

# **GALOIS GROUP OF CERTAIN ALGEBRAIC EXTENSIONS AND THEIR RELATIONS WITH PRIMES IN ARITHMETIC PROGRESSION**

Thesis

Submitted in partial fulfillment of the requirements for the degree of

**DOCTOR OF PHILOSOPHY**

by

SEHRA SAHU



DEPARTMENT OF MATHEMATICAL AND COMPUTATIONAL SCIENCES

NATIONAL INSTITUTE OF TECHNOLOGY KARNATAKA,

SURATHKAL, MANGALORE - 575 025

APRIL 2023



Dedicated to

***My family***

*who have been a constant source of support and encouragement throughout my life*



## DECLARATION

*By the Ph.D. Research Scholar*

I hereby declare that the Research Thesis entitled **GALOIS GROUP OF CERTAIN ALGEBRAIC EXTENSIONS AND THEIR RELATIONS WITH PRIMES IN ARITHMETIC PROGRESSION** which is being submitted to the **National Institute of Technology Karnataka, Surathkal** in partial fulfillment of the requirements for the award of the Degree of **Doctor of Philosophy in Mathematical and Computational Sciences** is a *bonafide report of the research work carried out by me*. The material contained in this Research Thesis has not been submitted to any University or Institution for the award of any degree.

*Sehra Sahu*  
25/08/2023  
(SEHRA SAHU)

Reg. No: 177081MA004

Department of Mathematical and Computational Sciences

Place: NITK, Surathkal.

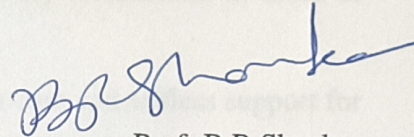
Date: 11/04/2023



ACKNOWLEDGEMENT

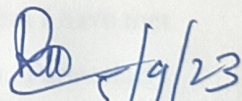
**CERTIFICATE**

This is to *certify* that the Research Thesis entitled **GALOIS GROUP OF CERTAIN ALGEBRAIC EXTENSIONS AND THEIR RELATIONS WITH PRIMES IN ARITHMETIC PROGRESSION** submitted by Ms. **SEHRA SAHU**, (Register Number: 177081MA004) as the record of the research work carried out by her is *accepted as the Research Thesis submission* in partial fulfillment of the requirements for the award of degree of **Doctor of Philosophy**.



Prof. B R Shankar

Research Supervisor



Chairman - DRPC

(Signature with Date and Seal)

Chairman  
DUGC / DPGC / DRPC  
Dept. of Mathematical and Computational Sciences  
National Institute of Technology Karnataka, Surathkal  
MANGALORE - 575 025





# ACKNOWLEDGEMENT

First and foremost, I am grateful to my advisor Prof B R Shankar, for his constant and unbiased support, patience, guidance and freedom to choose the area of research. Also, I thank my RPAC members from NITK, Dr V Murugan, Department of MACS and Dr Prashantha Kumar H, Department of ECE, for their comments and suggestions. They have supported the changes in the research work in the course duration.

I enjoyed my collaboration and discussion with Dr Karthick Babu, and I am obliged to him for his patience and work with me. I am grateful to Prof Pieter Moree for his valuable suggestions, which gave a good shape to one of my manuscripts. I am also grateful to Prof Balasubramanian, who mentored me via my collaborator in times of need.

I would like to thank my parents and siblings for their care and selfless support for whatever I chose to do in my life. I especially count on my mother for all she could and gave for a progressive living. I am thankful to all my teachers from primary school to college, who have propagated me to reach this stage. I am also grateful to my MSc lecturers, Dr G Janardhana Reddy and Dr Venkatrajam Marka, for their fair play in influencing me to choose a research career in Mathematics.

I extend my heartfelt thanks to my friends, colleagues and people whom I have met in certain workshops with whom I have had mathematical conversations. Particularly T P Thrivikram, Sumukha S, T Natarajan, Pooja Raut and Kummari Mallesham. I also want to mention Pranamyia, Venkatramana, Mahesh, Chaitanya G K, Palanivel, Saumya, Athira, Sundari, Revathy, Megha, Rashid, Amal, Sachin, Shashanka, Sai Prasanna, Bharadwaj, Saeed and many others, with whom I could discuss and learn academic stuff as well as distract myself from the monotony of life.

I also thank the department staff, Dr Vishwanath K P, Dr Sam Johnson and Prof Santosh George, for their insightful words and actions. This acknowledgement will remain incomplete for a crowd of people who have directly or indirectly made me a better person academically and otherwise. I thank the institute for a fantastic experience during the stay provided concerning the department, hostel, sports, security, and activities



meant for physical and mental fitness. The Department of MACS at NITK has provided the perfect environment to create this thesis.

Place: NITK, Surathkal

SEHRA SAHU

Date: 11/04/2023



# ABSTRACT

Explicit structure of Galois group of  $\mathbb{Q}(\sqrt{a_1}, \sqrt{a_2}, \dots, \sqrt{a_n})$  over  $\mathbb{Q}$  was calculated by Karthick Babu and Anirban Mukhopadhyay. Expanding this knowledge, the problem of finding an explicit Galois group of the field extension  $\mathbb{Q}(\sqrt{a_1}, \sqrt{a_2}, \dots, \sqrt{a_n}, \zeta_d)$  over  $\mathbb{Q}$  in terms of its action on  $\zeta_d$  and  $\sqrt{a_i}$  for  $1 \leq i \leq n$  has been studied.

Let  $p$  be an odd prime. If we have an integer  $g$  which generates a subgroup of index  $t$  in  $(\mathbb{Z}/p\mathbb{Z})^*$ , then we call  $g$  to be a  $t$ -near primitive root modulo  $p$ . Pieter Moree and Min Sha showed that each coprime residue class contains a positive density of primes  $p$  not having  $g$  as a  $t$ -near primitive root. In this note, for a subset  $\{a_1, a_2, \dots, a_n\}$  of  $\mathbb{Z} \setminus \{0\}$ , we shall prove that each such coprime residue class contains a positive density of primes  $p$  such that  $a_i$  is not a  $t$ -near primitive root. Additionally,  $a_i$ 's satisfy certain residue pattern modulo  $p$ , for  $1 \leq i \leq n$ .

*Keywords: Galois Group, Multi-Quadratic Extension, Cyclotomic Extension, Residue Pattern, Natural Density*



# Contents

Abstract of the Thesis . . . . .	i
<b>1 INTRODUCTION</b>	<b>1</b>
1.1 Number Fields . . . . .	2
1.2 Primes in Arithmetic Progression . . . . .	2
1.3 Galois Group . . . . .	2
1.4 Frobenius element . . . . .	3
<b>2 A counting problem with respect to primes in Arithmetic Progression</b>	<b>5</b>
2.1 Notations and Definitions . . . . .	5
2.2 Proof of Theorem 2.1.1 . . . . .	8
2.2.1 Arithmetic Lemmas . . . . .	8
2.3 Some Combinatorial Lemmas and Corollaries of Theorem 2.1.1 . . . . .	14
2.3.1 Some Corollaries of Theorem 2.1.1 . . . . .	20
2.4 A counting problem arising from Theorem 2.1.1 . . . . .	23
2.4.1 Notations . . . . .	24
<b>3 Explicit Galois group of <math>\mathbb{Q}(\sqrt{a_1}, \dots, \sqrt{a_n}, \zeta_d)</math> over <math>\mathbb{Q}</math></b>	<b>29</b>
3.1 The degree of $\mathbb{Q}(\sqrt{a_1}, \sqrt{a_2}, \dots, \sqrt{a_n}, \zeta_d)$ over $\mathbb{Q}$ . . . . .	29
3.2 The explicit Galois group of $\mathbb{Q}(\sqrt{a_1}, \sqrt{a_2}, \dots, \sqrt{a_n}, \zeta_d)$ over $\mathbb{Q}$ . . . . .	31
<b>4 Non-primitive roots with prescribed residue pattern</b>	<b>35</b>
4.1 Preliminary lemmas . . . . .	37
4.2 A positive density subset of $\mathcal{Q}_S(t, d, f, \theta)$ . . . . .	42
4.3 A positive density subset of $\mathcal{R}_S(t, d, f, \theta)$ . . . . .	44
<b>5 Conclusions and Future Scope</b>	<b>49</b>

**PUBLICATIONS** . . . . . 59





# Chapter 1

## INTRODUCTION

Chaos is the fundamental nature of existence. The distribution of primes is as such chaotic. Chaos Theory talks about a dynamic system where the slightest of change in the initial conditions in any non-linear system leads to unpredictable changes in the further stages. The current active research in this theory is about finding patterns in the variations of the system with respect to changes made in the initial conditions. Though the distribution of primes is not about dynamics, mathematicians tend to find patterns in this chaotic distribution to unravel the mystery of primes.

The notion of primes itself is naturally appealing. Evidently, primes are the building blocks of the entire number system. Starting from Gauss to the present generation number theorists, the distribution of primes has intrigued them. The beauty of seeing patterns in nature, especially symmetries, is another deep area of observation and research called Group Theory. Évariste Galois had observed a crucial interplay between the Groups and Fields.

One of the main applications of Number Theory in today's world is Cryptography. To have a direct application based research in this area, there are predominantly four tasks postulated by Zassenhaus (1987), a pioneer of computer algebra. These include computation of the ring of integers, the unit group, the Galois group and the ideal class group of a number field. There have been approaches in analytical, algebraic, algorithmic, elementary and several other ways to tackle these problems.

## 1.1 Number Fields

Any field which is a finite degree field extension of the field of rationals,  $\mathbb{Q}$ , is called a number field. Hence number fields are always algebraic extensions. Here degree means the dimension of the given field as a vector space over  $\mathbb{Q}$ . Evidently, number fields are of characteristic 0. This thesis deals with quadratic fields and their cyclotomic extensions.

## 1.2 Primes in Arithmetic Progression

The Dirichlet prime number theorem states that for any  $n \in \mathbb{N}$  and integer  $a$  such that  $\gcd(a, n) = 1$ , there exist infinitely many primes  $p$  such that  $p \equiv a \pmod{n}$ . For the case  $n = 1$ , the proof is attributed to Euclid.

Let  $p$  be an odd prime. If we have an integer  $g$  which generates an index  $t$  subgroup of  $(\mathbb{Z}/p\mathbb{Z})^*$ , then we call  $g$  to be a  $t$ -near primitive root modulo  $p$ . Using the notations of Moree and Sha (2019), for any integer  $t \geq 1$  and coprime integers  $f, d \geq 1$ , we write

$$\mathcal{P}_g(t) = \{p : p \equiv 1 \pmod{t}, p \nmid g, \text{ord}_p(g) = (p-1)/t\},$$
$$\mathcal{P}_g(t, d, f) = \{p : p \equiv f \pmod{d}, p \in \mathcal{P}_g(t)\}.$$

Further, Moree and Sha (2019) defined

$$\mathcal{Q}_g(t, d, f) = \{p : p \equiv f \pmod{d}, \text{ord}_p(g) \neq (p-1)/t\},$$
$$\mathcal{R}_g(t, d, f) = \{p : p \nmid g, p \equiv f \pmod{d}, p \equiv 1 \pmod{t} \text{ and } \text{ord}_p(g) \mid (p-1)/t\}.$$

In this thesis, we consider the generalization of the above sets as we replace the element  $g$  with a set  $S$ .

## 1.3 Galois Group

For a field extension  $E$  over  $F$ , the set of all automorphisms of  $E$  that fix  $F$  forms a group  $G$ . If this extension is Galois, this group is called the Galois group of  $E$  over  $F$ . Mathematically,

$$G = \text{Gal}(E/F) = \text{Aut}(E/F) = \{\sigma \in \text{Aut}(E) \mid \sigma(x) = x, \forall x \in F\}.$$

One can identify the algebraic structure of the field extension by studying this Galois

group. The Galois correspondence which establishes a correspondence between subfields of a Galois extension  $E$  over  $F$  and subgroups of  $\text{Gal}(E/F)$  is a powerful tool which can be applied to diverse areas of Mathematics.

## 1.4 Frobenius element

Ferdinand Georg Frobenius, a German mathematician, found a way to look at the primes,  $p$ , in Galois groups over  $\mathbb{Q}$  in the form of conjugacy classes.  $A$  is a Dedekind domain with fraction field  $K$ , and  $L/K$  is a finite separable extension of its fraction field (and  $B$  is the integral closure of  $A$  in  $L$ , also a Dedekind domain). We now consider the case where  $L/K$  is also normal, hence Galois, and let  $G := \text{Gal}(L/K)$ .

Let  $E/\mathbb{Q}$  be a finite Galois extension. When  $\wp$  is a prime lying over an unramified prime  $p$ , then there is a unique element  $\sigma \in \text{Gal}(E/\mathbb{Q})$  with the property

$$\sigma.x = x^p \pmod{\wp}, \forall x \in O_E,$$

which is called the Frobenius element where  $O_E$  is the ring of integers of  $E$ . Varying  $\wp$  over  $p$  changes  $\sigma$  to its conjugate. This collection of conjugates is called the Frobenius conjugacy class. The cardinality of this class is used to find the density of unramified primes satisfying the Frobenius condition as given above. This concept is encoded in the Chebotarev Density Theorem.

Moree and Sha (2019) showed that for any integer  $q > 2$  such that  $(q, 2dt) = 1$ , the set  $\mathcal{Q}_g(t, d, f)$  contains infinitely many primes  $p$  with natural density (over the set of primes)  $\frac{1}{[\mathbb{Q}(\zeta_d, \zeta_q, g^{1/q}) : \mathbb{Q}]}$ . Further, if the set  $\mathcal{R}_g(t, d, f)$  is nonempty, then they showed that for any integer  $q > 2$  such that  $(q, 2gdt) = 1$ , the set  $\mathcal{R}_g(t, d, f)$  contains infinitely many primes  $p$  for which  $g$  ceases to be a  $t$ -near primitive root modulo  $p$  with natural density  $\frac{1}{[\mathbb{Q}(\zeta_d, \zeta_{qt}, g^{1/qt}) : \mathbb{Q}]}$ . This thesis discusses generalizing their results to the set  $S = \{a_1, \dots, a_n\} \subset \mathbb{Z} \setminus \{-1, 0, 1\}$ .

There has been progress in developing multi-quadratic and cyclotomic extensions as separate field extensions over  $\mathbb{Q}$ . This thesis details the progress towards calculating the explicit structure of the Galois group of  $\mathbb{Q}(\sqrt{a_1}, \sqrt{a_2}, \dots, \sqrt{a_n}, \zeta_d)$  over  $\mathbb{Q}$ . This is

obtained in terms of its action on the cyclotomic part,  $\zeta_d$ , and the quadratic part,  $\sqrt{a_i}$ , for  $1 \leq i \leq n$ .

In the other portions, we find the density of primes in arithmetic progression involving certain conditions. The original idea proposed by Moree and Sha (2019) have shown the some application to *Genocchi numbers*,  $G_n = 2(1 - 2^n)B_n$ , where  $B_n$  is the  $n$ th Bernoulli number. If a prime  $p > 3$  divides at least one of the Genocchi numbers  $G_2, G_4, \dots, G_{p-3}$ , it is said to be  $G$ -irregular and  $G$ -regular otherwise. The  $G$ -regularity of primes can be linked to the divisibility of certain class numbers of cyclotomic fields.

## Chapter 2

# A counting problem with respect to primes in Arithmetic Progression

Prime numbers, though, have chaotic distribution; when we see the infinitude of primes under a particular sieve, there is more to explore. We can find the corresponding Dedekind zeta function and its analytical properties for the number fields we are dealing with. Though not discussed in this thesis, these are active areas of research.

### 2.1 Notations and Definitions

Some notations used majorly in chapters 2 and 3 are mentioned here. The definitions will be recalled at the required places as and when needed.

We shall use the letter  $p$  for an odd prime number. Also,  $\left(\frac{\cdot}{p}\right)$  represents the Jacobi symbol.

1. Let  $f$  be a real/complex valued function and  $g$  be a real valued function for comparison. If  $f$  is defined on some unbounded subset of positive reals, and  $g$  be strictly positive for large enough values of reals, then  $f = O(g)$  implies the claim that the inequality  $|f| \leq cg$  holds for some constant  $c > 0$ .
2. The Euler phi function is denoted by  $\varphi(n)$ .
3. A function  $\theta : S \rightarrow \{-1, 1\}$  denotes a choice of signs for  $S$ .
4.  $\mathcal{H} = \mathcal{H}(S) = \{T \subseteq S : \prod_{s \in T} s = \square\}$ , where  $\square$  denotes any perfect square.

5. If  $\left(\frac{s}{p}\right) = \theta(s)$ ,  $\forall s \in S$ , then we say that  $S$  has residue pattern  $\theta$  modulo  $p$ , where  $\left(\frac{\cdot}{p}\right)$  is the Jacobi symbol mod  $p$ .
6. Squarefree part for any  $n \in \mathbb{Z} \setminus \{0\}$ ,  $n = \prod_{i=1}^m p_i^{k_i}$  is given by  $\text{sqf}(n) = \prod_{i=1}^m p_i^{r_i}$ , where  $r_i \in \{0, 1\}$  such that  $k_i \equiv r_i \pmod{2}$ .
7. For  $T \subseteq S$ , we have  $\theta(T) := \prod_{s \in T} \theta(s)$ .
8.  $S(n, \theta) = \{p \in P : n < p \leq 2n \text{ such that } S \text{ satisfies the residue pattern } \theta \pmod{p}\}$ . Here  $P$  denotes the set of all primes.
9.  $|A|$  denotes the cardinality of the set  $A$ .
10.  $(p, B) = 1$  for a set  $B \implies (p, b) = 1 \forall b \in B$ .
11. The symmetric difference between sets  $A$  and  $B$  is represented by the symbol  $A \Delta B$  and  $A \setminus B$  denotes the set difference between  $A$  and  $B$ .
12. Given a set of primes  $S$ , if the limit
$$\delta(S) = \lim_{x \rightarrow \infty} \frac{|\{p \leq x : p \in S\}|}{|\{p \leq x\}|}$$
exists, then  $\delta(S)$  is called the natural density of  $S$ .

Let  $S = \{a_1, a_2, \dots, a_n\}$  be a finite subset of non-zero integers. Fried (1968) showed the existence of infinitely many primes  $p$  for which every element of the set  $S$  will be a quadratic residue. Additionally, he provided a criterion for  $a_i$ 's to be quadratic non-residues modulo  $p$ . The precise density of primes in Fried's result was computed by Balasubramanian et al. (2010) (Theorem 2.3).

Generalising the uniformity of either residues or non-residues among the elements of  $S$ , we deal with the function  $\theta$ , called the **choice of signs** for  $S$ .

Recently, Babu and Mukhopadhyay (2022) calculated the exact density of the collection of primes for which  $S$  has residue pattern  $\theta$  modulo  $p$ . Additionally, a criterion for a choice of signs  $\theta$  for  $S$  to be a residue pattern modulo  $p$  was also obtained for the positive density of primes.

To denote the **squarefree part of**  $n$ , we use the symbol  $\text{sqf}(n)$  for any non-zero integer  $n$ . For any finite subset  $T \subset \mathbb{Z} \setminus \{0\}$ , by  $\text{sqf}(T)$  we mean  $\text{sqf}(\prod_{s \in T} s)$ . Clearly, this function is completely multiplicative.

We shall find the density of primes in  $S(n, \theta)$ , the set of primes,  $p$ , such that  $n < p \leq 2n$  and  $S$  satisfying the residue pattern  $\theta \pmod{p}$ . The closest approach would be to find the asymptotic growth of such primes. Thus, the first result of this thesis is the following:

**Theorem 2.1.1.** *Let  $S$  be a finite subset of non-zero integers having  $\theta$  as a choice of signs for  $S$ . For any coprime integers  $f$  and  $d$  such that  $1 \leq f \leq d \leq (\log n)^A$  and a sufficiently large integer  $n \geq 3$  with  $A > 0$ , we have*

$$\sum_{\substack{p \equiv f \pmod{d} \\ p \in S(n, \theta)}} \log p = \frac{n}{\phi(d)} \cdot \frac{C(S, \theta, d)}{2^{|S|}} + O\left(\frac{n \log n}{\exp(C_1 \sqrt{\log n})}\right),$$

where  $C_1 = C_1(A, S)$ . Here,

$$C(S, \theta, d) = \begin{cases} \sum_{\substack{T \subseteq S \\ \text{sqf}(T) \equiv 1 \pmod{4} \\ |\text{sqf}(T)| \mid d}} \theta(T) \left(\frac{\text{sqf}(T)}{f}\right), & \text{when } 4 \nmid d, \\ \sum_{\substack{T \subseteq S \\ \text{sqf}(T) \equiv 1, 3 \pmod{4} \\ |\text{sqf}(T)| \mid d}} \theta(T) \left(\frac{\text{sqf}(T)}{f}\right), & \text{when } 4 \mid d \text{ \& } 8 \nmid d, \\ \sum_{\substack{T \subseteq S \\ |\text{sqf}(T)| \mid d}} \theta(T) \left(\frac{\text{sqf}(T)}{f}\right), & \text{when } 8 \mid d. \end{cases} \quad (2.1.1)$$

Let  $S = \{-10\}$ ,  $\theta(-10) = -1$ ,  $f = 3$ ,  $d = 8$ ,  $n = 10^6$ . Clearly  $8 \nmid d$ .

$$S(n, \theta) = S(10^6, \theta) = \{p : 10^6 < p \leq 2 \cdot 10^6 \text{ and } \left(\frac{-10}{p}\right) = \theta(-10)\}$$

$$\sum_{\substack{p \equiv 3 \pmod{8} \\ p \in S(10^6, \theta)}} \log p = \frac{10^6}{\phi(8)} \frac{C(\{-10\}, \theta, 8)}{2^{|\{-10\}|}} + O\left(\frac{10^6 \log(10^6)}{\exp(C_1 \sqrt{\log(10^6)})}\right)$$

$$C(\{-10\}, \theta, 8) = 0.$$

Hence,

$$\sum_{\substack{p \equiv 3 \pmod{8} \\ p \in S(10^6, \theta)}} \log p = O\left(\frac{10^6 \cdot 6}{\exp(C_1 \sqrt{6})}\right) \approx O\left(\frac{6 \cdot 10^6}{11.58^{C_1}}\right)$$

Outline of this chapter:

We will discuss the proof of the above Theorem in section 2.2. Analysis of  $C(S, \theta, d)$



will solve a counting problem. In section 2.3, we prove several combinatorial Lemmas, and as an application of those Lemmas, we discuss the positivity of  $C(S, \theta, d)$  in Lemma 2.3.5.

Further, we discuss some Corollaries of the above Theorem in section 2.3. Especially in the Corollary 4.1.8, in order for  $S$  to be a residue pattern modulo  $p$  for an infinite number of primes  $p$  of the type  $p \equiv f \pmod{d}$ , we shall present a necessary and sufficient condition for a choice of signs  $\theta$ .

In section 2.4, we will calculate the number of choice of signs for  $S$  that allow  $S$  to have a residue pattern of  $\theta$  modulo  $p$  for infinitely many primes  $p$  in an arithmetic progression.

## 2.2 Proof of Theorem 2.1.1

### 2.2.1 Arithmetic Lemmas

Recalling some basic results on Dirichlet characters which will be used for quadratic characters.

**Lemma 2.2.1.** *Let  $\chi_1$  and  $\chi_2$  be Dirichlet characters modulo coprime integers  $d_1$  and  $d_2$  respectively. We define  $\chi = \chi_1\chi_2$  as a character modulo  $d$ , where  $d = d_1d_2$ . Then  $\chi$  is principal modulo  $d$  if and only if  $\chi_1, \chi_2$  are principal modulo  $d_1, d_2$  respectively.*

*Proof:* If  $\chi_1$  and  $\chi_2$  are principal characters as given, then it is easy to see that  $\chi$  is principal modulo  $d$ .

Conversely, let  $\chi = \chi_1\chi_2$  be the principal character modulo  $d$ . Then  $\chi_2(n) = \overline{\chi_1}(n)$  holds by definition, if  $(n, d_1d_2) = 1$ . Suppose  $r_2 \neq 1$  is a reduced residue class modulo  $d_2$  such that  $(r_2, d_2) = 1$ . Since  $d_1$  and  $d_2$  are coprime, there exists a positive  $m$  satisfying  $r_2 + md_2 \equiv 1 \pmod{d_1}$ . Therefore, for any  $r_2 < d_2$  and  $(r_2, d_2) = 1$ , we have

$$1 = \overline{\chi_1}(1) = \chi_2(r_2 + md_2) = \chi_2(r_2)$$

Thus  $\chi_2$  is principal modulo  $d_2$ .

In a similar way, we can show that  $\chi_1$  is the principal character modulo  $d_1$ . □

**Remark 2.2.2.** *If  $(d_1, d_2) > 2$ , The above Lemma need not hold. For example, consider the non-principal Dirichlet characters  $\chi_6$  and  $\chi_9$  of modulus 6 and modulus 9 respectively, with the character tables as below:*

$n$	0	1	2	3	4	5	6	7	8
$\chi_9(n)$	0	1	-1	0	1	-1	0	1	-1

$n$	0	1	2	3	4	5
$\chi_6(n)$	0	1	0	0	0	-1

The character  $\chi = \chi_6\chi_9$  is principal modulo 18. We can see that both of these characters  $\chi_6$  and  $\chi_9$  are induced by some non-principal character modulo  $(d_1, d_2) = 3$ .

Further, if  $d_1$  and  $d_2$  are not coprime and  $\chi_1\chi_2$  is principal modulo  $[d_1, d_2]$ , then  $\chi_1$  and  $\chi_2$  both are induced by some character modulo  $t$ , where  $t|(d_1, d_2)$ . To prove this, it is enough to show that

$$\chi_2(k) = 1, \text{ for any } k \equiv 1 \pmod{(d_1, d_2)}, \text{ and } (k, d_2) = 1.$$

Since  $k \equiv 1 \pmod{(d_1, d_2)}$  we have  $k = 1 + l(d_1, d_2)$  for some positive integer  $l$ . Also, by the linearity of gcd, there exists  $m \in \mathbb{Z}^+$  which satisfies  $1 + l(d_1, d_2) + md_2 \equiv 1 \pmod{d_1}$ . This implies

$$\chi_2(k) = \chi_2(1 + l(d_1, d_2)) = \chi_2(1 + l(d_1, d_2) + md_2) = \overline{\chi_1}(1) = 1.$$

In a similar way,  $\chi_1$  is also induced by a character modulo  $t$  such that  $t|(d_1, d_2)$ . Since there are no non-principal characters modulo 2, Lemma 2.2.1 holds if we were to assume  $(d_1, d_2) = 2$ .

Corollary of Lemma 2.2.1:

**Corollary 2.2.3.** Let  $\chi_1$  and  $\chi_2$  be two characters modulo  $d_1$  and  $d_2$  respectively such that  $d_1 < d_2$  and  $d_1 \nmid d_2$ . If either  $\chi_1$  or  $\chi_2$  is primitive, then  $\chi_1\chi_2$  cannot be principal character modulo  $[d_1, d_2]$ .

**Remark 2.2.4** (Ch.5, Davenport (2000)). The Kronecker symbol  $\chi_m = \left(\frac{m}{\cdot}\right)$ , for every fundamental discriminant  $m$ , is a primitive quadratic character with conductor  $|m|$ .

Conversely, if  $\chi$  is a primitive quadratic character, a unique fundamental discriminant  $s$  exists so that  $\chi = \chi_s$ . Also, if  $s$  is not a fundamental discriminant, it is possible that  $\chi_s$  be primitive (e.g.,  $\chi_2$ ), nonprimitive (e.g.,  $\chi_4$ ) or not even a character (e.g.,  $\chi_3$ ).

Therefore, we shall make use of the law of reciprocity and convert Kronecker symbol  $\left(\frac{m}{\cdot}\right)$  into Jacobi symbol  $\left(\frac{\cdot}{m}\right)$  in the following lemma. This Jacobi symbol is a Dirichlet character modulo  $m$ .

**Lemma 2.2.5.** Let  $A$  and  $B$  be positive real numbers, and  $n \geq 3$  be a positive integer. Let  $s$  be a squarefree integer  $s \leq \log^B n$  such that  $s \nmid d$ . Then for any positive coprime integers,  $f, d$  satisfying  $1 \leq f \leq d \leq \log^A n$ , there exists  $C = C(A, B) > 0$  such that

$$\sum_{\substack{n < p \leq 2n \\ p \equiv f \pmod{d}}} \left(\frac{s}{p}\right) \ll n \cdot \exp(-C\sqrt{\log n})$$

holds.

*Proof:* Let  $s$  be odd. Then we can analyse the following two cases.

**Case I :** When  $s \equiv 1 \pmod{4}$ . Applying the quadratic reciprocity law, we have

$$\sum_{\substack{p \equiv f \pmod{d} \\ n < p \leq 2n}} \left( \frac{s}{p} \right) = \sum_{\substack{p \equiv f \pmod{d} \\ n < p \leq 2n}} \left( \frac{p}{s} \right) = \frac{1}{\varphi(d)} \sum_{\psi \pmod{d}} \bar{\psi}(f) \sum_{n < p \leq 2n} \left( \frac{p}{s} \right) \psi(p),$$

where the first summation runs across the set of all Dirichlet characters taken modulo  $d$ . Also, since  $s$  is an odd positive squarefree integer, the Jacobi symbol  $\left( \frac{\cdot}{s} \right)$  is primitive, taken modulo  $s$ . By Corollary 2.2.3, as  $s \nmid d$ ,  $\left( \frac{\cdot}{s} \right) \psi$  is a non-principal character modulo  $[d, s]$ . Applying Siegel's Theorem [Ch. 22, Davenport (2000)] we obtain the required result.

**Case II :** When  $s \equiv 3 \pmod{4}$ .

If  $4 \mid d$ , all the primes are of the form  $p \equiv f \pmod{d}$  are of the form 1 or 3  $\pmod{4}$ . Therefore, similar to the above case, we get

$$\sum_{\substack{p \equiv f \pmod{d} \\ n < p \leq 2n}} \left( \frac{s}{p} \right) = \left| \sum_{\substack{p \equiv f \pmod{d} \\ n < p \leq 2n}} \left( \frac{p}{s} \right) \right| \ll n \cdot \exp(-C_1 \sqrt{\log n}).$$

If  $4 \nmid d$ , then by applying the reciprocity law, we have

$$\begin{aligned} \sum_{\substack{p \equiv f \pmod{d} \\ n < p \leq 2n}} \left( \frac{s}{p} \right) &= \sum_{\substack{p \equiv f \pmod{d} \\ n < p \leq 2n \\ p \equiv 1 \pmod{4}}} \left( \frac{p}{s} \right) - \sum_{\substack{p \equiv f \pmod{d} \\ n < p \leq 2n \\ p \equiv 3 \pmod{4}}} \left( \frac{p}{s} \right) \\ &= \frac{1}{2\varphi(d)} \left( \sum_{\psi \pmod{d}} \bar{\psi}(f) \left( \sum_{\chi \pmod{4}} \bar{\chi}(1) \sum_{n < p \leq 2n} \left( \frac{p}{s} \right) \psi(p) \chi(p) \right. \right. \\ &\quad \left. \left. - \sum_{\chi \pmod{4}} \bar{\chi}(3) \sum_{n < p \leq 2n} \left( \frac{p}{s} \right) \psi(p) \chi(p) \right) \right). \end{aligned}$$

By Corollary 2.2.3, as  $4s \nmid d$ ,  $\left( \frac{\cdot}{s} \right) \psi \cdot \chi$  is a non-principal character modulo  $[d, 4s]$ .

Thus applying Siegel's Theorem [Ch. 22, Davenport (2000)] we obtain the required result.

Now, when  $s$  is even, we can write  $s = 2k$  for a squarefree and odd integer  $k$ . Then, we have

$$\sum_{\substack{n < p \leq 2n \\ p \equiv f \pmod{d}}} \left( \frac{s}{p} \right) = \sum_{\substack{n < p \leq 2n \\ p \equiv f \pmod{d} \\ p \equiv \pm 1 \pmod{8}}} \left( \frac{k}{p} \right) - \sum_{\substack{n < p \leq 2n \\ p \equiv f \pmod{d} \\ p \equiv \pm 3 \pmod{8}}} \left( \frac{k}{p} \right). \quad (2.2.1)$$

We use similar arguments as discussed for odd case to estimate the two sums in (2.2.1), from which we obtain the required result in the even case of  $s$ . □

The following Lemma treats the same character sum when  $s$  divides  $d$ ; as expected, we get the main term.

**Lemma 2.2.6.** *Let  $n \geq 3$  be an integer and  $A$  be a positive real number. Then for a squarefree integer  $s$  such that  $s \mid d$ , there exists a positive real constant  $C = C(A)$  such that for positive coprime integers  $f, d$  satisfying  $1 \leq f \leq d \leq \log^A n$ , we have*

$$\sum_{\substack{p \equiv f \pmod{d} \\ n < p \leq 2n}} \left( \frac{s}{p} \right) = \begin{cases} \left( \frac{s}{f} \right) \sum_{\substack{p \equiv f \pmod{d} \\ n < p \leq 2n}} 1 & \text{if } s \equiv 1 \pmod{4}, \\ \left( \frac{s}{f} \right) \sum_{\substack{p \equiv f \pmod{d} \\ n < p \leq 2n}} 1 & \text{if } s \equiv 3 \pmod{4} \text{ and } 4 \mid d, \\ \left( \frac{s}{f} \right) \sum_{\substack{p \equiv f \pmod{d} \\ n < p \leq 2n}} 1 & \text{if } s \equiv 2 \pmod{4} \text{ and } 8 \mid d, \\ O(n \cdot \exp(-C\sqrt{\log n})), & \text{otherwise.} \end{cases}$$

*Proof:* When  $s \equiv 1 \pmod{4}$ . Since  $s \mid d$  and  $p \equiv f \pmod{d}$  implies  $p \equiv f \pmod{s}$ . Applying the law of quadratic reciprocity, we have

$$\sum_{\substack{p \equiv f \pmod{d} \\ n < p \leq 2n}} \left( \frac{s}{p} \right) = \sum_{\substack{p \equiv f \pmod{d} \\ n < p \leq 2n}} \left( \frac{p}{s} \right) = \left( \frac{f}{s} \right) \sum_{\substack{p \equiv f \pmod{d} \\ n < p \leq 2n}} 1 = \left( \frac{s}{f} \right) \sum_{\substack{p \equiv f \pmod{d} \\ n < p \leq 2n}} 1.$$

Now, when  $s \equiv 3 \pmod{4}$ . Suppose  $4 \mid d$  then all primes  $p \equiv f \pmod{d}$  are of the form 1 or 3  $\pmod{4}$ . Since  $s \mid d$  and  $p \equiv f \pmod{d}$  implies  $p \equiv f \pmod{s}$ , applying the law of quadratic reciprocity, we have

$$\sum_{\substack{p \equiv f \pmod{d} \\ n < p \leq 2n}} \left(\frac{s}{p}\right) = \sum_{\substack{p \equiv f \pmod{d} \\ n < p \leq 2n}} (-1)^{\frac{p-1}{2}} \left(\frac{p}{s}\right) = \left(\frac{f}{s}\right) \sum_{\substack{p \equiv f \pmod{d} \\ n < p \leq 2n}} (-1)^{\frac{f-1}{2}} = \left(\frac{s}{f}\right) \sum_{\substack{p \equiv f \pmod{d} \\ n < p \leq 2n}} 1.$$

If  $4 \nmid d$ , we use similar arguments as in Lemma 2.2.5 to obtain the required result. The proof again makes use the Reciprocity law and Siegel's Theorem as in the above case when  $s \equiv 2 \pmod{4}$ . Thus, we omit the proof. □

### The Proof of Theorem 2.1.1:

Since  $S(n, \theta)$  is the set of primes,  $p$ , such that  $n < p \leq 2n$  and  $S$  satisfies the residue pattern  $\theta \pmod{p}$ , by the definition of the Legendre symbol, we can write

$$\sum_{\substack{p \in S(n, \theta) \\ p \equiv f \pmod{d}}} \log p = \frac{1}{2^{|S|}} \sum_{\substack{n < p \leq 2n \\ (p, S) = 1 \\ p \equiv f \pmod{d}}} \log p \prod_{s \in S} \left(1 + \theta(s) \left(\frac{s}{p}\right)\right).$$

For sufficiently large values of  $n$ , the condition  $(p, S) = 1$  can be skipped as we can consider  $(\log n)^B > \prod_{s \in S} s$  for some  $B > 0$ .

We write

$$\prod_{s \in S} \left(1 + \theta(s) \left(\frac{s}{p}\right)\right) = 1 + \sum_{\phi \neq T \subseteq S} \prod_{s \in T} \theta(s) \left(\frac{s}{p}\right) = 1 + \sum_{T \in \mathcal{H}^*} \theta(T) + \sum_{\substack{T \subseteq S \\ T \notin \mathcal{H}}} \theta(T) \prod_{s \in T} \left(\frac{s}{p}\right), \quad (2.2.2)$$

where  $\mathcal{H}$  is the set of subsets  $T$  of  $S$  such that product of elements of  $T$  is a perfect square. Also, denoting  $\mathcal{H}^* = \mathcal{H} \setminus \{\emptyset\}$ .

By convention, the empty product is 1, hence, we rewrite (2.2.2) as

$$\prod_{s \in S} \left(1 + \theta(s) \left(\frac{s}{p}\right)\right) = \sum_{\substack{T \subseteq S \\ T \notin \mathcal{H}}} \theta(T) \prod_{s \in T} \left(\frac{s}{p}\right) + \sum_{T \in \mathcal{H}} \theta(T).$$

Therefore, by substituting,

$$\begin{aligned} \frac{1}{2^{|S|}} \sum_{\substack{\phi \neq T \subseteq S \\ T \notin \mathcal{H}}} \theta(T) \sum_{\substack{n < p \leq 2n \\ p \equiv f \pmod{d}}} \prod_{s \in T} \left( \frac{s}{p} \right) \log p &= \frac{\sum_{T \in \mathcal{H}} \theta(T)}{2^{|S|}} \sum_{\substack{n < p \leq 2n \\ p \equiv f \pmod{d}}} \log p \\ &+ \frac{1}{2^{|S|}} \sum_{\substack{n < p \leq 2n \\ p \equiv f \pmod{d}}} \log p \prod_{s \in S} \left( 1 + \theta(s) \left( \frac{s}{p} \right) \right) \end{aligned}$$

As both  $d$  and  $\prod_{s \in S} s$  are both bounded by certain powers of  $\log n$ , we have the following cases:

**Case I:** When  $4 \nmid d$ , then by using Lemma 2.2.5 along with Lemma 2.2.6 and applying partial summation formula, we obtain

$$\begin{aligned} \sum_{\substack{p \in S(n, \theta) \\ p \equiv f \pmod{d}}} \log p &= \frac{1}{2^{|S|}} \sum_{\substack{T \notin \mathcal{H} \\ |\text{sqf}(T)| \mid d \\ \text{sqf}(T) \equiv 1 \pmod{4}}} \left( \frac{\text{sqf}(T)}{f} \right) \theta(T) \sum_{\substack{n < p \leq 2n \\ p \equiv f \pmod{d}}} \log p \\ &+ \frac{1}{2^{|S|}} \sum_{T \in \mathcal{H}} \theta(T) \sum_{\substack{n < p \leq 2n \\ p \equiv f \pmod{d}}} \log p + O\left( \frac{n \log n}{\exp(C_1 \sqrt{\log n})} \right). \quad (2.2.3) \end{aligned}$$

Also, if we write the squarefree part of a perfect square to be 1 by convention, then equation (2.2.3) can be rewritten as

$$\sum_{\substack{p \in S(n, \theta) \\ p \equiv f \pmod{d}}} \log p = \frac{1}{2^{|S|}} \sum_{\substack{T \subseteq S \\ |\text{sqf}(T)| \mid d \\ \text{sqf}(T) \equiv 1 \pmod{4}}} \left( \frac{\text{sqf}(T)}{f} \right) \theta(T) \sum_{\substack{n < p \leq 2n \\ p \equiv f \pmod{d}}} \log p + O\left( \frac{n \log n}{\exp(C_1 \sqrt{\log n})} \right).$$

**Case II:** When  $4 \mid d$  and  $8 \nmid d$ , then by using Lemma 2.2.5 along with Lemma 2.2.6 and applying partial summation formula, we obtain

$$\sum_{\substack{p \in S(n, \theta) \\ p \equiv f \pmod{d}}} \log p = \frac{1}{2^{|S|}} \sum_{\substack{T \subseteq S \\ |\text{sqf}(T)| \mid d \\ \text{sqf}(T) \equiv 1, 3 \pmod{4}}} \left( \frac{\text{sqf}(T)}{f} \right) \theta(T) \sum_{\substack{n < p \leq 2n \\ p \equiv f \pmod{d}}} \log p + O\left( \frac{n \log n}{\exp(C_1 \sqrt{\log n})} \right).$$

**Case III:** When  $8 \mid d$ , similar to the above cases, by using Lemma 2.2.5 along with Lemma 2.2.6 and applying partial summation formula, we obtain

$$\sum_{\substack{p \in S(n, \theta) \\ p \equiv f \pmod{d}}} \log p = \frac{1}{2^{|S|}} \sum_{\substack{T \subseteq S \\ |\text{sqf}(T)| \mid d}} \left( \frac{\text{sqf}(T)}{f} \right) \theta(T) \sum_{\substack{n < p \leq 2n \\ p \equiv f \pmod{d}}} \log p + O\left( \frac{n \log n}{\exp(C_1 \sqrt{\log n})} \right).$$

Also, since  $d \leq (\log n)^A$  for  $A > 0$ , we make use of Siegel-Walfisz Theorem to obtain,

$$\sum_{\substack{p \in S(n, \theta) \\ p \equiv f \pmod{d}}} \log p = \frac{C(S, \theta, d)}{2^{|S|}} \cdot \frac{n}{\varphi(d)} + O\left( \frac{n \log n}{\exp(C_1 \sqrt{\log n})} \right),$$

where  $C(S, \theta, d)$  is defined as in (2.1.1). This completes the proof of Theorem 2.1.1.  $\square$

### 2.3 Some Combinatorial Lemmas and Corollaries of Theorem 2.1.1

Let  $S \in \mathbb{Z}\{0\}$ , and  $\mathbf{P}(S)$  be the power set of  $S$ . We know that  $(\mathbf{P}(S), \Delta, \cap)$  is a commutative ring (in fact a Boolean ring). Also,  $(\mathbf{P}(S), \Delta)$  is an Abelian group with  $\emptyset$ , the empty set, being the identity element.  $(\mathbf{P}(S), \Delta)$  is isomorphic to  $\mathbb{F}_2 \times \cdots \times \mathbb{F}_2$  ( $|S|$  times).

Let  $\mathcal{H} = \mathcal{H}(S)$ , as earlier, be the function that captures perfect square kind of behaviour in the set  $S$ , namely

$$\mathcal{H} = \mathcal{H}(S) = \left\{ T \subseteq S : \prod_{s \in T} s = \square \right\}. \quad (2.3.1)$$

Also, we can see that  $\emptyset \in \mathcal{H}(S)$  by the convention that the empty product equals 1. Here henceforth,  $\square$  would be used to denote non-specific perfect squares. The subset

$\mathcal{H}(S)$  of  $\mathbf{P}(S)$  is closed under the symmetric difference. Indeed if  $S_1, S_2 \in \mathcal{H}(S)$ , then

$$\left( \prod_{s \in S_1 \Delta S_2} s \right) = \left( \prod_{s \in S_1} s \right) \left( \prod_{s \in S_2} s \right) \left( \prod_{s \in S_1 \cap S_2} s \right)^2 = \square = \left( \prod_{s \in S_1} s \right) \left( \prod_{s \in S_2} s \right) = \left( \prod_{s \in S_1 \cap S_2} s \right)^2.$$

Since  $S$  is a finite set, we have  $(\mathcal{H}(S), \Delta) \leq (\mathbf{P}(S), \Delta)$ .

In the following Lemmas, we will discuss some properties of the subgroup  $\mathcal{H}(S)$  and cosets of  $\mathcal{H}(S)$  in  $\mathbf{P}(S)$  will be discussed in the following lemmas. For any  $A \subseteq S$ , we use  $\bar{A}$  to denote the coset  $A \cdot \mathcal{H}(S)$ .

**Lemma 2.3.1.** *Let  $S$  be a finite set of non-zero integers. For any  $S_1 \in \mathbf{P}(S) \setminus \mathcal{H}(S)$ , the left coset  $S_1 \cdot \mathcal{H}(S)$  is of the form*

$$\bar{S}_1 = \{T \in \mathbf{P}(S) : \text{sqf}(T) = \text{sqf}(S_1)\}.$$

*In other words, there are precisely  $|\mathcal{H}(S)|$  elements of  $\mathbf{P}(S)$  such that the squarefree component of the product of all the elements of those subsets is the same.*

*Proof:* Let  $S'$  be a nonempty subset of  $S$  such that  $S' \not\subseteq \mathcal{H}(S)$ . Consider

$$S' \cdot \mathcal{H}(S) = \{S' \Delta T : T \in \mathcal{H}(S)\}.$$

Since  $\mathcal{H}(S)$  is closed under symmetric difference, we observe that

$$\text{sqf} \left( \prod_{s \in S_1 \Delta T} s \right) = \text{sqf} \left( \prod_{s \in S_1} s \right),$$

for all  $T \in \mathcal{H}(S)$ . Thus,  $S_1 \cdot \mathcal{H}(S) \subseteq \bar{S}_1$  holds.

Suppose  $S_2 \in \bar{S}_1$  with  $S_2 \neq S_1$ . We would want to show that there exists  $T \in \mathcal{H}(S)$  such that  $S_1 \Delta T = S_2$ . Consider

$$\prod_{s \in S_1 \Delta S_2} s = \frac{(\prod_{s \in S_1 \Delta S_2} s) (\prod_{s \in S_1 \cap S_2} s)^2}{(\prod_{s \in S_1 \cap S_2} s)^2} = \frac{(\prod_{s \in S_1} s) (\prod_{s \in S_2} s)}{(\prod_{s \in S_1 \cap S_2} s)^2} = \square.$$

This implies  $S_1 \Delta S_2 \in \mathcal{H}(S)$ . By choosing  $T = S_1 \Delta S_2$ , we have  $S_1 \Delta T = S_1 \Delta (S_1 \Delta S_2) = S_2$ . Hence, the converse holds:  $\bar{S}_1 \subseteq S_1 \cdot \mathcal{H}(S)$ .  $\square$

For every  $U \subseteq S$ , we define odd and even set partition of set  $\mathcal{H}(S)$ :

$$\mathcal{O}_U(S) = \{T \in \mathcal{H}(S) : |T \cap U| \text{ is odd}\}$$

$$\mathcal{E}_U(S) = \{T \in \mathcal{H}(S) : |T \cap U| \text{ is even}\}.$$

Here we use the convention that zero is even. Hence we assume  $\emptyset \in \mathcal{E}_A(S)$ .



**Lemma 2.3.2.**  $\mathcal{E}_A(S)$  is a subgroup of  $\mathcal{H}(S)$ . Further, if  $\mathcal{O}_A(S) \neq \emptyset$ , then  $\mathcal{E}_A(S)$  is an index 2 subgroup of  $\mathcal{H}(S)$ , or equivalently  $|\mathcal{O}_A(S)| = |\mathcal{E}_A(S)|$

*Proof:* For any  $A \subset S$ , define a map

$$\phi_A : \mathcal{H}(S) \rightarrow (\mathbb{Z}_2, \oplus_2) \text{ by } \phi_A(T) = |T \cap A| \pmod{2}.$$

For any  $T_1, T_2 \in \mathcal{H}(S)$ , we have

$$\begin{aligned} \phi_A(T_1 \triangle T_2) &= |(T_1 \triangle T_2) \cap A| \pmod{2} = (|T_1 \cap A| + |T_2 \cap A| - 2|T_1 \cap T_2 \cap A|) \pmod{2} \\ &= |T_1 \cap A| \pmod{2} \oplus_2 |T_2 \cap A| \pmod{2} = \phi_A(T_1) \oplus_2 \phi_A(T_2). \end{aligned}$$

Therefore,  $\phi_A$  is a homomorphism whose kernel is  $\mathcal{E}_A(S)$ . Suppose  $\mathcal{O}_A(S)$  is a non-empty, then  $\phi_A$  is surjective. Thus,  $\mathcal{E}_A(S)$  is an index 2 subgroup of  $\mathcal{H}(S)$  (equivalently,  $|\mathcal{O}_A(S)| = |\mathcal{E}_A(S)|$ ).  $\square$

Consider the quotient group  $\overline{\mathbf{P}(S)} = \mathbf{P}(S)/\mathcal{H}(S)$  with a binary operation  $\overline{S_1} \cdot \overline{S_2} = \overline{S_1 \triangle S_2}$  for  $\overline{S_1}, \overline{S_2} \in \overline{\mathbf{P}(S)}$ . It follows from Lemma 2.3.1 that any two subsets of  $S$  have the same squarefree part if and only if they lie in the same coset of the subgroup  $\mathcal{H}(S)$ . Thus,  $\text{sqf}(\overline{T})$  is well defined and equal to  $\text{sqf}(T)$  for every  $\overline{T} \in \overline{\mathbf{P}(S)}$ .

Conventionally, we write the squarefree part of a perfect square is 1. Hence we assume  $\text{sqf}(\overline{\phi}) = 1$ .

For any given positive integer  $d$ , we define the followings subsets of  $\overline{\mathbf{P}(S)}$ .

$$\begin{aligned} \overline{\mathcal{D}}_0 &= \left\{ \overline{T} \in \overline{\mathbf{P}(S)} : |\text{sqf}(\overline{T})| \mid d \right\} \\ \overline{\mathcal{D}}_1 &= \left\{ \overline{T} \in \overline{\mathbf{P}(S)} : |\text{sqf}(\overline{T})| \mid d \text{ and } \text{sqf}(\overline{T}) \equiv 1 \text{ or } 3 \pmod{4} \right\} \\ \overline{\mathcal{D}}_2 &= \left\{ \overline{T} \in \overline{\mathbf{P}(S)} : |\text{sqf}(\overline{T})| \mid d \text{ and } \text{sqf}(\overline{T}) \equiv 1 \pmod{4} \right\}. \end{aligned} \quad (2.3.2)$$

Note that  $\overline{\mathcal{D}}_2 \subseteq \overline{\mathcal{D}}_1 \subseteq \overline{\mathcal{D}}_0$ . In the following Lemma, we prove that  $\overline{\mathcal{D}}_0, \overline{\mathcal{D}}_1$  and  $\overline{\mathcal{D}}_2$  are subgroups of  $\overline{\mathbf{P}(S)}$ .

**Lemma 2.3.3.**  $\overline{\mathcal{D}}_0, \overline{\mathcal{D}}_1$  and  $\overline{\mathcal{D}}_2$  are subgroups of  $\overline{\mathbf{P}(S)}$ . Moreover, if there exists  $\overline{T_1} \in \overline{\mathbf{P}(S)}$  such that  $\text{sqf}(T_1) \equiv 2 \pmod{4}$  then  $\overline{\mathcal{D}}_1$  is an index 2 subgroup of  $\overline{\mathcal{D}}_0$ . Also, if there exists  $\overline{T_1} \in \overline{\mathbf{P}(S)}$  such that  $\text{sqf}(T_1) \equiv 3 \pmod{4}$  then  $\overline{\mathcal{D}}_2$  is an index 2 subgroup of  $\overline{\mathcal{D}}_1$ .

*Proof:* For any  $\overline{S_1}, \overline{S_2} \in \overline{\mathbf{P}(S)}$ , we observe that

$$\text{sqf}(\overline{S_1 \Delta S_2}) = \text{sqf}(\text{sqf}(\overline{S_1}) \cdot \text{sqf}(\overline{S_2})). \quad (2.3.3)$$

Let  $\overline{S_1}, \overline{S_2} \in \overline{\mathcal{D}_0}$ . Equivalently,  $|\text{sqf}(\overline{S_1})| \mid d$  and  $|\text{sqf}(\overline{S_2})| \mid d$ . Then by (2.3.3) it follows that  $|\text{sqf}(\overline{S_1 \Delta S_2})| \mid d$ . Thus  $\overline{\mathcal{D}_0}$  is a subgroup of  $\overline{\mathbf{P}(S)}$ .

Now we define a map  $\tau_1 : \overline{\mathcal{D}_0} \rightarrow \{1, -1\}$  by

$$\tau_1(\overline{T}) = \begin{cases} 1 & \text{if } \text{sqf}(\overline{T}) \text{ is odd} \\ -1 & \text{if } \text{sqf}(\overline{T}) \text{ is even.} \end{cases}$$

For any  $\overline{T_1}, \overline{T_2} \in \overline{\mathcal{D}_0}$ , using (2.3.3) we obtain  $\tau_1(\overline{T_1 \Delta T_2}) = 1$  if either both  $\text{sqf}(T_1)$  and  $\text{sqf}(T_2)$  are even or both are odd and  $\tau_1(\overline{T_1 \Delta T_2}) = -1$  if one of  $\text{sqf}(T_1)$  and  $\text{sqf}(T_2)$  is even and other one is odd. Thus  $\tau_1(\overline{T_1 \Delta T_2}) = \tau_1(\overline{T_1}) \cdot \tau_1(\overline{T_2})$  for every  $T_1, T_2 \in \overline{\mathcal{D}_0}$ . Therefore,  $\tau_1$  is a homomorphism with the kernel  $\overline{\mathcal{D}_1}$ .

Suppose there exists  $\overline{T_1} \in \overline{\mathbf{P}(S)}$  such that  $\text{sqf}(T_1) \equiv 2 \pmod{4}$ , then  $\tau_1$  is a surjective homomorphism. Thus  $\overline{\mathcal{D}_1}$  is an index 2 subgroup of  $\overline{\mathcal{D}_0}$ .

Define a map  $\tau_2 : \overline{\mathcal{D}_1} \rightarrow (\mathbb{Z}_4^*, \odot_4)$  by  $\tau_2(\overline{T}) = \text{sqf}(\overline{T}) \pmod{4}$ . For any  $\overline{T_1}, \overline{T_2} \in \overline{\mathcal{D}_1}$ , by (2.3.3) we have,

$$\begin{aligned} \tau_2(\overline{T_1 \Delta T_2}) &= \text{sqf}(\text{sqf}(\overline{T_1}) \cdot \text{sqf}(\overline{T_2})) \pmod{4} = \text{sqf}(\overline{T_1}) \text{sqf}(\overline{T_2}) \left( \prod_{\substack{p \mid \text{sqf}(\overline{T_1}) \\ p \mid \text{sqf}(\overline{T_2})}} p \right)^{-2} \pmod{4} \\ &= \text{sqf}(\overline{T_1}) \pmod{4} \odot_4 \text{sqf}(\overline{T_2}) \pmod{4} = \tau_2(\overline{T_1}) \odot_4 \tau_2(\overline{T_2}). \end{aligned}$$

Therefore,  $\tau_2$  is a homomorphism with the kernel  $\overline{\mathcal{D}_2}$ . Suppose there exists  $\overline{T_1} \in \overline{\mathbf{P}(S)}$  such that  $\text{sqf}(T_1) \equiv 3 \pmod{4}$ , then  $\tau_2$  is a surjective homomorphism. Thus  $\overline{\mathcal{D}_2}$  is an index 2 subgroup of  $\overline{\mathcal{D}_1}$ .  $\square$

Given  $\theta : S \rightarrow \{-1, 1\}$ , we also define

$$N_\theta = N_\theta(S) = \{s \in S : \theta(s) = -1\}. \quad (2.3.4)$$

**Lemma 2.3.4.** *Let  $S$  be a finite set of non-zero integers with a choice of signs  $\theta$  for  $S$ . For a squarefree positive integer  $f$  such that  $(f, \text{sqf}(T)) = 1$  for every  $T \in \mathbf{P}(S)$ , define*

$$\mu_f^\theta : \mathbf{P}(S) \rightarrow \{1, -1\} \text{ by } \mu_f^\theta(T) = \theta(T) \cdot \left( \frac{\text{sqf}(T)}{f} \right).$$

*Then  $\mu_f^\theta$  is a homomorphism.*

*Suppose  $\mathcal{O}_{N_\theta}(S) = \phi$ , then the map*

$$\overline{\mu}_f^\theta : \overline{\mathbf{P}(S)} \rightarrow \{1, -1\} \text{ defined by } \overline{\mu}_f^\theta(\overline{T}) = \theta(\overline{T}) \cdot \left( \frac{\text{sqf}(\overline{T})}{f} \right)$$

*is well-defined and a homomorphism.*

*Proof:* For any  $T_1, T_2 \in \mathbf{P}(S)$ , we observe that

$$\theta(T_1 \triangle T_2) = \prod_{s \in T_1 \triangle T_2} \theta(s) = \left( \prod_{s \in T_1} \theta(s) \right) \left( \prod_{s \in T_2} \theta(s) \right) \left( \prod_{s \in T_1 \cap T_2} (\theta(s))^2 \right)^{-1} = \theta(T_1) \theta(T_2). \quad (2.3.5)$$

Also, by the completely multiplicative property of the Jacobi symbol, we have

$$\left( \frac{\text{sqf}(T_1)}{f} \right) \cdot \left( \frac{\text{sqf}(T_2)}{f} \right) = \left( \frac{\text{sqf}(T_1) \text{sqf}(T_2)}{f} \right) = \left( \frac{\text{sqf}(\text{sqf}(T_1) \text{sqf}(T_2))}{f} \right) = \left( \frac{\text{sqf}(T_1 \triangle T_2)}{f} \right).$$

Thus,  $\mu_f^\theta(T_1 \triangle T_2) = \mu_f^\theta(T_1) \cdot \mu_f^\theta(T_2)$  holds for every  $T_1, T_2 \in \mathbf{P}(S)$ . Hence  $\mu_f^\theta$  is a homomorphism.

Suppose  $\mathcal{O}_{N_\theta}(S) = \phi$ , then  $\theta(T) = 1$  for every  $T \in \mathcal{H}(S)$ . Also, by definition of  $\mathcal{H}(S)$  it follows that  $\left( \frac{\text{sqf}(T)}{f} \right) = \left( \frac{1}{f} \right) = 1$  for every  $T \in \mathcal{H}(S)$ . Thus we obtain  $\mathcal{H}(S) \subseteq \ker(\mu_f^\theta)$ . Therefore, the map  $\overline{\mu}_f^\theta : \overline{\mathbf{P}(S)} \rightarrow \{1, -1\}$  defined by  $\overline{\mu}_f^\theta(\overline{T}) = \theta(\overline{T}) \cdot \left( \frac{\text{sqf}(\overline{T})}{f} \right)$  is well-defined and a homomorphism.  $\square$

As  $C(S, \theta, d)$  contributes to counting, it is natural to think about its non-negativity. In the following Lemma, we show that  $C(S, \theta, d) \geq 0$  and discuss criteria for its strict positivity.

**Lemma 2.3.5.** *Let  $S$ ,  $\theta$ ,  $f$  and  $d$  be stated as in Theorem 2.1.1. Let  $\overline{\mathcal{D}}_0, \overline{\mathcal{D}}_1$  and  $\overline{\mathcal{D}}_2$  be subsets of quotient group  $\overline{\mathbf{P}(S)}$  as defined in 2.3.2.*

*Then the constant  $C(S, \theta, d)$  in the main term of Theorem 2.1.1 is always greater or equal to 0. Also,*

- (i) *If  $4 \nmid d$ , then  $C(S, \theta, d) > 0$  holds iff  $\theta(\overline{T}) = \left( \frac{\text{sqf}(\overline{T})}{f} \right)$  and  $\mathcal{O}_{N_\theta}(S) = \phi$  for every  $\overline{T} \in \overline{\mathcal{D}}_2$ .*

(ii) If  $4 \mid d$  and  $8 \nmid d$ , then  $C(S, \theta, d) > 0$  holds iff  $\theta(\bar{T}) = \left(\frac{\text{sqf}(\bar{T})}{f}\right)$  and  $\mathcal{O}_{N_\theta}(S) = \phi$  for every  $\bar{T} \in \overline{\mathcal{D}_1}$ .

(iii) If  $8 \mid d$ , then  $C(S, \theta, d) > 0$  holds iff  $\theta(\bar{T}) = \left(\frac{\text{sqf}(\bar{T})}{f}\right)$  and  $\mathcal{O}_{N_\theta}(S) = \phi$  for every  $\bar{T} \in \overline{\mathcal{D}_0}$ .

*Proof:* It follows from Lemma 2.3.1 that any two subsets of  $S$  have the same squarefree part if and only if they lie in the same coset of the subgroup  $\mathcal{H}(S)$ . Then by using (2.3.2), we rewrite (2.1.1) as

$$C(S, \theta, d) = \begin{cases} \sum_{\bar{T} \in \overline{\mathcal{D}_2}} \left(\frac{\text{sqf}(\bar{T})}{f}\right) \sum_{U \in \mathcal{H}} \theta(T \Delta U) & \text{if } 4 \nmid d, \\ \sum_{\bar{T} \in \overline{\mathcal{D}_1}} \left(\frac{\text{sqf}(\bar{T})}{f}\right) \sum_{U \in \mathcal{H}} \theta(T \Delta U) & \text{if } 4 \mid d, 8 \nmid d, \\ \sum_{\bar{T} \in \overline{\mathcal{D}_0}} \left(\frac{\text{sqf}(\bar{T})}{f}\right) \sum_{U \in \mathcal{H}} \theta(T \Delta U) & \text{if } 8 \mid d. \end{cases} \quad (2.3.6)$$

For any  $S' \subseteq S$ , we observe that

$$|(S' \Delta U) \cap N_\theta(S)| = |(S' \cap N_\theta(S))| + |(U \cap N_\theta(S))| - 2|(S' \cap U) \cap N_\theta(S)| \text{ for } U \in \mathcal{H}(S)$$

Thus, depending on whether  $|S' \cap N_\theta(S)|$  is odd or even,  $|N_\theta(S) \cap (S' \Delta U)|$  and  $|N_\theta(S) \cap U|$  have opposite or same parity, respectively, for all  $U \in \mathcal{H}(S)$ . Therefore, if  $\mathcal{O}_{N_\theta}(S) \neq \phi$ , then by Lemma 2.3.2 we obtain  $\sum_{U \in \mathcal{H}} \theta(S' \Delta U) = 0$  for any  $S' \subseteq S$ .

Thus it follows from (2.3.6) that if  $\mathcal{O}_{N_\theta}(S) \neq \phi$ , then  $C(S, \theta, d) = 0$ . Thus for  $C(S, \theta, d)$  to be positive, it is necessary to have  $\mathcal{O}_{N_\theta}(S) = \phi$ .

Hence, now we assume  $\mathcal{O}_{N_\theta}(S)$  to be empty (equivalently,  $\theta(U) = 1$  for every  $U \in \mathcal{H}(S)$ ). Then by using (2.3.5), we rewrite (2.3.6) as

$$C(S, \theta, d) = \begin{cases} |\mathcal{H}(S)| \left( \sum_{\bar{T} \in \overline{\mathcal{D}_2}} \left(\frac{\text{sqf}(\bar{T})}{f}\right) \theta(\bar{T}) \right) & \text{if } 4 \nmid d, \\ |\mathcal{H}(S)| \left( \sum_{\bar{T} \in \overline{\mathcal{D}_1}} \left(\frac{\text{sqf}(\bar{T})}{f}\right) \theta(\bar{T}) \right) & \text{if } 4 \mid d, 8 \nmid d, \\ |\mathcal{H}(S)| \left( \sum_{\bar{T} \in \overline{\mathcal{D}_0}} \left(\frac{\text{sqf}(\bar{T})}{f}\right) \theta(\bar{T}) \right) & \text{if } 8 \mid d. \end{cases} \quad (2.3.7)$$

By Lemma 2.3.3, we know that  $\overline{\mathcal{D}}_0$ ,  $\overline{\mathcal{D}}_1$  and  $\overline{\mathcal{D}}_2$  are subgroups of  $\overline{\mathbf{P}(S)}$ . Since  $\mathcal{O}_{N_\theta}(S) = \phi$ , by Lemma 2.3.4, we have  $\overline{\mu}_f^\theta : \overline{\mathbf{P}(S)} \rightarrow \{1, -1\}$  is a homomorphism and hence the restriction of  $\overline{\mu}_f^\theta$  to the subgroups  $\overline{\mathcal{D}}_0$ ,  $\overline{\mathcal{D}}_1$  and  $\overline{\mathcal{D}}_2$  is also a homomorphism. Thus,  $C(S, \theta, d) \geq 0$  always holds.

In each case, the corresponding sum in (2.3.7) is positive if and only if  $\theta(\overline{T}) = \left(\frac{\text{sqf}(\overline{T})}{f}\right)$  for every  $\overline{T}$  in the respective subgroup. Thus, in each case  $C(S, \theta, d) > 0$  holds if and only if  $\mathcal{O}_{N_\theta}(S) = \phi$  and  $\theta(\overline{T}) = \left(\frac{\text{sqf}(\overline{T})}{f}\right)$  for every  $\overline{T}$  in the respective subgroup. This completes the proof.  $\square$

### 2.3.1 Some Corollaries of Theorem 2.1.1

From (Theorem 1, Babu and Mukhopadhyay (2022)), it follows that there exist infinitely many primes  $p$  such that  $S$  has residue pattern  $\theta$  modulo  $p$  iff  $\mathcal{H}(S)$  does not contain a subset  $T$  satisfying  $\theta(T) = -1$ .

**Remark 2.3.6.** *Given  $S \subseteq \mathbb{Z} \setminus \{0\}$  with a choice of signs  $\theta$  for  $S$  and positive integers  $f, d$  with  $1 \leq f \leq d$  and  $(f, d) = 1$ . Suppose  $4 \nmid d$  and there is a subset  $T \subseteq S$  such that  $\theta(T) \neq \left(\frac{\text{sqf}(T)}{f}\right)$ ,  $|\text{sqf}(T)| \mid d$  and  $\text{sqf}(T) \equiv 1 \pmod{4}$ , then there is no prime  $p$  of the form  $p \equiv f \pmod{d}$  such that  $S$  has residue pattern  $\theta$  modulo  $p$ .*

*If such a prime  $p \equiv f \pmod{d}$  exists, then from the proof of Lemma 2.2.6, we can see that*

$$\begin{aligned} -1 = \theta(T) \left(\frac{\text{sqf}(T)}{f}\right) &= \prod_{s \in T} \theta(s) \left(\frac{\text{sqf}(T)}{f}\right) = \left(\frac{\text{sqf}(T)}{f}\right) \prod_{s \in T} \left(\frac{s}{p}\right) \\ &= \left(\frac{\text{sqf}(T)}{f}\right) \left(\frac{\text{sqf}(T)}{p}\right) = \left(\frac{\text{sqf}(T)}{f}\right)^2 = 1, \end{aligned}$$

*which is absurd.*

*For the other two cases, one can similarly show that there exists a prime  $p$  of the form  $p \equiv f \pmod{d}$  such that  $S$  has residue pattern  $\theta$  modulo  $p$  only if the sufficient condition stated in Lemma 2.3.5 holds.*

Thus, we have the following Corollary by using Theorem 2.1.1 and Lemma 2.3.5.

**Corollary 2.3.7.** *Let  $S$  be a finite set of non-zero integers with a choice of signs  $\theta$  for  $S$ . Let  $f, d$  be positive coprime integers with  $f \leq d$ .*

**Case 1**  $4 \nmid d$

*There exist infinitely many primes  $p$  of the form  $p \equiv f \pmod{d}$  such that  $S$  has residue pattern  $\theta$  modulo  $p$  if and only if  $\mathcal{O}_{N_\theta}(S) = \phi$  and  $\theta(\overline{T}) = \left(\frac{\text{sqf}(\overline{T})}{f}\right)$  for every  $\overline{T} \in \overline{\mathcal{D}}_2$ . In this case, the asymptotic density*

$$\frac{1}{n} |S(n, \theta)| \rightarrow \frac{|\overline{\mathcal{D}}_2| \cdot |\mathcal{H}(S)|}{\phi(d) 2^{|S|}} \text{ as } n \rightarrow \infty.$$

**Case 2**  $4 \mid d$  and  $8 \nmid d$ 

There exist infinitely many primes  $p$  of the form  $p \equiv f \pmod{d}$  such that  $S$  has residue pattern  $\theta$  modulo  $p$  if and only if  $\mathcal{O}_{N_\theta}(S) = \phi$  and  $\theta(\bar{T}) = \left(\frac{\text{sqf}(\bar{T})}{f}\right)$  for every  $\bar{T} \in \overline{\mathcal{D}_1}$ . In this case, the asymptotic density

$$\frac{1}{n} |\mathcal{S}(n, \theta)| \rightarrow \frac{|\overline{\mathcal{D}_1}| \cdot |\mathcal{H}(S)|}{\varphi(d) 2^{|S|}} \quad \text{as } n \rightarrow \infty.$$

**Case 3**  $8 \mid d$ 

There exist infinitely many primes  $p$  of the form  $p \equiv f \pmod{d}$  such that  $S$  has residue pattern  $\theta$  modulo  $p$  if and only if  $\mathcal{O}_{N_\theta}(S) = \phi$  and  $\theta(\bar{T}) = \left(\frac{\text{sqf}(\bar{T})}{f}\right)$ , for every  $\bar{T} \in \overline{\mathcal{D}_0}$ . In this case, the asymptotic density

$$\frac{1}{n} |\mathcal{S}(n, \theta)| \rightarrow \frac{|\overline{\mathcal{D}_0}| \cdot |\mathcal{H}(S)|}{\varphi(d) 2^{|S|}} \quad \text{as } n \rightarrow \infty.$$

When does a set  $S$  support all residue patterns with the mentioned conditions? The following Corollary gives a necessary and sufficient condition for it.

**Corollary 2.3.8.** *Let  $f, d$  be positive integers with  $1 \leq f \leq d$  and  $(f, d) = 1$ .*

**Case 1**  $4 \nmid d$ 

A nonempty finite set  $S \subset \mathbb{Z} \setminus \{0\}$  supports all residue patterns for infinitely many primes  $p$  of the form  $p \equiv f \pmod{d}$  if and only if  $\mathcal{H}(S) = \{\phi\}$  and  $\overline{\mathcal{D}_2} = \{\phi\}$ .

**Case 2**  $4 \mid d$  and  $8 \nmid d$ 

A nonempty finite set  $S \subset \mathbb{Z} \setminus \{0\}$  supports all residue patterns for infinitely many primes  $p$  of the form  $p \equiv f \pmod{d}$  if and only if  $\mathcal{H}(S) = \{\phi\}$  and  $\overline{\mathcal{D}_1} = \{\phi\}$ .

**Case 3**  $8 \mid d$ 

A nonempty finite set  $S \subset \mathbb{Z} \setminus \{0\}$  supports all residue patterns for infinitely many primes  $p$  of the form  $p \equiv f \pmod{d}$  if and only if  $\mathcal{H}(S) = \{\phi\}$  and  $\overline{\mathcal{D}_0} = \{\phi\}$ .

In each case, for every choice of signs  $\theta : S \rightarrow \{-1, 1\}$  the density of the set  $\mathcal{S}(n, \theta)$  is  $\frac{1}{\varphi(d) 2^{|S|}}$ .

For example, let  $S$  be a nonempty finite set of primes that does not divide  $d$ , then it is easy to see that  $\mathcal{H}(S) = \{\phi\}$  and  $\overline{\mathcal{D}_0} = \{\phi\}$ . Therefore, every nonempty finite set of primes that does not divide  $d$  supports all residue patterns for infinitely many primes  $p$  of the form  $p \equiv f \pmod{d}$ . Here, we mention that the Corollary 2.3.8 is an analogue of primes in the arithmetic progression of (Theorem 2, M. Filaseta (1989)) and (Theorem 4.3 of Wright (2007)).

Specifically looking at the cases when the set  $S$  satisfies being quadratic residues and non-residues, respectively, we have the following Corollaries.

**Corollary 2.3.9.** *Let  $f, d$  be coprime positive integers with  $1 \leq f \leq d$ . Necessary and sufficient condition for a nonempty finite set  $S \subset \mathbb{Z} \setminus \{0\}$  to be a set of quadratic residue for infinitely many primes of the form  $p \equiv f \pmod{d}$  is given below for each case.*

**Case 1**  $4 \nmid d$

$$\theta(\bar{T}) = \left( \frac{\text{sqf}(\bar{T})}{f} \right), \text{ for every } \bar{T} \in \overline{\mathcal{D}}_2.$$

**Case 2**  $4 \mid d$  and  $8 \nmid d$

$$\theta(\bar{T}) = \left( \frac{\text{sqf}(\bar{T})}{f} \right), \text{ for every } \bar{T} \in \overline{\mathcal{D}}_1.$$

**Case 3**  $8 \mid d$

$$\theta(\bar{T}) = \left( \frac{\text{sqf}(\bar{T})}{f} \right), \text{ for every } \bar{T} \in \overline{\mathcal{D}}_0.$$

*The asymptotic density of primes of the form  $p \equiv f \pmod{d}$  for which all the elements of  $S$  are quadratic residues modulo  $p$  is*

$$\frac{|\overline{\mathcal{D}}_2| \cdot |\mathcal{H}(S)|}{\varphi(d)2^{|S|}} \text{ if } 4 \nmid d, \quad \frac{|\overline{\mathcal{D}}_1| \cdot |\mathcal{H}(S)|}{\varphi(d)2^{|S|}} \text{ if } 4 \mid d, 8 \nmid d \text{ and } \frac{|\overline{\mathcal{D}}_0| \cdot |\mathcal{H}(S)|}{\varphi(d)2^{|S|}} \text{ if } 8 \mid d. \quad (2.3.8)$$

*Proof:* Since we expect every element of  $S$  to be quadratic residue, the choice of signs is  $\theta \equiv 1$ . Therefore, the proof of Corollary 2.3.9 follows from Theorem 2.1.1, with  $N_\theta(S) = \phi$ . □

**Corollary 2.3.10.** *Let  $f, d$  be positive integers with  $1 \leq f \leq d$  and  $(f, d) = 1$ . Necessary and sufficient condition for a nonempty finite set  $S \subset \mathbb{Z} \setminus \{0\}$  to be a set of quadratic non-residue for infinitely many primes of the form  $p \equiv f \pmod{d}$  is given below for each case.*

**Case 1**  $4 \nmid d$

$\mathcal{H}(S)$  does not contain a subset of odd cardinality and  $\theta(\bar{T}) = \left( \frac{\text{sqf}(\bar{T})}{f} \right)$ , for every  $\bar{T} \in \overline{\mathcal{D}}_2$ .

**Case 2**  $4 \mid d$  and  $8 \nmid d$

$\mathcal{H}(S)$  does not contain a subset of odd cardinality and  $\theta(\bar{T}) = \left( \frac{\text{sqf}(\bar{T})}{f} \right)$ , for every  $\bar{T} \in \overline{\mathcal{D}}_1$ .

**Case 3**  $8 \mid d$

$\mathcal{H}(S)$  does not contain a subset of odd cardinality and  $\theta(\bar{T}) = \left( \frac{\text{sqf}(\bar{T})}{f} \right)$ , for every  $\bar{T} \in \overline{\mathcal{D}}_0$ .

*In each case, the asymptotic density of primes for which all the elements of  $S$  are quadratic nonresidues modulo  $p$  is stated as in (2.3.8).*

*Proof:* Since we expect every element of  $S$  to be quadratic nonresidue, the choice of signs is  $\theta \equiv -1$ . Therefore, the proof of Corollary 2.3.10 follows from Theorem 2.1.1, with  $N_\theta(S) = S$ .

## 2.4 A counting problem arising from Theorem 2.1.1

We gather the inputs necessarily required for cyclotomic and multi-quadratic field extensions. For multi-quadratic part, let  $\mathbf{F}(S)$  denote the set of all choice of signs  $\theta$  on  $S$ , which is an Abelian group under pointwise multiplication for any  $\theta_1, \theta_2 \in \mathbf{F}(S)$

$$\theta_1 \cdot \theta_2(s) = \theta_1(s) \cdot \theta_2(s), \quad \text{for every } s \in S.$$

Let

$$\mathbf{C}(S) = \{\theta \in \mathbf{F}(S) : \mathcal{O}_{N_\theta}(S) = \phi\}. \quad (2.4.1)$$

It follows from (Theorem 2, Babu and Mukhopadhyay (2022)) and (Lemma 2, Babu and Mukhopadhyay (2022)) that  $\mathbf{C}(S)$  is a subgroup of  $\mathbf{F}(S)$  of order  $\frac{2^{|S|}}{|\mathcal{H}(S)|}$ .

For cyclotomic part, for a positive integer  $d$ ,

$$\mathbb{Z}_d^* = \{1 \leq f < d : (f, d) = 1\}$$

is a group of units of the ring  $\mathbb{Z}_d$  of order  $\varphi(d)$ .

We expect the multi-quadratic and their cyclotomic extensions to interact as direct products. Also, it follows from Lemma 2.3.4 that  $\overline{\mu}_f^\theta$  is a well-defined map for all  $\theta \in \mathbf{C}(S)$ , hence we define the following subsets

$$\mathbf{D}_i(S) = \left\{ (f, \theta) \in \mathbb{Z}_d^* \times \mathbf{C}(S) : \overline{\mu}_f^\theta(\overline{T}) = \theta(\overline{T}) \left( \frac{\text{sqf}(\overline{T})}{f} \right) = 1, \forall \overline{T} \in \overline{\mathcal{D}}_i \right\} \quad (2.4.2)$$

of the direct product  $\mathbb{Z}_d^* \times \mathbf{C}(S)$  of the groups  $\mathbb{Z}_d^*$  and  $\mathbf{C}(S)$ , where for  $i = 0, 1$  and  $2$ ,  $\overline{\mathcal{D}}_i$  is defined as in (2.3.3).

It turns out that the subsets  $\mathbf{D}_i(S)$  are actually subgroups of  $\mathbb{Z}_d^* \times \mathbf{C}(S)$  for  $i = 0, 1, 2$ .

**Lemma 2.4.1.**  $\mathbf{D}_i(S)$  is a subgroup of  $\mathbb{Z}_d^* \times \mathbf{C}(S)$ , for  $i = 0, 1, 2$ .



*Proof:* Here, we prove that  $\mathbf{D}_0(S)$  is a subgroup of  $\mathbb{Z}_d^* \times \mathbf{C}(S)$ . The proof for  $\mathbf{D}_1(S)$  and  $\mathbf{D}_2(S)$  being the subgroups follows similarly.

Suppose  $(f_1, \theta_1), (f_2, \theta_2) \in \mathbf{D}_0(S)$ , then  $\overline{\mu_{f_1}^{\theta_1}}(\overline{T}) = 1$  and  $\overline{\mu_{f_2}^{\theta_2}}(\overline{T}) = 1$  holds, for all  $\overline{T} \in \overline{\mathcal{D}_0}$ . Let  $f \equiv f_1 f_2 \pmod{d}$ . Since  $\text{sqf}(\overline{T}) \mid d$  for every  $\overline{T} \in \overline{\mathcal{D}_0}$ , we have  $f \equiv f_1 f_2 \pmod{\text{sqf}(\overline{T})}$  for every  $\overline{T} \in \overline{\mathcal{D}_0}$ .

Therefore,

$$\overline{\mu_f^{\theta_1 \theta_2}}(\overline{T}) = \theta_1(\overline{T}) \theta_2(\overline{T}) \left( \frac{\text{sqf}(\overline{T})}{f} \right) = \theta_1(\overline{T}) \left( \frac{\text{sqf}(\overline{T})}{f_1} \right) \theta_2(\overline{T}) \left( \frac{\text{sqf}(\overline{T})}{f_2} \right) = 1.$$

Thus, we obtain  $\overline{\mu_f^{\theta_1 \theta_2}} \in \mathbf{D}_0(S)$ . This completes the proof of Lemma 2.4.1.  $\square$

$\mathbf{D}_i(S)$  contribute to finding the structure of the field extension and correspondingly the cardinality of the Galois group of multi-quadratic fields and their cyclotomic extensions over  $\mathbb{Q}$ . The cardinality of the same allows us to know the degree of this field extension.

**Theorem 2.4.2.**

$$|\mathbf{D}_i(S)| = \frac{2^{|S|} \varphi(d)}{|\mathcal{H}(S)| |\mathcal{D}_i|}, \text{ for } i = 0, 1, 2.$$

We require the following notations from (section 2, Babu and Mukhopadhyay (2022)) for the proof of the Theorem 2.4.2.

### 2.4.1 Notations

We define a map,  $\chi : (\mathbf{P}(S), \Delta) \rightarrow (\mathbb{F}_2^n, +)$ , by

$$\chi(T) = (\chi_T(a_1), \dots, \chi_T(a_n)),$$

where for every subset  $T \subseteq S$ ,  $\chi_T : S \rightarrow \{0, 1\}$  denotes the characteristic function of  $T$ , i.e., if  $a_i \in T$ , then  $\chi_T(a_i) = 1$ , otherwise  $\chi_T(a_i) = 0$ .

It is easy to see that  $\chi$  is an isomorphism. Also, observe that  $\mathbb{F}_2^n$  is a vector space over the field  $\mathbb{F}_2$ .

For any  $u = (u_1, u_2, \dots, u_n), v = (v_1, v_2, \dots, v_n) \in \mathbb{F}_2^n$ ,

$$\langle u, v \rangle = (u_1 v_1 + \dots + u_n v_n) \pmod{2},$$

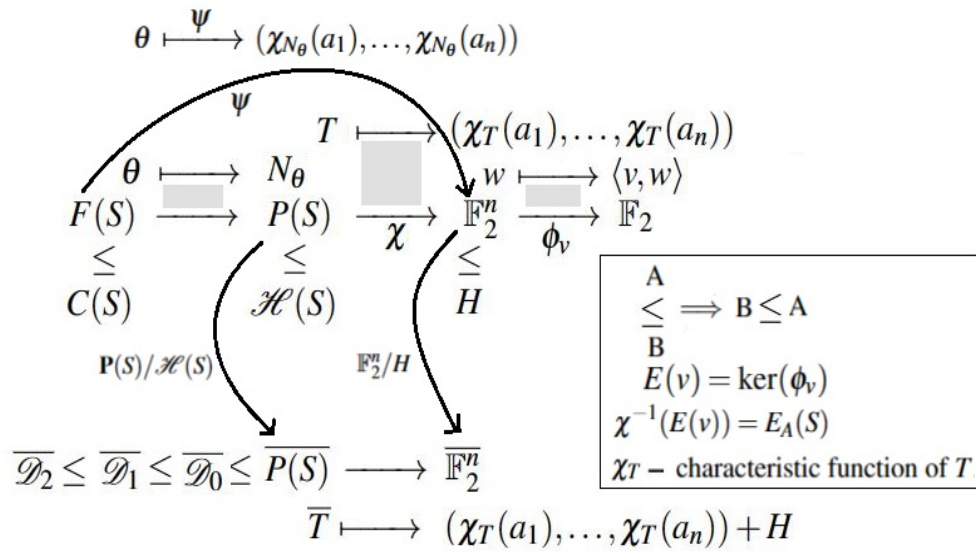


Figure 2.1 Various functions and maps involved in this chapter

defines a symmetric bilinear form on  $\mathbb{F}_2^n$ . Thus for any  $v \in \mathbb{F}_2^n$ , the map  $\phi_v : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$  defined by  $\phi_v(w) = \langle v, w \rangle$  is a linear functional with the kernel

$$E(v)(= \ker(\phi_v)) = \{w \in \mathbb{F}_2^n : \langle v, w \rangle = 0\}. \quad (2.4.3)$$

Clearly,  $E(v)$  is a proper maximal subspace of  $\mathbb{F}_2^n$  for any nonzero  $v \in \mathbb{F}_2^n$ .

We observe that

$$\chi^{-1}(E(v)) = E_A(S) = \{T \in \mathbf{P}(S) : |T \cap A| \text{ is even}\}, \text{ where } \chi(A) = v. \quad (2.4.4)$$

Also, we see that

$$H = \chi(\mathcal{H}(S)) = \{\chi(T) : T \in \mathcal{H}(S)\}$$

is a subgroup and hence a subspace of  $\mathbb{F}_2^n$ . Thus, we consider the quotient space  $\overline{\mathbb{F}_2^n} = \mathbb{F}_2^n/H$  which is isomorphic to  $\overline{\mathbf{P}(S)}$  by

$$\overline{\chi(T)} = (\chi_T(a_1), \dots, \chi_T(a_n)) + H.$$

Then  $\overline{D_i} = \overline{\chi(\mathcal{D}_i)}$  are subspaces of  $\overline{\mathbb{F}_2^n}$  for  $i = 0, 1, 2$ .

On the other hand, for any  $1 \leq f < d$  with  $(f, d) = 1$ , we consider a map  $\eta_f : S \rightarrow \{-1, 1\}$  by  $\eta_f(a_i) = \left(\frac{a_i}{f}\right)$ , for  $i = 1, 2, \dots, n$ . By the completely multiplicative property of Legendre symbol,  $\eta_f$  can be defined on  $\mathbf{P}(S)$  as follows

$$\eta_f(T) = \prod_{a_i \in T} \left(\frac{a_i}{f}\right) = \left(\frac{\prod_{a_i \in T} a_i}{f}\right) = \left(\frac{\text{sqf}(T)}{f}\right).$$

For every  $T \in \mathcal{H}(S)$ , it is easy to see that  $\eta_f(T) = 1$ . Equivalently, we have  $\mathcal{O}_{N_{\eta_f}}(S) = \emptyset$  which implies  $\eta_f \in \mathbf{C}(S)$ .

**Proof of Theorem 2.4.2:**

Observe that  $\mathbf{F}(S)$  is isomorphic to  $\mathbf{P}(S)$  through the map  $\theta \rightarrow N_\theta$ , and by the relation  $N_{\theta_1 \cdot \theta_2} = N_\theta \triangle N_{\theta_2}$ .

Therefore, define a map  $\psi : \mathbf{F}(S) \rightarrow \mathbb{F}_2^n$  by

$$\psi(\theta) = (\chi_{N_\theta}(a_1), \dots, \chi_{N_\theta}(a_n)).$$

Clearly,  $\psi$  is an isomorphism since it is a composition of two isomorphisms. Recall from the definition of  $\mathbf{C}(S)$  that a choice of signs  $\theta \in \mathbf{C}(S)$  if and only if  $|T \cap N_\theta|$  is even for all  $T \in \mathcal{H}(S)$ .

Thus, it follows from (2.4.4) that for a vector  $v \in \mathbb{F}_2^n$ , the kernel of corresponding linear functional  $\phi_v \in (\mathbb{F}_2^n)^*$  defined as in (2.4.3) contains  $H$  if and only if  $v \in \psi(\mathbf{C}(S))$ .

Thus, the map  $\phi_v$  induces a linear functional

$$\overline{\phi}_v : \overline{\mathbb{F}_2^n} \rightarrow \mathbb{F}_2 \text{ by } \overline{\phi}_v(\overline{w}) = \phi_v(w)$$

if and only if  $v \in \psi(\mathbf{C}(S))$ .

Also, it follows from (Theorem 2, Babu and Mukhopadhyay (2022)) that

$$|\psi(\mathbf{C}(S))| = \frac{2^n}{|H|}.$$

Denote  $\psi(\eta_f) = x$ . Since  $\eta_f \in \mathbf{C}(S)$ , the map  $\phi_x$  induces a linear functional on  $\overline{\mathbb{F}_2^n}$ . Our aim is to prove

$$|\mathbf{D}_i(S)| = \frac{2^{|S|} \varphi(d)}{|\mathcal{H}(S)| |\overline{\mathcal{D}}_i|},$$

for  $i = 0, 1, 2$ .

It is enough to prove that, for every  $1 \leq f < d$  with  $(f, d) = 1$ ,

$$|E_f| = |\{v \in \psi(\mathbf{C}(S)) : \overline{\phi}_v(\overline{t}) = \overline{\phi}_x(\overline{t}), \forall \overline{t} \in \overline{\mathcal{D}}_i\}| = \frac{|\psi(\mathbf{C}(S))|}{|\overline{\mathcal{D}}_i|} \text{ for } i = 0, 1, 2.$$

Equivalently,

$$|E_f| = |\{v \in \psi(\mathbf{C}(S)) : \overline{\phi}_{v+x}(\overline{t}) = 0, \forall \overline{t} \in \overline{\mathcal{D}}_i\}| = \frac{|\psi(\mathbf{C}(S))|}{|\overline{\mathcal{D}}_i|} \text{ for } i = 0, 1, 2. \quad (2.4.5)$$

Now, following the same arguments as discussed in (Theorem 2, Babu and Mukhopadhyay (2022)), we obtain

$$|E_{f+x}| = \frac{|\psi(\mathbf{C}(S))|}{|\overline{\mathcal{D}}_i|}$$

for  $i = 0, 1, 2$ . Thus, we conclude (2.4.5) holds for every  $1 \leq f < d$  with  $(f, d) = 1$ .

This completes the proof of Theorem 2.4.2.  $\square$



## Chapter 3

### Explicit Galois group of $\mathbb{Q}(\sqrt{a_1}, \dots, \sqrt{a_n}, \zeta_d)$ over $\mathbb{Q}$

We know that the degree of the multi-quadratic field  $\mathbb{Q}(\sqrt{a_1}, \sqrt{a_2}, \dots, \sqrt{a_n})$  over  $\mathbb{Q}$  is bound to be  $2^t$  for some non-negative integer  $t \leq n$ , where  $t$  depends on the algebraic cancellations among the  $\sqrt{a_i}$ 's. The arithmetic of multi-quadratic number fields plays a crucial role in the theory of elliptic curves (see Abel-Hollinger and Zimmer (1995), Laska and Lorenz (1985)). Balasubramanian et al. (2010) obtained an exact formula for the degree of the multi-quadratic field extensions  $\mathbb{Q}(\sqrt{a_1}, \sqrt{a_2}, \dots, \sqrt{a_n})$  over  $\mathbb{Q}$ . Recently Babu and Mukhopadhyay (2022) calculated the explicit structure of the Galois group of these multi-quadratic fields.

For a positive integer  $d \geq 3$ ,  $\zeta_d$  denotes a primitive  $d$ -th root of unity. In this chapter, we calculate the explicit structure of the Galois group of  $\mathbb{Q}(\sqrt{a_1}, \sqrt{a_2}, \dots, \sqrt{a_n}, \zeta_d)$  over  $\mathbb{Q}$  in terms of its action on  $\zeta_d$  and  $\sqrt{a_i}$  for  $1 \leq i \leq n$ .

The explicit structure of the Galois group of  $\mathbb{Q}(\sqrt{a_1}, \dots, \sqrt{a_n}, \zeta_{d_1}, \dots, \zeta_{d_k})$  over  $\mathbb{Q}$  will be discussed in Corollary 3.2.2. Here  $\zeta_{d_i}$  denotes the primitive  $d_i$ -th roots of unity, for  $1 \leq i \leq k$ .

#### 3.1 The degree of $\mathbb{Q}(\sqrt{a_1}, \sqrt{a_2}, \dots, \sqrt{a_n}, \zeta_d)$ over $\mathbb{Q}$

In this section, we give an exact formula for the degree of  $\mathbb{Q}(\sqrt{a_1}, \sqrt{a_2}, \dots, \sqrt{a_n}, \zeta_d)$  over  $\mathbb{Q}$ . Recalling Chebotarev's Density Theorem, as we use it to find the density of primes satisfying certain conditions which will be discussed in this section.

### Chebotarev's Density Theorem

Let  $\mathbb{K}/\mathbb{Q}$  be a Galois extension with Galois group  $\text{Gal}(\mathbb{K}/\mathbb{Q})$ . Let  $\sigma_p$  be its conjugacy class in  $\text{Gal}(\mathbb{K}/\mathbb{Q})$ . For any rational unramified prime  $p$ , let  $\sigma_p$  be a Frobenius element in  $\text{Gal}(\mathbb{K}/\mathbb{Q})$ . Then the relative density of the primes  $\{p : \sigma_p = C\}$  is  $\frac{|C|}{|\text{Gal}(\mathbb{K}/\mathbb{Q})|}$ .

We will need the behaviour of unramified primes using the following well-known Lemma.

**Lemma 3.1.1.** *Let  $m$  be a square-free integer let  $K = \mathbb{Q}(\sqrt{m})$  be a quadratic extension over  $\mathbb{Q}$ . Let  $O_K$  denote the ring of integers of  $K$ . Then for any odd prime  $p \geq 3$ , we have*

- (i)  $p$  ramifies in  $O_K$  if and only if  $p \mid m$ .
- (ii)  $p$  splits completely in  $O_K$  iff  $m$  is a square modulo  $p$ , or  $\left(\frac{m}{p}\right) = 1$ .
- (iii)  $p$  is inert in  $O_K$  iff  $m$  is not a square modulo  $p$ , i.e.,  $\left(\frac{m}{p}\right) = -1$ .

The number fields here are contained in a cyclotomic extensions, hence the Galois groups are abelian. Hence now we have a degree theorem for the multi-quadratic fields with cyclotomic extensions:

**Theorem 3.1.2.** *Let  $S = \{a_1, a_2, \dots, a_n\}$  be a finite subset of non-zero integers. Let  $\mathbb{K} = \mathbb{Q}(\sqrt{a_1}, \sqrt{a_2}, \dots, \sqrt{a_n}, \zeta_d)$  be a multi-quadratic field compositum with cyclotomic extension, where  $\zeta_d$  denotes the primitive  $d$ -th root of unity for  $d \geq 3$ . Then, we have*

$$[\mathbb{K} : \mathbb{Q}] = \frac{2^n \varphi(d)}{|\mathcal{H}(S)| |\mathcal{D}_0|}.$$

Note that, in the statement of Theorem 3.1.2, we assume  $8 \mid d$ . The proof of the other two cases follows similarly.

*Proof.* Since  $\mathbb{K}$  is a 2-elementary Abelian extension compositum with cyclotomic extension of  $\mathbb{Q}$ , we have  $\text{Gal}(\mathbb{K}/\mathbb{Q}) \simeq \mathbb{F}_2^t \times \mathbb{Z}_d^*$  for some  $1 \leq t \leq n$ .

In fact, if

$$f(x) = (x^2 - a_1)(x^2 - a_2) \dots (x^2 - a_n)(x^d - 1) \in \mathbb{Z}[x],$$

then  $\mathbb{K}/\mathbb{Q}$  is the splitting field of  $f(x)$ . Let

$$\mathbf{P}_1 := \{p > 2 : p \equiv 1 \pmod{d}, \left(\frac{a_i}{p}\right) = 1, \forall 1 \leq i \leq n\}.$$

Since  $\left(\frac{\text{sqf}(\bar{T})}{1}\right) = 1$ , for all  $\bar{T} \in \overline{\mathbf{P}}(S)$ , from Corollary 2.3.9, it follows that the density of  $\mathbf{P}_1$  is  $\frac{|\mathcal{H}(S)||\overline{\mathcal{D}}_0|}{2^n \varphi(d)}$ . Now, we will use Chebotarev's Density Theorem to calculate the relative density of  $\mathbf{P}_1$ .

To proceed as such, for  $p \in \mathbf{P}_1$ , we want to calculate the Frobenius element  $\sigma_p \in \text{Gal}(\mathbb{K}/\mathbb{Q})$ . It is enough to find the action of  $\sigma_p$  on  $\zeta_d$  and  $\sqrt{a_i}$  for each  $i$ .

Since  $p \equiv 1 \pmod{d}$ ,  $\sigma_p$  restricted to  $\mathbb{Q}(\zeta_d)$  is the identity. Also, since  $p \in \mathbf{P}_1$ , it follows from Lemma 4.1.7 that  $p$  splits completely in  $\mathbb{Q}(\sqrt{a_i})$ , for  $1 \leq i \leq n$ . Therefore, the Frobenius element  $\sigma_p \in \text{Gal}(\mathbb{K}/\mathbb{Q})$  satisfies

$$\sigma_p(\zeta_d) = \zeta_d \text{ and } \sigma_p(\sqrt{a_i}) = \sqrt{a_i},$$

for  $1 \leq i \leq n$ . Thus,  $\sigma_p$  is defined uniquely in  $\text{Gal}(\mathbb{K}/\mathbb{Q})$ . By the Chebotarev Density Theorem, the relative density of  $\mathbf{P}_1$  is

$$\frac{1}{[\mathbb{K} : \mathbb{Q}]} = \frac{|\mathcal{H}(S)||\overline{\mathcal{D}}_0|}{2^n \varphi(d)}.$$

This completes the proof of Theorem 3.1.2. □

### 3.2 The explicit Galois group of $\mathbb{Q}(\sqrt{a_1}, \sqrt{a_2}, \dots, \sqrt{a_n}, \zeta_d)$ over $\mathbb{Q}$

Now we discuss the explicit structure of the Galois group of  $\mathbb{Q}(\sqrt{a_1}, \sqrt{a_2}, \dots, \sqrt{a_n}, \zeta_d)$  over  $\mathbb{Q}$ . Precisely, we prove the following Theorem.

**Theorem 3.2.1.** *Let  $S = \{a_1, a_2, \dots, a_n\}$  be a finite set of non-zero integers. Let  $\mathbb{K} = \mathbb{Q}(\sqrt{a_1}, \sqrt{a_2}, \dots, \sqrt{a_n}, \zeta_d)$  denotes a multi-quadratic field compositum with cyclotomic extension, where  $\zeta_d$  denotes the primitive  $d$ -th root of unity for  $d \geq 3$ . Let  $(\mathbf{D}_0(S), *)$  be defined as in (2.4.2). Then there exists an explicit isomorphism between  $\mathbf{D}_0(S)$  and  $\text{Gal}(\mathbb{K}/\mathbb{Q})$ .*

Note that in the statement of Theorem 3.2.1, we assume  $8 \mid d$ . Recall that  $\mathbf{D}_0(S) = \left\{ (f, \theta) \in \mathbb{Z}_d^* \times \mathbf{C}(S) : \overline{\mu}_f^\theta(\bar{T}) = \theta(\bar{T}) \left( \frac{\text{sqf}(\bar{T})}{f} \right) = 1, \forall \bar{T} \in \overline{\mathcal{D}}_0 \right\}$ , where  $\overline{\mathcal{D}}_0 = \left\{ \bar{T} \in \overline{\mathbf{P}}(S) : |\text{sqf}(\bar{T})| \mid d \right\}$ . The proof for the other two cases follows similarly.

*Proof.* Since  $\mathbb{K}$  is a 2-elementary abelian extension compositum with cyclotomic extension of  $\mathbb{Q}$ , we have  $\text{Gal}(\mathbb{K}/\mathbb{Q}) \simeq \mathbb{F}_2^t \times \mathbb{Z}_d^*$  for some  $1 \leq t \leq n$ .

On the other hand, since  $F(S) \simeq \mathbb{F}_2^n$ , by using Lemma 2.4.1, we obtain that  $\mathbf{D}_0(S) \simeq \mathbb{F}_2^t \times \mathbb{Z}_d^*$  for some  $1 \leq t \leq n$ .

Also, it follows from Theorem 2.4.2 and Theorem 3.1.2 that

$$|\mathbf{D}_0(S)| = |\text{Gal}(\mathbb{K}/\mathbb{Q})| = \frac{2^n \varphi(d)}{|\mathcal{H}(S)||\overline{\mathcal{D}}_0|}.$$



Hence, we have  $(\text{Gal}(\mathbb{K}/\mathbb{Q}), \circ) \simeq (\mathbf{D}_0(S), *)$ .

In the rest of the proof, we show that there exists an explicit injective homomorphism between  $\text{Gal}(\mathbb{K}/\mathbb{Q})$  and  $\mathbf{D}_0(S)$ .

Let

$$\mathbf{P}(f, \theta) := \{p > 2 : p \equiv f \pmod{d}, \left(\frac{a_i}{p}\right) = \theta(a_i), \forall 1 \leq i \leq n\}.$$

By using Corollary 4.1.8, it follows that  $\mathbf{P}(f, \theta)$  contains infinitely many primes, for every  $\theta \in \mathbf{D}_0(S)$ . In fact, the relative density of  $\mathbf{P}(f, \theta)$  over the set of all primes  $\mathbf{P}$  is  $\frac{|\mathcal{H}(S)| |\overline{\mathcal{D}_0}|}{2^n \varphi(d)}$ .

For any  $p \in \mathbf{P}(f, \theta)$ , we want to calculate the Frobenius element  $\sigma_p \in \text{Gal}(\mathbb{K}/\mathbb{Q})$ . It is enough to find the action of  $\sigma_p$  on  $\zeta_d$  and  $\sqrt{a_i}$  for each  $i$ .

By using the definition of  $\mathbf{P}(f, \theta)$  and Lemma 4.1.7, we obtain that  $p$  either splits completely or is inert in  $\mathbb{Q}(\sqrt{a_i})$  respectively if  $a_i \in S \setminus N_\theta$  or  $a_i \in N_\theta$ .

Since  $p \equiv f \pmod{d}$ , the Frobenius element  $\sigma_p(\zeta_d) = \zeta_d^f$ . Therefore, for any  $p \in \mathbf{P}(f, \theta)$  the Frobenius element  $\sigma_p \in G$  satisfies

$$\sigma_p(\sqrt{a_i}) = \theta(a_i) \sqrt{a_i} = \begin{cases} \sqrt{a_i}, & \text{if } a_i \in S \setminus N_\theta \\ -\sqrt{a_i}, & \text{if } a_i \in N_\theta, \end{cases}$$

for  $1 \leq i \leq n$  and  $\sigma_p(\zeta_d) = \zeta_d^f$ . Hence  $\sigma_p$  is defined uniquely in  $\text{Gal}(\mathbb{K}/\mathbb{Q})$ .

Now, we define a map  $\Delta : \mathbf{D}_0 \rightarrow \text{Gal}(\mathbb{K}/\mathbb{Q})$  by

$$\Delta((f, \theta)) = \sigma_p, \text{ for some } p \in \mathbf{P}(f, \theta).$$

Clearly,  $\Delta$  is a well-defined and injective map. We claim that  $\Delta$  is a homomorphism.

Suppose  $\Delta((f_1, \theta_1)) = \sigma_{p_1}$  and  $\Delta((f_2, \theta_2)) = \sigma_{p_2}$ , with  $p_1 \in \mathbf{P}(f_1, \theta_1)$  and  $p_2 \in \mathbf{P}(f_2, \theta_2)$ , then

$$\Delta((f_1, \theta_1)) \circ \Delta((f_2, \theta_2))(\sqrt{a_i}) = \sigma_{p_1}(\sigma_{p_2}(\sqrt{a_i})) = \begin{cases} \sqrt{a_i}, & \text{if } a_i \in S \setminus (N_{\theta_1} \Delta N_{\theta_2}) \\ -\sqrt{a_i}, & \text{if } a_i \in N_{\theta_1} \Delta N_{\theta_2} \end{cases}$$

for  $1 \leq i \leq n$  and

$$\Delta((f_1, \theta_1)) \circ \Delta((f_2, \theta_2))(\zeta_d) = \sigma_{p_1}(\sigma_{p_2}(\zeta_d)) = \sigma_{p_1}(\zeta_d^{f_2}) = \zeta_d^{f_1 f_2 \pmod{d}} = \zeta_d^f,$$

where  $f \equiv f_1 f_2 \pmod{d}$ .

On the other hand, let  $\Delta((f, \theta_1 \cdot \theta_2)) = \sigma_p$ , where  $p \in \mathbf{P}(f, \theta_1 \cdot \theta_2)$  and  $f \equiv f_1 f_2 \pmod{d}$ . Then by the definition of  $\sigma_p$  and the relation  $N_{\theta_1 \cdot \theta_2} = N_{\theta_1} \Delta N_{\theta_2}$ , we obtain

$$\sigma_p(\sqrt{a_i}) = \begin{cases} \sqrt{a_i}, & \text{if } a_i \in S \setminus (N_{\theta_1} \Delta N_{\theta_2}) \\ -\sqrt{a_i}, & \text{if } a_i \in N_{\theta_1} \Delta N_{\theta_2} \end{cases}$$

for  $1 \leq i \leq n$  and  $\sigma_p(\zeta_d) = \zeta_d^f$ .

Thus we have,

$$\Delta((f_1, \theta_1)) \circ \Delta((f_2, \theta_2)) = \Delta((f_1, \theta_1) \cdot (f_2, \theta_2))$$

This completes the proof of Theorem 3.2.1. □

In the case of multi-quadratic and multi-cyclotomic extensions, the Galois group of such fields can be brought down to our problem of multi-quadratic and cyclotomic extensions. The following Corollary deals with it.

**Corollary 3.2.2.** *Let  $S = \{a_1, a_2, \dots, a_n\}$  be a finite set of non-zero integers and let  $3 \leq d_1 \leq \dots \leq d_k$  be integers with  $d = \text{lcm}(d_1, \dots, d_k)$ . Let  $\mathbb{L} = \mathbb{Q}(\sqrt{a_1}, \dots, \sqrt{a_n}, \zeta_{d_1}, \dots, \zeta_{d_k})$  be a multi-quadratic field compositum with several cyclotomic extensions, where  $\zeta_{d_i}$  denotes the primitive  $d_i$ -th root of unity, for  $i = 1, \dots, k$ . Let  $(\mathbf{D}_i(S), *)$  is defined as in (2.4.2), for  $d = \text{lcm}(d_1, \dots, d_k)$ ,  $i = 0, 1, 2$ . Then, there is an explicit isomorphism between  $\mathbf{D}_0(S)$  and  $\text{Gal}(\mathbb{L}/\mathbb{Q})$ .*

*Here, we assume  $8 \mid d$ . The proof for the other two cases follows similarly.*

The Proof of Corollary 3.2.2 follows similar to Theorem 3.2.1.



## Chapter 4

### Non-primitive roots with prescribed residue pattern

Given a set of primes  $S$ , the limit

$$\delta(S) = \lim_{x \rightarrow \infty} \frac{|\{p \leq x : p \in S\}|}{|\{p \leq x\}|},$$

if it exists, is called the natural density of  $S$ . An integer  $g$  with  $|g| > 1$  is a primitive root modulo  $p$  if  $p \nmid g$  and the multiplicative order of  $g$  modulo  $p$  ( $\text{ord}_p(g)$ ) equals  $p - 1$ .

Let  $\mathcal{P}_g$  be the set of primes  $p$  such that  $g$  is a primitive root modulo  $p$ . In 1927, E. Artin conjectured that there exist infinitely many primes  $p$  for which  $g$  is primitive root modulo  $p$  if  $g$  is not a square. Moreover, he also gave a conjectural formula for natural density  $\delta(\mathcal{P}_g)$ . In 1967, Hooley (1967a) proved Artin's conjecture under the Generalized Riemann Hypothesis (GRH) and determined  $\delta(\mathcal{P}_g)$ . In 1976, Matthews (1976) generalized Hooley's result under the assumption of GRH. Precisely, he proved that given nonzero integers  $a_1, \dots, a_n$ , there exists a non-negative constant  $C = C(a_1, \dots, a_n)$  such that

$$|\{p \leq x : \text{ord}_p(a_i) = p - 1, \forall i = 1, 2, \dots, n\}| = C \frac{x}{\log x} + O\left(\frac{(\log \log x)^{2^n - 1}}{(\log x)^2}\right).$$

Under GRH, the distribution of primes in a prescribed arithmetic progression for which  $g$  is primitive root modulo  $p$  is also studied in the literature; (see, Lenstra et al. (2014); Moree (1999, 2008)). We generalize the prescribed pattern by P. Moree, considering the set  $S$ , as mentioned earlier, instead of an element  $g$ .

On the other hand, for a prime  $p$ , if an integer  $g$  generates a subgroup of index  $t$  in  $(\mathbb{Z}/p\mathbb{Z})^*$ , then we say that  $g$  is a  $t$ -near primitive root modulo  $p$ . As mentioned in 1, Using the notations of Moree and Sha (2019), we have

$$\mathcal{P}_g(t) = \{p : p \nmid g, p \equiv 1 \pmod{t}, \text{ord}_p(g) = p - 1/t\},$$

$$\mathcal{P}_g(t, d, f) = \{p : p \equiv f \pmod{d}, p \in \mathcal{P}_g(t)\}.$$

Assuming GRH, Moree (2013) determined  $\delta(\mathcal{P}_g(t))$  when  $g > 1$  is squarefree.

Also as mentioned in 1, for  $t \geq 1$ ,  $g \notin \{-1, 0, 1\}$  and positive coprime integers  $f, d$ , we make use of the following sets defined by Moree and Sha (2019):

$$\mathcal{Q}_g(t, d, f) = \{p : p \equiv f \pmod{d}, \text{ord}_p(g) \neq (p - 1)/t\},$$

$$\mathcal{R}_g(t, d, f) = \{p : p \nmid bg, p \equiv f \pmod{d}, p \equiv 1 \pmod{t} \text{ and } \text{ord}_p(g) \mid (p - 1)/t\}.$$

They showed that for any integer  $q > 2$  and coprime to  $2dt$ , the set  $\mathcal{Q}_g(t, d, f)$  contains a subset of primes  $p$  having natural density  $\frac{1}{[\mathbb{Q}(\zeta_d, \zeta_{qt}, g^{1/q}) : \mathbb{Q}]}$ .

Further, suppose the set  $\mathcal{R}_g(t, d, f)$  is nonempty, then they showed that for any integer  $q > 2$  and coprime to  $2gdt$ , the set  $\mathcal{R}_g(t, d, f)$  contains a subset of primes  $p$  for which  $g$  is a non  $t$ -near primitive root modulo  $p$  having natural density  $\frac{1}{[\mathbb{Q}(\zeta_d, \zeta_{qt}, g^{1/qt}) : \mathbb{Q}]}$ .

Before describing our results, we define the quadratic residue pattern and discuss a few results.

Let  $S = \{a_1, a_2, \dots, a_n\}$  be a set of nonzero integers. In 1968, Fried (1968) showed that there are infinitely many primes  $p$  for which all the elements of  $S$  are quadratic residues. He also provided a necessary and sufficient condition for  $a_i$ 's to be quadratic nonresidues modulo  $p$ . In 2010, Balasubramanian et al. (2010) calculated the exact density of such primes in Fried's result. Earlier Wright (2007, 2008) had considered the above result qualitatively.

Recently Babu and Mukhopadhyay (2022), calculated the exact density of the set of primes for which  $S$  has residue pattern  $\theta$  modulo  $p$ . In chapter 2, we obtained the exact density of the set of primes  $p$  of the form  $p \equiv f \pmod{d}$  for which  $S$  has residue pattern

$\theta$  modulo  $p$ . Also, a necessary and sufficient condition for a choice of signs  $\theta$  for  $S$  to be a residue pattern modulo  $p$  for infinitely many primes of the form  $p \equiv f \pmod{d}$  was obtained.

Suppose  $S = \{a_1, a_2, \dots, a_n\}$  be a set of nonzero integers such that for any nonempty subset  $T$  of  $S$ , the product of all the elements in  $T$  is not a perfect square. For such a set, Dey and Kumar (2016), gave a lower bound for the density of the set of primes  $p$  for which the  $a_i$ 's are quadratic nonresidues but not primitive roots modulo  $p$ .

Let  $S = \{a_1, a_2, \dots, a_n\}$  be a subset of  $\mathbb{Z} \setminus \{0\}$  with a choice of signs  $\theta$  for  $S$ . In this paper, we give a lower bound for the density of primes in arithmetic progression for which the elements of  $S$  are not  $t$ -near primitive roots and satisfy a residue pattern  $\theta \pmod{p}$ .

For a positive integer  $t$  and positive coprime integers  $f, d$ , we define:

$$\mathcal{Q}_S(t, d, f, \theta) = \left\{ p : p \in \mathcal{Q}_{a_i}(t, d, f), \text{ and } \left( \frac{a_i}{p} \right) = \theta(a_i), \text{ for } i = 1, 2, \dots, n \right\},$$

$$\mathcal{R}_S(t, d, f, \theta) = \left\{ p : p \in \mathcal{R}_{a_i}(t, d, f) \text{ and } \left( \frac{a_i}{p} \right) = \theta(a_i), \text{ for } i = 1, 2, \dots, n \right\}.$$

In Theorem 4.2.1, we give a lower bound for the density of  $\mathcal{Q}_S(t, d, f, \theta)$ . Precisely, we show that the set  $\mathcal{Q}_S(t, d, f, \theta)$  contains a positive density subset of primes under a specific condition on  $\theta$ . In Theorem 4.3.1, we give a lower bound for the density of  $\mathcal{R}_S(t, d, f, \theta)$ . Precisely, for an odd positive integer  $t$ , we show that the set  $\mathcal{R}_S(t, d, f, \theta) \cap \mathcal{Q}_S(t, d, f, \theta)$  contains a positive density subset of primes under a specific condition on  $\theta$ .

## 4.1 Preliminary lemmas

We require the following lemmas for the proof of the theorems.

**Lemma 4.1.1.** (Dey and Kumar (2016), Lemma 2)

1. Let  $L$  and  $M$  be finite extensions over  $\mathbb{Q}$  with  $L \cap M = \mathbb{Q}$ . If one is a normal extension over  $\mathbb{Q}$ , then  $L$  and  $M$  are linearly disjoint over  $\mathbb{Q}$ .
2. Let  $L$  and  $M$  be finite extensions over  $\mathbb{Q}$  and let  $LM$  be their compositum over  $\mathbb{Q}$ . Then  $[LM : \mathbb{Q}] = [L : \mathbb{Q}][M : \mathbb{Q}]$  if and only if  $L$  and  $M$  are linearly disjoint over  $\mathbb{Q}$ .

3. Let  $\{L_i : i \in I\}$  be a linearly disjoint family of Galois extensions over  $\mathbb{Q}$  and let  $\prod_{i \in I} L_i$  be the compositum of  $L_i$ 's over  $\mathbb{Q}$ . Then

$$\text{Gal} \left( \prod_{i \in I} L_i / \mathbb{Q} \right) \cong \prod_{i \in I} \text{Gal} (L_i / \mathbb{Q}).$$

**Lemma 4.1.2.** (Pg. 592, Dummit and Foote (2004)) Suppose  $L$  be a Galois extension over  $\mathbb{Q}$  and  $M$  be any finite extension over  $\mathbb{Q}$ . Then

$$[LM : \mathbb{Q}] = \frac{[L : \mathbb{Q}][M : \mathbb{Q}]}{[L \cap M : \mathbb{Q}]}.$$

Further, if  $L$  and  $M$  both are Galois extensions over  $\mathbb{Q}$ , then

1. the intersection  $L \cap M$  is Galois over  $\mathbb{Q}$ ,
2. the composite  $LM$  is Galois over  $\mathbb{Q}$  and the Galois group is isomorphic to the subgroup

$$H = \{(\sigma, \tau) : \sigma|_{L \cap M} = \tau|_{L \cap M}\}$$

of the direct product  $\text{Gal} (L/\mathbb{Q}) \times \text{Gal} (M/\mathbb{Q})$ .

**Lemma 4.1.3.** (Weintraub (2009), Corollary 4.5.5) Let  $m$  be a nonzero square-free integer. Let

$$m' = \begin{cases} |m| & \text{if } m \equiv 1 \pmod{4}, \\ 4|m| & \text{otherwise.} \end{cases}$$

Then  $\mathbb{Q}(\sqrt{m}) \subseteq \mathbb{Q}(\zeta_n)$  if and only if  $n$  is multiple of  $m'$ .

**Lemma 4.1.4.** (Weintraub (2009), Corollary 4.2.8) Let  $m$  and  $n$  be positive integers and set  $d = \gcd(m, n)$  and  $l = \text{lcm}(m, n)$ . Then  $\mathbb{Q}(\zeta_m)\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_l)$  and  $\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_d)$ .

In particular, if  $m$  and  $n$  are relatively prime, then  $\mathbb{Q}(\zeta_m)\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{mn})$  and  $\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}$ .

**Lemma 4.1.5.** Let  $a_1, a_2, \dots, a_n$  be distinct nonzero integers and let  $p$  be an odd prime and  $k$  be a positive odd integer. Then  $p \equiv 1 \pmod{k}$  and  $a_i^{(p-1)/k} \equiv 1 \pmod{p}$ , for all  $i = 1, 2, \dots, n$  if and only if  $p$  splits completely in  $\mathbb{Q}(\zeta_k, a_1^{1/k}, a_2^{1/k}, \dots, a_n^{1/k})$ , where  $\zeta_k$  is a primitive  $k$ -th root of unity.

The proof of Lemma 4.1.5 follows similarly to Proposition 8 of Dey and Kumar (2016).

**Lemma 4.1.6.** Let  $a = \pm a_0^h$ , where  $a_0$  is positive but not of an exact power of a rational. For any positive odd integer  $k$  and a positive integer  $r$ , we have

$$[\mathbb{Q}(\zeta_{kr})\mathbb{Q}(\zeta_k, a^{1/k}) : \mathbb{Q}] = [\mathbb{Q}(\zeta_{kr}, a^{1/k}) : \mathbb{Q}] = \frac{\varphi(kr)k}{(k, h)} \quad (4.1.1)$$

and thus for any odd prime  $q \nmid rk$ , we have

$$\mathbb{Q}(\zeta_{kr}) \cap \mathbb{Q}(\zeta_{qk}, a^{1/qk}) = \mathbb{Q}(\zeta_{kr}) \cap \mathbb{Q}(\zeta_k, a^{1/k}) = \mathbb{Q}(\zeta_k). \quad (4.1.2)$$

*Proof.* (4.1.1) follows from Lemma 1 of Moree (2005) and the assumption that  $k$  is odd. To prove (4.1.2), it is enough to prove

$$[\mathbb{Q}(\zeta_{kr}) \cap \mathbb{Q}(\zeta_{qk}, a^{1/qk}) : \mathbb{Q}] = [\mathbb{Q}(\zeta_{kr}) \cap \mathbb{Q}(\zeta_k, a^{1/k}) : \mathbb{Q}] = \varphi(k).$$

Using Lemma 4.1.2 and (4.1.1), we write

$$[\mathbb{Q}(\zeta_{kr}) \cap \mathbb{Q}(\zeta_{qk}, a^{1/qk}) : \mathbb{Q}] = \frac{[\mathbb{Q}(\zeta_{kr}) : \mathbb{Q}][\mathbb{Q}(\zeta_{qk}, a^{1/qk}) : \mathbb{Q}]}{[\mathbb{Q}(\zeta_{qkr}, a^{1/qk}) : \mathbb{Q}]} = \frac{\varphi(kr) \frac{\varphi(qk)qk}{(qk, h)}}{\frac{\varphi(qkr)qk}{(qk, h)}}.$$

Since  $q \nmid rk$  is an odd prime, we have

$$[\mathbb{Q}(\zeta_{kr}) \cap \mathbb{Q}(\zeta_{qk}, a^{1/qk}) : \mathbb{Q}] = \frac{(q-1)\varphi(kr)\varphi(k)}{(q-1)\varphi(kr)} = \varphi(k).$$

Similarly, by using (4.1.1) and Lemma 4.1.2, we obtain

$$[\mathbb{Q}(\zeta_{kr}) \cap \mathbb{Q}(\zeta_k, a^{1/k}) : \mathbb{Q}] = \frac{\varphi(kr) \frac{\varphi(k)k}{(k, h)}}{\frac{\varphi(kr)k}{(kr, h)}} = \varphi(k).$$

This completes the proof of Lemma 4.1.6.  $\square$

Let  $m$  be an integer and  $p \nmid m$  be a prime number. If  $m$  is a square modulo  $p$  we put  $\left(\frac{m}{p}\right) = 1$ , and  $\left(\frac{m}{p}\right) = -1$  otherwise.

**Lemma 4.1.7.** *Let  $m$  be a squarefree integer and let  $K = \mathbb{Q}(\sqrt{m})$  be a quadratic extension over  $\mathbb{Q}$ . Let  $O_K$  be the ring of integers of  $K$ . Then for any odd prime  $p \geq 3$ , we have*

- (i)  $p$  ramifies in  $O_K$  if and only if  $p \mid m$ .
- (ii)  $p$  splits completely in  $O_K$  if and only if  $\left(\frac{m}{p}\right) = 1$ .
- (iii)  $p$  is inert in  $O_K$  if and only if  $\left(\frac{m}{p}\right) = -1$ .

For any non-zero integer  $n$ , we denote the squarefree part of  $n$  by  $\text{sqf}(n)$ . For any finite subset  $T \subset \mathbb{Z} \setminus \{0\}$ , by  $\text{sqf}(T)$  we mean  $\text{sqf}(\prod_{s \in T} s)$ . Let  $S$  be a finite set of non-zero integers with a choice of signs  $\theta$  for  $S$ . For any nonempty subset  $T \subseteq S$ , we set

$$\theta(T) := \prod_{s \in T} \theta(s). \quad (4.1.3)$$



Let  $\mathbf{P}(S)$  denote the set of all subsets of  $S$ . It is well-known that  $(\mathbf{P}(S), \Delta)$  is an abelian group having identity element  $\emptyset$  isomorphic to  $(\mathbb{Z}/2\mathbb{Z})^{|S|}$ , where  $\emptyset$  denotes the empty subset.

**Lemma 4.1.8.** (Babu and Mukhopadhyay (2022), Corollary 4.1) *Let  $S$  be a finite set of non-zero integers with a choice of signs  $\theta$  for  $S$ . Let  $f, d$  be positive integers with  $1 \leq f \leq d$  and  $(f, d) = 1$ .*

**Case 1**  $4 \nmid d$

*There exist infinitely many primes  $p$  of the form  $p \equiv f \pmod{d}$  such that  $S$  has residue pattern  $\theta$  modulo  $p$  if and only if  $\theta(T) = \left(\frac{\text{sqf}(T)}{f}\right)$  for every  $T \in \mathcal{D}_2^d$ . In this case, the asymptotic density of primes of the form  $p \equiv f \pmod{d}$  for which  $S$  has residue pattern  $\theta$  modulo  $p$  is  $\frac{|\mathcal{D}_2^d|}{\varphi(d)2^{|S|}}$ .*

**Case 2**  $4 \mid d$  and  $8 \nmid d$

*There exist infinitely many primes  $p$  of the form  $p \equiv f \pmod{d}$  such that  $S$  has residue pattern  $\theta$  modulo  $p$  if and only if  $\theta(T) = \left(\frac{\text{sqf}(T)}{f}\right)$  for every  $T \in \mathcal{D}_1^d$ . In this case, the asymptotic density of primes of the form  $p \equiv f \pmod{d}$  for which  $S$  has residue pattern  $\theta$  modulo  $p$  is  $\frac{|\mathcal{D}_1^d|}{\varphi(d)2^{|S|}}$ .*

**Case 3**  $8 \mid d$

*There exist infinitely many primes  $p$  of the form  $p \equiv f \pmod{d}$  such that  $S$  has residue pattern  $\theta$  modulo  $p$  if and only if  $\theta(T) = \left(\frac{\text{sqf}(T)}{f}\right)$  for every  $T \in \mathcal{D}_0^d$ . In this case, the asymptotic density of primes of the form  $p \equiv f \pmod{d}$  for which  $S$  has residue pattern  $\theta$  modulo  $p$  is  $\frac{|\mathcal{D}_0^d|}{\varphi(d)2^{|S|}}$ .*

Recall from 3,

$$[K : \mathbb{Q}] = \frac{2^n \varphi(d)}{|\mathcal{D}_i^d(S)|},$$

where  $\mathcal{D}_i^d(S)$  is defined as in (2.3.2). Here

$$i = \begin{cases} 0 & \text{if } 8 \mid d, \\ 1 & \text{if } 4 \mid d \text{ and } 8 \nmid d, \\ 2 & \text{if } 4 \nmid d. \end{cases} \quad (4.1.4)$$

**Lemma 4.1.9.** *Let  $S = \{a_1, a_2, \dots, a_n\}$  be a finite set of non-zero integers and  $m$  be an odd positive integer. Let  $L = \mathbb{Q}(a_1^{\frac{1}{m}}, a_2^{\frac{1}{m}}, \dots, a_n^{\frac{1}{m}}, \zeta_m)$ . Then the degree of the extension  $L$  over  $\mathbb{Q}$  is given by*

$$[L : \mathbb{Q}] = \frac{m^n \varphi(m)}{|\mathcal{H}_m(S)|},$$

where

$$\mathcal{H}_m(S) = \{(r_1, \dots, r_n) \in (\mathbb{Z}/m\mathbb{Z})^n : \prod_{i=1}^n a_i^{r_i} = k^m, \text{ for some } k \in \mathbb{Z}\}. \quad (4.1.5)$$

*Proof.* From Theorem 3.7.11 of Weintraub (2009), it follows that

$$[L : \mathbb{Q}(\zeta(m))] = |\langle \bar{a}_1, \dots, \bar{a}_n \rangle|,$$

where  $\langle \bar{a}_1, \dots, \bar{a}_n \rangle$  denotes the subgroup of  $\mathbb{Q}(\zeta_m)^*/(\mathbb{Q}(\zeta_m)^*)^n$  generated by  $a_1, \dots, a_n$ .

Consider the  $\mathbb{Z}/m\mathbb{Z}$  free module  $(\mathbb{Z}/m\mathbb{Z})^n$  with the basis  $S = \{a_1, \dots, a_n\}$ . Observe that  $\mathbb{Z}/m\mathbb{Z}$  acts on  $\mathbb{Q}(\zeta_m)^*/(\mathbb{Q}(\zeta_m)^*)^n$  by  $\alpha \cdot x = x^\alpha$ .

Consider the map  $f : (\mathbb{Z}/m\mathbb{Z})^n \rightarrow \langle \bar{a}_1, \dots, \bar{a}_n \rangle$ , which sends  $a_i \rightarrow \bar{a}_i$  and extend it linearly. Then  $\sum_i r_i a_i \in \ker f$  if and only if  $(r_1, \dots, r_n) \in \mathcal{H}_m(S)$ . Therefore, we obtain

$$[L : \mathbb{Q}(\zeta(m))] = \frac{m^n}{|\mathcal{H}_m(S)|}.$$

Further, from the assumption that  $m$  is odd and Proposition 4.1 of S.S. Wagstaff (1982), it follows that

$$[L : \mathbb{Q}] = \frac{m^n \varphi(m)}{|\mathcal{H}_m(S)|}.$$

□

## 4.2 A positive density subset of $\mathcal{Q}_S(t, d, f, \theta)$

**Theorem 4.2.1.** *Let  $d, f$  be coprime positive integers and let  $S = \{a_1, a_2, \dots, a_n\}$  be a subset of  $\mathbb{Z} \setminus \{-1, 0, 1\}$  with a choice of signs  $\theta$  for  $S$ . Let  $t \geq 1$  be an integer and  $q$  be the least odd prime such that*

$$q \nmid dta_1a_2 \cdots a_n.$$

*Suppose  $\left(\frac{\text{sqf}(T)}{f}\right) = \theta(T)$  holds for every  $T \in \mathcal{D}_i^d(S)$ , where the values of  $i$  are defined as in (4.1.4). Then the set  $\mathcal{Q}_S(t, d, f, \theta)$  contains a positive density subset of primes  $p$  having natural density*

$$\frac{|\mathcal{H}_q(S)||\mathcal{D}_i^d(S)|}{\varphi(d)(q-1)(2q)^n},$$

where  $\mathcal{D}_i^d(S)$ ,  $\mathcal{H}_q(S)$  are defined as in (2.3.2), (4.1.5) respectively.

*Proof.* We assume  $8 \mid d$ . The proof for the other two cases follows similarly.

Consider the number fields:

$$L_q = \mathbb{Q}(a_1^{1/q}, a_2^{1/q}, \dots, a_n^{1/q}, \zeta_q) \text{ and } M_d = \mathbb{Q}(\sqrt{a_1}, \sqrt{a_2}, \dots, \sqrt{a_n}, \zeta_d).$$

Let  $L = L_q M_d$  be the compositum of  $L_q$  and  $M_d$ .

Since  $q$  is an odd prime such that  $q \nmid a_1 a_2 \cdots a_n$  (equivalently, there is no subset  $T$  of  $S$  with  $\text{sqf}(T) = q$ ), it follows from Lemma 4.1.3 that  $L_q \cap \mathbb{Q}(\sqrt{a_1}, \sqrt{a_2}, \dots, \sqrt{a_n}) = \mathbb{Q}$  and since  $q \nmid d$ , by using (4.1.2) with  $k = 1$ , we obtain  $L_q \cap \mathbb{Q}(\zeta_d) = \mathbb{Q}$ .

Therefore, by (1) of Lemma 4.1.1, we conclude that  $L_q$  and  $M_d$  are linearly disjoint over  $\mathbb{Q}$ , that is  $L_q \cap M_d = \mathbb{Q}$ . Thus, by (2) of Lemma 4.1.1, we obtain

$$[L : \mathbb{Q}] = [L_q : \mathbb{Q}][M_d : \mathbb{Q}]. \quad (4.2.1)$$

Since  $L_q$  and  $M_d$  both are Galois extensions over  $\mathbb{Q}$ , by (3) of Lemma 4.1.1, we have

$$\text{Gal}(L/\mathbb{Q}) \cong \text{Gal}(L_q/\mathbb{Q}) \times \text{Gal}(M_d/\mathbb{Q}). \quad (4.2.2)$$

Now, consider the set

$$\mathbf{P}(\theta, d, q) = \{p \in \mathbf{P} : p \equiv f \pmod{d}, p \text{ splits completely in } L_q, \left(\frac{a_i}{p}\right) = \theta(a_i), \forall 1 \leq i \leq n\},$$

where  $\mathbf{P}$  is the set of all prime numbers.

We write  $\mathbf{P}(\theta, d, q) = \mathbf{P}(\theta, d) \cap \mathbf{P}(q)$ , where

$$\begin{aligned} \mathbf{P}(q) &= \{p \in \mathbf{P} : p \text{ splits completely in } L_q\}, \\ \mathbf{P}(\theta, d) &= \{p \in \mathbf{P} : p \equiv f \pmod{d}, \left(\frac{a_i}{p}\right) = \theta(a_i), \forall 1 \leq i \leq n\}. \end{aligned}$$

For any prime  $p \in \mathbf{P}(\theta, d, q)$ , we want to calculate the Frobenius element  $\sigma_p \in \text{Gal}(L/\mathbb{Q})$ . We observe that  $p \in \mathbf{P}(q)$  if and only if  $\sigma|_{L_q}$  is an identity element of the Galois group  $\text{Gal}(L_q/\mathbb{Q})$ .

Since by the assumption that  $\left(\frac{\text{sqf}(T)}{f}\right) = \theta(T)$  holds for every  $T \in \mathcal{D}_0^d(S)$ , using Lemma 4.1.8, we see that  $\mathbf{P}(\theta, d)$  contains infinitely many primes with the relative density  $\frac{|\mathcal{D}_0^d|}{2^n \varphi(d)}$ .

Since for any  $p \in \mathbf{P}(\theta, d)$  is of the form  $p \equiv f \pmod{d}$ , the Frobenius element

$$\sigma_p|_{K_d}(\zeta_d) = \zeta_d^f.$$

Also, for any  $p \in \mathbf{P}(\theta, d)$  it follows from Lemma 4.1.7 that

$$\sigma|_{K_d}(\sqrt{a_i}) = \theta(a_i)\sqrt{a_i}, \text{ for } 1 \leq i \leq n.$$

Therefore, the Frobenius element  $\sigma_p \in \text{Gal}(L/\mathbb{Q})$  satisfies

$$\begin{aligned} \sigma_p(a_i^{1/q}) &= a_i^{1/q}, \quad \sigma_p(\sqrt{a_i}) = \theta(a_i)\sqrt{a_i}, \text{ for } 1 \leq i \leq n, \\ \sigma_p(\zeta_q) &= \zeta_q \text{ and } \sigma_p(\zeta_d) = \zeta_d^f. \end{aligned}$$

Since the Galois group  $\text{Gal}(K_d/\mathbb{Q})$  is abelian, by (4.2.2), we note that the conjugacy class of  $\sigma_p$  contains only one element which is nothing but  $\sigma_p$  itself. Therefore, by Chebotarev Density Theorem, the density of  $\mathbf{P}(\theta, d, q)$  is  $\frac{1}{[L:\mathbb{Q}]}$ .

Thus, by using Theorem 3.1.2 and Lemma 4.1.9 with (4.2.1), we conclude that the density of  $\mathbf{P}(\theta, d, q)$  is

$$\frac{|\mathcal{H}_q(S)||\mathcal{D}_0^d(S)|}{\varphi(d)(q-1)(2q)^n}.$$

Finally, from Lemma 4.1.5, we observe that any  $p \in \mathbf{P}(\theta, d, q)$  satisfies

$$p \equiv 1 \pmod{q} \text{ and } a_i^{(p-1)/q} \equiv 1 \pmod{p},$$

for all  $i = 1, 2, \dots, n$ .

Since we assume  $q \nmid t$ , it follows that  $\text{ord}_p(a_i) \neq \frac{p-1}{t}$ , for  $i = 1, 2, \dots, n$  and for all  $p \in \mathbf{P}(\theta, d, q)$ . Hence, for any prime  $p$  in  $\mathbf{P}(\theta, d, q)$  we have  $p \equiv f \pmod{d}$ ,  $a_1, a_2, \dots, a_n$  are non  $t$ -near primitive roots and have residue pattern  $\theta$  modulo  $p$ .

This completes the proof of the Theorem 4.2.1. □

### Example:

Consider the set  $S = \{2, 3, 6\}$  with a choice of signs  $\theta(2) = 1, \theta(3) = -1$  and  $\theta(6) = -1$ . Suppose  $t = 5, f = 7$  and  $d = 8$ . Then by definition of  $\mathcal{D}_i^d(S)$  we see that

$$\mathcal{D}_0^8(S) = \{\phi, \{2\}, \{3, 6\}, \{2, 3, 6\}\}.$$

We choose  $q = 7$  as it is the least prime that does not divide 2, 3, 6, 5, 8 and therefore we have  $\mathcal{H}_7(S) = \{\phi\}$ .

Since

$$\left(\frac{\text{sqf}(\phi)}{7}\right) = \theta(\phi) = 1, \quad \left(\frac{\text{sqf}(\{2\})}{7}\right) = \theta(\{2\}) = 1, \quad \left(\frac{\text{sqf}(\{3, 6\})}{7}\right) = \theta(\{3, 6\}) = 1$$

$$\left( \frac{\text{sqf}(\{2, 3, 6\})}{7} \right) = \theta(\{2, 3, 6\}) = 1,$$

by using Theorem 4.2.1, we obtain that the set  $\mathcal{D}_S(5, 8, 7, (1, -1, -1))$  contains a positive density subset of primes  $p$  having natural density

$$\frac{|\mathcal{H}_7(S)||\mathcal{D}_0^8(S)|}{4 \times 6 \times (14)^3} = \frac{4}{4 \times 6 \times (14)^3} = \frac{1}{16464}.$$

Computationally, it is found that  $\mathcal{D}_S(5, 8, 7, (1, -1, -1)) = \{271, 631, 751, 991, \dots\}$

### 4.3 A positive density subset of $\mathcal{R}_S(t, d, f, \theta)$

**Theorem 4.3.1.** *Let  $S = \{a_1, a_2, \dots, a_n\}$  be a subset of  $\mathbb{Z} \setminus \{-1, 0, 1\}$  with a choice of signs  $\theta$  for  $S$ . Let  $f, d$  be positive coprime integers such that  $f \equiv 1 \pmod{(d, t)}$ . Let  $q$  be the least odd prime such that  $q \nmid dt a_1 a_2 \cdots a_n$ .*

*Suppose  $\left( \frac{\text{sqf}(T)}{f} \right) = \theta(T)$  holds for every  $T \in \mathcal{D}_i^{rt}(S)$ , where the values of  $i$  are defined as in (4.1.4). Then the set  $\mathcal{R}_S(t, d, f, \theta)$  contains a subset of primes  $p$  for which each  $a_i \in S$  is a non  $t$ -near primitive root modulo  $p$  having natural density*

$$\frac{|\mathcal{H}_{qt}(S)||\mathcal{D}_i^{rt}(S)|}{\varphi(rt)(q-1)(2qt)^n},$$

where  $r$  is a positive integer satisfying  $[d, t] = rt$ ,  $\mathcal{D}_i^{rt}(S)$  and  $\mathcal{H}_{qt}(S)$  are defined as in (2.3.2) and (4.1.5) respectively.

*Proof.* We assume  $8 \mid d$ . The proof for the other two cases follows similarly.

Consider the number fields

$$L_{qt} = \mathbb{Q}(a_1^{1/qt}, a_2^{1/qt}, \dots, a_n^{1/qt}, \zeta_{qt}) \text{ and } M_{dt} = \mathbb{Q}(\sqrt{a_1}, \sqrt{a_2}, \dots, \sqrt{a_n}, \zeta_t, \zeta_d).$$

Let  $L = L_{qt}M_{dt}$  be the compositum of  $L_{qt}$  and  $M_{dt}$ .

Since we assume  $[d, t] = rt$ , by Lemma 4.1.4 we write  $M_{dt} = \mathbb{Q}(\sqrt{a_1}, \sqrt{a_2}, \dots, \sqrt{a_n}, \zeta_{rt})$ . Also, since  $qt$  is odd and  $q \nmid dt a_1 a_2 \cdots a_n$ , it follows from Lemma 4.1.3 and (4.1.2) that

$$L_{qt} \cap M_{dt} = \mathbb{Q}(\zeta_t).$$

Therefore, by Lemma 4.1.2, we obtain that

$$[L : \mathbb{Q}] = \frac{[L_{qt} : \mathbb{Q}][M_{dt} : \mathbb{Q}]}{[\mathbb{Q}(\zeta_t) : \mathbb{Q}]}, \quad (4.3.1)$$

and since  $L_{qt}$  and  $M_{dt}$  both are Galois extensions over  $\mathbb{Q}$ , we also have

$$\text{Gal}(L/\mathbb{Q}) \cong \{(\sigma, \tau) \in \text{Gal}(L_{qt}/\mathbb{Q}) \times \text{Gal}(M_{dt}/\mathbb{Q}) : \sigma|_{\mathbb{Q}(\zeta_t)} = \tau|_{\mathbb{Q}(\zeta_t)}\}. \quad (4.3.2)$$

Now, consider the sets

$$\mathbf{P}(q, t) = \{p \in \mathbf{P} : p \text{ splits completely in } L_{qt}\},$$

$$\mathbf{P}(\theta, t, d) = \{p \in \mathbf{P} : \left(\frac{a_i}{p}\right) = \theta(a_i), \forall 1 \leq i \leq n, p \equiv f \pmod{d}, p \equiv 1 \pmod{t}\}.$$

For any prime  $p \in \mathbf{P}(q, t)$ , we calculate the Frobenius element  $\sigma_p \in \text{Gal}(L_{qt}/\mathbb{Q})$ . We observe that  $p$  splits completely in  $L_{qt}$  if and only if  $\sigma_p$  is an identity element of the Galois group  $\text{Gal}(L_{qt}/\mathbb{Q})$ .

Therefore, the Frobenius element  $\sigma_p \in \text{Gal}(L_{qt}/\mathbb{Q})$  satisfies

$$\sigma_p(a_i^{1/qt}) = a_i^{1/qt}, \text{ for } 1 \leq i \leq n, \sigma_p(\zeta_{qt}) = \zeta_{qt}.$$

First, we want to show that  $\mathbf{P}(\theta, t, d)$  is non-empty, and then for any prime  $p \in \mathbf{P}(\theta, t, d)$ , we want to calculate the Frobenius element  $\tau_p \in \text{Gal}(M_{dt}/\mathbb{Q})$ .

Since we assume  $f \equiv 1 \pmod{(d, t)}$ , by the Chinese remainder theorem, the congruences  $x \equiv 1 \pmod{t}$  and  $x \equiv f \pmod{d}$  have a solution. Hence, by Dirichlet's theorem for primes in arithmetic progression, there are infinitely many primes  $p$  satisfying  $p \equiv f \pmod{d}$  and  $p \equiv 1 \pmod{t}$ .

From the assumption that  $\left(\frac{\text{sqf}(T)}{f}\right) = \theta(T)$  holds for every  $T \in \mathcal{D}_0^{rt}(S)$  and Lemma 4.1.8, we see that  $\mathbf{P}(\theta, t, d)$  contains infinitely many primes with the relative density  $\frac{|\mathcal{D}_0^{rt}|}{2^n \varphi(rt)}$ .

Since any  $p \in \mathbf{P}(\theta, t, d)$  satisfies  $p \equiv f \pmod{d}$  and  $p \equiv 1 \pmod{t}$ , the Frobenius element  $\tau_p$  satisfies  $\tau_p(\zeta_d) = \zeta_d^f$  and  $\tau_p(\zeta_t) = \zeta_t$ . Also, for any  $p \in \mathbf{P}(\theta, t, d)$  it follows from Lemma 4.1.7 that

$$\tau_p(\sqrt{a_i}) = \theta(a_i)\sqrt{a_i}, \text{ for } 1 \leq i \leq n.$$

Therefore, the Frobenius element  $\tau_p \in \text{Gal}(M_{dt}/\mathbb{Q})$  satisfies

$$\tau_p(\sqrt{a_i}) = \theta(a_i)\sqrt{a_i}, \text{ for } 1 \leq i \leq n, \tau_p(\zeta_t) = \zeta_t \text{ and } \tau_p(\zeta_d) = \zeta_d^f.$$

We write  $\mathbf{P}(\theta, d, q, t) = \mathbf{P}(\theta, t, d) \cap \mathbf{P}(q, t)$ .

For any  $p \in \mathbf{P}(\theta, d, q, t)$ , we observe that

$$\sigma|_{\mathbb{Q}(\zeta_t)} = \tau_p|_{\mathbb{Q}(\zeta_t)}.$$

Thus, from (4.3.2), it follows that  $(\sigma_p, \tau_p) \in \text{Gal}(L/\mathbb{Q})$ . Since  $\sigma_p$  acts as the identity element on  $\text{Gal}(L_{qt}/\mathbb{Q})$  and the Galois group  $\text{Gal}(M_{dt}/\mathbb{Q})$  is abelian, the conjugacy class of  $(\sigma_p, \tau_p)$  contains only one element which is just  $(\sigma_p, \tau_p)$ . Therefore, by Chebotarev Density Theorem, the density of  $\mathbf{P}(\theta, d, q, t)$  is  $\frac{1}{[L:\mathbb{Q}]}$ .

Thus, by using Lemma 3.1.2 and Lemma 4.1.9 with (4.3.1), we conclude that the density of  $\mathbf{P}(\theta, d, q, t)$  is

$$\frac{|\mathcal{H}_{qt}(S)| |\mathcal{D}_0^{rt}(S)|}{\varphi(rt)(q-1)(2qt)^n}.$$

Finally, from Lemma 4.1.5, we observe that any  $p \in \mathbf{P}(\theta, d, q, t)$  satisfies

$$p \equiv 1 \pmod{qt} \text{ and } a_i^{(p-1)/qt} \equiv 1 \pmod{p},$$

for all  $i = 1, 2, \dots, n$ .

Since we assume  $q \nmid t$ , it follows that  $\text{ord}_p(a_i) \neq \frac{p-1}{t}$ , but  $\text{ord}_p(a_i) \mid \frac{p-1}{t}$ , for  $i = 1, 2, \dots, n$  and for all  $p \in \mathbf{P}(\theta, d, q, t)$ . Hence,

$$\mathbf{P}(\theta, d, q, t) \subseteq \mathcal{R}_S(t, d, f, \theta),$$

but  $a_1, a_2, \dots, a_n$  are non  $t$ -near primitive roots for any prime  $p$  in  $\mathbf{P}(\theta, d, q, t)$ . This completes the proof of the Theorem 4.3.1.  $\square$

### Example-1:

Consider the set  $S = \{2, 3, 6\}$  with a choice of signs  $\theta(2) = -1, \theta(3) = -1$  and  $\theta(6) =$

1. Suppose  $t = 3, f = 5$  and  $d = 8$ . Then by definition of  $\mathcal{D}_i^d(S)$  we see that

$$\mathcal{D}_0^{24}(S) = \{\phi, \{2\}, \{3\}, \{6\}, \{2, 3\}, \{2, 6\}, \{3, 6\}, \{2, 3, 6\}\}.$$

We choose  $q = 5$  as it is the least prime that does not divide 2, 3, 6, 8 and therefore we have  $\mathcal{H}_{15}(S) = \{\phi\}$ .

Since

$$\begin{aligned} \left(\frac{\text{sqf}(\phi)}{5}\right) &= \theta(\phi) = 1, \quad \left(\frac{\text{sqf}(\{2\})}{5}\right) = \theta(\{2\}) = -1, \quad \left(\frac{\text{sqf}(\{3\})}{5}\right) = \theta(\{3\}) = -1, \\ \left(\frac{\text{sqf}(\{6\})}{5}\right) &= \theta(\{6\}) = 1, \quad \left(\frac{\text{sqf}(\{2, 3\})}{5}\right) = \theta(\{2, 3\}) = 1, \quad \left(\frac{\text{sqf}(\{2, 6\})}{5}\right) = \theta(\{2, 6\}) = -1 \\ \left(\frac{\text{sqf}(\{3, 6\})}{5}\right) &= \theta(\{3, 6\}) = -1, \quad \left(\frac{\text{sqf}(\{2, 3, 6\})}{5}\right) = \theta(\{2, 3, 6\}) = 1, \end{aligned}$$

by using Theorem 4.3.1, we obtain that the set  $\mathcal{R}_S(3, 8, 5, (-1, -1, 1))$  contains a positive density subset of primes  $p$  for which 2, 3, 6 are non 3-near primitive root modulo  $p$  having natural density

$$\frac{|\mathcal{H}_{15}(S)| |\mathcal{D}_0^{24}(S)|}{8 \times 4 \times (30)^3} = \frac{8}{8 \times 4 \times (30)^3} = \frac{1}{108000}.$$

### Example-2:

Consider the set  $S = \{7, 8, 11\}$  with a choice of signs  $\theta(7) = 1, \theta(8) = -1$  and  $\theta(11) =$

1. Suppose  $t = 3, f = 4$  and  $d = 5$ . Then by definition of  $\mathcal{D}_i^d(S)$  we see that

$$\mathcal{D}_0^3(S) = \{\phi\}.$$

We choose  $q = 3$  as it is the least prime that does not divide 7, 8, 11, 5 and we hence we have  $\mathcal{H}_9(S) = \{\phi\}$ , since  $\left(\frac{\text{sqf}(\phi)}{4}\right) = \theta(\phi) = 1$ .

By using Theorem 4.3.1, we obtain that the set  $\mathcal{R}_S(3, 5, 4, (1, -1, 1))$  contains a positive density subset of primes  $p$  for which 7, 8, 11 are non 3-near primitive root modulo  $p$  having natural density

$$\frac{|\mathcal{H}_9(S)||\mathcal{D}_0^3(S)|}{\phi(3) \times (3-1) \times (18)^3} = \frac{1}{2 \times 2 \times (18)^3} = \frac{1}{23328}.$$

Computationally, it is found that  $\mathcal{R}_S(3, 5, 4, (1, -1, 1)) = \{19, \dots\}$ .

In Theorem 4.3.1, we studied the density of the set  $\mathcal{R}_S(t, d, f, \theta)$  for odd  $t$ . In the final remark, we will discuss about the set  $\mathcal{R}_S(t, d, f, \theta)$  when  $t$  is even.

**Remark 4.3.2.** *If  $t$  is even, then it is easy to see that  $\mathbb{Q}(\sqrt{a_1}, \sqrt{a_2}, \dots, \sqrt{a_n}) \subset L_{qt}$  and hence*

$$\sigma_p(a_i^{1/qt}) = a_i^{1/qt} \implies \sigma_p(\sqrt{a_i}) = \sqrt{a_i}, \text{ for every } 1 \leq i \leq n.$$

*On the other hand,*

$$\tau_p(\sqrt{a_i}) = \theta(a_i)\sqrt{a_i}, \text{ for } 1 \leq i \leq n.$$

*Therefore, the condition  $\sigma|_{L_{qt} \cap M_{dt}} = \tau_p|_{L_{qt} \cap M_{dt}}$  forces that  $\theta(a_i) = 1$ , for every  $1 \leq i \leq n$ .*

*For this reason, we expect that in case  $t$  is even, the set  $\mathcal{R}_S(t, d, f, \theta)$  contains a positive density of primes  $p$  for which each  $a_i \in S$  is a non  $t$ -near primitive root modulo  $p$  only if  $\theta \equiv 1$ .*





## Chapter 5

### Conclusions and Future Scope

We are recapitulating the chapters. To make the thesis self-contained, in Chapter 1, we give the mathematical background necessary to understand the subsequent chapters.

In Chapter 2, we give an asymptotic formula for the primes,  $p$ , that satisfy two conditions. One that primes lie between  $N$  and  $2N$  for a sufficiently large  $N \geq 3$  and satisfy arithmetic progression condition  $p \equiv f \pmod{d}$ . Two, for a given finite set  $S = \{a_1, a_2, \dots, a_n\} \subset \mathbb{Z} \setminus \{0\}$ , the set  $S$  satisfies a quadratic residue pattern  $\theta$ . Using this asymptotic formula, there is a revelation of a counting problem that aids in finding the cardinality of the Galois group of multi-quadratic and cyclotomic field extensions,  $K$ .

In Chapter 3, we continue this process and find the explicit structure of  $K$ . Though the structure of multi-quadratic extension was already known, this work shows cancellations among the multi-quadratic and cyclotomic parts of the field extension. Hence we obtain the degree of this field extension. Further, we get the explicit structure of its Galois group.

Using the knowledge obtained from the previous sections, in Chapter 4, we find the natural density of primes for which the elements of the set  $S$  are non-primitive and satisfy a prescribed residue pattern.

Figure

As mentioned in chapter 1, finding the Galois group of algebraic field extensions is one of the core areas in Computational Number Theory. In the future, we look for methods to find the Galois group of other kinds of number fields. For instance, Noether's conjecture that every finite group occurs as the Galois group of a number field over  $\mathbb{Q}$  is still open in general.

Transcendental field extensions could be another area of research with the wits of lack of algebraicity. Intuitively, it appears to be more random if considered as field extensions over  $\mathbb{Q}$ , validating applications to Quantum Cryptography.

Biasse and Vredendaal (2019) have mentioned heuristic algorithm to calculate  $S$ -class groups and  $S$ -unit group of multi-quadratic field extensions. As a sequel to the work done in this thesis, a modified algorithm to similarly find the so called  $S$ -class groups and  $S$ -unit group of the field  $\mathbb{Q}(\sqrt{a_1}, \dots, \sqrt{a_n}, \zeta_d)$  over  $\mathbb{Q}$  is being attempted.

## Bibliography

- Abel-Hollinger, C. S. and Zimmer, H. G. (1995). Torsion groups of elliptic curves with integral  $j$ -invariant over multiquadratic fields. In *Number-theoretic and algebraic methods in computer science (Moscow, 1993)*, pages 69–87. World Sci. Publ., River Edge, NJ.
- Babu, C. G. K. (2021). Primes in beatty sequence. *Proc. Indian Acad. Sci. Math. Sci.*, 131(14).
- Babu, C. G. K. and Mukhopadhyay, A. (2022). Quadratic residue pattern and the Galois group of  $\mathbb{Q}(\sqrt{a_1}, \sqrt{a_2}, \dots, \sqrt{a_n})$ . *Proc. Amer. Math. Soc.*, 150(10):4277–4285.
- Baker, R. C., Banks, W. D., Brüdern, J., Shparlinski, I. E., and Weingartner, A. J. (2013). Piatetski-Shapiro sequences. *Acta Arith.*, 157(1):37–68.
- Balasubramanian, R., Luca, F., and Thangadurai, R. (2010). On the exact degree of  $\mathbb{Q}(\sqrt{a_1}, \sqrt{a_2}, \dots, \sqrt{a_l})$  over  $\mathbb{Q}$ . *Proc. Amer. Math. Soc.*, 138(7):2283–2288.
- Banks, W. D. and Shparlinski, I. E. (2009). Prime numbers with Beatty sequences. *Colloq. Math.*, 115(2):147–157.
- Banks, W. D. and Yeager, A. M. (2011). Carmichael numbers composed of primes from a Beatty sequence. *Colloq. Math.*, 125(1):129–137.
- Bennett, M. A., Martin, G., O’Bryant, K., and Rechnitzer, A. (2018). Explicit bounds for primes in arithmetic progressions. *Illinois Journal of Mathematics*, 62(1-4):427–532.
- Biassé, J. F. and Vredendaal, C. (2019). Fast multiquadratic S-unit computation and application to the calculation of class groups. *The Open Book Series*, 2:103–118.

- Davenport, H. (2000). *Multiplicative number theory*, volume 74 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition. Revised and with a preface by Hugh L. Montgomery.
- Dey, P. K. and Kumar, B. (2016). An analogue of Artin's primitive root conjecture. *Integers*, 16:Paper No. A67, 7.
- Dummit, D. S. and Foote, R. M. (2004). *Abstract algebra*. Wiley, New York, 3rd edition.
- Fried, M. (1968). Arithmetical properties of value sets of polynomials. *Acta Arith.*, 15:91–115.
- Fried, M. (1974). On Hilbert's irreducibility theorem. *Journal of Number Theory*, 6(3):211–231.
- Graham, S. W. and Kolesnik, G. (1991). *van der Corput's method of exponential sums*, volume 126 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge.
- Gun, S., Luca, F., Rath, P., Sahu, B., and Thangadurai, R. (2007). Distribution of residues modulo  $p$ . *Acta Arith.*, 129(4):325–333.
- Hardy, G. H. and Wright, E. M. (2008). *An introduction to the theory of numbers*. Oxford University Press, Oxford, sixth edition. Revised by D. R. Heath-Brown and J. H. Silverman, With a foreword by Andrew Wiles.
- Harman, G. (2007). *Prime-detecting sieves*, volume 33 of *London Mathematical Society Monographs Series*. Princeton University Press, Princeton, NJ.
- Hooley, C. (1967a). On Artin's conjecture. *J. Reine Angew. Math.*, 225:209–220.
- Hooley, C. (1967b). On Artin's conjecture. *Journal für die reine und angewandte Mathematik*, 225:209–220.
- Laska, M. and Lorenz, M. (1985). Rational points on elliptic curves over  $\mathbf{Q}$  in elementary abelian 2-extensions of  $\mathbf{Q}$ . *J. Reine Angew. Math.*, 355:163–172.

- Lenstra, H. W., Moree, P., and Stevenhagen, P. (2014). Character sums for primitive root densities. *Mathematical Proceedings of the Cambridge Philosophical Society*, 157(3):489–511.
- Luca, F., Shparlinski, I. E., and Thangadurai, R. (2008). Quadratic non-residues versus primitive roots modulo  $p$ . *J. Ramanujan Math. Soc.*, 23(1):97–104.
- M. Filaseta, D. R. (1989). Sets which contain a quadratic residue modulo  $p$  for almost all  $p$ . *Math. J. Okayama Univ*, 39:1–8.
- Matthews, K. (1976). A generalisation of artin’s conjecture for primitive roots. *Acta Arithmetica*, 29(2):113–146.
- Moree, P. (1999). On primes in arithmetic progression having a prescribed primitive root. *Journal of Number Theory*, 78(1):85–98.
- Moree, P. (2005). On the distribution of the order and index of  $g(\text{mod } p)$  over residue classes—I. *Journal of Number Theory*, 114(2):238–271.
- Moree, P. (2008). On primes in arithmetic progression having a prescribed primitive root II. *Functiones et Approximatio Commentarii Mathematici*, 39(1):133 – 144.
- Moree, P. (2013). Near-primitive roots. *Functiones et Approximatio Commentarii Mathematici*, 48(1):133 – 145.
- Moree, P. and Sha, M. (2019). Primes in arithmetic progressions and nonprimitive roots. *Bulletin of the Australian Mathematical Society*, 100(3):388–394.
- Pyateckii-Šapiro, I. I. (1953). On the distribution of prime numbers in sequences of the form  $[f(n)]$ . *Mat. Sbornik N.S.*, 33(75):559–566.
- Ramaré, O. and Rumely, R. (1996). Primes in arithmetic progressions. *Math. Comp.*, 65(213):397–425.
- Rivat, J. and Wu, J. (2001). Prime numbers of the form  $[n^c]$ . *Glasg. Math. J.*, 43(2):237–254.

- Scharaschkin, V. (2011). The odd and even intersection properties. *Electron. J. Combin.*, 18(1):Paper 185, 8.
- S.S. Wagstaff, J. (1982). Pseudoprimes and a generalization of Artin's conjecture. *J. Number Theory*, 41(2):141–150.
- Steuding, J. and Technau, M. (2016). The least prime number in a Beatty sequence. *J. Number Theory*, 169:144–159.
- Tanti, J. and Thangadurai, R. (2013). Distribution of residues and primitive roots. *Proc. Indian Acad. Sci. Math. Sci.*, 123(2):203–211.
- Vaughan, R. C. (1977). On the distribution of  $\alpha_p$  modulo 1. *Mathematika*, 24(2):135–141.
- Vinogradov, I. M. (1937). A new estimate of a certain sum containing primes(russian). *Rec.math. Moscou, n. Ser.,2(44)*, No. 5:783–792.
- Vinogradov, I. M. (2004). *The method of trigonometrical sums in the theory of numbers*. Dover Publications, Inc., Mineola, NY. Translated from the Russian, revised and annotated by K. F. Roth and Anne Davenport, Reprint of the 1954 translation.
- Weintraub, S. H. (2009). *Galois theory*. Universitext. Springer, New York, second edition.
- Wright, S. (2007). Patterns of quadratic residues and nonresidues for infinitely many primes. *J. Number Theory*, 123(1):120–132.
- Wright, S. (2008). Quadratic residues and the combinatorics of sign multiplication. *J. Number Theory*, 128(4):918–925.
- Wright, S. (2009). Some enumerative combinatorics arising from a problem on quadratic nonresidues. *Australas. J. Combin.*, 44:301–315.
- Wright, S. (2013a). Quadratic nonresidues and the combinatorics of sign multiplication. *Ars Combin.*, 112:257–278.

Wright, S. (2013b). Quadratic residues and non-residues in arithmetic progression. *J. Number Theory*, 133(7):2398–2430.

Xi, P. (2013). Quadratic residues and non-residues for infinitely many Piatetski-Shapiro primes. *Acta Math. Sin. (Engl. Ser.)*, 29(3):515–522.





## APPENDIX

- **Siegels's Theorem** (Davenport (2000), Chapter 22):

Let  $n \geq 0$  be a positive integer. Let  $d$  be a positive integer satisfying  $d \leq \log^A n$  for some  $A > 0$ . Then for every non-principal character  $\chi \pmod{d}$ , we have:

$$\sum_{p \leq N} \chi(p) \ll n \cdot \exp(-C\sqrt{\log N})$$

- **Law of Quadratic Reciprocity:**

Given any integer  $n$  and odd and squarefree integer  $s$ , we have

$$\left(\frac{s}{n}\right) \left(\frac{n}{s}\right) = (-1)^{\frac{s-1}{2} \frac{n-1}{2}}.$$

- **Partial Summation Formula:**

$$\sum_{1 \leq n \leq x} a_n f(n) = C(x)f(x) - \int_1^x C(t)f'(t) dt$$



## PUBLICATIONS

### Journal publications:

1. Karthick Babu, Anirban Mukhopadhyay and **Sehra Sahu**. On the explicit Galois group of  $\mathbb{Q}(\sqrt{a_1}, \sqrt{a_2}, \dots, \sqrt{a_n}, \zeta_d)$  over  $\mathbb{Q}$  (*communicated*, January 2022).  
<http://arxiv.org/abs/2201.01159v1>
2. Karthick Babu and **Sehra Sahu**. Non primitive roots with a prescribed residue pattern. *Proceedings - Mathematical Sciences* 133, 9 (2023).  
<https://doi.org/10.1007/s12044-023-00728-4>

### Papers presented at Conferences:

1. **Sehra Sahu** and B. R. Shankar. A note on quadratic residue pattern and near primitive roots. *International Conference on Analysis and Number Theory - 2022*. Department of Mathematics, Ayya Nadar Janaki Ammal College, Sivakasi, Tamil Nadu, India. October 27-29, 2022.
2. **Sehra Sahu**. Explicit Galois Group of  $\mathbb{Q}(\sqrt{a_1}, \sqrt{a_2}, \dots, \sqrt{a_n}, \zeta_d)$  over  $\mathbb{Q}$ . *Indian Women and Mathematics - 2023*. Indian Institute of Science Education and Research Bhopal, Madhya Pradesh, India. July 13-15, 2023. (Poster presentation)



## BIODATA

**Name** : Sehra Sahu  
**Email** : sehrasahu@gmail.com  
**Date of Birth** : 23<sup>rd</sup> November 1993.  
**Permanent address** : Sehra Sahu,  
D/o Shri Dilharan Lal Sahu & Smt Rampyari Sahu,  
Flat No. 504-D,  
Lotus Homes Apartments,  
Bandlaguda, Nagaram  
Hyderabad 501301.

### **Educational Qualifications** :

<b>Degree</b>	<b>Year</b>	<b>Institution / University</b>
B.Sc. (Mathematics, Physics & Chemistry)	2014	St. Ann's Degree College, Mehdipatnam, Hyderabad
M.Sc. (Mathematics)	2016	Central University of Karnataka