SOME PROBLEMS IN ELLIPTIC CURVES AND DIOPHANTINE EQUATIONS

By

PALLAB KANTI DEY

MATH08201104005

Harish-Chandra Research Institute, Allahabad

A thesis submitted to the

Board of Studies in Mathematical Sciences

In partial fulfillment of requirements

for the Degree of

DOCTOR OF PHILOSOPHY

of

HOMI BHABHA NATIONAL INSTITUTE

August, 2016

STATEMENT BY AUTHOR

This dissertation has been submitted in partial fulfilment of requirements for an advanced degree at Homi Bhabha National Institute (HBNI) and is deposited in the Library to be made available to borrowers under rules of the HBNI.

Brief quotations from this dissertation are allowable without special permission, provided that accurate acknowledgement of source is made. Requests for permission for extended quotation from or reproduction of this manuscript in whole or in part may be granted by the Competent Authority of HBNI when in his or her judgement the proposed use of the material is in the interests of scholarship. In all other instances, however, permission must be obtained from the author.

Date: **Pallab Kanti Dey**

DECLARATION

I hereby declare that the investigation presented in the thesis has been carried out by me. The work is original and has not been submitted earlier as a whole or in part for a degree / diploma at this or any other Institution / University.

Date: **Pallab Kanti Dey**

List of Publications arising from the thesis

Journal

1. "Length of an arithmetic progression represented by a binary quadratic form", Pallab Kanti Dey and R. Thangadurai, *Amer. Math. Monthly*, **2014**, *Vol. 121, no. 10*, 932-936.

2. "Arithmetic progressions on $y^2 = x^3 + k$", Pallab Kanti Dey and Bibekananda Maji, *J. Integer Seq.*, **2016**, *Vol. 19*, *Article 16.7.4*.

3. "Diophantine equations concerning balancing and Lucas balancing numbers", Pallab Kanti Dey and S. S. Rout, *Archiv der Mathematik*, **2017**, *Vol. 108, no. 1*, 29-43.

4. "Elliptic curves with rank 0 over number fields", Pallab Kanti Dey, *Funct. Approx. Comment. Math.*, **2017**, *DOI: 10.7169/facm/1585*.

Others

1. "Torsion points over number fields", Pallab Kanti Dey, Communicated.

Date: **Pallab Kanti Dey**

To my
Family

ACKNOWLEDGEMENTS

First and most of all, I want to thank my family, especialy my parents for the encouragement and support all these years to complete my thesis successfully. Also I am grateful to my elder brother who is a constant source of inspiration for me.

I would like to express my deepest gratitude to my advisor Prof. R. Thangadurai for his guidance, warm encouragement and continued support. I express my sincere gratitude to Prof. Filip Najman for his advice and suggestions. I want to thank also to my friends-cum-coauthors Bibekananda Maji and Sudhansu Sekhar Rout for some useful collaborations.

I want to thank all the members of my Doctoral committee, for their constant support. I also thank all faculty members of HRI. I am thankful to the all other members of HRI for their cooperation and for making my stay at HRI comfortable.

I warmly thank my life partner Debalina for her constant support throughout my PhD career. I also want to thank my friends Pranabesh, Arunava, Rakesh, Rahul, Debika, Balesh, Mallesham, Soumyarup, Pradip, Mithun, Sumana, Arvind, Veekesh, Manikandan, Nabin, Tushar, Manish, Bhuwanesh, Pramod, Anup, Ritabrata, Subhroneel, Titas, Satadal, Suman Jyoti, Aritra, Abhishek Joshi, Samrat, Sarif, Avijit, Masud, Debasis Mondal, Dibya Kanti, Chiranjib, Sudipto, Samiran, Debasis Sadhukhan, Nayabanta, Abhishek Juyal, Jaban Meher, Pradip Rai, Jai Mehta, Kashi Vishwanadham, Divyang Vimani, Ramesh Manna, Eshita Mazumdar, Senthil Kumar, Snehbala Sinha, Sabyasachi Tarat, Sourav Niyogi, Nilay Kundu and many others.

Contents

Synopsis

In this thesis, we tackle some problems in Number Theory, especially in the topics related to 'Elliptic Curves, Diophantine Equations and Arithmetic Progressions'.

We divide the thesis into five chapters.

The *first chapter* entitled **"Elliptic curves over $\mathbb{Q}$ having rank 0 over number fields"** deals with a characterization of those elliptic curves in a family defined over $\mathbb{Q}$ having rank 0 over number fields. We elaborate this briefly here.

Let E be an elliptic curve defined over a number field K. By the Mordell-Weil Theorem, it is well-known that the set of all K-rational points of E, denoted by $E(K)$, is a finitely generated Abelian group. Hence, by the structure theorem for finitely generated Abelian groups, we have

$$E(K) \cong T \oplus \mathbb{Z}^r,$$

for some non-negative integer r and for a finite group T. The non-negative integer r is called the *rank* of E over K and the finite group T is called *the torsion subgroup* of $E(K)$.

Finding the rank of a given elliptic curve over K is a very difficult problem compared to that of computing its torsion group. We list some of the results (which will be useful

for further discussion) related to the rank as follows. If $E : y^2 = x^3 + bx$ is an elliptic curve over $\mathbb{Q}$, then, from [65], it is known that,

$$\text{Rank}(E(\mathbb{Q})) \leq 2\beta(2b) - 1,$$

where $\beta(2b)$ denotes the number of distinct primes $p|2b$. In particular, if b is a prime number, then we get,

$$\text{Rank}(E(\mathbb{Q})) \leq 2.$$

In [18], we tackle a problem of classifying the elliptic curves of the form $y^2 = x^3 + bx$ whose rank is 0 over a number field K. More precisely, let K be a number field with its degree $[K : \mathbb{Q}]$ not divisible by 4 and let $E : y^2 = x^3 + bx$ be an elliptic curve for some nonzero integer b. Then the main result of the first chapter of this thesis is as follows.

Theorem 0.0.1. *Let K be a number field with its degree $[K : \mathbb{Q}] \equiv 2 \pmod 4$ (respectively, $[K : \mathbb{Q}]$ is odd) and let b be a nonzero integer with $b \neq 4m^4$ (respectively, b be any nonzero integer) for any integer m. Then the elliptic curve $E : y^2 = x^3 + bx$ has rank 0 over K if and only if the Diophantine equation $X^4 + bY^4 = Z^2$ has only trivial solutions in K.*

In order to prove the above Theorem, first, we need to compute the torsion subgroup T of $E(K)$. Then, by assuming that E has rank 0 over K, we prove that $X^4 + bY^4 = Z^2$ has only trivial solutions in K. For the other implication of the theorem, we prove the contrapositive statement which is, by assuming E has non-zero rank over K, we construct a non-trivial solution for the Diophantine equation $x^4 + by^4 = z^2$ in K. We discuss this

proof in detail in Chapter 1.

The *second chapter* of this thesis entitled **"Torsion points over number fields"** deals with the explicit computation of the torsion subgroup of a class of elliptic curves over number fields.

Let K be a number field and let E be an elliptic curve defined over K. When $K = \mathbb{Q}$, by a theorem of Mazur [46], it is known that the torsion subgroup of $E(\mathbb{Q})$ is either cyclic of order m for some integer $1 \leq m \leq 10$ or $m = 12$, or of the form $\mathbb{Z}_2 \oplus \mathbb{Z}_{2m}$ for some integer $1 \leq m \leq 4$.

If K is a quadratic number field, then, by a result of Kamienny [34] and Kenku and Momose [35], the torsion subgroup of $E(K)$ is isomorphic to one of the $\mathbb{Z}_m$ for $1 \leq m \leq 18$, $m \neq 17$ or one of the $\mathbb{Z}_2 \oplus \mathbb{Z}_{2m}$ for $1 \leq m \leq 6$ or one of the $\mathbb{Z}_3 \oplus \mathbb{Z}_{3m}$ for $m = 1, 2$ or $\mathbb{Z}_4 \oplus \mathbb{Z}_4$. In 2011, Najman [53] has found all the possible torsion subgroups when K is a quadratic cyclotomic field.

In [19], we deal with the torsion subgroups of elliptic curves which are of the form $y^2 = x^3 + c$ with $c \in \mathbb{Q}$. For these classes of elliptic curves, we derive the precise torsion subgroup of $E(K)$ for any number field K whose degree $[K : \mathbb{Q}]$ is odd and $3 \nmid [K : \mathbb{Q}]$. Also, we compute the torsion subgroup when K is any quadratic number field. The main results of the second chapter are as follows.

Theorem 0.0.2. *Let K be a number field whose degree $[K : \mathbb{Q}]$ is odd and is not divisible by 3. Let $E : y^2 = x^3 + c$ be an elliptic curve for some 6-th power-free integer c. If T is the torsion subgroup of $E(K)$, then T is isomorphic to one of the following groups.*

(1) $T \cong \mathbb{Z}/6\mathbb{Z}$, *if* $c = 1$,

(2) $T \cong \mathbb{Z}/3\mathbb{Z}$, *if* $c \neq 1$ *is a square, or if* $c = -432$,

(3) $T \cong \mathbb{Z}/2\mathbb{Z}$, *if* $c \neq 1$ *is a cube,*

(4) $T = \{\mathcal{O}\}$, *the trivial group for all the other cases.*

Theorem 0.0.3. *Let* c *be a* 6*-th power-free integer and let* d *be a square-free integer. Let* $E : y^2 = x^3 + c$ *be an elliptic curve. If* T *is the torsion subgroup of* $E(\mathbb{Q}(\sqrt{d}))$, *then* T *is isomorphic to one of the following groups.*

(1) $T \cong \mathbb{Z}/6\mathbb{Z}$, $\begin{cases} \text{if } c = 1 \text{ and } d \neq -3, \\ \text{or } c = a^3 \text{ with } a \neq 1, -3 \text{ for some nonzero integer } a \text{ and } d = a, \end{cases}$

(2) $T \cong \mathbb{Z}/3\mathbb{Z}$, $\begin{cases} \text{if } c = 2t^3 \text{ with } t \neq 2, -6 \text{ for some nonzero integer } t \\ \text{ and } d \text{ is square-free part of } 2t \text{ or } -6t, \\ \text{or } c = b^2 \text{ with } b \neq 1, 4 \text{ for some nonzero integer } b, \\ \text{or } c = 16, -432 \text{ and } d \neq -3, \\ \text{or } c \text{ is neither a cube nor a square}, c \neq 2t^3 \text{ for any nonzero} \\ \text{ integer } t \text{ and } d \text{ is square-free part of } c, \end{cases}$

(3) $T \cong \mathbb{Z}/2\mathbb{Z}$, *if* $c = a^3$ *with* $a \neq 1$ *for some nonzero integer* a *and* $d \neq a$,

(4) $T \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$, *if* $c = 1, -27$ *and* $d = -3$,

(5) $T \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, *if* $c = 16, -432$ *and* $d = -3$,

(6) $T \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, *if* $c = a^3$ *with* $a \neq 1, -3$ *for some nonzero integer* a *and* $d = -3$,

(7) $T = \{O\}$, *the trivial group for all the other cases.*

In order to prove Theorem 0.0.2, we first show that the primes 2 and 3 are the only prime divisors of $|T|$, by reducing the elliptic curves modulo prime ideals of the given number field and using the Hasse-Davenport relation [73] which predicts the size of the elliptic curve group over finite fields. Then, using the addition formula [66] of points on the elliptic curves and mod n Galois representations associated to elliptic curves, we show that there does not exist any point of order 4 or 9 in T.

To prove Theorem 0.0.3, we first show that the possible orders of the elements of T are $2, 3$ or 6, using a result in [29] which gives a relation between n-torsion points of $E(\mathbb{Q}(\sqrt{d}))$, n-torsion points of $E(\mathbb{Q})$ and n-torsion points of $E^d(\mathbb{Q})$, where n is an odd positive integer and E^d is the d-th quadratic twist of E. We discuss this in detail in Chapter 2.

The *third chapter* entitled **"Arithmetic progressions on Elliptic curves"** deals with the existence of rational points on elliptic curves which form an arithmetic progression; and the maximal length of an arithmetic progression.

Arithmetic progressions on an algebraic curve is an area which has been studied recently by many authors. Let E be an algebraic curve over $\mathbb{Q}$. The rational points $P_1, P_2, \ldots, P_n$ on E are said to be in *x-arithmetic progression* (respectively, *y-arithmetic progression*), if their x-coordinates (respectively, y-coordinates) are in arithmetic progression over $\mathbb{Q}$ with some difference $d \in \mathbb{Q}$. Similarly, the points are said to be in *simultaneous arithmetic progression*, if both x-coordinates and y-coordinates simultaneously are in arithmetic progression over $\mathbb{Q}$. Let $S_x(E)$ (respectively, $S_y(E)$) denote the maximal length of x-arithmetic progression (respectively, y-arithmetic progression) over $\mathbb{Q}$ in E.

Also, we let $S_{x,y}(E)$ denote the maximal length of simultaneous arithmetic progression over $\mathbb{Q}$ in E.

In [26], Garcia-Selfa and Tornero showed the existence of infinitely many elliptic curves with $S_{x,y}(E) \geq 5$. In [48], Mohanty studied the integer points on the elliptic curve $E : y^2 = x^3 + k$ which are in arithmetic progression with difference 1, and proved that its maximal length in x-coordinates (respectively, in y-coordinates) is less than or equal to 2 (respectively, less than or equal to 4). Later, Lee and Vélez [40] considered the same family of elliptic curves and focused on arithmetic progression with difference > 1. They proved the existence of infinitely many elliptic curves $E : y^2 = x^3 + k$ with $S_x(E) \geq 4$ and $S_y(E) \geq 6$. For this family of elliptic curves, there is a Conjecture of Mohanty [49] which states that $S_x(E) \leq 4$.

In [20], we obtain an upper bound for $S_y(E)$ and $S_{x,y}(E)$ for all elliptic curves E of the form $E : y^2 = x^3 + k$. The main results of the third chapter are as follows.

Theorem 0.0.4. *Let $E : y^2 = x^3 + k$ be a given elliptic curve over $\mathbb{Q}$. Then $S_{x,y}(E) \leq 3$. Moreover, there exist infinitely many elliptic curves $E : y^2 = x^3 + k$ with $S_{x,y}(E) = 3$.*

Theorem 0.0.5. *Let $E : y^2 = x^3 + k$ be a given elliptic curve over $\mathbb{Q}$. Then $S_y(E) \leq 6$. Moreover, there exist infinitely many elliptic curves $E : y^2 = x^3 + k$ with $S_y(E) = 6$.*

The proof of Theorem 0.0.4 is elementary. However, to prove Theorem 0.0.5, we need to use a nontrivial result of Bremner [11]. We discuss these in detail in Chapter 3.

The *fourth chapter* entitled **"Perfect powers in a product of terms of some number sequences"** deals with finding out perfect powers in a product of terms coming

from certain number sequences like sequence of the balancing numbers and the Lucas balancing numbers. We also prove a conjecture, related to Diophantine equations, given in [8], using the properties of the Lucas balancing numbers.

Let P and Q be the nonzero integers with $P^2 + 4Q \neq 0$. Let α and β be the roots of the equation

$$x^2 - Px - Q = 0. \tag{1}$$

The *Lucas sequence of the first* and *the second kind* for the roots α and β are given by

$$U_n(P,Q) = \frac{\alpha^n - \beta^n}{\alpha - \beta} \text{ and } V_n(P,Q) = \alpha^n + \beta^n \text{ for all } n = 0, 1, \ldots \tag{2}$$

respectively. The Fibonacci sequence $(F_n)_{n\geq 0}$ is an example of the Lucas sequence of the first kind for $(P,Q) = (1,1)$ together with the initial conditions $F_0 = 0$ and $F_1 = 1$. The Lucas sequence of the second kind for $(P,Q) = (1,1)$ (which is also known as *the Lucas sequence*), is denoted by $(L_n)_{n\geq 0}$ with initial conditions $L_0 = 2$ and $L_1 = 1$. The Pell sequence $(P_n)_{n\geq 0}$ is an example of the first kind Lucas sequence for $(P,Q) = (2,1)$ with initial conditions $P_0 = 0, P_1 = 1$ and the Lucas-Pell sequence $(Q'_n)_{n\geq 0}$ is an example of the second kind Lucas sequence for $(P,Q) = (2,1)$ with initial conditions $Q'_0 = 2$ and $Q'_1 = 2$. We denote the associated Pell sequence by Q_n with the same recurrence relation as Q'_n with initial conditions $Q_0 = 1$ and $Q_1 = 1$.

In [44], Luca and Shorey considered the product of k-conscutive terms in Lucas sequence. They proved that

$$U_n U_{n+1} \cdots U_{n+(k-1)} = y^l \tag{3}$$

has only finitely many integer solutions (n, k, y, l) for $n \geq 1, k \geq 2, l \geq 2, y \geq 2$ which are effectively computable. In the same paper, they proved that a nonzero product of two or more consecutive Fibonacci numbers is never a perfect power except for the trivial case, namely, $F_1 \cdot F_2 = 1$. Recently, Bravo et al. [8] explicitly solved a similar problem for the Pell and the Lucas-Pell sequence as in (3). In fact, they proved that for any positive integers n, d, k and $l \geq 2, y \geq 2$ with $\gcd(n, d) = 1$, the only solutions of the equation $\prod_{i=0}^{k-1} P_{n+id} = y^l$ are $P_7 = 13^2$ and $P_1 \cdot P_7 = 13^2$ and the equation $\prod_{i=0}^{k-1} Q'_{n+id} = y^l$ has no solution.

Before we state our results, we shall introduce another binary number sequence known as the *balancing numbers sequence* which was originaly developed from a Diophantine equation. A positive integer n is called a *balancing number* if the Diophantine equation

$$\sum_{i=1}^{n-1} i = \sum_{j=n+1}^{m} j$$

has solution for some natural number m. Equivalently, the solutions (x, y) of the Pell's equation $8x^2 + 1 = y^2$ are called *the balancing numbers* and *the Lucas balancing numbers* respectively. Let us denote the n-th balancing number and the Lucas balancing number by B_n and C_n respectively. The balancing and the Lucas balancing numbers satisfy (1) for $(P, Q) = (6, -1)$. The Binet form of the balancing and the Lucas balancing numbers are given by

$$B_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}, \text{ and } C_n = \frac{\alpha^n + \beta^n}{2} \quad \text{for all } n = 0, 1, \cdots, \tag{4}$$

where $\alpha = 3 + \sqrt{8}$ and $\beta = 3 - \sqrt{8}$.

The main results of the fourth chapter are as follows.

Theorem 0.0.6. *The equation $2x^2 + 1 = 3^b y^m$ has no solution in positive integers x, b, y and m with $y > 1, m > 2$ and b and m are even integers.*

This was a conjecture in [8].

Theorem 0.0.7. *There are no integral solutions (n, d, k, y, l) to the Diophantine equation*

$$B_n B_{n+d} \cdots B_{n+(k-1)d} = y^l \tag{5}$$

where $n \geq 1, d \geq 1, k \geq 2, y \geq 1$ and $l \geq 2$ are integers with $\gcd(n, d) = 1$.

Theorem 0.0.8. *There are no integral solutions (n, d, k, y, l) to the Diophantine equation*

$$C_n C_{n+d} \cdots C_{n+(k-1)d} = y^l \tag{6}$$

where $n \geq 1, d \geq 1, k \geq 2, y \geq 1$ and $l \geq 2$ are integers with $\gcd(n, d) = 1$.

Atfirst, we prove that there does not exist a non-trivial perfect power in the sequence of balancing numbers as well as in the sequence of the Lucas-balancing numbers. Also, we prove that the Lucas-balancing numbers can not be written as a product of a perfect power and a power of 3 except for $C_1 = 3$. Using this, we prove Theorem 0.0.6. Then using the results of Sylvester [69], Shorey and Tijdeman [64] and some interesting properties of the balancing numbers and the Lucas balancing numbers, we prove Theorem 0.0.7 and Theorem 0.0.8. We discuss these results in detail in Chapter 4.

The *fifth and the final chapter* entitled **"Arithmetic progression represented by binary quadratic form"** deals with an upper bound for the length of an arithmetic progression represented by an integral binary quadratic form whose discriminant is not a perfect square of an integer.

Let $Q(x, y) = ax^2 + bxy + cy^2$ be an integral binary quadratic form of discriminant $d = b^2 - 4ac \neq 0$. In 2008, Alaca, Alaca and Williams [1] proved that Q represents an arithmetic progression of infinite length if and only if d is a perfect square. Hence, if d is not a perfect square, then Q represents an arithmetic progression of finite length. In [22], we obtain an upper bound for the length of an arithmetic progression represented by Q.

Theorem 0.0.9. *Let $Q(x, y) = ax^2 + bxy + cy^2$ be an integral binary quadratic form with discriminant $d = b^2 - 4ac \neq 0$. Suppose that d is not a perfect square and that Q represents an arithmetic progression $\{kn + \ell : n = 0, 1, \ldots, R - 1\}$ of length R, where k and ℓ are positive integers. Then there are absolute constants $C_1 > 0$ and $L_1 > 0$ such that $R < C_1 \ell (k^2|d|)^{L_1}$.*

By an application of a theorem of Linnik [41] and elementary number theory tricks, we prove the above result.

Another related question is as follows. "Does every nonzero integral binary quadratic form represents an arithmetic progression of length 3?" The following result answers this question.

Theorem 0.0.10. *Every nonzero integral binary quadratic form represents a nontrivial arithmetic progression of length 3 infinitely often.*

Chapter 1

Elliptic curves over $\mathbb{Q}$ having rank 0 over number fields

This chapter is devoted to find out a necessary and sufficent condition for Elliptic curves in a family defined over $\mathbb{Q}$ having rank 0 over number fields.

1.1 Introduction

1.1.1 Basics of number fields

Definition 1.1.1. A field $K \subseteq \mathbb{C}$ is called a *number field* if its vector space dimension over $\mathbb{Q}$ is finite. The vector space dimension of K over $\mathbb{Q}$ is called *the degree* of K and is denoted by $[K : \mathbb{Q}]$.

Definition 1.1.2. An *algebraic integer* in a number field K is an element of K which is a root of a monic polynomial with coefficients in $\mathbb{Z}$. The set of algebraic integers of a number field K is denoted by $\mathcal{O}_K$. It forms a ring and it is usually called *the ring of integers* of K.

Let $\mathcal{P}$ be a prime ideal of $\mathcal{O}_K$. Then $\mathcal{P} \cap \mathbb{Z}$ is a prime ideal of $\mathbb{Z}$ and hence there exists a prime number p such that $\mathcal{P} \cap \mathbb{Z} = p\mathbb{Z}$. In this case, we say that the prime ideal $\mathcal{P}$ in $\mathcal{O}_K$ is *lying above* p.

Proposition 1.1.1 ([24]). *Any ideal in $\mathcal{O}_K$ can be written as a product of prime ideals uniquely.*

Definition 1.1.3. Let p be prime in $\mathbb{Z}$, whose ideal factorization in $\mathcal{O}_K$ is given by

$$p\mathcal{O}_K = \mathcal{P}_1^{e_1}\mathcal{P}_2^{e_2}\dots\mathcal{P}_g^{e_g}, \tag{1.1}$$

where $\mathcal{P}_i$'s are distinct prime ideals lying above p and e_i's are positive integers. The integer e_i is called the *ramification index* of the prime ideal $\mathcal{P}_i$ for all $i = 1, 2, \dots, g$.

We say that a prime number p is *ramified* if the integer $e_i > 1$ for some $i \in \{1, \dots, g\}$; Otherwise, the prime number p is called *unramified*. Note that if the prime number p is unramified, then $e_i = 1$ for all $1 \leq i \leq g$.

Definition 1.1.4. Let p be prime in $\mathbb{Z}$ and let $\mathcal{P}$ be a prime ideal lying above p in $\mathcal{O}_K$. Then $\mathcal{O}_K/\mathcal{P}$ is a finite dimensional vector space over $\mathbb{Z}/p\mathbb{Z}$. Let $f = [\mathcal{O}_K/\mathcal{P} : \mathbb{Z}/p\mathbb{Z}]$. This integer f is called *the residual degree* of the prime ideal $\mathcal{P}$.

Both the residual degree and the ramification index are connected with the degree of the number field as follows.

Proposition 1.1.2 ([24]). *Let p be prime in $\mathbb{Z}$, whose ideal factorization in $\mathcal{O}_K$ is given by*

$$p\mathcal{O}_K = \mathcal{P}_1^{e_1}\mathcal{P}_2^{e_2}\dots\mathcal{P}_g^{e_g}, \tag{1.2}$$

where $\mathcal{P}_i$ is a prime ideal lying above p and the integer e_i is the ramification index of $\mathcal{P}_i$ for all $i = 1, 2, \dots, g$. Also let f_i's be the residual degree of $\mathcal{P}_i$ for $i = 1, 2, \dots, g$. Then, we have,

$$[K : \mathbb{Q}] = \sum_{i=1}^{g} e_i f_i. \tag{1.3}$$

1.1.2 Basics of elliptic curves

Definition 1.1.5. Let K be a field of characteristic $\neq 2, 3$. An *Elliptic curve* E over a field K, denoted by E/K, is an algebraic curve defined by an equation of the form

$$y^2 = f(x) = x^3 + bx + c$$

, where $b, c \in K$ and all roots of the polynomial f(x) are distinct.

We denote $E(K)$ to be the set of all K-rational points on E along with one extra point $\mathcal{O}$, which is known as *the point at infinity.*

$$E(K) := \{(x, y) \in K \times K : y^2 = f(x)\} \cup \{\mathcal{O}\}$$

Definition 1.1.6. Let $E/\mathbb{Q}$ be an elliptic curve and let $P_1, P_2 \in E(K)$ be two (not necessarily distinct) points, for some number field K. The line passing through P_1 and P_2 intersects the elliptic curve in a third K-rational point $P_3{}'$. Then we consider the line passing through $P_3{}'$ and $\mathcal{O}$. This line intersects the curve in a point, say, P_3. Using this, we define a binary operation, namely, addition '$\oplus$' in $E(K)$ as follows.

$$P_1 \oplus P_2 = P_3.$$

Note that if $P_1 = P_2$, then one takes the tangent line at P_1 on E and continue the same procedure as above to get P_3.

Proposition 1.1.3 ([66])**.** *Let E be an elliptic curve over a number field K. Then the set $E(K)$ forms an abelian group under the binary operation '$\oplus$' define above, with the point $\mathcal{O}$ as the identity element. The group $E(K)$ is called the Mordell-Weil group of E over K.*

Now we actually compute the point P_3 in terms of the coordinates of the points P_1 and P_2 and these formulae are known as *addition formulae.* Let

$$P_1 = (x_1, y_1), P_2 = (x_2, y_2) \text{ and } P_3{}' = (x_3, y_3).$$

Since the curve (or graph) is symmetric about X-axis, we have $P_1 \oplus P_2 = P_3 = (x_3, -y_3)$. Now, we compute x_3 and y_3 in terms of x_1, x_2, y_1 and y_2

First, we consider the equation of the line joining the points (x_1, y_1) and (x_2, y_2), which is

$$y = \lambda x + \nu, \tag{1.4}$$

where $\lambda = \dfrac{y_2 - y_1}{x_2 - x_1}$, provided $x_1 \neq x_2$ and $\nu = y_1 - \lambda x_1 = y_2 - \lambda x_2$.

By the construction, the line intersects the cubic in two points (x_1, y_1) and (x_2, y_2). In order to find the intersecting point, we substitute

$$y^2 = (\lambda x + \nu)^2 = x^3 + bx + c. \tag{1.5}$$

Putting everything on one side yields

$$x^3 - \lambda x^2 + (b - 2\lambda\nu)x + (c - \nu^2) = 0. \tag{1.6}$$

This is a cubic equation in x, and its three roots x_1, x_2 and x_3 give us the x coordinates of three intersecting points. Thus,

$$x^3 - \lambda x^2 + (b - 2\lambda\nu)x + (c - \nu^2) = (x - x_1)(x - x_2)(x - x_3). \tag{1.7}$$

Equating the coefficients of the x^2 term on either side, we find that $\lambda^2 - a = x_1 + x_2 + x_3$, and so

$$x_3 = \lambda^2 - x_1 - x_2, \quad y_3 = \lambda x_3 + \nu. \tag{1.8}$$

Now suppose that $x_1 = x_2$. Then, $y_2 = \pm y_1$. If $y_2 = -y_1$, then $P_1 \oplus P_2 = \mathcal{O}$. If $y_2 = y_1$, we need to find $P_1 \oplus P_1 = 2P_1$. With the relation $y^2 = x^3 + bx + c$, we can calculate the slope of the tangent which is given by,

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

Using this λ, we can find the formula for doubling a point.

Sometimes, it is convenient to have an explicit expression for $2P$ in terms of the coordinate of $P = (x, y)$. If we substitute $\lambda = \dfrac{3x^2 + b}{2y}$ into the formulae given in (1.8), we get,

$$x \text{ coordinate of } 2P := x(2P) = \frac{x^4 - 2bx^2 - 8cx + b^2}{4x^3 + 4bx + 4c}. \tag{1.9}$$

This formula for $x(2P)$ is known as the *duplication formula*. It comes very handy later in our computations. Similarly one can calculate $y(2P)$.

Definition 1.1.7. Minimal model of an elliptic curve E is the curve with minimal absolute value of the discriminant of all curves E' which are isomorphic to E.

Definition 1.1.8. Let $E : y^2 = x^3 + bx + c$ be an elliptic curve for some integers b, c. We say that E has *good reduction* at a prime p if $p \nmid \Delta$, where Δ is the discriminant of minimal model of E. Let $\mathcal{P}$ be a prime ideal in $\mathcal{O}_K$ lying above p. By considering E over K, we say that E has *good reduction* at the prime ideal $\mathcal{P}$ if $p \nmid \Delta$.

Definition 1.1.9. Let E be an elliptic curve over K and let $P \in E(K)$. The point P is said to be a *torsion point* in $E(K)$ if there exists an integer $m \geq 1$ such that $mP = \mathcal{O}$, but $m'P \neq \mathcal{O}$ for all integers $1 \leq m' < m$.

Theorem 1.1.1 (Mordell-Weil [65])**.** *Let E be an elliptic curve over a number field K. Then the group $E(K)$ is a finitely generated abelian group.*

By the structure theorem for the finitely generated Abelian groups, we can write

$$E(K) \cong T \oplus \mathbb{Z}^r,$$

for some non-negative integer r and a finite group T. The non-negative integer r is called the *rank* of E over K and T is called *the torsion subgroup* of $E(K)$. Sometimes, we may write $T = E(K)_{tors}$.

Theorem 1.1.2 (Merel [47])**.** *Let $d \geq 1$ be an integer. Then there exists a constant $B(d)$ depending only on d such that $|E(K)_{tors}| \leq B(d)$ for all elliptic curves E defined over any number field K with $[K : \mathbb{Q}] = d$.*

The bound $B(d)$ is not effective (as it relies on Falting's theorem). However he proved the following. If p is the largest prime divisor of $|E(K)_{tors}|$ for $[K : \mathbb{Q}] = d > 1$, then $p \leq d^{3d^2}$. This bound was later improved by Oesterle to $(1 + 3^{\frac{d}{2}})$ [1994, unpublished!].

Finding the rank of a given elliptic curve is a very difficult problem compared to that of the torsion subgroup. Some bounds related to the rank have been known for some classes of elliptic curves. If $E : y^2 = x^3 + bx$ is an elliptic curve over $\mathbb{Q}$, then, from [65], it is well-known that

$$\text{Rank}(E(\mathbb{Q})) \leq 2\beta(2b) - 1$$

where $\beta(2b)$ denotes the number of distinct primes $p|2b$. In particular, if b is a prime number, then

$$\text{Rank}(E(\mathbb{Q})) \leq 2.$$

In [38], Kudo and Motose computed the rank of an elliptic curve $y^2 = x^3 - px$ over $\mathbb{Q}$ for Fermat prime p and Mersenne prime p. Also Bremner and Casssels [9] computed that for all odd prime p with $p \equiv 5 \pmod 8$, the rank of $y^2 = x^3 + px$ over $\mathbb{Q}$ is 1. In [31], for odd prime p, the rank of elliptic curves of the form $y^2 = x^3 - px$ over $\mathbb{Q}$ has been studied. Also in [32], the rank of an elliptic curve $y^2 = x^3 + pqx$ over $\mathbb{Q}$ was considered with p and q are primes. In [67], Spearman proved that the rank of an elliptic curve of the form $y^2 = x^3 - px$ over $\mathbb{Q}$ is 2 for all primes p with $p = u^4 + v^4$ for some integers u and v. In [68], the rank has been computed for an elliptic curve of the form $y^2 = x^3 - 2px$ over $\mathbb{Q}$ with p is prime.

1.2 The main results

In [18], we consider a class of elliptic curves of the form $E : y^2 = x^3 + bx$ having rank 0 over a number field K with $4 \nmid [K : \mathbb{Q}]$ and b is any integer. More precisely, we prove the following results.

Theorem 1.2.1. *Let K be a number field with $[K : \mathbb{Q}] \equiv 2 \pmod 4$ and b be a nonzero integer with $b \neq 4m^4$ for any integer m. Then the elliptic curve $E : y^2 = x^3 + bx$ has rank 0 over K if and only if the Diophantine equation $X^4 + bY^4 = Z^2$ has only trivial solutions*

in K.

Theorem 1.2.2. *Let K be a number field of odd degree and b be a nonzero integer. Then the elliptic curve $E : y^2 = x^3 + bx$ has rank 0 over K if and only if the Diophantine equation $X^4 + bY^4 = Z^2$ has only trivial solutions in K.*

By a trivial solution (x, y, z) of a Diophantine equation $x^4+by^4 = z^2$, we mean (x, y, z) with $xyz = 0$.

Remark 1.2.1. *The statement of Theorem 1.2.1 is not true for $b = 4m^4$ for any integer m if we take $K = \mathbb{Q}(\sqrt{2})$. In this case, the elliptic curve $E : y^2 = x^3+4m^4x$ is isomorphic to the curve $E_4 : y^2 = x^3 + 4x$. The rank of E_4 over $\mathbb{Q}(\sqrt{2})$ is 0. Hence the rank of E over $\mathbb{Q}(\sqrt{2})$ is 0. But the Diophantine equation $x^4 + 4m^4y^4 = z^2$ has a nontrivial solution $(\sqrt{2}m, 1, 2\sqrt{2}m^2)$ over $\mathbb{Q}(\sqrt{2})$.*

In order to prove the above theorems, we need to compute the torsion subgroup of E over K. Indeed, we prove the following propositions.

Proposition 1.2.1. *Let $E : y^2 = x^3 + bx$ be an elliptic curve for some 4-th power-free integer b and let $E(K)$ be the group of K-rational points on E, where $[K : \mathbb{Q}]$ is odd. If T is the torsion subgroup of $E(K)$, then T is isomorphic to one of the following groups.*

1. *$T \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, if $-b$ is a square,*
2. *$T \cong \mathbb{Z}/4\mathbb{Z}$, if $b = 4$,*
3. *$T \cong \mathbb{Z}/2\mathbb{Z}$, otherwise.*

Proposition 1.2.2. *Let $E : y^2 = x^3 + bx$ be an elliptic curve for some 4-th powerfree integer b and let $E(K)$ be the group of K-rational points on E, where $[K : \mathbb{Q}] \equiv 2 \pmod 4$. If T is the torsion subgroup of $E(K)$, then T is isomorphic to one of the following groups.*

1. *$T \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$,* $\begin{cases} \text{if } b = 4 \text{ and } i \in K, \\ \text{or } b = -1 \text{ and } i \in K, \end{cases}$

2. $T \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $\begin{cases} \text{if } b = -1 \text{ and } i \notin K, \\ \text{or } b = t^2 \text{ for some nonzero integer } t \neq \pm 2 \text{ and } i \in K, \\ \text{or } -b \text{ is a square}, \\ \text{or } \sqrt{-b} \in K, \end{cases}$

3. $T \cong \mathbb{Z}/4\mathbb{Z}$, $\begin{cases} \text{if } b = 4 \text{ and } i \notin K, \\ \text{or } b = t^2 \text{ for some nonzero integer } t \neq \pm 2 \text{ and } \sqrt{2t} \in K, \end{cases}$

4. $T \cong \mathbb{Z}/2\mathbb{Z}$, *otherwise.*

Remark 1.2.2. *From Propositon 1.2.1 and Propositon 1.2.2, it is clear that the only prime divisor of* $|E(K)_{tors}|$ *is* 2 *for all elliptic curves* $E : y^2 = x^3 + bx$ *and for all number field* K *with* $[K : \mathbb{Q}]$ *is not divisible by* 4.

1.3 Preliminaries

To prove Theorem 1.2.1 we need to build up some tools.

Throughout this chapter, by an elliptic curve E, we mean, the curve $E : y^2 = x^3 + bx$ for some nonzero integer b. For any given odd prime p, by reducing the coefficients modulo p, we get, the elliptic curve $\bar{E}(\mathbb{F}_p)$ over $\mathbb{F}_p$.

Proposition 1.3.1 ([36])**.** *Let* $E : y^2 = x^3 + bx$ *be an elliptic curve, where* b *is a nonzero integer. Let* $p \equiv 3 \pmod 4$ *be an odd prime such that* $p \nmid \Delta$ *where* Δ *is the discriminant of* E*. Then, we have*

$$|\bar{E}(\mathbb{F}_p)| = p + 1.$$

Proposition 1.3.2 ([73])**.** *For any prime* p*, let* $|\bar{E}(\mathbb{F}_p)| = p + 1 - a$ *with* $|a| \leq 2\sqrt{p}$*. Let the quadratic equation* $X^2 - aX + p = (X - \alpha)(X - \beta)$ *for some complex numbers* α *and* β*. Then,*

$$|\bar{E}(\mathbb{F}_{p^n})| = p^n + 1 - (\alpha^n + \beta^n)$$

for all $n \geq 1$.

Corollary 1.3.1. *Let $E : y^2 = x^3 + bx$ be an elliptic curve, where b is a nonzero integer. Let $p \equiv 3 \pmod 4$ be an odd prime such that $p \nmid \Delta$ where Δ is the discriminant of E. Then, we have*

$$|\bar{E}(\mathbb{F}_{p^n})| = \begin{cases} p^n + 1, & \text{if } n \text{ is odd} \\ (p^{\frac{n}{2}} + 1)^2, & \text{if } n \equiv 2 \pmod 4. \end{cases}$$

Proof. By the assumption, $|\bar{E}(\mathbb{F}_p)| = p + 1 - a$, where $|a| \leq 2\sqrt{p}$. Hence by Proposition 1.3.1, we have $a = 0$ as $p \equiv 3 \pmod 4$. Consider,

$$X^2 + p = (X - i\sqrt{p})(X + i\sqrt{p}).$$

If we set $\alpha = i\sqrt{p}$ and $\beta = -i\sqrt{p}$, then, by Proposition 1.3.2, we have

$$|\bar{E}(\mathbb{F}_{p^n})| = \begin{cases} p^n + 1, & \text{if } n \text{ is odd} \\ (p^{\frac{n}{2}} + 1)^2, & \text{if } n \equiv 2 \pmod 4. \end{cases}$$

□

Proposition 1.3.3. *Let $E : y^2 = x^3 + bx + c$ be an elliptic curve for some integers b and c. Let T be the torsion subgroup of $E(K)$ for some number field K. Let $\mathcal{O}_K$ be the ring of integers in K. If E has good reduction at a prime ideal $\mathcal{P}$ in $\mathcal{O}_K$, then let ϕ be the reduction modulo $\mathcal{P}$ map on T. That is, the reduction map $\phi : T \longrightarrow \bar{E}(\mathcal{O}_K/\mathcal{P})$ is defined as $P = (x, y) \to \bar{P} = (\bar{x}, \bar{y})$ if $P \neq \mathcal{O}$ and $\mathcal{O} \to \bar{\mathcal{O}}$. Then, the reduction map ϕ is an injective homomorphism except finitely many prime ideals $\mathcal{P}$.*

Proof. It is given that ϕ is a reduction modulo $\mathcal{P}$ map. We need to prove that ϕ is an injective homomorphism. First we note that for a point Q on $E(K)$, we have,

$$\overline{-Q} = \phi(-Q) = \phi(x, -y) = \overline{(x, -y)} = (\overline{x}, -\overline{y}) = -\overline{Q}.$$

To show ϕ is a homomorphism, it is enough to prove that for the points Q_1, Q_2 and Q_3 in T,

$$\text{if } Q_1 \oplus Q_2 \oplus Q_3 = \mathcal{O}, \text{ then } \bar{Q_1} \oplus \bar{Q_2} \oplus \bar{Q_3} = \bar{\mathcal{O}},$$

since it implies that

$$\phi(Q_1 \oplus Q_2) = \phi(-Q_3) = -\bar{Q_3} = \bar{Q_1} \oplus \bar{Q_2} = \phi(Q_1) \oplus \phi(Q_2).$$

If any of Q_1, Q_2 or Q_3 equals $\mathcal{O}$, then the result follows from the fact that negatives goes to negatives. So we may assume that Q_1, Q_2 and Q_3 are not equal to $\mathcal{O}$. Let $P_1 = (x_1, y_1), P_2 = (x_2, y_2)$ and $P_3 = (x_3, y_3)$, where x_i, y_i's are in K.

From the definition of the group law on E, the condition $Q_1 \oplus Q_2 \oplus Q_3 = \mathcal{O}$ is equivalent to saying that Q_1, Q_2 and Q_3 lie on a line. Let

$$y = \lambda x + k$$

be the line passing through Q_1, Q_2 and Q_3 (If two or three of the points coincide, then the line has to satisfy certain tangency conditions).

From (1.8), we get

$$x_3 = \lambda^2 - x_1 - x_2, \quad y_3 = \lambda x_3 + k.$$

Since x_1, x_2, x_3 and y_3 are elements of K, we have $\lambda, k \in K$. Therefore, except for finitely many prime ideals $\mathcal{P}$, we can reduce λ and k modulo $\mathcal{P}$.

Substituting the equation of the line into the equation of the cubic, we know that the equation

$$x^3 + bx + c - (\lambda x + k)^2 = 0$$

has x_1, x_2 and x_3 as its roots. In other words, we have the factorization

$$x^3 + bx + c - (\lambda x + k)^2 = (x - x_1)(x - x_2)(x - x_3).$$

This is the relation that ensures that $Q_1 \oplus Q_2 \oplus Q_3 = \mathcal{O}$, regardless of whether or not the points are distinct.

Reducing this last equation modulo $\mathcal{P}$, we obtain

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

Also, we can reduce the equations $y_i = \lambda x_i + k$ to get

$$\bar{y_i} = \bar{\lambda}\bar{x_i} + \bar{k}, \quad i = 1, 2, 3.$$

This means that the line $y = \bar{\lambda}x + \bar{k}$ intersects the curve $\bar{E} : y^2 = x^3 + \bar{b}x$ at the three points $\bar{Q_1}, \bar{Q_2}$ and $\bar{Q_3}$. Further if two of the points among $\bar{Q_1}, \bar{Q_2}$ and $\bar{Q_3}$ are the same, say, $\bar{Q_1} = \bar{Q_2}$, then the line is tangent to $\bar{E}$ at $\bar{Q_1}$; and similarly, if all three points coincide, then the line has a triple order contact with $\bar{E}$. Therefore,

$$\bar{Q_1} \oplus \bar{Q_2} \oplus \bar{Q_3} = \bar{\mathcal{O}},$$

which completes the proof that ϕ is a homomorphism.

A nonzero point $(x, y) \in T$ is sent to the reduced point $(\bar{x}, \bar{y}) \in \bar{E}(\mathcal{O}_K/\mathcal{P})$, and that reduced point is not $\bar{\mathcal{O}}$ except finitely many prime ideals $\mathcal{P}$. So the kernel of the reduction map consists of only one point which is '$\mathcal{O}$'. Hence the map is injective. □

Remark 1.3.1. *Note that any elment in K can be written as $t^{-1}x$, for some $t \in \mathbb{Z}$ and $x \in \mathcal{O}_K$. Also note that number of prime ideals containing a given integer t is finite. Since by Theorem 1.1.2, T is a finite group, we have only finite number of prime ideals which contains denominators of the coordinates of any nontrivial point in T. Hence we can take the reduction modulo $\mathcal{P}$ homomorphism on T for all prime ideals $\mathcal{P}$ outside the finite set of prime ideals.*

Now consider the elliptic curve $E : y^2 = x^3 + bx$ with discriminant Δ, where b is a nonzero integer. Let K be a number field of degree $[K : \mathbb{Q}] = n$ for some positive integer n such that $4 \nmid n$. Let T be the torsion subgroup of $E(K)$. Then we have the following lemmas.

Lemma 1.3.1. *For any odd prime q, we have $q \nmid |T|$.*

Proof. Since $4 \nmid n$, we seperate two cases as n is odd and $n \equiv 2 \pmod 4$.

Case 1: n is odd.

Suppose q divides $|T|$. Then, by Dirichlet's theorem on primes in arithmetic progression [3], we can choose a prime p with $p \nmid \Delta$ and $p \equiv 2q(q+2)+1 \pmod{4q}$ as $(2q(q+2)+1, 4q) = 1$. Let $p\mathcal{O}_K = \mathcal{P}_1^{e_1}\mathcal{P}_2^{e_2}\dots\mathcal{P}_r^{e_r}$ be the ideal decomposition in $\mathcal{O}_K$ where $\mathcal{P}_1, \mathcal{P}_2, \dots, \mathcal{P}_r$ are prime ideals in $\mathcal{O}_K$ lying above p and e_i's are ramification index for $\mathcal{P}_i$'s. Also from Proposition 1.1.2, we have $\sum_{i=1}^{r} e_i f_i = n$ where f_i's are residual degree for $\mathcal{P}_i$'s.

Since n is odd, there exists a f_i which is an odd integer for some i. Let $\mathcal{P}_i$ be the corresponding prime ideal and consider the reduction map modulo $\mathcal{P}_i$. Since $|\mathcal{O}_K/\mathcal{P}_i| = p^{f_i}$ and f_i is odd, we have $|\bar{E}(\mathcal{O}_K/\mathcal{P}_i)| = p^{f_i}+1$ by Corollary 1.3.1, as $p \equiv 3 \pmod 4$. Hence by Proposition 1.3.3, we conclude that $q \mid (p^{f_i}+1)$. But we also have $p \equiv 1 \pmod q$ which implies $p^{f_i}+1 \equiv 2 \pmod q$, which is a contradiction as $q \nmid 2$. Therefore, any odd prime q does not divide $|T|$.

Case 2: $n \equiv 2 \pmod 4$.

Suppose q divides $|T|$. Then, by Dirichlet's theorem on primes in arithmetic progression [3], we can choose a prime p with $p \nmid \Delta$ and $p \equiv 2q(q+2)+1 \pmod{4q}$ as $(2q(q+2)+1, 4q) = 1$. Let $p\mathcal{O}_K = \mathcal{P}_1^{e_1}\mathcal{P}_2^{e_2}\dots\mathcal{P}_r^{e_r}$ be the ideal decomposition in $\mathcal{O}_K$ where $\mathcal{P}_1, \mathcal{P}_2, \dots, \mathcal{P}_r$ are prime ideals in $\mathcal{O}_K$ lying above p and e_i's are ramification index for $\mathcal{P}_i$'s. Also from Proposition 1.1.2, we have $\sum_{i=1}^{r} e_i f_i = n$ where f_i's are residual degree for $\mathcal{P}_i$'s.

Since $n \equiv 2 \pmod 4$, we see that one of f_i's is either odd or $f_i \equiv 2 \pmod 4$. We consider the corresponding prime ideal $\mathcal{P}_i$ and the reduction map modulo $\mathcal{P}_i$. Since $|\mathcal{O}_K/\mathcal{P}_i| = p^{f_i}$, by Corollary 1.3.1, we have $|\bar{E}(\mathcal{O}_K/\mathcal{P}_i)| = p^{f_i}+1$ if f_i is odd and $|\bar{E}(\mathcal{O}_K/\mathcal{P}_i)| = (p^{\frac{f_i}{2}}+1)^2$ if $f_i \equiv 2 \pmod 4$, as $p \equiv 3 \pmod 4$. Hence by Proposition 1.3.3, we conclude that $q \mid (p^t+1)$ for some integer t. But we also have $p \equiv 1 \pmod q$ which implies $p^t+1 \equiv 2 \pmod q$, which is a contradiction as $q \nmid 2$. Therefore, any odd prime q does not divide $|T|$.

□

Lemma 1.3.2. *T does not have an element of order 8.*

Proof. As before, we have two cases.

Case 1: n is odd.

Suppose T has an element of order 8. Then 8 divides $|T|$. By Dirichlet's theorem on primes in arithmetic progression [3], we can choose a prime p with $p \nmid \Delta$ and $p \equiv 3 \pmod 8$. Let $p\mathcal{O}_K = \mathcal{P}_1^{e_1}\mathcal{P}_2^{e_2}\dots\mathcal{P}_r^{e_r}$ be the ideal decomposition in $\mathcal{O}_K$ where $\mathcal{P}_1, \mathcal{P}_2, \dots, \mathcal{P}_r$ are prime ideals in $\mathcal{O}_K$ lying above p and e_i's are ramification index for $\mathcal{P}_i$'s. Also from Proposition 1.1.2, we have $\sum_{i=1}^{r} e_i f_i = n$ where f_i's are residual degree for $\mathcal{P}_i$'s.

Since n is odd, we see that one of f_i's is odd. We consider the corresponding prime ideal $\mathcal{P}_i$ and the reduction map modulo $\mathcal{P}_i$. Since $|\mathcal{O}_K/\mathcal{P}_i| = p^{f_i}$ and f_i is odd, we have $|\bar{E}(\mathcal{O}_K/\mathcal{P}_i)| = p^{f_i} + 1$ by Corollary 1.3.1, as $p \equiv 3 \pmod 4$. Hence by Proposition 1.3.3, we conclude that $8 \mid (p^{f_i} + 1)$. But we also have $p \equiv 3 \pmod 8$ which implies $p^{f_i} + 1 \equiv 4 \pmod 8$, which is a contradiction as $8 \nmid 4$. Therefore, T does not have any element of order 8.

Case 2: $n \equiv 2 \pmod 4$.

First we want to understand the points of order 4 in T. Indeed, we have the following claim.

Claim 1: *If $P = (x, y)$ is a point of order 4 in T, then we have $x^2 = b$.*

By the duplication formula [66], we have

$$x(2P) = \frac{(x^2 - b)^2}{4y^2}$$

and

$$y(2P) = \frac{(x^2 - b)(x^4 - 4bx^2 + b^2)}{8y^3}.$$

Since $P = (x, y)$ is of order 4 in T, we have $y(2P) = 0$ and hence we get,

$$(x^2 - b)(x^4 - 4bx^2 + b^2) = 0.$$

If $x^4 - 4bx^2 + b^2 = 0$, then $[\mathbb{Q}(x) : \mathbb{Q}] = 4$, as the polynomial $x^4 - 4bx^2 + b^2$ is an irreducible polynomial over $\mathbb{Q}$. Further since $n \equiv 2 \pmod 4$, we conclude that $x \notin K$.

Hence if $P = (x, y)$ is a point of order 4 in T, then $x^2 - b = 0$. This proves Claim 1.

If possible, we assume that T has an element of order 8. Therefore T must have an element, say, $P = (x, y)$ of order 4. Hence by Claim 1, we get $x^2 = b$.

Subcase 1**:** b is not a square.

In this case, $x = \pm\sqrt{b} \in \mathbb{Z}[\sqrt{d}]$ where d is a square-free part of b. Since b is 4-th power free integer, we let $b = t^2 d$ for some square-free integer t. Then $x = \pm t\sqrt{d}$ and $y^2 = \pm 2t^3 d\sqrt{d}$. Since $y \in K$ and $y^2 \in \mathbb{Z}[\sqrt{d}]$, we have $y \in \mathbb{Z}[\sqrt{d}]$. Now let $y = y_1 + y_2\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$. Therefore, the two relations $y_1^2 + dy_2^2 = 0$ and $y_1 y_2 = \pm t^3 d$ together imply that $dt^6 = -y_2^4$. Since t is square-free, $d = -1$ and $t = \pm 1$. Therefore we get $b = -1$. This implies that $K \supseteq \mathbb{Q}(i)$.

Let $Q = (x_1, y_1)$ be a point of order 8 in T and let $P = 2Q$. Then P is of order 4 in T where $x(P) = \pm i$. So, $8Q = \mathcal{O} \Rightarrow 4(2Q) = \mathcal{O} \Rightarrow x(2Q) = \pm i$. That is, if $Q = (x_1, y_1)$, then

$$\Rightarrow \frac{(x_1^2 + 1)^2}{4x_1(x_1^2 - 1)} = \pm i \quad \Longleftrightarrow \quad x_1^4 + 2x_1^2 + 1 = \pm(4ix_1^3 - 4ix_1).$$

By putting $r = ix_1 \in K$, we have

$$r^4 - 2r^2 + 1 = \pm(4r^3 + 4r) \quad \Longleftrightarrow \quad r^4 \pm 4r^3 - 2r^2 \pm 4r + 1 = 0.$$

Now consider the polynomials $f(X) = X^4 - 4X^3 - 2X^2 - 4X + 1$ and $g(X) = X^4 + 4X^3 - 2X^2 + 4X + 1$. We claim that $f(X)$ and $g(X)$ are irreducible polynomials in $\mathbb{Z}[X]$.

It is clear that $f(X)$ does not have any integer root. Suppose $f(X)$ is reducible in $\mathbb{Z}[X]$. Then, $f(X) = (X^2 + aX + a_1)(X^2 + bX + b_1)$ for some integers a, b, a_1 and b_1. Since the constant term in $f(X)$ is 1, either $a_1 = b_1 = 1$ or $a_1 = b_1 = -1$. If $f(X) = (X^2 + aX + 1)(X^2 + bX + 1)$, then we have relations: $a + b = -4$ and $ab = -4$, which is a contradiction to a and b are integers. If $f(X) = (X^2 + aX - 1)(X^2 + bX - 1)$, then we have relations: $a + b = -4$ and $a + b = 4$, which is impossible. Hence, $f(X)$ is irreducible in $\mathbb{Z}[X]$. Similarly, we can prove that $g(X)$ is also irreducible in $\mathbb{Z}[X]$.

Now, by Gauss lemma, $f(X)$ and $g(X)$ are irreducible polynomials over $\mathbb{Q}$. As a result, we see that $[\mathbb{Q}(r) : \mathbb{Q}] = 4$, which is a contradiction as $K \supseteq \mathbb{Q}(r)$ and $[K : \mathbb{Q}] = n \equiv 2$

(mod 4).

Subcase 2**:** b is a square.

Since b is 4-th power free, we can write $b = t^2$ for some nonzero square-free integer t. Let $Q = (x_1, y_1)$ be a point of order 8 in T. In this subcase, the elements of order 4 in T has x-coordinates $\pm t$. Hence $8Q = \mathcal{O} \Rightarrow 4(2Q) = \mathcal{O} \Rightarrow x(2Q) = \pm t$. That is,

$$\Rightarrow \frac{(x_1^2 - t^2)^2}{4x_1(x_1^2 + t^2)} = \pm t \quad \Longleftrightarrow \quad x_1^4 - 2t^2x_1^2 + t^4 = \pm(4tx_1^3 + 4t^3x_1).$$

By putting $r = x_1/t \in K$, we have

$$r^4 - 2r^2 + 1 = \pm(4r^3 + 4r) \quad \Longleftrightarrow \quad r^4 \pm 4r^3 - 2r^2 \pm 4r + 1 = 0.$$

Now consider the polynomials $f(X) = X^4 - 4X^3 - 2X^2 - 4X + 1$ and $g(X) = X^4 + 4X^3 - 2X^2 + 4X + 1$. As in the previous case, we see that $f(X)$ and $g(X)$ are irreducible polynomials over $\mathbb{Q}$ and hence $[\mathbb{Q}(r) : \mathbb{Q}] = 4$, which is a contradiction as $K \supseteq \mathbb{Q}(r)$ and $[K : \mathbb{Q}] = n \equiv 2 \pmod 4$. This proves the lemma.

□

Remark 1.3.2. *By Lemma 1.3.1 and Lemma 1.3.2, we see that the only possible order of nontrivial torsion points in T are either 2 or 4. Note that $(0, 0)$ is always a point of order 2.*

1.4 Proof of Proposition 1.2.1

Note that $P = (x, y)$ is a point of order 2 in $T \Longleftrightarrow 2P = \mathcal{O} \Longleftrightarrow P = -P \Longleftrightarrow 2y = 0 \Longleftrightarrow x(x^2 + b) = 0$. Therefore, either $x = 0$ or $x^2 + b = 0$. If $x = 0$, then the point $(0, 0)$ is a point of order 2. If $x \neq 0$, then $x = \pm\sqrt{-b}$.

Note that $-b$ must be a square of an integer. For otherwise, if $-b$ is not a square, then $x \notin K$, since K and $\mathbb{Q}(\sqrt{-b})$ are linearly disjoint number fields over $\mathbb{Q}$ (as $[K : \mathbb{Q}]$ is odd), which is a contradiction to $P \in E(K)$. Thus, as $-b$ is a square, $x \in \mathbb{Z} \subset K$. Thus,

if (x, y) is a point of order 2 in T, then $(x, y) = (0, 0)$ or $(\pm\sqrt{-b}, 0)$ with $-b$ is a square of an integer.

Now, let $P = (x, y)$ be an element of order 4 in T. Then by Claim 1 in Lemma 1.3.2, we have $x^2 - b = 0 \iff x = \pm\sqrt{b}$.

Again note that b is a square. If not, then $x = \sqrt{b}$, which is impossible because K and $\mathbb{Q}(\sqrt{b})$ are linearly disjoint over $\mathbb{Q}$. If b is a square, then $x \in \mathbb{Z} \subseteq K$. Let $b = a^2$ for some square-free integer a. Thus if $P = (x, y)$ is a point of order 4 in T, then $x = \pm a$. Then $y^2 = \pm 2a^3 \Rightarrow y = \pm 2a\sqrt{\pm\frac{a}{2}}$. Since $y \in K$, we have $\pm\frac{a}{2}$ must be a square. Since a is square-free, we conclude that $a = \pm 2$. Hence the only elements of order 4 are $(2, \pm 4)$ with $b = 4$.

In Lemma 1.3.1 and Lemma 1.3.2, we have seen that there are no points of order 8 or of order q for any odd prime q. Therefore, by combining all the cases, we get the desired result.

1.5 Proof of Proposition 1.2.2

First we compute all the points of order 2 in T. If $P = (x, y)$ is a point of order 2, then $2P = \mathcal{O} \iff P = -P \iff 2y = 0 \iff x(x^2 + b) = 0$. Therefore, if $P = (x, y) \in T$ is a point of order 2, then $x = 0$ or $x = \pm\sqrt{-b}$. If $x = 0$, then the point $(0, 0)$ is a point of order 2. If $x \neq 0$, then $x = \pm\sqrt{-b} \in K$.

Now, let $P = (x, y)$ be an element of order 4 in T. Then by Claim 1 in Lemma 1.3.2, we have $x^2 - b = 0 \iff x = \pm\sqrt{b}$.

Again note that b is a square. If not, then $x = \pm\sqrt{b} \Rightarrow y^2 = \pm 2b\sqrt{b}$, which is impossible because $y \in K$ and $[K : \mathbb{Q}] \equiv 2 \pmod 4$. Therefore, write $b = t^2$ for some square-free integer t. Thus, $x = \pm t \Rightarrow y^2 = \pm 2t^3$. Hence $y = \pm t\sqrt{\pm 2t}$.

If $\pm 2t$ is a square, then $t = \pm 2$, because t is square-free. Hence $b = 4$. In this case the possible elements of order 4 are $(2, \pm 4)$ and $(-2, \pm 4i)$.

If $\pm 2t$ is not a square, then $(t, \pm t\sqrt{2t})$ are the only points of order 4 in T, when $\sqrt{2t} \in K$ and $(-t, \pm t\sqrt{-2t})$ are the only points of order 4 in T, when $\sqrt{-2t} \in K$.

In Lemma 1.3.1 and Lemma 1.3.2, we have seen that there are no points of order 8 or of order q for any odd prime q.

Combining all the above cases, we get the desired result.

1.6 Proof of Theorem 1.2.1 and Theorem 1.2.2

First we prove two claims and we deduce Theorem 1.2.1 and 1.2.2.

Claim 1:

1. *Let K be a number field with $[K : \mathbb{Q}] \equiv 2 \pmod 4$ and $E : Y^2 = X^3 + bX$ be a given elliptic curve for some 4-th power free integer $b \neq 4$. If the rank of E over K is 0, then the equation $x^4 + by^4 = z^2$ has only trivial solutions over K.*

2. *Let K be a number field of odd degree and $E : Y^2 = X^3 + bX$ be a given elliptic curve for some 4-th power free integer b. If the rank of E over K is 0, then the equation $x^4 + by^4 = z^2$ has only trivial solutions over K.*

Suppose $(x, y, z) \in K^3$ with $xyz \neq 0$ is a nontrivial solution of the equation $x^4 + by^4 = z^2$. Dividing the equation by y^4 and by the change of variable

$$s \mapsto \frac{x}{y} \text{ and } t \mapsto \frac{z}{y^2},$$

we obtain the equation $s^4 + b = t^2$ for some $s, t \in K$. We can rewrite this equation as

$$r = s^2 \text{ and } r^2 + b = t^2.$$

Now, we multiply the last equation by r and using the relation $r = s^2$, we get

$$r^3 + br = (st)^2.$$

Then, by applying another change of variable $X = r$ and $Y = st$, we obtain an elliptic curve

$$E : Y^2 = X^3 + bX.$$

Since x, y and z are nonzero, we have r, s and t are nonzero. This implies that the corresponding X and Y are nonzero.

Case 1: $[K : \mathbb{Q}] \equiv 2 \pmod 4$.

By the assumption, the elliptic curve $E : Y^2 = X^3 + bX$ has rank 0 over K. Therefore, by Proposition 1.2.2, if $b \neq -1$ and b is not a square, we have

$$E(K) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \quad \text{or} \quad \mathbb{Z}/2\mathbb{Z}.$$

That is, every nontrivial element of this group is of order 2 and hence $Y = 0$, which forces that either $x = 0$ or $z = 0$, which is a contradiction. Hence, the equation $x^4 + by^4 = z^2$ has only trivial solutions over K if b is not a square and $b \neq -1$.

Suppose $b = -1$.

Subcase 1: $i \notin K$.

If $b = -1$ and $i \notin K$, as E has rank 0 over K by Proposition 1.2.2, we have

$$E(K) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

That is, every nontrivial element of this group is of order 2 and hence $Y = 0$ which forces that either $x = 0$ or $z = 0$, which is a contradiction. Hence, the equation $x^4 + by^4 = z^2$ has only trivial solutions over K, if $b = -1$ and $i \notin K$.

Subcase 2: $i \in K$.

If $b = -1$ and $i \in K$, as rank of E is 0 over K by Proposition 1.2.2, we have

$$E(K) \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Here $(0,0)$ and $(\pm 1,0)$ are elements of order 2 and $(i, \pm(1-i)), (-i, \pm(1+i))$ are elements of order 4. The points of order 2 will lead to trivial solution for the equation $x^4+by^4=z^2$ over K. Corresponding to the points of order 4, we have $r = s^2 = \pm i$, which is a contradiction because $s \in K$ and $[K : \mathbb{Q}]$ is not divisible by 4. Therefore, the equation $x^4 + by^4 = z^2$ has only trivial solutions for $b = -1$ and $i \in K$.

Now, we assume that b is a square and let $b = t^2$ for some nonzero integer t with $t \neq \pm 2$ as $b \neq 4$.

If $\sqrt{2t} \in K$, as E has rank 0 over K by Proposition 1.2.2, we have

$$E(K) \cong \mathbb{Z}/4\mathbb{Z}.$$

Here, $(0,0)$ is the only element of order 2 and $(t, \pm t\sqrt{2t})$ are elements of order 4. The point $(0,0)$ will lead to trivial solution for the equation $x^4+by^4=z^2$ over K. Corresponding to the point $(t, \pm t\sqrt{2t})$, we have $r = s^2 = t$, which is a contradiction as $s \in K$ and $\sqrt{2t} \in K$. Therefore, the equation $x^4 + by^4 = z^2$ has only trivial solutions in this case.

If $\sqrt{2t} \notin K$, as E has rank 0 over K and $b \neq 4$, by Proposition 1.2.2, we have

$$E(K) \cong \mathbb{Z}/2\mathbb{Z}.$$

Here, $(0,0)$ is the only element of order 2. Since the point $(0,0)$ leads to trivial solution for the equation $x^4 + by^4 = z^2$ over K, we are done.

Combining all the cases, we see that the equation $x^4 + by^4 = z^2$ has only trivial solutions over K for any nonzero 4-th power free integer $b \neq 4$ whenever E has rank 0 over K.

Case 2: $[K : \mathbb{Q}]$ is odd.

By the assumption, the elliptic curve $E : Y^2 = X^3+bX$ has rank 0 over K. Therefore, by Proposition 1.2.1, if $b \neq 4$, we have

$$E(K) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \quad \text{or} \quad \mathbb{Z}/2\mathbb{Z}.$$

That is, every nontrivial element of $E(K)$ is of order 2 and hence $Y = 0$ which forces that either $x = 0$ or $z = 0$, which is a contradiction. Hence, the equation $x^4 + by^4 = z^2$ has only trivial solutions over K if $b \neq 4$.

When $b = 4$, by Proposition 1.2.1 and the assumption that the rank of $E(K)$ is 0, we have

$$E(K) \cong \mathbb{Z}/4\mathbb{Z}.$$

Here, $(0, 0)$ is the only element of order 2 and $(2, \pm 4)$ are the only elements of order 4. Note that $(0, 0)$ will lead to trivial solution for the equation $x^4 + by^4 = z^2$ over K. Corresponding to the point $(2, \pm 4)$, we have $r = s^2 = 2 \iff s = \pm\sqrt{2}$. Since $s \in K$, we see that $\sqrt{2} \in K$, which is a contradiction because K and $\mathbb{Q}(\sqrt{2})$ are linearly disjoint over $\mathbb{Q}$. Therefore the equation $x^4 + by^4 = z^2$ has only trivial solutions in this case also.

Combining all the cases, we see that the equation $x^4 + by^4 = z^2$ has only trivial solutions over K for any nonzero 4-th power free integer b whenever E has rank 0 over K. This proves the Claim 1.

Claim 2: *Let $E : Y^2 = X^3 + bX$ be an elliptic curve over K, where K is any field with characteristic 0. If the equation $x^4 + by^4 = z^2$ has only trivial solutions over K, then E has rank 0 over K.*

Suppose E has positive rank over K. Then there exists a point $P = (X, Y)$ of infinite order in $E(K)$. Therefore, $XY \neq 0$.

By the duplication formula, we have

$$X(2P) = \frac{(X^4 - 2bX^2 + b^2)}{4Y^2} = \frac{(X^2 - b)^2}{(2Y)^2}.$$

Note that, $X(2P)$ is a square in K. Since P is of infinite order, so is $2P$. Therefore there exists a point $Q = (x', y')$ on E such that $x' = s^2$ and $y' = st$ for some nonzero $s, t \in K$. So we have,

$$s^2t^2 = s^6 + bs^2 \Rightarrow t^2 = s^4 + b.$$

Thus $(s, 1, t)$ is a nontrivial solution for the equation $x^4 + by^4 = z^2$ over K, which is a

contradiction to the assumption. Hence we conclude that if $x^4 + by^4 = z^2$ has only trivial solutions over K, then E has rank 0 over K, which proves the Claim 2.

To prove Theorem 1.2.1 and Theorem 1.2.2, it is enough to assume that b is a 4-th power free integer. If not, let $b = at^4$ for some 4-th power free integer a and nonzero integer t. Then (t^2x, t^3y) is a point on the elliptic curve $E : y^2 = x^3 + bx$ if and only if (x, y) is a point on $E_1 = y^2 = x^3 + ax$. Also (x, y, z) is a solution of the Diophantine equation $x^4 + by^4 = z^2$ if and only if (x, ty, z) is a solution of the Diophantine equation $x^4 + ay^4 = z^2$. Thus, it is enough to assume that b is a 4-th power-free integer. Then the theorems follow from Claim 1 and Claim 2. □

1.7 Applications

Definition 1.7.1. Let $E : y^2 = x^3 + bx + c$ be an elliptic curve for some integers b and c. Also let d be a nonzero rational number. Then the *d-quadratic twist* of E is the elliptic curve $E^d : dy^2 = x^3 + bx + c$.

Proposition 1.7.1 ([65])**.** *Let E^d be the d-quadratic twist of E. Then*

$$\textit{Rank } E(\mathbb{Q}(\sqrt{d})) = \textit{ Rank } E(\mathbb{Q}) + \textit{ Rank } E^d(\mathbb{Q}).$$

Corollary 1.7.1. *For any nonzero integer b, the Diophantine equation $x^4 + by^4 = z^2$ has only trivial solutions over $\mathbb{Q}$ if and only if it has only trivial solutions over $\mathbb{Q}(i)$.*

Proof. If $x^4 + by^4 = z^2$ has only trivial solutions over $\mathbb{Q}(i)$, then obviously it has trivial solutions over $\mathbb{Q}$.

Conversely, we assume that the equation $x^4 + by^4 = z^2$ has only trivial solutions over $\mathbb{Q}$. Then by Theorem 1.2.1, the elliptic curve $E : y^2 = x^3 + bx$ has rank 0 over $\mathbb{Q}$. Note that (-1)-quadratic twist of E is $E^{(-1)} : y^2 = x^3 + bx$, which is E itself. Therefore, by putting $d = -1$ in the formula in Proposition 1.7.1, we have

$$\text{Rank } E(\mathbb{Q}(\sqrt{-1})) = \text{ Rank } E(\mathbb{Q}) + \text{ Rank } E^{-1}(\mathbb{Q}) = 2 \text{ Rank } E(\mathbb{Q}).$$

Since Rank $E(\mathbb{Q})$ is 0, we have Rank $E(\mathbb{Q}(i)) = 0$. Then again by Theorem 1.2.1, $x^4 + by^4 = z^2$ has only trivial solutions over $\mathbb{Q}(i)$. □

Definition 1.7.2. A positive integer n is said to be a *congruent number* if n is the area of a right triangle whose sides are rational numbers.

The following equivalent formulation is known for congruent numbers.

Proposition 1.7.2 ([37])**.** *A positive square-free integer n is a congruent number if and only if the elliptic curve $E_n : y^2 = x^3 - n^2x$ has positive rank over $\mathbb{Q}$.*

Using Theorem 1.2.1, we deduce the following.

Corollary 1.7.2. *A positive square-free integer n is a congruent number if and only if $x^4 - y^4 = z^2$ has a nontrivial solution in $\mathbb{Q}(\sqrt{n})$.*

Proof. Let E^n be the n-quadratic twist of the elliptic curve $E : y^2 = x^3 - x$. Since E has rank 0 over $\mathbb{Q}$, by Proposition 1.7.1, we have Rank $E^n(\mathbb{Q})$ = Rank $E(\mathbb{Q}(\sqrt{n}))$. Hence by Proposition 1.7.2, we get n is a congruent number if and only if Rank $E(\mathbb{Q}(\sqrt{n})) > 0$. Then, by Theorem 1.2.1, we get, n is a congruent number if and only if $x^4 - y^4 = z^2$ has a nontrivial solution in $\mathbb{Q}(\sqrt{n})$. □

Chapter 2

Torsion points over number fields

This chapter is devoted to computing torsion subgroups explicitly over number fields for the elliptic curves which are of the form $E : y^2 = x^3 + c$ for some integer c.

2.1 Introduction

Let K be a number field and E be an elliptic curve defined over K. Then, by Theorem 1.1.1, the group $E(K)$ of K-ratonal points is a finitely generated Abelian group and $E(K) \cong T \oplus \mathbb{Z}^r$ where T is the torsion subgroup and r is the rank of E.

When $K = \mathbb{Q}$, Mazur found all the possible torsion subgroups of $E(K)$ as follows.

Theorem 2.1.1 (Mazur [46])**.** *The torsion subgroup of $E(\mathbb{Q})$ is either cyclic of order m for some integer $1 \leq m \leq 10$ or $m = 12$, or $\mathbb{Z}_2 \oplus \mathbb{Z}_{2m}$ for some integer $1 \leq m \leq 4$.*

If K is a quadratic field, then, Kamienny [34] and Kenku and Momose [35] found all possible torsion subgroups of $E(K)$.

Theorem 2.1.2. *If K is a quadratic field, then the torsion subgroup of $E(K)$ is isomorphic to either $\mathbb{Z}_m$ for $1 \leq m \leq 18, m \neq 17$ or $\mathbb{Z}_2 \oplus \mathbb{Z}_{2m}$ for $1 \leq m \leq 6$ or $\mathbb{Z}_3 \oplus \mathbb{Z}_{3m}$ for $m = 1, 2$ or $\mathbb{Z}_4 \oplus \mathbb{Z}_4$.*

Moreover in [33], Jeon, Kim and Park showed the following result.

Theorem 2.1.3. *Each of the* 26 *groups listed in Theorem 2.1.2 occurs infinitely often as the torsion subgroup of $E(K)$, when K varies over all quadratic fields and E varies over all elliptic curves over K.*

However, when we fix a quadratic field K, it is still unknown which of the 26 listed groups are actually appearing as torsion subgroup of $E(K)$. In 2011, Najman has computed all the possible torsion subgroup of $E(K)$, when K is a quadratic cyclotomic field. That is, when $K = \mathbb{Q}(i)$ or $\mathbb{Q}(\sqrt{-3})$. He also has found all the possibilities of torsion subgroup of $E(K)$ when $K = \mathbb{Q}(i)$ or $\mathbb{Q}(\sqrt{-3})$, by considering E as an elliptic curve over $\mathbb{Q}$.

Theorem 2.1.4 ([53])**.** *Let E be an elliptic curve over $\mathbb{Q}$. Then,*

(1) The torsion subgroup $E(\mathbb{Q}(i))_{tors}$ of $E(\mathbb{Q}(i))$ is either one of the groups stated in Theorem 2.1.1 or $\mathbb{Z}_4 \oplus \mathbb{Z}_4$;

(2) The torsion subgroup $E(\mathbb{Q}(\sqrt{-3}))_{tors}$ of $E(\mathbb{Q}(\sqrt{-3}))$ is either one of the groups stated in Theorem 2.1.1 or $\mathbb{Z}_3 \oplus \mathbb{Z}_3$ or $\mathbb{Z}_3 \oplus \mathbb{Z}_6$.

Theorem 2.1.5 ([54])**.** *We have,*

(1) Let E be an elliptic curve over $\mathbb{Q}(i)$. Then $E(\mathbb{Q}(i))_{tors}$ is either one of the groups stated in Theorem 2.1.1 or $\mathbb{Z}_4 \oplus \mathbb{Z}_4$;

(2) Let E be an elliptic over $\mathbb{Q}(\sqrt{-3})$. Then $E(\mathbb{Q}(\sqrt{-3}))_{tors}$ is either one of the groups stated in Theorem 2.1.1 or $\mathbb{Z}_3 \oplus \mathbb{Z}_3$ or $\mathbb{Z}_3 \oplus \mathbb{Z}_6$.

In 2016, Najman [55] found all possible torsion subgroups of $E(K)$, when E is an elliptic curve over $\mathbb{Q}$ and K is a cubic field.

Theorem 2.1.6 ([55])**.** *Let E be an elliptic curve over $\mathbb{Q}$. If K is a cubic field over $\mathbb{Q}$, then the torsion subgroup of $E(K)$ is isomorphic to either $\mathbb{Z}_m$ for $1 \leq m \leq 21, m \neq 11, 15, 16, 17, 19, 20$ or $\mathbb{Z}_2 \oplus \mathbb{Z}_{2m}$ for $1 \leq m \leq 7, m \neq 5, 6$.*

In 2006, Jeon, Kim and Park [33] considered K as a quartic number field and showed the following.

Theorem 2.1.7 ([33]). *If K varies over all quartic number fields and E varies over all elliptic curves over K, then the groups that appear as the torsion subgroup of $E(K)$ infinitely often are precisely the following;*

(1) $\mathbb{Z}/N_1\mathbb{Z}, 1 \leq N_1 \leq 24, N_1 \neq 19, 23$,

(2) $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N_2\mathbb{Z}, 1 \leq N_2 \leq 9$,

(3) $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3N_3\mathbb{Z}, 1 \leq N_3 \leq 3$,

(4) $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4N_4\mathbb{Z}, 1 \leq N_4 \leq 2$,

(5) $\mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$,

(6) $\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$.

Definition 2.1.1. A homomorphism $\phi : E(\mathbb{C}) \to E(\mathbb{C})$ is said to be an *isogeny*, if ϕ is defined by rational functions.

Definition 2.1.2. An isogeny $\phi : E(\mathbb{C}) \to E(\mathbb{C})$ is called a *multiplication by n map* for some integer n, if $\phi(P) = nP$ for all $P \in E(\mathbb{C})$.

Definition 2.1.3. Let E be an elliptic curve over $\mathbb{C}$. We say that E has a *complex multiplication* (or CM for short), if there is an endomorphism $\phi : E(\mathbb{C}) \to E(\mathbb{C})$ which is not a multiplication by n map for any integer n.

Example 2.1.1. The elliptic curve $E : y^2 = x^3 + c$ has the complex multiplication. It can be seen by considering the endomorphism

$$\phi(x, y) = \left(\frac{-1 + \sqrt{-3}}{2}x, -y\right).$$

Since $\left(\frac{-1 + \sqrt{-3}}{2}\right)^3 = 1$, it is easy to see that $\phi(x, y)$ is indeed a point on E for every point (x, y) on E.

The subject of torsion points on CM elliptic curves begins with the following result.

Theorem 2.1.8 ([56]). *Let E be a CM elliptic curve over $\mathbb{Q}$. Then $E(\mathbb{Q})_{tors}$ is isomorphic to one of the following groups; the trivial group, $\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/6\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Conversely, each such group occurs as a torsion subgroup for at least one CM elliptic curve over $\mathbb{Q}$.*

Theorem 2.1.9 ([36]). *Let $E : y^2 = x^3 + c$ be an elliptic curve for some integer c which is 6-th power-free. If T is the torsion subgroup of $E(\mathbb{Q})$, then T is isomorphic to one of the following groups.*

(1) $T \cong \mathbb{Z}/6\mathbb{Z}$, *if* $c = 1$,

(2) $T \cong \mathbb{Z}/3\mathbb{Z}$, *if* $c \neq 1$ *is a square, or if* $c = -432$,

(3) $T \cong \mathbb{Z}/2\mathbb{Z}$, *if* $c \neq 1$ *is a cube*,

(4) $T = \{\mathcal{O}\}$, *for otherwise.*

The follwing result computes the torsion subgroups for CM elliptic curves defined over number fields of odd degree.

Theorem 2.1.10 ([7]). *Let F be a number field of odd degree. Let E be a CM elliptic curve over F and let T be the torsion subgroup of $E(F)$. Then T is isomrphic to one of the following groups;*

(1) the trivial group, $\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/6\mathbb{Z}$ *or* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$,

(2) $\mathbb{Z}/p^n\mathbb{Z}$ *for any prime number* $p \equiv 3 \pmod 8$ *and* $n \in \mathbb{N}$,

(3) $\mathbb{Z}/2p^n\mathbb{Z}$ *for any prime number* $p \equiv 3 \pmod 4$ *and* $n \in \mathbb{N}$,

Conversely, each of the above stated groups arises as the torsion subgroup of $E(F)$ for a CM elliptic curve E defined over a number field F of odd degree.

2.2 The main results

In [19], we deal with CM elliptic curves of the form $y^2 = x^3 + c$ for some $c \in \mathbb{Q}$. Since, by a rational transformation, we can make this equation with integer coefficients, it is enough to assume that c is an integer. For this class of elliptic curves, we derive the precise torsion subgroup of $E(K)$ for any given number field K of odd degree over $\mathbb{Q}$ with its degree $[K : \mathbb{Q}]$ is not divisible by 3 and also for any quadratic field K over $\mathbb{Q}$.

For a given elliptic curve $E : y^2 = x^3 + c$ with $c \in \mathbb{Z}$, we can assume that c is a 6-th power free integer. If not, then we write $c = c_1 t^6$ for some nonzero integer c_1 which is a 6-th power free integer and for some nonzero integer t. Then note that (x, y) is a point on the elliptic curve $E_1 : y^2 = x^3 + c_1$ if and only if (t^2x, t^3y) is a point on E.

The main results of this chapter are the following theorems.

Theorem 2.2.1. *Let $E : y^2 = x^3 + c$ be an elliptic curve for some 6-th power free integer c and let K be a number field whose degree $[K : \mathbb{Q}]$ is odd and is not divisible by 3. If T is the torsion subgroup of $E(K)$, then T is isomorphic to one of the following groups.*

(1) $T \cong \mathbb{Z}/6\mathbb{Z}$, *if* $c = 1$,

(2) $T \cong \mathbb{Z}/3\mathbb{Z}$, *if* $c \neq 1$ *is a square, or if* $c = -432$,

(3) $T \cong \mathbb{Z}/2\mathbb{Z}$, *if* $c \neq 1$ *is a cube*,

(4) $T = \{\mathcal{O}\}$, *for otherwise.*

Theorem 2.2.2. *Let c be a 6-th power free integer and d be a square-free integer. Let $E : y^2 = x^3 + c$ be an elliptic curve. If T is the torsion subgroup of $E(\mathbb{Q}(\sqrt{d}))$, then T is isomorphic to one of the following groups.*

(1) $T \cong \mathbb{Z}/6\mathbb{Z}$, $\begin{cases} \text{if } c = 1 \text{ and } d \neq -3, \\ \text{or } c = a^3 \text{ with } a \neq 1, -3 \text{ for some nonzero integer } a \text{ and } d = a, \end{cases}$

(2) $T \cong \mathbb{Z}/3\mathbb{Z}$ $\begin{cases} \text{if } c = 2t^3 \text{ with } t \neq 2, -6 \text{ for some nonzero integer } t \\ \text{and } d \text{ is square-free part of } 2t \text{ or } -6t, \\ \text{or } c = b^2 \neq 1, 16 \text{ for some nonzero integer } b, \\ \text{or } c = 16, -432 \text{ and } d \neq -3, \\ \text{or } c \text{ is neither a cube nor a square}, c \neq 2t^3 \text{ for any nonzero} \\ \text{integer } t \text{ and } d \text{ is square-free part of } c, \end{cases}$

(3) $T \cong \mathbb{Z}/2\mathbb{Z}$, if $c = a^3$ with $a \neq 1$ for some nonzero integer a and $d \neq a$,

(4) $T \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$, if $c = 1, -27$ and $d = -3$,

(5) $T \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, if $c = 16, -432$ and $d = -3$,

(6) $T \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, if $c = a^3$ with $a \neq 1, -3$ for some nonzero integer a and $d = -3$,

(7) $T = \{O\}$, the trivial group for all the other cases.

2.3 Preliminaries

Throughout this chapter, by an elliptic curve E, we mean the curve defined by the equation $y^2 = x^3 + c$ for some nonzero integer c. For any elliptic curve E over a field L and for any positive integer n, define

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

Proposition 2.3.1 ([29]). *Let E be an elliptic curve defined over $\mathbb{Q}$. Let d be a square-free integer. Let $K = \mathbb{Q}(\sqrt{d})$ and let E^d be the d-quadratic twist of E. For any odd positive integer n,*

$$E(K)[n] \cong E(\mathbb{Q})[n] \times E^d(\mathbb{Q})[n].$$

Proposition 2.3.2 ([27]). *Let E be an elliptic curve defined over $\mathbb{Q}$ and let $R \in E(\mathbb{C})$ be a point of order n for some positive integer n. Then $[\mathbb{Q}(R) : \mathbb{Q}]$ divides $|GL_2(\mathbb{Z}/n\mathbb{Z})|$ where the field $\mathbb{Q}(R)$ is the smallest field containing $\mathbb{Q}$, $x(R)$ and $y(R)$.*

Proposition 2.3.3 ([36]). *Let $E : y^2 = x^3 + c$ be an elliptic curve for some nonzero integer c. Let $p \equiv 2 \pmod 3$ be an odd prime such that $p \nmid \Delta$ where Δ is the discriminant of E. Then, we have*

$$|\bar{E}(\mathbb{F}_p)| = p + 1.$$

Corollary 2.3.1. *Let $E : y^2 = x^3 + c$ be an elliptic curve for some non-zero integer c. Let $p \equiv 2 \pmod 3$ be an odd prime such that $p \nmid \Delta$ where Δ is the discriminant of E. Then, we have*

$$|\bar{E}(\mathbb{F}_{p^n})| = \begin{cases} p^n + 1, & \text{if } n \text{ is odd} \\ (p^{\frac{n}{2}} + 1)^2, & \text{if } n \equiv 2 \pmod 4. \end{cases}$$

Proof. We know that $|\bar{E}(\mathbb{F}_p)| = p + 1 - a$ for some integer $|a| \leq 2\sqrt{p}$. Hence, by Proposition 2.3.3, we have $a = 0$ as $p \equiv 2 \pmod 3$. Consider the factorization of the quadratic equation over $\mathbb{C}$ as

$$X^2 + p = (X - i\sqrt{p})(X + i\sqrt{p}).$$

By setting $\alpha = i\sqrt{p}$ and $\beta = -i\sqrt{p}$ and by Proposition 1.3.2, we get,

$$|\bar{E}(\mathbb{F}_{p^n})| = \begin{cases} p^n + 1, & \text{if } n \text{ is odd} \\ (p^{\frac{n}{2}} + 1)^2, & \text{if } n \equiv 2 \pmod 4. \end{cases}$$

□

Now, we consider the elliptic curve $E : y^2 = x^3 + c$ for some non-zero integer c with discriminant Δ. Let K be a number field of degree $[K : \mathbb{Q}] = n$ for some positive integer n such that n is odd and $3 \nmid n$. Let T be the torsion subgroup of $E(K)$. Then we have following lemmas.

Lemma 2.3.1. *For any odd prime $q > 3$, we have $q \nmid |T|$.*

Proof. Suppose q divides $|T|$. Then, by Dirichlet's theorem on primes in arithmetic progression [3], we can choose a prime p with $p \nmid \Delta$ and $p \equiv q^2+1 \pmod{3q}$ as $(q^2+1, 3q) = 1$. Let $p\mathcal{O}_K = \mathcal{P}_1^{e_1}\mathcal{P}_2^{e_2}\dots\mathcal{P}_r^{e_r}$ be the ideal decomposition in $\mathcal{O}_K$ where $\mathcal{P}_1, \mathcal{P}_2, \dots, \mathcal{P}_r$ are

prime ideals in $\mathcal{O}_K$ lying above p and e_i's are ramification index for $\mathcal{P}_i$'s. Also from Proposition 1.1.2, we have $\sum_{i=1}^{r} e_i f_i = n$ where f_i's are residual degree for $\mathcal{P}_i$'s.

Since n is odd, there is one f_i which is odd. Let $\mathcal{P}_i$ be the corresponding prime ideal and consider the reduction modulo $\mathcal{P}_i$ map. Since $|\mathcal{O}_K/\mathcal{P}_i| = p^{f_i}$ and f_i is odd, we have $|\bar{E}(\mathcal{O}_K/\mathcal{P}_i)| = p^{f_i} + 1$ by Corollary 2.3.1, as $p \equiv 2 \pmod 3$. Hence by Proposition 1.3.3, we conclude that $q \mid (p^{f_i} + 1)$. But we also have $p \equiv 1 \pmod q$ which implies $p^{f_i} + 1 \equiv 2 \pmod q$, which is a contradiction as $q \nmid 2$. Therefore, any odd prime $q > 3$ does not divide $|T|$. □

Lemma 2.3.2. *In T, there does not exist any element of order 4.*

Proof. Suppose there exists an element of order 4 in T. Then, 4 divides $|T|$. Therefore, by Dirichlet's theorem on primes in arithmetic progression [3], we can choose a prime p with $p \nmid \Delta$ and $p \equiv 5 \pmod{12}$ as $(5, 12) = 1$. Let $p\mathcal{O}_K = \mathcal{P}_1^{e_1}\mathcal{P}_2^{e_2}\dots\mathcal{P}_r^{e_r}$ be the ideal decomposition in $\mathcal{O}_K$ where $\mathcal{P}_1, \mathcal{P}_2, \dots, \mathcal{P}_r$ are prime ideals in $\mathcal{O}_K$ lying above p and e_i's are ramification index for $\mathcal{P}_i$'s. Also from Proposition 1.1.2, we have $\sum_{i=1}^{r} e_i f_i = n$ where f_i's are residual degree for $\mathcal{P}_i$'s.

Since n is odd, there is one f_i which is odd. Let $\mathcal{P}_i$ be the corresponding prime ideal and consider the reduction modulo $\mathcal{P}_i$ map. Since $|\mathcal{O}_K/\mathcal{P}_i| = p^{f_i}$ and f_i is odd, we have $|\bar{E}(\mathcal{O}_K/\mathcal{P}_i)| = p^{f_i} + 1$ by Corollary 2.3.1, as $p \equiv 2 \pmod 3$. Hence by Proposition 1.3.3, we conclude that $4 \mid (p^{f_i} + 1)$. But we also have $p \equiv 1 \pmod 4$ which implies $p^{f_i} + 1 \equiv 2 \pmod 4$, which is a contradiction as $4 \nmid 2$. Therefore, there does not exist any element of order 4 in $|T|$. □

Let $P = (x, y)$ be a point in $E(K)$. Then by the Duplication formula, we have

$$2P = \left(\frac{x(x^3 - 8c)}{4(x^3 + c)}, \frac{x^6 + 20cx^3 - 8c^2}{8y(x^3 + c)} \right).$$

Lemma 2.3.3. *Let $P = (x, y)$ be a point of order 2 in T. Then, $(x, y) = (-a, 0)$ for some nonzero square-free integer a satisfying $c = a^3$*

Proof. Note that $P = (x, y)$ is a point of order 2 in T if and only if $2P = \mathcal{O}$, as $P \neq \mathcal{O}$. This is equivalent to $P = -P \iff 2y = 0 \iff x^3 + c = 0$. Hence, the degree of $\mathbb{Q}(x)$ is

$[\mathbb{Q}(x):\mathbb{Q}] \leq 3$. Since $x \in K$ and its degree $[K:\mathbb{Q}]$ is an odd integer with $3 \nmid [K:\mathbb{Q}]$, we conclude that x is an integer. Hence, $c = a^3$ for some nonzero square-free integer a. In this case, $(-a, 0)$ is the only point of order 2 in T. Hence the lemma. □

Lemma 2.3.4. *Let $P = (x, y)$ be a point of order 3 in T. Then,*

$$P = \begin{cases} (0, \pm b) & \text{where } b \text{ is a non-zero integer with } c = b^2, \\ (12, \pm 36) & \text{only when } c = -432. \end{cases}$$

Proof. First, we claim that $P = (x, y)$ is a point of order 3 in T if and only if $x(x^3+4c) = 0$. For, $P \neq \mathcal{O}$ is a point of order 3 if and only if $3P = \mathcal{O} \iff 2P = -P$. Therefore, $x(2P) = x(-P) \iff \dfrac{x(x^3 - 8c)}{4(x^3 + c)} = x \iff x(x^3 + 4c) = 0$.

If $x = 0$, then $c = y^2$ with c is a 6-th power-free integer and $y \in K$. Since K is a number field of odd degree, we see that y must be integer and hence $c = b^2$ for some nonzero integer b.

If $x \neq 0$, then $x^3 + 4c = 0$. Then, the degree $[\mathbb{Q}(x) : \mathbb{Q}] \leq 3$. Since $x \in K$ and the degree $[K : \mathbb{Q}]$ is an odd integer with $3 \nmid [K : \mathbb{Q}]$, we conclude that x is an integer. Hence $c = 2t^3$ for some nonzero square-free integer t. Therefore, $y^2 = -6t^3$. Since $y \in K$ and K is a number field of odd degree, we conclude that y is also an integer. Hence, since $y^2 = -6t^3$, we conclude that $-6t$ is a square. Since t is a square-free integer, we get $t = -6$. Therefore, $c = -432$. In this case, $(12, \pm 36)$ are the points of order 3 in T. Hence the lemma. □

Lemma 2.3.5. *There does not exist any element of order 9 in T.*

Proof. Let $P = (x, y)$ be a point of order 9 in T. By Proposition 2.3.2, $[\mathbb{Q}(P) : \mathbb{Q}]$ divides $|GL_2(\mathbb{Z}/9\mathbb{Z})| = 3^5(3^2 - 1)(3 - 1) = 2^4 3^5$, which is a contradiction because $\mathbb{Q}(P)$ is contained in K and $[K : \mathbb{Q}]$ is odd with $3 \nmid [K : \mathbb{Q}]$. □

Now, we consider the elliptic curve $E : y^2 = x^3 + c$ for some nonzero integer c with discriminant Δ. Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic field for some square-free integer d and let T be the torsion subgroup of $E(K)$. Then we have the following lemmas.

Lemma 2.3.6. *There does not exist any element of order* 4 *in* T.

Proof. Let P be an element of order 4 in T. In that case, T contains an element of order 2 which forces that c to be a cube, say, a^3 for some nonzero integer a.

Note that, if $P = (x, y)$ is of order 4, then $y(2P) = 0 \iff x^6 + 20cx^3 - 8c^2 = 0 \iff x^3 = -10c \pm 6c\sqrt{3}$. Hence, for $d = 3$, we get, $x = (-1 \pm \sqrt{3})a \in \mathbb{Z}[\sqrt{3}]$. Therefore, for $d \neq 3$, there does not exist any element of order 4.

For $d = 3$, since $x \in \mathbb{Z}[\sqrt{3}]$ and $y^2 = x^3 + c \in \mathbb{Z}[\sqrt{3}]$, we get $y \in \mathbb{Z}[\sqrt{3}]$. Let $y = t_1 + t_2\sqrt{3}$ for some nonzero integers t_1 and t_2. Since $y^2 = x^3 + c$, we get two relations which are $t_1^2 + 3t_2^2 = -9c$ and $t_1t_2 = \pm 3c$. These two relations together give $t_1^2 + 3t_2^2 \mp 3t_1t_2 = 0$. By putting $t = \dfrac{t_1}{t_2} \in \mathbb{Q}$, we get

$$t^2 \mp 3t + 3 = 0 \Longrightarrow t = \frac{\pm 3 \pm \sqrt{-3}}{2},$$

a contradiction as $t \in \mathbb{Q}$. Hence, we conclude that there does not exist any element of order 4 in T. □

Lemma 2.3.7. *Let* $q > 3$ *be any prime number. Then there does not exist any element of order* q *in* T.

Proof. In Theorem 2.1.9, we have seen that $E(\mathbb{Q})$ does not have any element of order q for any prime $q > 3$. For any square-free integer d, we consider the d-quadratic twist of E which is $E^d : y^2 = (dx)^3 + cd^3$. Then by Theorem 2.1.9, $E^d(\mathbb{Q})$ does not have any element of order q. Hence, by the Proposition 2.3.1, we conclude that $E(K)[q] = \{\mathcal{O}\}$, which proves the lemma. □

Lemma 2.3.8. *There does not exist any element of order* 9 *in* T.

Proof. By Theorem 2.1.9, we have seen that $E(\mathbb{Q})$ does not have any element of order 9. Therefore, $E(\mathbb{Q})[9] \cong \mathbb{Z}/3\mathbb{Z}$ or $E(\mathbb{Q})[9] = \{\mathcal{O}\}$. Also, for any square-free integer d, by Theorem 2.1.9, the group $E^d(\mathbb{Q})$ does not have any element of order 9. Hence $E^d(\mathbb{Q})[9] \cong \mathbb{Z}/3\mathbb{Z}$ or $E^d(\mathbb{Q})[9] = \{\mathcal{O}\}$. Hence, by the Proposition 2.3.1, we conclude that

$E(K)[9] \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ or $E(K)[9] \cong \mathbb{Z}/3\mathbb{Z}$ or $E(K)[9] = \{\mathcal{O}\}$. Thus there does not exist any element of order 9 in T. □

Lemma 2.3.9. *Let $P = (x, y)$ be a point of order 2 in $T \subseteq E(\mathbb{Q}(\sqrt{d}))$. Then, $c = a^3$ for some nonzero square-free integer a and*

$$P = \begin{cases} (-a, 0) & \text{for any } d, \\ (-a\omega, 0), (-a\omega^2, 0) & \text{for } d = -3, \end{cases}$$

where $\omega = \dfrac{-1 + \sqrt{-3}}{2}$.

Proof. Note that $P = (x, y)$ be a point of order 2 in $T \iff P \neq \mathcal{O}$ and $2P = \mathcal{O}$ $\iff P = -P \iff 2y = 0 \iff x^3 + c = 0$. Hence, the degree $[\mathbb{Q}(x) : \mathbb{Q}] \leq 3$. Since $x \in K$ and $[K : \mathbb{Q}] = 2$, we conclude that $[\mathbb{Q}(x) : \mathbb{Q}] \leq 2$. Hence the polynomial $x^3 + c$ is reducible over $\mathbb{Q}$ and hence this polynomial has an integer root. Therefore, $c = a^3$ for some nonzero integer a.

Then $(-a, 0)$ is the only point of order 2 in T for $d \neq -3$. For $d = -3$, the points $(-a, 0), (-a\omega, 0)$ and $(-a\omega^2, 0)$ are the only points of order 2 in T. Hence the lemma. □

Lemma 2.3.10. *Let $P = (x, y)$ is a point of order 3 in $T \subseteq E(\mathbb{Q}(\sqrt{d}))$. If $c \neq 2t^3$ for any integer t, then*

$$P = \begin{cases} (0, \pm b) & \text{where } b \text{ is a non-zero integer satisfying } c = b^2, \\ (0, \pm\sqrt{c}) & \text{where } c \text{ is not a square and } d \text{ is the square free part of } c. \end{cases}$$

Proof. Note that $P = (x, y)$ be a point of order 3 in $T \iff P \neq \mathcal{O}$ and $3P = \mathcal{O}$ $\iff 2P = -P \iff x(2P) = x(-P) \iff \dfrac{x(x^3 - 8c)}{4(x^3 + c)} = x \iff x(x^3 + 4c) = 0$.

If $x^3 + 4c = 0$, then the degree $[\mathbb{Q}(x) : \mathbb{Q}] \leq 3$. Since $x \in K$ and $[K : \mathbb{Q}] = 2$, we see that $[\mathbb{Q}(x) : \mathbb{Q}] \leq 2$. Hence the polynomial $x^3 + 4c$ is reducible over $\mathbb{Q}$ and hence this polynomial has an integer root. Therefore, $4c = z^3$ for some non-zero integer z. Since c is an integer, we conclude that $c = 2t^3$ for some nonzero square-free integer t, which is a contradiction. Hence, $x^3 + 4c \neq 0$. Therefore, $x = 0$ and $y^2 = c$.

Since $y \in K$, we have two cases, namely, $y \in \mathbb{Z}$ and $y \notin \mathbb{Z}$. If $y \in \mathbb{Z}$, then, $c = b^2$ for some nonzero integer b. Therefore, $(0, \pm b)$ are the points of order 3 in T for any d. When $y \notin \mathbb{Z}$, then $(0, \pm\sqrt{c})$ are the points of order 3 in T, when d is the square-free part of c. Hence the lemma. □

Lemma 2.3.11. *Let $c = 2t^3$ be an integer for some square-free integer t. Let $P = (x, y)$ be a point of order 3 in $E(\mathbb{Q}(\sqrt{d}))$. Then, the point*

$$P = \begin{cases} (0, \pm 4) & \text{if } E : y^2 = x^3 + 16 \text{ for any } d, \\ (-4, \pm 4\sqrt{-3}), (-4\omega, \pm 4\sqrt{-3}) \text{ and } (-4\omega^2, \pm 4\sqrt{-3}) & \text{if } E : y^2 = x^3 + 16 \text{ and } d = -3, \\ (12, \pm 36) & \text{if } E : y^2 = x^3 - 432 \text{ for any } d, \\ (0, \pm 12\sqrt{-3}), (12\omega, \pm 36) \text{ and } (12\omega^2, \pm 36) & \text{if } E : y^2 = x^3 - 432 \text{ and } d = -3, \\ (0, \pm t\sqrt{2t}) & \text{if } E : y^2 = x^3 + 2t^3 \text{ with } t \neq 2 \text{ and } d \text{ is squarefree part of } 2t, \\ (-2t, \pm t\sqrt{-6t}) & \text{if } E : y^2 = x^3 + 2t^3 \text{ with } t \neq -6 \text{ and } d \text{ is squarefree part of } -6t. \end{cases}$$

Proof. We have already noted that a point of order 3 exists if and only if $x(x^3 + 4c) = 0$. If $x = 0$, then $y = \pm\sqrt{c} = \pm t\sqrt{2t}$. If $2t$ is a square, then $t = 2$ as t is square-free. In this case, $(0, \pm 4)$ are points of order 3 for any d. If $2t$ is not a square, then $(0, \pm t\sqrt{2t})$ are points of order 3 for d as a square-free part of $2t$.

If $x \neq 0$, then $x^3 = -4c = -8t^3$ and hence $x = -2t, -2t\omega, -2t\omega^2$ where ω is a third root of unity. In this case, $y = \pm\sqrt{-3c} = \pm t\sqrt{-6t}$. If $d = -3$ and $t = -6$, we have 8 points of order 3. If $-6t$ is a square, then $t = -6$ as t is square-free. In this case, $(12, \pm 36)$ are points of order 3 for any d. If $-6t$ is not a square, then $(12, \pm t\sqrt{-6t})$ are points of order 3 for d as a square-free part of $-6t$. If $d = -3$ and $t = 2$, we have 8 points of order 3.

Combining all the cases, we get the desired result. □

2.4 Proof of Theorem 2.2.1

By Lemma 2.3.1, Lemma 2.3.2 and Lemma 2.3.5, we see that, the only possible orders for the nontrivial tosion points in T are $2, 3$ and 6..

Case 1. (c is a cube and a square)

If c is a cube and a square, then $c = 1$ as c is 6-th power free. Hence, $(0, \pm 1)$ are the only points of order 3 in T by Lemma 2.3.4 and $(1, 0)$ is the only point of order 2 in T by Lemma 2.3.3. Since T is abelian, it has an element of order 6. Hence, $T \cong \mathbb{Z}/6\mathbb{Z}$.

Case 2. (c is a cube, but not a square)

Since c is a cube, but not a square, we can write $c = a^3$ for some nonzero square-free integer $a \neq 1$. In this case, the point $(-a, 0)$ is the only element of order 2 in T by Lemma 2.3.3. There does not exist any element of order 3 in T by Lemma 2.3.4. Hence in this case, $T \cong \mathbb{Z}/2\mathbb{Z}$.

Case 3. (c is a square, but not a cube)

Suppose c is a square, say, $c = a^2$ for some nonzero integer $a \neq 1$. In this case, there does not exist any element of order 2 in T by Lemma 2.3.3. Also $(0, \pm a)$ are the only points of order 3 in T by Lemma 2.3.4. Hence, in this case, $T \cong \mathbb{Z}/3\mathbb{Z}$.

Case 4. (c is neither a square nor a cube)

In this case, there does not exist any element of order 2 in T by Lemma 2.3.3. If $c = -432$, then $(12, \pm 36)$ are the only elements of order 3 in T by Lemma 2.3.4. So for $c = -432$, $T \cong \mathbb{Z}/3\mathbb{Z}$. For $c \neq -432$, there does not exist any element of order 3 in T by Lemma 2.3.4. Hence $T = \{\mathcal{O}\}$.

Thus combining all the cases, Theorem 2.2.1 follows.

2.5 Proof of Theorem 2.2.2

By Lemma 2.3.6, Lemma 2.3.7 and Lemma 2.3.8, we see that, the only possible orders for the nontrivial tosion points in T are $2, 3$ and 6.

Case 1. (c is a cube and a square)

If c is a cube and square, then $c = 1$ as c is 6-th power free.

If $d \neq -3$, then $(0, \pm 1)$ are the only points of order 3 by Lemma 2.3.10 and $(1, 0)$ is the only point of order 2 by Lemma 2.3.9. Since T is abelian, it has an element of order 6. Hence, we conclude that $T \cong \mathbb{Z}/6\mathbb{Z}$.

If $d = -3$, then, $(0, \pm 1)$ are the only points of order 3 by Lemma 2.3.10 and $(1, 0), (\omega, 0), (\omega^2, 0)$ are the only points of order 2 in T by by Lemma 2.3.9. Since T is abelian, it has an element of order 6. Hence, in this case, $T \cong \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Case 2. (c is a cube, but not a square)

Since c is a cube, but not a square, we write $c = a^3$ for some nonzero square-free integer $a \neq 1$. Then, $(0, \pm a\sqrt{a})$ are the only points of order 3 over $\mathbb{Q}(\sqrt{a})$ by Lemma 2.3.10.

For $d = -3$, the points $(-a, 0), (-a\omega, 0), (-a\omega^2, 0)$ are the only points of order 2 over $\mathbb{Q}(\sqrt{-3})$ by Lemma 2.3.9. If $a \neq -3$, then there does not exist any element of order 3 over $\mathbb{Q}(\sqrt{-3})$ by Lemma 2.3.10. Hence, in this case, T is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. If $a = -3$, then $c = -27$. In that case, the points $(0, \pm 3\sqrt{-3})$ are the only points of order 3 over $\mathbb{Q}(\sqrt{-3})$ by Lemma 2.3.10. Since T is abelian, it has an element of order 6. Hence, in this case, $T \cong \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

If $d \neq -3$, then the points $(0, \pm a\sqrt{a})$ are the only points of order 3 over $\mathbb{Q}(\sqrt{a})$ by Lemma 2.3.10 and $(-a, 0)$ is the only point of order 2 in T by Lemma 2.3.9. For $d = a$, T has an element of order 6. Hence, in this case, $T \cong \mathbb{Z}/6\mathbb{Z}$. For $d \neq a$, there does not exist any element of order 3 in T by Lemma 2.3.10. In this case, the point $(-a, 0)$ is the only element of order 2 in T. Hence, in this case $T \cong \mathbb{Z}/2\mathbb{Z}$.

Case 3. (c is a square, but not a cube)

If $c = 2t^3$ for some square-free integer t, then $c = 16$ as c is a square.

In this case, for $d = -3$, there does not exist any element of order 2 over $\mathbb{Q}(\sqrt{-3})$ by Lemma 2.3.9. But T has 8 points of order 3 over $\mathbb{Q}(\sqrt{-3})$ by Lemma 2.3.11. Hence, $T \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

If $d \neq -3$, then the points $(0, \pm 4)$ are the only points of order 3 over $\mathbb{Q}(\sqrt{d})$ by Lemma 2.3.11. Hence, in this case, $T \cong \mathbb{Z}/3\mathbb{Z}$.

If $c \neq 2t^3$ for any integer t, then we write $c = a^2$ for some integer a. Therefore, for any square-free integer d, the points $(0, \pm a)$ are the only points of order 3 over $\mathbb{Q}(\sqrt{d})$ by Lemma 2.3.10. Also there does not exist any element of order 2 by Lemma 2.3.9. Hence, in this case, $T \cong \mathbb{Z}/3\mathbb{Z}$.

Case 4. (c is neither a square nor a cube)

If $c = 2t^3$ for some square-free integer t, then $t \neq 2$ as c is not a square.

There does not exist any element of order 2 in T by Lemma 2.3.9. Now by Lemma 2.3.11, we conclude that for $t = -6$, T is isomorphic to $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ for $d = -3$ and T is isomorphic to $\mathbb{Z}/3\mathbb{Z}$ for $d \neq -3$. Also for $t \neq -6$, $T \cong \mathbb{Z}/3\mathbb{Z}$, if d is a square-free part of $2t$ or $-6t$ by Lemma 2.3.11.

If $c \neq 2t^3$ for any integer t, then there does not exist any element of order 2 in T by Lemma 2.3.9 and $(0, \pm\sqrt{c})$ are the only points of order 3 over $\mathbb{Q}(\sqrt{d})$ where d is the square-free part of c by Lemma 2.3.10. Hence, in this case, $T \cong \mathbb{Z}/3\mathbb{Z}$.

Thus combining all the cases, Theorem 2.2.2 follows.

Chapter 3

Arithmetic progressions on Elliptic curves

This chapter is devoted to finding an upper bounds for the lengths of sequences of rational points on curves of the type $y^2 = x^3 + k, k \in \mathbb{Q} \setminus \{0\}$, such that the ordinates of the points are in arithmetic progression, and also when both the abscissae and the ordinates of the points are separately the terms of two arithmetic progressions.

3.1 Introduction

Arithmetic progressions on algebraic curves is an area which is being studied recently by many authors. Let E be an algebraic curve over $\mathbb{Q}$.

Definition 3.1.1. A set of rational numbers $x_1, \ldots, x_n$ are said to be in *arithmetic progression of length* n over $\mathbb{Q}$ if there exists a non-zero rational number d such that $x_i = x_1 + (i-1)d$ for all $i = 1, 2, \ldots, n$, where d is called the *common difference*. The rational points $P_1, P_2, \ldots, P_n$ on E are said to be in *x-arithmetic progression* of length n (respectively, *y-arithmetic progression*) over $\mathbb{Q}$ if their x-coordinates (respectively, y-coordinates) are in arithmetic progression of length n over $\mathbb{Q}$.

Definition 3.1.2. The rational points $P_1, P_2, \ldots, P_n$ on E are said to be in *simultaneous arithmetic progression* of length n if both x-coordinates and y-coordinates simultaneously

are in arithmetic progression of length n over $\mathbb{Q}$, where permutation of y-coordinates is allowed.

Let $S_x(E)$ (respectively, $S_y(E)$) denote the maximal length of x-arithmetic progression (respectively, y-arithmetic progression) over $\mathbb{Q}$ on the elliptic curve E. Also, let $S_{x,y}(E)$ denote the maximal length of simultaneous arithmetic progression over $\mathbb{Q}$ on the elliptic curve E.

Bremner [12] and Campbell [14] studied the arithmetic progressions of rational points on elliptic curves with Weierstrass equation. MacLeod [45] and Ulas [70] have considered the arithmetic progressions of rational points on quartic models. Moody [50], Bremner [10], and González-Jiménez [28] have studied a similar problem on the Edwards curves. Also Moody [51] and Choudhry [16] have dealt with arithmetic progressions on the Huff curves. On higher genus elliptic curves, such questions were studied by Alvarado [2], Ulas ([71], [72]). Also, García-Selfa and Tornero [26] have studied the y-arithmetic progressions and the simultaneous arithmetic progressions on elliptic curves. More precisely, the known results which are needed for our purposes are as follows.

Theorem 3.1.1 (García-Selfa and Tornero [26])**.** *There exist infinitely many elliptic curves E over $\mathbb{Q}$ with $S_{x,y}(E) \geq 5$.*

Theorem 3.1.2 (García-Selfa and Tornero [26])**.** *There exist infinitely many elliptic curves E over $\mathbb{Q}$ with $S_y(E) \geq 7$.*

In 1975, Mohanty [48] studied the integral points on the elliptic curve $y^2 = x^3+k$ which are forming arithmetic progression with difference 1. Also in 1980, He [49] conjectured the following.

Conjecture 3.1.1. *Let $E : y^2 = x^3 + k$ be an elliptic curve for some $k \in \mathbb{Q}$. Then $S_x(E) \leq 4$.*

In 1992, Lee and Vélez [40] proved the following result.

Theorem 3.1.3 (Lee and Vélez [40])**.** *There are infinitely many elliptic curves of the form $E := y^2 = x^3 + k$ with $k \in \mathbb{Q}$ for which $S_x(E) \geq 4$ and $S_y(E) \geq 6$ hold.*

3.2 The main results

We shall state the main results [20] of this chapter which deals with the upper bounds for $S_{x,y}(E)$ and $S_y(E)$ for the elliptic curve $E : y^2 = x^3 + k$ with $k \in \mathbb{Q}^*$. Indeed, we prove the following results.

Theorem 3.2.1. *Let $E : y^2 = x^3 + k$ be an elliptic curve for some $k \in \mathbb{Q}$. Then $S_{x,y}(E) \leq 3$. Moreover, there exist infinitely many elliptic curves $E : y^2 = x^3 + k$ with $S_{x,y}(E) = 3$.*

Theorem 3.2.2. *Let $E : y^2 = x^3+k$ be an elliptic curve for some $k \in \mathbb{Q}$. Then $S_y(E) \leq 6$. Moreover, there exist infinitely many elliptic curves $E : y^2 = x^3 + k$ with $S_y(E) = 6$.*

3.3 Preliminaries

Bremner gave a rational parametrization for the cubic surface $x^3 + y^3 + cz^3 = c$ with $c \neq 1$. This parametrization is very much essential to prove Theorem 3.2.2.

Theorem 3.3.1 (Bremner, [11])**.** *The general rational solutions of the surface*

$$x^3 + y^3 + cz^3 = c \text{ with } c \neq 1 \tag{3.1}$$

are given, up to symmetry, by

$$(i)\ (\lambda, -\lambda, 1) \text{ and } (ii)\left(\frac{9}{c}\lambda^4 - 3\lambda, -\frac{9}{c}\lambda^4, \frac{9}{c}\lambda^3 - 1\right)$$

with $\lambda \in \mathbb{Q}$. *Moreover, if* $c = 2$, *we have,*

$$\begin{aligned}(iii)\ (x,y,z) =& (-4\lambda^2+6\lambda-1, -4\lambda^2+2\lambda+1, 4\lambda^2-4\lambda+1);\\ (iv)\ (x,y,z) =& \left(\frac{2}{27}(4\lambda^4-4\lambda^3-6\lambda^2+17\lambda-2)\ ,\right.\\ & \frac{4}{27}(2\lambda^4-8\lambda^3+6\lambda^2+4\lambda-13),\\ & \left.\frac{-1}{27}(8\lambda^4-20\lambda^3+24\lambda^2+16\lambda-37)\right)\end{aligned} \tag{3.2}$$

with $\lambda \in \mathbb{Q}$, *are the additional solutions.*

3.4 Proof of Theorem 3.2.1

Let d and d' be given nonzero rational numbers. Suppose $P_1 = (x_1, y_1)$ is a rational point on $E : y^2 = x^3 + k$ for some $k \in \mathbb{Q}$. Therefore, P_1 satisfies

$$y_1^2 = x_1^3 + k. \tag{3.3}$$

Suppose P_2 and P_3 are other rational points on E such that P_1, P_2 and P_3 form a simultaneous arithmetic progression with differences d and d' of length 3. Therefore, we let $P_2 = (x_1 + d, y_1 + d')$ and $P_3 = (x_1 - d, y_1 - d')$ and we get,

$$(y_1 + d')^2 = (x_1 + d)^3 + k \tag{3.4}$$

and

$$(y_1 - d')^2 = (x_1 - d)^3 + k. \tag{3.5}$$

By subtracting (3.5) from (3.4), we get,

$$4y_1d' = 6x_1^2d + 2d^3. \tag{3.6}$$

From (3.3) and (3.4), we get,

$$2y_1d' + d'^2 = 3x_1^2d + 3x_1d^2 + d^3. \tag{3.7}$$

Therefore, from (3.6) and (3.7), we get,

$$2d'^2 = 6x_1d^2 \iff x_1 = \frac{1}{3}\frac{d'^2}{d^2}. \tag{3.8}$$

Once we get x_1 as a function of d and d', we can get y_1 and k as a function of d and d'. Since this is true for a given non-zero rational numbers d and d', we conclude that there are infinitely many elliptic curves E of the form $y^2 = x^3 + k$ which admits $S_{x,y}(E) \geq 3$.

In order to finish the proof of the theorem, now it is enough to prove that $S_{x,y}(E) \leq 3$ for all elliptic curves $E : y^2 = x^3 + k$.

Let E be one such curve. If possible, let P_1, P_2, P_3 and P_4 be the rational points on E which form a simultaneous arithmetic progression of length 4 with some differences d and d' for the x and y coordinates respectively. Now, we need to consider several cases depending on the arrangement of coordinates of P_i's.

Case 1: $P_1 = (x_1-d, y_1-d'), P_2 = (x_1, y_1), P_3 = (x_1+d, y_1+d')$ and $P_4 = (x_1+2d, y_1+2d')$

Since P_1, P_2 and P_3 are in simultaneous arithmetic progression, by the previous discussion, we conclude that $x_1 = \frac{1}{3}\frac{d'^2}{d^2}$. Since P_4 is a rational point on E, we get

$$(y_1 + 2d')^2 = (x_1 + 2d)^3 + k. \tag{3.9}$$

From the equations (3.9) and (3.3), we get,

$$4y_1d' + 4d'^2 = 6x_1^2d + 12x_1d^2 + 8d^3. \tag{3.10}$$

Now, by putting $x_1 = d'^2/3d^2$ in (3.10), we arrive at $d = 0$, which is a contradiction. Thus, we conclude, in this case, $S_{x,y}(E) \leq 3$.

Case 2: $P_1 = (x_1, y_1), P_2 = (x_1+d, y_1+d'), P_3 = (x_1+2d, y_1+3d'), P_4 = (x_1+3d, y_1+2d')$

Since these are rational points on E, we have,

$$y_1^2 = x_1^3 + k. \tag{3.11}$$

$$(y_1 + d')^2 = (x_1 + d)^3 + k, \tag{3.12}$$

$$(y_1 + 3d')^2 = (x_1 + 2d)^3 + k, \tag{3.13}$$

and

$$(y_1 + 2d')^2 = (x_1 + 3d)^3 + k. \tag{3.14}$$

From the equations (3.13), (3.12) and (3.11), we get,

$$6{d'}^2 = -3x_1^2 d + 3x_1 d^2 + 5d^3. \tag{3.15}$$

Again from the equations (3.13), (3.14) and (3.11), we get,

$$6{d'}^2 = -15x_1^2 d - 57x_1 d^2 - 65d^3. \tag{3.16}$$

By combining the equations (3.15) and (3.16), we arrive at

$$6x_1^2 + 30x_1 d + 35d^2 = 0. \tag{3.17}$$

Clearly, the quadratic equation (3.17) in x_1 does not have any rational solutions and hence we conclude, in this case, $S_{x,y}(E) \leq 3$.

The remaining 22 cases can be proved similarly and we list them in the following Table 3.4.1.

From the table, we can see that the discriminant D is not a perfect square for a rational number d in all the cases. Hence, we conclude that x_1 cannot be rational, which is a contradiction. Therefore, in all the cases, we get, $S_{x,y}(E) \leq 3$. This completes the proof of Theorem 3.2.1.

Table 3.4.1

Cases	Points	Final Equation and Discriminant(D)
Case 3	$(x_1, y_1), (x_1 + d, y_1 + 2d')$ $(x_1 + 2d, y_1 + d'), (x_1 + 3d, y_1 + 3d')$	$3x_1^2 + 9x_1d + 8d^2 = 0$ D $= -15d^2$
Case 4	$(x_1, y_1), (x_1 + d, y_1 + 2d')$ $(x_1 + 2d, y_1 + 3d'), (x_1 + 3d, y_1 + d')$	$24x_1^2 + 84x_1d + 86d^2 = 0$ D $= -1200d^2$
Case 5	$(x_1, y_1), (x_1 + d, y_1 + 3d')$ $(x_1 + 2d, y_1 + d'), (x_1 + 3d, y_1 + 2d')$	$3x_1^2 + 14x_1d + 28d^2 = 0$ D $= -140d^2$
Case 6	$(x_1, y_1), (x_1 + d, y_1 + 3d')$ $(x_1 + 2d, y_1 + 2d'), (x_1 + 3d, y_1 + d')$	$6x_1^2 + 24x_1d + 29d^2 = 0$ D $= -120d^2$
Case 7	$(x_1, y_1 + d'), (x_1 + d, y_1 + 2d'),$ $(x_1 + 2d, y_1), (x_1 + 3d, y_1 + 3d')$	$3x_1^2 - 3x_1d - 8d^2 = 0$ D $= 105d^2$
Case 8	$(x_1, y_1 + d'), (x_1 + d, y_1 + 2d'),$ $(x_1 + 2d, y_1 + 3d'), (x_1 + 3d, y_1)$	$6x_1^2 + 12x_1d + 11d^2 = 0$ D $= -120d^2$
Case 9	$(x_1, y_1 + d'), (x_1 + d, y_1)$ $(x_1 + 2d, y_1 + 2d'), (x_1 + 3d, y_1 + 3d')$	$6x_1^2 + 6x_1d - d^2 = 0$ D $= 60d^2$
Case 10	$(x_1, y_1 + d'), (x_1 + d, y_1)$ $(x_1 + 2d, y_1 + 3d'), (x_1 + 3d, y_1 + 2d')$	$12x_1^2 + 36x_1d + 37d^2 = 0$ D $= -480d^2$
Case 11	$(x_1, y_1 + d'), (x_1 + d, y_1 + 3d')$ $(x_1 + 2d, y_1), (x_1 + 3d, y_1 + 2d')$	$15x_1^2 + 45x_1d + 44d^2 = 0$ D $= -615d^2$
Case 12	$(x_1, y_1 + d'), (x_1 + d, y_1 + 3d')$ $(x_1 + 2d, y_1 + 2d'), (x_1 + 3d, y_1)$	$12x_1^2 + 30x_1d + 25d^2 = 0$ D $= -300d^2$
Case 13	$(x_1, y_1 + 2d'), (x_1 + d, y_1)$ $(x_1 + 2d, y_1 + d'), (x_1 + 3d, y_1 + 3d')$	$12x_1^2 + 30x_1d + 25d^2 = 0$ D $= -300d^2$
Case 14	$(x_1, y_1 + 2d'), (x_1 + d, y_1)$ $(x_1 + 2d, y_1 + 3d'), (x_1 + 3d, y_1 + d')$	$15x_1^2 + 45x_1d + 44d^2 = 0$ D $= -615d^2$
Case 15	$(x_1, y_1 + 2d'), (x_1 + d, y_1 + d')$ $(x_1 + 2d, y_1), (x_1 + 3d, y_1 + 3d')$	$6x_1^2 + 12x_1d + 11d^2 = 0$ D $= -120d^2$
Case 16	$(x_1, y_1 + 2d'), (x_1 + d, y_1 + d')$ $(x_1 + 2d, y_1 + 3d'), (x_1 + 3d, y_1)$	$3x_1^2 - 3x_1d - 8d^2 = 0$ D $= 105d^2$
Case 17	$(x_1, y_1 + 2d'), (x_1 + d, y_1 + 3d')$ $(x_1 + 2d, y_1), (x_1 + 3d, y_1 + d')$	$12x_1^2 + 36x_1d + 37d^2 = 0$ D $= -480d^2$
Case 18	$(x_1, y_1 + 2d'), (x_1 + d, y_1 + 3d')$ $(x_1 + 2d, y_1 + d'), (x_1 + 3d, y_1)$	$6x_1^2 + 6x_1d - d^2 = 0$ D $= 60d^2$
Case 19	$(x_1, y_1 + 3d'), (x_1 + d, y_1)$ $(x_1 + 2d, y_1 + d'), (x_1 + 3d, y_1 + 2d')$	$6x_1^2 + 24x_1d + 29d^2 = 0$ D $= -120d^2$
Case 20	$(x_1, y_1 + 3d'), (x_1 + d, y_1)$ $(x_1 + 2d, y_1 + 2d'), (x_1 + 3d, y_1 + d')$	$3x_1^2 + 21x_1d + 28d^2 = 0$ D $= 105d^2$
Case 21	$(x_1, y_1 + 3d'), (x_1 + d, y_1 + d')$ $(x_1 + 2d, y_1), (x_1 + 3d, y_1 + 2d')$	$12x_1^2 + 42x_1d + 43d^2 = 0$ D $= -300d^2$
Case 22	$(x_1, y_1 + 3d'), (x_1 + d, y_1 + d')$ $(x_1 + 2d, y_1 + 2d'), (x_1 + 3d, y_1)$	$9x_1^2 + 27x_1d + 24d^2$ D $= -135d^2$
Case 23	$(x_1, y_1 + 3d'), (x_1 + d, y_1 + 2d')$ $(x_1 + 2d, y_1), (x_1 + 3d, y_1 + d')$	$6x_1^2 + 30x_1d + 35d^2$ D $= 60d^2$
Case 24	$(x_1, y_1 + 3d'), (x_1 + d, y_1 + 2d')$ $(x_1 + 2d, y_1 + d'), (x_1 + 3d, y_1)$	We arrive at $d = 0$.

3.5 Proof of Theorem 3.2.2

In order to prove Theorem 3.2.2, we need to construct infinitely many elliptic curves $E : y^2 = x^3 + k$ which admit $S_y(E) \geq 6$. Then we need to prove $S_y(E) \leq 6$ for all elliptic curves $E : y^2 = x^3 + k$.

Let r and d be two given nonzero rational numbers and we let $k = r^2 - d^3$. Since $r^2 = d^3 + k$, we see that $(d, \pm r)$ is a rational point on $E : y^2 = x^3 + k$. For some rational numbers x_1 and x_2, we suppose that $(x_1, \pm 3r)$ and $(x_2, \pm 5r)$ are rational points on E. Then we have $(d, \pm r), (x_1, \pm 3r)$ and $(x_2, \pm 5r)$ are the rational points on E forming an y-arithmetic progression of length 6. Therefore, we get,

$$8r^2 + d^3 = x_1^3, \quad 24r^2 + d^3 = x_2^3. \tag{3.18}$$

Hence,

$$16r^2 = x_2^3 - x_1^3 \tag{3.19}$$

and

$$2d^3 = 3x_1^3 - x_2^3. \tag{3.20}$$

Putting $X_1 = \dfrac{x_1}{d}$ and $X_2 = \dfrac{x_2}{d}$ in (3.20), we get,

$$3X_1^3 - X_2^3 = 2. \tag{3.21}$$

Note that the point $\left(\dfrac{1}{4}, \dfrac{-5}{4}\right)$ satisfies the equation (3.21) and hence we get,

$$x_1 = \frac{d}{4} \text{ and } x_2 = \frac{-5d}{4}.$$

By putting the values of x_1 and x_2 in (3.19), we get,

$$2^{10}r^2 = -126d^3. \tag{3.22}$$

Note that the equation (3.22) allows us to parameterize as follows. Choose any rational

number $q \in \mathbb{Q}^*$ and put $d = -14q^2$. Then, by (3.22), we get, $r = \pm\frac{147}{8}q^3$. Hence

$$k = r^2 - d^3 = \frac{197225}{64}q^6. \tag{3.23}$$

Thus, for any given rational number $q \in \mathbb{Q}^*$, we can find rational numbers d, r and k satisfying (3.23). This proves that there are infinitely many $E : y^2 = x^2 + k$ that admit $S_y(E) \geq 6$.

Next we shall prove that $S_y(E) \leq 6$ for all elliptic curve $E : y^2 = x^3 + k$.

Let $E : y^2 = x^3 + k$ be a given elliptic curve. Suppose E has 7 rational points which form an y-arithmetic progression with difference d for some $d \in \mathbb{Q}^*$. Without loss of generality, we may assume that these points are as follows.

$$P_1 = (x_1, y_1), P_2 = (x_2, y_1 + d), P_3 = (x_3, y_1 - d), P_4 = (x_4, y_1 + 2d),$$

$$P_5 = (x_5, y_1 - 2d), P_6 = (x_6, y_1 + 3d) \text{ and } P_7 = (x_7, y_1 - 3d).$$

Thus we have,

$$y_1^2 = x_1^3 + k, \tag{3.24}$$

$$(y_1 + d)^2 = x_2^3 + k, \tag{3.25}$$

$$(y_1 - d)^2 = x_3^3 + k, \tag{3.26}$$

$$(y_1 + 2d)^2 = x_4^3 + k, \tag{3.27}$$

$$(y_1 - 2d)^2 = x_5^3 + k, \tag{3.28}$$

$$(y_1 + 3d)^2 = x_6^3 + k, \tag{3.29}$$

and

$$(y_1 - 3d)^2 = x_7^3 + k. \tag{3.30}$$

From these equations, we can create the following equations;

$$4y_1 d = x_2^3 - x_3^3, \tag{3.31}$$

$$8y_1d = x_4^3 - x_5^3, \tag{3.32}$$

$$12y_1d = x_6^3 - x_7^3. \tag{3.33}$$

Case 1: $y_1 \neq 0$.

In this case, from (3.32), we conclude that either $x_4 \neq 0$ or $x_5 \neq 0$, as $d \neq 0$. Without loss of generality, we assume that $x_5 \neq 0$.

From the equations (3.31) and (3.32), we can get,

$$\begin{aligned} 2(x_2^3 - x_3^3) = x_4^3 - x_5^3 &\iff -8x_2^3 + 8x_3^3 + 4x_4^3 = 4x_5^3 \\ \iff \left(\frac{-2x_2}{x_5}\right)^3 + \left(\frac{2x_3}{x_5}\right)^3 + 4\left(\frac{x_4}{x_5}\right)^3 = 4 &\iff X^3 + Y^3 + 4Z^3 = 4 \end{aligned} \tag{3.34}$$

where $X = \dfrac{-2x_2}{x_5}, Y = \dfrac{2x_3}{x_5}$ and $Z = \dfrac{x_4}{x_5}$.

Now from the equations (3.33) and (3.32), we can get,

$$\begin{aligned} 2(x_7^3 - x_6^3) = 3(x_5^3 - x_4^3) &\iff 8x_7^3 - 8x_6^3 + 12x_4^3 = 12x_5^3 \\ \iff \left(\frac{2x_7}{x_5}\right)^3 + \left(\frac{-2x_6}{x_5}\right)^3 + 12\left(\frac{x_4}{x_5}\right)^3 = 12 &\iff U^3 + V^3 + 12W^3 = 12 \end{aligned} \tag{3.35}$$

where $U = \dfrac{2x_7}{x_5}, V = \dfrac{-2x_6}{x_5}$ and $W = \dfrac{x_4}{x_5}$.

By Theorem 3.3.1, up to symmetry, all the rational solutions of (3.34) are given by

$$(i)\ (\lambda, -\lambda, 1) \text{ and } \ (ii)\left(\frac{9}{4}\lambda^4 - 3\lambda, -\frac{9}{4}\lambda^4, \frac{9}{4}\lambda^3 - 1\right)$$

with $\lambda \in \mathbb{Q}$.

Again, by Theorem 3.3.1, up to symmetry, all the rational solutions of (3.35) are given by

$$(i)\ (\mu, -\mu, 1) \text{ and } \ (ii)\left(\frac{3}{4}\mu^4 - 3\mu, -\frac{3}{4}\mu^4, \frac{3}{4}\mu^3 - 1\right)$$

with $\mu \in \mathbb{Q}$.

Note that from the equations (3.34) and (3.35), we see that,

$$Z = W = \frac{x_4}{x_5}.$$

Therefore, we get either

$$\frac{9}{4}\lambda^3 - 1 = 1$$

or

$$\frac{3}{4}\mu^3 - 1 = 1$$

or

$$\frac{9}{4}\lambda^3 - 1 = \frac{3}{4}\mu^3 - 1$$

or

$$Z = W = 1.$$

However, it is easy to see that first three equality cannot happen with $\lambda, \mu \in \mathbb{Q}$ and hence, we get,

$$Z = W = 1 \implies x_4 = x_5.$$

Therefore, from the equations (3.27) and (3.28), we can get,

$$(y_1 + 2d) = \pm(y_1 - 2d).$$

Since $d \neq 0$, we conclude that $y_1 = 0$, which is a contradiction. Hence, in this case, we have, $S_y(E) \leq 6$.

Case 2: $y_1 = 0$.

Let the rational points forming y-arithmetic progression of length 7 be

$$P_1 = (x_1, 0), P_2 = (x_2, d), P_3 = (x_3, -d), P_4 = (x_4, 2d),$$

$$P_5 = (x_5, -2d), P_6 = (x_6, 3d), P_7 = (x_7, -3d),$$

for some non-zero rational number d. Therefore, one gets $k = (-x_1)^3, x_2 = x_3$, and $x_6 = x_7$. Moreover, we get,

$$d^2 = x_2^3 - x_1^3, \tag{3.36}$$

$$4d^2 = x_4^3 - x_1^3, \tag{3.37}$$

and

$$9d^2 = x_6^3 - x_1^3. \tag{3.38}$$

Since $k \neq 0$, we conclude that $x_1 \neq 0$.

Now from the equations (3.38), (3.37) and (3.36), we get,

$$\begin{aligned} x_6^3 - x_4^3 = 5(x_2^3 - x_1^3) &\iff \left(\frac{x_4}{x_1}\right)^3 + \left(\frac{-x_6}{x_1}\right)^3 + 5\left(\frac{x_2}{x_1}\right)^3 = 5 \\ &\iff L^3 + M^3 + 5N^3 = 5 \end{aligned} \tag{3.39}$$

where $L = \dfrac{x_4}{x_1}, M = \dfrac{-x_6}{x_1}$ and $N = \dfrac{x_2}{x_1}$. Therefore, by Theorem 3.3.1, up to symmetry, all the rational solutions of the equation (3.39) are given by

$$(i)\ (\nu, -\nu, 1) \text{ and } \ (ii)\left(\frac{9}{5}\nu^4 - 3\nu, -\frac{9}{5}\nu^4, \frac{9}{5}\nu^3 - 1\right),$$

with $\nu \in \mathbb{Q}$.

Note that since $d \neq 0$, we see that $N \neq 1$ in (3.39). Since $x_1 \neq 0$, we let $x_1 = q \in \mathbb{Q}^*$. Then, we get,

$$x_2 = \left(\frac{9}{5}\nu^3 - 1\right)q,\ x_4 = \left(\frac{9}{5}\nu^4 - 3\nu\right)q \text{ and } x_6 = \left(\frac{9}{5}\nu^4\right)q.$$

Now, substitute the values of x_2 and x_6 in the equations (3.36) and (3.38) and we get,

$$d^2 = \left[\left(\frac{9}{5}\nu^3 - 1\right)^3 - 1\right]q^3,$$

and

$$9d^2 = \left[\left(\frac{9}{5}\nu^4\right)^3 - 1\right] q^3.$$

Since LHS of (3.38) is equal to nine times LHS of (3.36), we get,

$$9\left[\left(\frac{9}{5}\nu^3 - 1\right)^3 - 1\right] = \left[\left(\frac{9}{5}\nu^4\right)^3 - 1\right],$$

which is equivalent to,

$$9(9t-5)^3 = 9^3t^4 + 1000,$$

with $\nu^3 = t$.

By putting $s = 3t$, we get the equation,

$$9s^4 - 243s^3 + 1215s^2 - 2025s + 2125 = 0. \tag{3.40}$$

By the rational root theorem, we conclude that (3.40) does not have any rational solutions. Hence our assumption that $S_y(E) \geq 7$ is wrong. Therefore, we have $S_y(E) \leq 6$ for all the elliptic curves $E : y^2 = x^3 + k$. □

Chapter 4

Perfect powers in a product of terms of some number sequences

This chapter is devoted to finding out the perfect powers in a product of terms which are coming from certain number sequences like sequnce of balancing numbers and Lucas balancing numbers. Also this chapter gives information about solving a recent conjecture on Diophantine equation using properties of Lucas balancing numbers.

4.1 Introduction

Definition 4.1.1. Let P and Q be non zero integers with $P^2 + 4Q \neq 0$. Let α and β be the roots of the equation

$$x^2 - Px - Q = 0. \tag{4.1}$$

Let α and β be the roots of the quadratic equation (4.1) in $\mathbb{C}$. Now, we define the following in terms of the roots α and β by

$$U_n(P,Q) = \frac{\alpha^n - \beta^n}{\alpha - \beta} \text{ and } V_n(P,Q) = \alpha^n + \beta^n, \quad \text{for all } n = 0, 1, \cdots \tag{4.2}$$

The sequence $\{U_n(P,Q)\}_n$ is called the *Lucas sequence of the first kind* and the sequence $\{V_n(P,Q)\}_n$ is called as the *Lucas sequence of the second kind*.

Example 4.1.1. The Fibonacci sequence $(F_n)_{n\geq 0}$ is an example of the Lucas sequence of

the first kind with $(P, Q) = (1, 1)$ and the initial conditions as $F_0 = 0$ and $F_1 = 1$. The Lucas sequence of the second kind for $(P, Q) = (1, 1)$, which is also known as the Lucas sequence, is denoted by $(L_n)_{n\geq 0}$ with the initial conditions $L_0 = 2$ and $L_1 = 1$.

The Pell sequence $(P_n)_{n\geq 0}$ is an example of the first kind Lucas sequence with $(P, Q) = (2, 1)$ and the initial conditions as $P_0 = 0, P_1 = 1$ and the n-th term P_n is known as the n-th *Pell number*. The Lucas-Pell sequence $(Q'_n)_{n\geq 0}$ is an example of the second kind Lucas sequence with $(P, Q) = (2, 1)$ and the initial conditions as $Q'_0 = 2$ and $Q'_1 = 2$. We denote the associated Pell sequence by Q_n with the same recurrence relation as Q'_n and the initial conditions as $Q_0 = 1$ and $Q_1 = 1$. The n-th term Q_n is known as *the n-th associated Pell number*.

Lemma 4.1.1. *The Pell numbers and the associated Pell numbers are related by the following equation*

$$Q_n^2 - 2P_n^2 = \begin{cases} 1 & \text{if } n \text{ is even} \\ -1 & \text{if } n \text{ is odd.} \end{cases} \tag{4.3}$$

Now we introduce another binary number sequence known as the *sequence of balancing numbers* which was originally developed from a Diophantine equation.

Definition 4.1.2. Balancing numbers b are integral solution of the Diophantine equation

$$\sum_{i=1}^{b-1} i = \sum_{j=b+1}^{m} j$$

for some natural number m [4, 25]. Equivalently, the solutions (x, y) of the Pell's equation $8x^2 + 1 = y^2$ are called *the balancing numbers* and the *Lucas balancing numbers* respectively. We discuss these in the following section.

4.1.1 Balancing and Lucas balancing numbers

Let us denote the n-th balancing number and the Lucas balancing number by B_n and C_n respectively. The balancing and the Lucas balancing numbers satisfy (4.1) for $(P, Q) =$

$(6, -1)$. Binet form of the balancing and the Lucas balancing numbers are given by

$$B_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}, \text{ and } C_n = \frac{\alpha^n + \beta^n}{2} \quad \text{for all } n = 0, 1, \cdots, \tag{4.4}$$

where $\alpha = 3 + \sqrt{8}$ and $\beta = 3 - \sqrt{8}$.

Lemma 4.1.2. *The balancing and the Lucas balancing numbers satisfy the following properties (see [57, 58]).*

(1) $B_{2n} = 2B_nC_n$,

(2) $C_n^2 - 8B_n^2 = 1$,

(3) $\gcd(B_m, B_n) = B_{\gcd(m,n)}$,

(4) $C_n = 4P_n^2 + (-1)^n$,

(5) $2B_n = P_{2n}$ *and* $2C_n = Q'_{2n} = 2Q_{2n}$,

(6) $B_{n+1} = 6B_n - B_{n-1}$ *for all integers* $n \geq 2$ *with* $B_0 = 0$ *and* $B_1 = 1$,

(7) $C_{n+1} = 6C_n - C_{n-1}$ *for all integers* $n \geq 2$ *with* $C_0 = 1$ *and* $C_1 = 3$.

Lemma 4.1.3 ([58])**.** *For all integers* $n \geq 0$*, we have*

$$B_n = P_nQ_n \tag{4.5}$$

where P_n *is the* n*-th Pell number and* Q_n *is the* n*-th associated Pell number.*

4.1.2 Perfect powers in binary recurrence sequences

Finding perfect powers in a binary recurrence sequence is an exciting problem in number theory. The Fibonacci numbers which are perfect squares were considered by Cohn [17] and he proved that a Fibonacci number F_n is a square only when $n = 0, 1, 2$ or 12. Later, Pethő [60] and also London - Finkenstein [43] proved that Fibonacci number F_n is a full

cube only when $n = 0, 1, 2$ or 6. Recently, Bugeaud et el.[13] showed that $0, 1, 8$ and 144 are the only perfect powers in the Fibonacci sequence using the Baker's theorem on linear forms in logarithms and the modular method which was used in proof of the Fermat's last theorem. Similar type of results exist for the Pell sequence. For example, Ljunggren [42] showed that a Pell number P_n is a square only if $n = 0, 1$ or 7 and Pethő [61] proved that these are the only perfect powers in Pell sequence. In general, there are several finiteness theorems for perfect powers in any non-degenerate binary recurrence sequences. For example, Pethő [59] and Shorey-Stewart [63] proved independently that there are only finitely many perfect powers with exponent greater than 1 in any non-trivial binary recurrence sequence, which are, in principle, effectively computable. But, for fixed P and Q, finding the perfect powers is a daunting task.

Erdős and Selfridge [23] proved that the product of at least two consecutive integers is never a perfect power. Inspired by this, Luca and Shorey [44] analogously considered the problem of a product of consecutive terms in the Lucas sequence. For any Lucas sequence of the first kind $(U_n)_{n\in\mathbb{N}}$, They proved that

$$U_n U_{n+1} \cdots U_{n+(k-1)} = y^l, \tag{4.6}$$

has only finitely many effectively computable solutions (n, k, y, l) with $n \geq 1, k \geq 2, l \geq 2$ and $y \geq 2$ are integers. In the same paper, they proved that a nonzero product of two or more consecutive Fibonacci numbers is never a perfect power except for the trivial case which is $F_1 \cdot F_2 = 1$. Recently, Bravo et al. [8] explicitly solved a similar problem (4.6) for the Pell and the Lucas-Pell sequences. In fact, they proved that for any positive integers n, d, k with $\gcd(n, d) = 1$ and integers $l \geq 2, y \geq 2$, the equation

$$\prod_{i=0}^{k-1} P_{n+id} = y^l$$

has only two solutions which are $P_7 = 13^2$ and $P_1 \cdot P_7 = 13^2$ and the equation

$$\prod_{i=0}^{k-1} Q'_{n+id} = y^l$$

has no solution.

4.2 The main results

In [21], we prove that there does not exist a non-trivial perfect power in the sequence of balancing numbers as well as in the sequence of the Lucas-balancing numbers. Also, we prove that the Lucas-balancing numbers can not be written as a product of a perfect power and a power of 3 except for $C_1 = 3$. Using this, we prove a conjecture given in [8]. Then, we show that there is no perfect power except the trivial one in the product of balancing numbers as well as in the product of the Lucas-balancing numbers where the indices of the terms are in arithmetic progression. More precisely, the main results of this chapter are the following.

Theorem 4.2.1. *The Diophantine equation $2x^2 + 1 = 3^b y^m$ has no solution in positive integers x, b, y and m, where the integers b and m are even, $y > 1$, and $m > 2$.*

Theorem 4.2.2. *There does not exist an integral solution (n, d, k, y, l) to the Diophantine equation*

$$B_n B_{n+d} \cdots B_{n+(k-1)d} = y^l \tag{4.7}$$

with $n \geq 1, d \geq 1, k \geq 2, y \geq 1$ and $l \geq 2$ are integers and $\gcd(n, d) = 1$.

Theorem 4.2.3. *There does not exist an integral solution (n, d, k, y, l) to the Diophantine equation*

$$C_n C_{n+d} \cdots C_{n+(k-1)d} = y^l \tag{4.8}$$

with $n \geq 1, d \geq 1, k \geq 2, y \geq 1$ and $l \geq 2$ are integers and $\gcd(n, d) = 1$.

4.3 Preliminaries

In this section, we prove some useful Lemmas which are essential to prove the main results. Throughout this chapter, $P(m)$ denotes the greatest prime divisor of a positive integer m, and let $\Delta(n,d,k) = n(n+d)\cdots(n+(k-1)d)$ for given positive integers n, d and k. Also denote $\Delta(n,1,k)$ by $\Delta(n,k)$.

Lemma 4.3.1. *Let $k \geq 3, n \geq 1$ and $d \geq 1$ be integers with $\gcd(n,d) = 1$. Then*

(1) for $n > k$ and $d = 1$, we have $P\Big(\Delta(n,k)\Big) > k$;

(2) for $n \geq 1$ and $d > 1$, we have $P\Big(\Delta(n,d,k)\Big) > k$ unless $(n,d,k) = (2,7,3)$.

Proof. Proof of (1) is due to Sylvester [69] and (2) is due to Shorey and Tijdeman [64]. □

Lemma 4.3.2. *Let $n \geq 1, d > 1$ and $k \geq 6$ be integers with $\gcd(n,d) = 1$. Then there is at least one integer i with $0 \leq i < k$ such that $n + id$ is odd and $P(n+id) > k$.*

Proof. See Theorem 5 in [8]. □

Lemma 4.3.3. *Let $x \geq 3$ be an integer. Then the interval $(2x/3, x]$ contains a prime.*

Proof. See Theorem 2 in [62]. □

Lemma 4.3.4. *Let $n \geq 2$ and $k \geq 2$ be integers with $n \leq 2k$. Then there exists a unique i with $0 \leq i \leq k-1$ such that $n+i$ is prime.*

Proof. Since $n \geq 2$ and $k \geq 2$, we have $n + k - 1 \geq 3$. By Lemma 4.3.3, the interval $\left(\frac{2(n+k-1)}{3}, n+k-1\right]$ contains a prime R(say). If $n \leq 2k-2$, we see that $\frac{2(n+k-1)}{3} = \frac{2n+2k-2}{3} \geq n$. If $n = 2k$, then $\frac{2(n+k-1)}{3} = \frac{2n+2k-2}{3} = n - \frac{2}{3}$. Also if $n = 2k-1$, then $\frac{2(n+k-1)}{3} = \frac{2n+2k-2}{3} = n - \frac{1}{3}$. Putting all together we get

$$R \geq \frac{2(n+k-1)}{3}.$$

Therefore, $2R > \frac{3R}{2} \geq n + k - 1$. Hence there exists a unique i with $0 \leq i \leq k-1$ such that $n + i = R$. □

Lemma 4.3.5 ([39]). *Let $k \geq 2$ be an integer and n be an odd integer with $n > 2k$. Then*

$$P\Big(\prod_{i=0}^{k-1}(n+2i)\Big) > 3.5k$$

unless $(n,k) \in \{(5,2),(7,2),(25,2),(243,2),(9,4),(13,5),(17,6),(15,7),(21,8),(19,9)\}$.

Lemma 4.3.6. *Let $D = 2^a 3^b$ be an integer for some non-negative integers a and b. Then the only solutions to the equation*

$$x^2 - Dy^n = \pm 1 \tag{4.9}$$

in positive integers (x,y,n) with $n \geq 3$ are given by

$$\begin{aligned}(x,y,n,D) =&\{(1,1,n,2),(2,1,n,3),(3,1,n,8),(5,1,n,24),(7,1,n,48),(17,1,n,288),\\ &(3,2,3,1),(5,2,3,3),(7,2,4,3),(17,2,5,9),(239,13,4,2)\}.\end{aligned}$$

Proof. See Corollary 1.4 in [5]. □

4.3.1 Properties of balancing and the Lucas balancing numbers

Lemma 4.3.7. *Let p be an odd prime and let m and n be positive integers with $m \mid n$. If p divides the $gcd\Big(B_m, \frac{B_n}{B_m}\Big)$, then $p \mid \dfrac{n}{m}$.*

Proof. Since $m \mid n$, for some integer t, we have, $n = mt$. Since $p \mid B_m$, using the Binet form for the balancing numbers given in (4.4), we set $(\frac{\alpha}{\beta})^m \equiv 1 \pmod{(p)}$. Now,

$$\begin{aligned}\frac{B_n}{B_m} = \frac{\alpha^n - \beta^n}{\alpha^m - \beta^m} &= \beta^{mt-m}\frac{\left(\frac{\alpha}{\beta}\right)^{mt} - 1}{\left(\frac{\alpha}{\beta}\right)^{m} - 1}\\ &= \beta^{mt-m}\Big[(\frac{\alpha}{\beta})^{m(t-1)} + \left(\frac{\alpha}{\beta}\right)^{m(t-2)} + \cdots + 1\Big]\\ &\equiv t\beta^{mt-m} \pmod{(p)}\end{aligned}$$

Since $p \mid \frac{B_n}{B_m}$, we conclude that $t \equiv 0 \pmod{p}$. Hence the lemma. $\square$

Let $\{U_n\}_{n\in\mathbb{N}}$ be a Lucas sequence of the first kind or the second kind. A positive integer m is called a *primitive divisor* of U_n for some positive integer n, if $m \mid U_n$, but $m \nmid U_i$ for all $i < n$. In [15], Carmichael proved the existence of primitive divisors for a real Lucas sequences. Using this, we have the following lemma.

Lemma 4.3.8 ([15])**.** *Let $n \neq 1, 2, 6$ be a positive integer. Also, let p be an odd prime which is a primitive divisor for B_n. Then, $p \equiv \pm 1 \pmod{n}$.*

Lemma 4.3.9. *Let p be an odd prime and let $e > 0$ be an integer. If $q \mid B_{p^e}$ for some prime q, then $q \geq 2p - 1$.*

Proof. By Lemma 4.1.2(3), for any integer n with $p \nmid n$, we see that $\gcd(B_{p^e}, B_n) = 1$. If $p \mid n$, then $\gcd(B_{p^e}, B_n) = B_{p^f}$ for some integer f with $1 \leq f < e$. Thus, $q \mid B_{p^e}$ implies q is a primitive divisor of B_{p^e} or a primitive divisor of B_{p^f} for some integer f with $1 \leq f < e$. By Lemma 4.3.8, we have $q \equiv \pm 1 \pmod{p^t}$ for some integer t with $1 \leq t \leq e$. Since q is an odd prime, we get $q \equiv \pm 1 \pmod{2p^t}$. Therefore, we have $q \geq 2p^t - 1 \geq 2p - 1$. $\square$

Lemma 4.3.10. *Let $n = R^e p_1^{e_1} \cdots p_r^{e_r}$ be the prime factorization of the integer n where $R = P(n)$ and $p_1, p_2, \cdots, p_r, R$ are distinct primes. Then*

$$\gcd\left(B_{R^e}, \frac{B_n}{B_{R^e}}\right) = 1.$$

Proof. If $R = 2$, then we have $n = R^e$ and $\gcd\left(B_{R^e}, \frac{B_n}{B_{R^e}}\right) = \gcd(B_{R^e}, 1) = 1$. Therefore, we can assume that R is an odd prime. Since R^e is an odd integer, B_{R^e} is odd. Let us assume that an odd prime $q \mid \gcd\left(B_{R^e}, \frac{B_n}{B_{R^e}}\right)$. Then by Lemma 4.3.7, we get $q \mid \frac{n}{R^e} \Rightarrow q \mid p_1^{e_1} \cdots p_r^{e_r}$. Therefore, $q = p_i$ for some i with $1 \leq i \leq r$ and hence $q < R$. Also, since $q \mid B_{R^e}$, by Lemma 4.3.9, we have $q \geq 2R - 1$, which is a contradiction to $q < R$. Thus, there does not exist any prime divisor of $\gcd\left(B_{R^e}, \frac{B_n}{B_{R^e}}\right)$. Hence the lemma follows. $\square$

Lemma 4.3.11. *Let m and n be integers with $n \geq 1$, $m \geq 1$ and $\gcd(m, n) = 1$. Then*

$$\gcd(C_m, C_n) = 3^r$$

for some non-negative integer r.

Proof. Since all the Lucas balancing numbers are odd, 2 is not a prime divisor of $\gcd(C_m, C_n)$. Let p be an odd prime divisor of $\gcd(C_m, C_n)$ and let (p) denote the principal ideal $p\mathbb{Z}[\sqrt{2}]$ in the ring $\mathbb{Z}[\sqrt{2}]$. Then, using Binet form for C_m given in (4.4), we get

$$\alpha^m + \beta^m \equiv 0 \pmod{(p)} \text{ implies } \left(\frac{\alpha}{\beta}\right)^m \equiv -1 \pmod{(p)}.$$

Similarly, $\left(\frac{\alpha}{\beta}\right)^n \equiv -1 \pmod{(p)}$. Since $\gcd(m, n) = 1$, there exist integers r and s such that $mr + ns = 1$. Thus, we have $\left(\frac{\alpha}{\beta}\right)^{mr+ns} \equiv \left(\frac{\alpha}{\beta}\right) \pmod{(p)}$ which implies $(-1)^{r+s} \equiv \left(\frac{\alpha}{\beta}\right) \pmod{(p)}$. Therefore, $\alpha \equiv \pm\beta \pmod{(p)}$. If $\alpha \equiv \beta \pmod{(p)}$, then $4\sqrt{2} \equiv 0 \pmod{(p)}$ which is not possible as $p \neq 2$. If $\alpha \equiv -\beta \pmod{(p)}$, then $6 \in (p)$. Since $p \neq 2$, the only possibility is $p = 3$. Therefore, 3 is the only possible prime divisor of $\gcd(C_m, C_n)$. Thus, $\gcd(C_m, C_n) = 3^r$ for some non-negative integer r. □

Following two properties of the Lucas-Pell Sequences $\{Q_n\}_{n\geq 1}$ will be helpful to calculate the gcd $\left(C_R, \frac{C_n}{C_R}\right)$, where R is the largest prime factor of n.

Lemma 4.3.12 ([8])**.** *For any integer $n \geq 2$, there exists a prime number p which is a primitive divisor of Q_n and $p \equiv \pm 1 \pmod{2n}$.*

Lemma 4.3.13 ([8])**.** *Let m and b be positive integers such that $m \mid n$ and $\frac{n}{m}$ is an odd integer. If a prime number p divides the gcd $\left(Q_m, \frac{Q_n}{Q_m}\right)$, then $p \mid \frac{n}{m}$.*

Lemma 4.3.14. *Let $n > 1$ be a given integer. Let $R = P(n)$ and suppose that n/R is an odd integer. Then*

$$\gcd\left(C_R, \frac{C_n}{C_R}\right) = 3^a$$

for some non-negative integer a.

Proof. Suppose R is an odd prime. Let $p \neq 3$ be an odd prime such that $p \mid \gcd\left(C_R, \frac{C_n}{C_R}\right)$. By Lemma 4.1.2 (5), we conclude that

$$p \mid \gcd\left(\frac{Q'_{2R}}{2}, \frac{Q'_{2n}}{Q'_{2R}}\right) = \left(Q_{2R}, \frac{Q_{2n}}{Q_{2R}}\right).$$

Therefore, by Lemma 4.3.13, we get, $p \mid \dfrac{n}{R}$ as n/R is odd and hence we conclude that $p \leq R$. Also, $p \mid C_R$. If p is not a primitive divisor of C_R, then $p \mid C_i$ for some integer i with $1 \leq i \leq R$. Then, by Lemma 4.3.11, we get $\gcd(C_R, C_i) = 3^b$ for some integer b with $b \geq 0$. This implies $p = 3$, which is a contradiction to our assumption. Thus, p is a primitive divisor of $C_R = Q'_{2R}/2$ and hence by Lemma 4.3.12, we have $p \equiv \pm 1 \pmod{4R}$ which implies $p \geq 4R - 1$, a contradiction to $p \leq R$. Thus, 3 is the only possible prime divisor of $\gcd\left(C_R, \frac{C_n}{C_R}\right)$.

If $R = 2$, then $n = 2^a$ for some positive integer a. Since n/R is an odd integer, we must have $n = 2$. Thus, the desired gcd is 1. Hence the lemma follows. □

4.4 Perfect powers concerning $(B_n)_{n\in\mathbb{N}}$ and $(C_n)_{n\in\mathbb{N}}$

We now show that except for $B_1 = 1$, there is no other perfect powers in the sequence of balancing numbers.

Lemma 4.4.1. *For any positive integers y and $l \geq 2$, the equation*

$$B_m = y^l \tag{4.10}$$

has no solution for all integers $m \geq 2$.

Proof. Suppose there exists an integer $m \geq 2$ for which $B_m = y^l$ for some positive integers y and l with $l \geq 2$. By Lemma 4.1.3, we can write $B_m = P_m Q_m$ where (P_m, Q_m) is a solution of (4.3), that is,

$$Q_m^2 - 2P_m^2 = \pm 1. \tag{4.11}$$

It is clear that $\gcd(P_m, Q_m) = 1$. Since B_m is a perfect power satisfying (4.5), we conclude that $Q_m = y_1^l$ and $P_m = x_1^l$ for some positive coprime integers x_1 and y_1 with $x_1 y_1 = y$. Since, by [61], P_r is a perfect power for $r \geq 2$ if and only if $r = 7$, we conclude that $m = 7$. But, for $m = 7$, we can just compute and see that Q_m is not a perfect power. Hence, $P_m Q_m = B_m$ can not be a perfect power for $m \geq 2$. □

Lemma 4.4.2. *Let n and k be positive integers such that $k < n$. Then the equation*

$$\prod_{i=n}^{n+k-1} B_i = y^l \tag{4.12}$$

has no solution for any integers $y \geq 2$ and $l \geq 2$.

Proof. Since $k < n$, by Lemma 4.3.1(1), the set $\{n, n+1, \cdots, n+k-1\}$ contains an element which has a prime factor R such that $R > k$. If R divides both $(n+i)$ and $(n+j)$ for some integers i and j with $0 \leq i, j \leq k-1$, then $R \mid (i-j)$, which is a contradiction to $|i-j| < k$. Hence, R divides $n+i$ for a unique i with $0 \leq i \leq k-1$. Therefore, $\gcd(R, n+j) = 1$ for all $j = 0, 1, \cdots, k-1$ and $j \neq i$, which implies that

$$\gcd(B_R, B_{n+j}) = B_{\gcd(R,n+j)} = B_1 = 1.$$

Further,

$$\gcd\left(B_R, \prod_{\substack{j=0 \\ j\neq i}}^{k-1} B_{n+j}\right) = 1.$$

Suppose (4.12) has a solution for some integers y and $l \geq 2$. Then

$$\prod_{i=n}^{n+k-1} B_i = B_R \frac{B_{n+i}}{B_R} \cdot \prod_{\substack{j=0 \\ j\neq i}}^{k-1} B_{n+j} = y^l. \tag{4.13}$$

By Lemma 4.3.10 and by the unique factorization in integers, we conclude that $B_R = y_R^l$ for some integer y_R, which is a contradiction to Lemma 4.4.1. □

Lemma 4.4.3. *For any positive integers y and l with $l \geq 2$, the equation*

$$C_n = y^l \tag{4.14}$$

has no solution for integers $n \geq 1$.

Proof. Suppose there exist positive integers y and $l \geq 2$ such that $C_n = y^l$ for some positive integer n. We divide the proof into two cases.

Case I. (l is even).

It is enough to prove the result for $l = 2$. By Lemma 4.1.2(2), we have

$$8B_n^2 = y^4 - 1. \tag{4.15}$$

Multiplying (4.15) by y^2 and putting $s = 2B_n y$ and $r = y^2$, we get $2s^2 = r^3 - r$. Again multiplying this equation by 8 and substituting $Y := 4s$ and $X := 2r$ gives an elliptic curve

$$E : Y^2 = X^3 - 4X. \tag{4.16}$$

Using MAGMA [6], we see that all the integral points (X, Y) satisfying (4.16) are (o, o) and $(\pm 2, 0)$. Hence, $Y = 0$. Therefore, we get either $B_n = 0$ or $C_n = 0$, which is a contradiction, as $n \geq 1$. Thus, C_n can not be a perfect square.

Case II. (l is odd).

By Lemma 4.1.2(4), the equation (4.14) becomes

$$(2P_n)^2 - y^l = \pm 1. \tag{4.17}$$

In Lemma 4.3.6, by taking $D = 1$, we see that for $l \geq 3$ the solution set for (4.17) is $(2P_n, y, l) = (3, 2, 3)$, which is a contradiction as $2P_n \neq 3$. This completes the proof of the lemma. □

Lemma 4.4.4. *For any positive integers y, a and b with $b \geq 2$, the equation*

$$C_n = 3^a \cdot y^b \tag{4.18}$$

has no solution for any integer $n > 1$.

Proof. We will divide the proof into two cases.

Case I. (n is an even integer).

Since $3 \nmid C_2$, by Lemma 4.1.2 (7) (the recurrence relation for C_n), we see that $3 \nmid C_n$. Hence, C_n can not be expressed as $3^a \cdot y^b$.

Case II (n is an odd integer).

We further divide this case into sub cases according to the parity of a and b.

Sub case I. (a and b both are even).

In this case, we can write

$$C_n = \left(3^{\frac{a}{2}} \cdot y^{\frac{b}{2}}\right)^2, \tag{4.19}$$

which is not possible by Lemma 4.4.3.

Sub case II. (a is odd and b is even).

In this case, we can write

$$C_n = 3t^2 \tag{4.20}$$

for some integer t. By Lemma 4.1.2 (2), using the relation $C_n^2 - 8B_n^2 = 1$ in (4.20), we have

$$9t^4 - 8B_n^2 = 1. \tag{4.21}$$

Now, multiplying by t^2 both sides of (4.21) and substituting $r := t^2$ and $s := 2B_n t$, we get

$$2s^2 = 9r^3 - r. \tag{4.22}$$

Again, multiplying by 648 in (4.22) and assuming $Y := 36s$ and $X := 18r$, we get an elliptic curve

$$E : Y^2 = X^3 - 36X. \tag{4.23}$$

Using MAGMA [6], we see that All the integral points (X, Y) satisfying (4.23) are $(\pm 6, 0)$, $(-3, \pm 9)$, $(-2, -8)$, $(0, 0)$, $(12, \pm 36)$, $(18, \pm 72)$ and $(294, \pm 5040)$.

If $Y = 0$, then we get either $B_n = 0$ or $C_n = 0$, which is not possible. If $Y = -8$, (respectively, $Y = \pm 9$), then $s = -\dfrac{2}{9}$, (respectively $s = \pm\frac{1}{4}$) which is not possible again because s is an integer.

If $(X, Y) = (12, \pm 36)$, then $r = \dfrac{2}{3}$ and $s = \pm 1$, which is again impossible because r is an integer.

If $(X, Y) = (18, \pm 72)$, then $(r, s) = (1, \pm 2)$. This implies $t = \pm 1$ and $B_n t = \pm 1$, which is a contradiction to $n > 1$.

Finally, if $(X, Y) = (294, \pm 5040)$, then $r = \dfrac{49}{3}$, This violates the integrality of r. Thus, C_n can not be of the form $3t^2$ for any integer t.

Subcase III. (b is odd).

Using the relation $C_n = 4P_n^2 - 1$ in (4.18) and then putting $x := 2P_n$, we arrive at

$$x^2 - 3^a \cdot y^b = 1. \tag{4.24}$$

Then, by taking $D = 3^a$ in Lemma 4.3.6, we see that the possible set of solutions $(x, y, b, 3^a)$ for the above equation is as follows:

$$\{(2, 1, b, 3), (5, 2, 3, 3), (7, 2, 4, 3), (17, 2, 5, 9)\}.$$

The last three quadruples in the above set are not possible because the integer x in the equation (4.24) is an even integer. Finally, the quadruple $(2, 1, b, 3)$ will lead to $n = 1$, which is a contradiction to $n > 1$. This completes the proof of lemma. □

Lemma 4.4.5. *For any positive integers m, y and $l > 1$, the equation*

$$\prod_{i=1}^{m} C_i = y^l \tag{4.25}$$

has no solution.

Proof. Suppose there exist positive integers m, y and $l > 1$ such that

$$\prod_{i=1}^{m} C_i = y^l$$

holds true. Let R be the largest prime $\leq m$. By Bertrand' postulate $m < 2R$. Hence, for all integers $i = 1, 2, \ldots, m$ with $R \neq i$, we have, $\gcd(R, i) = 1$. Therefore, by Lemma 4.3.11, for each $i \neq R$ with $1 \leq i \leq m$, we have

$$\gcd(C_R, C_i) = 3^{r_i}$$

for some non-negative integer r_i. Hence, we can write $C_R = 3^t u$ and $C_i = 3^{r_i} v_i$ for some integers r, t, v_i with $3 \nmid u$ and $\gcd(u, v_i) = 1$. Then (4.25) becomes,

$$3^t u \prod_{\substack{i=1 \\ i \neq R}}^{m} 3^{r_i} v_i = y^l$$

and this implies

$$u \cdot \prod_{\substack{i=1 \\ i \neq R}}^{m} v_i = 3^k y^l$$

for some integer k. Since $\gcd(u, v_i) = 1$ for all $i \neq R$, we have $u = 3^k y_1^l$ or $u = y_1^l$, for some divisor y_1 of y. Thus, $C_R = 3^{t_1} y_1^l$ for some non-negative integer t_1, which is not possible by Lemma 4.4.3 and 4.4.4. □

4.5 Proof of Theorem 4.2.1

Suppose there exist positive integers $x, b, y > 1$, and m with b and $m > 2$ are even integers such that the relation

$$2x^2 + 1 = 3^b y^m \tag{4.26}$$

holds true.

We first claim that x is an even integer in (4.26). Suppose on the contrary that x is an odd integer. Then $x^2 \equiv 1 \pmod 4$ and hence

$$2x^2 + 1 \equiv 3 \pmod 4. \tag{4.27}$$

Since b is an even integer, $3^b \equiv 1 \pmod 4$. Also, as m is an even integer and y is an odd integer, we get, $y^m \equiv 1 \pmod 4$. Therefore, $2x^2 + 1 \equiv 3^b y^m \equiv 1 \pmod 4$, which is a contradiction to (4.27). Hence, $x = 2r$ for some integer r.

Now, the equation (4.26) becomes

$$8r^2 + 1 = (3^{b/2} y^{m/2})^2. \tag{4.28}$$

We know that if the Pell's equation $a^2 - 2b^2 = 1$ has a solution, then $a = Q_{2t}$ and $b = P_{2t}$ for some integer $t \geq 1$. Then by Lemma 4.1.2, $a = C_t$ and $b = 2B_t$. Hence by the equation (4.28), we conclude that $B_t = r$ and $C_t = 3^{b/2} y^{m/2}$, which is a contradiction to Lemma 4.4.4 because m is even with $m > 2$ and b is even with $b \geq 2$. □

4.6 Proof of Theorem 4.2.2

Suppose that there exist positive integers n, d and k such that

$$B_n B_{n+d} \cdots B_{n+(k-1)d} = y^l$$

for some integers $y \geq 2$ and $l \geq 2$.

If $d > 1$ and $k \geq 2$, then by Lemma 4.3.1(2), we get $R = P(\Delta(n, d, k)) > k$ except for $(n, d, k) = (2, 7, 3)$.

If $(n, d, k) = (2, 7, 3)$, then (4.7) becomes $B_2 B_9 B_{16} = y^l$. But this is not possible for any l. Therefore, $(n, d, k) \neq (2, 7, 3)$.

Since $(n, d, k) \neq (2, 7, 3)$, we have $R > k$. Therefore, $R \mid \Delta(n, d, k)$. Suppose $R \mid (n + id)$ and $R \mid (n + jd)$ for some $i \neq j$ with $0 \leq i < j \leq k - 1$. Then, $R \mid (j - i)d$. Since $(j - i) < k$ and $R > k$, we conclude that $R \mid d$. Since $\gcd(n, d) = 1$, we see that $R \nmid n$ and hence $R \nmid (n + rd)$ for any $0 \leq r \leq k - 1$ which implies that $R \nmid \Delta(n, d, k)$, a contradiction. Hence, R divides exactly one of $(n + rd)$ with $0 \leq r \leq k - 1$.

Let $n + id = R^e p_1^{e_1} \cdots p_r^{e_r}$ with $P(n + id) = R$ for some i with $0 \leq i \leq k - 1$. Since

$\gcd(R^e, n+rd) = 1$ for all $r \neq i$ with $0 \leq r \leq k-1$, we get

$$\gcd(B_{n+rd}, B_{R^e}) = 1. \tag{4.29}$$

Since $P(n+id) = R$, by Lemma 4.3.10, we have

$$\gcd\left(B_{R^e}, \frac{B_{n+id}}{B_{R^e}}\right) = 1. \tag{4.30}$$

Now, we can express (4.7) as

$$B_{R^e}\frac{B_{n+id}}{B_{R^e}}\prod_{\substack{r=0\\r\neq i}}^{k-1} B_{n+rd} = y^l. \tag{4.31}$$

From (4.29) and (4.30), we can see that

$$\gcd\left(B_{R^e}, \frac{B_{n+id}}{B_{R^e}}\prod_{\substack{r=0\\r\neq i}}^{k-1} B_{n+rd}\right) = 1. \tag{4.32}$$

By (4.31), (4.32) and the unique factorization in integers, we conclude that B_{R^e} is a perfect power, which is a contradiction to Lemma 4.4.1. Thus, (4.7) has no solution.

When $d = 1$ and $n > k$, then by Lemma 4.4.2, we can conclude that (4.7) has no solution.

Now, consider the final case $d = 1$ and $n \leq k$. By Lemma 4.3.4, there exists a unique i with $0 \leq i \leq k-1$ such that $R = P(\Delta(n,k)) = n+i$. So, $\gcd(R,t) = 1$ for $n \leq t \leq n+k-1$ and $t \neq n+i$, which gives $\gcd(B_R, B_t) = 1$. Thus, $\gcd(B_R, \prod_{\substack{j=0\\j\neq i}}^{k-1} B_{n+j}) = 1$. Hence, using Lemma 4.3.10, we conclude that B_R is a perfect power, which is a contradiction to Lemma 4.4.1. This completes the proof of the theorem.

4.7 Proof of Theorem 4.2.3

Suppose there exist positive integers n, d and k such that equation (4.8) is true for some integers $y > 1$ and $l > 1$.

Suppose $k = 2$. Then (4.8) becomes

$$C_n C_{n+d} = y^l.$$

Since $\gcd(n, d) = 1$, we have $\gcd(n, n + d) = 1$. Therefore, by Lemma 4.3.11, we get, $\gcd(C_n, C_{n+d}) = 3^r$ for some non-negative integer r. Thus, by the unique factorization in integers, we get $C_n = 3^r y_1^l$ for some integers $r \geq 0$ and $y_1 > 0$, which is not possible by Lemmas 4.4.3 and 4.4.4. Hence this case cannot happen.

Suppose $k = 3$. Then, we can express (4.8) as

$$C_n C_{n+d} C_{n+2d} = y^l.$$

If n is even, then $n + d$ is odd. Let $P(n + d) = R$ and hence R is an odd prime. Since $\gcd(n, d) = 1$, we see that, $R \nmid n$ and $R \nmid n(n + 2d)$. Hence, $\gcd(C_R, C_n) = 3^a$ for some integer $a \geq 0$ and $\gcd(C_R, C_{n+2d}) = 3^b$ for some integer $b \geq 0$. By Lemma 4.3.14, we get $\gcd\left(C_R, \frac{C_{n+d}}{C_R}\right) = 3^c$ for some integer $c \geq 0$. Therefore, $C_R = 3^r y_1^l$ for some integers $r \geq 0$ and $y_1 > 0$, which is not possible by Lemmas 4.4.3 and 4.4.4.

If n is odd, then $n+2d$ is also odd. Let $P(n) = R$ and hence R is an odd prime. Since $\gcd(n, d) = 1$, we see that $R \nmid (n + d)$ and $R \nmid (n + 2d)$. Hence, $\gcd(C_R, C_{n+d}) = 3^a$ for some integer $a \geq 0$, $\gcd(C_R, C_{n+2d}) = 3^b$ for some integer $b \geq 0$ and $\gcd\left(C_R, \frac{C_n}{C_R}\right) = 3^c$ for some integer $c \geq 0$. Thus, $C_R = 3^r y_1^l$ for some integers $r \geq 0$ and $y_1 > 0$, which has no solution, by Lemmas 4.4.3 and 4.4.4.

Suppose $k = 4$. Then, the equation (4.8) becomes $C_n C_{n+d} C_{n+2d} C_{n+3d} = y^l$. Without loss of generality, we assume that n and $n + 2d$ are odd. Let $P(n + 2d) = R$ and hence R is an odd prime. Then $R \nmid n$, $R \nmid (n + d)$ and $R \nmid (n + 3d)$. Now, we proceed as in

the proof of the case of $k = 3$, we conclude that $C_R = 3^r y_1^l$ for some integers $r \geq 0$ and $y_1 > 0$, which is not possible by Lemmas 4.4.3 and 4.4.4.

Suppose $k = 5$. Then we write the equation (4.8) as

$$C_n C_{n+d} C_{n+2d} C_{n+3d} C_{n+4d} = y^l.$$

If n is even, then $n + d, n + 3d$ are odd integers. Then one of them is not divisible by 3, say, $n + d$. Let $P(n + d) = R$ and hence $R > 3$ is an odd prime. Hence, $R \nmid (n + 3d)$, $R \nmid n(n + 2d)$ and $R \nmid (n + 4d)$ as $R > 3$. Hence, $\gcd(C_R, C_n) = 3^a$ for some integer $a \geq 0$, $\gcd(C_R, C_{n+2d}) = 3^b$ for some integer $b \geq 0$, $\gcd(C_R, C_{n+3d}) = 3^c$ for some integer $c \geq 0$ and $\gcd(C_R, C_{n+4d}) = 3^e$, for some integer $e \geq 0$. By Lemma 4.3.14, we get, $\gcd\left(C_R, \frac{C_{n+d}}{C_R}\right) = 3^t$ for some non-negative integer t. Therefore, $C_R = 3^r y_1^l$ for some integers $r \geq 0$ and $y_1 > 0$, which is a contradiction by Lemmas 4.4.3 and 4.4.4.

If n is odd, then $n + 2d$ is also odd. Let $P(n + 2d) = R$ and hence R is an odd prime. Then, $R \nmid n$, $R \nmid (n + d)$, $R \nmid (n + 3d)$ and $R \nmid (n + 4d)$. Hence, $\gcd(C_R, C_n) = 3^a$ for some integer $a \geq 0$, $\gcd(C_R, C_{n+d}) = 3^b$ for some integer $b \geq 0$, $\gcd(C_R, C_{n+3d}) = 3^c$ for some integer $c \geq 0$ and $\gcd(C_R, C_{n+4d}) = 3^e$ for some integer $e \geq 0$. Also by Lemma 4.3.14, we know that $\gcd\left(C_R, \frac{C_{n+2d}}{C_R}\right) = 3^t$ for some integer $t \geq 0$. Thus, $C_R = 3^r y_1^l$ for some integer $r \geq 0$ which has no solution by Lemmas 4.4.3 and 4.4.4.

Now, consider the case $k \geq 6$ and $d > 1$. Then by Lemma 4.3.2, there exists at least one integer i satisfying $0 \leq i < k$ such that $P(n+id) = R > k$ and $n+id$ is an odd integer. This implies that R is an odd prime. Since R divides $n + id$, we note that $R \nmid n + jd$ for all integers $j \neq i$ with $0 \leq j < k$. For, suppose $R \mid (n + rd)$ for some $r \neq i$ with $0 \leq r < k$. Then $R \mid (r - i)d$. Since $|r - i| < k$ and $R > k$, we get $R \mid d$, a contradiction to $\gcd(n, d) = 1$. Therefore, R divides $n + id$ and $R \nmid n + jd$ for all integers $j \neq i$ with $0 \leq j < k$. Thus, $\gcd(C_R, C_{n+rd}) = 3^{a_r}$ for some integer $a_r \geq 0$ and for all integers $r \neq i$.

Since $n + id$ is an odd integer and R is an odd prime, we see that $\frac{n+id}{R}$ is an odd integer. Hence, by Lemma 4.3.14, $\gcd\left(C_R, \frac{C_{n+id}}{C_R}\right) = 3^b$ for some integer $b \geq 0$.

Let $C_R = 3^c u$ where $3 \nmid u$ and for some integer $c \geq 0$. Therefore, $\gcd\left(u, \frac{C_{n+jd}}{C_R}\right) = 1$ and also $\gcd(u, C_{n+rd}) = 1$ for all integers $r \neq j$. We can rewrite (4.8) as

$$3^c u \cdot \frac{C_{n+jd}}{C_R} \prod_{\substack{i=1 \\ i \neq j}}^{k-1} C_{n+id} = y^l. \tag{4.33}$$

From the above arguments, we conclude that $u = 3^r y_1^l$ for some integers $r \geq 0$ and $y_1 > 0$ which in turn implies that $C_R = 3^{c+r} y_1^l$, a contradiction to Lemmas 4.4.3 and 4.4.4.

Finally, consider the case $k \geq 6$ and $d = 1$. In this case, the equation becomes

$$\prod_{i=1}^{k-1} C_{n+i} = y^l. \tag{4.34}$$

If $n \leq 2k$, then by Lemma 4.3.4, there exists a unique integer i with $0 \leq i \leq k-1$ such that $R = P(n(n+1)\cdots(n+k-1)) = n+i$. Hence, $\gcd(R, t) = 1$ for all integer t with $n \leq t \leq n+k-1$ and $t \neq n+i$. This implies $\gcd(C_R, C_t) = 3^a$ for some integer $a \geq 0$. Thus, $C_R = 3^r y_1^l$ for some integers $r \geq 0$ and $y_1 > 0$, which is not possible by Lemmas 4.4.3 and 4.4.4.

If $n > 2k$, then by Lemma 4.3.5, we get an integer i for which $n+i$ is odd with $R = P(n+i) > k$ and $R \nmid (n+j)$ for all $j = 1, 2, \cdots, k-1$ with $j \neq i$. Hence, once again we arrive at $C_R = 3^a y_1^l$ for some integer $a \geq 0$, which is a contradiction by Lemmas 4.4.3 and 4.4.4. This completes the proof of the Theorem 4.2.3.

Chapter 5

Arithmetic progression represented by binary quadratic form

This chapter is devoted to finding an upper bound for the length of an arithmetic progression which is represented by an integral binary quadratic form whose discriminant is not a perfect square and to discussing about the representation of 3*-term arithmetic progression by an integral binary quadratic form.*

5.1 Introduction

Definition 5.1.1. An *integral binary quadratic form* is a homogeneous polynomial of degree 2 over integers in two variables.

Let $Q(x, y) = ax^2 + bxy + cy^2$ be an integral binary quadratic form.

Definition 5.1.2. The form $Q(x, y)$ is said to be *primitive* if a, b and c are relatively prime integers. *The discriminant* of $Q(x, y)$ is defined to be $b^2 - 4ac$. We denote the discriminant of $Q(x, y)$ by d.

Definition 5.1.3. The form $Q(x, y)$ is said to be *positive-definite* (respectively, *negative-definite*) if it's discriminant d is positive (respectively, negative).

Definition 5.1.4. An integer n is said to be *represented by the integral binary quadratic form* if there exist integers r and s such that $n = Q(r, s) = ar^2 + brs + cs^2$.

Definition 5.1.5. Let $a_1, a_2, \ldots, a_n$ be integers which are in arithmetic progression. They are said to be in *arithmetic progression represented by the integral binary quadratic form* $Q(x, y)$ if for all $i = 1, 2, \ldots, n$, the term a_i is represented by the integral binary quadratic form $Q(x, y)$.

Let $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$. For $k \in \mathbb{N}$ and $l \in \mathbb{N}$, we have

$$k\mathbb{N}_0 + l = \{l, k + l, 2k + l, \ldots\}$$

is an arithmetic progression in positive integers. We consider an integral binary quadratic form $ax^2 + bxy + cy^2$ with $a, b, c \in \mathbb{Z}$ and ask the question "Can the form $ax^2 + bxy + cy^2$ represent every integer in the arithmetic progression $k\mathbb{N}_0+l$ for any natural numbers k and l?" Regarding this question, A. Alaca, Ş. Alaca and K. S. Williams [1] gave a necessary and sufficient condition for the representation of arithmetic progression of infinite length by Q.

Theorem 5.1.1 ([1])**.** *A binary quadratic form $ax^2 + bxy + cy^2$ with $a, b, c \in \mathbb{Z}$ can represent all the integers in arithmetic progression $k\mathbb{N}_0 + l$ for some $k, l \in \mathbb{N}$ if and only if its discriminant is a nonzero perfect square.*

Now suppose that d is not a perfect square so that Q cannot represent an arithmetic progression of infinite length. We address the question "How long can an arithmetic progression represented by Q be?" In [22], we obtain an upper bound for the length of any arithmetic progression represented by Q.

The least length of a nontrivial arithmetic progression is 3. Now we can ask the question "Does every nonzero integral binary quadratic form represent an arithmetic progression of length 3?" Two deep results of Weber [74] and Green [30] positively answer the above question for a positive-definite integral binary quadratic form.

Theorem 5.1.2 (Weber [74])**.** *If Q is a primitive integral binary quadratic form which is positive-definite, then the set of primes that are represented by Q has positive relative density.*

Theorem 5.1.3 (Green [30])**.** *Any subset of primes having positive relative density has a* 3*-term arithmetic progression.*

Thus, by putting these two deep results together, we see that every primitive, positive-definite, integral binary quadratic form represents a 3-term arithmetic progression infinitely often. In [22], we prove in a elementary way that any nonzero integral binary quadratic form represents a nontrivial arithmetic progression of length 3 infinitely often.

5.2 The main results

The main results [22] of this chapter are as follows.

Theorem 5.2.1. *Let $Q(x, y) = ax^2 + bxy + cy^2$ be an integral binary quadratic form with discriminant $d = b^2 - 4ac \neq 0$. Suppose that d is not a perfect square and that Q represents an arithmetic progression $\{kn + \ell : n = 0, 1, \ldots, R-1\}$ of length R, where k, ℓ and R are positive integers. Then there are absolute constants $C_1 > 0$ and $L_1 > 0$ such that $R < C_1 \ell (k^2|d|)^{L_1}$.*

Remark 5.2.1. *There is no loss of generality in assuming that Q represents an arithmetic progression of positive integers, since if Q only represents an arithmetic progression of negative integers, then $-Q$ represents an arithmetic progression of positive integers.*

Theorem 5.2.2. *Every nonzero integral binary quadratic form represents a nontrivial arithmetic progression of length* 3 *infinitely often*

Remark 5.2.2. *The statement of Theorem 5.2.2 is not true, in general, if we replace* 3 *by a larger integer. For example, the form $Q(x, y) = x^2$ does not represent an arithmetic progression of length* 4 *as there do not exist four squares in arithmetic progression (see [6]).*

5.3 Preliminaries

To prove Theorem 5.2.1, we need to build up some tools.

Lemma 5.3.1 ([3]). *If m and n are both positive integers and d is any nonzero integer, then*

$$\left(\frac{d}{m}\right) = \left(\frac{d}{n}\right) \text{ if } m \equiv n \pmod{|d|}.$$

Lemma 5.3.2 ([3]). *If $d \equiv 0$ or $1 \pmod 4$ is not a perfect square, then there exists an integer a satisfying*

$$\left(\frac{d}{a}\right) = -1, \quad 1 \leq a \leq |d| - 1.$$

In 1944, Y. V. Linnik [41] gave an upper bound for the least prime in an arithmetic progression which is as follows.

Theorem 5.3.1 (Linnik [41]). *Let a and d be any given positive coprime integers with $1 \leq a \leq d-1$ and p be the least prime in the arithmetic progression $\{a + nd : n \in \mathbb{N}\}$. Then there exist positive absolute constants C and L such that,*

$$p \leq Cd^L.$$

Remark 5.3.1. *By a deep result of Xylouris [75], one has $L \leq 5.2$.*

Proposition 5.3.1. *Let $N \equiv 0 \pmod 4$ be a nonzero integer which is not a perfect square. Then there exist absolute constants $C > 0$ and $L > 0$ for which there is a prime $p \neq 2$ satisfying*

$$p \leq C|N|^L, \quad \left(\frac{N}{p}\right) = -1.$$

Proof. Since $N \equiv 0 \pmod 4$ is not a perfect square, by Lemma 5.3.2, there is an integer a satisfying

$$\left(\frac{N}{a}\right) = -1, \quad 1 \leq a \leq |N| - 1.$$

Clearly $(a, |N|) = 1$. Hence by Theorem 5.3.1, there are absolute constants $C > 0$ and $L > 0$ such that the least prime p in the arithmetic progression

$$\{|N|k + a : k = 0, 1, 2, \ldots\}$$

satisfies

$$p \leq C|N|^L.$$

Since p belongs to this arithmetic progression, we have $p \equiv a \pmod{|N|}$ and by Lemma 5.3.1, we deduce

$$\left(\frac{N}{p}\right) = \left(\frac{N}{a}\right) = -1.$$

Finally, as $N \equiv 0 \pmod 4$ and $\left(\frac{N}{p}\right) = -1$, we see that $p \neq 2$. □

5.4 Proof of Theorem 5.2.1

Given that the arithmetic progression $\{km + l | m = 0, 1, \ldots, R-1\}$ of length R is represented by the form $Q(x, y)$. In order to prove

$$R \leq C_1 \ell (k^2|d|)^{L_1},$$

we first contruct an integer n satisfying $1 \leq n \leq C^3 l |N|^{3L}$ for some suitable integer N and for some positive absolute constants C and L such that $p \mid (kn + l)$ and $p^2 \nmid (kn + l)$ for some prime p. Then we prove that $kn + l$ is not represented by $Q(x, y)$ so that $R < n < C^3 l |N|^{3L}$ and achieve the result. Hence first we need to contruct such an integer n.

Set $N = 4k^2 d$, so that N is a nonzero integer with $N \equiv 0 \pmod 4$ which is not a perfect square. By Proposition 5.3.1, there are absolute constants $C > 0$ and $L > 0$ for which there is a prime $p \neq 2$ satsifying

$$p \leq C|N|^L, \quad \left(\frac{N}{p}\right) = -1.$$

Hence $\left(\frac{4k^2d}{p}\right) = -1$ and thus

$$(d,p) = (k,p) = 1, \left(\frac{d}{p}\right) = -1.$$

If $p|ac$, then

$$-1 = \left(\frac{b^2-4ac}{p}\right) = \left(\frac{b^2}{p}\right) = 0 \text{ or } 1,$$

which is impossible. Hence $(ac,p) = 1$.

As $(k,p) = 1$, there exists an integer t with $1 \le t < p^2$ such that $kt \equiv 1 \pmod{p^2}$. Define the integer u by $u = (kt-1)/p^2$ so that $kt = 1 + up^2$. As $kt \ge 1$, we see that $u \ge 0$. Further, as $up^2 < kt < kp^2$, we have $u < k$. Hence

$$kt = 1 + up^2,\ 1 \le t < p^2,\ 0 \le u < k.$$

We now construct an integer n with $1 \le n < C^3\ell|N|^{3L}$ such that $p|(kn+\ell)$ and $p^2 \nmid (kn+\ell)$.

If $p > \ell$, we choose $n = t(p-\ell)$. Note that $1 \le n < p^3$. Since $p \le C|N|^L$, it is clear that $n < C^3|N|^{3L} \le C^3\ell|N|^{3L}$. Also, we see that

$$kn + \ell = kt(p-\ell) + \ell = (1+up^2)(p-\ell) + \ell = p(1 + up^2 - up\ell),$$

so that $p|(kn+\ell)$ and $p^2 \nmid (kn+\ell)$ as required.

If $p \le \ell$ and $p \nmid \ell$, we choose $n = \ell t(p-1)$. Note that $1 \le n < \ell p^3 \le C^3\ell|N|^{3L}$. Moreover, we have

$$kn + \ell = k\ell t(p-1) + \ell = \ell(1+up^2)(p-1) + \ell = \ell p(1 + up^2 - up)$$

so that $p|(kn+\ell)$ and $p^2 \nmid (kn+\ell)$.

If $p \le \ell$ and $p\|\ell$, we choose $n = tsp$, where the positive integer $s = \ell/p$ is not divisible

by p. Clearly, $1 \le n < \ell p^3 < C^3 \ell |N|^{3L}$. Here

$$kn + \ell = ktsp + \ell = (1 + up^2)sp + sp = sp(2 + up^2),$$

so that $p|(kn + \ell)$ and $p^2 \nmid (kn + \ell)$, as $p \neq 2$ and $p \nmid s$.

Finally, if $p \le \ell$ and $p^2|\ell$, we choose $n = tp$. Note that $1 \le n < p^3 \le C^3|N|^{3L} \le C^3\ell|N|^{3L}$. In this case we have

$$kn + \ell = ktp + \ell = (1 + up^2)p + \ell = p(1 + up^2 + (\ell/p)),$$

so that $p|(kn + \ell)$ and $p^2 \nmid (kn + \ell)$, as $p|(\ell/p)$.

This completes the construction of an integer n satisfying $1 \le n < C^3\ell|N|^{3L}$ such that $p|(kn + \ell)$ and $p^2 \nmid (kn + \ell)$ for some prime p satisfying $\left(\frac{d}{p}\right) = -1$.

Next we show that the integer $kn+\ell$ is not represented by Q. Suppose on the contrary that the integer $kn + \ell$ is represented by Q. Then there exist integers x and y such that $kn+\ell = ax^2+bxy+cy^2$. Since $p|(kn+\ell)$, we have $ax^2+bxy+cy^2 \equiv 0 \pmod{p}$. Therefore, since

$$4a(ax^2 + bxy + cy^2) = (2ax + by)^2 - (b^2 - 4ac)y^2,$$

we see that $(2ax + by)^2 \equiv dy^2 \pmod{p}$. If $p \nmid y$, then $d \equiv ((2ax + by)z)^2 \pmod{p}$ for some integer z such that $yz \equiv 1 \pmod{p}$. This contradicts that $\left(\frac{d}{p}\right) = -1$. If $p|y$, then $p|(2ax + by)$ and hence $p|2ax$. But since $p \neq 2$ and $p \nmid a$, we get $p|x$. Therefore p^2 divides $ax^2 + bxy + cy^2 = kn + \ell$, contradicting the fact that $p^2 \nmid (kn + \ell)$. This completes the proof that the integer $kn + \ell$ is not represented by Q.

Since all the integers $\ell, k + \ell, 2k + \ell, \ldots, (R - 1)k + \ell$ are represented by Q, we must have $n > R - 1$, that is, $R \le n$. Since $n < C^3\ell|N|^{3L}$, we get

$$R < C^3\ell|4k^2d|^{3L} = C_1\ell(k^2|d|)^{L_1},$$

where L_1 and C_1 are absolute constants satisfying $L_1 = 3L > 0$ and $C_1 = C^3 2^{6L} > 0$.

This proves the theorem.

5.5 Proof of Theorem 5.2.2

Let $Q(x, y) = ax^2 + bxy + cy^2$ be a nonzero, integral binary quadratic form. Since Q is nonzero, at least one of the integers a, b and c is nonzero. We consider the following cases;

Case 1: $a \neq 0$.

Let x be a positive integer. Then we see that the values

$$Q(2x^2 - 1, 0) = a(4x^4 - 4x^2 + 1),$$

$$Q(2x^2 + 2x + 1, 0) = a(4x^4 + 8x^3 + 8x^2 + 4x + 1) = a(4x^4 - 4x^2 + 1) + a(8x^3 + 12x^2 + 4x)$$

and

$$Q(2x^2 + 4x + 1, 0) = a(4x^4 + 16x^3 + 20x^2 + 8x + 1) = a(4x^4 - 4x^2 + 1) + 2a(8x^3 + 12x^2 + 4x)$$

form a non-trivial arithmetic progression of length 3. Since x is any arbitrary integer, we conclude that Q represents a non-trivial arithmetic progression of length 3 infinitely often.

Case 2: $a = 0$

In this case, $Q(x, y) = bxy + cy^2$ and its discriminant is $d = b^2$.

Subcase (i): $b \neq 0$

Since d is a nonzero perfect square, by Theorem 5.1.1 the form $Q(x, y)$ represents an infinite arithmetic progression in positive integers and hence it represents a nontrivial arithmetic progression of length 3 infinitely often.

Subcase (ii): $b = 0$

In this case, we have, $Q(x, y) = cy^2$, where $c \neq 0$, as $a = b = 0$. Then, taking x to be any integer and proceeding similarly as in the first case, we deduce that $Q(x, y)$ represents infinitely many nontrivial arithmetic progressions of length 3. This proves the theorem.

Bibliography

[1] A. Alaca, Ş. Alaca and K. S. Williams, Arithmetic progressions and binary quadratic forms, *Amer. Math. Monthly* **115** (2008), no. 3, 252-254.

[2] A. Alvarado, An arithmetic progression on quintic curves, *J. Integer Seq.* **12** (2009), no. 7, Article 09.7.3.

[3] R. Ayoub, An introduction to the analytic theory of numbers, American Mathematical Society, Providence, RI, (1963).

[4] A. Behera and G. K. Panda, On the square roots of triangular numbers, *The Fib Quart.* **37**(2)(1999), 98-105.

[5] M. A. Bennentt, Product of consecutive integers, *Bull. London Math. Soc.* **36**(2004), 683-694.

[6] W. Bosma, J. Cannon and C. Playoust, The Magma algebra system. I. The user language, *J. Symbolic Comput.***24**(1997), 235-265.

[7] A. Bourdon, P. L. Clark and J. Stankewicz, Torsion points on CM elliptic curves over real number fields, *Transactions of the AMS.* (To appear).

[8] J. J. Bravo, P. Das, S. Guzmán and S. Laishram, Powers in products of terms of Pell's and Pell-Lucas Sequences, *Int. J. Number Theory*, **11**(4)(2015), 1259-1274.

[9] A. Bremner and J. W. S. Cassels, On the equation $Y^2 = X(X^2 + p)$, *Math. Comp.* **42** (1984), 257-264.

[10] A. Bremner, Arithmetic progressions on Edwards curves, *J. Integer Seq.* **16** (2013), no. 8, Article 13.8.5.

[11] A. Bremner, On Diagonal Cubic Surfaces, *Manuscripta Math.* **62** (1988), no.1, 21-32.

[12] A. Bremner, Arithmetic progression on Elliptic Curves, *Experiment. Math.* **8** (1999), no. 4, 409-413.

[13] Y. Bugeaud, M. Mignotte, and S. Siksek, Classical and modular approaches to exponential Diophantine equations I. Fibonacci and Lucas perfect powers, *Ann. of Math.* **163**(3) (2006), 969-1018.

[14] G. Campbell, A note on arithmetic progressions on elliptic curves, *J. Integer Seq.* **6** (2003), Article 03.1.3.

[15] R. D. Carmichael, On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$, *Ann. of Math.* **15** (1913), 30-70.

[16] A. Choudhry, Arithmetic progressions on Huff curves, *J. Integer Seq.* **18** (2015), no. 5, Article 15.5.2.

[17] J. H. E. Cohn, On square Fibonacci numbers, *J. London Math. Soc.* **39** (1964), 537-540.

[18] Pallab Kanti Dey, Elliptic curves with rank 0 over number fields, *Funct. Approx. Comment. Math.* (2017), DOI: 10.7169/facm/1585.

[19] Pallab Kanti Dey, Torsion points over number fields, Communicated.

[20] Pallab Kanti Dey and Bibekananda Maji, Arithmetic progression on $y^2 = x^3 + k$, *J. Integer Seq.* **19** (2016), Article 16.7.4.

[21] Pallab Kanti Dey and S. S. Rout, Diophantine equations concerning balancing and Lucas balancing numbers, *Archiv der Mathematik* **108**(1) (2017), 29-43.

[22] Pallab Kanti Dey and R. Thangadurai, The length of an arithmetic progression represented by a binary quadratic form, *Amer. Math. Monthly* **121** (2014), no. 10, 932-936.

[23] P. Erdős and J. L. Selfridge, The product of consecutive integers is never a power, *Illinois J. Math.* **19** (1975), 292-301.

[24] J. Esmonde and M. Ram Murty, Problems in algebraic number theory, Springer-Verlag, New York, (2006).

[25] R. P. Finkelstein, The house problem, *Amer. Math. Monthly* **72** (1965), 1082-1088.

[26] I. García-Selfa and J. Tornero, Searching for simultaneous arithmetic progressions on elliptic curves, *Bull. Austral. Math. Soc.* **71** (2005), no. 3, 417-424.

[27] E. González-Jiménez, Complete classification of the torsion structures of rational elliptic curves over quintic number fields, *arXiv: 1607.01929*.

[28] E. González-Jiménez, On arithmetic progressions on Edwards curves, *Acta Arith.* **167** (2015), no. 2, 117-132.

[29] E. González-Jiménez and J. M. Tornero, Torsion of rational elliptic curves over quadratic fields, *Revista de la Real Academia de Ciencias Exactas, Físicas y Naturales. Serie A. Matemática* **108** (2) (2014), 923-934.

[30] B. Green, Roth's theorem in the primes, *Annals of Math.* **161** (2005), 1609-1636.

[31] A. J. Hollier, B. K. Spearman and Q. Yang, On the rank and integral points of ellipitc curves $y^2 = x^3 - px$, *Int. J. of Algebra* **3**(2009), 401-406.

[32] A. J. Hollier, B. K. Spearman and Q. Yang, Elliptic Curves $y^2 = x^3 + pqx$ with maximal rank, *Int. Math. Forum* **5** (2010), 1105-1110.

[33] D. Jeon, C. H. Kim and E. Park, On the torsion of elliptic curves over quartic number fields, *J. London Math. Soc.* (2) **74** (2006), 1-12.

[34] S. Kamienny, Torsion points on elliptic curves and q-coefficients of modular forms, *Invent. Math.* **109** (1992), 221-229.

[35] M.A Kenku and F. Momose, Torsion points on elliptic curves defined over quadratic fields, *Nagoya Math.* **109** (1988), 125-149.

[36] A. Knapp, Elliptic Curves, Princeton Univ. Press, (1992).

[37] N. Koblitz, Introduction to Elliptic Curves and Modular Forms, Springer-Verlag, New York, (1993).

[38] T. Kudo and K. Motose, On group structures of some special elliptic curves, *Math J. Okayam Univ.* **47** (2005), 81-84.

[39] S. Laishram and T. N. Shorey, Irreducibility of generalized Hermite-Laguerre polynomials, *Funct. Approx. Comment. Math.*, **47**(1) (2012), 51-64.

[40] J. B. Lee and W. Y. Vélez, Integral solutions in arithmetic progression for $y^2 = x^3 + k$, *Period. Math. Hungar.* **25** (1992), 31-49.

[41] Y. V. Linnik, On the least prime in an arithmetic progression I. The basic theorem, *Rec. Math. (Mat. Sbornik) N. S.* **15** (57) (1944), 139-178.

[42] W. Ljunggren, Zur Theorie der Gleichung $x^2 + 1 = Dy^4$, *Avh. Norske Vid Akad. Oslo* **5** (1942), 298-311.

[43] J. London and R. Finkelstein, On Fibonacci and Lucas numbers which are perfect powers, *The Fib Quart.* **7** (1969), 476-481

[44] F. Luca and T. N. Shorey, Diophantine equations with products of consecutive terms in Lucas sequences, *J. Number Theory* **114** (2005), 298-311.

[45] A. MacLeod, 14-term arithmetic progressions on quartic elliptic curves, *J. Integer Seq.* **9** (2006), no. 1, Article 06.1.2.

[46] B. Mazur, Rational isogenies of prime degree, *Invent. Math.* **44**(1978), 129-162.

[47] L. Merel, Bornes pour la torsion des courbes elliptiques sur les corps de nombres, *Inventiones Mathematicae* **124** (1996), 437-449.

[48] S. P. Mohanty, On consecutive integral solutions for $y^2 = x^3 + k$, *Proc. Amer. Math. Soc.* **48** (1975) 281-285.

[49] S. P. Mohanty, Integral solutions in arithmetic progression for $y^2 = x^3 + k$, *Acta Math. Acad. Sci. Hungar.* **34** (1980), no. 3-4, 261-265.

[50] D. Moody, Arithmetic progressions on Edward curves, *J. Integer Seq.* Vol. 14 (2011), Article 11.1.7.

[51] D. Moody, Arithmetic progressions on Huff curves, *Annales Mathematicae et Informaticae*, **38** (2011), 111-116.

[52] L. J. Mordell, Diophantine Equations, Pure and Applied Mathematics, Vol. 30, Academic Press, London (1969).

[53] F. Najman, Torsion of elliptic curves over quadratic cyclotomic fields, *Math. J. Okayama Univ.* **53** (2011), 75-82.

[54] F. Najman, Complete classication of torsion of elliptic curves over quadratic cyclotomic elds, *J. Number Theory* **130** (2010), 1964-1968.

[55] F. Najman, Torsion of rational elliptic curves over cubic fields and sporadic points on $X_1(n)$, *Math. Res. Letters* **23** (2016), 245-272.

[56] L. Olson, Points of finite order on elliptic curves with complex multiplication, *Manuscripta math.* **14** (1974), 195205.

[57] G. K. Panda, Some fascinating properties of balancing numbers, *Congr. Numerantium* **194** (2009), 185-189.

[58] G. K. Panda and P. K. Ray, Some links of balancing and cobalancing numbers with Pell and associated Pell numbers, *Bull. Inst. Math. Acad. Sin.(N.S.)* **6**(1) (2011), 41-72.

[59] A. Pethő, Perfect powers in second order linear recurrences, *J. Number Theory* **15** (1982), 5-13.

[60] A. Pethő, Full cubes in the Fibonacci sequence, *Publ. Math. Debrecen* **30** (1983), 117-127.

[61] A. Pethő, The Pell sequence contains only trivial perfect powers, *Coll. Math. Soc. J. Bolyai, 60 sets, Graphs and Numbers, Budapest* (1991), 561-568.

[62] J. B. Rosser and L. Schoenfeld, Approximate formulas for some functions of prime numbers, *Illinois J.Math.* **6** (1962), 64-94.

[63] T. N. Shorey and C. L. Stewart, On the Diophantine equation $ax^{2t}+bx^{t}y+cy^{2}=d$ and pure powers in recurrence sequences, *Math. Scand.* **52** (1983), 24-36.

[64] T. N. Shorey and R. Tijdeman, On the greatest prime factor of an arithmetical progression, in A tribute to P. Erdős, eds. A Baker, B. Bollobás, and A. Hajnal, *Cambridge University Press*, Cambridge, (1990), 385-389.

[65] J. H. Silverman, The arithmetic of elliptic curves, Springer-Verlag, New York, (1992).

[66] J. H. Silverman and J.Tate, Rational points on elliptic curves, Springer-Verlag, New York, (1992).

[67] B. K. Spearman, Elliptic curves $y^2 = x^3 - px$ of rank two, *Math. J. Okayama Univ.* **49** (2007), 183-184.

[68] B. K. Spearman, On the group structure of elliptic curves $y^2 = x^3 - 2px$, *Int. J. of Algebra* **1** (2007), 247-250.

[69] J. J. Sylvester, On arithmetical series, *Messenger of Math.* **21**(1-19) (1892), 87-120; Math. Papers 4 (1912), 687-731.

[70] M. Ulas, A note on arithmetic progressions on quartic elliptic curves, *J. Integer Seq.* Vol. 8 (2005), Article 05.3.1.

[71] M. Ulas, On arithmetic progressions on genus two curves, *Rocky Mountain J. Math.* **39** (2009), 971-980.

[72] M. Ulas, Rational points in arithmetic progressions on $y^2 = x^n + k$, *Canad. Math. Bull.* **55** (2012), no. 1, 193-207.

[73] L. C. Washington, Elliptic curves number theory and cryptography, Chapman and Hall/CRC, Florida, (2003).

[74] H. Weber, Beweis des Satzes, daß jede eigentlich primitive quadratische Form un endliche viele Primzahlen darzustellen fähig ist, *Math. Annalen* **20** (1882), 301-329.

[75] T. Xylouris, Űber die Linniksche Konstante, *Diplomarbeit, Universität Bonn* (2009), (arXiv:0906.2749v1 [math.NT] 15 Jun 2009).