational field and as a result it will have a corresponding point in $C(\mathbb{Q})$ itself. Now we know that no subgroup of order 21 can be found for E over a quadratic extension of $\mathbb{Q}$. Now P will belong to E defined over some quadratic extension of $\mathbb{Q}$ if $x(P) \in \mathbb{Q}$. So as a result $\mathbb{Z}/21\mathbb{Z} \not\subset E(W)$. So E (W) doesnot have a torsion subgroup of order 21. Hence $E(\mathbb{Q}(i))$ doesn't have a point of order 21.

Case 2- If the quadratic cyclotomic field is $\mathbb{Q}(3i)$, then again let us assume that W be an quadratic extension of K.

Now here E(K) will have a point of order 3 as $E(K)_{2/} = \{P \in E(K): [3]P = 0\}$

And also $E^{(d)}(K)_{2/} = \{P \in E(K): [7]P = 0\}$ for some d in $_{o}k$.

Hence $E^{(d)}(K)$ will have a point of order 7. So from these two results we can easily assume that E will have a subgroup of order 21 over W. It is a K-rational subgroup as image of each

summand of $E^{(d)}(K)_{2/}$ is a K-rational subgroup of E(W). Now by the theorem of B. Newmann if we fixed the field of the elliptic curve as $K = \mathbb{Q}(3i)$, then the modular curve

$X_0(20)(K)$ doesn't have any non cuspidol points. So it is not possible to have a 21-order K- rational subgroup over the field $\mathbb{Q}(3i)$. Hence it contradicts our initial assumption. So it is suffice to say E(K) has no point of order 21.

Now we will use the result of this theorem to deduce some results about the torsion subgroup of $E(F)_{2/}$ where F is an abelian extension of a quadratic cyclotomic field K.

Theorem 2: Let E be an elliptic curve defined over a quadratic cyclotomic field K. Then

$E(F)_{2/}$ can only be isomorphic to $\mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}$ for m=3 but cannot be isomorphic to the same torsion group for m=5,7 and 9.

Proof: Let E be an elliptic curve over the quadratic cyclotomic field K and F be an abelian quadratic

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 October 2023*

extension of K.
Now there will be some point P in E(K) for some odd n such that if

$E(K)_2/ \cong \{[n]P = 0\}$

Then $E(F)_2/ \simeq E^{d1}(F)_2/ \oplus E^{d2}(F)_2/ \oplus \dots \dots\dots E^{dm}(F)_2/$ for some $d_1, d_2, \dots \dots . d_m$ in $_{o}k$.

These odd numbers can only be either multiples of 3,5,7,9 or their products among each other and they are the only numbers dividing the order of $E(F)_{tors}$. Now the field F doesn't contain any primitive n^{th} root of unity for n=5,7 and 9. So $\mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}$ cannot be isomorphic to some subgroup of E(F) for n={5,7,9}. That means the only possible option here is $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$.
Again as $E(\mathbb{Q}(i))$ and $E(\mathbb{Q}(3i))$ cannot have a point of order 21 according to our previous

theorem. Thus $E(F)_2/$ cannot be isomorphic to $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/7\mathbb{Z}$ as order of the point must divide order of this group. Similarly for $\mathbb{Z}/9\mathbb{Z} \oplus \mathbb{Z}/7\mathbb{Z}$, if it needs to be isomorphic it must contain a point of order 63. However that is not possible as it will imply that it will also contain a point of order 21 which again violates our previous theorem.
Also E(F) cannot have any K rational subgroups of order 35 and 45 which means E(F) doesn't contain any point of order 35 or 45. So E(F) doesn't contain a subgroup isomorphic to $\mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/7\mathbb{Z}$ and $\mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z}$.
Again if E(F) contains a subgroup isomorphic to $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z}$ then

$E(K) = \{P \in E(K): [9]P = 0\}$

And it also have an K-rational subgroup of order 3. Now E(K) should have a K-rational subgroup of order 27. But we already know that E(K) doesn't have a K-rational subgroup of order 27 for any quadratic cyclotomic field K. Hence $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z}$ is also not a viable isomorphic group here.
Therefore, combining all these results it is safe to assume that $E(F)_2/$ can be isomorphic to only $\mathbb{Z}/\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/5\mathbb{Z}$, $\mathbb{Z}/7\mathbb{Z}$, $\mathbb{Z}/9\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$.

Result and Conclusions

In conclusion, the exploration of torsion points on elliptic curves over complex quadratic fields unveils a rich interplay between these algebraic structures and complex . The intricate nature of these fields offers a unique lens through which the behavior and distribution of torsion points can be comprehensively understood. Through meticulous analysis and application of mathematical frameworks, this research has shed light on the properties and limitations of torsion subgroups within these specific domains.
Here in this paper, we have shown that elliptic curve over specific quadratic cyclotomic field like $\mathbb{Q}(i)$ and $\mathbb{Q}(3i)$ cannot have torsion point of order 21. This result will give us that certain combination of torsion subgroup will not be possible for those quadratic cyclotomic field.
However there are still many other combinations of torsion subgroups for different torsion point that are yet to be checked for. Also in the second theorem we have shown isomorphism
of $E(F)_2/$ with certain types of torsion subgroups upto m=9. In our further results we will try to extend our research to higher values of m, thereby contributing more in the study of elliptic curve theory.

References

1. Silverman, Joseph H., and John T. Tate. "Rational points on elliptic curves." Springer Science & Business Media, 2012.
2. Washington, Lawrence C. "Elliptic curves: Number theory and cryptography." CRC Press, 2008.
3. Silverman, Joseph H. "The arithmetic of elliptic curves." Springer Science & Business Media, 2009.
4. Miret, Jordi, and Francesc Joan. "Elliptic curve cryptosystems in characteristic three." Journal of Mathematical Cryptology 1.3 (2007): 199-213.
5. Flynn, E. V., and M. J. Grannell. "On the torsion of elliptic curves over quadratic fields." Mathematics of Computation 62.206 (1994): 225-234.
6. Elkies, Noam D. "Elliptic and modular curves over quadratic fields and related computational issues." Computational Perspectives on Number Theory: Proceedings of a Conference in Honor of A.O.L. Atkin (1993): 21-76.
7. Balakrishnan, Jennifer S., and Ken Ono. "The arithmetic of rational isogeny classes over quadratic fields." Mathematics of Computation 81.278 (2012): 2415-2440.
8. Gross, Benedict H., and Don B. Zagier. "Heegner points and derivatives of L-series." Inventiones mathematicae 84.2 (1986): 225-320.
9. Mazur, Barry. "Rational isogenies of prime degree." Inventiones mathematicae 44.2 (1978): 129-162.
10. Kolyvagin, Victor A. "Finiteness of E (Q) and X (E, Q) for a subclass of Weil curves." Izvestiya Akademii nauk SSSR. Seriya matematicheskaya 52.3 (1988): 522-540.
11. Rubin, Karl. "The 'main conjectures' of Iwasawa theory for imaginary quadratic fields." Inventiones mathematicae 103.1 (1991): 25-68.

12. Clark, Pete L., and Nicholas A. Ramsey. "Lattice methods for hyperelliptic curves." Mathematics of Computation 85.300 (2016): 1681-1701.
13. Cremona, John E., and David Rusin. "Finding all elliptic curves with good reduction outside a given set of primes." Experimental Mathematics 6.3 (1997): 175-186.
14. Schoof, René. "Elliptic curves over finite fields and the computation of square roots mod p." Mathematics of Computation 44.170 (1985): 483-494.
15. Parent, Paul. "Torsion subgroups of elliptic curves with complex multiplication over quadratic fields." Mathematics of Computation 74.252 (2005): 389-405.
16. Laska, Jason N. "The structure of the torsion subgroups of elliptic curves overquadratic fields." Mathematics of Computation 82.283 (2013): 837-856.
17. Diamond, Fred, and Jerry Shurman. "A first course in modular forms." Springer Science & Business Media, 2005.
18. Niven, Ivan, Herbert S. Zuckerman, and Hugh L. Montgomery. "An introduction to the theory of numbers." John Wiley & Sons, 2019.
19. Lang, Serge. "Elliptic functions." Springer Science & BusinessMedia, 2003.
20. Knapp, Anthony W. "Elliptic curves." Princeton University Press, 1992.
21. Serre, Jean-Pierre. "Rational points on curves over finite fields." Contemporary Mathematics 67 (1987): 83-95.
22. Cassels, J.W.S., and E.V. Flynn. "Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2." London Mathematical Society Lecture Note Series 230 (1996): 13-32.
23. Koblitz, Neal. "Introduction to elliptic curves and modular forms." Springer Science & Business Media, 1993.
24. Gross, Benedict H. "Heights and the special values of L-series." Number theory related to Fermat's last theorem. Springer, New York, NY, 1996. 115-187.
25. Zhang, Shouwu. "Heights of Heegner points on Shimura curves." Annals of Mathematics (2003): 1059-1107.
26. Levere, K. M., & Kahlon, P. K. (2019). Investigating Mathematics Anxiety over Time in University Engineering Students. International Journal of Learning, Teaching and Educational Research, 18(7), 51-69. https://doi.org/10.26803/IJLTER.18.7.4
27. Moussa, N. M., & Saali, T. (2022). Factors Affecting Attitude Toward Learning Mathematics: A Case of Higher Education Institutions in the Gulf Region. SAGE Open, 12(3). https://doi.org/10.1177/21582440221123023
28. Navida, G. S. (2022). Mathematics Anxiety, Conception and Performance of the University Freshmen Students. International Journal of Scientific and Management Research, 5(03). https://doi.org/10.37502/ijsmr.2022.5302
29. OECD. (2016). Equations and Inequalities: Making mathematics accessibleto all. https://core.ac.uk/download/580015639.pdf