SOME PROBLEMS IN ALGEBRAIC AND COMBINATORIAL NUMBER THEORY CONNECTED WITH FINITE ABELIAN GROUPS

By
BIDISHA ROY
MATH08201504001

Harish-Chandra Research Institute, Prayagraj

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

November, 2019

Homi Bhabha National Institute[1]

Recommendations of the Viva Voce Committee

As members of the Viva Voce Committee, we certify that we have read the dissertation prepared by Bidisha Roy entitled "Some Problems in Algebraic and Combinatorial Number Theory connected with Finite Abelian Groups" and recommend that it may be accepted as fulfilling the thesis requirement for the award of Degree of Doctor of Philosophy.

Chairman - Prof. B. Ramakrishnan	**Date:** 9/3/2020
Guide / Convener – Prof. R. Thangadurai	**Date:** 09/03/2020.
Examiner – Prof. B. Sury	**Date:** 9/3/20
Member 1- Prof. D. Surya Ramana	**Date:** 9/3/20
Member 2- Prof. Gyan Prakash	**Date:** 09/03/2020
Member 3- Prof. Punita Batra	**Date:** 9/3/2020

Final approval and acceptance of this thesis is contingent upon the candidate's submission of the final copies of the thesis to HBNI.

I/~~We~~ hereby certify that I/~~we~~ have read this thesis prepared under my/our direction and recommend that it may be accepted as fulfilling the thesis requirement.

Date: 09.03.2020

Place: Prayagraj

Prof. R. Thangadurai
Guide

[1] This page is to be included only for final submission after successful completion of viva voce.

STATEMENT BY AUTHOR

This dissertation has been submitted in partial fulfillment 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 judgment the proposed use of the material is in the interests of scholarship. In all other instances, however, permission must be obtained from the author.

Bidisha Roy

BIDISHA ROY

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.

Bidisha Roy

BIDISHA ROY

List of Publications arising from the thesis

Journal

1. “Quadratic nonresidues and nonprimitive roots satisfying a coprimality conditions,” Jaitra Chattopadhyay, Bidisha Roy, Subha Sarkar and R. Thangadurai, *Bull. Aust. Math. Soc.*, **2019**, *99*, 177-183.

2. “On sums of polynomial-type exceptional Units in Z/nZ,” Anand, Jaitra Chattopadhyay and Bidisha Roy, *Arch. Math. (Basel)*, **2020**, *114*, 271-283.

3. “On zero-sum subsequences in a finite abelian p-group of length not exceeding a given number,” Bidisha Roy and R. Thangadurai, *J. Number Theory*, **2018**, *191*, 246-257.

Others

1. “Torsion groups of Mordell cuves over cubic and sextic fields,” Pallab Kanti Dey and Bidisha Roy, Submitted.

Conferences

1. Pesented a talk “ On Quadratic non residues non primitive roots” in International Conference on Class Groups of Number Fields and Related Topics-2018 at Harish-Chandra Research Institute, Allahabad, India, October-2018.

2. Presented a talk “On zero-sum subsequences in a finite abelian p-group” in Fifth mini symposium of the Roman Number Theory Association at Università Roma Tre, Rome, Italy, April-2019.

Bidisha Roy

BIDISHA ROY

Dedicated to

My Father

ACKNOWLEDGEMENTS

At first, I would like to thank my Ph.D. supervisor, Prof. R. Thangadurai, for his constant support, inspiration and good wishes throughout my HRI-days. He always supports me to retain my focus in mathematics and overcome difficulties in academic as well as non-academic issues.

I am thankful to my Doctoral committee members Prof. B. Ramakrishnan, Prof. D. Surya Ramana, Prof. P. Batra and Prof. G. Prakash, for their constant encouragement. I wish to thank all faculty members of HRI who taught us in our course-work which stimulated me to look into some concepts more deeply. Specially, I wish to mention about Prof. N Raghavendra who guided me in my first year project of Ph.D. course-work and could make me confident to continue further.

At the starting of my Ph.D., Prof. S. D. Adhikari motivated me to enjoy and carry forward in Number theory and at the end, I am really thankful to him for his initiative. I am thankful to Prof. A. Bremner, Prof. A. Robertson and Prof. W. A. Schmid for supporting me to pursue my career. I wish to take opportunity to thank Prof. M. J. Schlosser, Prof. F. Najman and Prof. E. González-Jiménez for making my Ph.D. time more fruitful in several ways. Specially, I would like to mention about Najman who taught me how to concentrate endlessly on a particular topic. I am thankful to Prof. T. E. V. Balaji and Prof. A.V. Jayanthan for their nice teaching in my M.Sc. and for their constant motivation to continue in mathematics.

All my collaborators (Jaitra, Subha, Aaron Robertson, Thanga sir, Pallab da and Anand) could make my Ph.D. life less stressful with some collaboration in proper time and I am thankful for their support.

Also, I would like to thank HRI administrative staffs for their efforts to make my Ph.D.-journey smooth and I specially thank 'HRI-Mess' which I think the best part of HRI. My HRI days could not be so nice without the endless support of HRI mess workers who always serve us whole-heartily.

I am thankful to my parents and brother for their continuous support in their own way. It is not possible to pursue my Ph.D. without their support and encouragement. I should obviously thank Ankur who always tried his best to support me.

Whenever I needed some fresh air from outside-HRI, I got enough oxygen from my friend group of M.Sc. batch (M & I). They supported me in every walk of my life in last few years. So, I really owe them a lot and special mention goes to Chanda for giving enormous time to me.

Last but not the least, I would like to thank all my friends & well-wishers who taught me many aspects of life. Specially, I wish to mention about my friends in HRI and batch mates (Deba, Jaitra, Subha and Lalit) who made my HRI days significant and memorable. All my juniors and seniors in HRI made my life comfortable and enjoyable in HRI with their constant attachment. It is incomplete without referring Bobo who gifted me some nice moments in HRI.

Contents

Summary **1**

1 Torsion groups of Mordell curves over cubic and sextic fields **3**
1.1 Introduction . . . 3
1.2 Main results . . . 8
1.3 Preliminaries . . . 11
1.3.1 Basics on Number field . . . 11
1.3.2 Basics on elliptic curves over number field . . . 11
1.3.3 Basics on elliptic curves over finite field . . . 16
1.4 Proof of Theorem 1.2.1 . . . 19
1.5 Proof of Theorem 1.2.2 . . . 26
1.6 Proof of Theorem 1.2.3 . . . 30
1.7 Proof of Theorem 1.2.4 . . . 37

2 Quadratic non-residues and non-primitive roots satisfying a co-primality condition **43**
2.1 Introduction . . . 44
2.2 Main results . . . 45
2.3 Preliminaries . . . 46
2.4 Proof of Theorem 2.2.1 . . . 56
2.5 Proof of Corollary 2.2.2 . . . 61

3 On sums of polynomial-type exceptional units in $\mathbb{Z}/n\mathbb{Z}$ **63**
3.1 Introduction . . . 63
3.2 Main results . . . 65
3.3 Preliminaries . . . 67
3.4 Proof of Theorem 3.2.1 . . . 73
3.5 Proof of Corollary 3.2.4 . . . 75
3.6 Proof of Corollary 3.2.5 . . . 76
3.7 Concluding remarks . . . 78

4 On zero-sum subsequences in a finite abelian p-group of length not exceeding a given number **83**
4.1 Introduction 84
4.2 Main result 88
4.3 Preliminaries 88
4.4 Proof of Theorem 4.2.1 107

Bibliography **111**

Summary

This thesis deals with some problems of algebraic and combinatorial number theory connected with finite abelian groups. In the first two chapters, we discuss a problem related to elliptic curves and a problem regarding the distribution of quadratic residues which are non-primitive roots. The last two chapters are dedicated to combinatorial number theory. In the third and fourth chapter, we consider have considered a problem generalizing *exceptional units* in the ring $\mathbb{Z}/n\mathbb{Z}$ and a problem on zero-sum subsequences in some finite abelian p-groups.

In the first chapter, we discuss torsion groups of elliptic curves defined over number fields which is a classical topic and it has a vast literature in algebraic number theory. In this chapter, we classify torsion groups of rational Mordell curves explicitly over cubic fields as well as over sextic fields. Also, we classify torsion groups of Mordell Curves over cubic fields. For Mordell curves over sextic fields, we compute all possible torsion groups.

In the second chapter, we discuss a problem regarding distribution of residues. More precisely, we proved the following. *Let $q \geq 1$ be any integer and let $\epsilon \in [\frac{1}{11}, \frac{1}{2})$ be a given real number. Then for all primes p satisfying*

$$p \equiv 1 \pmod{q}, \quad \log\log p > \frac{\log 6.83}{\frac{1}{2} - \epsilon} \text{ and } \frac{\phi(p-1)}{p-1} \leq \frac{1}{2} - \epsilon,$$

there exists a quadratic non-residue g which is not a primitive root modulo p such that gcd $\left(g, \frac{p-1}{q}\right) = 1$.

In the third chapter, we generalize *exceptional units* to a polynomial version and solve a problem involving that. We know that a unit u in a commutative ring R with unity is said to be *exceptional* if $u - 1$ is also a unit. We introduce a notion of polynomial version of exceptional unit (abbreviated as f-exunits) for any $f(X) \in \mathbb{Z}[X]$. In fact, we find the number of representations of a non-zero element of $\mathbb{Z}/n\mathbb{Z}$ as a sum of two f-exunits, for an infinite family of polynomials f of each degree ≥ 1. We also derive the exact formulae for certain infinite families of linear and quadratic polynomials. This generalizes a result of Sander.

In the last chapter, we consider a problem in *zero-sum theory*. For a finite abelian additive group G and for a subset $L \subseteq \mathbb{N}$, we know the constant $s_L(G)$ as the least positive integer t such that every sequence over G of length t contains a zero-sum subsequence of length ℓ for some $\ell \in L$. For $L = \{1, 2, \ldots, a\}$, we denote the constant $s_L(G)$ by $s_{\leq a}(G)$. In this chapter, we compute this constant for many class of abelian p-groups. In particular, it proves a conjecture of Schmid and Zhuang.

CHAPTER 1

Torsion groups of Mordell curves over cubic and sextic fields

In this chapter, we classify torsion groups of rational Mordell Curves explicitly over cubic fields as well as over sextic fields. Also, we classify torsion groups of Mordell Curves over cubic fields. For Mordell curves over sextic fields, we compute all possible torsion groups.

1.1 Introduction

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

Definition 1.1.2 An *Elliptic curve* E over a field K is a curve of the form

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

where $a_1, \ldots, a_6 \in K$.

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

Theorem 1.1.3 *[89] Let E be an elliptic curve defined over K. Then $E(K)$ is a finitely generated abelian group.*

Hence, by the structure theorem of finitely generated abelian groups, we have $E(K) \cong T \oplus \mathbb{Z}^r$, for some non-negative integer r. We call r as the *rank of the elliptic curve* E and T is called the *torsion subgroup* of $E(K)$. Sometimes we may write $T = E(K)_{tors}$.

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

Notation 1.1.4 For an integer $d \geq 1$, we define $\Phi'(d) = \{E(K)_{tors} : K/\mathbb{Q}$ is a number field of degree d and E is an elliptic curve defined over $K\}$. For any two element $A, B \in \Phi'(d)$, we say $A \sim B$ if and only if $A \cong B$. Then $\sim$ is an equivalence relation on $\Phi'(d)$ and let $\Phi(d) := \Phi'(d)/\sim$. In short, for a fixed natural number $d \geq 1$, the set of all possible torsion subgroups of elliptic curves defined over number field of degree d is denoted by $\Phi(d)$.

Theorem 1.1.5 *[61] Let $d \geq 1$ be an integer. Then the number of elements in $\Phi(d)$ is finite.*

When we restrict elliptic curves over $\mathbb{Q}$, we define the following notation in a similar way.

Notation 1.1.6 When K varies over any number field of degree d and E varies over any any rational elliptic curve, then the set of all possible torsion subgroups of $E(K)$ (up-to isomorphism) is denoted by $\Phi_{\mathbb{Q}}(d)$.

Note that when $K = \mathbb{Q}$, we see that $\Phi(1) = \Phi_{\mathbb{Q}}(1)$.

When $K = \mathbb{Q}$, in [60], Mazur proved that

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

By a result of Kamienny [46] and by another result of Kenku and Momose [48], it is known that

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

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

Also, in [45], it has been proved that if K varies over all cubic number fields and E varies over all elliptic curves over K, then the group structures which appear infinitely often as $E(K)_{tors}$ are exactly the following

$$\mathbb{Z}/m\mathbb{Z}; \qquad 1 \leq m \leq 20, m \neq 17, 19$$
$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}; \qquad 1 \leq n \leq 7.$$

From the above information, we can say that the set of these 25 groups is a subset of $\Phi(3)$. Moreover, in the same paper [45], they proved that if E varies over all rational elliptic curves, then each elements of $\Phi(1)$ occurs infinitely often as $E(\mathbb{Q})_{tors}$. They have also mentioned that all 26 groups in $\Phi(2)$ occur infinitely often as $E(K)_{tors}$, when K varies over all quadratic number fields and E varies over all elliptic curves over K.

Moreover, in [44], it has been determined that which groups of the form $\mathbb{Z}/M\mathbb{Z} \oplus \mathbb{Z}/N\mathbb{Z}$ occur infinitely often as torsion groups $E(K)_{tors}$ when K varies over all quartic number fields and E varies over all elliptic curves over K. However in general it is still unknown about the set $\Phi(d)$ for $d \geq 3$.

Najman in [68] focused only on rational elliptic curves and determined $\Phi_{\mathbb{Q}}(2)$ as follows.

Theorem 1.1.7 *[68] We have*

$$\begin{aligned}\Phi_{\mathbb{Q}}(2) &= \{\mathbb{Z}/m\mathbb{Z}, \qquad m = 1, \ldots, 10, 12, 15, 16\} \\ &\cup \{\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z}, \qquad 1 \leq m \leq 6\} \\ &\cup \{\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3m\mathbb{Z}, \qquad m = 1, 2\} \\ &\cup \{\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}\}.\end{aligned}$$

In the same paper, Najman [68] showed that

$$\begin{aligned}\Phi_{\mathbb{Q}}(3) = \; &\{\mathbb{Z}/m\mathbb{Z} : 1 \leq m \leq 21, m \neq 11, 15, 16, 17, 19, 20\} \\ &\cup \{\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z} : 1 \leq m \leq 7, m \neq 5, 6\}\end{aligned}$$

Very recently, González-Jiménez and Najman in [38] completely determined the set $\Phi_{\mathbb{Q}}(4)$. Priorer to the above, González-Jiménez [37] had provided all possible elements in the set $\Phi_{\mathbb{Q}}(5)$. For a given elliptic curve $E/\mathbb{Q}$ with torsion subgroup $G = E(\mathbb{Q})_{tors}$, H.B. Daniels and González-Jiménez, in [10], studied what groups (up to isomorphism) can occur as the torsion subgroup of E base-extended to K, a degree 6 extension of $\mathbb{Q}$. This is a first step towards the complete classification of $\Phi_{\mathbb{Q}}(6)$. In [38], it is also proved that $\Phi_{\mathbb{Q}}(d) = \Phi(1)$ for any integer d not divisible by $2, 3, 5$ and 7.

In Notation 1.1.4, if we restrict E to those elliptic curves with complex

multiplication (we call *CM curves*), then all possible torsion subgroups over number fields of degree d is denoted by $\Phi^{CM}(d)$. Analogously, following the Notation 1.1.6, we define $\Phi^{CM}_{\mathbb{Q}}(d)$. The set $\Phi^{CM}(1)$ was determined by Olson in [73]. Recently, Clark et al. in [9] have computed the sets $\Phi^{CM}(d)$ for $2 \leq d \leq 13$.

Definition 1.1.8 Any elliptic curve of the form $y^2 = x^3 + c$ which is defined over number field K (equivalently $c \in K$) is called *Mordell curve*.

At first, Knapp [49] focused on the family of rational Mordell curves and completely classified torsion subgroups upto isomorphism which is as follows.

Theorem 1.1.9 ([49], Page 134) *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) $T \cong \{\mathcal{O}\}$, *otherwise.*

In particular, it is known that this family of curves are CM elliptic curves. In the case of Mordell curves, we denote by $\Phi^M(d)$ (respectively $\Phi^M_{\mathbb{Q}}(d)$) the analogue of the sets $\Phi(d)$ (respectively $\Phi_{\mathbb{Q}}(d)$) but restrict to Mordell curves. The set $\Phi^M(1)$ was determined completely in [49]. Recently, P. Dey in [12] computed the set $\Phi^M_{\mathbb{Q}}(d)$, for $d = 2$ and all $d \geq 5$ with $gcd(d, 6) = 1$.

We have mentioned earlier that for an elliptic curve with complex multiplication, we don't know about the set $\Phi^{CM}(d)$, when d is even. Since Mordell curve is a member of the family of elliptic curves with complex multiplication, the complete determination of $\Phi^M(6)$ can shed light to even case.

1.2 Main results

In this chapter, we prove the following theorems

Theorem 1.2.1 *[14] We have*

$$\Phi_{\mathbb{Q}}^{M}(3) = \{\mathbb{Z}/9\mathbb{Z}, \mathbb{Z}/6\mathbb{Z}, \mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}, \mathcal{O}\}.$$

Moreover, if $K/\mathbb{Q}$ is a cubic field and if $E : y^2 = x^3 + c$ is a rational Mordell curve for any 6-th power-free integer c, then $T := E(K)_{tors}$ is isomorphic to

(1) $\mathbb{Z}/9\mathbb{Z}$, *if* $c = 16$ *and* $K = \mathbb{Q}(r)$ *with* r *satisfying* $r^3 - 3r^2 + 1 = 0$,

(2) $\mathbb{Z}/6\mathbb{Z}$,
- *if c is both square and cube in K,*
- *or $c = -27$ and 4 is a cube in K,*

(3) $\mathbb{Z}/3\mathbb{Z}$,
- *if $c(\neq 16)$ is a square but not a cube in K,*
- *or $c = 16$ and $K \neq \mathbb{Q}(r)$ with r satisfying $r^3 - 3r^2 + 1 = 0$,*
- *or $4c$ is a cube and $-3c$ is a square in K,*

(4) $\mathbb{Z}/2\mathbb{Z}$,
- *if $c(\neq -27)$ is a cube but not a square in K,*
- *or $c = -27$ but 4 is not a cube in K,*

(5) $\{\mathcal{O}\}$, *otherwise.*

Theorem 1.2.2 *[14] We have*

$$\Phi^{M}(3) = \{\mathbb{Z}/9\mathbb{Z}, \mathbb{Z}/6\mathbb{Z}, \mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}, \mathcal{O}\}.$$

Moreover, if $E : y^2 = x^3 + c$ is a Mordell curve defined over a cubic field K, then $T := E(K)_{tors}$ is isomorphic to

(1) $\mathbb{Z}/9\mathbb{Z}$,
- *if c is a square and $4c$ is a cube in K with $K = \mathbb{Q}(r)$ where r satisfying $r^3 - 3r^2 + 1 = 0$,*

(2) $\mathbb{Z}/6\mathbb{Z}$, $\begin{cases} \text{if } c \text{ is both square and cube in } K, \\ \text{or } c, 4 \text{ are cubes and } -3c \text{ is a square in } K, \end{cases}$

(3) $\mathbb{Z}/3\mathbb{Z}$, $\begin{cases} \text{if } c \text{ is a square and } 4c \text{ is a cube in } K \text{ with } K \neq \mathbb{Q}(r) \text{ where } r \\ \quad \text{satisfying } r^3 - 3r^2 + 1 = 0, \\ \text{or } c \text{ is a square but } 4c \text{ is not a cube in } K, \\ \text{or } 4c \text{ is a cube and } -3c \text{ is a square in } K, \end{cases}$

(4) $\mathbb{Z}/2\mathbb{Z}$, $\begin{cases} \text{if } c \text{ is a cube but not a square in } K \text{ and } -3c \text{ is not a square in } K, \\ \text{or } c \text{ is a cube but not a square in } K \text{ and } 4 \text{ is not a cube in } K, \end{cases}$

(5) $\{\mathcal{O}\}$, *otherwise.*

Theorem 1.2.3 *[14] We have*

$$\Phi_{\mathbb{Q}}^{M}(6) = \Phi_{\mathbb{Q}}^{M}(3) \cup$$

$$\{\mathbb{Z}/9\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}, \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}\}.$$

Moreover, if $K/\mathbb{Q}$ is a sextic field an if $E : y^2 = x^3 + c$ is a Mordell curve for any 6-th power-free integer c and ω be a primitive cubic root of unity, then $T := E(K)_{tors}$ is isomorphic to

(1) $\mathbb{Z}/9\mathbb{Z}$, $\begin{cases} \text{if } c \text{ is a square and } 4c \text{ is a cube in } K, \omega \notin K \text{ and } \mathbb{Q}(r) \subset K \text{ with } r \\ \quad \text{satisfying } r^3 - 3r^2 + 1 = 0, \end{cases}$

(2) $\mathbb{Z}/6\mathbb{Z}$, $\begin{cases} \text{if } c \text{ is both square and cube in } K \text{ and } \omega \notin K, \\ \text{or } c, 4 \text{ are cubes in } K \text{ and } -3c \text{ is a square in } K \text{ but } \omega \notin K, \end{cases}$

(3) $\mathbb{Z}/3\mathbb{Z}$, $\begin{cases} \text{if } c \text{ is a square but not a cube in } K \text{ and } 4c \text{ is not a cube in } K, \\ \text{or } c \text{ is a square and } 4c \text{ is a cube in } K, \omega \notin K \text{ and } \mathbb{Q}(r) \not\subset K \text{ with } r \\ \quad \text{satisfying } r^3 - 3r^2 + 1 = 0, \\ \text{or } c \text{ is not a cube in } K, 4c \text{ is a cube and } -3c \text{ is a square in } K \text{ but} \\ \omega \notin K, \end{cases}$

(4) $\mathbb{Z}/2\mathbb{Z}$, $\begin{cases} \text{if } c \text{ is a cube but not a square in } K \text{ and } 4 \text{ is not a cube in } K, \\ \text{or } c \text{ is a cube but not a square in } K \text{ and } -3c \text{ is not a square in } K, \end{cases}$

(5) $\mathbb{Z}/9\mathbb{Z}\oplus\mathbb{Z}/3\mathbb{Z}$, $\begin{cases} \text{if } c \text{ is a square and } 4c \text{ is a cube in } K, \omega \in K \text{ and } \mathbb{Q}(r) \subset K \text{ with } r \\ \quad \text{satisfying } r^3 - 3r^2 + 1 = 0, \end{cases}$

(6) $\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$, *if c is both square and cube in K, 4 is a cube in K and* $\omega \in K$,

(7) $\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, *if c is both square and cube in K, 4 is not a cube in K and* $\omega \in K$,

(8) $\mathbb{Z}/3\mathbb{Z}\oplus\mathbb{Z}/3\mathbb{Z}$, $\begin{cases} \text{if } c \text{ is a square and not a cube in } K, 4c \text{ is a cube in } K, \omega \in K \text{ and} \\ \quad \mathbb{Q}(r) \not\subset K \text{ with } r \text{ satisfying } r^3 - 3r^2 + 1 = 0, \end{cases}$

(9) $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, *if c is a cube but not a square in K and* $\omega \in K$,

(10) $\{\mathcal{O}\}$, *otherwise.*

Theorem 1.2.4 *[14] We have*

$$\Phi^M(6) = \Phi^M_{\mathbb{Q}}(6) \cup \{\mathbb{Z}/19\mathbb{Z}, \mathbb{Z}/7\mathbb{Z}, \mathbb{Z}/14\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}\}.$$

1.3 Preliminaries

1.3.1 Basics on Number field

In this section, we shall state some basics results in algebraic number theory which are useful later. All the results can be found in [52].

Proposition 1.3.1 *Let K be a number field and $\mathcal{O}_K$ be the ring of integers of K. For a prime number $p \in \mathbb{Z}$, the principal ideal can be written uniquely as a product of prime ideals. That is, $p\mathcal{O}_K = \mathcal{P}_1^{e_1} \cdots \mathcal{P}_r^{e_r}$ where $\mathcal{P}_1, \ldots, \mathcal{P}_r$ are prime ideals in $\mathcal{O}_K$ and r is some integer.*

Here e_i is called the *ramification index* of $\mathcal{P}_i$.

Definition 1.3.2 Let p be a prime number in $\mathbb{Z}$ and $\mathcal{P}$ be a prime ideal in $\mathcal{O}_K$ such that $\mathcal{P}\mathcal{O}_K \cap \mathbb{Z} = p\mathbb{Z}$. Then $\mathcal{O}_K/\mathcal{P}$ is a finite dimensional vector space over $\mathbb{Z}/p\mathbb{Z}$ and the dimension is $f = [\mathcal{O}_K/\mathcal{P} : \mathbb{Z}/p\mathbb{Z}]$. The number f is called the *residue degree* of $\mathcal{P}$.

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

Notation 1.3.4 For a number field K, we denote the algebraic closure of K by $\overline{K}$. The Galois group of $\overline{K}$ over K is denoted by $Gal(\overline{K}/K)$, where $Gal(\overline{K}/K)$ is the inverse limit of $Gal(L/K)$ as L varies over all finite Galois extensions of K.

1.3.2 Basics on elliptic curves over number field

Let K be a field. We consider elliptic curves as defined in Definition 1.1.2. If $char(\overline{K}) \neq 2$, then the substitution $y \mapsto \frac{1}{2}(y - a_1x - a_3)$ transforms E to the

form

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

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

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

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

$$y^2 = x^3 + ax + b, \qquad \text{for some } a, b \in K. \tag{1.1}$$

For any point $Q = (x, y)$ on the curve (1.1), we denote its reflection as $-Q = (-x, y)$. For any two points Q_1 and Q_2 on the curve, the line joining Q_1 and Q_2 cuts the curve E on the third point $Q_3 = Q_1 + Q_2$. We define "addition" of Q_1 and Q_2 by $Q_1 \oplus Q_2 = -Q_3$ which is a point on the curve. Since $E(K)$ forms a group under the binary operation $\oplus$, we want to describe duplication formula explicitly.

Addtion formula

Let $Q_1 = (x_1, y_1)$ and $Q_2 = (x_2, y_2)$ be two points on the curve (1.1) and $Q_3 = (x_3, y_3)$ be the point $Q_1 + Q_2$ as described above, where x_3 and y_3 can be computed as follows.

Case 1: $(x_1 \neq x_2)$

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

This line intersects the cubic E already in two points (x_1, y_1) and (x_2, y_2). For finding the third intersecting point, we substitute $y = \lambda x + \nu$ in the curve

(1.1) and get $y^2 = (\lambda x + \nu)^2 = x^3 + bx + c \Leftrightarrow x^3 - \lambda x^2 + (b - 2\lambda\nu)x + (c - \nu^2) = 0$ which we can write as

$$x^3 - \lambda x^2 + (b - 2\lambda\nu)x + (c - \nu^2) = (x - x_1)(x - x_2)(x - x_3). \tag{1.2}$$

After equating the coefficients of the x^2 term on both side, we get $\lambda^2 - a = x_1 + x_2 + x_3$ and thus

$$x_3 = \lambda^2 - x_1 - x_2, \text{ and } y_3 = \lambda x_3 + \nu. \tag{1.3}$$

Case 2: $(x_1 = x_2)$.

If $y_2 = -y_1$, then we get $Q_1 \oplus Q_2 = \mathcal{O}$, the point at infinity. If $y_2 = y_1$, then we calculate $Q_1 \oplus Q_1 = 2Q_1$. For the curve (1.1), we calculate the slope of the tangent which is given by,

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

Putting the value λ in the formula (1.3), we get the point $2Q_1$. Thus, we have

$$x \text{ coordinate of } 2Q_1 := x(2Q_1) = \frac{x^4 - 2bx^2 - 8cx + b^2}{4x^3 + 4bx + 4c}. \tag{1.4}$$

This formula is called as the *duplication formula*. Similarly one can calculate the y coordinate of $2Q_1 := y(2Q_1)$

$$= \frac{2x^6 + 4ax^5 + 10ax^4 + 40bx^3 - 10a^2x^2 - (4a^3 + 8ab)x - (2a^3 + 16b^2)}{8y^3}. \tag{1.5}$$

In a similar way, for an integer $n \geq 2$ and for any point P of an elliptic curve E, one can calculate $x(nP)$ and $y(nP)$. It turns out that they are rational functions in terms of x and y (see reference [89], Page: 110).

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

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

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

We observe that

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

and we define

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

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

Theorem 1.3.5 *([89], page:86) Let E be an elliptic curve defined over number field K. Then for any positive integer $n \geq 2$, the group of all n-torsion points $E[n] \cong \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$.*

Definition 1.3.6 Let $E : y^2 = x^3 + a_2x^2 + a_4x + a_6$ be an elliptic curve defined over K. For a $d \in K^*/(K^*)^2$, the *d-quadratic twist* of E is the curve E^d which is defined by the equation

$$y^2 = x^3 + da_2x^2 + d^2a_4x + d^3a_6.$$

In the following lemma, we get the structure of n-torsion subgroup involving the n-torsion subgroups of the given elliptic curve and its d-quadratic twist.

Lemma 1.3.7 ([39], Corollary 4) *Let E be an elliptic curve defined over a*

number field K. Let E^d be the d-quadratic twist of E for some $d \in K^*/(K^*)^2$. Then for any odd positive integer n,

$$E(K(\sqrt{d}))[n] \cong E(K)[n] \oplus E^d(K)[n].$$

Definition 1.3.8 [89] Let E_1 and E_2 be two elliptic curves defined over a field K. A *morphism* from E_1 to E_2 is a rational map which is regular at every point of E_1.

Definition 1.3.9 [89] Let E_1 and E_2 be elliptic curves. An *isogeny* from E_1 to E_2 is a morphism

$$\phi : E_1 \to E_2, \text{ satisfying } \phi(\mathcal{O}) = \mathcal{O}.$$

If both E_1 and E_2 are defined over a number field K, then an isogeny ϕ between them is called a K- *rational isogeny.*

A K-rational isogeny $\phi : E_1 \to E_2$ is called *K-rational isogeny of degree n* if the kernel of ϕ, denoted by $\ker \phi$, is $Gal(\bar{K}/K)$-invariant cyclic group of order n. In this case, we say that E/K has an *n-isogeny.*

Lemma 1.3.10 ([68], Proposition 14) *Let E be a rational elliptic curve and $K/\mathbb{Q}$ be a cubic field. Suppose $E(K)$ has a point of order 9. Then $E/\mathbb{Q}$ has either an isogeny of degree 9 or two independent isogenies of degree 3.*

Definition 1.3.11 Let $E : y^2 = x^3 + bx + c$ be an elliptic curve defined over the number field K. Then *j-invariant* of E is defined as

$$j = j(E) = 12^3 \frac{12b^3}{12b^3 + 27c^2}.$$

Theorem 1.3.12 *([89] Page: 45) Two elliptic curves defined over a number field K are isomorphic over $\overline{K}$ if and only if they both have the same j-invariant.*

Theorem 1.3.13 *[89] Let $K/\mathbb{Q}$ be a number field and $E : y^2 = x^3 + c$ be a Mordell curve defined over K. If an elliptic curve E' is isomorphic to E, then E' is of the from $y^2 = x^3 + c'$, where $c' = b^6 c$, for some $b \in K^*$.*

Theorem 1.3.14 *[51] Let E be an elliptic curve defined over a number field K and $P \in E(K)$ be a point of order at least 4. Then E can be written of the form*

$$y^2 + (1-c)xy - by = x^3 - bx^2 \tag{1.6}$$

for some $b, c \in K$ with $P = (0, 0)$.

The curve defined in (1.6) is called as the *Kubert-Tate normal form* of E, and we denote this curve simply by $E(b, c)$. The j-invariant of this elliptic curve is given by

$$j(b,c) = \frac{(16b^2 + 8b(1-c)(c+2) + (1-c)^4)^3}{b^3(16b^2 - b(8c^2 + 20c - 1) - c(1-c)^3)}. \tag{1.7}$$

1.3.3 Basics on elliptic curves over finite field

For a given elliptic curve $E : y^2 = x^3 + bx + c$ with $b, c \in \mathbb{Z}$, it is natural to look at E by reducing the co-efficients modulo a prime p.

Definition 1.3.15 Let $E : y^2 = x^3 + bx + c$ be an elliptic curve defined over number field K with discriminant $\Delta = 4b^3 - 27c^2$. If a prime number $p \in \mathbb{Z}$ satisfies the condition $p \nmid \Delta$, then we say E has *good reduction at prime p*. Let $\mathcal{P} \subset \mathcal{O}_K$ be a prime ideal lying above p. If $\mathcal{P}$ does not divide Δ, then we say that E has a *good reduction* at $\mathcal{P}$.

Notation 1.3.16 If E has good reduction at a prime p, then we denote $y^2 \equiv x^3 + bx + c \pmod{p}$ (equivalently $y^2 = x^3 + \overline{b}x + \overline{c}$) by $\overline{E}$.

In the following proposition, we record the nature of the reduction map over a given number field.

Proposition 1.3.17 ([13], Proposition 4) *Let E be an elliptic curve defined over K and T be the torsion subgroup of $E(K)$. Let $\mathcal{O}_K$ be the ring of integers of K and let $\mathcal{P}$ be a prime ideal in $\mathcal{O}_K$. Suppose E has good reduction at $\mathcal{P}$. Let ϕ be the reduction modulo $\mathcal{P}$ map on T which means the reduction map $\phi : T \longrightarrow \bar{E}(\mathcal{O}_K/\mathcal{P})$ is defined as $\phi(P) = \phi((x,y)) = \bar{P} = (\bar{x}, \bar{y})$ if $P \neq \mathcal{O}$ and $\phi(\mathcal{O}) = \bar{\mathcal{O}}$. Then, the reduction map ϕ is an injective homomorphism except for finitely many prime ideal $\mathcal{P}$.*

If E has good reduction at a prime $p \in \mathbb{Z}$, then $\overline{E} : y^2 = x^3 + \bar{b}x + \bar{c}$ is an elliptic curve defined over $\mathbb{F}_p$. Hasse-Weil theorem in [93] states that $-2\sqrt{p} \leq |\overline{E}(\mathbb{F}_p)| - p - 1 \leq 2\sqrt{p}$. Now, in the following three lemma we shall give information regarding the cardinality of torsion subgroups of elliptic curves defined over finite fields. Note that, since $\mathbb{F}_p$ is a finite field, $T = \overline{E}(\mathbb{F}_p)_{tors} = \overline{E}(\mathbb{F}_p)$.

Lemma 1.3.18 ([49], Lemma 5.12, p. 149) *Let $E : y^2 = x^3 + c$ be an elliptic curve for some nonzero integer c. Let $p \equiv 2 \pmod 3$ be a prime for which E has good reduction at p. Then, we have*

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

Lemma 1.3.19 ([12], Corollary 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 a prime for which E has good reduction at p. Then, for any natural number n, we have*

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

Lemma 1.3.20 *Let $E_p : y^2 = x^3 + c$ be an elliptic curve defined over $\mathbb{F}_{p^3}$ and assume that $p \equiv 2 \pmod 3$ be an odd prime. Then we have*

$$|E_p(\mathbb{F}_{p^3})| = p^3 + 1.$$

Proof. The multiplicative group $(\mathbb{F}_{p^3})^\times$ has order $p^3 - 1$. Since $p \equiv 2 \pmod 3$, we observe that $p^3 - 1 \not\equiv 0 \pmod 3$ and hence there is no element of order 3 in $(\mathbb{F}_{p^3})^\times$. Therefore, the homomorphism $a \to a^3$ is a bijection on $(\mathbb{F}_{p^3})^\times$. In particular, for each $y \in \mathbb{F}_{p^3}$, the element $y^2 - c$ has a unique cubic root, which we can consider as x. Thus, in this process, we obtain p^3 number of points on $E_p(\mathbb{F}_{p^3})$. With the additional point at infinity, we see that $E_p(\mathbb{F}_{p^3})$ has $p^3 + 1$ points. □

Now for given prime p, we see the existence of an elliptic curve with some specified relevant properties in the following proposition.

Proposition 1.3.21 ([93], Theorem 4.3, p. 98) *Let $q = p^n$ be a power of a prime p and set $N = q + 1 - a$. Then, there is an elliptic curve E defined over $\mathbb{F}_q$ such that $|E(\mathbb{F}_q)| = N$ iff $|a| \leq 2\sqrt{q}$ and a satisfies one of the following conditions.*

1. $\gcd(a, p) = 1$,
2. *n is even and $a = \pm 2\sqrt{q}$,*
3. *n is even, $p \not\equiv 1 \pmod 3$ and $a = \pm\sqrt{q}$,*
4. *n is odd, $p = 2$ or 3 and $a = \pm p^{(n+1)/2}$,*
5. *n is even, $p \not\equiv 1 \pmod 4$ and $a = 0$,*
6. *n is odd and $a = 0$.*

Definition 1.3.22 [93] Let K be a field with characteristic p and E be an elliptic curve defined over the field K. If $E[p] \cong \{\mathcal{O}\}$, then E is called *supersingular elliptic curve*.

In the next proposition and lemma, we provide some criteria to determine the supersingularity of elliptic curves which will be needed later.

Proposition 1.3.23 ([89], Theorem 4.1, p. 148) *Let $\mathbb{F}_q$ be a finite field of characteristic $p \geq 3$. Let E be an elliptic curve over $\mathbb{F}_q$ given by a Weierstrass equation*

$$E : y^2 = f(x),$$

where $f(x) \in \mathbb{F}_q[x]$ is a cubic polynomial with distinct roots in $\overline{\mathbb{F}}_q$. Then E is supersingular if and only if the coefficient of x^{p-1} in $f(x)^{(p-1)/2}$ is zero.

Lemma 1.3.24 ([93], Proposition 4.31, p. 130) *Let E be an elliptic curve over $\mathbb{F}_q$, where q is a power of the prime p. Let $a = q + 1 - |E(\mathbb{F}_q)|$. Then E is supersingular if and only if $a \equiv 0 \pmod{p}$.*

1.4 Proof of Theorem 1.2.1

Throughout this section, $K/\mathbb{Q}$ stands for a cubic number field. We denote a rational Mordell curve of the form $y^2 = x^3 + c$ for some integer c, simply by E. Also note T stands for the torsion subgroup of $E(K)$.

Lemma 1.4.1 *For any prime $q \geq 5$, there is no element in T of order q.*

Proof. Suppose there exists an element of order q in T. Then q divides $|T|$. Since $\gcd(2, 3q) = 1$, by Dirichlet's theorem on primes in arithmetic progressions, there exist infinitely many primes $p \equiv 2 \pmod{3q}$. Therefore there is a prime $p \equiv 2 \pmod{3q}$ such that E has good reduction at p. We consider such a prime and let

$p\mathcal{O}_K = \mathcal{P}_1^{e_1}\mathcal{P}_2^{e_2}\mathcal{P}_3^{e_3}$ be the ideal decomposition in $\mathcal{O}_K$ where $\mathcal{P}_1, \mathcal{P}_2, \mathcal{P}_3$ are prime ideals in $\mathcal{O}_K$ lying above p and $0 \leq e_i \leq 1$. For $i = 1, 2, 3$, if f_i's are the residual degree of $\mathcal{P}_i$, then by Proposition 1.3.3 we know that $e_1f_1 + e_2f_2 + e_3f_3 = 3$. Hence we have a prime ideal $\mathcal{P}_j$ with $f_j = 1$ or 3 for some $j = 1, 2, 3$.

Now, we consider the reduction mod $\mathcal{P}_j$ map. Since $p \equiv 2 \pmod 3$, by Lemma 1.3.19, we get $|\overline{E}(\mathcal{O}_K/\mathcal{P}_j)| = p^{f_j} + 1$. Hence by Proposition 1.3.17, q divides $|T|$ and thus we get $q \mid (p^{f_j} + 1)$. Since $p \equiv 2 \pmod 3$, we get $0 \equiv p^{f_j} + 1 \equiv 2^{f_j} + 1 \pmod q$. Since $f_j = 1$ or 3, we see that $3 \equiv 0 \pmod q$ or $9 \equiv 0 \pmod q$, which is a contradiction to $q \geq 5$. □

Lemma 1.4.2 *Let ω be a cube root of unity. Then,*

$$E(K)[2] \cong \begin{cases} \mathbb{Z}/2\mathbb{Z}, & \text{if } c^{\frac{1}{3}} \in K \text{ or } c^{\frac{1}{3}}\omega \in K \text{ or } c^{\frac{1}{3}}\omega^2 \in K, \\ \mathcal{O}, & \text{otherwise.} \end{cases}$$

Proof. If $P = (x, y)$ is a point of order 2, then $y = 0$ and x satisfies the polynomial equation $x^3 + c = 0$. If K contains either $c^{\frac{1}{3}}$ or $c^{\frac{1}{3}}\omega$ or $c^{\frac{1}{3}}\omega^2$, then $-x \in K$ which implies $(-x)^3 = c \in K$. Thus, in this case, $E(K)[2] \cong \mathbb{Z}/2\mathbb{Z}$; otherwise it is trivial. □

Lemma 1.4.3 *Let E be a rational Mordell curve. Then,*

$$E(K)[3] \cong \begin{cases} \mathbb{Z}/3\mathbb{Z}, & \text{if } c^{\frac{1}{2}} \in K, \\ & \text{or} \\ & \text{if } (-3c)^{\frac{1}{2}} \in K \text{ with } (4c)^{\frac{1}{3}} \in K \text{ or } (4c)^{\frac{1}{3}}\omega \in K \text{ or } (4c)^{\frac{1}{3}}\omega^2 \in K, \\ \mathcal{O}, & \text{otherwise,} \end{cases}$$

where ω is a cube root of unity.

Proof. If $P = (x, y)$ is a point of order 3, then x-coordinate of P satisfies $x(x^3 + 4c) = 0$.

If $x = 0$, then c is a square in K. In that case, we conclude that $E(K)[3] \cong \mathbb{Z}/3\mathbb{Z}$.

If $x \neq 0$, then we get $x^3 + 4c = 0$ and hence $y^2 = -3c$. Since $X^2 + 3$ is an irreducible polynomial over K, we note that $c = y^2$ and $-3c = y^2$ can not be true together. Hence, in this case, we get $E(K)[3] \cong \mathbb{Z}/3\mathbb{Z}$, if $(-3c)^{\frac{1}{2}} \in K$ with $(4c)^{\frac{1}{3}} \in K$ or $(4c)^{\frac{1}{3}}\omega \in K$ or $(4c)^{\frac{1}{3}}\omega^2 \in K$. □

Lemma 1.4.4 *T has no element of order 4.*

Proof. Suppose $P = (x, y) \in T$ is an element of order 4. Then, $2P$ is a point of order 2 and therefore

$$y(2P) = 0 \iff x^6 + 20cx^3 - 8c^2 = 0 \iff x^3 = -10c \pm 6c\sqrt{3}.$$

Since $x^3 \in K$, we see that $10c \pm 6c\sqrt{3} \in K$ which in turn implies $\sqrt{3} \in K$, which is a contradiction as K is a cubic field. This proves the lemma. □

Lemma 1.4.5 *Let E be a rational Mordell curve. Then,*

$$E(K)[6] \cong \begin{cases} \mathbb{Z}/6\mathbb{Z}, & \text{if } c \text{ is a square as well as cube in } K \text{ or} \\ & \text{if } c = -27 \text{ and } 4 \text{ is a cube in } K, \\ \mathbb{Z}/3\mathbb{Z}, & \text{if } c \text{ is a square but not a cube in } K \text{ or} \\ & \text{if } -3c \text{ is a square in } K \text{ and } 4c \text{ is a cube in } K, \\ \mathbb{Z}/2\mathbb{Z}, & \text{if } c \neq -27 \text{ is a cube but not a square in } K \text{ or} \\ & \text{if } c = -27 \text{ but } 4 \text{ is not a cube in } K, \\ \mathcal{O}, & \text{otherwise.} \end{cases}$$

Proof. **Case 1.** (c is a square as well as cube in K)

Since c is a square in K, by Lemma 1.4.3, there are two points of order 3 in $E(K)[6]$. Also, since c is a cube in K, by Lemma 1.4.2, there is only one point of order 2 in $E(K)[6]$. Hence, it has an element of order 6. Thus, we conclude that $E(K)[6] \cong \mathbb{Z}/6\mathbb{Z}$.

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

Since c is a cube in K, $E(K)[6]$ has only one element of order 2 by Lemma 1.4.2. If $E(K)[6]$ has an element of order 3, by Lemma 1.4.3, we see that $-3c$ is a square and $4c$ is a cube in K. Since both c and $4c$ are cubes, we see that 4 is a cube in K. Again, if c is not a cube of an integer, we observe that $K = \mathbb{Q}(c^{1/3})$, which is not possible as c is not a power of 2. Hence c is a cube of an integer. As $[K : \mathbb{Q}] = 3$, we observe that $-3c$ is also a square of an integer. Now, combining the above two facts, we obtain $c = -27$. Therefore, in this case, $E(K)[6] \cong \mathbb{Z}/6\mathbb{Z}$ when 4 is a cube in K.

Thus, if $c \neq -27$ or 4 is not a cube in K, we conclude that $E(K)[6] \cong \mathbb{Z}/2\mathbb{Z}$.

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

Since c is not a cube in K, by Lemma 1.4.2, $E(K)[6]$ has no element of order 2. Again, since c is a square, by Lemma 1.4.3, we conclude that $E(K)[6] \cong \mathbb{Z}/3\mathbb{Z}$.

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

Since c is not a cube in K, by Lemma 1.4.2, $E(K)[6]$ has no element of order 2. If $E(K)[6]$ has an element of order 3, by Lemma 1.4.3, we see that $-3c$ is a square in K and $4c$ is a cube in K. Thus, we conclude that $E(K)[6] \cong \mathbb{Z}/3\mathbb{Z}$.□

Lemma 1.4.6 *T has an element of order 9 if and only if $c = 16$ and $K = \mathbb{Q}(r)$ with r satisfying the relation $r^3 - 3r^2 + 1 = 0$.*

Proof. Let $P = (x, y)$ be an element of order 9 in $E(K)_{tors}$. Then $3P$ is a point of order 3 in $E(K)_{tors}$ and hence we get $x(3P)(x(3P)^3 + 4c) = 0$.

If $(x(3P)^3 + 4c) = 0$, then $c = -\frac{a^3}{4}$ for some $a \in K$, where $x(3P) = a$. Now, let α be the slope of the line joining P and $2P$. Then by the addition formula, we have

$$\alpha^2 - x - \frac{x(x^3 - 8c)}{4(x^3 + c)} = a = x(3P),$$

where $\alpha = \left(\frac{7x^6 - 4cx^3 + 16c^2}{6xy(x^3 + 4c)}\right)^2$.

This equation can be written explicitly as

$$x^9 - 9ax^8 + 24a^3x^6 + 18a^4x^5 + 3a^6x^3 - 9a^7x^2 - a^9 = 0.$$

By substituting $x = at$ for some $t \in K$, the above equation becomes

$$t^9 - 9t^8 + 24t^6 + 18t^5 + 3t^3 - 9t^2 - 1 = 0.$$

Using *magma*, we see that the polynomial $f(X) = X^9 - 9X^8 + 24X^6 + 18X^5 + 3X^3 - 9X^2 - 1$ is irreducible over $\mathbb{Q}$. Since $[K : \mathbb{Q}] = 3$, the relation $t^9 - 9t^8 + 24t^6 + 18t^5 + 3t^3 - 9t^2 - 1 = 0$ is impossible. Therefore we get $x(3P)^3 + 4c \neq 0$.

Thus, we conclude $x(3P) = 0$, which implies that c is a square in K. Again, by the addition formula, we get

$$\left(\frac{7x^6 - 4cx^3 + 16c^2}{6xy(x^3 + 4c)}\right)^2 - x - \frac{x(x^3 - 8c)}{4(x^3 + c)} = 0.$$

The above equation reduces to

$$(x^3 + c)(x^9 - 96cx^6 + 48c^2x^3 + 64c^3) = 0.$$

If $x^3 + c = 0$ then we have $2P = \mathcal{O}$, which is a contradiction to P is of order 9.

Hence we get

$$x^9 - 96cx^6 + 48c^2x^3 + 64c^3 = 0. \tag{1.8}$$

Putting $4c = t \in K$, the above equation further reduces to

$$x^9 - 24tx^6 + 3t^2x^3 + t^3 = 0.$$

This equation can be rewritten as

$$(x^3 + t)^3 = 27tx^6, \tag{1.9}$$

which shows that t is a cube in K, say v^3 for some $v \in K$. Since cube root of unity, $\omega \notin K$, from equation (1.9), we have

$$x^3 + v^3 = 3vx^2.$$

After Substituting $\frac{x}{v} = r \in K$, the above equation reduces to

$$r^3 - 3r^2 + 1 = 0. \tag{1.10}$$

Since the polynomial $r^3 - 3r^2 + 1$ is an irreducible polynomial and K is a cubic field, we see that $K = \mathbb{Q}(r)$. As the equation (1.10) has three real roots, $\mathbb{Q}(r)/\mathbb{Q}$ is a normal extension.

Also we have $\dfrac{y^2}{c} = \dfrac{x^3}{c} + 1$. Since c is a square in K with $c = \dfrac{v^3}{4}$ and $r = \dfrac{x}{v}$, by putting $\gamma = y/\sqrt{c} \in K$, we get

$$\gamma^2 = 4r^3 + 1. \tag{1.11}$$

Combining equations (1.10) and (1.11), we have

$$\gamma^6 - 99\gamma^4 + 243\gamma^2 - 81 = 0,$$

which further implies

$$(\gamma^3 - 9\gamma^2 - 9\gamma + 9)(\gamma^3 + 9\gamma^2 - 9\gamma - 9) = 0.$$

By letting $f(X) = X^3 - 9X^2 - 9X + 9$, we see that either $f(\gamma) = 0$ or $f(-\gamma) = 0$. Without loss of generality, we assume $f(\gamma) = 0$. Since $f(X)$ is irreducible over $\mathbb{Q}$, we conclude that $K = \mathbb{Q}(r) = \mathbb{Q}(\gamma)$.

Hence, if T has a point of order 9 in K, then c is a square in K and $4c$ is a cube in K such that $K = \mathbb{Q}(r)$ with r satisfying the relation $r^3 - 3r^2 + 1 = 0$.

Now, we assume that $4c$ is not a cube of an integer. Therefore, we have $\mathbb{Q}((4c)^{1/3}) = \mathbb{Q}(r)$ which is not possible as $\mathbb{Q}(r)/\mathbb{Q}$ is a normal extension but $\mathbb{Q}((4c)^{1/3})/\mathbb{Q}$ is not a normal extension. Thus $4c$ is a cube of an integer. Since $[K : \mathbb{Q}] = 3$, we have c is a square of an integer also. Thus, we conclude that $c = 16$.

Conversely, we have that c is a square in K and $4c$ is a cube in K where $K = \mathbb{Q}(r)$ with r satisfying the relation $r^3 - 3r^2 + 1 = 0$. Therefore, we can show that $((4c)^{1/3}r, \pm c^{1/2}\gamma_1)$, $((4c)^{1/3}r, \pm c^{1/2}\gamma_2)$ and $((4c)^{1/3}r, \pm c^{1/2}\gamma_3)$ are all points of order 9 in K, where $\gamma_1, \gamma_2, \gamma_3$ are roots of the equation $\gamma^3 - 9\gamma^2 - 9\gamma + 9 = 0$.□

Lemma 1.4.7 *T has no element of order* 18 *and* 27.

Proof. Suppose T has an element of order 18 or 27. Hence there exists an element of order 9 in T. Thus, by Lemma 1.4.6, we have $c = 16$ and $K = \mathbb{Q}(r)$ with r satisfying the relation $r^3 - 3r^2 + 1 = 0$. In this case, by using *magma*, we see that $T \cong \mathbb{Z}/9\mathbb{Z}$, which is a contradiction. Hence T has no element of order

18 or 27. □

Now we are ready to prove Theorem 1.2.1.

Proof of Theorem 1.2.1. 1.4.1, 1.4.4, 1.4.5, 1.4.6 and 1.4.7, we conclude that the possible orders of any element of T is either 2 or 3 or 6 or 9 and the proof follows. □

1.5 Proof of Theorem 1.2.2

Throughout this section, $K/\mathbb{Q}$ stands for a cubic number field. We denote a Mordell curve of the form $y^2 = x^3 + c$ with $c \in K$, simply by E. Also, we denote T as the torsion subgroup of $E(K)$.

Lemma 1.5.1 *For any odd prime $q \geq 5$, there is no element in T of order q.*

Proof. Suppose there exists an element of order q in T. Then q divides $|T|$. Since $\gcd(2, 3q) = 1$, by Dirichlet's theorem on primes in arithmetic progressions, there exist infinitely many primes $p \equiv 2 \pmod{3q}$. Therefore there is a prime $p \equiv 2 \pmod{3q}$ such that E has good reduction at p. We can consider such a prime and also assume that $p\mathcal{O}_K = \mathcal{P}_1^{e_1}\mathcal{P}_2^{e_2}\mathcal{P}_3^{e_3}$ is the ideal decomposition in $\mathcal{O}_K$ where $\mathcal{P}_1, \mathcal{P}_2, \mathcal{P}_3$ are prime ideals in $\mathcal{O}_K$ lying above p and $0 \leq e_i \leq 1$. If f_i's are then residual degree of $\mathcal{P}_i$ for $i = 1, 2, 3$, then we know that $e_1f_1 + e_2f_2 + e_3f_3 = 3$. Therefore there exists a prime ideal $\mathcal{P}_j$ such that $f_j = 1$ or 3 for some $j = 1, 2, 3$

Now, we consider the reduction mod $\mathcal{P}_j$ map. Note that $|\mathcal{O}_K/\mathcal{P}_|| = p^{f_j}$, where $f_i = 1$ or 3. Since $p \equiv 2 \pmod 3$, by Lemma 1.3.19 and 1.3.20, we get $|\overline{E}(\mathcal{O}_K/\mathcal{P}_j)| = p^{f_j} + 1$. Proposition 1.3.17 assures that we can find a prime p which satisfies all above conditions along with the map $\phi : T \longrightarrow \bar{E}(\mathcal{O}_K/\mathcal{P}_j)$ is injective. As q divides $|T|$, we conclude that $q \mid (p^{f_j} + 1)$. Since $p \equiv 2 \pmod 3$, we get $0 \equiv p^{f_j} + 1 \equiv 2^{f_j} + 1 \pmod q$. We observe that $f_j = 1$ or 3 implies either

$3 \equiv 0 \pmod{q}$ or $9 \equiv 0 \pmod{q}$ respectively. It is a contradiction to the fact that q is a prime greater than or equal to 5. □

Lemma 1.5.2 *Let ω be a cube root of unity. Then,*

$$E(K)[2] \cong \begin{cases} \mathbb{Z}/2\mathbb{Z}, & \text{if } c^{\frac{1}{3}} \in K \text{ or } c^{\frac{1}{3}}\omega \in K \text{ or } c^{\frac{1}{3}}\omega^2 \in K, \\ \mathcal{O}, & \text{otherwise.} \end{cases}$$

Proof. Proof is similar to the proof of Lemma 1.4.2 and we omit the proof here. □

Lemma 1.5.3 *Let ω be a cube root of unity. Then,*

$$E(K)[3] \cong \begin{cases} \mathbb{Z}/3\mathbb{Z}, & \text{if } c^{\frac{1}{2}} \in K, \\ & \text{or} \\ & \text{if } (-3c)^{\frac{1}{2}} \in K \text{ with } (4c)^{\frac{1}{3}} \in K \text{ or } (4c)^{\frac{1}{3}}\omega \in K \\ & \text{or } (4c)^{\frac{1}{3}}\omega^2 \in K, \\ \mathcal{O}, & \text{otherwise.} \end{cases}$$

Proof. Proof is similar to the proof of Lemma 1.4.3 and we omit the proof here. □

Lemma 1.5.4 *T has no element of order 4.*

Proof. Proof is similar to the proof of Lemma 1.4.4 and hence we omit the proof here. □

Lemma 1.5.5 *Let E be a Mordell curve over K. Then,*

$$E(K)[6] \cong \begin{cases} \mathbb{Z}/6\mathbb{Z}, & \text{if } c \text{ is a square as well as cube in } K \text{ or }, \\ & \text{if } -3c \text{ is a square in } K \text{ and } c, 4c \text{ are cubes in } K, \\ \mathbb{Z}/3\mathbb{Z}, & \text{if } c \text{ is a square but not a cube in } K \text{ or}, \\ & \text{if } -3c \text{ is a square in } K \text{ and } 4c \text{ is a cube in } K \text{ but} \\ & \quad c \text{ is not a cube in } K, \\ \mathbb{Z}/2\mathbb{Z}, & \text{if } c \text{ is a cube but not a square in } K \text{ and} \\ & \quad -3c \text{ is not a square in } K \text{ or}, \\ & \text{if } c \text{ is a cube but not a square in } K \text{ and} \\ & \quad 4c \text{ is not a cube in } K, \\ \mathcal{O}, & \text{otherwise.} \end{cases}$$

Proof. **Case 1.** (c is a square as well as cube in K)

Since c is a square in K, by Lemma 1.5.3, there are two points of order 3 in $E(K)[6]$. Also, since c is a cube in K, by Lemma 1.5.2, there is only one point of order 2 in $E(K)[6]$. Hence, it has an element of order 6. Thus, we conclude that $E(K)[6] \cong \mathbb{Z}/6\mathbb{Z}$.

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

Since c is a cube in K, $E(K)[6]$ has only one element of order 2 by Lemma 1.5.2. If $E(K)[6]$ has an element of order 3, by Lemma 1.5.3, we see that $-3c$ is a square in K and $4c$ is a cube in K. In this case, $E(K)[6] \cong \mathbb{Z}/6\mathbb{Z}$. Thus, if $-3c$ is not a square in K or $4c$ is not a cube in K, we obtain that $E(K)[6] \cong \mathbb{Z}/2\mathbb{Z}$.

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

Since c is not a cube in K, by Lemma 1.5.2, $E(K)[6]$ has no element of order 2. Since c is a square, by Lemma 1.5.3, we conclude that $E(K)[6] \cong \mathbb{Z}/3\mathbb{Z}$.

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

Since c is not a cube in K, by Lemma 1.5.2, $E(K)[6]$ has no element of order 2. If $E(K)[6]$ has an element of order 3, by Lemma 1.5.3, we see that $-3c$ is a square in K and $4c$ is a cube in K. Thus, we conclude that $E(K)[6] \cong \mathbb{Z}/3\mathbb{Z}$.□

Lemma 1.5.6 *T has an element of order 9 if and only if c is a square in K, $4c$ is a cube in K and $K = \mathbb{Q}(r)$ with r satisfying the relation $r^3 - 3r^2 + 1 = 0$.*

Proof. Proof is similar to the proof of Lemma 1.4.6 and we omit it here. □

Lemma 1.5.7 *T has no element of order 27.*

Proof. We assume that there exists an element of order 27 in T. Then 27 divides $|T|$. Since $\gcd(2, 27) = 1$, by Dirichlet's theorem on primes in arithmetic progressions, there exist infinitely many primes $p \equiv 2 \pmod{27}$. Therefore there is a prime $p \equiv 2 \pmod{27}$ such that E has good reduction at p. We consider such a prime and also assume $p\mathcal{O}_K = \mathcal{P}_1^{e_1}\mathcal{P}_2^{e_2}\mathcal{P}_3^{e_3}$ is the ideal decomposition in $\mathcal{O}_K$ where $\mathcal{P}_1, \mathcal{P}_2, \mathcal{P}_3$ are prime ideals in $\mathcal{O}_K$ lying above p and $0 \leq e_i \leq 1$. If f_i's are the residual degrees of $\mathcal{P}_i$ for $i = 1, 2, 3$, then we know that $e_1f_1+e_2f_2+e_3f_3 = 3$. Then there exists a prime ideal $\mathcal{P}_j$ such that $f_j = 1$ or 3 for some $j = 1, 2, 3$

Since $f_j \in \{1, 3\}$, we know $|\overline{E}(\mathcal{O}_K/\mathcal{P}_j)| \in \{p + 1, p^3 + 1\}$ by Lemmas 1.3.19 and 1.3.20. Again since the reduction map $\phi : T \longrightarrow \bar{E}(\mathcal{O}_K/\mathcal{P}_j)$ is injective except for finitely many primes, we conclude that $|T|$ divides $|\bar{E}(\mathcal{O}_K/\mathcal{P}_j)|$ and hence 27 divides $|\bar{E}(\mathcal{O}_K/\mathcal{P}_j)|$. This is impossible as $p \equiv 2 \pmod{27}$. Hence there is no element of order 27 in the group T. □

Lemma 1.5.8 *T has no element of order 18.*

Proof. Assume that T has a point of order 18. Then it has a point of order 2, which forces $c = a^3$ for some $a \in K$. Since T has a point of order 9, say

$P = (x, y)$, then we have

$$x^{12} - 95a^3x^9 - 48a^6x^6 + 112a^9x^3 + 64a^{12} = 0.,$$

from the proof of Lemma 1.4.6.

After substituting $t = \frac{x}{a} \in K$, the above equation reduces to

$$t^{12} - 95t^9 - 48t^6 + 112t^3 + 64 = 0 \Rightarrow (t^3 + 1)(t^9 - 96t^6 + 48t^3 + 64) = 0.$$

Since $(t^3 + 1) \neq 0$, we have $(t^9 - 96t^6 + 48t^3 + 64) = 0$. Now consider the polynomial $f(t) = (t^9 - 96t^6 + 48t^3 + 64)$ and using *magma*, we get that $f(t)$ is an irreducible polynomial in $\mathbb{Z}[t]$. Hence $[\mathbb{Q}(t) : \mathbb{Q}] = 9$, which is a contradiction as $t \in K$ and $[K : \mathbb{Q}] = 3$. Hence there is no point of order 18 in T. □

Proof of Theorem 1.2.2. By Lemmas 1.5.1, 1.5.2, 1.5.3, 1.5.4, 1.5.6, 1.5.7 and 1.5.8, we conclude that the only possible orders of any nontrivial element of T is either 2 or 3 or 6 or 9 and the proof follows. □

1.6 Proof of Theorem 1.2.3

Throughout this section K stands for a sextic field. We denote a rational Mordell curve of the form $y^2 = x^3 + c$ for $c \in \mathbb{Z}$, simply by E. We also denote T as the torsion subgroup of $E(K)$.

Lemma 1.6.1 *Let $q > 3$ be any prime. Then there does not exist any element of order q in T.*

Proof. Suppose there exists an element of order q in T. Then q divides $|T|$. Sine $\gcd(2, 3q) = 1$, by Dirichlet's theorem on primes in arithmetic progressions, there exist infinitely many primes $p \equiv 2 \pmod{3q}$. Therefore there is a prime

$p \equiv 2 \pmod{3q}$ such that E has good reduction at p. We consider such a prime and assume that $p\mathcal{O}_K = \mathcal{P}_1^{e_1} \cdots \mathcal{P}_6^{e_6}$ is the ideal decomposition in $\mathcal{O}_K$ where $\mathcal{P}_1, \ldots, \mathcal{P}_6$ are prime ideals in $\mathcal{O}_K$ lying above p and $0 \leq e_i \leq 1$. If f_i's are then residual degree of $\mathcal{P}_i$ for $i = 1, \ldots, 6$, then we know that $\sum_{i=1}^{6} e_i f_i = 6$. Therefore there exists a prime ideal $\mathcal{P}_j$ such that f_j is either 1 or 2 or 3 or 6 for some $j = 1, 2, \ldots, 6$.

Now, we consider the reduction mod $\mathcal{P}_j$ map. Now we have $|\mathcal{O}_K/\mathcal{P}_j| = p^{f_j}$, where $f_j = 1, 2, 3$ or 6. Since $p \equiv 2 \pmod 3$, we get $|\overline{E}(\mathcal{O}_K/\mathcal{P}_j)| \mid (p^3 + 1)^2$ by Lemma 1.3.19. Proposition 1.3.17 assures that we can find a prime p which satisfies all above conditions along with the map $\phi : T \longrightarrow \bar{E}(\mathcal{O}_K/\mathcal{P}_j)$ is injective. As q divides $|T|$, we conclude that $q \mid (p^3 + 1)$. But we also have $p \equiv 2 \pmod q$, which implies $p^3 + 1 \equiv 9 \pmod q$. It is a contradiction as $q > 3$. Hence there does not exist any point of order $q > 3$. □

Lemma 1.6.2 *Let E be a rational Mordell curve. Then*

$$E(K)[2] \cong \begin{cases} \mathbb{Z}/2\mathbb{Z}, & \text{if } c^{\frac{1}{3}} \text{ or } c^{\frac{1}{3}}\omega \text{ or } c^{\frac{1}{3}}\omega^2 \in K \text{ but } \sqrt{-3} \notin K \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}, & \text{if } \sqrt{-3} \text{ and } c^{\frac{1}{3}} \in K \\ \mathcal{O}, & \text{otherwise,} \end{cases}$$

where ω is a cube root of unity.

Proof. We consider two cases as follows.

Case 1. The polynomial $X^3 + c$ is reducible in $\mathbb{Q}[X]$.

In this case $c = a^3$ for some non zero integer a. Therefore, $x^3 + a^3 = (x + a)(x^2 - ax + a^2) = 0$ implies that the point $(-a, 0)$ is a solution or $(\omega a, 0)$ and $(\omega^2 a, 0)$ are two solutions. Thus, we conclude that the point of order 2 is

$$P = \begin{cases} (-a, 0) & \text{if } \sqrt{-3} \notin K \\ (-a, 0), (\omega a, 0), (\omega^2 a, 0) & \text{if } \sqrt{-3} \in K \end{cases}.$$

Case 2. The polynomial $X^3 + c$ is irreducible over $\mathbb{Q}$.

In this case, if $c^{\frac{1}{3}} \in K$ and $\sqrt{-3} \in K$, then $(-c^{\frac{1}{3}}, 0)$, $(\omega c^{\frac{1}{3}}, 0)$ and $(\omega^2 c^{\frac{1}{3}}, 0)$ are points of order 2 in T. If $\sqrt{-3} \notin K$, then $(-c^{\frac{1}{3}}, 0)$ is the only point of order 2 whenever $c^{\frac{1}{3}} \in K$.

Hence combining both the cases we have the result. □

Lemma 1.6.3 *Let E be a rational Mordell curve. Then*

$$E(K)[3] \cong \begin{cases} \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}, & \text{if } (4c)^{\frac{1}{3}}, \sqrt{-3} \text{ and } \sqrt{-3c} \in K \\ \mathbb{Z}/3\mathbb{Z}, & \text{if } (4c)^{\frac{1}{3}} \text{ and } \sqrt{-3c} \in K \text{ but } \sqrt{c} \notin K \\ & \text{or } \sqrt{c} \in K \text{ but } \sqrt{-3} \text{ or } (4c)^{\frac{1}{3}} \notin K \\ \mathcal{O} & \text{otherwise.} \end{cases}$$

Proof. If $P = (x, y)$ be a point of order 3 in T, then

$$x(x^3 + 4c) = 0.$$

Case 1. $x = 0$.

In this case, $y^2 = c$ and hence $\sqrt{c} \in K$. Therefore, $(0, \pm\sqrt{c})$ are the only possible points of order 3 in T.

Case 2. $x \neq 0$.

In this case, we have $x^3 + 4c = 0$ and hence $y^2 = -3c$. Therefore $(-(4c)^{\frac{1}{3}}, \pm\sqrt{-3c})$, $(-(4c)^{\frac{1}{3}}\omega, \pm\sqrt{-3c})$ or $(-(4c)^{\frac{1}{3}}\omega^2, \pm\sqrt{-3c})$ are the possible points of order 3 in T.

Combining both cases we have the desired result. □

Lemma 1.6.4 *T does not have any element of order 4.*

Proof. We assume that $P = (x, y)$ is an element of order 4 in T. Then we note $y(2P) = 0 \iff x^6 + 20cx^3 - 8c^2 = 0 \iff x^3 = -10c \pm 6c\sqrt{3}$. Since $x \in K$, we

get $x^3 \in K$ and we already have $c \in K$. Thus, we get $\frac{x^3+10c}{6c} = \sqrt{3} \in K$. Hence, we conclude $K = K_1(\sqrt{3})$, where K_1 is a cubic subfield of K. If $c^{\frac{1}{3}} \in K_1$, then we get $x = (-1 \pm \sqrt{3})c^{\frac{1}{3}} \in K$.

Since $y \in K$, we can write $y = t_1 + t_2\sqrt{3}$ for some $t_1, t_2 \in K_1$. Since $y^2 = x^3 + c \in K = K_1(\sqrt{3})$, we get $(t_1 + t_2\sqrt{3})^2 = (-10c \pm 6c\sqrt{3}) + c \in K$. Since $\{1, \sqrt{3}\}$ is a basis of K over K_1, we get two relations which are $t_1^2 + 3t_2^2 = -9c$ and $t_1t_2 = \pm 3c$. These two relations together imply $t_1^2 + 3t_2^2 \pm 3t_1t_2 = 0$. Putting $t = \dfrac{t_1}{t_2} \in K_1$, we get

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

This implies that $\sqrt{3} \in K_1$ which is a contradiction as K_1 is a cubic extension over $\mathbb{Q}$. This contradiction implies that $c^{\frac{1}{3}} \notin K$ and thus we get $x \notin K$. Hence, we conclude that there does not exist any element of order 4 in $E(K)_{tors}$. □

Lemma 1.6.5 *T has an element of order 9 if and only if c is a square, $4c$ is a cube in K and $\mathbb{Q}(r) \subset K$ with r satisfying the relation $r^3 - 3r^2 + 1 = 0$..*

Proof. Let $P = (x, y)$ be an element of order 9 in $E(K)_{tors}$.

Then following the proof of Lemma 1.4.6, x satisfies the polynomial equation

$$(x^3 + t)^3 = 27tx^6,$$

where $t = 4c \in K$ with c is a square in K. From this equation we observe that t is a cube in K, say v^3 for some $v \in K$. Then we can write

$$(x^3 + v^3 - 3vx^2)(x^3 + v^3 - 3v\omega x^2)(x^3 + v^3 - 3v\omega^2 x^2) = 0,$$

where ω is a cube root of unity. Substituting $\dfrac{x}{v} = r_1 \in K$, $\dfrac{x}{v\omega} = r_2 \in K$ and

$\frac{x}{v\omega^2} = r_3 \in K$, the above equation reduces to

$$r^3 - 3r^2 + 1 = 0, \tag{1.12}$$

where $r \in K$ is one of r_1, r_2 and r_3. Since the polynomial $r^3 - 3r^2 + 1$ is an irreducible polynomial and K is a cubic field, we see that $\mathbb{Q}(r) \subset K$ is a cubic extension over $\mathbb{Q}$. Also, note that $\mathbb{Q}(r)/\mathbb{Q}$ is a normal extension as the equation (1.12) has three real roots.

Also we have $\frac{y^2}{c} = \frac{x^3}{c} + 1$. Since c is a square in K with $c = \frac{v^3}{4}$ and $r = \frac{x}{v}$, by putting $\gamma = y/\sqrt{c} \in K$, we get

$$\gamma^2 = 4r^3 + 1. \tag{1.13}$$

Combining equations (1.12) and (1.13), we have

$$\gamma^6 - 99\gamma^4 + 243\gamma^2 - 81 = 0,$$

which further implies,

$$(\gamma^3 - 9\gamma^2 - 9\gamma + 9)(\gamma^3 + 9\gamma^2 - 9\gamma - 9) = 0.$$

By letting $f(X) = X^3 - 9X^2 - 9X + 9$, we see that either $f(\gamma) = 0$ or $f(-\gamma) = 0$. Without loss of generality, we assume $f(\gamma) = 0$. Since $f(X)$ is irreducible over $\mathbb{Q}$, we conclude that $\mathbb{Q}(\gamma) \subset K$ is a cubic extension over $\mathbb{Q}$. Since $r \in \mathbb{Q}(\gamma)$, we observe that $\mathbb{Q}(\gamma) = \mathbb{Q}(r)$.

Hence, if T has a point of order 9 in K, then c is a square and $4c$ is a cube in K where $\mathbb{Q}(r) \subset K$ with r satisfying the relation $r^3 - 3r^2 + 1 = 0$.

Conversely, if c is a square in K and $4c$ is a cube in K where $\mathbb{Q}(r) \subset$

K with r satisfying the relation $r^3 - 3r^2 + 1 = 0$, then we can show that $((4c)^{1/3}r, \pm c^{1/2}\gamma_1), ((4c)^{1/3}r, \pm c^{1/2}\gamma_2), ((4c)^{1/3}r, \pm c^{1/2}\gamma_3)$ are points of order 9 in K, where $\gamma_1, \gamma_2, \gamma_3$ are roots of the equation $\gamma^3 - 9\gamma^2 - 9\gamma + 9 = 0$. In fact if $\omega \notin K$, then there are 6 points of order 9 in T and if $\omega \in K$, then there are 18 points of order 9 in T. □

Lemma 1.6.6 *T has no element of order 27.*

Proof. Suppose T has an element of order 27. Hence there exists an element of order 9 in T. Thus, by Lemma 1.6.5, we see that c is a square, $4c$ is a cube in K and $K = \mathbb{Q}(r)$ with r satisfying the relation $r^3 - 3r^2 + 1 = 0$. Hence $K = \mathbb{Q}(r)(\sqrt{d})$ for some $d \in (\mathbb{Q}(r)/\mathbb{Q}(r)^2)^*$. Then, by Lemma 1.3.7, we have

$$E(K)[27] \cong E(\mathbb{Q}(r))[27] \times E^d(\mathbb{Q}(r))[27].$$

Since, by Lemma 1.5.7, there are no points of order 27 in $E(\mathbb{Q}(r))$ and $E^d(\mathbb{Q}(r))$, we conclude that there are no elements of order 27 in $E(K)$. □

Lemma 1.6.7 *T has no element of order 18.*

Proof. Proof is similar to the proof of Lemma 1.5.8 and we omit here. □

Proof of Theorem 1.2.3. By Lemmas 1.6.1, 1.6.2, 1.6.3, 1.6.4, 1.6.5, 1.6.6 and 1.6.7, we conclude that the only possible orders for the nontrivial torsion points in T are $2, 3, 6$ and 9.

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

Subcase *a*. ($\sqrt{-3} \notin K$)

Since c is a square in K, there are two points of order 3 by Lemma 1.6.3. Again c is a cube in K implies that there is only one point of order 2 in T by Lemma 1.6.2. Hence, $T \cong \mathbb{Z}/6\mathbb{Z}$.

Subcase *b*. $(\sqrt{-3} \in K)$

Since c is a square in K, there are eight points of order 3 by Lemma 1.6.3, if $4^{\frac{1}{3}} \in K$. Also c is a cube in K provides that there are three points of order 2 in T by Lemma 1.6.2. Hence, in this case, $T \cong \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$. If $4^{\frac{1}{3}} \notin K$, then there are only two points of order 3 by Lemma 1.6.3 and we obtain $T \cong \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

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

In this case, write $c = a^3$ for $a \in K$.

Subcase *a*. $(\sqrt{-3} \in K)$

Since c is a cube in K, there are three points of order 2 in T by Lemma 1.6.2. Also we observe that there does not exist any element of order 3 by Lemma 1.6.3. Hence, $T \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

Subcase *b*. $(\sqrt{-3} \notin K)$

In this case, $(-a, 0)$ is the only point of order 2 in T by Lemma 1.6.2. If $-3c$ is a square in K and $4^{\frac{1}{3}} \in K$, then there are two points of order 3 by Lemma 1.6.3. Since T is abelian, it has an element of order 6 and hence $T \cong \mathbb{Z}/6\mathbb{Z}$. If $-3c$ is not a square in K or $4^{\frac{1}{3}} \notin K$, then there does not exist any element of order 3 in T by Lemma 1.6.3 and we conclude $T \cong \mathbb{Z}/2\mathbb{Z}$.

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

At first we observe that there are no elements of order 2 in T.

Subcase *a*. $(\sqrt{-3} \in K)$

Since c is square in K, there are 8 points of order 3 in T by Lemma 1.6.3 whenever $4c$ is a cube in K. If $\mathbb{Q}(r) \subset K$ with r satisfying $r^3 - 3r^2 + 1 = 0$, then by Lemma 1.6.5, there are 18 points of order 9 in T and thus $T \cong \mathbb{Z}/9\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$. If $\mathbb{Q}(r) \not\subset K$, then there are no points of order 9 in T and Hence $T \cong \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$. If $4c$ is not a cube in K, then there are two points of order 3 in T by Lemma 1.6.3 and we obtain $T \cong \mathbb{Z}/3\mathbb{Z}$.

Subcase *b*. ($\sqrt{-3} \notin K$)

In this case, there are two elements of order 3 in T by Lemma 1.6.3. If $4c$ is a cube in K and $\mathbb{Q}(r) \subset K$ with r satisfying $r^3 - 3r^2 + 1 = 0$, then by Lemma 1.6.5, there are 6 points of order 9 in T and thus $T \cong \mathbb{Z}/9\mathbb{Z}$. If $4c$ is a cube in K and $\mathbb{Q}(r) \not\subset K$, then there are no points of order 9 in T and Hence $T \cong \mathbb{Z}/3\mathbb{Z}$. If $4c$ is not a cube in K, then we have $T \cong \mathbb{Z}/3\mathbb{Z}$.

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

Since c is not a cube, there are no elements of order 2 in T. If $4c$ is a cube in K and $-3c$ is a square in K, then there are two elements of order 3 in T and in that case, $T \cong \mathbb{Z}/3\mathbb{Z}$.

Hence combining all the cases, Theorem 1.2.3 follows. □

1.7 Proof of Theorem 1.2.4

If K varies over all sextic number fields and E varies over all elliptic curves with complex multiplication over K, then, in [9] Clark *et al.,* computed the following all possible collection of torsion subgroups;

$$E(K)_{tors} \in \begin{cases} \mathbb{Z}/m\mathbb{Z} \text{ for } m = 1, 2, 3, 4, 6, 7, 9, 10, 14, 18, 19, 26, \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z} \text{ for } m = 2, 4, 6, 14, \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z} \text{ for } m = 3, 6, 9, \\ \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}. \end{cases} \tag{1.14}$$

Now onwards, throughout this section, K stands for a sextic numer field and we denote the Mordell curve of the form $y^2 = x^3 + c$ for $c \in K$, simply by E.

Since any Mordell curve belongs to the family of elliptic curves with complex multiplication, (1.14) provides all possible collection for $E(K)_{tors}$.

If we restrict $c \in \mathbb{Q}$, then by Theorem 1.2.3 we have already proved

$$E(K)_{tors} \in \Phi_{\mathbb{Q}}^{M}(6) = \begin{cases} \mathbb{Z}/m\mathbb{Z} \text{ for } m = 1, 2, 3, 6, 9, \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z} \text{ for } m = 2, 6, \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z} \text{ for } m = 3, 9, \\ \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}. \end{cases}$$

Now, our task is to eliminate some groups listed in (1.14) and we show that the other groups in the above listing (1.14) can occur as $E(K)_{tor}$.

Lemma 1.7.1 *The groups $\mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ do not appear as $E(K)_{tors}$, for any K.*

Proof. It is enough to prove that there is no element of order 4 in $E(K)_{tors}$. By the similar approach of the proof of Lemma 1.6.4, one can prove the result and we omit the proof here. □

Lemma 1.7.2 *The groups $\mathbb{Z}/10\mathbb{Z}$ and $\mathbb{Z}/26\mathbb{Z}$ do not appear as $E(K)_{tors}$, for any K.*

Proof. It is enough to prove that there do not exist any element of order 5 and 13 in $E(K)_{tors}$. Let us assume that there exists a point of order ℓ in $E(K)_{tors}$, where ℓ is either 5 or 13. Then, ℓ divides $|E(K)_{tors}|$. Now, we set $q = 13$. Since $\gcd(5, 12q) = 1$, by Dirichlet's theorem on primes in arithmetic progressions, there are infinitely many primes $p \equiv 5 \pmod{12q}$. We consider such a prime and also assume $p\mathcal{O}_K = \mathcal{P}_1^{e_1} \cdots \mathcal{P}_6^{e_6}$ is the ideal factorization in $\mathcal{O}_K$ where $\mathcal{P}_1, \ldots, \mathcal{P}_6$ are prime ideals in $\mathcal{O}_K$ lying above p and with $0 \leq e_i \leq 1$. Also we know that $\sum_{i=1}^{6} e_i f_i = 6$ where f_i's are residual degree for $\mathcal{P}_i$'s. Hence we can choose a prime ideal for which residual degree is either $1, 2, 3$ or 6.

Let $\mathcal{P}_i$ be such a prime ideal and consider the reduction modulo $\mathcal{P}_i$ map. Note that $|\mathcal{O}_K/\mathcal{P}_i| = p^{f_i}$, where $f_i = 1, 2, 3$ or 6.

Since 2 and 3 both divide 6, it is enough to calculate $|\overline{E}(\mathcal{O}_K/\mathcal{P}_i)|$ only for $f_i = 6$. Since $p \equiv 2 \pmod 3$, by Proposition 1.3.23, we see that E is a supersingular elliptic curve over $\mathbb{F}_{p^6}$. Therefor, we get $E(\mathbb{F}_{p^6}) = p^6 + 1 - a$ with $|a| \leq 2p^3$. Also, by Lemma 1.3.24, we get $p \mid a$ and by Proposition 1.3.21, we have either $a = \pm p^3$ or $\pm 2p^3$.

Also, for $f_i = 1, 2, 3$ or 6, we have either $|\overline{E}(\mathcal{O}_K/\mathcal{P}_i)|$ divides $(p^3 \pm 1)^2$ or $|\overline{E}(\mathcal{O}_K/\mathcal{P}_i)|$ divides $(p^6 \pm p^3 - 1)$. Proposition 1.3.17 assures that we can find a prime p which satisfies all above conditions along with the map $\phi : T \longrightarrow \bar{E}(\mathcal{O}_K/\mathcal{P}_j)$ is injective. As q divides $|T|$, we conclude that $q \mid (p^3 \pm 1)$ or $q \mid (p^6 \pm p^3 - 1)$ that is, $13 \mid (p^3 \pm 1)$ or $13 \mid (p^6 \pm p^3 - 1)$. Since $p \equiv 5 \pmod q \equiv 5 \pmod{13}$ and ℓ is either 5 or 13, we see that $\ell \not| (p^3 \pm 1)$ and $\ell \not| (p^6 \pm p^3 - 1)$, which is a contradiction. Hence there does not exist any point of order 5 or 13. This completes the proof. □

Lemma 1.7.3 *The group $\mathbb{Z}/14\mathbb{Z}$ does not appear as $E(K)_{tors}$, for any K.*

Proof. Suppose $E(K)_{tors} \cong \mathbb{Z}/14\mathbb{Z}$. In this case, we first observe that $E(K)[2] \cong \mathbb{Z}/2\mathbb{Z}$. Since $E(K)_{tors}$ has a point of order 2, we see that c is a cube in K, say, $c = a^3$ for some $a \in K$. Since $E(K)_{tors}$ contains exactly one nontrivial point of order 2, by Lemma 1.6.2, we get $\sqrt{-3} \notin K$. Let $P = (x, y)$ be a point of order 7 in $E(K)_{tors}$. Then the corresponding division polynomial equation is

$$(7t^2 - 4t + 16)(t^6 + 564t^5 - 5808t^4 - 123136t^3 - 189696t^2 - 49152t + 4096) = 0,$$

where $t = \frac{x^3}{a^3} \in K$.

If $(7t^2 - 4t + 16) = 0$, then we get $t = \frac{2 \pm 6\sqrt{-3}}{7}$. This is a contradiction as

$\sqrt{-3} \notin K$. Thus,

$$t^6 + 564t^5 - 5808t^4 - 123136t^3 - 189696t^2 - 49152t + 4096 = 0. \qquad (1.15)$$

Putting $t = s^3 = (\frac{x}{a})^3$ in (1.15), we get

$$s^{18} + 564s^{15} - 5808s^{12} - 123136s^9 - 189696s^6 - 49152s^3 + 4096 = 0.$$

Using *magma*, we conclude that the polynomial in s variable is an irreducible polynomial over $\mathbb{Q}$, which is a contradiction as $s \in K$ and $[K : \mathbb{Q}] = 6$. Therefore there does not exist a point of order 7 in $E(K)_{tors}$. Hence the group $\mathbb{Z}/14\mathbb{Z}$ does not appear as a torsion subgroup in $E(K)$. □

Lemma 1.7.4 *The group $\mathbb{Z}/18\mathbb{Z}$ does not appear as $E(K)_{tors}$, for any K.*

Proof. Proof of this lemma is similar to the proof of Lemma 1.5.8 and we omit the proof here. □

Lemma 1.7.5 *The group $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$ does not appear as $E(K)_{tors}$, for any K.*

Proof. At first observe that $E(K)[2] \ncong \{\mathcal{O}\}$ and hence c is a cube in K. Since $E(K)_{tors}$ contains eight nontrivial elements of order 3, by Lemma 1.6.3 we conclude that $\sqrt{-3} \in K$. Since $\sqrt{-3} \in K$ and c is a cube in K, by Lemma 1.6.2 we see that $E(K)_{tors}$ has three points of order 2. This is a contradiction as there is only one nontrivial point of order 2 in $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$. □

Lemma 1.7.6 *The groups $\mathbb{Z}/19\mathbb{Z}, \mathbb{Z}/7\mathbb{Z}$, and $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$ appear as a torsion subgroup of $E(K)$ for some K.*

Proof. **Case 1:** $(\mathbb{Z}/19\mathbb{Z})$

In this case, we let $K = \mathbb{Q}[e]/ < e^6 + e^4 - e^3 - 2e^2 + e + 1 >$ and consider the elliptic curve E over K in Kubert-Tate Normal form as

$$E(2e^5 - e^4 + 2e^3 - 4e^2 + 2, 2e^5 - 2e^4 + 4e^3 - 4e^2 - 2e + 3).$$

Then by Theorem 1.3.14, E is a Mordell curve over K. Hence, by a calculation in [9], page 523, we get $E(K)_{tors} \simeq \mathbb{Z}/19\mathbb{Z}$.

Case 2: $(\mathbb{Z}/7\mathbb{Z})$

We let $K = \mathbb{Q}(2^{\frac{1}{3}}, \zeta_3)$, where ζ_3 is a cube root of unity. Then by Theorem 1.3.14, the elliptic curve $E(\zeta_3, -1)$ over K is in Kubert-Tate Normal form. Therefore, by the equation (1.7), we get $j(E) = 0$ and by Theorem 1.3.13, E is a Mordell curve over K. Hence, by a calculation in [9], page 521, we get $E(K)_{tors} \cong \mathbb{Z}/7\mathbb{Z}$.

Case 3: $(\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z})$

We let $K = \mathbb{Q}((6\zeta_3 + 30)^{\frac{1}{3}}))$, where ζ_3 is a cube root of unity. Then, we consider the elliptic curve $E : y^2 = x^3 - \frac{\zeta_3+5}{36}$ over K. In this case, using *magma*, we can prove that $E(K)_{tors} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$. □

Hence proof of Theorem 1.2.4 follows by Lemmas 1.7.1, 1.7.2, 1.7.3, 1.7.4, 1.7.5 and 1.7.6. □

CHAPTER 2

Quadratic non-residues and non-primitive roots satisfying a coprimality condition

Let $q \geq 1$ be any integer and let $\epsilon \in [\frac{1}{11}, \frac{1}{2})$ be a given real number. In this chapter, we prove that for all primes p satisfying

$$p \equiv 1 \pmod{q}, \quad \log\log p > \frac{\log 6.83}{\frac{1}{2} - \epsilon} \text{ and } \frac{\phi(p-1)}{p-1} \leq \frac{1}{2} - \epsilon,$$

there exists a quadratic non-residue g which is not a primitive root modulo p such that $gcd\left(g, \frac{p-1}{q}\right) = 1$.

2.1 Introduction

Let p be an odd prime number. We know that there are exactly $\frac{p-1}{2}$ quadratic residues as well as non-residues modulo p. It is a well known fact that the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic (see [4]). An element of $(\mathbb{Z}/p\mathbb{Z})^*$ is called a *primitive root* modulo p if it is a generator of this cyclic group.

The distribution of quadratic residues, non-residues and primitive roots is a very fundamental area in number theory and has been a topic of immense interest to mathematicians for centuries.

In this chapter, we deal with the question that how many quadratic residue (respectively, non-residue) g module p satisfying the condition $\gcd(g, p-1) = 1$?

Since there are $\phi(p-1)$ numbers among $1, 2, \ldots, p-1$ which are co -prime to $p-1$ and roughly half of them are quadratic residues (respectively, non-residues), we expect the answer to the above question is $\frac{\phi(p-1)}{2}$. In fact, we estimate this in Theorem 2.3.11.

Since $\frac{\phi(p-1)}{2}$ is large enough, it is possible to ask the same question in subsets like the set of all primitive roots and its complement in the set of all non-residues modulo p.

In 2010, Levin, Pomerance and Soundararajan [54] showed the existence of a primitive root with the aforementioned co-primality condition. More precisely, they proved the following result.

Theorem 2.1.1 *For all prime numbers $p \geq 5$, there exists a primitive root g modulo p which satisfies the condition $gcd(g, p-1) = 1$.*

Levin, Pomerance and Soundararajan [54] considered this problem (Theorem 2.1.1) to tackle a particular case of an important problem in computational number theory, namely, discrete log problem. More precisely, they prove Theorem 2.1.1 to tackle the fixed point discrete log problem as follows,

Question 2.1.2 *For a given primitive root g in $(\mathbb{Z}/p\mathbb{Z})^*$, does there exists an integer $t \in [1, p-1]$ such that $g^t \equiv t \pmod{p}$?*

Indeed, Theorem 2.1.1 solves the fixed point discrete log problem affirmatively. In this chapter, we deal with the similar problem (in Corollary 2.2.2) for quadratic non-residues which are not primitive roots. For notational convenience, we abbreviate 'a quadratic non-residue which is not a primitive root' by QNRNP modulo p.

Earlier also, QNRNP modulo p has been considered in several articles. For instance in [40], Gun *et al.* proved the following theorem which gives information regarding consecutive QNRNPs modulo p.

Theorem 2.1.3 *Let $\epsilon \in (0, \frac{1}{2})$ be fixed and N be any positive integer. Assume that p is a prime number with $p \geq \exp((\frac{2}{\epsilon})^{8N})$ and satisfying $\frac{\phi(p-1)}{p-1} \leq \frac{1}{2} - \epsilon$. Then there exist N consecutive QNRNP's modulo p.*

For further information on this related problem, see [40], [43] and [57]. Motivated by Theorems 2.1.1 and 2.1.3, in this chapter, we prove the following Theorem 2.2.1 for QNRNP residues.

2.2 Main results

Theorem 2.2.1 *[5] Let $q \geq 1$ be an integer and $\epsilon \in [\frac{1}{11}, \frac{1}{2})$. Let p be a prime satisfying*

$$p \equiv 1 \pmod{q}, \quad \log\log p > \frac{\log 6.83}{\frac{1}{2} - \epsilon} \text{ and } \frac{\phi(p-1)}{p-1} \leq \frac{1}{2} - \epsilon.$$

Assume $N_p = \{g : 1 \leq g \leq p-1, g \text{ is QNRNP and } \gcd(g, \frac{p-1}{q}) = 1\}$. Then

$$N_p = \phi\left(\frac{p-1}{q}\right)\left(\frac{q}{2} - \frac{q}{p-1}\phi(p-1)\right) + O\left(p^{1-\epsilon}\frac{\phi(p-1)}{p-1}\log p\right).$$

In particular, there exists an integer g satisfying $1 < g < p-1$ and $gcd\left(g, \frac{p-1}{q}\right) = 1$ such that g is a QNRNP modulo p and when $q = 1$, there exists an integer g with $1 < g < p-1$ and $gcd(g, p-1) = 1$ such that g is a QNRNP modulo p.

In the statement of Theorem 2.2.1, one of the conditions on p is a natural condition. If $\frac{\phi(p-1)}{p-1} = \frac{1}{2}$, then one can easily check that every non-residue modulo p is a primitive root modulo p. The condition $\frac{\phi(p-1)}{p-1} \leq \frac{1}{2} - \epsilon$ makes sure that $p-1$ has enough odd prime factors and hence abundance of QNRNP residues modulo p.

As an application, we solve the fixed point discrete log problem for the cyclic subgroup (analogous to Question 2.1.2) generated by a QNRNP as follows.

Corollary 2.2.2 *[5] Let $\epsilon \in [\frac{1}{11}, \frac{1}{2})$ be a real number. Let p be a prime satisfying*

$$\log\log p > \frac{\log 6.83}{\frac{1}{2} - \epsilon} \text{ and } \frac{\phi(p-1)}{p-1} \leq \frac{1}{2} - \epsilon.$$

Then there is a QNRNP g and an integer $x \in [1, p-1]$ such that x is QNRNP and $g^x \equiv x \pmod{p}$.

In [54], first they proved their result for all large primes and used the computations to check their result for small primes. However, computations may be cumbersome in our result stated in Theorem 2.2.1 because of various parameters.

2.3 Preliminaries

In this section, we start with the definition of *character of a group*.

Definition 2.3.1 Ler G be an arbitrary group. A complex-valued function f defined on G is called a *character of G* if f has the following multiplicative

property

$$f(ab) = f(a)f(b),$$

for all $a, b \in G$ and $f(c) \neq 0$ for some $c \in G$.

Every group G has one character, namely, the function which is identity on G. This is called the *principal character of* G. It is well known that *a finite abelian group* G *of order* n *has exactly* n *distinct characters* (see for instance [4]).

Let G be a finite abelian group of order n and the principal character of G is denoted by f_1. Other characters are denoted by $f_2, f_3, \ldots, f_n$ and let $\widehat{G} = \{f_1, \ldots, f_n\}$. We can define a binary operation on $\widehat{G}$ as

$$(f_i f_j)(g) = f_i(g) f_j(g),$$

for all $g \in G$.

Theorem 2.3.2 *(Dual group of G) [4] The set* $\widehat{G}$ *forms an abelian group of order* n *with respect to the above binary operation and it is called as the dual group of* G*. Moreover,* $G \cong \widehat{G}$ *also holds.*

Let G be a finite abelian group of order n. Also let f be a character of G. Since G is a group, the multiplicative property of f implies that $f(G)$ is a group and f is a group homomorphism from G onto $f(G)$. Since $|G| = n$, by the homomorphism property of f, we see that $f(g)^n = 1$, for all $g \in G$. Thus, it implies $f(G) \cong \mu_n$, the multiplicative group of n-th roots of unity.

In this chapter, we take G to be $(\mathbb{Z}/p\mathbb{Z})^*$, for any odd prime p. Hence, any homomorphism $\chi : G \to \mu_{p-1}$ is a character of $(\mathbb{Z}/p\mathbb{Z})^*$. Since $(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic, $\widehat{(\mathbb{Z}/p\mathbb{Z})^*}$ is also cyclic.

Also assume that $\chi : (\mathbb{Z}/p\mathbb{Z})^* \to \mu_{p-1}$ is a character modulo p such that

χ is a generator of $\widehat{(\mathbb{Z}/p\mathbb{Z})^*}$. For all integers ℓ with $0 \leq \ell \leq p-2$, we get $\chi^\ell(\zeta) = \chi(\zeta^\ell)$ is also a character modulo p. Write $(\mathbb{Z}/p\mathbb{Z})^* = \{\chi_0, \chi_1, \ldots, \chi_{p-2}\}$ with χ_0 is the principal character and $\chi_\ell = \chi^\ell$.

As we mentioned in introduction, an element $\zeta \in (\mathbb{Z}/p\mathbb{Z})^*$ is said to be a primitive root modulo p if ζ generates the cyclic group $(\mathbb{Z}/p\mathbb{Z})^*$. Hence, we easily see that QNRNP's are precisely the elements of the set $\{\zeta^\ell : \ell = 1, 3, \ldots, p-2 \text{ and } (\ell, p-1) > 1\}$.

Suppose $\chi(\zeta) = \eta$. Since χ is a generator of the dual group of $(\mathbb{Z}/p\mathbb{Z})^*$ and ζ is a primitive root modulo p, we get that η is a primitive $(p-1)$-th root of unity. Since χ is a homomorphism, $\chi(\zeta^i) = \chi^i(\zeta) = \eta^i$ holds. Hence, by the above observation, we get

$$\chi(\kappa) = \eta^\ell \text{ with } (\ell, p-1) > 1, \ell \text{ odd} \Leftrightarrow \kappa \text{ is QNRNP module } p. \tag{2.1}$$

Following [40], for non negative integer ℓ, we define

$$\beta_\ell(p-1) = \sum_{\substack{1 \leq i \leq p-1 \\ i \quad odd \\ (i,p-1)>1}} (\eta^i)^\ell \qquad \text{and} \qquad \alpha_\ell(p-1) = \sum_{\substack{1 \leq i \leq p-1 \\ (i,p-1)=1}} (\eta^i)^\ell, \tag{2.2}$$

where $\alpha_\ell(p-1)$ is known as *Ramanujan sums*.

Now, we list some basic lemmas and results which will be useful to us in course of the proof of Theorem 2.2.1.

Lemma 2.3.3 *[40] For all integers ℓ with $0 < \ell < p-1$, we have*

$$\beta_\ell(p-1) = -\alpha_\ell(p-1).$$

Proof. Since

$$\sum_{i=0}^{p-1} \eta^i = 0 = \sum_{i=0}^{\frac{p-3}{2}} \eta^{2i}$$

holds, we get the lemma. □

Lemma 2.3.4 *(characteristic function for QNRNP's) [40] For any $x \in (\mathbb{Z}/p\mathbb{Z})^*$, we have*

$$\sum_{\ell=0}^{p-2} \beta_\ell (p-1)\chi_\ell(x) = \begin{cases} p-1; & \text{if } x \text{ is a QNRNP,} \\ 0; & \text{otherwise.} \end{cases}$$

Proof. Since $x \in (\mathbb{Z}/p\mathbb{Z})^*$, let $x \not\equiv 0 \pmod{p}$. Also, let η be a primitive $(p-1)$-th root of unity. Now we consider $\eta^{i_1}, \eta^{i_2}, \ldots, \eta^{i_k}$, where $1 < i_1 < \cdots < i_k \leq p-2$ and $(i_j, p-1) > 1$ with i_j is odd for all $j = 1, \ldots, k$. Now, the expression

$$1 + \eta^{i_m}\chi_1(x) + (\eta^{i_m})^2\chi_2(x) + \cdots + (\eta^{i_m})^{p-2}\chi_{p-2}(x)$$

gives the value $p-1$ if $(\chi_1(x))^{-1} = \eta^{i_m}$ and zero otherwise whenever $x \neq 0$. Equivalently, $\chi_1(x) = \eta^{-i_m}$ with $(-i_m.p-1) > 1 \Leftrightarrow x$ is a QNRNP. Thus, by summing over m, the above resulting expressions, we get

$$\begin{aligned} &\sum_{m=1}^{k} \left(1 + \eta^{i_m}\chi_1(x) + (\eta^{i_m})^2\chi_2(x) + \cdots + (\eta^{i_m})^{p-2}\chi_{p-2}(x)\right) \\ &= \sum_{m=1}^{k} (\eta^{i_m})^0\chi_0(x) + \sum_{m=1}^{k} (\eta^{i_m})^1\chi_1(x) + \cdots + \sum_{m=1}^{k} (\eta^{i_m})^{p-2}\chi_{p-2}(x) \\ &= \beta_0(p-1)\chi_0(x) + \cdots + \beta_{p-2}(p-1)\chi_{p-2}(x), \text{ by (2.2)} \\ &= \begin{cases} p-1; & \text{if } x \text{ is a QNRNP,} \\ 0; & \text{otherwise.} \end{cases} \end{aligned}$$

which completes the proof of the lemma. □

Now, we shall state some basic definitions and results as follows.

Definition 2.3.5 [66] For any positive integer n, the Möbius function μ is

$\mu(1) = 1$ and for $n > 1$, we write $n = p_1^{a_1} \dots p_k^{a_k}$ and define

$$\mu(n) = \begin{cases} (-1)^k; & \text{if } a_1 = \cdots = a_k = 1, \\ 0; & \text{otherwise.} \end{cases}$$

Lemma 2.3.6

(1) (Page no. 167 in [84] and Chapter-3 in [66])

Let $\omega(n)$ denote the number of distinct prime divisors of n. Then we have

$$\omega(p-1) \leq (1.385)\frac{\log p}{\log \log p}$$

for all primes $p \geq 5$.

(2) [4] For any positive integer n, let $\mu(n)$ denote the Möbius function. Then, we have

$$\sum_{d|n} \mu(d) = \begin{cases} 1; & \text{if } n = 1, \\ 0; & \text{if } n > 1. \end{cases}$$

(3) [90] For any odd prime p and any divisor q of $p-1$, we have

$$\sum_{d|\frac{p-1}{q}} |\mu(d)| = 2^{\omega\left(\frac{p-1}{q}\right)}.$$

(4) [65, 85] For any integer $n > 90$, we have $\phi(n) > \frac{n}{\log n}$, where $\phi(n)$ is the Euler's totient-function.

Proof. (1) The proof of this part is little technical and we omit the proof here.

(2) When $n = 1$, this result is trivially true from Definition 2.3.5. For $n > 1$, we write $n = p_1^{a_1} \dots p_k^{a_k}$.

Also note that, $\mu(d)$ gives nonzero value whenever $d = 1$ or d is a product of distinct prime numbers.

Hence, we get

$$\begin{aligned}\sum_{d|n}\mu(d) &= 1+\mu(p_1)+\cdots+\mu(p_k)+\sum_{1\le i<j\le k}\mu(p_ip_j)+\cdots+\mu(p_1\cdots p_k)\\ &= 1+\binom{k}{1}(-1)+\binom{k}{2}(-1)^2+\cdots+\binom{k}{k}(-)^k\\ &= (1-1)^k=0.\end{aligned}$$

(3) At first, let $\omega(\frac{p-1}{q}) = n$ and we write $\frac{p-1}{q} = p_1^{a_1}\cdots p_n^{a_n}$.

Now,

$$\begin{aligned}2^n &= 1+\binom{n}{1}\cdot 1+\binom{n}{2}\cdot 1^2+\cdots+\binom{n}{n}\cdot 1^n\\ &= 1+\binom{n}{1}\cdot|-1|+\binom{n}{2}\cdot|(-1)^2|+\cdots+\binom{n}{n}\cdot|(-1)^n|\\ &= |\mu(1)|+|\mu(p_1)|+\cdots+|\mu(p_k)|+\sum_{1\le i<j\le n}|\mu(p_ip_j)|+\cdots+|\mu(p_1\cdots p_n)|\\ &= \sum_{d|n}|\mu(d)|\end{aligned}$$

and the proof follows.

(4) New elementary proof of this result can be found in [85].

□

Lemma 2.3.7 *(Theorem: 272 in [41]) If* $\gcd(\ell, m) = a$, *then*

$$\alpha_\ell(m) = \phi(m)\frac{\mu(\frac{m}{a})}{\phi(\frac{m}{a})}.$$

Lemma 2.3.8 *[90] We have,*

$$\sum_{\ell=0}^{p-2} |\alpha_\ell(p-1)| = 2^{\omega(p-1)}\phi(p-1).$$

Proof. Using Lemma 2.3.7, we get

$$\begin{aligned}\sum_{\ell=0}^{p-2} |\alpha_\ell(p-1)| &= \sum_{\ell=0}^{p-2} \phi(p-1)\frac{|\mu\left(\frac{p-1}{\gcd(\ell,p-1)}\right)|}{\phi\left(\frac{p-1}{\gcd(\ell,p-1)}\right)} \\ &= \phi(p-1)\sum_{d|p-1,d>0} \frac{|\mu(\frac{p-1}{d})|}{\phi(\frac{p-1}{d})}\phi\left(\frac{p-1}{d}\right) \\ &= \phi(p-1)2^{\omega(p-1)}, \qquad \text{by Lemma 2.3.6(3).}\end{aligned}$$

□

The following result is a standard theorem to estimate a character sum over an interval which was first proved by Pólya and I.M.Vinogradov independently. The proof of this theorem can be found in [4].

Theorem 2.3.9 *(Pólya-Vinogradov) Let p be any odd prime and χ be a non-principal character modulo p. Then, for any integers $0 \leq M < N \leq p-1$, we have,*

$$\left|\sum_{m=M}^{N} \chi(m)\right| \leq \sqrt{p}\log p.$$

Later, this theorem has been studied in literature by several mathematicians. In 2011, D. A. Frolenkov provided a numerically explicit version of Pólya-Vinogradov which was an improvement of the previous version by C. Pomerance [77]. In 2013, D.A. Frolenkov and K. Soundararajan[24] obtained a sharper version which is as follows.

Theorem 2.3.10 *[24] Let $p \geq 100$ be any odd prime and χ be a non-principal*

character modulo p. Then, for any integers $0 \leq M < N \leq p-1$, we have,

$$\left|\sum_{m=M}^{N} \chi(m)\right| \leq \frac{\sqrt{p}}{\pi\sqrt{2}}(\log p + 6) + \sqrt{p}.$$

Assuming a little improvement of Pólya-Vinogradov, improvement of some well known theorems have been shown (see for instance [59, 23]). Smoothed version of Pólya-Vinogradov can be found in [1].

In the following theorem, we estimate the number of quadratic non-residues modulo p which are coprime with $p-1$. Though this estimate is expected, we include here for completeness.

Theorem 2.3.11 *Let $q \geq 1$ be an integer and $\epsilon \in (0, \frac{1}{2})$. Let p be a prime satisfying*

$$p \equiv 1 \pmod{q} \text{ and } \log\log p > \frac{\log 2.63}{\frac{1}{2} - \epsilon}.$$

Consider the set $Q_p := \{g : 1 < g < p-1, \left(\frac{g}{p}\right) = -1 \text{ and } gcd\left(g, \frac{p-1}{q}\right) = 1\}$. Then, we get

$$Q_p = \frac{q}{2}\phi\left(\frac{p-1}{q}\right) + O\left(p^{1-\epsilon}\log p\right).$$

In particular, when $q = 1$, for all prime $p > \exp 7.19$, there exists an integer g with $1 < g < p-1$ and $gcd(g, p-1) = 1$ such that g is a non-residue modulo p.

Proof. Let $q \geq 1$ be a given integer and let $\epsilon \in (0, \frac{1}{2})$ be also given. Now, we consider all primes $p \equiv 1 \pmod{q}$ with $\log\log p > \frac{\log 2.63}{\frac{1}{2}-\epsilon}$. By Dirichlet's theorem on primes in arithmetic progressions, we can see that there are infinitely many such primes.

For any integer m, we get the following characteristic function of quadratic

non-residues.

$$g(m) := \frac{1}{2}\left(1 - \left(\frac{m}{p}\right)\right) = \begin{cases} 1; & \text{if } m \text{ is a quadratic non-residue,} \\ 0; & \text{for otherwise.} \end{cases}$$

By letting $Q_p := \sum_{\substack{m=1 \\ (m, \frac{p-1}{q})=1}}^{p-1} g(m)$, we see that Q_p counts the number of Quadratic non-residues in $\{1, \dots, p-1\}$ which are relatively prime with $\frac{p-1}{q}$.

To finish the proof of Theorem 2.3.11, it suffices to prove that $Q_p \geq 1$ for all primes $p > \exp 7.19$ satisfying $p \equiv 1 \pmod{q}$.

Therefore, we consider

$$\begin{aligned} Q_p &= \sum_{\substack{m=1 \\ \left(m, \frac{p-1}{q}\right)=1}}^{p-1} g(m) \\ &= \frac{1}{2} \sum_{\substack{m=1 \\ \left(m, \frac{p-1}{q}\right)=1}}^{p-1} \left(1 - \left(\frac{m}{p}\right)\right) \\ &= \frac{1}{2}\left(q\phi\left(\frac{p-1}{q}\right) - \sum_{\substack{m=1 \\ \left(m, \frac{p-1}{q}\right)=1}}^{p-1} \left(\frac{m}{p}\right)\right), \end{aligned}$$

where we have used the fact that the number of integers m in $\{1, \dots, p-1\}$ such that $\left(m, \frac{p-1}{q}\right) = 1$ is $q\phi\left(\frac{p-1}{q}\right)$. Now, we see that

$$\begin{aligned} Q_p - \frac{1}{2}q\phi\left(\frac{p-1}{q}\right) &= -\frac{1}{2}\sum_{m=1}^{p-1}\left(\frac{m}{p}\right) \sum_{d \mid \left(m, \frac{p-1}{q}\right)} \mu(d), \text{ by Lemma 2.3.6 (2)} \\ &= -\frac{1}{2}\sum_{m=1}^{p-1}\left(\frac{m}{p}\right) - \frac{1}{2}\sum_{m=1}^{p-1}\left(\frac{m}{p}\right) \sum_{\substack{d \mid \left(m, \frac{p-1}{q}\right) \\ d>1}} \mu(d) \end{aligned}$$

$$= 0 - \frac{1}{2}\sum_{d|\frac{p-1}{q}} \mu(d) \sum_{t=1}^{\frac{p-1}{d}} \left(\frac{d}{p}\right)\left(\frac{t}{p}\right)$$

$$= -\frac{1}{2}\sum_{d|\frac{p-1}{q}} \mu(d)\left(\frac{d}{p}\right) \sum_{t=1}^{\frac{p-1}{d}} \left(\frac{t}{p}\right).$$

Hence, by Theorem 2.3.9 and Lemma 2.3.6 (3), we get

$$\left|Q_p - \frac{1}{2}q\phi\left(\frac{p-1}{q}\right)\right| \leq \frac{1}{2}\sum_{d|\frac{p-1}{q}} |\mu(d)| \left|\sum_{t=1}^{\frac{p-1}{d}} \left(\frac{t}{p}\right)\right| \leq \frac{1}{2}\cdot 2^{\omega\left(\frac{p-1}{q}\right)}\sqrt{p}\log p. \quad (2.3)$$

Now observe that for $\epsilon \in (0, \frac{1}{2})$ if $p > \exp\exp\frac{\log 2.63}{(\frac{1}{2}-\epsilon)}$, then we get the following

$$p^{\frac{1}{2}-\epsilon} > p^{\frac{\log 2.63}{\log\log p}} > 2^{\omega(p-1)}, \quad (2.4)$$

by Lemma 2.3.6 (1).

Since $\omega\left(\frac{p-1}{q}\right) \leq \omega(p-1)$ holds, by (2.3) and (2.4) we conclude

$$\left|Q_p - \frac{q}{2}\phi\left(\frac{p-1}{q}\right)\right| \leq \frac{1}{2}\sqrt{p}\log p \cdot p^{\frac{1}{2}-\epsilon}. \quad (2.5)$$

This proves the first part of Theorem.

Now when $q = 1$, we have to show that $Q_p \geq 1$, for all prime $p > \exp(7.19)$.

By (2.5), it is enough to show that

$$\frac{1}{2}\phi(p-1) - \frac{1}{2}\sqrt{p}p^{\frac{1}{2}-\epsilon}\log p > 0 \Leftrightarrow \phi(p-1) > p^{1-\epsilon}\log p.$$

Again by Lemma 2.3.6(4), the above inequality holds if

$$\frac{p-1}{\log(p-1)} > p^{1-\epsilon}\log p \quad (2.6)$$

is true.

If we choose $\epsilon = 1/100$, then $\exp\exp\frac{\log 2.63}{(\frac{1}{2}-\epsilon)} < \exp(7.19)$.

For all prime $p > \exp(7.19)$ with $\epsilon = \frac{1}{100}$, the inequality (2.6) is also true which completes the proof of the theorem.

2.4 Proof of Theorem 2.2.1

Let $q \geq 1$ be a given integer and let $\epsilon \in [\frac{1}{11}, \frac{1}{2})$ be also given. Now, we consider all primes $p \equiv 1 \pmod{q}$ with $\frac{\phi(p-1)}{p-1} \leq \frac{1}{2} - \epsilon$. By Dirichlet's theorem on primes in arithmetic progressions, we can see that there are infinitely many such primes.

By Lemma 2.3.4, for any integer m with $\gcd(m, p) = 1$, we let,

$$f(m) := \frac{1}{p-1}\sum_{\ell=0}^{p-2}\beta_\ell(p-1)\chi_\ell(m) = \begin{cases} 1; & \text{if } m \text{ is a QNRNP,} \\ 0; & \text{for otherwise.} \end{cases}$$

By letting $N_p := \sum_{\substack{m=1 \\ (m,\frac{p-1}{q})=1}}^{p-1} f(m)$, we see that N_p counts the number of QNRNP's in $\{1, \ldots, p-1\}$ which are relatively prime with $\frac{p-1}{q}$.

To finish the proof of Theorem 1, it suffices to prove that $N_p \geq 1$ for all primes $p > \exp\exp\frac{\log 6.83}{\frac{1}{2}-\epsilon}$ satisfying $p \equiv 1 \pmod{q}$ and $\frac{\phi(p-1)}{p-1} \leq \frac{1}{2} - \epsilon$.

Therefore, we consider

$$\begin{aligned} N_p &= \sum_{\substack{m=1 \\ (m,\frac{p-1}{q})=1}}^{p-1} f(m) \\ &= \frac{1}{p-1}\sum_{\substack{m=1 \\ (m,\frac{p-1}{q})=1}}^{p-1}\sum_{\ell=0}^{p-2}\beta_\ell(p-1)\chi_\ell(m) \end{aligned}$$

$$= \frac{1}{p-1}\sum_{\ell=0}^{p-2}\beta_\ell(p-1)\sum_{\substack{m=1\\(m,\frac{p-1}{q})=1}}^{p-1}\chi_\ell(m)$$

$$= \frac{1}{p-1}\left(\beta_0(p-1)q\phi\left(\frac{p-1}{q}\right)+\sum_{\ell=1}^{p-2}\beta_\ell(p-1)\sum_{\substack{m=1\\(m,\frac{p-1}{q})=1}}^{p-1}\chi_\ell(m)\right),$$

where we have used the fact that the number of integers m in $\{1,\ldots,p-1\}$ such that $\left(m,\frac{p-1}{q}\right)=1$ is $q\phi\left(\frac{p-1}{q}\right)$.

Let us define

$$\begin{aligned}E_p &:= N_p-\frac{1}{p-1}\beta_0(p-1)q\phi\left(\frac{p-1}{q}\right)\\ &= N_p-\phi\left(\frac{p-1}{q}\right)\left(\frac{q}{2}-\frac{q}{p-1}\phi(p-1)\right), \text{ since } \beta_0(p-1)=\frac{p-1}{2}-\phi(p-1)\\ &= \frac{1}{p-1}\sum_{\ell=1}^{p-2}\beta_\ell(p-1)\sum_{\substack{m=1\\(m,\frac{p-1}{q})=1}}^{p-1}\chi_\ell(m). \qquad (2.7)\end{aligned}$$

In order to prove $N_p\geq 1$, we need to get an upper bound for E_p. For that, we need to estimate $\sum_{\substack{m=1\\(m,\frac{p-1}{q})=1}}^{p-1}\chi_\ell(m)$ and $\frac{1}{p-1}\sum_{\ell=1}^{p-2}\beta_\ell(p-1)$ separately.

First we consider the sum $\sum_{\substack{m=1\\(m,\frac{p-1}{q})=1}}^{p-1}\chi_\ell(m)$ as follows. For a given integer ℓ with $1\leq\ell\leq p-2$, we have

$$\begin{aligned}\sum_{\substack{m=1\\(m,\frac{p-1}{q})=1}}^{p-1}\chi_\ell(m) &= \sum_{m=1}^{p-1}\chi_\ell(m)\sum_{d\mid\left(m,\frac{p-1}{q}\right)}\mu(d)\\ &= \sum_{d\mid\frac{p-1}{q}}\mu(d)\sum_{t=1}^{\frac{p-1}{d}}\chi_\ell(d)\chi_\ell(t)\end{aligned}$$

$$= \sum_{d|\frac{p-1}{q}} \mu(d)\chi_\ell(d) \sum_{t=1}^{\frac{p-1}{d}} \chi_\ell(t),$$

by Lemma 2.3.6 (2). Hence, by Theorem 2.3.9 and Lemma 2.3.6 (3), we get

$$\left| \sum_{\substack{m=1 \\ (m,\frac{p-1}{q})=1}}^{p-1} \chi_\ell(m) \right| \leq \sum_{d|\frac{p-1}{q}} |\mu(d)| \left| \sum_{t=1}^{\frac{p-1}{d}} \chi_\ell(t) \right| \leq 2^{\omega\left(\frac{p-1}{q}\right)} \sqrt{p} \log p.$$

Also, by Lemma 2.3.3 and Lemma 2.3.8, we see that

$$\left| \sum_{\ell=1}^{p-2} \beta_\ell(p-1) \right| \leq \sum_{\ell=1}^{p-2} |\beta_\ell(p-1)| \leq \sum_{\ell=0}^{p-2} |\alpha_\ell(p-1)| = 2^{\omega(p-1)}\phi(p-1).$$

Thus, using the above two estimates in (2.7), we get,

$$\begin{aligned} |E_p| &= \left| N_p - \frac{1}{p-1}\beta_0(p-1)q\phi\left(\frac{p-1}{q}\right) \right| \\ &\leq \frac{1}{p-1} \sum_{\ell=1}^{p-2} |\beta_\ell(p-1)| \cdot \left| \sum_{\substack{m=1 \\ (m,\frac{p-1}{q})=1}}^{p-1} \chi_\ell(m) \right| \\ &\leq 2^{\omega\left(\frac{p-1}{q}\right)+\omega(p-1)} \frac{\phi(p-1)}{p-1} \sqrt{p} \log p. \end{aligned} \tag{2.8}$$

Observe that (2.8) implies

$$-2^{\omega\left(\frac{p-1}{q}\right)+\omega(p-1)} \frac{\phi(p-1)}{p-1} \sqrt{p} \log p \leq N_p - \frac{q\phi\left(\frac{p-1}{q}\right)}{(p-1)} \beta_0(p-1),$$

which is equivalent to

$$N_p \geq \frac{\phi\left(\frac{p-1}{q}\right)}{\frac{p-1}{q}} \beta_0(p-1) - 2^{\omega\left(\frac{p-1}{q}\right)+\omega(p-1)} \frac{\phi(p-1)}{p-1} \sqrt{p} \log p.$$

Thus to establish $N_p > 0$, it is enough to show that,

$$\frac{\phi\left(\frac{p-1}{q}\right)}{\frac{p-1}{q}}\beta_0(p-1) - 2^{\omega\left(\frac{p-1}{q}\right)+\omega(p-1)}\frac{\phi(p-1)}{p-1}\sqrt{p}\log p > 0,$$

which is equivalent of showing that

$$\beta_0(p-1) > 2^{\omega\left(\frac{p-1}{q}\right)+\omega(p-1)}\frac{\phi(p-1)}{q\phi\left(\frac{p-1}{q}\right)}\sqrt{p}\log p. \tag{2.9}$$

Now, it is clear that

$$\phi(p-1) \leq q\phi\left(\frac{p-1}{q}\right) \iff \frac{\phi(p-1)}{q\phi\left(\frac{p-1}{q}\right)} \leq 1. \tag{2.10}$$

Since $\omega\left(\frac{p-1}{q}\right) \leq \omega(p-1)$, by (2.9) and (2.10), it is enough to prove that

$$\beta_0(p-1) > 4^{\omega(p-1)}\sqrt{p}\log p, \tag{2.11}$$

for primes $p > \exp\exp\frac{\log 6{\cdot}83}{\frac{1}{2}-\epsilon}$ satisfying $\frac{\phi(p-1)}{p-1} \leq \frac{1}{2} - \epsilon$.

Let p be a prime satisfying $p > \exp\exp\frac{\log 6.83}{\frac{1}{2}-\epsilon}$. Therefore, we get

$$p^{\frac{1}{2}-\epsilon} > p^{\frac{\log 6.83}{\log\log p}}. \tag{2.12}$$

By Lemma 2.3.6 (1), we also know that

$$\omega(p-1) \leq 1.385\frac{\log p}{\log\log p}.$$

Therefore, we get

$$4^{\omega(p-1)} \leq 4^{1.385\frac{\log p}{\log\log p}} \leq 6.83^{\frac{\log p}{\log\log p}} = p^{\frac{\log 6.83}{\log\log p}} < p^{\frac{1}{2}-\epsilon}. \tag{2.13}$$

Now, by (2.7), (2.8) and (2.13), we get

$$N_p = \phi\left(\frac{p-1}{q}\right)\left(\frac{q}{2} - \frac{q}{p-1}\phi(p-1)\right) + O\left(p^{1-\epsilon}\frac{\phi(p-1)}{p-1}\log p\right)$$

and this proves the first part of Theorem.

Hence, from (2.12), we have,

$$p^{\frac{1}{2}-\epsilon} > 4^{\omega(p-1)} \iff p^{1-\epsilon}(\log p) > 4^{\omega(p-1)}\sqrt{p}\log p.$$

In order to prove (2.11), it is enough to show that

$$\beta_0(p-1) > p^{1-\epsilon}\log p \tag{2.14}$$

for all primes $p > \exp\exp\frac{\log 6.83}{\frac{1}{2}-\epsilon}$ satisfying $\frac{\phi(p-1)}{p-1} \leq \frac{1}{2} - \epsilon$.

Note that the condition

$$\frac{\phi(p-1)}{p-1} \leq \frac{1}{2} - \epsilon \iff \epsilon(p-1) \leq \frac{p-1}{2} - \phi(p-1) = \beta_0(p-1).$$

Therefore, to prove (2.14), it is enough to prove that $\epsilon(p-1) \geq p^{1-\epsilon}\log p$, for all primes $p > \exp\exp\dfrac{\log 6.83}{\frac{1}{2}-\epsilon}$.

Since $\epsilon \in [\frac{1}{11}, \frac{1}{2})$, we write $\epsilon = \frac{1}{c}$ for some real number c with $2 < c \leq 11$ and note that

$$\log\log p > \frac{\log 6.83}{\frac{1}{2}-\epsilon} > 3.84 \times 1.22 > 4.68 \qquad \text{and} \qquad \log p > e^{4.68} > 107.7.$$

In order to prove $\epsilon(p-1) \geq p^{1-\epsilon}\log p$ for all primes $p > \exp\exp\dfrac{\log 6.83}{\frac{1}{2}-\epsilon}$, it

is enough to prove that

$$\frac{p}{1.1} > \frac{1}{\epsilon}p^{1-\epsilon}\log p \iff p > (1.1c)^c(\log p)^c \iff \log p > c\log(1.1c) + c\log\log p.$$

Since we know $e^x/x \geq 22$ for all $x \geq 4.68$, we apply for $x = \log\log p$ and see that

$\log p > 2c\log\log p$ for all $2 < c \leq 11$.

Hence, it is enough to prove that

$$\log p > c\log(1.1) + c\log c + \frac{\log p}{2} \iff \log p > 2c\log(1.1) + 2c\log c.$$

Since $c \leq 11$, we see that

$$2c\log(1.1) + 2c\log c \leq 22\log(1.1) + 22\log 11 \leq 54.86 < 107.7 < \log p.$$

Thus the inequality in (2.14) holds true, which completes the proof of the theorem. □

2.5 Proof of Corollary 2.2.2

By Theorem 2.2.1, there is a QNRNP x modulo p satisfying $x \in [1, p-1]$ and $\gcd(x, p-1) = 1$. Let y be the multiplicative inverse of x modulo $p-1$. Put $g = x^y$. Then note that g is also a QNRNP modulo p. Hence, we get $g^x \equiv x^{xy} \equiv x \pmod{p}$. □

CHAPTER 3

On sums of polynomial-type exceptional units in $\mathbb{Z}/n\mathbb{Z}$

A unit u in a commutative ring R with unity is called exceptional if $u-1$ is also a unit. We introduce a notion of polynomial version of exceptional unit (abbreviated as f-exunits) for any $f(X) \in \mathbb{Z}[X]$. In this chapter, we find the number of representations of a non-zero element of $\mathbb{Z}/n\mathbb{Z}$ as a sum of two f-exunits, for an infinite family of polynomials f of each degree ≥ 1. We also derive the exact formulae for certain infinite families of linear and quadratic polynomials. This generalizes a result of Sander in [83].

3.1 Introduction

In this chapter, we start with the following definition of *exceptional unit*.

Definition 3.1.1 (Exceptional unit) An element u in a commutative ring R with unity is said to be an *exceptional unit* if both u and $u-1$ are units in R.

For the rest of this chapter, following [83], we shall abbreviate exceptional units as *exunits*.

Nagell [67] introduced exunits in connection with certain Diophantine equations. From then onwards, it gained rapid popularity among number theorists and found many applications in various seemingly diverse areas of number theory. For instance, Lenstra [53] showed that the existence of a certain number of exunits in a sequence in the ring of integers $\mathcal{O}_K$ of an algebraic number field K, implies that $\mathcal{O}_K$ is an Euclidean domain with respect to the norm map. He used this criterion to prove that some number fields are norm-Euclidean that were previously unknown. Later, J. Houriet [42] obtained 42 new Euclidean number fields by a computational method which also depends on exunits.

J. H. Silverman (in [87] and [88]) connected exceptional unit with Lehmer's conjecture of small Mahler measure. Other than applications of exunits in number fields, many mathematicians are interested about quantitative nature of exunits. For instance, G. Nilkash discussed this topic in [70] and [71]. In particular, he determined all exunits in quartic number field in [71].

In number theory, one of the most important rings to work with is $\mathbb{Z}/n\mathbb{Z}$ and it is interesting to study the exunits in this ring. We use the notation $\mathcal{E}_n$ to denote the set of exunits in $\mathbb{Z}/n\mathbb{Z}$. Note that, for an integer $a \geq 1$, $a \pmod n \in \mathcal{E}_n$ if and only if $\gcd(a, n) = \gcd(a-1, n) = 1$. Equivalently, $a \pmod n \in \mathcal{E}_n$ if and only if $\gcd(a(a-1), n) = 1$. This point of view motivated us to investigate the co-primality condition of the values of any polynomial $f(X) \in \mathbb{Z}[X]$ instead of $X(X-1)$ in particular. Thus we introduce "f-exunits" as follows.

Definition 3.1.2 Let $n \geq 2$ be an integer and let $f(X) \in \mathbb{Z}[X]$. An integer a with $1 \leq a \leq n$ is said to be an *f-exunit* if $\gcd(f(a), n) = 1$. We denote the set of all f-exunits in $\mathbb{Z}/n\mathbb{Z}$ by $\mathcal{E}_{f,n}$.

Remark 3.1.3 Note that, if f is a constant polynomial, then $|\mathcal{E}_{f,n}| = 0$ or n. Therefore, for the rest of the discussion, we shall assume that f is a non-constant polynomial. Also, in particular, if we take $f(X) = X^2 - X$, then clearly $\mathcal{E}_{f,n} = \mathcal{E}_n$. Thus f-exunit is indeed a generalization of exunit in $\mathbb{Z}/n\mathbb{Z}$.

We observe that the existence of an exunit in $\mathbb{Z}/n\mathbb{Z}$ is equivalent to the existence of a solution of the equation $x + y = 1$ with $x, y \in (\mathbb{Z}/n\mathbb{Z})^*$. For any integer c with $1 \leq c \leq n-1$, it is therefore natural to study the more general equation $x + y = c$ in $(\mathbb{Z}/n\mathbb{Z})^*$.

Sander addressed this question in [83] and determined the number of solutions of the equation $x + y = c$ with $x, y \in \mathcal{E}_n$. In 2019, D. Dolžan (in [15]) generalized this representation problem over finite ring. C. Miguel (in [63] and [64]) also generalized some of the properties of exunits over finite commutative rings.

In this chapter, we consider the analogous representation problem for f-exunits, for certain infinite families of polynomials f over $\mathbb{Z}$. More precisely, our main theorem is as follows.

3.2 Main results

Theorem 3.2.1 *[3] Let $r \geq 1$ be an integer and let $a_1, \ldots, a_r, b_1, \ldots, b_{r-1}$ and b_r be positive integers such that $\gcd(a_j t + b_j, a_k t + b_k) = 1$ for all $1 \leq j \neq k \leq r$ and for all integer t. Let $n \geq 2$ be an integer such that $\gcd\left(n, \prod_{i=1}^{r} a_i b_i\right) = 1$ and consider $f(X) = \prod_{i=1}^{r}(a_i X + b_i)$. For an integer c with $1 \leq c \leq n-1$, let*

$$\mathcal{E}_{f,n}(c) := \{(x, y) \in \mathcal{E}_{f,n} \times \mathcal{E}_{f,n} : x + y \equiv c \pmod{n}\}.$$

Then

$$|\mathcal{E}_{f,n}(c)| = n \prod_{p|n} \left(1 - \frac{N^f(p,c)}{p}\right), \tag{3.1}$$

where $N^f(p,c) = \#\{\ell \pmod p \mid$ *either* $f(\ell) \equiv 0 \pmod p$ *or* $f(c-\ell) \equiv 0 \pmod p\}$.

Remark 3.2.2 In Proposition 3.3.3, we shall establish the existence of a polynomial f of any given degree that satisfies the aforementioned co-primality condition. Also, note that if $f(X) = \prod_{i=1}^{r}(a_iX + b_i)$ satisfies the hypotheses of Theorem 3.2.1, then so does the polynomial $g(X) = \prod_{i=1}^{r}(a_imX + b_i)$ for any integer m for which $\gcd(n,m) = 1$. In other words, we have an infinite family of polynomials satisfying the hypotheses of Theorem 3.2.1.

Remark 3.2.3 We shall observe in Proposition 3.7.1, that the expression (3.1) holds for any non-constant polynomial $f(X) \in \mathbb{Z}[X]$ and for any $n = p$, where p is a prime number. In other words, $|\mathcal{E}_{f,p}(c)| = p\left(1 - \frac{N^f(p,c)}{p}\right)$ holds for any c with $1 \le c \le p-1$. Therefore, it is reasonable to expect that (3.1) holds for any non-constant polynomial over $\mathbb{Z}$ and for any integer $n \ge 2$, but the techniques used in the proof of our main result can be applied only for the particular type of polynomials considered in Theorem 3.2.1.

For linear and quadratic polynomials, we get the following results as corollaries of Theorem 3.2.1.

Corollary 3.2.4 *[3] Let $n \ge 2$ be an integer and let $f(X) = aX + b \in \mathbb{Z}[X]$ be a linear polynomial such that $\gcd(ab,n) = 1$. Then for any integer $c \ge 1$ with $1 \le c \le n-1$, we have $|\mathcal{E}_{f,n}(c)| = n \prod_{p|n} \left(1 - \frac{N^f(p,c)}{p}\right)$, where*

$$N^f(p,c) = \begin{cases} 1 & ;\ \text{if } ac \equiv -2b \pmod p \\ 2 & ;\ \text{if } ac \not\equiv -2b \pmod p. \end{cases}$$

Corollary 3.2.5 *[3] Let $f(X) = (aX+1)(bX+1) \in \mathbb{Z}[X]$ be a quadratic polynomial such that $\gcd(at+1, bt+1) = 1$ for all integer t. Let $n \geq 2$ be an integer with $\gcd(2ab, n) = 1$. Then for any integer c with $1 \leq c \leq n-1$, we have $|\mathcal{E}_{f,n}(c)| = n \prod_{p|n} \left(1 - \frac{N^f(p,c)}{p}\right)$, where*

$$N^f(p,c) = \begin{cases} 2 & ; \text{ if } a+b \equiv -abc \pmod{p} \\ 3 & ; \text{ if } ac \equiv -2 \pmod{p} \text{ or } bc \equiv -2 \pmod{p} \\ 4 & ; \text{ otherwise .} \end{cases}$$

3.3 Preliminaries

In this section, we give the necessary account of the results which will be used in the course of the proofs of our results. We first give a formula for the cardinality of $\mathcal{E}_{f,n}$ in the following lemma which was mentioned as an exercise in [72] (Exercise 47 after section 2.3).

Lemma 3.3.1 *Let $f(X) \in \mathbb{Z}[X]$ and $n \geq 2$ be an integer. Then*

$$|\mathcal{E}_{f,n}| = n \prod_{p|n} \left(1 - \frac{N^f(p)}{p}\right),$$

where $N^f(p)$ stands for the number of solutions of the congruence $f(X) \equiv 0 \pmod{p}$.

Proof. Let a be an integer with $1 \leq a \leq n$. Then the probability that $a \in \mathcal{E}_{f,n}$ is $\frac{|\mathcal{E}_{f,n}|}{n}$. On the other hand, $\gcd(f(a), n) = 1$ if and only if $\gcd(f(a), p) = 1$ for all prime divisor p of n. That is $a \in \mathcal{E}_{f,n}$ if and only if $a \in \mathcal{E}_{f,p}$ for all prime $p \mid n$. Equivalently, $a \in \mathcal{E}_{f,n}$ if and only if $f(a) \not\equiv 0 \pmod{p}$ for all prime $p \mid n$. Since

for a given prime $p \mid n$, the probability that $a \in \mathcal{E}_{f,p}$ is $\left(1 - \frac{N^f(p)}{p}\right)$, we have

$$\frac{|\mathcal{E}_{f,n}|}{n} = \prod_{p|n} \left(1 - \frac{N^f(p)}{p}\right).$$

This completes the proof of Lemma 3.3.1. □

The next important lemma is about the mutually co-prime values of two linear polynomials over $\mathbb{Z}$ and it will play a crucial role in the proof of Corollary 3.2.5. The proof can be found in [50] but we present it here for the sake of completeness.

Lemma 3.3.2 *[50] Let a and c be integers with $a < c$ and let $f(X) = aX + 1$ and $g(X) = cX + 1$ be polynomials. Let $a = q_1^{m_1} \dots q_s^{m_s}$ and $c - a = p_1^{n_1} \dots p_t^{n_t}$ be the respective prime factorizations. Then the condition $\gcd(f(k), g(k)) = 1$ holds true for all integers k if and only if $\{p_1, \dots, p_t\} \subseteq \{q_1, \dots, q_s\}$.*

Proof. Let $A = \{q_1, \dots, q_s\}$ and $B = \{p_1, \dots, p_t\}$. Assume that $f(k)$ and $g(k)$ are relatively prime for all integers k. If $B \not\subseteq A$, there exists $p_i \in B \setminus A$ for some $i \in \{1, \dots, t\}$. Since $p_i \notin A$, we have $p_i \nmid a$ and hence the congruence $aX + 1 \equiv 0 \pmod{p_i}$ has a solution t_0 in $\mathbb{Z}$. In other words, $p_i \mid f(t_0)$. Also, $p_i \in B$ implies that $p_i \mid (c - a)$. Thus we obtain

$$p_i \mid \{(at_0 + 1) + (c - a)t_0\} = ct_0 + 1 = g(t_0).$$

This implies $p_i \mid \gcd(f(t_0), g(t_0))$, which contradicts our hypothesis that $\gcd(f(k), g(k)) = 1$ for all $k \in \mathbb{Z}$. Hence $B \subseteq A$.

Conversely, suppose that $B \subseteq A$. In order to prove $\gcd(f(\ell), g(\ell)) = 1$ for an integer ℓ, it is enough to prove that for a prime number p, if $p \mid f(\ell)$, then $p \nmid g(\ell)$. For that, we choose a prime number p such that $p \mid f(\ell) = (a\ell + 1)$. Then $p \nmid a$ and $p \nmid \ell$. Since $p \nmid a$, we have $p \notin A$. By our assumption, $B \subseteq A$

and hence $p \notin B$. Then $p \nmid (c-a)$ and so $p \nmid (c-a)\ell$. Now,

$$g(\ell) = c\ell + 1 = (a\ell + 1) + (c-a)\ell.$$

Since $p \mid (a\ell + 1)$ and $p \nmid (c-a)\ell$, we conclude that $p \nmid g(\ell)$. This completes the proof of the lemma. □

In order to prove Theorem 3.2.1, we need to exploit the fact that the linear factors of $f(X)$ are pairwise relatively prime, when evaluated at any integer. A priori, we may not always find such a polynomial. But the following proposition guarantees the existence of a polynomial fulfilling the required criterion. More precisely, we prove the following.

Proposition 3.3.3 *[3] Let $r \geq 2$ be an integer. Then there exist a polynomial $f(X) = \prod_{i=1}^{r}(a_iX + b_i)$ for some integers a_i and b_i for $i = 1, \ldots, r-1$ and r such that $\gcd(b_i, b_j) = 1 = \gcd(a_ik + b_i, a_jk + b_j)$ for all integers k, whenever $i \neq j$.*

Proof. We shall use induction on r. Note that, for $r = 2$, the polynomial $(5X + 3)(8X + 5)$ is a required choice for f. For, if an integer d divides both $5k+3$ and $8k+5$ for some integer k, then $d \mid \{5(8k+5) - 8(5k+3)\} = 1$, which implies $d = 1$.

Now, suppose that there exists a polynomial $g(X) = \prod_{i=1}^{r-1}(a_iX + b_i)$ of degree $r-1$ such that $a_ik + b_i$ and $a_jk + b_j$ are relatively prime whenever $i \neq j$. We shall construct a polynomial $f(X)$ of degree r using $g(X)$. We first choose two positive integers a and b such that $\gcd(b_i, b) = 1$ for all $i \in \{1, \ldots, r-1\}$ and let $m = \prod_{i=1}^{r-1}(a_ib - ab_i)$. Now, let

$$f(X) = (a_1mX + b_1)\ldots(a_{r-1}mX + b_{r-1})(amX + b).$$

Claim. $\gcd(a_jmk + b_j, amk + b) = 1$ for all $j \in \{1, \ldots, r-1\}$ and for all $k \in \mathbb{Z}$.

If possible, suppose $\gcd(a_jmt+b_j, amt+b) > 1$ for some integer t and some $j \in \{1, \ldots, r-1\}$. Let p be a prime divisor of $\gcd(a_jmt + b_j, amt + b)$. Then $p \mid \{a_j(amt + b) - a(a_jmt + b_j)\} = a_jb - ab_j$. From the construction of m, we have $(a_jb - ab_j) \mid m$. Thus we get $p \mid m$.

Therefore, we have $p \mid m, p \mid (a_jmt+b_j)$ and $p \mid (amt+b)$. Thus $p \mid b$ and $p \mid b_j$, which contradicts our assumption that $\gcd(b_j, b) = 1$ for all $j \in \{1, \ldots, r-1\}$. Hence $\gcd(a_jmk + b_j, amk + b) = 1$ for all $j \in \{1, \ldots, r-1\}$, for all $k \in \mathbb{Z}$ and the claim follows.

Now, by our induction hypothesis, we have $\gcd(a_ik + b_i, a_jk + b_j) = 1$ for all integers k and for all integers i and j with $1 \leq i \neq j \leq r-1$. Therefore, the induction hypothesis along with the above claim imply that all the linear factors of $f(X)$ are pairwise co-prime, when evaluated at any integer t. This completes the proof of Proposition 3.3.3. □

The next lemma is a generalization of the Chinese remainder theorem and will be useful in the proof of Theorem 3.2.1.

Lemma 3.3.4 *[76, 95] Let $0 \leq a_i < n_i$ be integers for all $i = 1, 2, \ldots, k-1$ and k. Suppose that $a_i \equiv a_j \pmod{\gcd(n_i, n_j)}$ for all $1 \leq i < j \leq k$. Then the system of congruences,*

$$\begin{aligned} & x \equiv a_1 \pmod{n_1} \\ & \vdots \\ & x \equiv a_{k-1} \pmod{n_{k-1}} \\ \text{and} \quad & x \equiv a_k \pmod{n_k}. \end{aligned}$$

has a unique solution $x_0 \pmod{n}$, where $n = lcm(n_1, \ldots, n_k)$.

The following lemma, proved in [83], is useful to compute the cardinality of

$\{(x, y) \in \mathcal{E}_{f,n} \times \mathcal{E}_{f,n} : x + y \equiv c \pmod{n}\}$.

Lemma 3.3.5 *[83] Let $c_1, \ldots, c_{k-1}$ and c_k be fixed integers. Then the following statements are true.*

(1) The arithmetic function g defined by

$$g(n) = g_{c_1,\ldots,c_k}(n) := \sum_{\substack{a=1 \\ \gcd(a-c_i,n)=1 \\ i=1,\ldots,k}}^{n} 1$$

is a multiplicative function.

(2) For any prime number p and an integer $m \geq 1$,

$$g_{c_1,\ldots,c_k}(p^m) = p^{m-1}(p - v_p(c_1, \ldots, c_k)),$$

where $v_p(c_1, \ldots, c_k) = \#\{\ell \pmod{p} \mid \ell \equiv c_i \pmod{p}$ for some $i \in [1, k]\}$.

Proof. (1) Let m and n be two positive integers such that $\gcd(m, n) = 1$. We have to prove that $g(mn) = g(m)g(n)$.

Now, we observe

$$g(mn) = \sum_{\substack{a=1 \\ \gcd(a-c_i,mn)=1 \\ i=1,\ldots,k}}^{mn} 1 = \sum_{s=0}^{n-1} \sum_{\substack{r=1 \\ \gcd(sm+r-c_i,mn)=1 \\ i=1,\ldots,k}}^{m} 1. \tag{3.2}$$

Note that $\gcd(t, mn) = 1$ if and only if $\gcd(t, m) = 1 = \gcd(t, n)$ holds. Using this fact in (3.2), we get

$$g(mn) = \sum_{\substack{r=1 \\ \gcd(r-c_i,m)=1 \\ i=1,\ldots k}}^{m} \sum_{\substack{s=0 \\ \gcd(sm+r-c_i,n)=1 \\ i=1,\ldots,k}}^{n-1} 1. \tag{3.3}$$

For a fixed $r \in [1, m]$, we observe

$$\sum_{\substack{s=0 \\ \gcd(sm+r-c_i,n)=1 \\ i=1,\ldots,k}}^{n-1} 1 = \sum_{\substack{\ell=1 \\ \gcd(\ell-c_i,n)=1 \\ i=1,\ldots,k}}^{n} 1 = g(n). \tag{3.4}$$

After putting (3.4) in (3.3), we get

$$g(mn) = \sum_{\substack{r=1 \\ \gcd(r-c_i,m)=1 \\ i=1,\ldots k}}^{m} g(n) = g(n) \sum_{\substack{r=1 \\ \gcd(r-c_i,m)=1 \\ i=1,\ldots k}}^{m} 1 = g(n)g(m)$$

and this proves the first part of Lemma.

(2) For any prime number p and an integer $m \geq 1$,

$$\begin{aligned} g_{c_1,\ldots,c_k}(p^m) &= \sum_{\substack{\ell=1 \\ \gcd(\ell-c_i,p^m)=1 \\ i=1,\ldots k}}^{p^m} 1 = \sum_{\substack{\ell=1 \\ p\nmid(\ell-c_i) \\ i=1,\ldots k}}^{p^m} 1 \\ &= \sum_{s=0}^{p^{m-1}-1} \sum_{\substack{r=1 \\ p\nmid(sp+r-c_i) \\ i=1,\ldots,k}}^{p} 1 \\ &= \sum_{s=0}^{p^{m-1}-1} \sum_{\substack{r=1 \\ p\nmid(r-c_i) \\ i=1,\ldots,k}}^{p} 1 \\ &= p^{m-1}(p - v_p(c_1,\ldots,c_k)), \end{aligned}$$

where $v_p(c_1,\ldots,c_k) = \#\{\ell \pmod p \mid \ell \equiv c_i \pmod p \text{ for some } i \in [1,k]\}$. □

3.4 Proof of Theorem 3.2.1

By considering the definition of $\mathcal{E}_{f,n}$, we have

$$
\begin{aligned}
|\mathcal{E}_{f,n}(c)| &= \sum_{\substack{x=1\\ \gcd(f(x),n)=1}}^{n} \sum_{\substack{y=1\\ \gcd(f(y),n)=1\\ y+x\equiv c \pmod n}}^{n} 1 = \sum_{\substack{x=1\\ \gcd(f(x),n)=1}}^{n} \sum_{\substack{y=1\\ \gcd(f(y),n)=1\\ y\equiv c-x \pmod n}}^{n} 1 \\
&= \sum_{\substack{x=1\\ \gcd(f(x),n)=1}}^{n} \sum_{\substack{y=1\\ y\equiv c-x \pmod n}}^{n} \left(\sum_{d \mid \gcd(f(y),n)} \mu(d) \right), \text{ by Lemma 2.3.6(2)} \\
&= \sum_{\substack{x=1\\ \gcd(f(x),n)=1}}^{n} \sum_{\substack{y=1\\ y\equiv c-x \pmod n}}^{n} \left(\sum_{d_1 \mid \gcd(a_1y+b_1,n)} \mu(d_1) \right) \dots \left(\sum_{d_r \mid \gcd(a_ry+b_r,n)} \mu(d_r) \right) \\
&= \sum_{\substack{x=1\\ \gcd(f(x),n)=1}}^{n} \sum_{d_1 \mid n} \mu(d_1) \dots \sum_{d_r \mid n} \mu(d_r) \sum_{\substack{y=1\\ y\equiv c-x \pmod n\\ a_1y+b_1\equiv 0 \pmod{d_1}\\ \vdots\\ a_ry+b_r\equiv 0 \pmod{d_r}}}^{n} 1.
\end{aligned}
$$

Since $\gcd(n, a_1 \dots a_r) = 1$, we have $\gcd(d_i, a_i) = 1$ for all $i \in \{1, \dots, r\}$. In other words, $\overline{a_i}$ has a multiplicative inverse in $\mathbb{Z}/d_i\mathbb{Z}$, where $\overline{a_i}$ denotes the residue of a_i in $\mathbb{Z}/d_i\mathbb{Z}$. We rewrite the following set of equations in a different manner as follows.

$$
\begin{aligned}
y &\equiv c - x \pmod n \\
a_1y + b_1 &\equiv 0 \pmod{d_1} \Leftrightarrow y \equiv -a_1'b_1 \pmod{d_1}, \text{ where } a_1a_1' \equiv 1 \pmod{d_1} \\
&\vdots \\
a_ry + b_r &\equiv 0 \pmod{d_r} \Leftrightarrow y \equiv -a_r'b_r \pmod{d_r}, \text{ where } a_ra_r' \equiv 1 \pmod{d_r}.
\end{aligned}
$$

By our hypotheses, $a_ik + b_i$ and $a_jk + b_j$ are co-prime for all integers k and for all integers i and j with $1 \le i \ne j \le r$. Therefore, d_i and d_j are co-prime whenever $i \ne j$ and thus all the hypotheses of Lemma 3.3.4 are satisfied. Hence

the above mentioned set of congruences admit a unique solution for y if and only if

$$\begin{aligned} c-x &\equiv -a_1'b_1 \pmod{d_1} \\ &\vdots \\ c-x &\equiv -a_r'b_r \pmod{d_r} \end{aligned}$$

hold. Using these three congruences, we rewrite the previous expression of $|\mathcal{E}_{f,n}(c)|$ in the following way,

$$|\mathcal{E}_{f,n}(c)| = \sum_{\substack{x=1 \\ \gcd(f(x),n)=1}}^{n} \left(\sum_{\substack{d_1 \mid n \\ d_1 \mid (c-x+a_1'b_1)}} \mu(d_1) \right) \cdots \left(\sum_{\substack{d_r \mid n \\ d_r \mid (c-x+a_r'b_r)}} \mu(d_r) \right).$$

Using the fact $\gcd(d_i, a_i) = 1$ for all $i \in \{1, \ldots, r\}$, we get

$$\begin{aligned} |\mathcal{E}_{f,n}(c)| &= \sum_{\substack{x=1 \\ \gcd(f(x),n)=1}}^{n} \left(\sum_{\substack{d_1 \mid n \\ d_1 \mid a_1(c-x+a_1'b_1)}} \mu(d_1) \right) \cdots \left(\sum_{\substack{d_r \mid n \\ d_r \mid a_r(c-x+a_r'b_r)}} \mu(d_r) \right) \\ &= \sum_{\substack{x=1 \\ \gcd(f(x),n)=1}}^{n} \left(\sum_{\substack{d_1 \mid n \\ d_1 \mid (a_1c-a_1x+b_1)}} \mu(d_1) \right) \cdots \left(\sum_{\substack{d_r \mid n \\ d_r \mid (a_rc-a_rx+b_r)}} \mu(d_r) \right) \\ &= \sum_{\substack{x=1 \\ \gcd(f(x),n)=1 \\ \gcd(a_1c-a_1x+b_1,n)=\cdots=\gcd(a_rc-a_rx+b_r,n)=1}}^{n} 1 \\ &= g_{-\frac{b_1}{a_1},\ldots,-\frac{b_r}{a_r},c+\frac{b_1}{a_1},\ldots,c+\frac{b_r}{a_r}}(n), \end{aligned}$$

where $\dfrac{1}{a_i}$ stands for the multiplicative inverse of a_i in $(\mathbb{Z}/n\mathbb{Z})^*$ for all $i = 1, \ldots, r$

$$= \prod_{p|n} g_{-\frac{b_1}{a_1},\ldots,-\frac{b_r}{a_r},c+\frac{b_1}{a_1},\ldots,c+\frac{b_r}{a_r}}(p^{e_p(n)}), \qquad \text{(since } g \text{ is multiplicative, by Lemma 3.3.5)}$$

where $e_p(n)$ is the highest power of p appearing in the prime factorizarion of n

$$= n\prod_{p|n}\left(1-\frac{v_p(-\frac{b_1}{a_1},\ldots,-\frac{b_r}{a_r},c+\frac{b_1}{a_1},\ldots,c+\frac{b_r}{a_r})}{p}\right)$$

$$= n\prod_{p|n}\left(1-\frac{N^f(p,c)}{p}\right), \qquad \text{where}$$

$$N^f(p,c) = \sum_{\substack{\ell=1 \\ p|(\ell+\frac{b_1}{a_1})\ldots(\ell+\frac{b_r}{a_r}) \text{ or} \\ p|(c+\frac{b_1}{a_1}-\ell)\ldots(c+\frac{b_r}{a_r}-\ell)}}^{p} 1 = \sum_{\substack{\ell=1 \\ p|(a_1\ell+b_1)\ldots(a_r\ell+b_r) \text{ or} \\ p|(a_1(c-\ell)+b_1)\ldots(a_r(c-\ell)+b_r)}}^{p} 1$$

$$= \#\left\{\ell \pmod p \mid \text{ either } f(\ell)\equiv 0 \pmod p \text{ or } f(c-\ell)\equiv 0 \pmod p\right\}.$$

This completes the proof of Theorem 3.2.1. □

3.5 Proof of Corollary 3.2.4

In the light of Theorem 3.2.1, we only need to prove that

$$N^f(p,c) = \begin{cases} 1 & ; \text{if } ac \equiv -2b \pmod p \\ 2 & ; \text{if } ac \not\equiv -2b \pmod p. \end{cases}$$

for all prime number $p \mid n$.

Since $\gcd(ab,n)=1$, for every prime divisor p of n, we have $\gcd(ab,p)=1$. Let p be any prime divisor of n. Since $aX+b\equiv 0 \pmod p$ has a unique solution modulo p, in order to compute $N^f(p,c)$, we need to know whether a common solution to the equations $aX+b\equiv 0 \pmod p$ and $aX-ac-b\equiv 0 \pmod p$ exists.

Suppose that $ac\equiv -2b \pmod p$. In this case, we prove that there exists $\ell \pmod p$ satisfying $f(\ell)\equiv 0 \pmod p$ and $f(c-\ell)\equiv 0 \pmod p$ and hence

we get $N^f(p,c) = 1$. Since $ac \equiv -2b \pmod{p}$, we get $ac + b \equiv -b \pmod{p}$ and hence $c + ba' \equiv -ba' \pmod{p}$, where $aa' \equiv 1 \pmod{p}$. Then we note that $f(-ba') \equiv a(-ba')+b \equiv 0 \pmod{p}$ and $f(c+ba') \equiv f(-ba') \equiv 0 \pmod{p}$. Thus $-ba'$ is a common solution modulo p and hence we conclude that $N^f(p,c) = 1$.

Suppose that $ac \not\equiv -2b \pmod{p}$. If there is a common solution ℓ satisfying $a\ell + b \equiv 0 \pmod{p}$ and $ac + b - a\ell \equiv 0 \pmod{p}$, then adding these two congruences, we get $ac \equiv -2b \pmod{p}$ which is a contradiction. Hence in this case, $N^f(p,c) = 2$. □

3.6 Proof of Corollary 3.2.5

In view of Theorem 3.2.1, it suffices to prove that

$$N^f(p,c) = \begin{cases} 2 & ; \text{if } a+b \equiv -abc \pmod{p} \\ 3 & ; \text{if } ac \equiv -2 \pmod{p} \text{ or } bc \equiv -2 \pmod{p} \\ 4 & ; \text{otherwise .} \end{cases}$$

for all prime number $p \mid n$.

Let us fix a prime divisor p of n. For an integer ℓ, we have $f(\ell) = (a\ell+1)(b\ell+1)$ and $f(c-\ell) = (ac+1-a\ell)(bc+1-b\ell)$. Since, by hypothesis, $\gcd(ab,n) = 1$, we have $\gcd(ab,p) = 1$. Thus each of the linear congruences $a\ell+1 \equiv 0 \pmod{p}$, $b\ell+1 \equiv 0 \pmod{p}$, $a\ell+1-ac \equiv 0 \pmod{p}$ and $b\ell+1-bc \equiv 0 \pmod{p}$ has a unique solution $\pmod{p}$. In order to compute $N^f(p,c)$, we need to know about the common solutions of $f(X) \equiv 0 \pmod{p}$ and $f(c-X) \equiv 0 \pmod{p}$.

Claim. A common solution of $f(X) \equiv 0 \pmod{p}$ and $f(c-X) \equiv 0 \pmod{p}$ exists if and only if either $a+b \equiv -abc \pmod{p}$ or $ac \equiv -2 \pmod{p}$ or $bc \equiv -2 \pmod{p}$.

Suppose ℓ is a common solution of $f(X) \equiv 0 \pmod{p}$ and $f(c-X) \equiv 0 \pmod{p}$. Then $(a\ell+1)(b\ell+1) \equiv 0 \pmod{p}$ and $(ac+1-a\ell)(bc+1-b\ell) \equiv 0 \pmod{p}$. We note that since $\gcd(ak+1, bk+1) = 1$ for all integer k, by Lemma 3.3.2 we have, the set of prime divisors of $b-a$ is a subset of the set of prime divisors of a. In particular, $\gcd(b-a, p) = 1$. Now, if $a\ell+1 \equiv 0 \pmod{p}$ and $b\ell+1 \equiv 0 \pmod{p}$, then $p \mid (b-a)\ell$. Since $\gcd(b-a, p) = 1$, we have $p \nmid (b-a)$. Therefore, we must have $\ell \equiv 0 \pmod{p}$. This together with $a\ell+1 \equiv 0 \pmod{p}$ implies that $1 \equiv 0 \pmod{p}$, which is a contradiction. Hence $a\ell+1 \equiv 0 \pmod{p}$ and $b\ell+1 \equiv 0 \pmod{p}$ do not have a common solution $\pmod{p}$. In a similar way, we can also show that $ac+1-a\ell \equiv 0 \pmod{p}$ and $bc+1-b\ell \equiv 0 \pmod{p}$ do not have a common solution $\pmod{p}$.

Suppose that $a\ell+1 \equiv 0 \pmod{p}$ and $b(c-\ell)+1 \equiv 0 \pmod{p}$. Let a' and b' be integers such that $aa' \equiv 1 \pmod{p}$ and $bb' \equiv 1 \pmod{p}$. Then we have $\ell \equiv -a' \pmod{p}$ and hence $b(c-\ell)+1 \equiv b(c+a')+1 \equiv 0 \pmod{p}$. Therefore, $ba'+1 \equiv -bc \pmod{p}$ which implies that $a+b \equiv -abc \pmod{p}$. Similarly, if $b\ell+1 \equiv 0 \pmod{p}$ and $a(c-\ell)+1 \equiv 0 \pmod{p}$ together implies that $a+b \equiv -abc \pmod{p}$.

Now, suppose $a\ell+1 \equiv 0 \pmod{p}$ and $a(c-\ell)+1 \equiv 0 \pmod{p}$ hold simultaneously for some integer ℓ. Then from $\ell \equiv -a' \pmod{p}$, we get $a(c+a')+1 \equiv 0 \pmod{p}$ and thus $c+a' \equiv -a' \pmod{p}$. This implies $ac \equiv -2 \pmod{p}$. Similarly, the existence of a common solution of $bX+1 \equiv 0 \pmod{p}$ and $b(c-X)+1 \equiv 0 \pmod{p}$ implies that $bc \equiv -2 \pmod{p}$.

Conversely, first suppose $a+b \equiv -abc \pmod{p}$. Now, multiplying both sides of the congruence $a+b \equiv -abc \pmod{p}$ by $a'b'$, we get $c+b' \equiv -a' \pmod{p}$. We note that $-a'$ is the solution of the congruence $a\ell+1 \equiv 0 \pmod{p}$ and $c+b'$ is the solution of the congruence $bc+1-b\ell \equiv 0 \pmod{p}$. Thus in this case, $aX+1 \equiv 0 \pmod{p}$ and $b(c-X)+1 \equiv 0 \pmod{p}$ have a common solution.

Similarly, we can show that $bX+1 \equiv 0 \pmod{p}$ and $a(c-X)+1 \equiv 0 \pmod{p}$ have a common solution, namely, $-b'$. Hence we get $N^f(p,c) = 2$ in this case.

Next, we consider the case when $ac \equiv -2 \pmod{p}$. Multiplying both sides of the congruence by a', we get $c + a' \equiv -a' \pmod{p}$. Now, $-a'$ is the solution of $aX + 1 \equiv 0 \pmod{p}$ and $c + a'$ is the solution of $a(c - X) + 1 \equiv 0 \pmod{p}$. Hence the congruences $a\ell + 1 \equiv 0 \pmod{p}$ and $ac + 1 - a\ell \equiv 0 \pmod{p}$ have a common solution $\pmod{p}$. Similarly, we can also show that $b\ell + 1 \equiv 0 \pmod{p}$ and $bc + 1 - b\ell \equiv 0 \pmod{p}$ have a common solution $\pmod{p}$, when $bc \equiv -2 \pmod{p}$. Both the conditions $ac \equiv -2 \pmod{p}$ and $bc \equiv -2 \pmod{p}$ cannot occur simultaneously, for otherwise, it would imply $2(a-b) \equiv 0 \pmod{p}$, which is a contradiction to the fact that $\gcd(a-b, p) = 1$ and p is odd . Therefore, the solution of the congruence $a\ell + 1 \equiv 0 \pmod{p}$ is distinct from that of $b\ell + 1 \equiv 0 \pmod{p}$. Henc e we get $N^f(p,c) = 3$, if $ac \equiv -2 \pmod{p}$ or $bc \equiv -2 \pmod{p}$ and the proof of the claim follows.

Finally, if $a + b \not\equiv -abc \pmod{p}$, $ac \not\equiv -2 \pmod{p}$ and $bc \not\equiv -2 \pmod{p}$, then from the above claim, it follows that all the four congruences $aX + 1 \equiv 0 \pmod{p}$, $bX + 1 \equiv 0 \pmod{p}$, $a(c - X) + 1 \equiv 0 \pmod{p}$ and $b(c - X) + 1 \equiv 0 \pmod{p}$ have pairwise distinct solutions $\pmod{p}$. Hence $N^f(p,c) = 4$ in this case. This completes the proof of Corollary. □

3.7 Concluding remarks

By Proposition 3.3.3 and Remark 3.2.2, it is clear that the expression (3.1) holds for an infinite family of polynomials over $\mathbb{Z}$. In view of Remark 3.2.3, in the following proposition, we prove that the expression (3.1) also holds for any non-constant polynomial over $\mathbb{Z}$ and when n is a prime number p. However, the argument in Proposition 3.7.1 does not go through for n other than primes.

Proposition 3.7.1 *Let $f(X) \in \mathbb{Z}[X]$ be a non-constant polynomial and p be any prime number. For an integer c with $1 \leq c \leq p-1$, let $\mathcal{E}_{f,p}(c) := \{(x,y) \in \mathcal{E}_{f,p} \times \mathcal{E}_{f,p} : x+y \equiv c \pmod{p}\}$. Then*

$$|\mathcal{E}_{f,p}(c)| = p\left(1 - \frac{N^f(p,c)}{p}\right),$$

where $N^f(p,c) = \#\{\ell \pmod{p} \mid$ either $f(\ell) \equiv 0 \pmod{p}$ or $f(c-\ell) \equiv 0 \pmod{p}\}$.

Proof. For a non-constant polynomial $f(X) \in \mathbb{Z}[X]$, the set of all f-exunits in $\mathbb{Z}/p\mathbb{Z}$, $\mathcal{E}_{f,n}$, is $\{1 \leq a \leq p : p \nmid f(a)\}$. Therefore, we see that $\mathcal{E}_{f,p}(c) = \{1 \leq a \leq p : p \nmid f(a)\} \cap \{1 \leq a \leq p : p \nmid f(c-a)\}$. Thus, we obtain

$$\begin{aligned} |\mathcal{E}_{f,p}(c)| &= |\{1 \leq a \leq p : p \nmid f(a)\} \cap \{1 \leq a \leq p : p \nmid f(c-a)\}| \\ &= p - |\{1 \leq a \leq p : f(a) \equiv 0 \pmod{p}\} \cup \{1 \leq a \leq p : f(c-a) \equiv 0 \pmod{p}\}| \\ &= p - N^f(p,c) \end{aligned}$$

and the proof follows.

The above Proposition shows that when n is a prime number, the expression (3.1) is valid for any polynomial $f(X) \in \mathbb{Z}[X]$. This motivates us to ask the following question.

Question 3.7.2 *For any non-constant polynomial $f(X) \in \mathbb{Z}[X]$ and for an integer $n \geq 2$, does the expression (3.1) hold to be true?*

In the remaining part of this section, we provide a few observations regarding the infinite family of polynomials mentioned in Theorem 3.2.1.

(i) For any integer $N \geq 1$, we consider the following set

$$A := \{f(X) \in \mathbb{Z}[X] : \deg(f) = r \text{ and } H(f) \leq N\},$$

where $f(X) = (a_1X + b_1)\cdots(a_rX + b_r)$ is as in Theorem 3.2.1 and $H(f)$ is the height of the polynomial f (defined as the maximum of its coefficients in modulus value). We claim that $|A| \geq N^{1/r(r-1)}$.

For a given $(a_1, \ldots, a_r)$, where $1 \leq a_i \leq N^{1/r^2(r-1)}$, we consider $m = \prod_{\substack{i,j=1 \\ i>j}}^{r}(a_i - a_j)$ and $f(X) = (a_1mX + 1)\cdots(a_rmX + 1)$. Since $|m| \leq (N^{1/r^2(r-1)})^{\frac{r(r-1)}{2}} = N^{1/2r}$, one can easily check that $H(f) \leq N$ and $\gcd(a_imk+1, a_jmk+1) = 1$ for all integer k. Since a_i is any integer in between 1 and $N^{1/r^2(r-1)}$, we get $|A| \geq (N^{1/r^2(r-1)})^r = N^{1/r(r-1)}$. Therefore, we ask the following question.

Question 3.7.3 *What is the lower bound for $|A|$ as a function of N?*

(ii) To answer Question 3.7.3, several families of polynomials satisfying the co-primality condition in Theorem 3.2.1 are needed. Hence this leads to ask the more general question as follows.

Question 3.7.4 *Given an integer $r \geq 1$, classify all positive integers $a_1, \ldots, a_r, b_1, \ldots, b_r$ such that $\gcd(a_ik + b_i, a_jk + b_j) = 1$ for all integers k and $i \neq j$.*

Under certain assumptions, we provide the answer to Question 3.7.4 for the particular case $r = 3$ in the following proposition.

Proposition 3.7.5 *Let $f_1(X) = pX+1$, $f_2(X) = qX+1$ and $f_3(X) = rX+1$ be three polynomials over $\mathbb{Z}$ such that $1 < p < q < r$ and there are exactly two prime numbers among p, q and r. Assume that for any $k \in \mathbb{Z}$ and for $1 \leq i < j \leq 3$, we have $\gcd(f_i(k), f_j(k)) = 1$. Then either $(p, q, r) = (2, 3, 4)$ or $(p, q, r) = (2, 3, 6)$.*

Proof. We denote the set of all prime divisors of an integer n by $\mathfrak{p}(n)$ and we define $\mathfrak{p}(1) = \emptyset$. Since the hypothesis of the proposition satisfies all the

conditions of Lemma 3.3.2, we get $\mathfrak{p}(q-p) \subseteq \mathfrak{p}(p)$, $\mathfrak{p}(r-q) \subseteq \mathfrak{p}(q)$ and $\mathfrak{p}(r-p) \subseteq \mathfrak{p}(p)$. Then we observe that among p, q and r, exactly one can be odd number and hence exactly one of those two prime numbers has to be even prime. Now we claim that $p = 2$.

If $q = 2$, then $f_1(X) = X + 1$ and hence there is no choice of $f_3(X)$. Again if $r = 2$, then $f_2(X) = X + 1$ and we can not find any suitable $f_1(X)$. Hence the claim follows.

We observe that another odd prime number must be q. For otherwise, since $\mathfrak{p}(r-2) \subseteq \mathfrak{p}(2)$, we get $r = 3$ which is not possible as $2 = p < q < r$. Thus we get r is an even composite number. Again $\mathfrak{p}(q-2) \subseteq \mathfrak{p}(2)$ implies that $q = 3$ since q is an odd prime number.

Now $\mathfrak{p}(r-2) \subseteq \mathfrak{p}(2)$ implies that $r = 2^s + 2$ with $s \geq 1$ and $\mathfrak{p}(r-3) \subseteq \mathfrak{p}(3)$ implies $r = 3^t + 3$ with $t \geq 0$. Combining these two relations we get $2^s - 3^t = 1$. We claim that either $s = 1, t = 0$ or $s = 2, t = 1$ are two possible solutions.

To prove this claim, first observe that if $(s, t) \neq (1, 0)$, then s is even. For, if s is odd, then $2^s - 3^t \equiv 2 \pmod 3$, which is not possible since $2^s - 3^t = 1$. Thus, let $s = 2k$, for some integer $k \geq 1$. Now the equation becomes $3^t = 2^s - 1 = 2^{2k} - 1 = (2^k - 1)(2^k + 1)$. Therefore, by the unique factorization in $\mathbb{Z}$, we conclude that

$$2^k - 1 = 3^u \text{ and } 2^k + 1 = 3^v$$

for some integers u and v. From this, we get $3^v - 3^u = 2$ and the only possibility is $(u, v) = (0, 1)$. This, in turn, implies that $k = 1$ and hence we get $s = 2$. Plugging this in the original equation $2^s - 3^t = 1$, we get $t = 1$. Hence the only choice is either $(p, q, r) = (2, 3, 4)$ or $(p, q, r) = (2, 3, 6)$. □

CHAPTER 4

On zero-sum subsequences in a finite abelian p-group of length not exceeding a given number

Let G be a finite abelian group written additively. For a subset $L \subseteq \mathbb{N}$, we define the constant $s_L(G)$ as the least positive integer t such that every sequence over G of length t contains a zero-sum subsequence of length ℓ for some $\ell \in L$. For $L = \{1, 2, \ldots, a\}$, we denote the constant $s_L(G)$ by $s_{\leq a}(G)$. In this chapter, we compute this constant for many class of abelian p-groups. In particular, it proves a conjecture of Schmid and Zhuang [86].

4.1 Introduction

Let G be a finite abelian additive group with exponent $\exp(G)$. A sequence S over G is written as

$$S = \prod_{i=1}^{|S|} g_i = \prod_{g \in G} g^{v_g(S)} \text{ with } v_g(S) \in \mathbb{Z}_{\geq 0}$$

where $v_g(S)$ is called the *multiplicity* of g in S and $|S|$ denotes the length of the sequence S. By the definition of multiplicity, we see that

$$|S| = \sum_{g \in G} v_g(S) \in \mathbb{Z}_{\geq 0}.$$

The sum of all the terms of the sequence S is given by

$$\sigma(S) = \sum_{g \in G} v_g(S) g \in G.$$

A sequence S over G is called a *zero-sum sequence* if $\sigma(S) = 0$. For any integer $k \in \mathbb{Z}_{\geq 0}$ and for a sequence S over G, we define

$$N^k(S) = \left| \left\{ I \subset [1, |S|] \ : \ \sum_{i \in I} g_i = 0, |I| = k \right\} \right|, \tag{4.1}$$

which denotes the number of zero-sum subsequences of S of length k.

For a subset $L \subseteq \mathbb{N}$, we define a constant $s_L(G)$ which is the least positive integer t such that given any sequence S over G of length $|S| \geq t$ satisfying $N^\ell(S) \geq 1$ for some integer $\ell \in L$.

When $L = \{1, \ldots, k\}$ for a given positive integer $k \geq 1$, the constant $s_L(G)$ is denoted by $s_{\leq k}(G)$.

Definition 4.1.1 [81] If $L = \mathbb{N}$, then $s_L(G)$ is denoted by $D(G)$ and it is called

Davenport constant. In other words, $D(G)$ is defined as the least positive integer t such that any given sequence S over G of length $\geq t$ satisfying $N^k(S) \geq 1$ for some integer $k \geq 1$.

The other well-known constant $\eta(G)$ is nothing but $\eta(G) = s_{\leq \exp(G)}(G)$.

Definition 4.1.2 If $L = \{\exp(G)\}$, then $s_L(G)$ is denoted by $s(G)$ and it is called *Erdős-Ginzurg-Ziv-constant (EGZ-constant).*

These constants $D(G)$ and $\eta(G)$ have received a lot of attention (see for instance [6, 16, 17, 19, 20, 21, 27, 30, 32, 36, 86, 91, 55]). When G is a cyclic group, we have $\eta(G) = |G|$, $D(G) = |G|$ and $s(G) = 2|G| - 1$. When $G \cong C_p^2$ for a prime p, Olson [74, 75] proved in 1969 that $\eta(C_p^2) = 3p - 2$ and for any p-group G, he proved that $D(G) = D^*(G)$ where, for any finite abelian group $G' \cong C_{m_1} \oplus \cdots \oplus C_{m_r}$ with $1 < m_1 \leq m_2 \leq \cdots \leq m_r$ are integers satisfying $m_i | m_{i+1}$, the constant $D^*(G')$ is defined by

$$D^*(G') = 1 + \sum_{i=1}^{r} (m_i - 1). \tag{4.2}$$

Analogously, in 1983, Kemnitz [47] conjectured that $s(C_p^2) = 4p-3 = \eta(C_p^2)+p-1$ and it was confirmed by C. Reiher [80] in 2007.

If $G \cong C_m \oplus C_n$ with $m|n$ is the abelian group of rank 2, then it is known that $\eta(G) = 2m+n-2 = s(G)-n+1$ as given in [32] and $D(G) = m+n-1 = D^*(G)$.

In 1992, Geroldinger [33] proved that $D(G) > D^*(G)$ for infinitely many finite abelian groups G with $r(G) \geq 4$. Recently, in [55], some finer results were obtained for some finite abelian groups.

Before that, van Emde Boas [18] (in 1969), R. Meshulam [62] (in 1990), Alford et al. [2] (in 1994), Rath et al. [79] (in 2008) proved a general upper

bound as follows;

$$D(G) \leq \exp(G)\left(1 + \log \frac{|G|}{\exp(G)}\right).$$

In 2014, Gao, Moriya, Pal and Thangadurai [7] proved a linear bound which states that

$$D(C_{n_1} \oplus \cdots \oplus C_{n_r}) \leq n_r + n_{r-1} + (c(3) - 1)n_{r-2} + \cdots + (c(r-2) - 1)n_1$$

for some computable constants $c(r)$ which depends only on r.

Recently in 2018, B. Girand [34] proved the following result.

$$D(C_n^r) \leq r(n-1) + 1 + d(r)\left(\frac{n}{P(n)} - 1\right),$$

where $P(n)$ is the greatest prime power dividing n with the convention $P(1) = 1$ and $d(r)$ is a computable constant depends only on r. Moreover, he proved that $D(C_n^r) \underset{n\to+\infty}{\sim} rn$ which confirms the following Conjecture 4.1.1(a) in asymptotic sense.

The following Conjecture 4.1.1(a) regarding exact values of $D(G)$ is in the literature for long time but it can be found formally stated in [27].

Conjecture 4.1.1 *(a) [27] For all integers n, $r \geq 1$, $D(C_n^r) = r(n-1) + 1$.*

(b) [69] $D(G) \leq \sum_{i-1}^{r} m_i$, where, for any finite abelian group $G \cong C_{m_1} \oplus \cdots \oplus C_{m_r}$ with $1 < m_1 \leq m_2 \leq \cdots \leq m_r$ are integers satisfying $m_i | m_{i+1}$.

(c) [25, 26] $D(G) = D^*(G)$, for all finite abelian group of rank 3.

Regarding the relation between $\eta(G)$ and $s(G)$, Gao and Geroldinger [27] (in 2006) conjectured the following for any finite abelian group.

Conjecture 4.1.2 *[27] For every finite abelian group G, the relation $s(G) = \eta(G) + \exp(G) - 1$ holds.*

In general, for any group G of rank ≥ 3, nothing much is known. For any odd prime p, it is known that $\eta(C_p^3) \geq 8p-7$ ([17]) and $\eta(C_p^4) \geq 19p-18$ ([16]) and their exact values are still unkonwn. In 2007, Gao, Hou, Schmid and Thangadurai [29] conjectured that $s(C_n^3) = 9n-8$, for any odd positive integer n. Recently, Fan, Gao, Wang and Zhong [21] determined the value $\eta(G)$ for special type of abelian groups of rank 3. Very recently, Girand and Schmid ([35]) determined $\eta(G)$ for the group $G = C_2 \oplus C_n \oplus C_m$ with $2|n|m$.

Apart from these results, Schmid and Zhuang [86] proved that if G is a finite abelian p-group with $D(G) = 2\exp(G)-1$, then $\eta(G) = 2D(G) - \exp(G) = s(G) - \exp(G)+1$. Moreover, they conjectured the following.

Conjecture 4.1.3 *([86]) Let G be a finite abelian p-group satisfying $D(G) \leq 2\exp(G)-1$. Then*

$$\eta(G) = 2D(G) - \exp(G) = s(G) - \exp(G) + 1.$$

In 2016, Gao, Han and Zhang [28] proved Conjecture 4.1.3 for the abelian p-groups G satisfying $p > 2r(H)$ and $\left\lceil \frac{2D(H)}{\exp(H)} \right\rceil$ is either even or at most 3. Recently, in [8], Chintamani, Paul and Thangadurai considered similar problem for the complementary case and obtained an upper bound.

The constants $s_{\leq k}(G)$ was introduced by Delorme, Ordaz and Quiroz [11]. It is easy to see that if $k \geq D(G)$, then $s_{\leq k}(G) = D(G)$ and if $1 \leq k < \exp(G)$, we see that $s_{\leq k}(G) = \infty$. In general, the problem of determining exact value of $s_{\leq k}(G)$ is quite difficult. In 2010, Freeze and Schmid [22] proved that $s_{\leq 3}(C_2^r) = 2^{r-1}+1$. In 2017, Wang and Zhao [92] proved that when $G = C_m \oplus C_n$, the constant $s_{\leq D(G)-k}(G) = D(G)+k$ for all integers $k \in [0, m-1]$ and $s_{r-k}(C_2^r) = r+2$ for all $r-k \in \left[\left\lceil \frac{2r+2}{3} \right\rceil, r\right]$.

4.2 Main result

It is clear that $s_{\leq \exp(G)+\ell}(G) \leq \eta(G)$ for all integers $\ell \geq 0$. In this chapter, we prove that $s_{\leq \exp(G)+\ell}(G) \leq \eta(G) - \ell$ for many finite abelian p-groups and for many integers $\ell \geq 0$. Moreover, we prove the equality for $\ell = 0$ and when $G \cong C_{p^m} \oplus C_{p^n}$ with $n \geq m+1$, we prove the equality for all integers $\ell \leq p^m - 1$, which matches with the result of Wang and Zhao [92]. Moreover, in this chapter, we prove the following result.

Theorem 4.2.1 *[82] Let H be a finite abelian p-group with $\exp(H) = p^m$ for some integer $m \geq 1$ and for a prime number $p > 2r(H)$. Let $D(H)$ be its Davenport constant such that $D(H) - 1 = kp^m + t$ for some integers $k \geq 1$ and $0 \leq t \leq p^m - 1$. Let n be an integer satisfying $p^n \geq 2(D(H) - 1)$ and let $G = C_{p^n} \oplus H$. Let ℓ be any integer satisfying $\ell = ap^m + t'$ for some integer a with $0 \leq a \leq k - 1$ and for some integer t' with $0 \leq t' \leq t$. Then, we have*

$$s_{\leq \exp(G)+\ell}(G) \leq \exp(G) + 2(D(H) - 1) - \ell = 2D(G) - \exp(G) - \ell.$$

Moreover, when $\ell = 0$, we get the equality which proves Conjecture 4.1.3 for all such p-groups G and when $G \cong C_{p^m} \oplus C_{p^n}$ with $n \geq m + 1$, for all integers $0 \leq \ell \leq p^m - 1$, we get

$$s_{\leq \exp(G)+\ell}(G) = 2D(G) - \exp(G) - \ell.$$

By refining the method employed in [28], we shall prove Theorem 4.2.1.

4.3 Preliminaries

We start with the following definition of *Group Ring*.

Definition 4.3.1 Let G be a finite abelian group and R be a commutative ring with 1, unit element. Consider the formal expressions

$$R[G] := \left\{ \sum_{g \in G} a_g g : a_g \in R \right\}.$$

In this set $R[G]$, we declare two elements

$$x = \sum_{g \in G} a_g g \text{ and } y = \sum_{g \in G} b_g g$$

are said to be equal if and only if

$$a_g = b_g \text{ for all } g \in G.$$

Note that since $1 \in R$, we identify $g \in G$ as a element of $R[G]$ by writing $1.g \in R[G]$. Also note that $1 = 1.e \in R[G]$ where e is the identity element of G. We can define component wise addition as follows; If

$$x = \sum_{g \in G} a_g g \text{ and } y = \sum_{g \in G} b_g g$$

are the elements of $R[G]$, we define

$$x + y = \sum_{g \in G} (a_g + b_g) g.$$

Then note that since $a_g, b_g \in R$ and it is a ring, $a_g + b_g = c_g \in R$. Therefore, $x + y \in R[G]$. It can be easily check that with respect to addition $(R[G], +)$ is an abelian group. Also, with respect to multiplication of the ring R, we define

a multiplication in $R[G]$ as follows; If

$$x = \sum_{g \in G} a_g g \text{ and } y = \sum_{g \in G} b_g g$$

are the elements of $R[G]$, we define

$$x.y = \sum_{g \in G} c_g g \text{ where } c_g = \sum_{g_1, g_2 \in G} \sum_{g_1 g_2 = g} a_{g_1} b_{g_2}.$$

Note that since R is a ring, it is clear that $c_g \in R$ and hence $x.y \in R[G]$. Thus $(R[G], +, .)$ forms a commutative ring. Also, note that we can identify G inside $R[G]$ because for any element $g \in G$, we define $a_g = 1 \in R$ and $1.g \in R[G]$. This commutative ring $R[G]$ is called *group ring*.

Lemma 4.3.2 *For an abelian group G, we have*

$$D^*(G) \leq D(G) \leq |G|.$$

Proof. First we prove the upper bound. Let $S = a_1 a_2 \dots a_{|G|}$ be a given sequence of elements of G of length $|G|$. Construct a new sequence $T = b_1 b_2 \dots b_{|G|}$ of elements of G of length $|G|$, where

$$b_i = a_1 + a_2 + \cdots + a_i \text{ for all } i = 1, 2, \dots, |G|.$$

If all the elements of b_i are distinct, then as the length of T is $|G|$, then there exists j such that $b_j = 0$. If all the elements are not distinct, then there exist $i < j$ such that $b_i = b_j$ which means that

$$a_1 + a_2 + \cdots + a_i = a_1 + a_2 + \cdots + a_i + a_{i+1} + \cdots + a_j.$$

This gives us that $a_{i+1} + \cdots + a_j = 0$, which proves the upper bound.

Now to prove the lower bound, we need to construct a sequence S of elements of G of length $D^*(G) - 1$ which does not contain any zero-sum subsequence. Let $G \cong C_{m_1} \oplus \cdots \oplus C_{m_r}$ with $m_1 m_2 \ldots m_r = |G|$. Let $x_i = 1$ be the generator of C_{m_i}, for all $i = 1, 2, \ldots, r$. We embed x_i in G as $x_i = (0, \ldots, 0, 1, 0, \ldots, 0)$ where 1 is in the ith position and rest is 0 as an element of C_{m_i}. Now consider the sequence

$$S = \left(\underbrace{x_1, \ldots, x_1}_{m_1 - 1 \text{ times}}, \ldots \underbrace{\ , \ }_{x_r, \ldots, x_{r_{m_r - 1 \text{ times}}}} \right)$$

of elements of G of length $D^*(G) - 1$. Clearly, this sequence doesn't have a zero-sum subsequence in it because, any subsequence sum has a i-th co-ordinate which is non-zero as 1 repeats at most $m_i - 1$ times. This proves the lower bound. □

Corollary 4.3.3 *Let $G = C_n$ be the cyclic group of order n. Then*

$$D(C_n) = n.$$

Proof. Since $|G| = n = D^*(G)$, by the above theorem, we get the result. □

Theorem 4.3.4 *[74] Let G be a finite abelian p-group written multiplicatively such that $G \cong C_{p^{e_1}} \oplus \cdots \oplus C_{p^{e_r}}$. If S is a sequence over G with $|S| = \ell \geq 1 + \sum_{i=1}^{r} (p^{e_i} - 1) = D^*(G)$, then for $g = e$,*

$$1 - N_e^1(S) + N_e^2(S) - \cdots (-1)^\ell N_e^\ell(S) = a_1 \equiv 0 \pmod{p}.$$

and for $g \neq e$,

$$-N_g^1(S) + N_g^2(S) - \cdots (-1)^\ell N_g^\ell(S) = a_g \equiv 0 \pmod{p},$$

where $N_g^i(S)$ denotes the number of subsequences of S of i-length whose product is equal to g, for each $g \in G$ and for $1 \leq i \leq |S|$.

Proof. Since $G \cong C_{p^{e_1}} \oplus \cdots \oplus C_{p^{e_r}}$, let x_i be the generator of $C_{p^{e_i}}$, for $i = 1, \ldots, r$. Then any element $g \in G$ will be of the form $g = x_1^{a_1} \ldots x_r^{a_r}$. First note that if $h \in G$ and $h = uv$, then we can write

$$(1 - h) = (1 - uv) = (1 - u) + u(1 - v).$$

Therefore, we can write any element $(1 - x_1^{a_1} \ldots x_r^{a_r})$ as follows;

$$\begin{aligned}
(1 - x_1^{a_1} \ldots x_r^{a_r}) &= (1 - x_1) + x_1(1 - x_1) + \cdots + x_1^{a_1 - 1}(1 - x_1) \\
&+ x_1^{a_1}(1 - x_2) + x_1^{a_1}x_2(1 - x_2) + \cdots + x_1^{a_1}x_2^{a_2 - 1}(1 - x_2) \\
&\cdots \quad \cdots\cdots \\
&+ x_1^{a_1} \ldots x_{r-1}^{a_{r-1}}(1 - x_r) + x_1^{a_1} \ldots x_{r-1}^{a_{r-1}}x_r(1 - x_r) \\
&+ \ldots + x_1^{a_1} \ldots x_r^{a_r}.
\end{aligned}$$

Since $x_i^{c_i}$ are elements of G and all $(1 - x_j) \in \mathbb{Z}[G]$ a group ring element, we note that right hand side element lies in the group ring $\mathbb{Z}[G]$.

Now, consider the given sequence $S = g_1 \ldots g_\ell$ of elements of G of length ℓ such that $\ell \geq 1 + \sum_{i=1}^{r}(p^{e_i} - 1)$. Since each element of the sequence g_i is of the form $x_1^{a_1} \ldots x_r^{a_r}$ for some integers $a_i \geq 0$, by the above observation, we see that

$$(1 - g_1) \cdots (1 - g_\ell) = \sum_{g \in G} g J_g,$$

where $J_g = (1 - x_1)^{c_1} \cdots (1 - x_r)^{c_r}$ with $\sum_{i=1}^{r} c_i \geq \ell$ and $c_i \geq 0$ integers. Since

$\ell \geq \sum_{i=1}^{r}(p^{e_i}-1)+1$, we conclude that

$$\sum_{i=1}^{r} c_i \geq \ell > \sum_{i=1}^{r}(p^{e_i}-1).$$

For all $i = 1, 2, \ldots, r$, if we have $c_i \leq p^{e_i} - 1$, then we get

$$\sum_{i=1}^{r} c_i \leq \sum_{i=1}^{r}(p^{e_i}-1) < \ell$$

which is impossible. Hence there exists i such that $1 \leq i \leq r$ and $c_i \geq p^{e_i}$. Then consider that element of the group ring

$$(1-x_i)^{c_i} = (1-x_i)^{p^{e_i}}(1-x_i)^{c_i - p^{e_i}}.$$

By the binomial expansion, we see that

$$(1-x_i)^{p^{e_i}} = 1 - p^{e_i}x_i + p \cdot \text{ elements of } \mathbb{Z}[G] + (-1)^{p^{e_i}} x_i^{p^{e_i}} \in \mathbb{Z}[G].$$

As x_i is a generator of $C_{p^{e_i}}$, we have $x_i^{p^{e_i}} = 1$ in $C_{p^{e_i}}$. If p is an odd prime, then $(-1)^{p^{e_i}} = -1$ and hence, in this case, we get

$$(1-x_i)^{p^{e_i}} = 1 - p \cdot \text{ elements of } \mathbb{Z}[G] - 1 = p \cdot \text{ elements of } \mathbb{Z}[G] \in p\mathbb{Z}[G].$$

When $p = 2$, then

$$(1-x_i)^{2^{e_i}} = 1 - 2 \cdot \text{ elements of } \mathbb{Z}[G] + 1 = 2 \cdot \text{ elements of } \mathbb{Z}[G] \in 2\mathbb{Z}[G].$$

In both cases, we get $(1-x_i)^{p^{e_i}} \in p\mathbb{Z}[G]$. This implies for each $g \in G$, we see

that $J_g \in p\mathbb{Z}[G]$ which in turn implies

$$(1-g_1)\cdots(1-g_\ell) = \sum_{g\in G} gJ_g \in p\mathbb{Z}[G]. \tag{4.3}$$

Note that we know the following identity:

$$(1-y_1)\cdots(1-y_r) = 1 - \sum_{i=1}^{r} y_i + \sum_{i<j} y_iy_j - \cdots (-1)^r y_1 \ldots y_r. \tag{4.4}$$

Therefore, in the expression $(1-g_1)(1-g_2)\cdots(1-g_\ell)$, even length subsequences product comes with $+$ sign, while odd length subsequences product comes with $-$ sign. In above, we see that

$$(1-g_1)(1-g_2)\cdots(1-g_\ell) = \sum_{g\in G} a_g g, \tag{4.5}$$

where a_g denotes the number of subproducts of $g_1 \ldots g_\ell$ is equal to g. Thus, by (4.3) and (4.4), $a_g \equiv 0 \pmod{p}$ for all $g \in G$.

When $g = e$, we take the ring element $1 \in \mathbb{Z}$ and write it as $1.e \in \mathbb{Z}[G]$. Hence for $g = e$, by (4.5), we get

$$1 - N_e^1(S) + N_e^2(S) - \cdots (-1)^\ell N_e^\ell(S) = a_e \equiv 0 \pmod{p}.$$

On the other hand, when $g \neq e$, by (4.5), we get

$$-N_g^1(S) + N_g^2(S) - \cdots (-1)^\ell N_g^\ell(S) = a_g \equiv 0 \pmod{p}.$$

Thus, we get the theorem. □

Theorem 4.3.5 *[74] Let G be a finite belian p-group written multiplicatively.*

Then

$$D(G) = D^*(G).$$

Proof. By Lemma 4.3.2, we know that $D(G) \geq D^*(G)$. We need to prove that $D(G) \leq D^*(G)$.

Let $S = g_1 g_2 \dots g_{D^*(G)}$ be given sequence in G. By Theorem 4.3.4, we get

$$-N_e^1(S) + N_e^2(S) - \cdots (-1)^{|S|} N_e^{|S|}(S) \equiv -1 \pmod{p}.$$

This means that either $N_e^i(S) \neq 0$, for some $1 \leq i \leq |S|$. Therefore, there exists a non-empty subsequence of length i such that its product is e. This implies $D(G) \leq D^*(G)$. □

From the last two theorems, we get the following two corollaries for any finite abelian additive p-groups which we list as a lemma.

Lemma 4.3.6 *[74] Let G be a finite abelian p-group written additively. Then $D(G) = D^*(G)$. Moreover, if S is a sequence over G with $|S| = \ell \geq D^*(G)$, then*

$$1 - N^1(S) + N^2(S) - \cdots + (-1)^{\ell} N^{\ell}(S) \equiv 0 \pmod{p},$$

where $N^i(S)$ is defined in equation (4.1).

Lemma 4.3.7 *([18]) Let H be a finite abelian p-group with $D(H) \leq p^n - 1$ and let $G = C_{p^n} \oplus H$. Then, $D(G) = p^n + D(H) - 1 = \exp(G) + D(H) - 1$.*

Proof. Since G is also a finite abelian p-group, by Lemma 4.3.6, it is clear that $D(G) = D^*(G) = D^*(H) + p^n - 1 = p^n + D(H) - 1$. Again we have $D(H) \leq p^n - 1$ which implies $\exp(G) = p^n$. Hence the proof follows. □

Lemma 4.3.8 *([16]) Let G be any finite abelian p-group with exponent $\exp(G)$ such that $D(G) \leq 2\exp(G) - 1$. Then $\eta(G) \geq 2D(G) - \exp(G)$.*

Proof. We can write $G = H \oplus \langle a \rangle$, where H is a subgroup of G and a is an element of order $\exp(G)$. Since $D(G) \leq 2\exp(G) - 1$, we also have $D(H) \leq 2\exp(G) - 1$. Hence, by Lemma 4.3.7, we get

$$D(G) = D(H) + \exp(G) - 1. \tag{4.6}$$

Let $T = g_1 \dots g_\ell$ be a sequence over H of length $|T| = \ell = D(H) - 1$ which has no zero-sum subsequence. Now we construct the following the sequence over G

$$S = \underbrace{a \dots a}_{(\exp(G)-1)-times} g_1 \dots g_\ell (g_1 + a) \dots (g_\ell + a)$$

and obviously it has no zero-sum subsequence of any length ℓ_1, where $1 \leq \ell_1 \leq \exp(G)$. This implies $\eta(G) \geq |S| + 1 = 2(D(H) - 1) + \exp(G)$. Therefore, using (4.6), we get $\eta(G) \geq 2D(G) - \exp(G)$. □

Lemma 4.3.9 *([28]) Let G be a finite abelian p-group and let m be a positive integer. If S is a sequence over G of length $|S| \geq D(G) + p^m - 1$, then we have*

$$1 + \sum_{j=1}^{\lfloor \frac{|S|}{p^m} \rfloor} (-1)^j N^{jp^m}(S) \equiv 0 \pmod{p}.$$

Proof. Let us assume $G \oplus C_{p^m} = G \oplus \langle a \rangle$, where $\langle a \rangle = C_{p^m}$. Also assume $\Phi : G \to G \oplus C_{p^m}$ be defined by $\Phi(g) = g + a$ for every $g \in G$. Let $S = g_1 \dots g_\ell$ be a sequence over G. Hence $\Phi(S) = (g_1 + a) \dots (g_\ell + a)$ is a sequence over $G \oplus C_{p^m}$.

Since $|\Phi(S)| = D(G) + p^m - 1 = D^*(G)$, we can apply Lemma 4.3.6 to the

sequence $\Phi(S)$ and hence we get

$$1+\sum_{j=1}^{\lfloor \frac{|S|}{p^m} \rfloor}(-1)^j N^{jp^m}(\Phi(S)) \equiv 0 \pmod{p}.$$

Note that, $\Phi(T)$ is a zero-sum subsequence of $\Phi(S)$ over $G \oplus C_{p^m}$ if and only if T is a zero-sum subsequence of S and $|T| \equiv 0 \pmod{p^m}$.

Using this observation, we get

$$1+\sum_{j=1}^{\lfloor \frac{|S|}{p^m} \rfloor}(-1)^j N^{jp^m}(S) \equiv 0 \pmod{p}$$

which completes the proof. □

Throughout this section, now on, we take H to be a finite abelian p-group of rank $r(H)$ and exponent $\exp(H) = p^m$ for some positive integer m. Also, we write $D(H)-1 = kp^m+t$ for some positive integer k and a non-negative integer t satisfying $0 \le t \le p^m-1$. Choose any integer n such that $p^n \ge 2(D(H)-1)$ and let $G = C_{p^n} \oplus H$. Let ℓ be any integer satisfying $\ell = ap^m + t'$ for some integer a with $0 \le a \le k-1$ and for some integer t' with $0 \le t' \le t$.

We need the following lemma which was proved in ([28]) for the case when $\ell = 0$. We prove for all integers ℓ satisfying as above.

Lemma 4.3.10 *Let $v = (k+1)p^m - D(H) = p^m - t - 1$. Let S be a sequence over G of length $|S| = p^n + 2(D(H)-1) - \ell$ such that $N^b(S) = 0$ for all integers b with $1 \le b \le p^n + \ell$. Then for any integers $i \in [0, k-a-1]$, $h \in [0, v+\ell]$ or $i = k-a$ and $h = v+\ell$ and for any subsequence T of S of length $|T| = |S| - ip^m$, we have*

$$1+\sum_{u=0}^{h}\binom{h}{u}\sum_{j=a+1}^{k}(-1)^{j-1}N^{p^n+jp^m-u}(T) \equiv 0 \pmod{p}. \tag{4.7}$$

Proof. First, we claim the following.

Claim. $N^i(S) = 0$ for all $i \in [1, p^n + \ell] \cup [p^n + D(H), |S|]$.

Since S has no zero-sum subsequence of length $\leq p^n + \ell$, by the hypothesis, we assume that $N^i(S) \neq 0$ for some integer $i \in [p^n + D(H), |S|]$. Let W be a zero-sum subsequence of S of length $|W| = i \geq p^n + D(H)$. Since $D(G) = p^n + D(H) - 1$, there exist two disjoint zero-sum subsequences W_1 and W_2 such that $|W_1| \leq |W_2|$ and $W = W_1W_2$. Since $N^j(S) = 0$ for any $j \in [1, p^n + \ell]$, it is clear that $|W_b| \geq p^n + \ell + 1$ for all integers $b = 1, 2$. Therefore, $|S| \geq |W| = |W_1| + |W_2| \geq 2p^n + 2\ell + 2$, which is a contradiction to the assumption that $|S| \leq 2p^n$. Therefore, we get the claim.

In order to get those congruences, we need to apply Lemma 4.3.9 suitably. In order to apply Lemma 4.3.9, we shall consider the finite abelian group $G' = G \oplus C_{p^m}$ and consider the homomorphism $f : G \to G'$ by $f(g) = g + e$ where e is a generator of the cyclic group C_{p^m}. Under this homomorphism, we consider the image of the given sequence $f(S)$.

Let i be a fixed integer with $0 \leq i \leq k - a - 1$. Let T be a subsequence of S of length $|T| = |S| - ip^m = p^n + 2(D(H) - 1) - \ell - ip^m$. Let h be a fixed integer with $0 \leq h \leq v + \ell$ and consider the sequence $T0^h$. Then,

$$\begin{aligned} |T0^h| &= |T| + h = p^n + D(H) - 1 + D(H) - 1 + h - \ell - ip^m \\ &= D(G) + kp^m + t + h - ap^m - t' - ip^m \\ &= D(G) + (k - a - i)p^m + t - t' + h \\ &\geq D(G) + p^m \end{aligned}$$

holds true for all integers $i \in [0, k - a - 1]$ and for all integers $h \in [0, v + \ell]$ as

$t' \leq t$. Also, when $i = k - a$, we take $h = v + \ell$ so that we get

$$|T0^{v+\ell}| = D(G) + t - \ell + v + \ell = D(G) + t + p^m - t - 1 = D(G) + p^m - 1.$$

Now, we apply Lemma 4.3.9 to the sequence $f(T0^h)$ to get

$$1 + \sum_{j=1}^{z} (-1)^j N^{jp^m}(f(T0^h)) \equiv 0 \pmod{p} \tag{4.8}$$

where $z = \left\lfloor \frac{|T0^h|}{p^m} \right\rfloor$, for all integers $i \in [0, k-a-1]$ and $h \in [0, v+\ell]$ and when $i = k - a$, take $h = v + \ell$. Note that for each integer $j = 1, 2, \ldots, z$, we have

$$N^{jp^m}(f(T0^h)) = \sum_{u=0}^{h} \binom{h}{u} N^{jp^m - u}(T).$$

Therefore, for every integers $i \in [0, k-a-1]$ and $h \in [0, v+\ell]$ or when $i = k-a$, we take $h = v + \ell$, we get,

$$1 + \sum_{u=0}^{h} \binom{h}{u} \sum_{j=1}^{z} (-1)^{j-1} N^{jp^m - u}(T) \equiv 0 \pmod{p}.$$

Since, by claim, we know that $N^b(T) = 0$ for all $b \in [1, p^n + \ell] \cup [p^n + D(H), |T|]$, and $p^n + D(H) = p^n + (k+1)p^m - v$, we get

$$1 + \sum_{u=0}^{h} \binom{h}{u} \sum_{j=a+1}^{k} (-1)^{j-1} N^{p^n + jp^m - u}(T) \equiv 0 \pmod{p}$$

is true for all integers $i \in [0, k-a-1]$ and $h \in [0, v+\ell]$ and when $i = k - a$, take $h = v + \ell$. From this, we get the required congruences. □

Now, we shall prove the following refinement of Lemma 3.1 (3.3) in [28].

Lemma 4.3.11 *Let $v = (k+1)p^m - D(H) = p^m - t - 1$. Let S be a sequence over*

G of length $|S| = p^n + 2(D(H) - 1) - \ell$ for some integer ℓ satisfying $\ell = ap^m + t'$ for some integer a with $0 \le a \le k-1$ and for some integer t' with $0 \le t' \le t$ such that $N^b(S) = 0$ for all integers b with $1 \le b \le p^n + \ell$. For any integers i and h satisfying $0 \le i \le k-a-1$ and $0 \le h \le v + \ell$, we have

$$\binom{|S|}{ip^m} + \sum_{j=a+1}^{k} (-1)^{j-1} \sum_{u=0}^{h} \binom{h}{u} \binom{|S| - p^n - jp^m + u}{ip^m} N^{p^n + jp^m - u}(S) \equiv 0 \pmod{p}. \tag{4.9}$$

and

$$\binom{|S|}{(k-a)p^m} + \sum_{u=0}^{v+\ell} \binom{v+\ell}{u} \sum_{j=a+1}^{k} (-1)^{j-1} \binom{|S| - p^n - jp^m + u}{(k-a)p^m} N^{p^n + jp^m - u}(S) \equiv 0 \pmod{p}. \tag{4.10}$$

Proof. In order to get (4.9), we take a subsequence T of S such that $|T| = |S| - ip^m$ for a given integer i with $0 \le i \le k-a-1$. Then for any integer $h \in [0, v+\ell]$, by (4.7), we get

$$1 + \sum_{u=0}^{h} \binom{h}{u} \sum_{j=a+1}^{k} (-1)^{j-1} N^{p^n + jp^m - u}(T) \equiv 0 \pmod{p}.$$

Now we sum over all the subsequences T with $|T| = |S| - ip^m$ and we get

$$\sum_{T, |T| = |S| - ip^m} \left(1 + \sum_{u=0}^{h} \binom{h}{u} \sum_{j=a+1}^{k} (-1)^{j-1} N^{p^n + jp^m - u}(T) \right) \equiv 0 \pmod{p}. \tag{4.11}$$

Since each subsequence W of S with $|W| \le |S| - ip^m$ can be extended to a subsequence T of length $|T| = |S| - ip^m$ in

$$\binom{|S| - |W|}{|T| - |W|} = \binom{|S| - |W|}{|S| - |T|} = \binom{|S| - |W|}{ip^m}$$

ways, by starting with 0 length subsequence W of S, we see that the number of ways to get subsequences T of S with $|T| = |S| - ip^m$ is $\binom{|S|}{ip^m}$. Then, using this and expanding the sum in (4.11), we arrive at (4.9). To get (4.10), we put $i = k - a$ and $h = v + \ell$ in (4.7) and apply the same proceedure. This proves the lemma. □

Corollary 4.3.12 *Let S be a sequence over G as defined in Lemma 4.3.11. For any integer i with $0 \le i \le k - a - 1$ and for every integer h with $1 \le h \le v + \ell$, we have*

$$\binom{|S|}{ip^m} + \sum_{j=a+1}^{k} (-1)^{j-1} \binom{|S| - p^n - jp^m}{ip^m} N^{p^n+jp^m}(S) \equiv 0 \pmod{p} \qquad (4.12)$$

and

$$\sum_{j=a+1}^{k} (-1)^{j-1} \binom{|S| - p^n - jp^m + h}{ip^m} N^{p^n+jp^m-h}(S) \equiv 0 \pmod{p}. \qquad (4.13)$$

Proof. To prove (4.12), we put $h = 0$ in (4.9) (Lemma 4.3.11) and we get the congruence.

We shall prove (4.13) by induction on h. When $h = 1$, by (4.9) (Lemma 4.3.11), we get,

$$\binom{|S|}{ip^m} + \sum_{j=a+1}^{k} (-1)^{j-1} \left[\binom{1}{0} \binom{|S| - p^n - jp^m}{ip^m} N^{p^n+jp^m}(S) + \binom{1}{1} \binom{|S| - p^n - jp^m + 1}{ip^m} N^{p^n+jp^m-1}(S) \right] \equiv 0 \pmod{p}.$$

Therefore, by (4.12), we get (4.13) with $h = 1$.

Suppose we assume (4.13) is true for all integers $b < h$ and we shall prove

for h. We shall rewrite (4.9) with h as follows.

$$\binom{|S|}{ip^m} + \sum_{j=a+1}^{k} (-1)^{j-1} \sum_{b=0}^{h} \binom{h}{b} \binom{|S| - p^n - jp^m + \ell}{ip^m} N^{p^n+jp^m-b}(S) \equiv 0 \pmod{p}$$

$$\implies \binom{|S|}{ip^m} + \sum_{b=0}^{h-1} \binom{h}{\ell} \sum_{j=a+1}^{k} (-1)^{j-1} \binom{|S| - p^n - jp^m + b}{ip^m} N^{p^n+jp^m-b}(S)$$
$$+ \sum_{j=a+1}^{k} (-1)^{j-1} \binom{|S| - p^n - jp^m + h}{ip^m} N^{p^n+jp^m-h}(S) \equiv 0 \pmod{p}$$

By applying induction hypothesis, we get,

$$\sum_{j=a+1}^{k} (-1)^{j-1} \binom{|S| - p^n - jp^m + h}{ip^m} N^{p^n+jp^m-h}(S) \equiv 0 \pmod{p}$$

as required. □

Theorem 4.3.13 *([58]) Let p be a prime number. Let a and b be positive integers with $a = a_n p^n + a_{n-1}p^{n-1} + \cdots + a_0$ with $a_i \in \{0, 1, \ldots, p-1\}$ and $b = b_n p^n + b_{n-1}p^{n-1} + \cdots + b_0$ with $b_i \in \{0, 1, \ldots, p-1\}$. Then*

$$\binom{a}{b} \equiv \binom{a_n}{b_n} \binom{a_{n-1}}{b_{n-1}} \cdots \binom{a_0}{b_0} \pmod{p}.$$

where $\binom{a_i}{b_i} = 0$, if $a_i < b_i$ and $\binom{0}{0} = 1$.

Proof. At first note that

$$\begin{aligned}(1+x)^a &= (1+x)^{a_n p^n + a_{n-1}p^{n-1} + \cdots + a_0} \\ &= (1+x)^{a_n p^n} \cdots (1+x)^{a_1 p} (1+x)^{a_0}\end{aligned}$$

$$\equiv \quad (1+x^{p^n})^{a_n}\cdots(1+x^p)^{a_1}(1+x)^{a_0} \pmod{p}.$$

If $b<a$, then coefficient of x^b of $(1+x)^a$ is $\binom{a}{b}$ and the coefficient of x^b on right is $\binom{a_n}{b_n}\binom{a_{n-1}}{b_{n-1}}\cdots\binom{a_0}{b_0} \pmod{p}$. Thus comparing those suitable coefficients, the result follows. □

Theorem 4.3.14 *([28]) Let n and k be positive integers with $1 \le 2k \le n$. Let A be the following $(k+1)\times(k+1)$ matrix with positive integers*

$$A = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \binom{n}{1} & \binom{n-1}{1} & \cdots & \binom{n-k}{1} \\ \binom{n}{2} & \binom{n-1}{2} & \cdots & \binom{n-k}{2} \\ \cdots & & \cdots & \\ \binom{n}{k} & \binom{n-1}{k} & \cdots & \binom{n-k}{k} \end{pmatrix}.$$

Then, the determinant of A is

$$\det(A) = \left(\prod_{t=1}^{k} t!\right)^{-1} \prod_{0\le i<j\le k} (i-j).$$

Proof. It is given that

$$A = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ n & n-1 & \cdots & n-k \\ \frac{n(n-1)}{2!} & \frac{(n-1)(n-2)}{2!} & \cdots & \frac{(n-k)(n-k-1)}{2!} \\ \cdots & & \cdots & \\ \frac{n\cdots(n-k+1)}{k!} & \frac{(n-1)\cdots(n-k)}{k!} & \cdots & \frac{(n-k)\cdots(n-2k+1)}{k!} \end{pmatrix}.$$

Therefore, we note that $\det(A) = \frac{1}{\prod\limits_{1\leq t\leq k} t!}\det(B)$, where

$$B = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ n & n-1 & \cdots & n-k \\ n(n-1) & (n-1)(n-2) & \cdots & (n-k)(n-k-1) \\ \cdots & & \cdots & \\ n\cdots(n-k+1) & (n-1)\cdots(n-k) & \cdots & (n-k)\cdots(n-2k+1) \end{pmatrix}.$$

Now, we denote the i-th row of B by $Row_B(i)$. At first, we replace $Row_B(3)$ by $Row_B(3) + Row_B(2)$ and get the following matrix

$$B = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ n & n-1 & \cdots & n-k \\ n^2 & (n-1)^2 & \cdots & (n-k)^2 \\ \cdots & & \cdots & \\ n\cdots(n-k+1) & (n-1)\cdots(n-k) & \cdots & (n-k)\cdots(n-2k+1) \end{pmatrix}.$$

Here we denote the new matrix also by B. Now, we consider the polynomial $f_i(x) = x(x-1)\cdot(x-i+2) = x^{i-1}+a_{i-2}x^{i-2}+\cdots+a_1x$. Using coefficients of this polynomial, for $4 \leq i \leq k+1$, we successively replace $Row_B(i)$ by $Row_B(i) - a_{i-2}Row_B(i-1) - \cdots - a_1Row_B(2)$. For simplicity, after each row-replacement, we denote the new matrix by B. Therefore, after all row-replacements, we get

$$C = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ n & n-1 & \cdots & n-k \\ n^2 & (n-1)^2 & \cdots & (n-k)^2 \\ \cdots & & \cdots & \\ n^k & (n-1)^k & \cdots & (n-k)^k \end{pmatrix}.$$

Next, we note that $\det(C)$ is a Vandermonde determinant and $\det(C) = \det(B)$. Hence, we get

$$\det(A) = \frac{1}{\prod\limits_{1\le t\le k} t!}\det(C) = \frac{1}{\prod\limits_{1\le t\le k} t!}\prod_{0\le i<j\le k}(n-j-n+i) = \frac{1}{\prod\limits_{1\le t\le k} t!}\prod_{0\le i<j\le k}(i-j).$$

□

The following is the crucial observation for the proof of Theorem 4.2.1.

Theorem 4.3.15 *[82] Let S be a sequence over G which is defined as in Lemma 4.3.11. Then for every integer $j \in [a+1, k]$ and for every integer $h \in [1, v+\ell]$, we get,*

$$N^{p^n+jp^m-h}(S) \equiv 0 \pmod{p}.$$

Proof. Since $p^n \ge 2(D(H)-1) = 2(kp^m+t)$ and $p > 2r(H)$, we see that $2k+1 < p$. Let h be a fixed integer such that $1 \le h \le v+\ell$. For any integer $j = a+1, a+2, \ldots, k$, we see that

$$|S| - p^n - jp^m + h = p^n + 2(kp^m+t) - p^n - jp^m + h - \ell = (2k-j)p^m + 2t + h - \ell.$$

Note that

$$2t+h-\ell \le 2t+v+\ell-\ell = 2t+p^m-t-1 = t+p^m-1 \le p^m-1+p^m-1 = 2p^m-2,$$

as $t \le p^m - 1$. Hence, for each integer $j = a+1, a+2, \ldots, k$, we see that

$$|S| - p^n - jp^m + h = (2k-j+c)p^m + f$$

where $c = 0$ or 1 depending on values t and h and for some integer $0 \le f < p^m$.

Therefore, by Theorem 4.3.13, we get

$$\binom{|S|-p^n-jp^m+h}{ip^m} = \binom{(2k-j)p^m+2t+h}{ip^m} \equiv \binom{2k-j+c}{i} \pmod{p} \tag{4.14}$$

for all integers $j = a+1, a+2, \ldots, k$ and $i = 0, 1, \ldots, k-a-1$ where $c = 0$ or 1.

Let h be a fixed integer with $1 \leq h \leq v+\ell$ and let

$$X_j = (-1)^{j-1} N^{p^n+jp^m-h}(S)$$

for every integer $j = a+1, a+2, \ldots, k$. Then by the congruence (4.13) in Corollary 4.3.12, we get a system of $k-a$ number of linear equations in $k-a$ variables over $\mathbb{F}_p$ as follows.

$$X_{a+1} + X_{a+2} + \cdots + X_k = 0;$$

$$\begin{aligned}\binom{|S|-p^n-p^m+h}{p^m} X_{a+1} + \binom{|S|-p^n-2p^m+h}{p^m} X_{a+2} + \\ \cdots + \binom{|S|-p^n-kp^m+h}{p^m} X_k = 0;\end{aligned}$$

$$\cdots \qquad \cdots \qquad \cdots$$

$$\begin{aligned}\binom{|S|-p^n-p^m+h}{(k-a-1)p^m} X_{a+1} + \binom{|S|-p^n-2p^m+h}{(k-a-1)p^m} X_{a+2} + \\ \cdots + \binom{|S|-p^n-kp^m+h}{(k-a-1)p^m} X_k = 0;\end{aligned}$$

By (4.14), the coefficient matrix of the above system of linear equations over $\mathbb{F}_p$

is

$$\begin{pmatrix} 1 & 1 & \cdots & 1 \\ \binom{2k-a-1+c}{1} & \binom{2k-a-2+c}{1} & \cdots & \binom{2k-k+c}{1} \\ \binom{2k-a-1+c}{2} & \binom{2k-a-2+c}{2} & \cdots & \binom{2k-k+c}{2} \\ \cdots & & \cdots & \\ \binom{2k-a-1+c}{k-a-1} & \binom{2k-a-2+c}{k-a-1} & \cdots & \binom{2k-k+c}{k-a-1} \end{pmatrix}$$

whose determinant, by Theorem 4.3.14, is non-zero modulo p, by taking $n = 2k-1+c$ in Theorem 4.3.14. Hence the above system must have zero solutions in $\mathbb{F}_p$. This proves the theorem. □

4.4 Proof of Theorem 4.2.1

We prove that $s_{\leq p^n+\ell}(G) \leq p^n + 2(D(H)-1) - \ell$ for all integers ℓ satisfying $\ell = ap^m + t'$ for some integer a with $0 \leq a \leq k-1$ and for some integer t' with $0 \leq t' \leq t$ where t is an integer satisfying $D(H) - 1 = kp^m + t$ with $0 \leq t \leq p^m - 1$.

Let S be a sequence over G of length $|S| = p^n + 2(D(H)-1) - \ell$. Suppose that $N^b(S) = 0$ for all integers $1 \leq b \leq p^n + \ell$. Then, by Theorem 4.3.15, we know that

$$N^{p^n+jp^m-h}(S) \equiv 0 \pmod{p}$$

for all integers $j \in [a+1, k]$ and integers $h \in [1, v+\ell]$. Therefore, by Lemma 4.3.11, we get,

$$\binom{|S|}{(k-a)p^m} + \sum_{j=a+1}^{k} (-1)^{j-1} \binom{|S| - p^n - jp^m}{(k-a)p^m} N^{p^n+jp^m}(S) \equiv 0 \pmod{p} \tag{4.15}$$

and by Corollary 4.3.12 (4.12), we get,

$$\binom{|S|}{ip^m} + \sum_{j=a+1}^{k} (-1)^{j-1} \binom{|S| - p^n - jp^m}{ip^m} N^{p^n+jp^m}(S) \equiv 0 \pmod{p} \qquad (4.16)$$

holds true for all integers $i \in [0, k-a-1]$.

Now, we put

$$X_j = (-1)^{j-1} N^{p^n+jp^m}(S)$$

for all $j = a+1, a+2, \ldots, k$ and $X_a = 1$. Then, by (4.15) and (4.16), we get a system of $(k-a+1)$ linear equations in $(k-a+1)$ unknowns over $\mathbb{F}_p$ as follows.

$$\binom{|S|}{0} X_a + \binom{|S| - p^n - p^m}{0} X_{a+1} + \cdots + \binom{|S| - p^n - kp^m}{0} X_k \equiv 0 \pmod{p};$$

$$\cdots \qquad \cdots \qquad \cdots$$

$$\binom{|S|}{(k-a-1)p^m} X_a + \binom{|S| - p^n - p^m}{(k-a-1)p^m} X_{a+1} + \cdots + \binom{|S| - p^n - kp^m}{(k-a-1)p^m} X_k \equiv 0 \pmod{p};$$

$$\binom{|S|}{(k-a)p^m} X_a + \binom{|S| - p^n - p^m}{(k-a)p^m} X_{a+1} + \cdots + \binom{|S| - p^n - kp^m}{(k-a)p^m} X_k \equiv 0 \pmod{p}.$$

Now, we need to compute the determinant of the coefficient matrix of the above system. We shall prove that this determinant is non-zero modulo p, which in turn implies that the system has only zero solutions modulo p. This is a contradiction to $X_a \not\equiv 0 \pmod{p}$, which proves the theorem. Hence, we need to compute the

coefficients modulo p and its determinant. Since the calculation is the same as in the proof of Theorem 4.3.15, we omit the details here. This proves the upper bound for $s_{\leq p^n+\ell}(G)$.

Note that when $\ell = 0$, by Lemma 4.3.7, Lemma 4.3.8 and by the above upper bound, we get

$$s_{\leq p^n}(G) = \eta(G) = p^n + 2(D(H) - 1).$$

Now, we shall assume that $G \cong C_{p^m} \oplus C_{p^n}$ with $n \geq m+1$. Then $H = C_{p^m}$ and $D(H)-1 = p^m-1$. Hence $t = p^m-1$ and $0 \leq \ell \leq t = p^m-1$. In order to prove the lower bound for $s_{\leq \exp(G)+\ell}(C_{p^m} \oplus C_{p^n})$, we consider the following sequence

$$S = (0,e)^{p^n-1}(f,0)^{p^m-1}(f,e)^{p^m-1-\ell}$$

over $G \cong C_{p^m} \oplus C_{p^n}$ of length $p^n + 2(p^m-1) - \ell = \exp(G) + 2(D(H)-1) - \ell$, where e is a generator of C_{p^n} and f is a generator of C_{p^m}. If T is a zero-sum subsequence of S of length $\leq p^n + \ell$, then

$$T = (0,e)^a(f,0)^b(f,e)^c$$

for some non-negative integers a, b and c. Since $p^n \geq pp^m$ with $p \geq 5$ and T is a zero-sum sequence, we see that $a + c = p^n$ and $b + c = p^m$. Therefore, $a + 2c + b = p^n + p^m$. Since $|T| = a + b + c = p^n + z$ where $z \leq \ell$, then we get $c = p^m - z \geq p^m - \ell$, which is a contradiction to the fact that $c \leq p^m - 1 - \ell$. Therefore, $N^b(S) = 0$ for all integers $0 \leq b \leq p^n + \ell$. This proves the lower bound. □

Bibliography

[1] K. Adamczewski and E. Treviño, *The smoothed Pólya-Vinogradov inequality*, Integers, **15** (2015), A20.

[2] W. R. Alford, A. Granville and C. Pomerance, *There are infinitely many Carmichael numbers,* Ann. of Math., **139** (1994), 703-722.

[3] Anand, J. Chattopadhyay and B. Roy, *On sums of polynomial-type exceptional Units in* $\mathbb{Z}/n\mathbb{Z}$., Arch. Math. (Basel), **114** (2020), 271–283.

[4] T. M. Apostol, *Introduction to Analytic Number Theory*, Undergraduate Texts in Mathematics, Springer-Verlag, New York-Heidelberg (1976).

[5] J. Chattopadhyay, B. Roy, S. Sarkar and R. Thangadurai, *Quadratic nonresidues and nonprimitive roots satisfying a coprimality conditio,* Bull. Aust. Math. Soc., **99** (2019), 177-183.

[6] R. Chi, S. Y. Ding, W. D. Gao, A. Geroldinger and W. A. Schmid, *On zero-sum subsequences of restricted size IV*, Acta Math. Hung., **107** (2005), 337-344.

[7] M. N. Chintamani, B. K. Moriya, W. D. Gao, P. Paul and R. Thangadurai, *New upper bounds for the Davenport and for the Erdös-Ginzburg-Ziv constants,* Arch. Math. (Basel), **98** (2012), 133-142.

[8] M. N. Chintamani, P. Paul and R. Thangadurai, *On short zero-sum sequences over abelian p-groups*, Integers, **17** (2017), A50.

[9] P. L. Clark, P. Corn, A. Rice and J. Stankewicz, *Computation on elliptic curves with complex multiplication,* LMS J. Comput. Math., **17** (2014), 509-535.

[10] H. B. Daniels and E. González-Jiménez, *On the torsion of rational elliptic curves over sextic fields,* Math. Comp., **89** (2020), 411-435.

[11] C. Delorme, O. Ordaz and D. Quiroz, *Some remarks on Davenport constant*, Discrete Math., **237** (2001), 119-128.

[12] P. K. Dey, *Torsion groups of a family of elliptic curves over number fields,* Czechoslovak Math. J., **69** (2019), 161-171.

[13] P. K. Dey, *Elliptic curves with rank* 0 *over number fields,* Funct. Approx. Comment. Math., **56** (2017), 25-37.

[14] P. K. Dey and B. Roy, *Torsion groups of Mordell curves over cubic and sextic fields,* arXiv:1908.07791 (2019).

[15] D. Dolžan, *The sums of exceptional units in a finite ring*, Arch. Math. (Basel), **112** (2019), 581-586.

[16] Y. Edel, C. Elsholtz, A. Geroldinger, S. Kubertin and L. Rackham, *Zero-sum problems in finite Abelian groups and affine gaps*, Quarterly J. Math., Oxford II. Ser., **58** (2007), 159-186.

[17] C. Elsholtz, *Lower bounds for multidimensional zero sums*, Combinatorica, **24** (2004), 351-358.

[18] P. van Embde Boas, *A combinatorial problem on finite abelian groups II,* Reports of the Mathmatisch Centrum Amsterdam, ZW-1969-007.

[19] Y. S. Fan, W. D. Gao, G. Q. Wang, Q. H. Zhong and J. J. Zhuang, *On short zero-sum subsequences of zero-sum sequences*, Electronic J. Combinatorics, **19** (2012).

[20] Y. S. Fan, W. D. Gao and Q. H. Zhong, *On the Erdős-Ginzburg-Ziv constant of finite Abelian groups of high rank*, J. Number Theory, **131** (2011), 1864-1874.

[21] Y. S. Fan, W. D. Gao, L. L. Wang and Q. H. Zhong, *Two zero-sum invariants on finite Abelian groups*, European J. Combinatorics, **34** (2013), 1331-1337.

[22] M. Freeze and W. Schmid, *Remarks on a generalization of the Davenport constant*, Discrete Math., **310** (2010), 3373-3389.

[23] E. Fromm and L. Goldmakher, *Improving the Burgess bound via Pólya-Vinogradov,* Proc. Amer. Math. Soc., **147** (2019), 461-466.

[24] D. A. Frolenkov and K. Soundararajan, *A generalization of the Pólya-Vinogradov inequality,* Ramanujan J., **31** (2013), 271-279.

[25] W. D. Gao, *On Davenport's constant of finite Abelian groups with rank three,* Discrete Math., **222** (2000), 111-124.

[26] W. D. Gao and A. Geroldinger, *Zero-sum problems and coverings by proper cosets,* European J. Combin., **24** (2003), 531-549.

[27] W. D. Gao and A. Geroldinger, *Zero-sum problems in abelian groups; A survey*, Expo. Math., **24** (2006), 337-369.

[28] W. D. Gao, D. Han and H. Zhang, *The EGZ-constant and short zero-sum sequences over finite abelian groups*, J. Number Theory, **162** (2016), 601-613.

[29] W. D. Gao, Q. H. Hou, W. A. Schmid and R. Thangadurai, *On short zero-sum subsequences. II,* Integers, **7** (2007), A21.

[30] W. D. Gao and R. Thangadurai, *On zero-sum sequences of prescribed length*, Aequationes Math., **72** (2006), 201-212.

[31] A. Geroldinger, D. J. Grynkiewicz and W. A. Schmid, *Zero-sum problems with congruence conditions*, Acta Math. Hungar., **131** (2011), 323-345.

[32] A. Geroldinger and F. Halter-Koch, *Non-unique factorizations, Algebraic, Combinatorial and Analytic Theory, Pure and Applied Mathematics,* Chapman & Hall/CRC, **278** (2006).

[33] A. Geroldinger and R. Schneider, *On Davenport's constant,* J. Combin. Theory Ser. A, **61** (1992), 147-152.

[34] B. Girard, *An asymptotically tight bound for the Davenport constant,*. J. Éc. polytech. Math., **5** (2018), 605-611.

[35] B. Girard and W. A. Schmid, *Direct zero-sum problems for certain groups of rank three,* J. Number Theory, **197** (2019), 297-316

[36] B. Girard and W. A. Schmid, *Inverse zero-sum problems for certain groups of rank three,* arXiv:1809.03178 (2018).

[37] E. González-Jiménez, *Complete classification of the torsion structures of rational elliptic curves over quintic number fields,* J. Algebra, **478** (2017), 484-505.

[38] E. González-Jiménez and F. Najman, *Growth of torsion groups of elliptic curves upon base change,* arXiv:1609.02515v6 (2019).

[39] E. González-Jiménez and J. M. Tornero, *Torsion of rational elliptic curves over quadratic fields,* Rev. R. Acad. Cienc. Exactas Fís. Nat. Ser. A Mat. RACSAM, **108** (2014), 923-934.

[40] S. Gun, F. Luca, P. Rath, B. Sahu and R. Thangadurai, *Distribution of residues modulo p*, Acta Arith., **129** (2007), 325-333.

[41] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, Sixth edition. Revised by D. R. Heath-Brown and J. H. Silverman. With a foreword by Andrew Wiles. Oxford University Press, Oxford, (2008).

[42] J. Houriet, *Exceptional units and Euclidean number fields*, Arch. Math., **88** (2007), 425-433.

[43] T. Jarso and T. Trudgian, *Quadratic non-residues that are not primitive roots*, Math. Comp., **88** (2019), 1251-1260 .

[44] 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.

[45] D. Jeon, C. H. Kim and A. Schweizer, *On the torsion of elliptic curves over cubic number fields,* Acta Arith., **113** (2004), 291-301.

[46] S. Kamienny, *Torsion points on elliptic curves and q-coefficients of modular forms,* Invent. Math., **109** (1992), 221-229.

[47] A. Kemnitz, *On a lattice point problem*, Ars. Combin., **16b** (1983), 151-160.

[48] M. A. Kenku and F. Momose, *Torsion points on elliptic curves defined over quadratic fields,* Nagoya Math. J., **109** (1988), 125-149.

[49] A. W. Knapp, *Elliptic Curves,* Mathematical Notes, Vol. 40, Princeton Univ. Press, Princeton, (1992).

[50] M. L. Knox, T. McDonald and P. Mitchell, *Evaluationally relatively prime polynomials*, Notes on Number Theory and Discrete Mathematics, **21** (2015), 36-41.

[51] D. S. Kubert, *Universal bounds on the torsion of elliptic curves,* Proc. Lond. Math. Soc., **33** (1976), 193-237.

[52] S. Lang, *Algebraic number theory. Second edition. Graduate Texts in Mathematics*, 110. Springer-Verlag, New York, (1994).

[53] H. W. Lenstra, *Euclidean number fields of large degree*, Invent. Math., **38** (1977), 237-254.

[54] M. Levin, C. Pomerance and K. Soundararajan, *Fixed points for discrete logarithms*, Lecture Notes in Comput. Sci., **6197** (2010), 6-15.

[55] C. Liu, *On the lower bound of Davenport constant*, arXiv:1810.08346 (2018).

[56] S. R. Louboutin, *Non-Galois cubic number fields with exceptional units*, Publ. Math. Debrecen, **91** (2017), 153-170.

[57] F. Luca, I. E. Shparlinski and R. Thangadurai, *Quadratic non-residue verses primitive roots modulo p*, J. Ramanujan Math. Soc., **23** (2008), 97-104.

[58] F. E. A. Lucas, *Sur les congruences des nombres eulériens et les coefficients différentiels des functions trigonométriques suivant un module premier (French)*, Bull. Soc. Math. France, **6** (1878), 49-54.

[59] A. P. Mangerel, *Short Character Sums and the Pólya-Vinogradov Inequality,* arXiv:1905.09238 (2019).

[60] B. Mazur, *Modular curves and the Eisenstein ideal,* Inst. Hautes Études Sci. Publ. Math., **47** (1977), 33-186.

[61] L. Merel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres,* Invent. Math, **124** (1996), 437-449.

[62] R. Meshulam, *An uncertainty inequality and zero subsums,* Discrete Math, **84** (1990), 197-200.

[63] C. Miguel, *On the sumsets of exceptional units in a finite commutative ring*, Monatsh. Math., **186** (2018), 315-320.

[64] C. Miguel, *Sums of exceptional units in finite commutative rings*, Acta Arith., **188** (2019), 317-324.

[65] L. Moser, *On the equation* $\phi(n) = \pi(n)$, Pi Mu Epsilon J. **1** (1951), 101-110.

[66] M. R. Murty, *Problems in analytic number theory.* Graduate Texts in Mathematics, **206**, Readings in Mathematics. Springer-Verlag, New York, (2001).

[67] T. Nagell, *Sur un type particulier d'unités algébriques*, Ark. Mat., **8** (1969) 163-184.

[68] F. Najman, *Torsion of rational elliptic curves over cubic fields and sporadic points on $X_1(n)$,* Math. Res. Letters, **23** (2016), 245-272.

[69] W. Narkiewicz and J. Sliwa, *Finite Abelian groups and factorization problems, II,* Colloq. Math., **46** (1982), 115-122.

[70] G. Niklasch, *Counting exceptional units,* Journés Arithmétiques, Barcelona, (1995), Collect. Math. **48** (1997), 195-207.

[71] G. Niklasch and N.P. Smart, *Exceptional units in a family of quartic number fields*, Math. Comp., **67** (1998), 759-772.

[72] I. Niven, H. S. Zuckerman and H. L. Montgomery, *An introduction to the theory of numbers,* Fifth edition, John Wiley & Sons,, New York, (1991).

[73] L. D. Olson, *Points of finite order on elliptic curves with complex multiplication,* Manuscripta math., **14** (1974), 195-205.

[74] J. E. Olson, *A combinatorial problem on finite Abelian groups I*, J. Number Theory, **1** (1969), 8-10.

[75] J. E. Olson, *A combinatorial problem on finite Abelian groups II*, J. Number Theory, **1** (1969), 195-199.

[76] O. Ore, *The general Chinese remainder theorem*, Amer. Math. Monthly, **59** (1952), 365-370.

[77] C. Pomerance, *Remarks on the Pólya-Vinogradov inequality*, Integers, **11** (2011), 531-542.

[78] D. Poulakis, *Integer points on algebraic curves with exceptional units*, J. Austral. Math. Soc. Ser. A, **63** (1997), 145-164.

[79] P. Rath, K. Srilakshmi and R. Thangadurai, *On Davenport's constant,* Int. J. Number Theory, **4** (2008), 107-115.

[80] C. Reiher, *On Kemnitz' conjecture concerning lattice points in the plane*, Ramanujan J., **13** (2007), 333-337.

[81] K. Rogers, *A Combinatorial problem in Abelian groups,* Proc. Cambridge Phil. Soc., **59** (1963), 559-562.

[82] B. Roy and R. Thangadurai, *On zero-sum subsequences in a finite abelian p-group of length not exceeding a given number,* J. Number Theory, **191** (2018), 246-257.

[83] J.W. Sander, *Sums of exceptional units in residue class rings*, J. Number Theory, **159** (2016), 1-6.

[84] J. Sándor, D. S. Mitrinović and B. Crstici, *Handbook on Number Theory I*, Second printing of the 1996 original. Springer, Dordrecht, (2006).

[85] C. Sanna, *A new elementary proof of the inequality* $\phi(n) > \pi(n)$, Notes on Number Theory and Discrete Mathematics, **18** (2012), 35-37.

[86] W. A. Schmid and J. J. Zhuang, *On short zero-sum subsequences over p-groups*, Ars. Combin., **95** (2010), 343 - 352.

[87] J.H. Silverman, *Exceptional units and numbers of small Mahler measure*, Exp. Math., **4** (1995), 69-83.

[88] J.H. Silverman, *Small Salem numbers, exceptional units, and Lehmer's conjecture*, Rocky Mountain J. Math., **26** (1996), 1099-1114.

[89] J. H. Silverman, *The arithmetic of elliptic curves,* Springer-Verlag, Graduate text in Mathematics, **106**, New York, (1992).

[90] M. Szalay, *On the distribution of the primitive roots mod p*, Mat. Lapok, **21** (1970), 357-362.

[91] R. Thangadurai, *Interplay between four conjectures on certain zero-sum problems*, Expo. Math., **20** (2002), 215-228.

[92] C. Wang and K. Zhao, *On zero-sum subsequences of length not exceeding a given number*, J. Number Theory, **176** (2017), 365-374.

[93] L. C. Washington, *Elliptic curves. Number theory and cryptography,* Second edition. Discrete Mathematics and its Applications (Boca Raton). Chapman and Hall/CRC, Florida, (2008).

[94] L. C. Washington, *Introduction to cyclotomic fields*, Second edition, **83**, Graduate Texts in Mathematics, Springer-Verlag, New York, (1997).

[95] G. Xu, *On solving a generalized Chinese remainder theorem in the presence of remainder errors, Geometry, algebra, number theory, and their information technology applications*, Springer Proc. Math. Stat., **251** (2018), 461-476.

[96] Q. H. Yang and Q. Q. Zhao, *On the sumsets of exceptional units in* $\mathbb{Z}_n$*,* Monatsh. Math., **182** (2017), 489-493.