Elliptic curves, modular forms, and the associated exponential sums

Dissertation

for the award of the degree
"Doctor rerum naturalium" (Dr. rer. nat.)
of the Georg-August-Universität Göttingen

within the doctoral program
"Mathematical Sciences"
of the Georg-August University School of Science (GAUSS)

submitted by
Subham Bhakta
from Talpur, Hooghly

Göttingen, 2023

Thesis committee

Harald Andrés Helfgott
Mathematisches Institut, Georg-August-Universität Göttingen

Jörg Brüdern
Mathematisches Institut, Georg-August-Universität Göttingen

Damaris Schindler
Mathematisches Institut, Georg-August-Universität Göttingen

Members of the Examination Board

First reviewer:
Harald Andrés Helfgott
Mathematisches Institut, Georg-August-Universität Göttingen

Second reviewer:
Jörg Brüdern
Mathematisches Institut, Georg-August-Universität Göttingen

Further members of the Examination Board

Terry Gannon
Department of Mathematics and Statistics, University of Alberta

Preda Mihăilescu
Mathematisches Institut, Georg-August-Universität Göttingen

Gerlind Plonka-Hoch
Institut für numerische und angewandte Mathematik
Georg-August-Universität Göttingen

Thomas Schick
Mathematisches Institut, Georg-August-Universität Göttingen

Date of the oral examination: 27.03.2023

Contents

Acknowledgements

I am deeply grateful to my supervisor, Prof. Harald Helfgott, whose exceptional support has been instrumental throughout this journey. Without his guidance and encouragement, completing this thesis would not have been possible. I have gleaned invaluable lessons from his unwavering dedication to both research and teaching, and his exemplary work ethic has inspired me profoundly. Prof. Helfgott has not only served as my mentor in Mathematics but has also provided invaluable guidance in navigating various challenges in daily life. I would also like to extend my heartfelt thanks to Prof. Jitendra Bajpai for his unwavering assistance and guidance over the past four years. Prof. Bajpai introduced me to the captivating realm of vector-valued automorphic forms and has been a constant source of support and inspiration. He has been like a big brother, always willing to engage in mathematical discussions regardless of his busy schedule. I consider myself incredibly fortunate to have had the privilege of learning from and working alongside these two remarkable individuals.

I am fortunate to have opportunities of discussing Mathematics with Daniele Dona, Aryan Farzad, Lifan Guan, R. Muneeswaran, Simon Myerson, Kunjakanan Nath, and others. Several excellent teachers and mathematicians taught me, Prof. Jörg Brüdern, Prof. Damaris Schindler at the university of Göttingen, Prof. Srilakshmi Krishnamoorthy at IISER, Thiruvananthapuram, Prof. Sinnou David at CMI, Chennai and Prof. K. Srinivas at IMSc, Chennai.

I had the great privilege to work with my research collaborators, Jitendra Bajpai, Renan Finder, Victor García, Srilakshmi Krishnamoorthy, Daniel Loughran, R. Muneeswaran, Simon Myerson, and Masahiro Nakahara. I sincerely thank them all for teaching me various mathematical stuff. It was an amazing experience to work with all of them.

I am deeply grateful to the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation program (grant ID 648329) for generously funding my doctoral studies. This financial support provided me with the stability and resources necessary to pursue my research

with dedication and focus. It also enabled me to participate in numerous summer schools and conferences, where I had the opportunity to engage with esteemed mathematicians and broaden my academic horizons.

I extend my heartfelt thanks to my wife, Sulakhana, for her unwavering belief in me. Despite the challenges posed by the COVID-19 pandemic, her steadfast support never wavered, even during the two years we were unable to meet in person. I am truly fortunate to have such a supportive partner by my side.

Lastly, I am grateful to my parents for their endless support and understanding of my aspirations. They have made countless sacrifices to ensure that I could pursue my education and follow my dreams. Their unwavering encouragement has been a source of strength throughout my journey.

Preface

In this thesis, the author studies certain arithmetic objects associated with Elliptic curves and Modular forms. Chapter 1 provides a walk-through of the contents presented in this thesis. The main results of this thesis are highlighted in this chapter.

In Chapter 2, the exponential sums associated with the linear recurrence sequences over prime fields are studied. This chapter provides the essential tools to prove the main results of Chapter 3, where the author studies the additivity of the Fourier coefficients of a modular form over specific finite fields. These two chapters are written based on the author's published article [10], jointly written with J. Bajpai and V.C. García.

Chapter 4 is about the theory of Galois representations and their images. In this chapter, the author discusses how Chebotarev's density theorem can be used to study some related analytic problems. This chapter is written based on [10], author's preprint [14], and [15]. Chapter 5 is about studying the additive properties of the Fourier coefficients and controlling the size of the solutions. This chapter is written based on [15], jointly written with S. Krishnamoorthy and R. Muneeswaran.

Roughly speaking, the Hecke theory provides the necessary tools for studying the exponential sums for classical modular forms in Chapters 3, 4, and 5. The same does not work for noncongruence/nonclassical modular forms. In Chapter 6 and Chapter 7, the author studies one of the generalizations of modular forms in higher dimensions called vector-valued automorphic forms. In these two chapters, vector-valued automorphic forms are concerned with any discrete subgroup of $\mathrm{PSL}_2(\mathbb{R})$, and any representation of it. In particular, the growth of the associated Fourier coefficients is studied, and the non-triviality of an associated exponential sum is established. This is based on the joint work with J. Bajpai and R. Finder, which was recently accepted for publication, and the preprint can be found in [9]. The vector-valued automorphic forms can be divided into two classes, namely the admissible and logarithmic. In addition to the growth problem, Chapter 7 also studies

the lifting of logarithmic vector-valued automorphic forms and the associated growth. This is based on the joint work with J. Bajpai in [8].

In Chapter 8, the author studies a special family of non-linear recurrence sequences known as elliptic sequence(s). Roughly speaking, the terms of any such sequence are related to the denominators of the points on an elliptic curve over $\mathbb{Q}$. In this chapter, the periodicity of these sequences is concerned with modulo any composite numbers. Moreover, it is shown that the parity of the valuations could be controlled. This is based on a joint work with D. Loughran, S. Myerson, and M. Nakahara, whose preprint can be found in [16]. Moreover, an analogy with the classical *Wieferich-prime* problem is addressed, and some known results for the associated exponential sums are also discussed.

Author contributions

Chapter 1

This chapter delves into the motivations, historical context, and pivotal findings of this thesis. The insights into exponential sums linked with linear recurrence sequences over finite fields were imparted to me by Bajpai and García. Additionally, Bajpai provided valuable insights into the background of vector-valued modular forms. While Theorem 1.4.2 is stated, its proof is omitted in this thesis. Nevertheless, the key methodology is elaborated on in detail on page 29. The contents of pages 29-30 are the outcome of collaborative efforts with Myerson, Loughran, and Nakahara. The remainder of the introduction represents my original contributions.

Chapter 2

I gained insight into the historical background of exponential sums over prime fields through discussions with García and Bajpai. They initially established the case $\nu = 1$ in Theorem 2.2.1. Subsequently, I extended their work to cover the case $\nu = 2$. Finally, through collaborative discussions, we resolved the case $\nu > 2$ using one of Garaev's techniques. Corollary 2.3.1 follows immediately from the non-triviality of the exponential sums, as highlighted by Bajpai and García. Building on this observation, I proceeded to prove Theorem 2.3.2 and provided Example 2.3.3 in support.

Chapter 3

The suggestion from Bajpai and García to investigate exponential sums with $a(p^n)$ by studying those associated with linear recurrence sequences

was instrumental. We encountered difficulty in demonstrating that the non-trivial estimate in part (i) of Theorem 3.0.1 holds for almost all primes ℓ. However, following a suggestion from Shparlinski during an email exchange, I successfully devised the proof for Lemma 3.1.1. Subsequently, with guidance from Bajpai and García on the results of Bourgain and others regarding exponential sums associated with prime fields, I completed the proofs of both parts of Theorem 3.0.1 and derived Corollary 3.1.2.

Section 3.2 represents my independent contribution. Notably, the condition in part (i) of Theorem 3.0.1 closely resembles the study of Sato-Tate for newforms. Intrigued by this similarity, I investigated the implications of extending beyond newforms. Upon suggestions from Sawin in one of my Math Overflow posts, I familiarized myself with the Generalized Sato-Tate conjecture. Delving into the literature, I provided a brief discussion on this topic and applied it to prove Theorem 3.0.2.

Chapter 4

Section 4.1 is my contribution. In this section, I delve into the study of $\mathbb{Q}$-linear combinations of newforms modulo composite numbers. The inspiration for this analysis stems from the works of Serre, Masser, Wüstholz, and Jones, on the Galois representations.

Moving on to Section 4.2, Proposition 1 and Theorem 4.2.3 are my original contributions. To support these results, I referenced a classical result (Lemma 4.2.2) mentioned on Stack Exchange, which is also discussed in this chapter.

In Section 4.3, I begin by discussing the fact that the non-trivial estimate of the exponential sum in Chapter 3 holds under certain conditions, particularly when certain elements in $\mathbb{F}_\ell^*$ possess sufficiently large orders. This phenomenon, introduced to me by Bajpai and García, is attributed to Bourgain. I then explore the attachment of the Galois representation and leverage Chebotarev's theorem to determine conditions under which large orders occur. Utilizing this framework, I conducted computations leading to Theorems 4.3.1 and 4.3.2 . Lastly, Section 4.4 presents my original contributions.

Remark. The research discussed in Chapter 2, Chapter 3, and specific sections of Chapter 4 has been published in *Research in Number Theory*.

Chapter 5

In this chapter, I study solubility to

$$\sum_{i=1}^{O(1)} a(n_i) \equiv a \pmod{m},\ n_i = m^{O(1)}.$$

Initially, I collaborated with Krishnamoorthy and Muneeswaran on this project. Section 5.1 primarily comprises auxiliary lemmas essential for the entire chapter. In Section 5.2, I formulated Lemma 5.2.1 and Lemma 5.2.2, drawing insights from Shparlinski's work on the Ramanujan-tau function. The derivation of Corollary 5.2.3 was a collective effort with Krishnamoorthy and Muneeswaran, who initially proposed versions of Lemma 5.2.5 and Lemma 5.2.6. Later, I refined the solutions, arguably enhancing their elegance. Proposition 5.2.7 is my independent contribution, inspired by Shparlisnki's ideas.

While I authored Proposition 5.2.8 and Corollary 5.2.9, Krishnamoorthy and Muneeswaran assisted in refining their presentation. Initially, I proposed approaches to prove Theorem 5.3.1 and Theorem 5.3.2, but through extensive discussions with them, we developed accurate proofs. Krishnamoorthy and Muneeswaran further utilized these results to complete the entries in Table 5.1.

The conceptualization and discussions in Section 5.4 were primarily driven by my ideas. However, after extensive discussions among us, I refined the concepts and presented them as polished versions.

Remark. This chapter has been accepted for publication in the journal *International Journal of Number Theory*.

Chapter 6

In Sections 6.1.1 and 6.2, Bajpai introduced me to the realm of vector-valued automorphic forms. The proof of Theorem 6.2.12 was primarily derived from the contributions of Bajpai and Finder. Additionally, I formulated Lemma 65 to provide a more explicit representation of α in the bound $O(n^{\alpha})$.

My contributions are evident in Sections 6.4 and 6.5, where I discuss some applications of growth results. Inspired by Bajpai's insights into Mason's work on attaching the L-function to vector-valued modular forms, I developed these sections.

Section 6.1.2 is my independent work, shaped by various suggestions from Bajpai, Finder, and Patterson. This section plays a crucial role in the subsequent chapter.

Chapter 7

Bajpai introduced the work of Knopp-Mason on logarithmic vector-valued automorphic forms for $\mathrm{SL}_2(\mathbb{Z})$. In this chapter, my task was to extend this study to any Fuchsian group of the first kind. I established Lemma 6.3.3, providing the logarithmic expansion, and utilized the results from Section 6.1.2 to derive the polynomial growth of the logarithmic representations in Section 7.2.1. Lemma 7.2.4, originally due to Bajpai and Finder, was employed to prove the logarithmic case of Theorem 1.3.1 in Section 7.2.3. The primary results of Sections 7.3 and 7.4 stemmed from my contributions. Bajpai assisted me in crafting the examples in Section 7.3.2.

The concept of lifting of vector-valued automorphic forms was introduced to me by Bajpai, leading to the contents of Sections 7.4.1 and 7.4.2. Subsequently, I carried out the work in Sections 7.4.3 and 7.5.

Remark. The content found in Chapters 6, Sections 7.1, 7.2, and 7.3, has been published in the *Journal of Number Theory*. Sections 7.4, 7.5, and additional material not included in this thesis is submitted for publication.

Chapter 8

Drawing from insights gained from one of my old arXiv preprints, I delved into the arithmetic properties of the denominators e_n associated with elliptic curves, and (elliptic) Wieferich primes. Theorem 8.0.6 stands as my original contribution, and I am currently engaged in expanding upon this discovery. However, the crux of the proof of Theorem 8.0.6 lies in Proposition 8.0.5. Myerson mentioned Theorem 8.1.6 by Verzobio, which I utilized to establish the proof of Proposition 8.1.9. Although Proposition 8.2.1 may have existed in the literature, the explicit constant dependency on P in Lemma 8.2.3 is unnecessary for the scope of this chapter. I used Proposition 8.2.1 to complete the proof of Proposition 8.0.5.

Section 8.3 represents my endeavor to expand upon [16, Section 6]. In this section, Lemma 8.3.2 is credited to Loughran and Mashahiro. Section 8.4 encapsulates my contribution.

Remark. Sections 8.1, 8.2, Theorem 1.4.2, and other related results are published in *Proceedings of the London Mathematical Society*.

On the notations

Throughout the thesis, we denote $\mathbb{C}$, the field of complex numbers. Say that, two functions $f \sim g$, if their domain is in $\mathbb{C}$, and if $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1$. We write $f \ll g$ for $|f| \leq c|g|$ where c is a constant irrespective of the domains of f and g, often $f = O(g)$ is written to denote the same. Moreover, we denote $f = o(g)$ when $\lim_{x\to\infty} \frac{|f(x)|}{|g(x)|} = 0$. By $O_{a,\ldots,z}(A)$ we mean a quantity with absolute value at most cA for some positive constant c depending on $a, \ldots, z$ only; if the subscripts are omitted the implied constant is absolute. We write $A \ll_{a,\ldots,z} B$ for $A = O_{a,\ldots,z}(B)$ and $A = o(B)$ for $A/B \to 0$

We denote $\mathbb{Z}$ be the set of all integers. For any integer $N \geq 1$, denote

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \subset \mathrm{SL}_2(\mathbb{Z}) \mid c \equiv 0 \pmod{N} \right\}$$

and

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \subset \mathrm{SL}_2(\mathbb{Z}) \mid a, d \equiv 1 \; c \equiv 0 \pmod{N} \right\}.$$

In the following table, we record all the notations and symbols for the reader's convenience and reference.

$\mathbb{Q}$	the field of rational numbers
$\overline{\mathbb{Q}}$	algebraic closure of $\mathbb{Q}$
$\mathbb{P}^n(\mathbb{Q})$	the projective space of dimension n over $\mathbb{Q}$
$\mathbb{Q}[x]$	the ring of polynomials in variable x and coefficients in $\mathbb{Q}$
$\mathbb{Q}_p$	the field of p-adic numbers
$\nu_p(\cdot)$	p-adic valuation
H	standard height on $\mathbb{P}^n(\mathbb{Q})$
$\mathbb{Z}_p$	the ring of p-adic integers
$\mathbb{N}$	the set of natural numbers
$\phi(\cdot)$	Euler's phi function
$\mu(\cdot)$	Möbius function
$\omega(\cdot)$	number of distinct prime factors
$\Omega(\cdot)$	number of prime factors counted with multiplicity
$\mathbb{R}$	the field of real numbers
$\mathbb{R}[x]$	the ring of polynomials in variable x and coefficients in $\mathbb{R}$
$e(z)$	exponential function $z \mapsto e^{2\pi \mathrm{i} z}$
$\mathbb{C}[x]$	the ring of polynomials in variable x and coefficients in $\mathbb{C}$
$\mathcal{O}_K$	ring of integers in a number field K
$\mathbb{F}_p$	prime field, with p a prime
comm(G)	commutator subgroup of G
$\mathbb{H}$	the complex upper half plane
i	a square root of -1 in $\mathbb{C}$
q	$\exp(2\pi \mathrm{i} \tau)$, for any $\tau \in \mathbb{H}$
ζ_m	the standard m-th primitive root of unity in $\mathbb{C}$
$\mathbb{X}(\tau)$	vector-valued automorphic forms
$\mathbb{X}_{[n]}$	the n^{th} vector-valued Fourier coefficients of vvaf $\mathbb{X}(\tau)$
E/K	an elliptic curve over a number field K
Weierstrass equation for E	$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$
$E(\mathbb{Q})$	the $\mathbb{Q}$-points on the elliptic curve E
$\widehat{h}$	the canonical height on $E(\mathbb{Q})$.

Chapter 1

General Introduction

1.1 Classical modular forms and Waring type problems

Let f be a modular form of weight $k \in 2\mathbb{Z}$ and level N such that it has a Fourier expansion

$$f(z) = \sum_{n=0}^{\infty} a(n) e^{2\pi i n z}, \quad \Im(z) \geq 0,$$

with $a(n)$ be the n^{th} Fourier coefficient. In this thesis, we shall restrict to the family of modular forms with rational coefficients, that is, $f(z)$ with $a(n) \in \mathbb{Q}$ for every n. We say that $f(z)$ is a cuspform if $a(0) = 0$, and consider Hecke eigenforms or simply eigenforms in the space of cusp forms of weight k for the congruence subgroup $\Gamma_1(N)$ with trivial nebentypus. We study solubility to the equation,

$$a(n_1) + a(n_2) + \cdots a(n_{O(1)}) = a,$$

where a is a given integer, and $a(n)$ is the n^{th} Fourier coefficient of a modular form. This problem presents an intriguing aspect due to the multiplicative nature and polynomial growth exhibited by the Fourier coefficients. This characteristic establishes a connection with the classical Waring's problem, offering a link between the two concepts

When f is an eigenform with integer Fourier coefficients, it follows from Deligne-Serre that for any prime ℓ, there exists a corresponding Galois representation

$$\rho_f^{(\ell)} : \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right) \longrightarrow \mathrm{GL}_2\left(\mathbb{Z}_\ell\right)$$

such that $\mathrm{tr}(\rho_f^{(\ell)}(\mathrm{Frob}_p)) = a(p)$, for any prime $p \nmid N\ell$. For a quick reference about this correspondence, we refer the interested reader to [37, Chapter 3].

In particular, $a(p) \pmod{\ell}$ is determined by the trace of the corresponding Frobenius element in $\mathrm{GL}_2(\mathbb{Z}_\ell/\ell\mathbb{Z}_\ell) = \mathrm{GL}_2(\mathbb{F}_\ell)$. In certain cases, Chebotarev's density theorem implies that given any $\lambda \in \mathbb{F}_\ell$, there exists a prime p such that $a(p) \equiv \lambda \pmod{\ell}$. However, the set of primes p possessing this property has a density strictly less than 1. This prompts consideration of other primes p that do not exhibit this property. In this context, we address the following Waring-type question in Chapter 3.

Question. *Does there exist an absolute constant s such that for any given primes p and ℓ, any element of $\mathbb{F}_\ell$ can be written as a sum of at most s elements of the set $\{a(p^n)\}_{n\geq 1}$?*

A related question was studied by Shparlinski in [85] for the Ramanujan's τ function, where $\tau(n)$ is defined by the identity

$$\Delta(z) = q\prod_{n\geq 1}(1-q^n)^{24} = \sum_{n\geq 1}\tau(n)q^n, \quad \text{with } q = \exp(2\pi i z).$$

In [85], it is proved that the set $\{\tau(n)\}_{n\geq 1}$ is an additive basis modulo any prime ℓ, that is, there exists an absolute constant s such that the Waring-type congruence

$$\tau(n_1) + \cdots + \tau(n_s) \equiv \lambda \pmod{\ell}$$

is solvable for any residue class $\lambda \pmod{\ell}$.

Shparlinski's work was later generalized by Garaev, García and Konyagin over the global field $\mathbb{Q}$. More precisely, in [41], the authors proved that for any $\lambda \in \mathbb{Z}$, the equation

$$\sum_{i=1}^{s}\tau(n_i) = \lambda$$

always has a solution for $s = 74,000$.

Later García and Nicolae [43] extended this result for coefficients $a(n)$ of newforms of arbitrary weight k and level N. Roughly speaking, a newform of level N is a normalized eigenform which is not a cuspform of level N' for any proper divisor N' of N. For details and basics on modular forms, we refer the reader to [29]. More precisely, they proved that for any $\lambda \in \mathbb{Z}$, the equation

$$\sum_{i=1}^{s}a(n_i) = \lambda$$

always has a solution for some $s \leq c(f)$ with $c(f)$ satisfying

$$c(f) \ll (2N^{3/8})^{\frac{k-1}{2}+\varepsilon} k^{\frac{3}{16}k+O(1)+\varepsilon} \log(k+1).$$

The proof of the above two results are connected to the identity $a(p^2) = a^2(p) - p^{k-1}$ and the solubility of the equation

$$p_1^{k-1} + \cdots + p_s^{k-1} = N, \quad \text{for primes } p_1, \ldots, p_s.$$

We are studying the finite field version of this additivity problem by obtaining nontrivial exponential sums associated with coefficients of modular forms, in the sense of [85]. We are working with the class of forms that García and Nicolae [43] considered but with Fourier coefficients evaluated only at prime powers. In particular, we prove in Chapter 3 the following.

Theorem 1.1.1 (Bajpai, Bhakta, García)**.** *Let f be a newform without CM and with rational Fourier coefficients. here is an absolute constant s_0 independent to f, such that any element of $\mathbb{F}_\ell$ can be written as a sum of at most s_0 elements of the set $\{a(p^n)\}_{n\geq 0}$ for almost all primes p and ℓ.*

To prove this, we shall primarily focus on the exponential sums of type

$$\max_{\xi \in \mathbb{F}_\ell^*} \left| \sum_{n \leq \tau} \mathbf{e}_\ell \left(\xi a(p^n)\right) \right|$$

where p, ℓ are primes, and τ is a suitable parameter which we shall specify later. More precisely, we shall prove the following in Chapter 3.

Theorem 1.1.2 (Bajpai, Bhakta, García)**.** *Let $f(z)$ be an eigenform with rational coefficients $a(n)$. Let $\mathcal{P}$ be the set of primes p such that $a(p^u) \neq 0$ for any $u \in \mathbb{N}$. Then for any $p \in \mathcal{P}$, and any $0 < \varepsilon < 1/2$, there exists a $\delta = \delta(\varepsilon) > 0$ such that the following estimate*

$$\max_{\xi \in \mathbb{F}_\ell^*} \left| \sum_{n \leq \tau} \mathbf{e}_\ell \left(\xi a(p^n)\right) \right| \leq \tau \ell^{-\delta}, \tag{1.1}$$

holds for $\pi(y) + O_{f,p}(y^{2\varepsilon})$ many primes $\ell \leq y$, where the least period τ of the linear recurrence sequence $\{a(p^n)\} \pmod{\ell}$ depends on both p and ℓ, and $\pi(y)$ denotes the number of primes up to y.

A newform is said to have complex multiplication (CM) by a quadratic Dirichlet character ϕ if $f = f \otimes \phi$, where we define the twist as

$$f \otimes \phi = \sum_{n=1}^{\infty} a(n)\phi(n)q^n.$$

In Theorem 3.0.1, the condition $a(p^u) \neq 0$ holds for almost all prime p provided that f is a newform without CM. This is a consequence of Sato-Tate conjecture, and this proves Theorem 1.1.1.

When f is a normalized eigenform, it is well known that $a(n)$ is a multiplicative function and for any prime $p \nmid N$ satisfies the relation

$$a(p^{n+2}) = a(p)a(p^{n+1}) - p^{k-1}a(p^n), \quad n \geq 0.$$

Moreover, we have $a(p^n) = a(p)^n$ for any prime $p \mid N$. These facts come from the properties of Hecke operators, see [29, Proposition 5.8.5]. If $a(p) \in \mathbb{Q}$, then one can consider $a(p) \pmod{\ell} \in \mathbb{F}_\ell$ naturally for any large enough prime ℓ. For instance, ℓ can be taken to be any prime, not dividing the denominators of the Fourier coefficients. On the other hand, any cuspform can be uniquely written as a $\mathbb{C}$-linear combination of pairwise orthogonal eigenforms with Fourier coefficients coming from $\mathbb{C}$. See [29, Chapter 5] for a brief review of the Hecke theory of modular forms. However, here we are concerned with all such cuspforms, which can be uniquely written as a $\mathbb{Q}$-linear combination of pairwise orthogonal eigenforms with Fourier coefficients coming from $\mathbb{Q}$. In this case, the sequence $\{a(p^n)\}$ is a linear recurrence sequence of possibly higher degrees. For these families of cuspforms, we prove Theorem 3.0.2 in Chapter 3. We do this under the assumption of the *Generalized Sato Tate conjecture*, which is about the independency of the Sato Tate distributions associated to the eigenforms.

To prove Theorem 1.1.2 and Theorem 3.0.2, we study exponential sums associated to linear recurrence sequences. Let $r \geq 1$ be an integer and p be an arbitrary prime number. A *linear recurrence sequence* $\{s_n\}$ of order r in $\mathbb{F}_p$ consists of a recursive relation

$$s_{n+r} \equiv a_{r-1}s_{n+r-1} + \cdots + a_0 s_n \pmod{p}, \quad \text{with } n = 0, 1, 2, \ldots,$$

and initial values $s_0, \ldots, s_{r-1} \in \mathbb{F}_p$. Here $a_0, \ldots, a_{r-1} \in \mathbb{F}_p$ are fixed. The case when associated characteristic polynomial $\omega(x)$ is irreducible, had been studied by Korobov [57], Katz [49] and Shparlinski [84]. In Chapter 2, we prove the following.

Theorem 1.1.3 (Bajpai, Bhakta, García)**.** *Let p be a large prime number and $\varepsilon > \varepsilon' > 0$. Suppose that $\{s_n\}$ is a nonzero linear recurrence sequence with positive order and period τ in $\mathbb{F}_p$ such that its characteristic polynomial $\omega(x)$ has distinct roots in its splitting field, and $(\omega(0), p) = 1$. Set $\omega(x) = \prod_i^{\nu} \omega_i(x)$ as a product of distinct irreducible polynomials in $\mathbb{F}_p[x]$, and for each i, α_i denotes a root of $\omega_i(x)$. If all polynomials $\omega_i(x)$ have the same degree, i.e. $\deg \omega_i(x) = r > 1$, and the system $\tau_i = \operatorname{ord} \alpha_i$, satisfies*

a) $\max\limits_{\substack{d<r \\ d|r}} \gcd(\tau_i, p^d - 1) < \tau_i p^{-\varepsilon}$, *for any* $1 \leq i \leq \nu$,

b) $\gcd(\tau_i, \tau_j) < p^{\varepsilon'}$, *for some pair* $i \neq j$ *along with* $\mathbb{F}_p(\alpha_i) \cong \mathbb{F}_p(\alpha_j)$,

then there exists a $\delta = \delta(\varepsilon, \varepsilon') > 0$ such that

$$\max_{\xi \in \mathbb{F}_p^*} \left| \sum_{n \leq \tau} \mathbf{e}_p\left(\xi s_n\right) \right| \leq \tau p^{-\delta}.$$

Even for the irreducible case, our bound improves any known previous bounds. It turns out that this extends [19, Corollary] due to Bourgain, where all of the irreducible factors have degree $r = 1$, while Theorem 1.1.3 deals with the case $r \geq 2$. Our approach, which relies on the sum-product phenomenon, provides an improvement over Theorem 3.1 of [84] for the same class of linear recurrence sequences, obtaining non-trivial exponential sums in a larger range. To be more precise, if $p(r)$ denotes the least prime divisor of r then any $\tau > p^{r/p(r)+\varepsilon}$ satisfies

$$\tau p^{-\varepsilon} > p^{r/p(r)} \geq \max_{\substack{d<r \\ d|r}} \gcd(\tau, p^d - 1).$$

In particular, our result works for any $\tau > p^{r/p(r)+\varepsilon}$, while bound in [84] is nontrivial if $\tau > p^{r/2-1/6+\varepsilon}$. This is an improvement if $p(r) > 2$, more precisely when r is odd.

In Theorem 1.1.2, we took a fixed prime p and looked for primes ℓ for which a non-trivial estimate to (1.1) holds. However, this result is valid for almost all primes ℓ, that too only for the without CM case, and we do not know explicitly which of the primes are being excluded in this process. Thus, one may naturally ask, what if we now fix a prime ℓ and find out for how many primes p the sum at (1.1) is non-trivial? In this regard, we prove the following result in Chapter 4.

Theorem 1.1.4 (Bajpai, Bhakta, García). *Let $f(z)$ be a newform of weight k, without CM and with integer Fourier coefficients. Consider the set $\mathcal{P}_k = \{\ell \text{ prime} \mid (k-1, \ell-1) = 1\}$. Then, for any fixed $\varepsilon > 0$ and any large enough $\ell \in \mathcal{P}_k$, the set of primes p satisfying*

$$\max_{\xi \in \mathbb{F}_\ell^*} \left| \sum_{n \leq \tau} \mathbf{e}_\ell \left(\xi a(p^n) \right) \right| \leq \tau \ell^{-\delta}$$

have density at least $1 + O_\varepsilon\left(\frac{1}{\ell^{1-3\varepsilon}}\right)$, where $\delta = \delta(\varepsilon)$ is same as in Theorem 2.2.1.

Being determined by a Chebotarev-type condition, any such p in Theorem 1.1.4 could [93] be large. Specifically, they could grow exponentially as a function of ℓ. In Chapter 5, we study the equation

$$\sum_{i=1}^{O(1)} a(n_i) \equiv a \pmod{m}, \ n_i = m^{O(1)},$$

for any composite number m. For every prime $\ell \mid m$, the strategy is to study the exponential sum $\sum_{\substack{u_1 \in U_1, \ u_2 \in U_2 \\ a(n) \pmod{\ell} = u_1 u_2}} \mathbf{e}_\ell \left(\lambda(u_1 u_2 - a) \right), \ \forall \lambda \in \mathbb{F}_\ell^*$, over a suitably large subset $U_1 \times U_2$ of $\mathbb{F}_\ell \times \mathbb{F}_\ell$, which satisfies $\#U_1 \#U_2 > \ell^{1+c}$ for some $c > 0$. To find explicit c, we use the sum-product estimates over finite fields by Rudnev and Shkredov in [75] and [4], which says that for any small subset A of $\mathbb{F}_\ell$, $\max\{|A+A|, |A \cdot A|\} \gg |A|^{1+1/5}$. The main outcome of this approach is the following.

Theorem 1.1.5 (Bhakta, Krishnamoorthy, Muneeswaran). *Let $f(z)$ be any Hecke eigenform with rational coefficients, and S_1, S_2 be any set of primes having positive density with $S_1 \cap S_2 = \phi$. Then there exists an integer N_{S_1,S_2} such that for any integer m with all prime factors larger than N_{S_1,S_2}, and $L^{1/77} \geq m/L$, where L is the largest prime factor of m, and for any $a \in \mathbb{Z}/m\mathbb{Z}$, we can write*

$$\sum_{i=1}^{s} a(n_i) \equiv a \pmod{m}, \ n_i \leq m^{130/33}, \ \forall 1 \leq i \leq s,$$

for some $s \leq 52$. Furthermore, all the prime factors of any such n_i are bounded by $O(m^{65/66})$, and they belong to $S_1 \cup S_2$. Additionally, each n_i has at least one prime factor from both S_1 and S_2.

The reader may note that Theorem 1.1.5 is an improvement over the main result of Shparlinski [85, Theorem 3]. This is because, when $m = \ell$ is a prime, Shparlinski's solutions have order $O(\ell^4)$, while our bound has order $\ell^{130/33}$. Moreover, we have an explicit bound on the number of required terms in the summation. In this context, let us again recall the main result of García and Nicolae in [43]. Their result could be used to have a sharper polynomial bound, but their result does not guarantee a uniform bound on the number of terms.

In Chapter 5, we shall also prove an analog of the same result for a broader family of cuspforms. Moreover, we shall also show that, given any $\varepsilon > 0$, it is possible to produce solutions with all prime factors are $O(m^{\varepsilon})$. In that case, we require ω many pairwise disjoint sets of primes $S_1, S_2, \cdots S_\omega$ with $\varepsilon(1 + \frac{\omega-2}{81}) \gg 2$, and record this result as Theorem 5.3.2 in Chapter 5.

1.2 Galois representations of composite moduli

Serre, in one of his seminal papers [79], entitled *Divisibilité de certaines fonctions arithmétiques*, presented several crucial results concerning the divisibility of certain sequences of integers. As a direct application, he showed that for any integer m, $a(n) \equiv 0 \pmod{m}$ for almost all integers n. In fact, there is a constant $\alpha > 0$ such that $a(n) \not\equiv 0 \pmod{m}$ for $O(x/(\log x)^{\alpha})$ many integers $n \leq x$. However, we do not know whether each non-zero residue class $a \in \mathbb{Z}/m\mathbb{Z}$ can be written as $a(n) \pmod{m}$ with equal proportion. It was mentioned by Serre in page 20 of [79] that, for any odd m, any integer M, and any non-zero $a \in \mathbb{Z}/m\mathbb{Z}$,

$$\#\{n \leq x \mid a(n) \equiv a \pmod{m}\} \gg \frac{x}{\log x}(\log\log x)^M. \tag{1.2}$$

Proof of this argument was based on showing that, for a positive density of primes $p \equiv 1 \pmod{m}$ and $q \equiv -1 \pmod{m}$ the corresponding Hecke operators T_p and T_q acts respectively as 2 and 0 on the $\mathbb{Z}$-module of all holomorphic modular forms with coefficients in $\mathbb{Q}$.

In Chapter 4, we discuss the theory of Galois representations for composite modulus and study the distribution of $\{a(n) \pmod{m} \mid \omega(n) = O(1)\}$, where $\omega(n)$ denotes the number of distinct prime factors of n. Specifically, motivated by Serre's lower bound at (1.2), we delve into the limiting distribution for certain cusp forms with rational coefficients, yielding the following result.

Theorem 1.2.1 (Bhakta, Krishnamoorthy, Muneeswaran)**.** *Let $M \geq 1$ be any integer, and f be any newform without CM, and with coefficients in $\mathbb{Q}$.*

Then under the certain assumptions on m, the following asymptotic formula holds for any tuple

$$\frac{\#\{n \leq x \mid a(n) = a \pmod m,\ \omega(n) = M\}}{\#\{n \leq x \mid \omega(n) = M\}} \sim d_a(m)\frac{1}{m^M},$$

for some $d_a(m) > 0$, which is an effectively computable constant.

We shall write a more precise version in Theorem 4.2.3 in Chapter 4, and for a much broader family of cuspforms.

In Chapter 4, we shall also discuss a special phenomenon regarding the Galois representations for composite modulus, which we call the local-global property of Galois representations: let $E/\mathbb{Q}$ be an elliptic curve. Serre introduced the following representation,

$$\rho_{E,m} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{Aut}_{\mathbb{C}}(E[m]) \cong \mathrm{GL}_2\big(\mathbb{Z}/m\mathbb{Z}\big),$$

where $E[m]$ is the set of m-torsion points in $E(\mathbb{C})$. Serre's open image theorem says that, if E is without complex multiplication, then there exists a constant $c_E > 0$ such that for any prime $\ell > c_E$, the associated representation $\rho_{E,\ell}$ is surjective. It is conjectured that c_E is uniformly bounded. For the known bounds on c_E, the reader may refer to Cojocaru [27] and Zywina [101]. When E has complex multiplication, the surjectivity is not true for large primes; see page 12 in [25]. In general, whether the elliptic curve E is without complex multiplication or not, Serre showed that for any $m \in \mathbb{N}$ with $(m, 30) = 1$, $\rho_{E,m}$ is surjective if and only if $\rho_{E,\ell}$ is surjective for any prime $\ell \mid m$.

In Chapter 4, we shall discuss an analog of Serre's result for elliptic curves over arbitrary number fields. Let E be an elliptic curve over a number field K. The understanding of $\mathrm{im}(\rho_{E,m}) = \mathrm{Gal}(K(E[m])/K)$ requires comprehending each of the groups $\mathrm{Gal}(K(E[m_1])/K)$, $\mathrm{Gal}(K(E[m_2])/K)$, and the *entanglement* $K(E[m_1]) \cap K(E[m_2])$. Studying entanglements is an active area of research, and interested readers may consult [69] for further exploration. While we do not delve deeply into entanglements in this thesis, we extend Serre's analog to pairs of elliptic curves and modular forms of arbitrary weights.

1.3 Vector-valued automorphic forms

Let G be a discrete subgroup of $\mathrm{PSL}_2(\mathbb{R})$. A vector-valued automorphic form of G with respect to a representation $\rho : \mathrm{G} \to \mathrm{GL}_m(\mathbb{C})$ is a holomorphic function $\mathbb{X} : \mathbb{H} \to \mathbb{C}^m$ which has functional and cuspidal behaviour. When ρ

satisfies certain properties and G has finite volume under the natural action on the upper half plane $\mathbb{H} := \{\tau = x + iy \in \mathbb{C} \mid y > 0\}$, then any such vector-valued automorphic form admits a Fourier expansion at any cusp of G.

In the congruence case, let $f : \mathbb{H} \to \mathbb{C}$ be a modular form of level N and weight $k \in \mathbb{Z}$. It is known that $f(\tau)$ has a Fourier expansion at any cusp and the Fourier coefficients have polynomial-growth. To be precise, it is known that the n^{th}-Fourier coefficient $f_{[n]}$ is $\ll n^k$. Throughout the thesis, whenever we state a bound on the Fourier coefficients, we always mean a bound for the absolute value of the same. Note that, when f is a cusp form, it is known that $f_{[n]}$ is $\ll n^{\frac{k}{2}}$. Both of these bounds are obtained by studying the behavior of the function $F(z) = y^\sigma |f(z)|$ in the fundamental domain for any $\sigma \in \mathbb{R}$, and then by comparing $F(z)$ with $F(\gamma z)$ for any $\gamma \in \Gamma_0(N)$ and z in the fundamental domain. We refer the interested reader to [78] about the discussion on the sharper bounds of $f_{[n]}$. Moreover, Selberg mentions in the same article that conjecturally, we may have $f_{[n]} \ll n^{\frac{k}{2}-\frac{1}{2}+\varepsilon}$ for any $\varepsilon > 0$. When f is a normalized Hecke eigenform, it follows from the multiplicativity of the Fourier coefficients and Deligne's bound $f_{[p^\alpha]} \leq (\alpha+1)p^{\alpha\left(\frac{k}{2}-\frac{1}{2}\right)}$ (see [17, 28]) that $f_{[n]} \ll n^{\frac{k}{2}-\frac{1}{2}} d(n)$, where $d(\cdot)$ is the divisor function. This, in particular, settles the conjectural bound since it is known that $d(n) \leq \exp\left(O\left(\frac{\log n}{\log\log n}\right)\right)$. There are some known lower bounds available for $f_{[n]}$ (see [70]), and these results suggest that Deligne's bound is sharp. For applications of growth estimates of the Fourier coefficients of modular forms, we refer the interested reader to [77].

This thesis is concerned with establishing the growth of Fourier coefficients of vector-valued automorphic forms of non-cocompact Fuchsian groups of the first kind. The term *non-cocompact* has been used to specify that the Fuchsian groups of the first kind under consideration are equipped with at least one cusp. To be explicit about the use of the terms vector-valued modular form (vvmf) and vector-valued automorphic form (vvaf), we will make the following distinction between them: ***vvaf for a group commensurable with*** $\mathrm{PSL}_2(\mathbb{Z})$ ***will usually be referred to as vvmf.*** In this sense, we will call our vector-valued functions for Fuchsian groups of the first kind studied in this thesis *vector-valued automorphic forms*.

In the same article [78] mentioned above, Selberg made use of vector-valued modular forms to apply the Rankin-Selberg the method more broadly. This was enough to demand the development of the theory of vector-valued modular forms. Since then, numerous attempts have been made, and theory has slowly emerged. For example, they could be an important tool for understanding the

modular forms for noncongruence subgroups of the modular group. Observe that every component of $\mathbb{X}(\tau)$ will be a scalar-valued modular form for the $\ker(\rho)$, where one could not rule out the possibility of having $\ker(\rho)$ to be a noncongruence subgroup. This could be, on its own, a motivation to study vector-valued modular forms to understand scalar-valued modular forms for noncongruence subgroups. Later in the 1980s, Eichler and Zagier explained in [31] how Jacobi forms and Siegel modular forms could be studied through vector-valued modular forms. For more details on the importance of vector-valued modular forms, see the introduction of [7, 38], and references therein.

Roughly speaking, a vvmf for $\mathrm{PSL}_2(\mathbb{Z})$ of weight $k \in 2\mathbb{Z}$ with respect to a representation $\rho : \mathrm{PSL}_2(\mathbb{Z}) \to \mathrm{GL}_m(\mathbb{C})$ is a vector-valued holomorphic function $\mathbb{X} : \mathbb{H} \to \mathbb{C}^m$ which has a certain functional and cuspidal behaviour. For detailed definition and explanation, see Chapter 6. If $\rho(t)$ is diagonalizable, where $t = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, then each component $\mathbb{X}_i(\tau)$ of $\mathbb{X}(\tau)$ has a convergent q-expansion at cusp infinity. In particular, we can talk about n^{th}-Fourier coefficients $\mathbb{X}_{[i,n]}$'s of $\mathbb{X}_i$'s. We will call such ρ *admissible* otherwise *logarithmic*, which we shall discuss briefly in Chapter 6 and Chapter 7. In the same spirit as in the classical scalar-valued case, Knopp and Mason [51] showed that all of these $\mathbb{X}_{[i,n]} \ll n^{k+2\alpha}$, and the bound is of order $n^{\frac{k}{2}+\alpha}$ when $\mathbb{X}(\tau)$ is a vector-valued cusp form, where α is a constant such that $\|\rho(\gamma)\| \ll \|\gamma\|^{\alpha}$. We always denote norm $\|\cdot\|$ of a matrix in $\mathrm{GL}_n(\mathbb{R})$ as the usual Euclidean norm in $\mathbb{R}^{n^2}$.

For *logarithmic* representation of non-cocompact Fuchsian group of the first kind, the associated vvaf $\mathbb{X}(\tau)$ is a linear combination of certain Fourier expansions, where the coefficients are polynomials in τ, see [53] and Definition 7.1.3. Knopp and Mason [54] have also studied the growth of the Fourier coefficients for vector-valued modular forms of the modular group with respect to the logarithmic representations.

In Chapter 6 and Chapter 7, we prove a generalization of the estimates established by Knopp and Mason in [51, 54] for the Fourier coefficients of vector-valued automorphic forms. More precisely, we shall prove the following.

Theorem 1.3.1 (Bajpai, Bhakta, Finder)**.** *Let* G *be a non-cocompact Fuchsian group of the first kind and* $\rho : \mathrm{G} \to \mathrm{GL}_m(\mathbb{C})$ *be a representation such that all the eigenvalues of the image of each parabolic element have norm* 1.[1] *Let* $\mathfrak{c}$ *be any cusp of* G*. Then there exists a constant* α*, depending on* G*, with the following properties.*

[1] In certain cases we do not need any restriction on the representation, which will be discussed later in Section 6.2.

(i) *If $\mathbb{X}(\tau)$ is a holomorphic vector-valued automorphic form of even integer weight k with respect to ρ, then the sequence of Fourier coefficients of $\mathbb{X}$ at the cusp $\mathfrak{c}$ is $O(n^{k+2\alpha})$.*

(ii) *If $\mathbb{X}(\tau)$ is a vector-valued cusp form, the sequence of Fourier coefficients is $O(n^{k/2+\alpha})$.*

(iii) *Moreover, if $k + 2\alpha < 0$, then $\mathbb{X}(\tau) \equiv 0$.*[2]

In our approach for the admissible case, we build upon the classical methodology, yet the primary hurdle lies in establishing a polynomial bound [9, Lemma 5.3] for the representation ρ. We achieve this by leveraging Beardon's structure theorem for words [9, Lemma 2.4]. However, transitioning to the logarithmic case presents a technical challenge due to the logarithmic representations exhibiting weaker growth. To tackle this issue in Section 7.2.2, we employ a bridging technique to establish a connection between two regions in the upper half-plane.

As a consequence to Theorem 1.3.1, we deduce that for any $1 \leq i \leq m$ and $\alpha \in [0, 1]$, we have the following

$$\sum_{1 \leq n \leq X} \mathbb{X}_{[i,n]} e(n\alpha) \ll X^{k/2} \log X,$$

where $\mathbb{X}_{[i,n]}$ is the n^{th} Fourier coefficient of the i^{th} component of $\mathbb{X}(\tau)$. We shall prove Theorem 1.3.1 for the admissible cases in Chapter 6 and the logarithmic cases in Chapter 7. It will follow from the proof of Theorem 1.3.1 that, for unitary representations, α may be taken to 0. Here by unitary representation, we mean that each element in the image of ρ is a unitary matrix. In particular, when ρ is 1-dimensional, we have recovered the classical bound for the scalar-valued case. The proof is divided into two cases: admissible vvaf and logarithmic vvaf. For their definitions and details, see Section 6.2. We study both cases based on a very classical approach by first looking at what happens to $\|\mathbb{X}(z)\|$ in a suitable fundamental domain and then to know what happens for arbitrary τ in $\mathbb{H}$, we write $\tau = \gamma z$ for z in the fundamental domain and compare $\|\mathbb{X}(\gamma z)\|$ with $\|\mathbb{X}(z)\|$ for any $\gamma \in \mathrm{G}$. In this process, we shall show in Lemma 7.2.3 that the polynomial-growth of ρ based on the structure theorem for elements in Fuchsian groups, first given by Eichler [30, Satz 1], and later generalized by Beardon [12, Theorem 2].

[2]We shall later see that the constants are different for the admissible and logarithmic cases. Here we are considering a maximum of them.

In Chapter 7, we shall discuss sufficient criteria for a representation to have polynomial-growth. It turns out that any element of G has a sufficiently nice enough decomposition in which only finitely many distinct non-parabolic elements are involved. Roughly speaking, this is the reason why polynomial-growth of ρ depends only on the parabolic elements. We record this criterion as Proposition 7.3.1 in Chapter 7. Furthermore, we shall also see what happens to the holomorphic functions on the upper-half plane, which satisfy the functional property with respect to a representation with polynomial-growth. More precisely, we prove the following.

Theorem 1.3.2 (Bajpai, Bhakta, Finder)**.** *Let* G *be a non-cocompact Fuchsian group of the first kind,* $\mathbb{X} : \mathbb{H} \to \mathbb{C}^m$ *be a vector-valued holomorphic function, and* $\rho : \mathrm{G} \to \mathrm{GL}_m(\mathbb{C})$ *be a representation. Suppose that* $\mathbb{X}(\tau)$ *is non-zero, and* $\mathbb{X}(\gamma\tau) = (c\tau + d)^k \rho(\gamma)\mathbb{X}(\tau), \forall \gamma \in \mathrm{G}, \tau \in \mathbb{H}$, *where* $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. *Then, we have the following.*

(a) If ρ *is irreducible and there exists a constant* $\zeta > 0$ *such that* $\|\mathbb{X}(x+iy)\| \ll y^{-\zeta}$ *for all* $x + iy \in \mathbb{H}$, *then*

$$\|\rho(\gamma)\| \ll \|\gamma\|^{2\zeta - k}, \ \forall \gamma \in \mathrm{G}.$$

(b) More generally, if ρ *is irreducible and* $\|\mathbb{X}(x+iy)\| \ll \max_{0 \le j \le m-1}\{|x+iy|^j y^{-\zeta}\}$ *for all* $x + iy \in \mathbb{H}$, *then*

$$\|\rho(\gamma)\| \ll \max\{\|\gamma\|^{j+2\zeta-k}\}_{0 \le j \le m-1}, \ \forall \gamma \in \mathrm{G}.$$

(c) If ρ *is not necessarily irreducible, then some subrepresentation* ρ' *of* ρ *must have a similar growth. In particular, if* ρ *is decomposable, then some of the irreducible components of* ρ *have similar growth.*

The reader may consider this as a converse to Theorem 1.3.1. In particular, this shows that the assumption on representation ρ is necessary and sufficient in Theorem 1.3.1.

Let H be a Fuchsian group of the first kind, ρ be an associated representation, and G be another Fuchsian group of the first kind such that H has finite index in G. Let $\mathbb{X}(\tau)$ be a vector-valued automorphic form associated ρ and write $\mathrm{G}/\mathrm{H} = \{g_1, g_2, \cdots, g_r\}$. Then $\widetilde{X}(\tau) := (\mathbb{X}(g_1^{-1}\tau), \mathbb{X}(g_2^{-1}\tau), \cdot, \mathbb{X}(g_r^{-1}\tau))$ is a vvaf associated to the induced representation $\mathrm{Ind}_{\mathrm{H}}^{\mathrm{G}}(\rho)$. Bajpai in [7] proved that if $\mathbb{X}(\tau)$ is admissible, then $\widetilde{X}$ is admissible as well. In Chapter 7, we first extend this to any arbitrary representations. Consequently, we show that if $\mathbb{X}(\tau)$ is an admissible vvaf of weight 0 associated to H, then the growth of the Fourier coefficients for any lift $\widetilde{\mathbb{X}}(\tau)$, depends only on H. However, it turns out that in the logarithmic case, the exponent might increase a bit.

1.4 Valuations and character sums for Elliptic sequences

Let $n \neq \pm 1$ be any fixed integer. Classically, a rational prime p is called a non-Wieferich prime with respect to base n, if

$$n^{p-1} \equiv 1 \pmod{p} \text{ and } n^{p-1} \not\equiv 1 \pmod{p^2},$$

holds simultaneously. It is not known whether there are infinitely many non-Wieferich primes or not. Under ABC conjecture, it is known that there are infinitely many non-Wieferich primes with (non-trivial) base n. By non-trivial, we mean $n \neq \pm 1$. Silverman showed that there are at least $c \log x$ many non-Wieferich primes up to x, for some constant $c > 0$, depending on base a. The reader may note that heuristically, the number of Wieferich primes up-to x

$$\sum_{p \leq x} \frac{1}{p} = \log \log x,$$

as the probability that $\frac{n^{p-1}-1}{p}$ is divisible by p can be naively guessed to be $\frac{1}{p}$. Specifically, heuristically, the number of non-Wieferich primes up to x is approximately $\frac{x}{\log x} - \log \log x$.

Let G be a commutative algebraic group, and $P \in G(\mathbb{Q})$ is a point of infinite order. An analogous problem in this generalized situation asks whether $N_p P \equiv 1 \pmod{p^2}$, where $N_p = |G(\mathbb{F}_p)|$. For instance, when we take G to be the multiplicative group $\mathbb{G}_m$, and $P \in \mathbb{G}_m(\mathbb{Q})$ to be a *non-torsion* unit, the problem then asks about the order of P when reduced modulo p^2.

Silverman studied this general problem over elliptic curves. He showed that under ABC, there are infinitely many (in fact, an asymptotic lower bound of order $c\sqrt{\log x}$) non-Wieferich primes for elliptic curves with j invariant 0 and 1728. This assumption on the invariant j was later removed by Kühn and Müller [60]. The author recently considers the number field analog in [13], and a lower bound of the same order is achieved.

In Chapter 2, we study linear recurrence sequences and the associated exponential sums. In Chapter 8, we shall introduce the special kind of nonlinear recurrence sequences, widely known as *elliptic sequences*. An elliptic sequence $\{\beta_n\}$ is a non-linear recurrence sequence of the form

$$\beta_{n+m}\beta_{n-m}\beta_r^2 = \beta_{m+r}\beta_{m-r}\beta_n^2 - \beta_{n+r}\beta_{n-r}\beta_m^2.$$

Generally, it is difficult to control the valuations of terms of an elliptic sequence. A prime p is called an *elliptic non-Wieferich* prime if $\nu_p(\beta_n) = 1$

for some integer n. As already mentioned, Silverman [87] showed that, under the ABC conjecture, the number of such primes $p \leq x$ has the lower bound of order $\sqrt{\log x}$. In Chapter 8, we shall show that it is possible unconditionally to count the number of primes p for which $\mathrm{ord}(\chi(p)) \nmid v_p(\beta_n)$, for some n, and some Dirichlet character χ. The importance lies in the understanding of the p-adic valuations of points in $E(\mathbb{Q}_p)$. However, we generally lack control over the size of this valuation, due to the connections with elliptic Wieferich primes. In this context, our objective is to showcase the achievement of managing the valuations modulo $\mathrm{ord}(\chi)$. Specifically, we will establish the following outcome.

Theorem 1.4.1 (Bhakta)**.** *Let χ be a Dirichlet character satisfying certain properties. Then unconditionally we get at least $\gg_\chi \frac{\sqrt{\log x}}{\log\log x}$ many such primes p up-to x.*

We shall state this more precisely in Chapter 8. This is proved by showing that there exists a set of primes ℓ of positive density, for which $\mathrm{ord}(\chi(p)) \nmid v_p(\beta_\ell)$ for some prime p. We record this as Proposition 8.0.5. To prove Theorem 1.4.1, we need the following assumptions on the Dirichlet character χ:

$$\begin{aligned}
&\chi(|\beta_\alpha|) \neq 0, 1, \quad \text{or} \\
&\chi(-|\beta_\alpha|) \neq 0, 1 \text{ and } 4 \nmid \pi, \quad \text{or} \\
&\chi(-|\beta_\alpha|) \neq 0, 1 \text{ and } P \in E(\mathbb{R})^0.
\end{aligned}$$

We briefly study the proportion of the characters satisfying these conditions. One of the key features of this chapter is the study of associated character sums. For prime p, and any Dirichlet character χ modulo p, we study

$$S_{\chi,\pi}(P) = \sum_{1 \leq n \leq R} \chi(\beta_n),$$

where R is the order of $P \pmod p$. To estimate this, we follow the approach of Shparlinski and Stange in [86]. Under certain conditions on the sequence (β_n), we obtain non-trivial bounds when χ does not have a large order, and $R \gg p^{1-\varepsilon}$. We note that this is related to the *elliptic analog of Artin's primitive root conjecture*. However, we shall show that a much smaller exponent $1/3 - \varepsilon$ could be achieved. In particular, one can use [21, Theorem 2] by Bourgain, Gilbichuck to obtain non-trivial bounds for the associated multi-linear exponential sums.

Basic Sieving tools show that almost all integers are not sums of two squares. Landau and Ramanujan independently proved a famous theorem that

quantifies this result, showing that for large B, the number of positive integers below B that are the sum of two square numbers behaves asymptotically as $\asymp \frac{B}{(\log B)^{1/2}}$. Building upon Proposition 8.0.5, [16] establishes an elliptic counterpart, which can be stated as follows.

Theorem 1.4.2 (Bhakta, Loughran, Myerson, Nakahara)**.** *Let E be an elliptic curve over $\mathbb{Q}$ given by an integral Weierstrass equation. Let $P \in E(\mathbb{Q})$ have infinite order with $P \in E(\mathbb{R})^0$. Then there exists $\omega = \omega(E, P) > 0$ such that*

$$\#\{n \in \mathbb{Z} \colon |n| \leq B, y(nP) \text{ is a sum of two squares}\} \ll_{E,P} \frac{B}{(\log B)^{\omega}}.$$

Here $E(\mathbb{R})^0$ denotes the connected component of the identity of $E(\mathbb{R})$, and $y(nP)$ denotes the y-coordinate of the point nP. The result shows that for almost all multiples of P, the y-coordinate is not a sum of two (rational) squares. The key tools in the proof are sieves and elliptic divisibility sequences. In the classical sieve framework, the standard strategy involves sieving with the homomorphisms $\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$, for many primes p. Kowalski [59] introduced an elliptic analog of the sieve setup, involving sieving with homomorphisms from $E(\mathbb{Q}) \to E(\mathbb{Z}/p\mathbb{Z})$. This sieve operates similarly to the traditional integer sieve, employing reductions modulo primes p where $\operatorname{ord}(P \pmod p) = \ell_p$ is itself a prime. In this context, understanding the p-adic valuations of points $\ell_p P \in E(\mathbb{Q}_p)$ is crucial. Our strategy in [16] focused on eliminating certain multiples of a given non-torsion point, where we can control the valuation modulo suitable integers. This is where Proposition 8.0.5 plays an important role.

To establish Proposition 8.0.5, the crucial property is that elliptic divisibility sequences exhibit periodicity modulo any arbitrary integer (as stated in Proposition 8.1.10). We achieve this in Chapter 8 using the work of Verzobio [97], which does not seem to have been proven in the literature before in this generality. In our proof, we also have to be careful with signs, which requires us to use [90] and equidistribution results for multiples of irrational numbers modulo 1.

In this regard, we would like to point out that the proof of Theorem 1.4.2 in [16] gives an explicit value for ω, but we doubt that the bound is sharp. The following question seems quite challenging.

Question 1.4.3. *Does there exist an elliptic curve E over $\mathbb{Q}$ such that the set*

$$\{(x, y) \in E(\mathbb{Q}) \colon y \text{ is a sum of two squares}\} \tag{1.3}$$

is infinite?

The following heuristic suggests (1.3) should be quite sparse: The numerator and denominator of $y(nP)$ have size $\exp(O_{E,P}(n^2))$, and a proportion $1/n$ of such integers are sums of two squares. One might therefore ask if $\sum_{n\leq B} 1/n \sim \log B$ is roughly the true order of magnitude in Theorem 1.4.2, providing it is infinite. Versions of this problem were raised by Poonen [66, Question 33, p55] and Browning [24, Problem 10, pp3181-2].

Chapter 2

Exponential sums for linear recurrence sequences

Let $r \geq 1$ be an integer and p be an arbitrary prime number. A *linear recurrence sequence* $\{s_n\}$ of order r in $\mathbb{F}_p$ consists of a recursive relation

$$s_{n+r} \equiv a_{r-1}s_{n+r-1} + \cdots + a_0 s_n \pmod{p}, \quad \text{with } n = 0, 1, 2, \ldots, \tag{2.1}$$

and initial values $s_0, \ldots, s_{r-1} \in \mathbb{F}_p$. Here $a_0, \ldots, a_{r-1} \in \mathbb{F}_p$ are fixed. The *characteristic polynomial* $\omega(x)$ *associated to* $\{s_n\}$ is

$$\omega(x) = x^r - a_{r-1}x^{r-1} - \cdots - a_1 x - a_0.$$

Under certain assumptions, linear recurrence sequences become periodic modulo p, see [58, Lemma 6.4] and [62, Theorem 6.11].

Let p be a prime number and $\omega(x)$ be the characteristic polynomial of a linear recurrence sequence $\{s_n\}$ defined by equation (2.1). If $(a_0, p) = 1$ and at least one of the $s_0, \ldots, s_{r-1}$ are not divisible by p, then the sequence $\{s_n\}$ is periodic modulo p, that is for some $T \geq 1$,

$$s_{n+T} \equiv s_n \pmod{p}, \qquad n = 0, 1, 2, \ldots .$$

The least positive period is denoted by τ. Moreover, $\tau \leq p^r - 1$ and τ divides T for any period $T \geq 1$ of the sequence $\{s_n\}$.

2.1 On the known estimates for the prime fields

In 1953, Korobov [57] obtained bounds for rational exponential sums involving linear recurrence sequences in residue classes. In particular, for the fields of

order p, if $\{s_n\}$ is a linear recurrence sequence of order r with $(a_0, p) = 1$ and period τ, it follows that

$$\left|\sum_{n\leq\tau} \mathbf{e}_p\left(s_n\right)\right| \leq p^{r/2}. \tag{2.2}$$

Note that such a bound is nontrivial if $p^{r/2} < \tau$ and asymptotically effective only if $p^{r/2}/\tau \to 0$ as $p \to \infty$. Estimate (2.2) is optimal in general terms, indeed Korobov [58] showed that there is a linear recurrence sequence $\{s_n\}$ with length r satisfying

$$\frac{1}{2}p^{r/2} < \left|\sum_{n\leq\tau} \mathbf{e}_p\left(s_n\right)\right| \leq p^{r/2}.$$

In turn, for any given $\varepsilon > 0$, it has been proved that there exists a class of linear recurrence sequences with a better upper bound

$$\left|\sum_{n\leq\tau} \mathbf{e}_p\left(s_n\right)\right| \leq \tau^{1/2+\varepsilon}.$$

However, the proof of the existence is ineffective in the sense that we do not know any explicit characteristics of such family, see [35, Section 5.1].

The case when the associated polynomial $\omega(x)$ is irreducible in $\mathbb{F}_p[x]$, was widely studied. In particular, from a more general result due to Katz [49, Theorem 4.1.1.] it follows that if $\omega(0) = 1$ then

$$\left|\sum_{n\leq\tau} \mathbf{e}_p\left(s_n\right)\right| \leq p^{(r-1)/2}.$$

Shparlinski [84] improved Korobov's bound for all nonzero linear recurrence sequences with irreducible characteristic polynomial $\omega(x)$ in $\mathbb{F}_p[x]$. From [84, Theorem 3.1] we get

$$\max_{\xi\in\mathbb{F}_p^*}\left|\sum_{n\leq\tau} \mathbf{e}_p\left(\xi s_n\right)\right| \leq \tau p^{-\varepsilon/(r-1)} + r^{3/11}\tau^{8/11}p^{(3r-1)/22},$$

for any given $\varepsilon > 0$ and with period τ satisfying that

$$\max_{\substack{d<r\\ d|r}} \gcd(\tau, p^d - 1) < \tau p^{-\varepsilon}. \tag{2.3}$$

In particular, if r is fixed then the upper bound is non trivial for $\tau \geq p^{r/2-1/6+\varepsilon}$.

We already pointed out that the inequality (2.2) is nontrivial for $\tau > p^{r/2+\varepsilon}$, so the most important case occurs when $\tau \leq p^{r/2+\varepsilon}$. If $\tau \leq p^{r/2+\varepsilon}$, then condition (2.3) is needed to obtain a non-trivial bound suggested by an example given in [84, Section 1]. In this particular example, the exponential sums of type

$$\left| \sum_{n=1}^{(p^m-1)/2} \mathbf{e}_p\left(\mathrm{Tr}(ag^{2n})\right) \right| = \frac{(p^m-1)}{2},$$

are considered for certain a in $\mathbb{F}_{p^m}^*$ with g a generator of $\mathbb{F}_{p^m}^*$ and m be any even integer. It is worth noting that $\{\mathrm{Tr}(ag^{2n})\}$ is indeed a linear recurrence sequence of order m in $\mathbb{F}_p$.

2.2 On the improved estimate

In this section, we consider the general case when the associated polynomial $\omega(x)$ is not necessarily irreducible, and deduce the following key result.

Theorem 2.2.1 (Bajpai, Bhakta, García)**.** *Let p be a large prime number and $\varepsilon > \varepsilon' > 0$. Suppose that $\{s_n\}$ is a nonzero linear recurrence sequence with positive order and period τ in $\mathbb{F}_p$ such that its characteristic polynomial $\omega(x)$ has distinct roots in its splitting field, and $(\omega(0), p) = 1$. Set $\omega(x) = \prod_i^{\nu} \omega_i(x)$ as a product of distinct irreducible polynomials in $\mathbb{F}_p[x]$, and for each i, α_i denotes a root of $\omega_i(x)$. If all polynomials $\omega_i(x)$ have the same degree, i.e. $\deg \omega_i(x) = r > 1$, and the system $\tau_i = \operatorname{ord} \alpha_i$, satisfies*

a) $\max\limits_{\substack{d<r \\ d|r}} \gcd(\tau_i, p^d - 1) < \tau_i p^{-\varepsilon}, \quad$ *for any* $1 \leq i \leq \nu,$ (2.4)

b) $\gcd(\tau_i, \tau_j) < p^{\varepsilon'}$, *for some pair $i \neq j$ along with $\mathbb{F}_p(\alpha_i) \cong \mathbb{F}_p(\alpha_j)$,*

then there exists a $\delta = \delta(\varepsilon, \varepsilon') > 0$ such that

$$\max_{\xi \in \mathbb{F}_p^*} \left| \sum_{n \leq \tau} \mathbf{e}_p\left(\xi s_n\right) \right| \leq \tau p^{-\delta}. \tag{2.5}$$

It turns out that, this extends [19, Corollary] due to Bourgain, where all of the irreducible factors have degree $r = 1$, while Theorem 2.2.1 deals with the case $r \geq 2$.

Recalling the example of Shparlinski in [84, Section 1], we already noticed in Section 2.1 that, condition **a)** of Theorem 2.2.1 is needed if $\omega(x)$ is irreducible in $\mathbb{F}_p[x]$. We shall discuss more about this condition later in Remark 2.2.3.

Now, we illustrate with an example that all of the $\gcd(\tau_i, \tau_j)'s$ cannot be too large. In other words, we need condition **b)** (or some other condition) to obtain a non-trivial bound in Theorem 2.2.1. For example, let $r = 2$ and g be a generator of $\mathbb{F}_{\ell^2}^*$. Then, consider the sequence

$$s_n = \operatorname{Tr}\left(g^{n(\ell^2+1)/2} - g^n\right),$$

with characteristic polynomial $(x-g)(x-g^{\ell})(x-g^{(\ell^2+1)/2})(x-g^{\ell(\ell^2+1)/2})$. Note that

$$\tau_2 = \operatorname{ord} g = \ell^2 - 1 \text{ and } \tau_1 = \operatorname{ord} g^{(\ell^2+1)/2} = \tfrac{\ell^2-1}{\gcd(\ell^2-1,(\ell^2+1)/2)}.$$

It is easy to see that $\gcd(\ell^2-1, (\ell^2+1)/2) = 1$, so $\gcd(\tau_1, \tau_2) = \ell^2 - 1$. On another hand we note that $\gcd(\tau_1, \ell - 1) = \ell - 1$. Then, one can show that

$$\begin{aligned}
\sum_{n=1}^{\ell^2-1} \mathbf{e}_\ell(s_n) &= \sum_{n=1}^{\ell^2-1} \mathbf{e}_\ell\left(\operatorname{Tr}\left(g^{n(\ell^2+1)/2} - g^n\right)\right) \\
&= \sum_{n=1}^{(\ell^2-1)/2} \mathbf{e}_\ell\left(\operatorname{Tr}\left(g^{2n(\ell^2+1)/2} - g^{2n}\right)\right) + \sum_{n=1}^{(\ell^2-1)/2} \mathbf{e}_\ell\left(\operatorname{Tr}\left(g^{(2n-1)(\ell^2+1)/2} - g^{2n-1}\right)\right) \\
&= \frac{\ell^2-1}{2} + \sum_{n=1}^{(\ell^2-1)/2} \mathbf{e}_\ell\left(\operatorname{Tr}\left(-2g^{2n-1}\right)\right) = \frac{\ell^2-1}{2} + \sum_{h\in H} \mathbf{e}_\ell\left(\operatorname{Tr}\left(-2gh\right)\right),
\end{aligned}$$

where $H = \langle g^2 \rangle$.

Let p be any prime and q be any power of p. Then, the classical theorem about additive sums for one-variable polynomial, due to A. Weil (see [59, Theorem 3.2]), states that for a given polynomial $f(x) \in \mathbb{F}_q[x]$ with degree d, $d < q$, $\gcd(d, q) = 1$ and a nontrivial additive character ψ in $\mathbb{F}_q$, we have

$$\left|\sum_{x\in\mathbb{F}_q} \psi(f(x))\right| \leq (d-1)\sqrt{q}. \tag{2.6}$$

Consider

$$1 + 2\sum_{h\in H} \mathbf{e}_\ell\left(\operatorname{Tr}\left(-2gh\right)\right) = \sum_{x\in\mathbb{F}_{\ell^2}} \psi(x^2),$$

where $\psi(\omega) = \mathbf{e}_\ell(\operatorname{Tr}(-2g\omega))$ is a nonzero additive character of $\mathbb{F}_{\ell^2}$. Applying (2.6) with $f(x) = x^2$, it follows that

$$\left|\sum_{h\in H} \mathbf{e}_\ell(\operatorname{Tr}(-2gh))\right| \le \left|\sum_{x\in\mathbb{F}_{\ell^2}} \psi(x^2)\right| \le \ell.$$

Therefore, the linear recurrence sequence $\{s_n\}$ satisfies

$$\sum_{n=1}^{\ell^2-1} \mathbf{e}_\ell(s_n) = \frac{\ell^2-1}{2} + O(\ell).$$

We now need to discuss some necessary background. Let K be a finite field of characteristic p and F be an extension of K with $[F:K] = r$. The *trace* function $\operatorname{Tr}_{F/K} : F \to K$ is defined by

$$\operatorname{Tr}_{F/K}(z) = z + z^p + \cdots + z^{p^{r-1}}, \qquad z \in F.$$

The following properties of $\operatorname{Tr}_{F/K}(z)$ are well known.

$$\operatorname{Tr}_{F/K}(az+w) = a\operatorname{Tr}_{F/K}(z) + \operatorname{Tr}_{F/K}(w), \quad \text{for all } a \in K,\ z, w \in F. \tag{2.7}$$

$$\operatorname{Tr}_{F/K}(a) = ra, \quad \text{for any} \quad a \in K. \tag{2.8}$$

$$\operatorname{Tr}_{F/K}(z^p) = \operatorname{Tr}_{F/K}(z), \quad \text{for any} \quad z \in F. \tag{2.9}$$

Throughout this section, $F = \mathbb{F}_q$, $K = \mathbb{F}_p$ with $q = p^r$ and we will simply write $\operatorname{Tr}(z)$ instead $\operatorname{Tr}_{F/K}(z)$.

Let $\{s_n\}$ be a linear recurrence sequence of order $r \ge 1$ in $\mathbb{F}_p$ with characteristic polynomial $\omega(x)$ in $\mathbb{F}_p[x]$. It is well known that n^{th}-term can be written in terms of the roots of the characteristic polynomial, see Theorem 6.21 in [62]. Therefore, if the roots $\alpha_0, \ldots, \alpha_{r-1}$ of $\omega(x)$ are all distinct in its splitting field, then

$$s_n = \sum_{i=0}^{r-1} \beta_i \alpha_i^n, \quad \text{for } n = 0, 1, 2, \ldots, \tag{2.10}$$

where $\beta_0, \ldots, \beta_{r-1}$ are uniquely determined by initial values $s_0, \ldots, s_{r-1}$, and belong to the splitting field of $\omega(x)$ over $\mathbb{F}_p$. If the characteristic polynomial $\omega(x)$ is irreducible and α is a root, then its r distinct conjugates are

$$\alpha, \alpha^p, \ldots, \alpha^{p^{r-2}}, \alpha^{p^{r-1}}.$$

Hence, the coefficients s_n are given by

$$s_n = \sum_{i=0}^{r-1} \beta_i \alpha^{p^i n}, \qquad n = 0, 1, 2, 3, \ldots .$$

One of our main tools is the bound for Gauss sum in finite fields given by Bourgain and Chang [20, Theorem 2]. This will be required to prove Theorem 2.2.1. Assume that for a given $\alpha \in \mathbb{F}_q$ and $\varepsilon > 0$, such that $\operatorname{ord}\alpha = t$ satisfies

$$t > p^{\varepsilon} \quad \text{and} \quad \max_{\substack{1\le d<r\\ d\mid r}} \gcd(t, p^d - 1) < tp^{-\varepsilon}. \tag{2.11}$$

Then, there exists a $\delta = \delta(\varepsilon) > 0$ such that for any nontrivial additive character ψ of $\mathbb{F}_q$, we have

$$\left|\sum_{n\le t} \psi(\alpha^n)\right| \le tp^{-\delta}.$$

Note that the second assumption in (2.11) implies the first one whenever $r \ge 2$.

2.2.1 Proof of Theorem 2.2.1

We proceed by induction over ν. Before that, following properties (2.7) and (2.8) of trace function we write

$$s_n = \operatorname{Tr}\left(r^{-1}s_n\right) = r^{-1}\operatorname{Tr}\left(\sum_{i=1}^{\nu}(\beta_{i,0}\alpha_i^n + \cdots + \beta_{i,r-1}\alpha_i^{p^{r-1}n})\right) = r^{-1}\sum_{i=1}^{\nu}\sum_{j=0}^{r-1}\operatorname{Tr}\left(\beta_{i,j}\alpha_i^{p^j n}\right).$$

By the assumption, $[\mathbb{F}_p(\alpha_i) : \mathbb{F}_p] = r$ for any $1 \le i \le \nu$. In other words, any such α_i is in $\mathbb{F}_{p^r}$. We then have, $r = [\mathbb{F}_p(\alpha_1, \ldots, \alpha_\nu) : \mathbb{F}_p]$ and $z^{p^r} = z$ for any $z \in \mathbb{F}_p(\alpha_1, \ldots, \alpha_\nu)$. In addition, from (2.9) it follows that, $\operatorname{Tr}(z^p) = \operatorname{Tr}(z)$ for any $z \in \mathbb{F}_p(\alpha_1, \ldots, \alpha_\nu)$. Then, for each pair (i, j), raising each argument $\beta_{i,j}\alpha_i^{p^j n}$ to the power p^{r-j}

$$\operatorname{Tr}\left(\beta_{i,j}\alpha_i^{p^j n}\right) = \operatorname{Tr}\left(\beta_{i,j}^{p^{r-j}}\alpha_i^{p^j n\cdot p^{r-j}}\right) = \operatorname{Tr}\left(\beta_{i,j}^{p^{r-j}}\alpha_i^{p^r n}\right) = \operatorname{Tr}\left(\beta_{i,j}^{p^{r-j}}\alpha_i^{n}\right).$$

This implies that

$$\begin{aligned} s_n &= r^{-1}\sum_{i=1}^{\nu}\sum_{j=0}^{r-1}\operatorname{Tr}\left(\beta_{i,j}^{p^{r-j}}\alpha_i^n\right) = r^{-1}\sum_{i=1}^{\nu}\operatorname{Tr}\left(\left(\sum_{j=0}^{r-1}\beta_{i,j}^{p^{r-i}}\right)\alpha_i^n\right) \\ &= \operatorname{Tr}(\gamma_1\alpha_1^n) + \cdots + \operatorname{Tr}(\gamma_\nu\alpha_\nu^n), \end{aligned} \tag{2.12}$$

where $\gamma_i = r^{-1}\sum_{j=0}^{r-1}\beta_{i,j}^{p^{r-i}}$, for each $1 \le i \le \nu$.

The case $\nu = 1$ follows from Bourgain and Chang [20, Theorem 2], considering the additive character $\operatorname{Tr}(\gamma_1 x)$. We shall proceed inductively, and $\nu = 2$ will be the base case. We start by denoting $h = \gcd(\tau_1, \tau_2)$. It is clear that $\operatorname{lcm}(\tau_1, \tau_2) = \tau_1\tau_2/h$ is a period of s_n, then

$$\left|\sum_{n\le\tau}\mathbf{e}_p(\xi s_n)\right| = \frac{\tau}{\tau_1\tau_2/h}\left|\sum_{n\le\frac{\tau_1\tau_2}{h}}\mathbf{e}_p(\xi s_n)\right|.$$

Hence, it is enough to prove that

$$\left|\sum_{n\leq \frac{\tau_1\tau_2}{h}} \mathbf{e}_p\left(\xi s_n\right)\right| \leq \frac{\tau_1\tau_2}{h} p^{-\delta}, \quad \text{with } (\xi, p) = 1,$$

for some $\delta = \delta(\varepsilon) > 0$. Dividing the range of the sum $n \leq \tau_1\tau_2/h$ into the form $n = mh + u_0$ with $m \leq \tau_1\tau_2/h^2$ and $0 \leq u_0 \leq h-1$, we have

$$\begin{aligned}\left|\sum_{n\leq \frac{\tau_1\tau_2}{h}} \mathbf{e}_p\left(\xi s_n\right)\right| &= \left|\sum_{u_0=0}^{h-1} \sum_{n\leq \frac{\tau_1\tau_2}{h^2}} \mathbf{e}_p\left(\xi s_{nh+u_0}\right)\right| \leq \sum_{u_0=0}^{h-1} \left|\sum_{n\leq \frac{\tau_1\tau_2}{h^2}} \mathbf{e}_p\left(\xi s_{nh+u_0}\right)\right| \\ &\leq h \times \max_{0\leq u_0\leq h-1} \left|\sum_{n\leq \tau_1\tau_2/h^2} \mathbf{e}_p\left(\xi s_{nh+u_0}\right)\right|. \end{aligned} \tag{2.13}$$

Let (n_1, n_2) be a tuple with $n_i \leq \frac{\tau_i}{h}$. Since $\gcd(\frac{\tau_1}{h}, \frac{\tau_2}{h}) = 1$, by Chinese remainder theorem, there exist integers m_1, m_2 with $\gcd(m_1, \frac{\tau_1}{h}) = \gcd(m_2, \frac{\tau_2}{h}) = 1$, such that

$$\left|\left\{n \pmod{\tfrac{\tau_1\tau_2}{h^2}} : 1 \leq n \leq \frac{\tau_1\tau_2}{h^2}\right\}\right| = \left|\left\{n_1m_1\tfrac{\tau_2}{h} + n_2m_2\tfrac{\tau_1}{h} \pmod{\tfrac{\tau_1\tau_2}{h^2}} : 1 \leq n_i \leq \frac{\tau_i}{h}\right\}\right|. \tag{2.14}$$

Moreover, the pair (m_1, m_2) has the following property: given (n_1, n_2), with $1 \leq n_i \leq \tau_i/h$, then $n = n_1m_1\frac{\tau_2}{h} + n_2m_2\frac{\tau_1}{h}$ satisfies

$$n \equiv n_1 \pmod{\tfrac{\tau_1}{h}} \text{ and } n \equiv n_2 \pmod{\tfrac{\tau_2}{h}},$$

and n is unique modulo $\frac{\tau_1\tau_2}{h^2}$. Since $\frac{\tau_1}{h} = \operatorname{ord}\alpha_1^h$ and $\frac{\tau_2}{h} = \operatorname{ord}\alpha_2^h$, then

$$\alpha_i^{hn} = \alpha_i^{h(n_1m_1\frac{\tau_2}{h} + n_2m_2\frac{\tau_1}{h})} = \alpha_i^{hn_i}, \quad 1 \leq i \leq 2. \tag{2.15}$$

Combining (2.14) and (2.15), we have

$$\begin{aligned}\left|\sum_{n\leq \frac{\tau_1\tau_2}{h^2}} \mathbf{e}_p\left(\xi s_{nh+u_0}\right)\right| &= \left|\sum_{n_1\leq \frac{\tau_1}{h}} \mathbf{e}_p\left(\operatorname{Tr}\left(\xi\gamma_1\alpha_1^{n_1h+u_0}\right)\right)\right| \times \left|\sum_{n_2\leq \frac{\tau_2}{h}} \mathbf{e}_p\left(\operatorname{Tr}\left(\xi\gamma_2\alpha_2^{n_2h+u_0}\right)\right)\right| \\ &= \left|\sum_{n_1\leq \frac{\tau_1}{h}} \mathbf{e}_p\left(\operatorname{Tr}\left(\gamma_1'\alpha_1^{n_1h}\right)\right)\right| \times \left|\sum_{n_2\leq \frac{\tau_2}{h}} \mathbf{e}_p\left(\operatorname{Tr}\left(\gamma_2'\alpha_2^{n_2h}\right)\right)\right|, \end{aligned} \tag{2.16}$$

with $\gamma_1' = \xi\gamma_1\alpha_1^{u_0}, \gamma_2' = \xi\gamma_2\alpha_2^{u_0}$ in $\mathbb{F}_p(\alpha_1, \alpha_2)$. Since $\{s_n\}$ is a nonzero sequence, therefore $\gamma_i' \neq 0$, at least for some $1 \leq i \leq 2$. First, let us assume that $\gamma_1', \gamma_2' \neq 0$.

Each $\mathbf{e}_p\left(\operatorname{Tr}\left(\xi\gamma_i' z\right)\right)$ corresponds to a nontrivial additive character, say $\psi_i(z)$, in $\mathbb{F}_p(\alpha_i) = \mathbb{F}_{p^r}$. In order to satisfy condition (2.11), we first recall assumptions $h < p^{\varepsilon'}$, $\varepsilon > \varepsilon' > 0$ and $\max_{\substack{d<r \\ d|r}} \gcd(\tau_i, p^d - 1) < \tau_i p^{-\varepsilon}$ for some $i \in \{1, 2\}$. Without loss of generality, let us assume that $i = 1$. Then, for any $d|r$ with $1 \leq d < r$, we have

$$\gcd\left(\tfrac{\tau_1}{h}, p^d - 1\right) \leq \gcd(\tau_1, p^d - 1) < \tau_1 p^{-\varepsilon} < \frac{\tau_1}{h} p^{-(\varepsilon - \varepsilon')}.$$

Therefore, by Bourgain and Chang [20, Theorem 2] it follows that

$$\left|\sum_{n_1 \leq \tau_1/h} \mathbf{e}_p\left(\operatorname{Tr}\left(\gamma_1'\alpha_1^{n_1 h}\right)\right)\right| = \left|\sum_{n_1 \leq \tau_1/h} \psi_1(\alpha_1^{n_1 h})\right| \leq \frac{\tau_1}{h} p^{-\delta}.$$

On the other hand, bounding trivially we have

$$\left|\sum_{n_2 \leq \tau_2/h} \mathbf{e}_p\left(\operatorname{Tr}\left(\gamma_2'\alpha_2^{n_2 h}\right)\right)\right| = \left|\sum_{n_2 \leq \tau_2/h} \psi_2(\alpha_2^{n_2 h})\right| \leq \frac{\tau_2}{h}.$$

Thus, combining above equations with (2.13) and (2.16) we get

$$\max_{\xi \in \mathbb{F}_p^*} \left|\sum_{n \leq \frac{\tau_1\tau_2}{h}} \mathbf{e}_p\left(\xi s_n\right)\right| \leq h \times \frac{\tau_1\tau_2}{h^2} p^{-\delta} = \frac{\tau_1\tau_2}{h} p^{-\delta}.$$

Now, let us assume that one of the $\lambda_i' = 0$, say for $i = 2$. Arguing exactly as few lines above, it follows from assumption (a) that

$$\left|\sum_{n_1 \leq \tau_1/h} \mathbf{e}_p\left(\operatorname{Tr}\left(\gamma_1'\alpha_1^{n_1 h}\right)\right)\right| \leq \frac{\tau_1}{h} p^{-\delta}, \quad \text{and} \quad \left|\sum_{n_2 \leq \tau_2/h} \mathbf{e}_p\left(\operatorname{Tr}\left(\gamma_2'\alpha_2^{n_2 h}\right)\right)\right| = \frac{\tau_2}{h}.$$

Hence, the desired bound follows. This conclude the case $\nu = 2$.

Now, we proceed by induction over ν, and assume Theorem 2.2.1 to be true up to $\nu - 1$. We follow the idea due to Garaev [40, Section 4.4]. Considering (2.12) and periodicity, for any $t \geq 1$ we get

$$\begin{aligned}
\tau\left|\sum_{n \leq \tau} \mathbf{e}_p\left(\xi s_n\right)\right|^{2t} &= \sum_{m \leq \tau}\left|\sum_{n \leq \tau} \mathbf{e}_p\left(\xi s_{m+n}\right)\right|^{2t} \\
&= \sum_{m \leq \tau}\left|\sum_{n \leq \tau} \mathbf{e}_p\left(\xi(\operatorname{Tr}\left(\gamma_1\alpha_1^{m+n}\right) + \cdots + \operatorname{Tr}\left(\gamma_\nu\alpha_\nu^{m+n}\right))\right)\right|^{2t} \\
&\leq \sum_{n_1 \leq \tau} \cdots \sum_{n_{2t} \leq \tau}\left|\sum_{m \leq \tau} \mathbf{e}_p\left(\xi \sum_{i=1}^{\nu} \operatorname{Tr}\left(\gamma_i\alpha_i^m\left(\alpha_i^{n_1} + \cdots - \alpha_i^{n_{2t}}\right)\right)\right)\right|.
\end{aligned}$$

Raising to the power $2t$, and applying Cauchy–Schwarz, we have

$$\tau^{2t}\left|\sum_{n\leq\tau}\mathbf{e}_p\left(\xi s_n\right)\right|^{4t^2}\leq\tau^{2t(2t-1)}\sum_{n_1\leq\tau}\cdots\sum_{n_{2t}\leq\tau}\left|\sum_{m\leq\tau}\mathbf{e}_p\left(\xi\sum_{i=1}^{\nu}\mathrm{Tr}\left(\gamma_i\alpha_i^m\left(\alpha_i^{n_1}+\cdots-\alpha_i^{n_{2t}}\right)\right)\right)\right|^{2t}.$$

Given $(\lambda_1,\cdots,\lambda_\nu)\in\mathbb{F}_q^\nu$, let $J_t(\lambda_1,\cdots,\lambda_\nu)$ denote the number of solutions of the system

$$\begin{cases}\alpha_1^{n_1}+\cdots+\alpha_1^{n_t} &= \alpha_1^{n_{t+1}}+\cdots+\alpha_1^{n_{2t}}+\lambda_1\\ \quad\vdots\quad\vdots & \quad\vdots\quad\vdots\quad\vdots\\ \alpha_\nu^{n_1}+\cdots+\alpha_\nu^{n_t} &= \alpha_\nu^{n_{t+1}}+\cdots+\alpha_\nu^{n_{2t}}+\lambda_\nu\end{cases}$$

with $1\leq n_1,\cdots,n_{2t}\leq\tau$. Therefore,

$$\left|\sum_{n\leq\tau}\mathbf{e}_p\left(\xi s_n\right)\right|^{4t^2}\leq\tau^{4t^2-4t}\sum_{\lambda_1\in\mathbb{F}_q}\cdots\sum_{\lambda_\nu\in\mathbb{F}_q}J_t(\lambda_1,\cdots,\lambda_\nu)\left|\sum_{m\leq\tau}\mathbf{e}_p\left(\xi\sum_{i=1}^{\nu}\mathrm{Tr}\left(\gamma_i\lambda_i\alpha_i^m\right)\right)\right|^{2t}. \tag{2.17}$$

Note that writing $J_\nu(\lambda_1\cdots,\lambda_\nu)$ in terms of character sums, it follows that

$$\begin{aligned}J_t(\lambda_1\cdots,\lambda_\nu)&=\frac{1}{q^\nu}\sum_{x_1\in\mathbb{F}_q}\cdots\sum_{x_\nu\in\mathbb{F}_q}\left|\sum_{n\leq\tau}\mathbf{e}_p\left(\mathrm{Tr}\left(x_1\alpha_1^n\right)\right)\cdots\mathbf{e}_p\left(\mathrm{Tr}\left(x_\nu\alpha_\nu^n\right)\right)\right|^{2t}\times\\ &\qquad\times\mathbf{e}_p\left(\mathrm{Tr}\left(x_1\lambda_1\right)\right)\cdots\mathbf{e}_p\left(\mathrm{Tr}\left(x_\nu\alpha_\nu^n\right)\right)\\ &\leq\frac{1}{q^\nu}\sum_{x_1\in\mathbb{F}_q}\cdots\sum_{x_\nu\in\mathbb{F}_q}\left|\sum_{n\leq\tau}\mathbf{e}_p\left(\mathrm{Tr}\left(x_1\alpha_1^n\right)\right)\cdots\mathbf{e}_p\left(\mathrm{Tr}\left(x_\nu\alpha_\nu^n\right)\right)\right|^{2t}\\ &\leq J_t(0,\ldots,0)=:J_{t,\nu}.\end{aligned}$$

In particular, we note that $J_{t,\nu}\leq J_{t,\nu-1}$. From (2.17), it follows that

$$\left|\sum_{n\leq\tau}\mathbf{e}_p\left(\xi s_n\right)\right|^{4t^2}\leq\tau^{4t^2-4t}J_{t,\nu}\sum_{m_1\leq\tau}\cdots\sum_{m_{2t}\leq\tau}\sum_{\lambda_1\in\mathbb{F}_q}\cdots\sum_{\lambda_\nu\in\mathbb{F}_q}\mathbf{e}_p\left(\sum_{i=1}^{\nu}\mathrm{Tr}\left(\xi\gamma_i\lambda_i(\alpha_i^{m_1}+\cdots-\alpha_i^{m_{2t}})\right)\right).$$

Note that $a\gamma\lambda$, with $a\gamma\neq0$, runs over $\lambda\in\mathbb{F}_q$, then $\mathbf{e}_p\left(\mathrm{Tr}\left(a\theta\lambda z\right)\right)$ runs through all additive characters ψ in $\widehat{\mathbb{F}}_q$, evaluated at z. Then, the above expression can be written as

$$\begin{aligned}\left|\sum_{n\leq\tau}\mathbf{e}_p\left(\xi s_n\right)\right|^{4t^2}&\leq\tau^{4t^2-4t}J_{t,\nu}\sum_{m_1\leq\tau}\cdots\sum_{m_{2t}\leq\tau}\prod_{i=1}^{\nu}\left(\sum_{x\in\mathbb{F}_q}\mathbf{e}_p\left(x(\alpha_i^{m_1}+\cdots-\alpha_i^{m_{2t}})\right)\right)\\ &\leq\tau^{4t^2-4t}q^\nu J_{t,\nu}^2\leq\tau^{4t^2-4t}q^\nu J_{t,\nu-1}^2.\end{aligned} \tag{2.18}$$

We now require an estimate for $J_{t,\nu-1}$, and write

$$J_{t,\nu-1} = \frac{1}{q^{\nu-1}} \sum_{\lambda_1 \in \mathbb{F}_q} \cdots \sum_{\lambda_{\nu-1} \in \mathbb{F}_q} \left| \sum_{m \le \tau} \mathbf{e}_p \left(\operatorname{Tr} \left(\lambda_1 \alpha_1^m + \cdots + \lambda_{\nu-1} \alpha_{\nu-1}^m \right) \right) \right|^{2t}$$
$$= \frac{\tau^{2t}}{q^{\nu-1}} + O\left(\left(\max_{\substack{(\lambda_1,\ldots,\lambda_{\nu-1}) \in \mathbb{F}_q^{\nu-1} \\ (\lambda_1,\ldots,\lambda_{\nu-1}) \neq 0}} \left| \sum_{m \le \tau} \mathbf{e}_p \left(\operatorname{Tr} \left(\lambda_1 \alpha_1^m + \cdots + \lambda_{\nu-1} \alpha_{\nu-1}^m \right) \right) \right| \right)^{2t} \right). \tag{2.19}$$

Finally, we note that $s'_m = \operatorname{Tr}\left(\lambda_1 \alpha_1^m + \cdots + \lambda_{\nu-1} \alpha_{\nu-1}^m\right)$ defines a linear recurrence sequence with period τ' dividing τ, which in particular satisfies induction hypothesis. Therefore

$$\left| \sum_{m \le \tau} \mathbf{e}_p \left(\operatorname{Tr} \left(\lambda_1 \alpha_1^m + \cdots + \lambda_{\nu-1} \alpha_{\nu-1}^m \right) \right) \right| \le \tau p^{-\delta'},$$

for some $\delta' = \delta'(\varepsilon) > 0$. Now, taking $t > d(\nu-1)/2\delta'$ (where $d = [\mathbb{F}_q : \mathbb{F}_p]$) and combining with (2.19), we get

$$J_{t,\nu-1} \ll \frac{\tau^{2t}}{q^{\nu-1}}.$$

We conclude the proof combining the above estimate with (2.18) to get

$$\max_{\xi \in \mathbb{F}_p^*} \left| \sum_{n \le \tau} \mathbf{e}_p \left(\xi s_n \right) \right| \le \tau p^{-\delta}, \quad \text{with} \quad \delta = \tfrac{d(\nu-2)}{4t^2}.^1$$

The following is an immediate corollary of this theorem which will be quite handy in establishing several results in the next chapter.

Corollary 2.2.2. *Suppose that $\{s_n\}$ is a nonzero linear recurrence sequence of order $r \ge 2$ such that its characteristic polynomial $\omega(x)$ is irreducible in $\mathbb{F}_p[x]$. If its period τ satisfies*

$$\max_{\substack{d<r \\ d|r}} \gcd(\tau, p^d - 1) < \tau\, p^{-\varepsilon},$$

then there exists a $\delta = \delta(\varepsilon) > 0$ such that

$$\max_{\xi \in \mathbb{F}_p^*} \left| \sum_{n \le \tau} \mathbf{e}_p \left(\xi s_n \right) \right| \le \tau p^{-\delta}.$$

[1] To get a non-trivial estimate, we must have a non zero δ. This is true when $\nu > 2$. Hence our induction step starts from $\nu = 2$.

Remark 2.2.3. It is possible to relax the condition (a) by assuming that

$$\max_{\substack{d<r\\ d|r}} \gcd(\tau_i, p^d - 1) < \tau_i p^{-\varepsilon}$$

holds for some $1 \leq i \leq \nu$ for which $\lambda_i' \neq 0$, where λ_i' is defined in the proof of Theorem 2.2.1. Also, note that $\lambda_i' = 0$ if and only if $\lambda_i = 0$.

Since $\{s_n\}$ is a nonzero linear recurrence sequence, there exists some $1 \leq i \leq \nu$ for which $\lambda_i \neq 0$. We discussed in Section 2.1 that why (a) (or some other condition) is needed to prove the irreducible case of Theorem 3.0.1. Now, for the reducible case, some of the λ_i could be 0. For the worst-case scenario, let us assume that only one of them is nonzero, say for $i = 1$. Then, it follows from (2.12) that we are back to considering the irreducible case, and then we need the condition (a) for $i = 1$. In particular, we need (a) (or some other condition) for each irreducible component of the underlying $\omega(x)$.

2.3 Impact on Waring-type problems

In the present section, we combine Theorem 2.2.1 with classical analytical tools to prove that a linear recurrence sequence $\{s_n\}$ is an additive basis over prime fields, under some assumptions. Moreover, we discuss the advantages of nontrivial exponential sums obtained in Theorem 2.2.1 to prove it.

2.3.1 Waring-type problems with linear recurrence sequences

Let $\{s_n\}$ be a nonzero linear recurrence sequence modulo ℓ as in (2.1) with order r, period τ and $(a_0, \ell) = 1$. Given an integer $k \geq 2$, for any residue class $\lambda \pmod{\ell}$, we denote by $T_k(\lambda)$ the number of solutions of the congruence

$$s_{n_1} + \cdots + s_{n_k} \equiv \lambda \pmod{\ell}, \quad \text{with} \quad 1 \leq n_1, \ldots, n_k \leq \tau.$$

Then, writing $T_k(\lambda)$ in terms of exponential sums, we get

$$T_k(\lambda) = \frac{1}{\ell} \sum_{\xi=0}^{\ell-1} \sum_{n_1 \leq \tau} \cdots \sum_{n_k \leq \tau} \mathbf{e}_\ell \left(\xi(s_{n_1} + \cdots + s_{n_k} - \lambda)\right).$$

Taking away the term $\xi = 0$ and using triangle inequality, it is clear that

$$\begin{aligned}\left|T_k(\lambda) - \frac{\tau^k}{\ell}\right| &= \frac{1}{\ell}\left|\sum_{\xi=1}^{\ell-1}\sum_{n_1\le\tau}\cdots\sum_{n_k\le\tau}\mathbf{e}_\ell\left(\xi(s_{n_1}+\cdots+s_{n_k}-\lambda)\right)\right| \\ &\le \frac{1}{\ell}\sum_{\xi=1}^{\ell-1}\left|\sum_{n_1\le\tau}\cdots\sum_{n_k\le\tau}\mathbf{e}_\ell\left(\xi(s_{n_1}+\cdots+s_{n_k})\right)\right| \\ &\le \frac{1}{\ell}\sum_{\xi=1}^{\ell-1}\left(\left|\sum_{n_1\le\tau}\mathbf{e}_\ell\left(\xi s_{n_1}\right)\right|\cdots\left|\sum_{n_k\le\tau}\mathbf{e}_p\left(\xi s_{n_k}\right)\right|\right) \\ &\le \left(\max_{\xi\in\mathbb{F}_\ell^*}\left|\sum_{n\le\tau}\mathbf{e}_\ell\left(\xi s_n\right)\right|\right)^k. \end{aligned} \tag{2.20}$$

Assume that we have an exponential sum bound of the type

$$\max_{\xi\in\mathbb{F}_\ell^*}\left|\sum_{n\le\tau}\mathbf{e}_\ell\left(\xi s_n\right)\right| \le R\,. \tag{2.21}$$

Then, combining (2.20) and (2.21) we get $\left|T_k(\lambda) - \frac{\tau^k}{\ell}\right| \le R^k$. Now, if $(R/\tau)^k\ell$ goes to zero as $\ell\to\infty$, we obtain an effective asymptotic formula for $T_k(\lambda)$. In particular, $T_k(\lambda) > 0$ for ℓ large enough. For instance, if $\tau \ge \ell^{r/2+\varepsilon}$ we employ Korobov's bound (2.2) with $R = \ell^{r/2}$ to get

$$\left|T_k(\lambda) - \frac{\tau^k}{\ell}\right| \le \frac{\tau^k}{\ell}\left((\ell^{r/2}/\tau)^k\ell\right) \le \frac{\tau^k}{\ell}\left(\ell^{1-k\varepsilon}\right),$$

therefore $T_k(\lambda) = \frac{\tau^k}{\ell}(1+o(1))$ for $k > 1/\varepsilon$ in the range $\tau \ge \ell^{r/2+\varepsilon}$. If the characteristic polynomial $\omega(x)$ of $\{s_n\}$ is irreducible with $\deg(\omega) \ge 2$ and the least period τ satisfies $\gcd(\tau, \ell^d - 1) < \tau\ell^{-\varepsilon}$ for any divisor $d < r$ of r, then by Corollary 2.2.2 we choose $R = \tau\ell^{-\delta}$ for some positive $\delta = \delta(\varepsilon)$, to get

$$\left|T_k(\lambda) - \frac{\tau^k}{\ell}\right| \le \frac{\tau^k}{\ell}\left((\tau\ell^{-\delta}/\tau)^k\ell\right) = \frac{\tau^k}{\ell}\left(\ell^{1-k\delta}\right).$$

Thus, $T_k(\lambda) > 0$ when $k > 1/\delta$ and $\max_{\substack{d<r\\ d|r}}\gcd(\tau, \ell^d - 1) < \tau\ell^{-\varepsilon}$. Let us summarize the above discussion in the form of following corollary.

Corollary 2.3.1. *Let ℓ be a prime number, $k > 0$ be any integer, $\varepsilon > 0$, and $\{s_n\}$ be a linear recurrence sequence of order $r \ge 2$ in $\mathbb{F}_\ell$. If the characteristic polynomial $\omega(x)$ in $\mathbb{F}_\ell[x]$ is irreducible with $(\omega(0), \ell) = 1$, the least period τ satisfies*

$$\max_{\substack{d<r\\ d|r}}(\tau, \ell^d - 1) < \tau\ell^{-\varepsilon},$$

and for every integer λ, let $T_k(\lambda)$ denote the number of solutions of the congruence

$$s_{n_1} + \cdots + s_{n_k} \equiv \lambda \pmod{\ell}, \quad \textit{with} \quad 1 \le n_1, \ldots, n_k \le \tau,$$

then there exists an integer $k_0 > 0$ such that for any $k \ge k_0$, $T_k(\lambda) = \frac{\tau^k}{\ell}(1 + o(1))$.

We are now ready to prove the main result of this section.

Theorem 2.3.2 (Bajpai, Bhakta, García)**.** *Let $\{s_n\}$ be a linear recurrence sequence in $\mathbb{Z}$, whose characteristic polynomial $\omega(x) \in \mathbb{Z}[x]$ is monic, irreducible, and having prime degree. Then for a set of primes ℓ with positive density, the sequence $\{s_n\}$ is an additive basis modulo ℓ. More precisely, there exists an absolute constant c such that the Waring-type congruence*

$$s_{n_1} + \cdots + s_{n_c} \equiv \lambda \,(\mathrm{mod}\ \ell)$$

is solvable for any residue class $\lambda \,(\mathrm{mod}\ \ell)$.

Proof. Let $\mathbb{Q}_\omega$ denote the splitting field of ω and G_ω be $\mathrm{Gal}\,(\mathbb{Q}_\omega/\mathbb{Q})$. Note that $\deg(\omega)$ divides $|G_\omega|$ and G_ω is contained in the symmetric group $S_{\deg(\omega)}$. By the Cauchy's theorem, there exists an element in G_ω of order $\deg(\omega)$. In particular, there is a $\deg(\omega)$-cycle in G_ω because $\deg(\omega)$ is prime. By Chebotarev's density theorem, the set of such primes ℓ for which $\omega(x) \,(\mathrm{mod}\ \ell)$ is irreducible, have positive density, see Theorem of Frobenius in [92, Page 11]. We are now interested to work with these primes.

Let α be a root of $\omega(x) \pmod{\ell}$, and τ be the period of sequence $\{s_n\} \pmod{\ell}$. We then have $\tau = \mathrm{ord}\,(\alpha)$. Since $\omega(x) \pmod{\ell}$ is irreducible, one can write

$$\omega(x) \pmod{\ell} = \prod_{i=0}^{\deg(\omega)-1} (x - \alpha^{\ell^i}),$$

and in particular, $\omega(0) \pmod{\ell} = (-\alpha)^{1+\ell+\ell^2+\cdots+\ell^{\deg(\omega)-1}}$. Note that $(\omega(0), \ell) = 1$, for all but finitely many primes ℓ. We now need to verify the condition of Corollary 2.3.1 for $d = 1$ because $\deg(\omega)$ is prime. Observe that $\gcd(\mathrm{ord}\ \alpha, \ell - 1) = \frac{\mathrm{ord}\ \alpha}{\mathrm{ord}\ \alpha^{\ell-1}}$. Fix any $0 < \varepsilon < 1/2$, and now the proof is complete if $\mathrm{ord}\left(\alpha^{\ell-1}\right) > \ell^{\varepsilon}$ holds for almost all primes ℓ.

For any integer t, we have the following

$$\alpha^{(\ell-1)t} = 1 \implies \alpha^{rt} = \left(\prod_{i=0}^{r-1} \alpha^{\ell^i}\right)^t \implies \alpha^{2rt} = \omega(0)^{2t}.$$

In particular, α is a root of both $\omega(x) \pmod{\ell}$ and $\prod_{t \le T} \left(x^{2rt} - \omega(0)^{2t}\right) \pmod{\ell}$.

Now, given a large positive parameter T, we consider the resultant

$$R(T) = \mathrm{Res}\left(\omega(x), \prod_{t \le T} \left(x^{2rt} - \omega(0)^{2t}\right)\right).$$

Counting the number of distinct prime factors of the resultant as in the proof of Lemma 3.1.1, we see that $|\{\ell \text{ prime } | \text{ ord}\,(\alpha^{\ell-1}) \leq T\}| = O(T^2)$. For any large $y > 0$, taking $T = y^{\varepsilon}$, we see that there exists a δ such that

$$\max_{\xi \in \mathbb{F}_\ell^*} \left| \sum_{n \leq \tau} \mathbf{e}_\ell\left(\xi s_n\right) \right| \leq \tau \ell^{-\delta}$$

holds, for at least $c_\omega \pi(y) + O(y^{2\varepsilon})$ many primes $\ell \leq y$, for some constant (which depends only on ω) $c_\omega > 0$. Now, the proof follows immediately from Corollary 2.3.1. □

For further explanation, one can consider the following example.

Example 2.3.3. Consider the classical case of Fibonacci sequence $\{F_n\}$. In this case, the characteristic polynomial is $x^2 - x - 1$. It is, of course, a monic, irreducible, and of a prime degree. This polynomial is irreducible modulo prime ℓ, iff we have the Legendre symbol $\left(\frac{5}{\ell}\right) = -1$. The set of such primes has density $1/2$. Corollary 2.3.1 says, for almost all of these primes, $\{F_n\}$ is an additive basis modulo ℓ. For the other primes, we use Lemma 3.1.1. Given any $0 < \varepsilon < 1/2$, for $\pi(y) + O(y^{2\varepsilon})$ many primes $\ell \leq y$, we have

$$\text{ord}\,\alpha_\ell > \ell^{\varepsilon}, \qquad \text{ord}\,\beta_\ell > \ell^{\varepsilon} \quad \text{and} \quad \text{ord}\,(\alpha_\ell \beta_\ell^{-1}) > \ell^{\varepsilon},$$

where α_ℓ and β_ℓ are the roots of $x^2 - x - 1 \pmod{\ell}$. It then follows from [19, Corollary, page 479] that there exists a $\delta = \delta(\varepsilon) > 0$ such that

$$\max_{\substack{(c,d) \in \mathbb{F}_\ell \times \mathbb{F}_\ell \\ (c,d) \neq (0,0)}} \left| \sum_{n \leq \ell - 1} \mathbf{e}_\ell\left(c\alpha^n + d\beta^n\right) \right| \leq \ell^{1-\delta}.$$

In particular, we then have

$$\max_{\xi \in \mathbb{F}_\ell^*} \left| \sum_{n \leq \tau} \mathbf{e}_\ell\left(\xi F_n\right) \right| \leq \tau \ell^{-\delta},$$

which guarantees the existence of an absolute constant, as we saw in the proof of Theorem 2.3.2. With this, we have an inexplicit result for the Fibonacci sequences compared to the third author in [42]. However, Theorem 2.3.2 provides a general result for a large class of linear recurrence sequences.

Chapter 3

Fourier coefficients supported at the prime powers

In this chapter, we study the effect of linear recurrence sequence and Theorem 2.2.1 in the behavior of the exponential sums associated with certain Fourier coefficients of modular forms. When f is a normalized eigenform of weight k and level N, it is well known that $a(n)$ is a multiplicative function and for any prime $p \nmid N$ satisfies the relation

$$a(p^{n+2}) = a(p)a(p^{n+1}) - p^{k-1}a(p^n), \quad n \geq 0. \tag{3.1}$$

Moreover, we have $a(p^n) = a(p)^n$ for any prime $p \mid N$. These facts come from the properties of Hecke operators, see [29, Proposition 5.8.5]. If $a(p) \in \mathbb{Q}$, then one can consider $a(p) \pmod{\ell} \in \mathbb{F}_\ell$ naturally for any large enough prime ℓ. For instance, ℓ can be taken to be any prime not dividing the denominators of the Fourier coefficients. On the other hand, any cuspform can be uniquely written as a $\mathbb{C}$-linear combination of pairwise orthogonal eigenforms with Fourier coefficients coming from $\mathbb{C}$. See [29, Chapter 5] for a brief review of the Hecke theory of modular forms. However, here we are concerned with all such cuspforms which can be uniquely written as a $\mathbb{Q}$-linear combination of pairwise orthogonal eigenforms with Fourier coefficients coming from $\mathbb{Q}$. In this case, the sequence $\{a(p^n)\}$ is a linear recurrence sequence of possibly higher degrees. Let us now recall the main results of this chapter.

Theorem 3.0.1 (Bajpai, Bhakta, García)**.** *Let $f(z)$ be an eigenform with rational coefficients $a(n)$. Let $\mathcal{P}$ be the set of primes p such that $a(p^u) \neq 0$ for any $u \in \mathbb{N}$. Then the following is true.*

(i) The set of primes $\mathcal{P}$ satisfies that given $p \in \mathcal{P}$, for any $0 < \varepsilon < 1/2$ there exists a $\delta = \delta(\varepsilon) > 0$ such that the following estimate

$$\max_{\xi \in \mathbb{F}_\ell^*} \left| \sum_{n \leq \tau} \mathbf{e}_\ell \left(\xi a(p^n) \right) \right| \leq \tau \ell^{-\delta}, \tag{3.2}$$

holds for $\pi(y) + O_{f,p}(y^{2\varepsilon})$ many primes $\ell \leq y$, where the least period τ of the linear recurrence sequence $\{a(p^n)\} \pmod{\ell}$ depends on both p and ℓ, and $\pi(y)$ denotes the number of primes up to y which is asymptotically equivalent to $\frac{y}{\log y}$.

(ii) For the exceptional set of primes $p \notin \mathcal{P}$, let u be the least natural number such that $a(p^u) = 0$. Then for any $0 < \varepsilon < 1/2$, there exists a $\delta = \delta(\varepsilon) > 0$ such that the following estimate

$$\max_{\xi \in \mathbb{F}_\ell^*} \left| \sum_{n \leq \tau} \mathbf{e}_\ell \left(\xi a(p^n) \right) \right| = \frac{\tau}{u+1} + O(\tau \ell^{-\delta} + u). \tag{3.3}$$

holds for $\pi(y) + O_{f,p}(y^{2\varepsilon})$ many primes $\ell \leq y$.

More generally, we shall prove the following.

Theorem 3.0.2 (Bajpai, Bhakta, García)**.** *Let $f(z)$ be a cusp form which is not necessarily an eigenform, and can be written as a $\mathbb{Q}$-linear combination of newforms with rational coefficients. Suppose that there are r_2 many components with CM, then under the assumption of GST hypothesis[1] there exists a set of primes p with density at least 2^{-r_2} such that for any $0 < \varepsilon < 1/2$ there exists a $\delta = \delta(\varepsilon) > 0$ for which the following estimate*

$$\max_{\xi \in \mathbb{F}_\ell^*} \left| \sum_{n \leq \tau} \mathbf{e}_\ell \left(\xi a(p^n) \right) \right| \leq \tau \ell^{-\delta}, \tag{3.4}$$

holds for $c_f \pi(y) + O_{f,p}(y^{2\varepsilon})$ many primes $\ell \leq y$, where $c_f > 0$ is a constant.

3.1 Order of the roots of the characteristic polynomial

In the case of normalized eigenforms, the sequence $\{a(p^n)\}$ defines a linear recurrence sequence of order two when $p \nmid N$, otherwise it is of order one. This is one of the tools for Theorem 3.0.1. However, we do not need to assume that the form is normalized because the normalizing factor is in $\mathbb{Q}$, and we can realize that to be an element of $\mathbb{F}_\ell^*$ for any large enough prime ℓ. Before going into the proof of this theorem, we develop a tool which will be quite useful throughout. We state it in the form of following lemma.

Lemma 3.1.1. *Let $\omega(x) = x^2 + ax + b \in \mathbb{Z}[x]$ be a quadratic polynomial with $b \neq 0$ and let α, β be its roots such that none of the α, β or $\alpha\beta^{-1}$ is a root of unity. For any prime ℓ, let α_ℓ, β_ℓ be its roots in the splitting field of $\omega(x)$ over $\mathbb{F}_\ell$.*

Then, given $0 < \varepsilon < 1/2$, for $\pi(y) + O_\omega(y^{2\varepsilon})$ many primes $\ell \leq y$, we have

$$\operatorname{ord} \alpha_\ell > \ell^\varepsilon, \qquad \operatorname{ord} \beta_\ell > \ell^\varepsilon \quad \text{and} \quad \operatorname{ord} (\alpha_\ell \beta_\ell^{-1}) > \ell^\varepsilon.$$

[1] See Section 3.2.1 for the discussion about GST hypothesis.

Proof. Given a large positive parameter T, we begin by considering the polynomial

$$G_T(x) = \prod_{t \le T} (x^t - 1)(x^{2t} - b^t) \in \mathbb{Z}[x].$$

It is clear that $\omega(x) \pmod{\ell}$ has distinct roots for all but finitely many primes ℓ, since $a^2 - 4b \neq 0$. For any such prime ℓ, let α_ℓ and β_ℓ be the distinct roots in its splitting field. We now consider the resultant $\mathrm{Res}(\omega(x), G_T(x))$, and note that

$$\mathrm{Res}(\omega(x), G_T(x)) \pmod{\ell} = \prod_{1 \le i \le 3T} (\alpha_\ell - \mu_i)(\beta_\ell - \mu_i),$$

where each μ_i is a root of $G_T(x)$ in its splitting field over $\mathbb{F}_\ell$.

In particular, $\mathrm{Res}(\omega(x), G_T(x)) \equiv 0 \pmod{\ell}$ if and only if $\omega(x) \pmod{\ell}$ and $G_T(x) \pmod{\ell}$ have common roots in some finite extension of $\mathbb{F}_\ell$. Additionally, since $\alpha_\ell \beta_\ell = b$, it follows that $\mathrm{ord}\,(\alpha_\ell \beta_\ell^{-1}) \le T$ if and only if $\alpha_\ell^{2t} - b^t = 0$ (or $\beta_\ell^{2t} - b^t = 0$), for some $t \le T$. Therefore, α_ℓ (or β_ℓ) is a common root of $\omega(x) \pmod{\ell}$ and $G_T(x) \pmod{\ell}$ if $\mathrm{ord}\,\alpha_\ell$ or $\mathrm{ord}\,(\alpha_\ell \beta_\ell^{-1})$ (or $\mathrm{ord}\,\beta_\ell$ or $\mathrm{ord}\,(\alpha_\ell \beta_\ell^{-1})$) is less than T. Now, the Sylvester matrix of $\omega(x)$ and $G_T(x)$ is a square matrix of order $2 + \deg(G_T(x)) \ll T^2$, and entries bounded by an absolute constant M (which depends on a, b and not on ℓ or the parameter T). Then, by Hadamard's inequality, the determinant

$$\mathrm{Res}(\omega(x), G_T(x)) \le T^{T^2} \times M^{T^2} \ll M^{2T^2 \log T}.$$

Note that $\mathrm{Res}(\omega(x), G_T(x))$ is zero if and only if $\alpha^t = 1, \beta^t = 1$ or $(\alpha\beta^{-1})^t = 1$ for some $t \le T$, which, following our assumption, can not happen. In particular, the resultant has at most $O_\omega\left(T^2\right)$ many distinct prime divisors. This shows that

$$|\{\ell \text{ prime} \mid \mathrm{ord}\,\alpha_\ell \le T \quad \text{or} \quad \mathrm{ord}\,\beta_\ell \le T \quad \text{or} \quad \mathrm{ord}\,\alpha_\ell {\beta_\ell}^{-1} \le T\}| = O_\omega(T^2).$$

Choosing $T = y^\varepsilon$, the number of primes $\ell \le y$ such that

$$\mathrm{ord}\,\alpha_\ell \le \ell^\varepsilon \quad \text{or} \quad \mathrm{ord}\,\beta_\ell \le \ell^\varepsilon \quad \text{or} \quad \mathrm{ord}\,(\alpha_\ell \beta_\ell^{-1}) \le \ell^\varepsilon$$

is $O_\omega\left(y^{2\varepsilon}\right)$. □

3.1.1 Proof of Theorem 3.0.1

If $p \mid N$, then $a(p^n) = a(p)^n$ for any n. We only need to consider

$$\max_{\xi \in \mathbb{F}_\ell^*} \left| \sum_{n \le \tau} \mathbf{e}_\ell\left(\xi a(p)^n\right) \right|. \tag{3.5}$$

If $p \notin \mathcal{P}$, then there exists u such that $a(p^u) = 0$. Since $p \mid N$, we have $a(p) = 0$. In this case, the sum is $O(1)$ because we have $\tau = 1$.

On the other hand, if $p \in \mathcal{P}$, then for any prime ℓ large enough τ is simply the order of $a(p) \pmod{\ell}$ in $\mathbb{F}_\ell^*$. Due to Lemma 3.1.1, we may assume that $\tau > p^\varepsilon$ holds for $\pi(y) + O_{f,p}(y^{2\varepsilon})$ many primes $\ell < y$. Hence, this case is settled down by [22, Theorem 6].

Let us now consider the case $p \nmid N$. The characteristic polynomial of (3.1) is

$$\omega(x) = x^2 - a(p)x + p^{k-1}, \tag{3.6}$$

and has discriminant $a^2(p) - 4p^{k-1}$. We note that in our case the discriminant does not vanish, otherwise $|a(p)| = 2p^{(k-1)/2}$ is absurd, with $a(p)$ being an integer and $p^{(k-1)/2}$ irrational. Let $\mathbb{P}$ be the set of all primes. We divide the proof for primes $p \in \mathcal{P}$ and $p \in \mathbb{P} \setminus \mathcal{P}$. Since $a^2(p) - 4p^{k-1} \neq 0$, for any $p \in \mathcal{P}$, we write $a^2(p) - 4p^{k-1} = u^2 D_p$, with $D_p < 0$ square-free and $u \neq 0$. Let us split the cases according to $D_p \pmod{\ell}$ is quadratic residue, zero or non quadratic residue modulo ℓ. Set

$$\mathbb{P} = \mathbb{P}_0 \cup \mathbb{P}_1 \cup \mathbb{P}_{-1}, \quad \text{where } \mathbb{P}_\nu = \left\{ \ell \in \mathbb{P} \ : \ \left(\frac{D_p}{\ell}\right) = \nu \right\}.$$

For $\nu = 0, 1, -1$, we also define

$$\mathbb{P}_\nu(x) = \mathbb{P}_\nu \cap [1, x], \quad \pi_\nu(x) = |\mathbb{P}_\nu(x)| \quad \text{and} \quad \kappa_\nu = \lim_{x\to\infty} \frac{\pi_\nu(x)}{\pi(x)}.$$

It is clear that $\pi_\nu(x) = \pi(x)(\kappa_\nu + o(1))$, and $\kappa_0 + \kappa_1 + \kappa_{-1} = 1$.

Note that for a given prime p, the associated polynomial $\omega(x) \pmod{\ell}$ has a single root in $\mathbb{F}_\ell$ if and only if $u^2 D_p \equiv 0 \pmod{\ell}$. Since such equation has finitely many solutions for ℓ, we get $\kappa_0 = 0$. On the other hand, Chebotarev's density theorem implies that the uniform distribution of primes ℓ such that $\omega(x) \pmod{\ell}$ is irreducible or has distinct roots in $\mathbb{F}_\ell$. Equivalently, the primes ℓ satisfying $\left(\frac{D_p}{\ell}\right) = \pm 1$ are distributed in the same proportion, therefore $\kappa_{-1} = \kappa_1 = 1/2$. We now turn to establish nontrivial exponential sums for $\{a(p^n)\} \pmod{\ell}$ with $\ell \in \mathbb{P}_\nu$, for $\nu = \pm 1$.

Case 1. $\ell \in \mathbb{P}_{-1}$:

we want to show that the inequality (3.2) is satisfied by $\frac{\pi(y)}{2} + O(y^{2\varepsilon})$ many primes $\ell \leq y$ in $\mathbb{P}_{-1}$. In this case the associated polynomial (3.6) is irreducible modulo ℓ, then the idea is to employ Corollary 2.2.2. Let α and $\beta = \alpha^\ell$ be the conjugate roots of (3.6) in its splitting field $\mathbb{F}_\ell(\alpha)$. For a given $\varepsilon > 0$, from Lemma 3.1.1 it follows that for $\pi(y) + O(y^{2\varepsilon})$ many primes $\ell \leq y$, the following inequalities

$$\operatorname{ord} \alpha^\ell = \operatorname{ord} \alpha > \ell^\varepsilon \quad \text{and} \quad \operatorname{ord} \alpha\beta^{-1} = \operatorname{ord} \alpha^{1-\ell} > \ell^\varepsilon \tag{3.7}$$

hold. Combining the identity

$$\operatorname{ord} \alpha^{\ell-1} = \frac{\operatorname{ord} \alpha}{\gcd(\operatorname{ord} \alpha, \ell - 1)}$$

with the second inequality of (3.7), we get

$$\gcd(\operatorname{ord}\alpha, \ell-1) = \frac{\operatorname{ord}\alpha}{\operatorname{ord}\alpha^{\ell-1}} = \frac{\operatorname{ord}\alpha}{\operatorname{ord}\alpha^{1-\ell}} < (\operatorname{ord}\alpha)\ell^{-\varepsilon}.$$

Applying Corollary 2.2.2 we complete the proof of this case.

Case 2. $\ell \in \mathbb{P}_1$**:**

let α, β be the roots of $\omega(x) \pmod{\ell}$ inside $\mathbb{F}_\ell^*$. From (2.10) it follows that for $n \geq 0$, $a(p^n) \equiv c\alpha^n + d\beta^n \pmod{\ell}$, for some constants c, d in $\mathbb{F}_\ell$, with $(\alpha, \beta) \neq (0,0)$. It is clear that $\ell - 1$ is a period of the sequence $a(p^n) \pmod{\ell}$, and hence τ divides $\ell - 1$. We have

$$\sum_{n\leq\tau} \mathbf{e}_\ell\left(\xi a(p^n)\right) = \frac{\tau}{\ell-1} \sum_{n\leq\ell-1} \mathbf{e}_\ell\left(\xi a(p^n)\right) = \frac{\tau}{\ell-1} \sum_{n\leq\ell-1} \mathbf{e}_\ell\left(\xi(c\alpha^n + b\beta^n)\right).$$

From Lemma 3.1.1, there is a subset of $\mathbb{P}_1$ with $\frac{\pi(y)}{2} + O_{f,p}(y^{2\varepsilon})$ many primes $\ell \leq y$ such that $\operatorname{ord}\alpha$, $\operatorname{ord}\beta$ and $\operatorname{ord}(\alpha\beta^{-1})$ are bigger than ℓ^ε. It follows from [19, Corollary, page 479] that there exists a $\delta = \delta(\varepsilon) > 0$ such that

$$\max_{\substack{(c,d)\in\mathbb{F}_\ell\times\mathbb{F}_\ell \\ (c,d)\neq(0,0)}} \left| \sum_{n\leq\ell-1} \mathbf{e}_\ell\left(c\alpha^n + d\beta^n\right) \right| \leq \ell^{1-\delta}.$$

Hence, part (i) of Theorem 3.0.1 holds. Now for a proof of part (ii), assume that p belongs to the exceptional set $\mathbb{P} \setminus \mathcal{P}$, that is $a(p^u) = 0$ for some $u \geq 1$. We consider $u = u(p)$ to be the least such integer. Since the discriminant is nonzero (the roots α and β of (3.6) are distinct), we get

$$a(p^u) = \frac{\alpha^{u+1} - \beta^{u+1}}{\alpha - \beta} = 0.^2$$

Set $b(u+1) = a(p^u)$, then it follows that for all $n \geq 1$ we have

$$b(n(u+1)) = a(p^{n(u+1)-1}) = \frac{\alpha^{n(u+1)} - \beta^{n(u+1)}}{\alpha - \beta} = 0.$$

[2]The explicit expression of $a(p^u)$ can be obtained by using induction on u along with the fact that $\alpha + \beta = a(p), \alpha\beta = p^{k-1}$ and the recurrence relation at (3.1).

Therefore,

$$\sum_{n\le\tau}\mathbf{e}_\ell\left(\xi a(p^n)\right)=\sum_{n=0}^{\tau-1}\mathbf{e}_\ell\left(\xi b(n+1)\right)=\left(\sum_{n=0}^{\lfloor\tau/(u+1)\rfloor}\sum_{e=0}^{u}\mathbf{e}_\ell\left(\xi b(n(u+1)+e)\right)\right)+O(u)$$

$$=\left(\sum_{n=0}^{\lfloor\tau/(u+1)\rfloor}\mathbf{e}_\ell\left(\xi b(n(u+1))\right)+\sum_{e=1}^{u}\sum_{n=0}^{\lfloor\tau/(u+1)\rfloor}\mathbf{e}_\ell\left(\xi b(n(u+1)+e)\right)\right)+O(u) \tag{3.8}$$

$$=\left\lfloor\frac{\tau}{u+1}\right\rfloor+\left(\sum_{e=1}^{u}\sum_{n=0}^{\lfloor\tau/(u+1)\rfloor}\mathbf{e}_\ell\left(\xi b(n(u+1)+e)\right)\right)+O(u).$$

First of all observe that u is odd. As otherwise, if u is even then we would get

$$\alpha^{u+1}+\beta^{u+1}=2\alpha^{u+1}=\pm 2p^{\frac{(u+1)(k-1)}{2}},$$

which is absurd as $\alpha^{u+1}+\beta^{u+1}$ is a rational, but $p^{\frac{(u+1)(k-1)}{2}}$ is not. Now, for any $0<e<u+1$ we have

$$b((u+1)n+e)=\alpha^{(u+1)n}\frac{(\alpha^e-\beta^e)}{\alpha-\beta}=\left(\pm p^{\frac{(u+1)(k-1)}{2}}\right)^n a(p^{e-1}),$$

where the sign on the right-hand side above depends on the sign of α^{u+1}. Without loss of generality, we are assuming that this sign is negative. It is easy to see that our next argument applies to the positive sign case as well. Since u is fixed, so are all the e's up to $u-1$. In particular, we may consider large primes ℓ for which all of the $a(p^e)\not\equiv 0 \pmod{\ell}$ for any $1\le e\le u-1$. Then, we have

$$\sum_{n=0}^{\tau/(u+1)}\mathbf{e}_\ell\left(\xi b(n(u+1)+e)\right)=\sum_{n=0}^{\tau/(u+1)}\mathbf{e}_\ell\left(\xi\left(-p^{\frac{(u+1)(k-1)}{2}}\right)^n a(p^{e-1})\right).$$

Due to Lemma 3.1.1, we may assume that $t_u=\operatorname{ord}\left(-p^{(k-1)(u+1)/2}\right)>\ell^{\varepsilon}$ holds for $\pi(y)+O(y^{2\varepsilon})$ many primes $\ell\le y$. Now, by [22, Corollary 1] it follows that

$$\left|\sum_{n\le t}\mathbf{e}_\ell\left(\xi\left(-p^{\frac{(u+1)(k-1)}{2}}\right)^n a(p^{e-1})\right)\right|\le t\ell^{-\delta},\quad\text{for some }\delta=\delta(\varepsilon/2)>0, \tag{3.9}$$

and for any $t_u\ge t>\ell^{\varepsilon}$.

Writing $[\tau/(u+1)]=qt_u+r$, with $0\le r<t_u$ it follows that

$$\sum_{n\le\tau/(u+1)}\mathbf{e}_\ell\left(\xi\alpha^{(u+1)n}a(p^{e-1})\right)=q\sum_{n\le t_u}\mathbf{e}_\ell\left(\xi\alpha^{(u+1)n}a(p^{e-1})\right)+$$
$$+\sum_{n\le r}\mathbf{e}_\ell\left(\xi\alpha^{(u+1)n}a(p^{e-1})\right).$$

The estimate $\left|\sum_{n\leq t_u}\mathbf{e}_\ell\left(\xi\alpha^{(u+1)n}a(p^{e-1})\right)\right|\leq t_u\ell^{-\delta}$ follows from (3.9). If $r\leq \ell^{\varepsilon/2}$, then we get trivially $\left|\sum_{n\leq r}\mathbf{e}_\ell\left(\xi\alpha^{(u+1)n}a(p^{e-1})\right)\right|\leq \ell^{\varepsilon/2}$. If $\ell^{\varepsilon/2}\leq r<t_u$, then from (3.9) it follows that

$$\left|\sum_{n\leq r}\mathbf{e}_\ell\left(\xi\alpha^{(u+1)n}a(p^{e-1})\right)\right|\leq t_u\ell^{-\delta}.$$

Therefore,

$$\left|\sum_{n\leq r}\mathbf{e}_\ell\left(\xi\alpha^{(u+1)n}a(p^{e-1})\right)\right|\leq \max\left\{\ell^{\varepsilon/2},t_u\ell^{-\delta}\right\}.$$

Recalling that $t_u\geq\ell^{\varepsilon}$, we can also assume that $t_u\ell^{-\delta}\geq\ell^{\varepsilon/2}$ by taking small enough δ. Thus,

$$\left|\sum_{n\leq \tau/(u+1)}\mathbf{e}_\ell\left(\xi\alpha^{(u+1)n}a(p^{e-1})\right)\right|\leq (qt_u+t_u)\ell^{-\delta}\ll\frac{\tau}{u+1}\ell^{-\delta}.$$

Finally, combining the above inequality with (3.8) we obtain

$$\begin{aligned}\max_{\xi\in\mathbb{F}_\ell^*}\left|\sum_{n\leq\tau}\mathbf{e}_\ell\left(\xi a(p^n)\right)\right|&=\left\lfloor\frac{\tau}{u+1}\right\rfloor+O\left(\tau\ell^{-\delta}+u\right)\\&=\frac{\tau}{u+1}+O\left(\tau\ell^{-\delta}+u\right).\end{aligned}$$

This conclude the proof for all exceptional set of primes $p\in\mathbb{P}\setminus\mathcal{P}$.

3.1.2 Consequences of Theorem 3.0.1

Let us consider an exponential sum of type $S(p,x,\alpha)=\sum_{p^n\leq x}\mathbf{e}(\alpha a(p^n))$, for $\alpha\in[0,1]$. As one of the consequences of Theorem 3.0.1, we want to study this exponential sum when α is a rational whose denominator is a prime. In this regard, we have the following result.

Corollary 3.1.2. *Let f be an eigenform of weight k and level N with rational coefficient. Then for a given $0<\varepsilon<1/2$, there exists a $\delta(\varepsilon)>0$ such that for at least $\gg\frac{(\log x)^{1-\delta/(2+\delta)}}{\log\log x}$ many primes ℓ, we have the following estimates:*

$$\max_{\xi\in\mathbb{F}_\ell^*}\left|\sum_{p^n\leq x}\mathbf{e}_\ell\left(\xi a(p^n)\right)\right|=\begin{cases}O\left((\log x/\log p)^{1-\delta/(2+\delta)}\right) & \text{if}\quad p\notin\mathcal{P}\\ \frac{1}{u+1}\frac{\log x}{\log p}+O\left((\log x/\log p)^{1-\delta/(2+\delta)}\right) & \text{if}\quad p\in\mathcal{P}\end{cases}.$$

Proof. Consider the same $\delta := \delta(\varepsilon)$ as in Theorem 3.0.1 and any prime

$$\ell \in \left[(\log x/\log p)^{1/2-\delta/(4+2\delta)}, 2(\log x/\log p)^{1/2-\delta/(4+2\delta)}\right].$$

Following Theorem 3.0.1, we have

$$\max_{\xi\in\mathbb{F}_\ell^*}\left|\sum_{n\le\tau}\mathbf{e}_\ell\left(\xi a(p^n)\right)\right| \le \frac{\tau}{\ell^\delta} \tag{3.10}$$

holds, for at least $\gg \frac{(\log x)^{1-\delta/(2+\delta)}}{\log\log x}$ primes ℓ. For these primes, we also have $\tau \le \ell^2 < \frac{\log x}{\log p}$. In particular,

$$\max_{\xi\in\mathbb{F}_\ell^*}\left|\sum_{p^n\le x}\mathbf{e}_\ell\left(\xi a(p^n)\right)\right| \le \frac{\log x}{\ell^\delta\log p} + O\left(\ell^2\right) = O\left((\log x/\log p)^{1-\delta/(2+\delta)}\right).$$

On the other hand, let $p \in \mathcal{P}$ be a prime, then by Theorem 3.0.1 we have

$$\max_{\xi\in\mathbb{F}_\ell^*}\left|\sum_{n\le\tau}\mathbf{e}_\ell\left(\xi a(p^n)\right)\right| = \frac{\tau}{u+1} + O\left(\frac{\tau}{\ell^\delta} + u\right),$$

holds, for some u depending on p, and for at least $\gg \frac{(\log x)^{1-\delta/(2+\delta)}}{\log\log x}$ primes ℓ. Due to Lemma 3.1.1, we can assume that $\tau > \ell^\delta$ holds by choosing small enough δ, for at least $\gg \frac{(\log x)^{1-\delta/(2+\delta)}}{\log\log x}$ primes ℓ. Arguing similarly as in the previous case, we get the desired main term, and the error term that we get

$$O\left(\frac{\log x}{\ell^\delta\log p} + \frac{u\log x}{\tau\log p}\right) = O\left(\frac{\log x}{\ell^\delta\log p}\right) = O\left((\log x/\log p)^{1-\delta/(2+\delta)}\right),$$

where the last equality holds because $\tau > \ell^\delta$. □

Corollary 3.1.3. *Let f be an eigenform of weight k and level N with rational coefficients. For $\pi(y) + O_f(y^{2\varepsilon})$ many primes $\ell \le y$ we have the following property. Given $0 < \varepsilon < 1/2$ and $p_1, \cdots, p_\nu$ be any set of distinct primes such that $a(p_i^u) \ne 0$ for all $u \ge 1$ and $1 \le i \le \nu$, there exists a $\delta = \delta(\varepsilon) > 0$ such that*

$$\max_{\xi\in\mathbb{F}_\ell^*}\left|\sum_{n_1\le\tau_1}\cdots\sum_{n_\nu\le\tau_\nu}\mathbf{e}_\ell\left(\xi a(p_1^{n_1}\cdots p_\nu^{n_\nu})\right)\right| \le \tau_1\cdots\tau_\nu\ell^{-\delta}.$$

Proof. Set

$$S_\nu(\xi) = \left|\sum_{n_1\le\tau_1}\cdots\sum_{n_\nu\le\tau_\nu}\mathbf{e}_\ell\left(\xi a(p_1^{n_1}\cdots p_\nu^{n_\nu})\right)\right|.$$

We proceed by induction. Case $\nu = 1$ is done by Theorem 3.0.1. Now, by multiplicativity it follows that

$$|S_\nu(\xi)| \leq \sum_{n_1 \leq \tau_1} \left| \sum_{n_2 \leq \tau_2} \cdots \sum_{n_\nu \leq \tau_\nu} \mathbf{e}_\ell\left(\xi a(p_1^{n_1}) a(p_2^{n_2} \cdots p_\nu^{n_\nu})\right) \right|$$

$$\leq \tau_2 \cdots \tau_\nu \sum_{\substack{n_1 \leq \tau_1 \\ a(p_1^{n_1}) \equiv 0 \pmod{\ell}}} 1 + \sum_{\substack{n_1 \leq \tau_1 \\ a(p_1^{n_1}) \not\equiv 0 \pmod{\ell}}} \left| \sum_{n_2 \leq \tau_2} \cdots \sum_{n_\nu \leq \tau_\nu} \mathbf{e}_\ell\left(\xi a(p_1^{n_1}) a(p_2^{n_2} \cdots p_\nu^{n_\nu})\right) \right|$$

By the induction hypothesis, the second term on the right-hand side of the above equation is bounded by $\tau_1 \tau_2 \cdots \tau_\nu \ell^{-\delta}$, for some $\delta > 0$ depending on ε. On the other hand, note that $\sum_{\substack{n_1 \leq \tau_1 \\ a(p_1^{n_1}) \equiv 0 \pmod{\ell}}} 1$ counts the number of solutions of the congruence

$$a(p_1^n) \equiv 0 \pmod{\ell}, \qquad n \leq \tau_1.$$

Writing it as an exponential sum we get

$$\sum_{\substack{n_1 \leq \tau_1 \\ a(p_1^{n_1}) \equiv 0 \pmod{\ell}}} 1 = \frac{1}{\ell} \sum_{x=0}^{\ell-1} \sum_{n_1 \leq \tau_1} \mathbf{e}_\ell\left(x(a(p_1^{n_1}))\right)$$

$$= \frac{\tau_1}{\ell} + O\left(\max_{x \in \mathbb{F}_\ell^*} \left| \sum_{n_1 \leq \tau_1} \mathbf{e}_\ell\left(x(a(p_1^{n_1}))\right) \right| \right).$$

We can bound the error term by Theorem 3.0.1 and without loss of generality assuming $\delta < 1$, we get the sum above is simply $\frac{\tau_1}{\ell} + O_f(\tau_1 \ell^{-\delta})$. This is further bounded by $2\tau_1 \ell^{-\delta}$, because the explicit constant in Theorem 3.0.1 is exactly 1. Therefore,

$$|S_\nu(\xi)| \leq \tau_2 \cdots \tau_v \left(2\tau_1 \ell^{-\delta}\right) + \ \tau_1 \tau_2 \cdots \tau_\nu \ell^{-\delta},$$

for some $\delta = \delta(\varepsilon) > 0$. This shows that the inequality

$$\max_{\xi \in \mathbb{F}_\ell^*} \left| \sum_{n_1 \leq \tau_1} \cdots \sum_{n_\nu \leq \tau_\nu} \mathbf{e}_\ell\left(\xi a(p_1^{n_1} \cdots p_\nu^{n_\nu})\right) \right| \leq 3\tau_1 \cdots \tau_\nu \ell^{-\delta}$$

holds for almost all prime ℓ, and this completes the proof because we can remove the extra factor 3 by taking primes ℓ large enough. □

3.2 Generalized Sato-Tate and a dense set

We shall now prove Theorem 3.0.2. Write

$$a_f(p^n) = \sum_{i=1}^{r} a_i a_{f_i}(p^n),$$

where $a_i \in \mathbb{Q}$, and f_i is a newform with rational coefficients for every $1 \leq i \leq r$. Let $\omega^{(i,p)}$ be the characteristic polynomial of $a_{f_i}(p^n)$ and $D_i(p)$ be its discriminant.

Consider

$$\mathcal{S}_1 = \left\{ \ell \text{ prime} \mid \left(\frac{D_i(p)}{\ell} \right) = 1, \forall 1 \leq i \leq r \right\}.$$

It is clear that $\mathcal{S}_1$ has positive density. One can verify this by considering primes congruent to 1 modulo $8\prod_{i=1}^{r} D_i(p)$. This works well because, we then have

$$\left(\frac{-1}{\ell} \right) = 1, \left(\frac{2}{\ell} \right) = 1 \text{ and } \left(\frac{\ell}{\text{odd}(D_i(p))} \right) = 1, \forall 1 \leq i \leq r,$$

where odd(.) denotes odd part of the corresponding number. These conditions altogether imply $\ell \in \mathcal{S}_1$. Let $\alpha^{(i,p)}$ and $\beta^{(i,p)}$ be the roots of $\omega^{(i,p)}$. So for any $\ell \in \mathcal{S}_1$, we can write

$$\omega^{(i,p)}(x) \pmod{\ell} = \prod_{1 \leq i \leq r} \left(x - \alpha_\ell^{(i,p)} \right) \left(x - \beta_\ell^{(i,p)} \right),$$

where for every i, j, $\alpha_\ell^{(i,p)}, \beta_\ell^{(j,p)}$ are in $\mathbb{F}_\ell$. Now, we consider the set of primes

$$\begin{aligned} \mathcal{S}_2 = &\left\{ p \text{ prime} \mid \alpha^{(i,p)}(\beta^{(j,p)})^{-1} \text{ is not root of unity, } \forall\ i, j \right\} \\ &\cup \left\{ p \text{ prime} \mid \alpha^{(i,p)}(\alpha^{(j,p)})^{-1} \text{ is not root of unity, } \forall i \neq j \right\}. \end{aligned}$$

Lemma 3.2.1. *Let $\varepsilon > 0$ be any given real. Then for any prime $p \in \mathcal{S}_2$, the following inequalities are true for $\pi(y) + O_{f,p}(y^{2\varepsilon})$ many primes $\ell \leq y$.*

- $\text{ord}\,(\alpha_\ell^{(i,p)}(\beta_\ell^{(j,p)})^{-1}) > \ell^\varepsilon$, $\text{ord}\,(\alpha_\ell^{(i,p)}) > \ell^\varepsilon$ *and* $\text{ord}\,(\beta_\ell^{(j,p)}) > \ell^\varepsilon$, *for all* $1 \leq i, j \leq r$, *and*
- $\text{ord}\,(\alpha_\ell^{(i,p)}(\alpha_\ell^{(j,p)})^{-1}) > \ell^\varepsilon$, *for all* $1 \leq i \neq j \leq r$,

Proof. It is enough to prove the result only for $i, j \in \{1, 2\}$. Consider the Galois extension $K = \mathbb{Q}\left(\alpha^{(1,p)}, \alpha^{(2,p)}\right)$. Let $\mathfrak{L}$ be a prime ideal lying over ℓ in $\mathcal{O}_K$. It is clear that

$$\{\alpha_\ell^{(1,p)}, \alpha_\ell^{(2,p)}, \beta_\ell^{(1,p)}, \beta_\ell^{(2,p)}\} = \{\alpha^{(1,p)}, \alpha^{(2,p)}, \beta^{(1,p)}, \beta^{(2,p)}\} \pmod{\mathfrak{L}}, \tag{3.11}$$

because both of these sets serve as a set of roots of the equation $\omega(x) \pmod{\ell}$ and $\omega(x) \pmod{\mathfrak{L}}$ respectively. Note that $\omega(x) \pmod{\mathfrak{L}}$ coincides with $\omega(x) \pmod{\ell}$. It follows from (3.11) that the right hand side does not depend on the choice of prime $\mathfrak{L}$ lying over ℓ, so there is no problem in working with a fixed $\mathfrak{L}$ lying over ℓ. It is now clear that,

$$\left\{ \alpha_\ell^{(i,p)}(\beta_\ell^{(j,p)})^{-1} \right\}_{1 \leq i,j \leq 2} = \left\{ \alpha^{(i,p)}(\beta^{(j,p)})^{-1} \right\}_{1 \leq i,j \leq 2} \pmod{\mathfrak{L}}.$$

Consider $R(T) = \mathrm{Res}\left(\omega_1(x), g_T(x)\right)$, where $\omega_1(x) = \left(x - \alpha^{(1,p)}\right)\left(x - \beta^{(1,p)}\right)$ and

$$g_T(x) = \prod_{t \leq T} \left(x^t - \alpha^{(2,p)t}\right)\left(x^t - \beta^{(2,p)t}\right).$$

It is clear that $R(T) \neq 0$ for any $T \in \mathbb{N}$ as $p \in \mathcal{S}_2$ by assumption. Now, consider the set of primes

$$\left\{\ell \text{ prime} \mid \mathrm{ord}\left(\alpha_\ell^{(i,p)}(\beta_\ell^{(j,p)})^{-1}\right), \mathrm{ord}\left(\alpha_\ell^{(i,p)}(\alpha_\ell^{(j,p)})^{-1}\right) \leq T \text{ for some } i \neq j \in \{1,2\}\right\}. \tag{3.12}$$

For any prime ℓ in the set above, and for any prime $\mathfrak{L}$ in $\mathcal{O}_K$ lying over ℓ, $\omega_1(x) \pmod{\mathfrak{L}}$ and $g_T(x) \pmod{\mathfrak{L}}$ have a common root, Therefore, $R(T) \pmod{\mathfrak{L}} = 0$. Since both $\omega_1(x)$ and $g_T(x)$ are in $\mathbb{Z}[x]$, it is clear that $R(T) \in \mathbb{Z}$, and so $R(T) \pmod{\ell} = 0$ as well. Now, one can estimate the number of prime divisors of $R(T)$ similar to as in Lemma 3.1.1. This shows that

$$\mathrm{ord}\left(\alpha_\ell^{(i,p)}(\beta_\ell^{(j,p)})^{-1}\right) > \ell^\varepsilon, \text{ and } \mathrm{ord}\left(\alpha_\ell^{(i,p)}(\alpha_\ell^{(j,p)})^{-1}\right) > \ell^\varepsilon$$

holds for all $i \neq j \in \{1,2\}$, and $\pi(y) + O_{f,p}(y^{2\varepsilon})$ many primes $\ell \leq y$. Rest of the cases can be dealt with Lemma 3.1.1. □

3.2.1 GST: Beyond Sato-Tate

When f is a newform without CM, then Sato-Tate conjecture says that the normalized coefficients $\frac{a(p)}{2p^{\frac{k-1}{2}}}$ are equidistributed in $[-1,1]$ with respect to the measure

$$\mu_{\mathrm{non}-CM} = \frac{2}{\pi}\int \sin^2(\theta)\,\mathrm{d}\theta.$$

On the other hand, if f is with CM, then the corresponding Sato-Tate distribution is

$$\mu_{CM} = \frac{1}{2\pi}\int \frac{\mathrm{d}x}{\sqrt{1-x^2}} = \frac{1}{2\pi}\int 1\,\mathrm{d}\theta,$$

on $[0,\pi] - \{\frac{\pi}{2}\}$. Moreover, at $\theta_p = \frac{\pi}{2}$, $a(p)$ becomes zero, and it is known that the set of such primes p has density exactly $\frac{1}{2}$. Let us now give a short overview of Sato-Tate distribution. Consider the L-function defined by

$$L(s, \mathrm{Sym}^m f) = \prod_{p \nmid N}\prod_{i=0}^{m}\left(1 - \alpha_p^i \beta_p^{m-i} p^{-s}\right)^{-1},$$

where α_p, β_p are normalized roots of (3.6). In other words, if $\widetilde{\alpha}_p, \widetilde{\beta}_p$ are the roots of (3.6), then we define $\alpha_p = \frac{\widetilde{\alpha}_p}{p^{\frac{k-1}{2}}}, \beta_p = \frac{\widetilde{\beta}_p}{p^{\frac{k-1}{2}}}$. Serre in [80] showed that if for all integer $m \geq 0, L(s, \mathrm{Sym}^m(f))$ extends analytically to $\mathrm{Re}(s) \geq 1$ and does not vanish there, then the Sato–Tate conjecture holds true for f. Note that Barnet-Lamb et

al. have proved the conjecture in [11] working with this L-function. However, to estimate the size of $\mathcal{S}_2$ we will have more than one newform to play with, and it will be helpful to have their distributions independent. ***This independency property is stated as Generalized Sato-Tate (GST) hypothesis.*** In this article, we shall always work with the newforms that obey this hypothesis. For example, in Theorem 3.0.2, it is assumed that all the associated newforms satisfy the GST hypothesis.

3.2.2 A consequence of GST

To prove Theorem 3.0.2, we need to study the set $\mathcal{S}_2$. We have that luxury when the associated newforms satisfy GST.

Lemma 3.2.2. *Suppose that there are r_1 many components without CM and r_2 many components with CM in f. Then under the GST hypothesis, density of $\mathcal{S}_2$ is 2^{-r_2}.*

Proof. We start by writing

$$\alpha^{(j,p)} = p^{\frac{k-1}{2}} e^{i\theta_{j,p}}, \beta^{(j,p)} = p^{\frac{k-1}{2}} e^{-i\theta_{j,p}}, \forall 1 \leq j \leq r.$$

So, the problem is reduced to study the set of primes

$$\{p \text{ prime} \mid \theta_{i,p} \pm \theta_{j,p} \in \mathbb{Q} \times \pi, \text{ for some } 1 \leq i, j \leq r\}. \tag{3.13}$$

It follows from the discussion above that the density of this set is bounded by

$$\left(\frac{2}{\pi}\right)^{r_1} \left(\frac{1}{2\pi}\right)^{r_2} \int_S \cdots \int \sin^2(\theta_1) \sin^2(\theta_2) \cdots \sin^2(\theta_{r_1}) \, \mathrm{d}\theta_1 \, \mathrm{d}\theta_2 \cdots \mathrm{d}\theta_r, \tag{3.14}$$

where $S = \{(\theta_1, \theta_2, \cdots, \theta_r) \in [0, \pi]^r \mid \theta_i \pm \theta_j \in \mathbb{Q} \times \pi \text{ for some } 1 \leq i, j \leq r\}$. Just for the sake of simplicity and to have a feel of what is going on, let us first do the case when there is only one component.

Case 1, $r = 1$:

suppose that the given component is without CM. If $\alpha_p^{(1,p)} \beta_p^{-(1,p)}$ is a root of unity then this implies that $\theta_{1,p} \in \pi \times \mathbb{Q}$. By Sato-Tate, density of such primes is bounded by

$$\left(\frac{2}{\pi}\right) \int_{\theta \in \pi \times \mathbb{Q}} \sin^2(\theta) \, \mathrm{d}\theta.$$

Since the integral above runs over a set of measure zero, the integral is zero, and for this particular case density of $\mathcal{S}_2$ is indeed 1. Now, suppose that the given component is with CM. In this case, the density of $\mathcal{S}_2$ is

$$\left(\frac{1}{2\pi}\right) \int_{\theta \in [0,\pi] \setminus \pi \times \mathbb{Q}} \sin^2(\theta) \, \mathrm{d}\theta = \frac{1}{2}.$$

Case 2, $r \geq 2$:

for this general case, it is enough to show that the integral over S in (3.14) is zero. This is because, due to GST, we are now working on the measure

$$\left(\frac{2}{\pi}\right)^{r_1}\left(\frac{1}{2\pi}\right)^{r_2}\int\cdots\int \sin^2(\theta_1)\sin^2(\theta_2)\cdots\sin^2(\theta_{r_1})\,\mathrm{d}\theta_1\,\mathrm{d}\theta_2\cdots\,\mathrm{d}\theta_r, \tag{3.15}$$

and with respect to this measure, $[0,\pi]^r$ has measure $\left(\frac{1}{2}\right)^{r_2}$. We can write $S = \bigcup_{1\leq i,j\leq r} S_{i,j}$, where the set $S_{i,j}$ is defined to be the tuples for which $\theta_i \pm \theta_j \in \mathbb{Q}\times\pi$. It is now enough to show that each of these sets $S_{i,j}$ has a zero measure. Note that the integral over $S_{i,j}$ is crudely bounded by $\iint\limits_{S_{i,j}} 1\,\mathrm{d}\theta_i\,\mathrm{d}\theta_j$. It is evident that

$$\iint\limits_{S_{i,j}} 1\,\mathrm{d}\theta_i\,\mathrm{d}\theta_j = \iint\limits_{\theta_i+\theta_j\in\mathbb{Q}\times\pi} 1\,\mathrm{d}\theta_i\,\mathrm{d}\theta_j \;+\; \iint\limits_{\theta_i-\theta_j\in\mathbb{Q}\times\pi} 1\,\mathrm{d}\theta_i\,\mathrm{d}\theta_j,$$

as $\mathbb{Q}\times\mathbb{Q}$ has zero measure. We now note that

$$\iint\limits_{\theta_i-\theta_j\in(a,b)} 1\,\mathrm{d}\theta_i\,\mathrm{d}\theta_j \leq \int\limits_0^{\pi}\int\limits_a^{b} 1\,\mathrm{d}t\,\mathrm{d}\theta \ll |b-a|, \tag{3.16}$$

for any $b > a$. In particular, for any $\varepsilon > 0$,

$$\iint\limits_{\theta_i-\theta_j\in\mathbb{Q}\times\pi} 1\,\mathrm{d}\theta_i\,\mathrm{d}\theta_j \ll \sum_{k=1}^{\infty}\frac{\varepsilon}{2^k} = \varepsilon.$$

The last implication above follows from the standard argument to show a countable set always has a zero measure. In particular, the second integral of (3.16) is zero. On the other hand, just by replacing θ_j with $\pi - \theta_j$, we get

$$\iint\limits_{\theta_i+\theta_j\in\mathbb{Q}\times\pi} 1\,\mathrm{d}\theta_i\,\mathrm{d}\theta_j = -\iint\limits_{\theta_i-\theta_j\in\mathbb{Q}\times\pi} 1\,\mathrm{d}\theta_i\,\mathrm{d}\theta_j.$$

This just shows that the integral over $S_{i,j}$ at (3.16) is zero, which completes the proof. □

3.2.3 Proof of Theorem 3.0.2

Let $p \in \mathcal{S}_2$ be a prime, then we can write

$$\sum_{i=1}^{r} a_i a_{f_i}(p^n) \pmod{\ell} = \sum_{i=1}^{r} a_i^{(\ell)}\left(c^{(i,\ell)}\alpha^{n(i,\ell)} + d^{(i,\ell)}\beta^{n(i,\ell)}\right),$$

where $a_i^{(\ell)}, c^{(i,\ell)}$ and $d^{(i,\ell)}$ are all in $\mathbb{F}_\ell$. On the other hand, all the roots $\alpha^{(i,\ell)}$ and $\beta^{(i,\ell)}$ are in $\mathbb{F}_\ell$, as $\ell \in \mathcal{S}_1$. The proof now follows by [19, Corollary, page 479] combining with Lemma 3.2.1 and Lemma 3.2.2. □

Remark 3.2.3. It is known, due to Thorner, that GST holds for $r = 2$ when both f_1 and f_2 are without CM and not twist-equivalent. We say that f_1 and f_2 are twist-equivalent if there exists a primitive Dirichlet character χ such that $f_1 = f_2 \otimes \chi$. For more details, we refer the reader to Theorem 1.3 in [94].

3.2.4 Waring-type problems for modular forms

Let us now recall our discussion from Chapter 1 about Waring problems for modular forms. This section assumes that the modular form is a newform without CM. Fix any $0 < \varepsilon < \frac{1}{2}$, say $\varepsilon = \frac{1}{3}$. Then taking $\delta := \delta(\varepsilon)$ as in Theorem 3.0.1, the following estimate

$$\max_{\xi \in \mathbb{F}_\ell^*} \left| \sum_{n \leq \tau} \mathbf{e}_\ell \left(\xi a(p^n) \right) \right| \leq \tau \ell^{-\delta},$$

holds for almost all primes p and ℓ. The discussion in Section 2.3.1 shows that $T_s(\lambda) > 0$ for any $\lambda \in \mathbb{F}_\ell$, and $s > 1/\delta$, where $T_s(\lambda)$ is the number of solutions of the congruence

$$a(p^{n_1}) + \cdots + a(p^{n_s}) \equiv \lambda \pmod{\ell}, \quad \text{with} \quad 1 \leq n_1, \ldots, n_s \leq \tau.$$

Moreover, this s does not depend on the choice of the eigenform because δ does not. More precisely, we have the following result.

Corollary 3.2.4. *Let f be a newform without CM and with rational Fourier coefficients. We say, a proposition $\mathcal{Q}_f(p, \ell, s)$ is true if and only if, any element of $\mathbb{F}_\ell$ can be written as a sum of at most s elements of the set $\{a(p^n)\}_{n \geq 0}$. Then, there is an absolute constant s_0 such that $\mathcal{Q}_f(p, \ell, s_0)$ is true for almost all primes p and ℓ. Moreover, s_0 does not depend on the choice of f.*

We obtain the following result as an immediate consequence of Theorem 4.3.1.

Corollary 3.2.5. *Suppose the newform is without CM and with integer Fourier coefficients. Then there exists an absolute constant s_0 such that, for any large prime ℓ satisfying the coprimality condition $(\ell - 1, k - 1) = 1$, the proposition $\mathcal{Q}_f(p, \ell, s_0)$ is true for a set of primes p with density at least $1 + O_{f,p}\left(\frac{1}{\sqrt{\ell}}\right)$. Moreover, s_0 does not depend on the choice of f.*

Chapter 4

Galois representation associated to elliptic curves and modular forms

Let $f(z)$ be any newform of weight k and level N. From Deligne-Serre correspondence, we have an associated Galois representation

$$\rho_f^{(\ell)} : \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right) \longrightarrow \mathrm{GL}_2\left(\mathbb{Z}/\ell\mathbb{Z}\right),$$

such that $a(p) \pmod{\ell} \equiv \mathrm{tr}\left(\rho_f^{(\ell)}(\mathrm{Frob}_p)\right)$ for any prime $p \nmid N\ell$. It is clear that the characteristic polynomial of $\rho_f^{(\ell)}(\mathrm{Frob}_p)$ is same as $x^2 - a(p)x + p^{k-1} \pmod{\ell}$. When f is without CM it follows from Ribet [74, Theorem 3.1] that, the image of this representation is given by

$$\Delta_{k,\ell} = \left\{A \in \mathrm{GL}_2\left(\mathbb{Z}_\ell\right) \mid \det(A) \in \left((\mathbb{Z}/\ell\mathbb{Z})^*\right)^{k-1}\right\},$$

except possibly for finitely many primes ℓ. More generally, for any integer $e \geq 1$, we have a Galois representation

$$\rho_{f,\ell^e} : \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right) \longrightarrow \mathrm{GL}_2\left(\mathbb{Z}/\ell^e\mathbb{Z}\right)$$

satisfying that $a(p) \pmod{\ell^e} \equiv \mathrm{tr}\left(\rho_{f,\ell^e}(\mathrm{Frob}_p)\right)$, and

$$\mathrm{im}(\rho_{f,\ell^e}) = \Delta_k(\ell^e) := \{A \in \mathrm{GL}_2\left(\mathbb{Z}/\ell^e\mathbb{Z}\right) \mid \det(A) \in \left((\mathbb{Z}/\ell^e\mathbb{Z})^*\right)^{k-1}\}.$$

Now given any composite number m, we can naturally associate a Galois representation $\rho_{f,m} := \prod_{\ell^e || m} \rho_{f,\ell^e}$, and denote $\mathrm{G}_{f,m}$ to be its image. Due to Ribet's result, we immediately have the following.

Corollary 4.0.1. *Suppose that $f(z)$ is any newform without CM. Then there exists a finite set of primes S_f such that*

$$\mathrm{G}_m = \Delta_k(m) = \{A \in \mathrm{GL}_2(\mathbb{Z}/mZ) \mid \det(A) \in ((\mathbb{Z}/m\mathbb{Z})^*)^{k-1}\},$$

for any integer m co-prime to any prime from S_f.

Consider the prime factorization $m = \prod_{\ell|m} \ell^e$. Take any residue class $a \in \mathbb{Z}/\ell^e\mathbb{Z}$ and $\lambda \in (\mathbb{Z}/\ell^e\mathbb{Z})^*$. Denote $N_{a,\lambda}(\ell^e)$ be the number of matrices in $\Delta_k(\ell^e)$ of trace a and determinant λ. We know from [65, Corollary 6.0.7] that

$$N_{a,\lambda}(\ell^e) = \begin{cases} \ell^{2e}, \text{ if } a^2 - 4\lambda = 0. \\ \ell^e(\ell^e + 1), \text{ if } a^2 - 4\lambda \text{ is a non} - \text{zero square in } \mathbb{Z}/\ell^e\mathbb{Z}. \\ \ell^e(\ell^e - 1) \text{ if } a^2 - 4\lambda \text{ is not square in } \mathbb{Z}/\ell^e\mathbb{Z}. \end{cases} \tag{4.1}$$

Lemma 4.0.2. *Let $m = \prod_{\ell|m} \ell^e$ be any integer, and a be any residue class in $\mathbb{Z}/m\mathbb{Z}$, and $\lambda \in (\mathbb{Z}/m\mathbb{Z})^*$. Then we have,*

$$N_{a,\lambda}(m) := \#\{A \in \Delta_k(m) \mid \mathrm{tr}(A) = a, \ \det(A) = \lambda\} = m^2 + O\left(\frac{2^{\omega(m)}m^2}{\ell}\right),$$

where ℓ is the smallest prime factor of m.

Proof. By the Chinese remainder theorem, we can write

$$\Delta_k(m) = \prod_{\ell^e||m} \Delta_k(\ell^e).$$

Therefore it is enough to prove that the result when m is a prime power. The result now follows from (4.1). □

Remark 4.0.3. In particular, for any m with large enough prime factors, all trace values are equidistributed in $\Delta_k(m)$.

4.1 Representations for cuspforms and image

Now let $f_1, f_2, \cdots, f_r$ be a set of newforms, of weights respectively $k_1, k_2, \cdots, k_r$. Then we can associate a Galois representation $\rho_{f_1,f_2,\cdots,f_r,m} : \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right) \to \mathrm{GL}_{2r}(\mathbb{Z}/m\mathbb{Z})$ defined by the map

$$\sigma \mapsto \begin{pmatrix} \rho_{f_1,\ell}(\sigma) & & & \\ & \rho_{f_2,\ell}(\sigma) & & \\ & & \ddots & \\ & & & \rho_{f_r,\ell}(\sigma) \end{pmatrix}. \tag{4.2}$$

Image of this map is contained in $\Delta_{k_1,k_2,\cdots,k_r}(m)$, where $\Delta_{k_1,k_2,\cdots,k_r}(m)$ denotes the set of all block matrices of size 2×2 in $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ in which determinant of each block is a $k_i - 1^{th}$ power of some element in the multiplicative group $(\mathbb{Z}/m\mathbb{Z})^*$.

Definition 4.1.1. *Let ℓ be a prime. Two newforms f_i and f_j of weight and level respectively k_i, k_j and N_i, N_j, are said to be ℓ-equivalent, i.e. $f_i \sim_\ell f_j$, if there exists a quadratic character*

$$\chi : (\mathbb{Z}/N_iN_j\ell\mathbb{Z})^* \to \mathbb{C}^*,$$

satisfying $a_f(p) = \chi(p)a_g(p) \pmod{\ell}$ for any prime $p \nmid N_iN_j$. Moreover we say that f_i and f_j are twist equivalent, i.e. $f_i \sim f_j$, if there exists a quadratic character χ satisfying $a_f(p) = \chi(p)a_g(p)$ for any prime $p \nmid N_iN_j$.

The reader may note that if $f_i \sim f_j$, their weights k_i and k_j should be the same. More importantly, we have the following.

Lemma 4.1.2. *If two newforms f_i, f_j are not twist-equivalent, then they are ℓ-equivalent for only finitely many primes ℓ.*

Proof. For the sake of contradiction, let us assume that $f_i \sim_\ell f_j$ for infinitely many primes ℓ. Then for each prime $p \nmid N_iN_j$ there exists infinitely many primes $\ell > N_iN_jp$ satisfying $a_i(p) \equiv \pm a_j(p) \pmod{\ell}$. It is evident that for every prime $p \nmid N_iN_j$, there exists a sign $\sigma_p \in \{\pm 1\}$ satisfying $a_p(p) = \sigma_p a_j(p)$. Now define a quadratic character χ modulo with $\chi(p) := \sigma_p$, for any prime p not dividing N_iN_j. □

With this notion of equivalence, we have the following fact.

Lemma 4.1.3. *Let $f_1, f_2, \cdots, f_r$ by any set of pairwise twist-inequivalent newforms without CM. Then there exists a finite set of primes S_f such that, $\mathrm{G}_{f_1,f_2,\cdots,f_r,m}$ contains $\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})^r$ for any integer m co-prime to any prime from S_f.*

Before proving this, let G be any finite group and denote Occ(G) be the isomorphism classes of non-abelian simple groups coming as the quotient of composite factors of some subgroup of G. We then recall the crucial result from [27].

Lemma 4.1.4. *Let m be any integer co-prime to 30, and G be any subgroup of $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$. Then the following holds.*

$$\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z}) \subseteq \mathrm{G} \text{ if and only if } \mathrm{PSL}_2(\mathbb{Z}/\ell\mathbb{Z}) \in \mathrm{Occ}(\mathrm{G}),$$

for every prime $\ell | m$.

Proof of Lemma 4.1.3. It follows from Lemma 4.1.2 that, there exists a finite set of primes P_f such that, any of f_i, f_j are not ℓ-equivalent for any prime $\ell \notin P_f$. Then we make P_f bigger if necessary, to ensure that each $\rho_{f_i,\ell}$ has image $\Delta_{k_i}(\ell)$, and in particular contains $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$. Now it follows from Lemma 5.1 in [63] by taking $e = \ell - 1$ that, image of $\mathrm{G}_{f_i,f_j,\ell}$ contains $\mathrm{SL}_2(\mathbb{F}_\ell)$ for any $\ell \notin P_f$. Now it follows from [73, Lemma 5.2.2] that $\mathrm{G}_{f_1,f_2,\cdots,\ell}$ contains $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})^r$, since $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$ is self commutator for any prime $\ell \geq 5$. In particular, the image contains any matrix of type $(I, I, \cdots, \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z}), I, \cdots, I)$.

Moreover, any $(I, I, \cdots, \mathrm{PSL}_2(\mathbb{Z}/\ell\mathbb{Z}), I, \cdots, I) \in \mathrm{Occ}(\mathrm{G}_{f_1,f_2,\cdots,f_r,m})$ for any such integer m, as long as all the prime factors of m are larger than 5. Then it follows from Lemma 4.1.4 that $\mathrm{G}_{f_1,f_2,\cdots,f_r,m}$ contains $(I, I, \cdots, \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z}), I, \cdots, I)$ and this completes the proof. □

Lemma 4.1.5. *Let $f_1, f_2, \cdots, f_r$ by any pairwise twist-inequivalent newforms without CM of the same weight k. Then there exists a finite set of primes S_f such that,*

$$\mathrm{G}_{f_1,\cdots,f_r,m} = \Delta_k^{(r)}(m) := \left\{ \begin{pmatrix} A_1 & & & \\ & A_2 & & \\ & & \ddots & \\ & & & A_r \end{pmatrix} \mid \det(A_1) = \cdots = \det(A_r) \in ((\mathbb{Z}/m\mathbb{Z})^*)^{k-1} \right\}.$$

for any integer m co-prime to any prime from S_f.

Proof. It follows from Corollary 4.0.1, and by induction that each projection

$$\pi_i : \mathrm{G}_{f_1,\cdots,f_r,m} \to \mathrm{GL}_2(\mathbb{Z}/mZ)$$

has the property that $\mathrm{im}(\pi_i) = \Delta_k(m),\ \forall 1 \leq i \leq r$. For $r = 2$, the result follows from the proof of Lemma 3.3 in [47], combining with Lemma 4.1.3. Note that we are using Lemma 4.1.3 to rule out the case (b) of Lemma 3.3 in [47].

Now by induction,

$$\mathrm{G}_{f_1,\cdots,f_{r-1},m} = \left\{ \begin{pmatrix} A_1 & & & \\ & A_2 & & \\ & & \ddots & \\ & & & A_r \end{pmatrix} \mid \det(A_1) = \cdots = \det(A_{r-1}) \in (\mathbb{Z}/m\mathbb{Z}^*)^{k-1} \right\}$$

and $\mathrm{G}_{f_r,m} = \Delta_k(m)$. If $\mathrm{G}_{f_1,\cdots,f_r,m}$ does not have the desired image, then by Goursat's lemma (Lemma 3.2 in [47]), there exists a normal subgroup N_1 of $\mathrm{G}_{f_1,\cdots,f_{r-1},m}$ and a normal subgroup N_2 of $\mathrm{G}_{f_r,m}$ and an isomorphism $\psi : \mathrm{G}_{f_1,\cdots,f_{r-1},m}/\mathrm{N}_1 \to \mathrm{G}_{f_r,m}/\mathrm{N}_2$ such that

$$\mathrm{G}_{f_1,\cdots,f_r,m} = \{(g_1, g_2) \mid \psi(g_1\mathrm{N}_1) = g_2\mathrm{N}_2\}.$$

If N_2 contains $\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})$ then clearly N_1 is contained in $\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})^{r-1}$, because

$$\mathrm{N}_1 \times \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z}) \subseteq \mathrm{N}_1 \times \mathrm{N}_2 \subseteq \Delta_k^{(r)}(m).$$

Due to the isomorphism ψ, we have $\mathrm{N}_1 = \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})^{r-1}$ and $\mathrm{N}_2 = \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})$. In particular,

$$\mathrm{G}_{f_1,\cdots,f_{r-1},m}/\mathrm{N}_1 = \mathrm{G}_{f_r,m}/\mathrm{N}_2 = (\mathbb{Z}/m\mathbb{Z})^*.$$

This implies that ψ must be the identity map, because $\mathrm{G}_{f_1,\cdots,f_r,m}$ is the graph of ψ, which of course lies inside $\Delta_k^{(r)}(m)$. The proof is now complete. □

4.2 Distribution of Fourier coefficients

In this section, we study $\{a(n) \pmod m\}$ when n has only finitely many prime factors. The one prime factor case is just an immediate consequence of Lemma 4.1.5 and Chebotarev's density theorem when the corresponding $f(z)$ is a newform. For a larger family of cuspforms, we have the following result when we study over n with $\omega(n) = 1$.

Proposition 4.2.1. *Let $f = c_1 f_1 + c_2 f_2 \cdots + c_r f_r$ be any cuspform with coefficients in $\mathbb{Q}$. Assume that all the f_i are pairwise twist-inequivalent newforms without CM of same weight k. Then there exists an integer N_f such that for any integer m co-prime to N_f satisfying $m \sim \phi(m)$, and $2^{\omega(m)+r} = o(\ell)$, where ℓ is the smallest prime factor of m, the set*

$$\{a(p) \pmod m \mid p, \text{ prime}\},$$

is equidistributed.

Proof. Take any residue class $a \in \mathbb{Z}/m\mathbb{Z}$. It follows from Lemma 4.0.2 that for each tuple $(a_1, a_2, \cdots, a_r) \in (\mathbb{Z}/m\mathbb{Z})^r$ and $(\lambda_1, \lambda_2, \cdots, \lambda_r) \in ((\mathbb{Z}/m\mathbb{Z})^*)^r$,

$$\#\{\mathrm{diag}(A_1, \cdots, A_r) \in (\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}))^r \mid \det(A_i) = \lambda_i,\ \mathrm{tr}(A_i) = a_i\ \forall 1 \leq i \leq r\}.$$

is $m^{2r} + O(2^{r+\omega(m)} m^{2r}/\ell)$, where ℓ is the least prime factor of m. In particular,

$$\frac{\#\{A \in \Delta_k^{(r)}(m) \mid \mathrm{tr}(A_1) = a_1, \cdots, \mathrm{tr}(A_r) = a_r\}}{\frac{\phi(m)}{(\phi(m),k-1)}} = m^{2r} + O(2^{r+\omega(m)} m^{2r}/\ell). \quad (4.3)$$

Therefore, the set

$$\{p \mid a_1(p) = a_1,\ a_2(p) = a_2, \cdots a_r(p) = a_r\}$$

has density $\frac{\frac{\phi(m)}{(\phi(m),k-1)}(m^{2r}+O(2^{r+\omega(m)}m^{2r}/\ell))}{\#\Delta_k(m)}$, which is precisely $\frac{m^{2r}+O(2^{r+\omega(m)}m^{2r}/\ell)}{\#\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})^r}$. Now the number of tuples $(a_1, a_2, \cdots, a_r)$ with $c_1a_1 + c_2a_2 \cdots + c_ra_r = a$ is m^{r-1}. Therefore we have $a(p) = a$, for a set of primes p with density

$$m^{r-1}\frac{m^{2r} + O(2^{r+\omega(m)}m^{2r}/\ell)}{\#\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})^r} \sim \frac{1}{m},$$

for any m satisfying $m \sim \phi(m)$, and $2^{\omega(m)+r} = o(\ell)$, where ℓ is the smallest prime factor of m. □

Now to study $\{a(n) \pmod m\}$ with n having more than one prime factor. For any integer $M \geq 1$, denote

$$N_M(x) = \{n \leq x \mid \omega(n) = M\}.$$

It is a classical result [68] that $\#N_M(x) \sim \frac{1}{(M-1)!}\frac{x}{(\log x)}(\log\log x)^{M-1}$. We now need the following generalization. [1]

[1] For proof, the reader may refer to Lucia's answer on https://mathoverflow.net/questions/156982/chebotarev-density-theorem-for-k-almost-primes.

Lemma 4.2.2. *Let $P_1, \ldots, P_r$ be disjoint subsets of the primes with density respectively $\alpha_1, \ldots, \alpha_r$. Let $N(M; a_1, \ldots, a_r)$ denote the set of integers that are products of M primes with exactly a_j of these primes chosen from the set P_j. Let us assume that all $\alpha_j \geq 0,\ a_j \geq 1$, then for any fixed integer M and as $x \to \infty$, we have the following.*

$$\sum_{\substack{n \leq x \\ n \in N(M; a_1, \ldots, a_r)}} 1 \sim M \prod_{j=1}^{r} \frac{\alpha_j^{a_j}}{(a_j)!} \frac{x}{(\log x)} (\log \log x)^{M-1}.$$

We now consider the factorizations of any $a \in \mathbb{Z}/m\mathbb{Z}$ in-to M many terms over $\mathbb{Z}/m\mathbb{Z}$. Let us write a factorization $a = a_1 a_2 \cdots a_M$, with all $a_i \in \mathbb{Z}/m\mathbb{Z}$. Now given any tuple $\vec{a} = (a_1, a_2, \cdots, a_M) \in (\mathbb{Z}/m\mathbb{Z})^M$, denote $p(\vec{a}) = a_1 a_2 \cdots a_M$. We say that two vectors $\vec{a_1}$ and $\vec{a_2}$ are equivalent, i.e. $\vec{a_1} \sim_{S_M} \vec{a_2}$ if and only if they differ by a permutation in S_M. Given any element $\vec{a} \in (\mathbb{Z}/m\mathbb{Z})^M$, denote $n_{\vec{a}} = \prod_{1 \leq i \leq k} n_i!$, where $a_1, a_2, \cdots, a_k$ are the set of all distinct terms that appear in $\vec{a}$ with a_i appearing n_i times. In particular, we have $\sum_{1 \leq i \leq k} n_i = M$. We shall use these notations to study the case of newforms in the next theorem.

To generalize that, we need to work with $M_{r \times M}(\mathbb{Z}/m\mathbb{Z})$, the ring of matrices over $\mathbb{Z}/m\mathbb{Z}$ with r-rows and M-columns. Then we consider the natural action of S_M on the columns of $M_{r \times M}(\mathbb{Z}/m\mathbb{Z})$. Given any element $A \in M_{r \times M}(\mathbb{Z}/m\mathbb{Z})$, denote $C_1(A),\ C_2(A), \cdots C_M(A)$ and $R_1(A),\ R_2(A), \cdots R_r(A)$ respectively be the columns, and the rows of A. Moreover, denote n_A to be the number $\prod_{1 \leq i \leq k} n_i!$, where $C_1, C_2, \cdots, C_k$ be the set of all distinct columns that appear in A with C_i appearing n_i times.

Theorem 4.2.3 (Bhakta, Krishnamoorthy, Muneeswaran)**.** *Let $M \geq 1$ be any integer, and $f = c_1 f_1 + c_2 f_2 \cdots + c_r f_r$ be any cuspform with coefficients in $\mathbb{Q}$. Assume that all the f_i are pairwise twist-inequivalent newforms without CM of same weight k. Then there exists an integer N_f such that for any integer m co-prime to N_f satisfying $m \sim \phi(m)$, and $2^{\omega(m)+r} = o(\ell)$, where ℓ is the smallest prime factor of m, the following asymptotic formula holds for any tuple $\vec{a} = (a_1, a_2, \cdots, a_r) \in (\mathbb{Z}/m\mathbb{Z})^r$.*

$$\frac{\#\{n \in N_M(x) \mid a_1(n) = a_1, a_2(n) = a_2 \cdots, a_r(n) = a_r\}}{\#N_M(x)} \sim d_{\vec{a}}(m) \frac{1}{m^{rM}},$$

for some $d_{\vec{a}}(m) > 0$, which is an effectively computable constant.

Proof. Let us first do the case $r = 1$. We use Lemma 4.2.2 and Proposition 4.2.1 to get

$$\frac{\#\{n \in N_M(x) \mid a(n) = a\}}{\#N_M(x)} \sim \frac{1}{m^M} \sum_{\substack{\vec{a} \in (\mathbb{Z}/m\mathbb{Z})^M / S_M \\ p(\vec{a}) = a}} \frac{M!}{n_{\vec{a}}}.$$

Now for the case $r \geq 1$, we use the proof of Proposition 4.2.1 for $r \geq 1$. More precisely, for each tuple $(a^{(1)}, a^{(2)}, \cdots, a^{(r)}) \in (\mathbb{Z}/m\mathbb{Z})^r$, the set

$$\{p \mid a_1(p) = a^{(1)}, a_2(p) = a^{(2)}, \cdots, a_r(p) = a^{(r)}\}$$

has density $\sim \frac{1}{m^r}$. Similarly, as in the case $r = 1$, it follows from Lemma 4.2.2 that the required proportion is given by

$$\frac{1}{m^{rM}} \sum_{\substack{A \in M_{r\times M}(\mathbb{Z}/m\mathbb{Z})/S_M \\ p(R_1(A))=a_1,\ p(R_2(A))=a_2,\cdots p(R_r(A))=a_r}} \frac{M!}{n_A},$$

the proof is now complete taking $d_{\vec{a}}(m)$ to be the summation in the above line.

□

Remark 4.2.4. Writing $m = \ell_1^{e_1}\ell_2^{e_2}...\ell_s^{e_s}$, for any $a \in \mathbb{Z}/m\mathbb{Z}$ we have an element in $\mathbb{Z}/\ell_1^{e_1}\mathbb{Z} \times \mathbb{Z}/\ell_2^{e_2}\mathbb{Z} \times ... \times \mathbb{Z}/\ell_s^{e_S}\mathbb{Z}$ of the form $(u_1\ell_1^{n_1}, u_2\ell_2^{n_2}, ..., u_s\ell_s^{n_s})$ where u_i are units in $\mathbb{Z}/\ell_i^{e_i}$, and $0 \leq n_i \leq e_i$. Then the number of ways of writing a as product of M elements in $(\mathbb{Z}/m\mathbb{Z})$ (not counting under the equivalence by S_M) is

$$\phi(m)^{M-1} \prod_{j=1}^{s} \left(\sum_{i_{M-2}=0}^{n_j} \sum_{i_{M-3}=0}^{i_{M-2}} ... \sum_{i=0}^{i_1} 1 \right). \tag{4.4}$$

Let us first look for the case $M = 2$ and $m = \ell^e$. Let us write $a = u\ell^n$, where u is a unit in $\mathbb{Z}/\ell^e\mathbb{Z}$ and $n \in \{0, 1, 2, ..., e\}$. Then the number of times that a as a product of M number of terms is the same as the number of times ℓ^n as a product of M terms. Hence it is enough to compute the number of ways of writing a as a product of two terms only for ℓ^n. Any ℓ^n can be written as the product of two terms in the following ways

$$\ell^n = u(u^{-1}l^n) = (u\ell)(u^{-1}\ell^{n-1})... = (u\ell^{n-1})(u^{-1}\ell) = (u\ell^n)u^{-1},$$

for any unit $u \in \mathbb{Z}/\ell^e\mathbb{Z}$. Hence the number of times ℓ^n can be written as product of two terms is $(n + 1)\phi(\ell^e)$.

In general, the number of times a can be written as product of M terms is

$$\left(\sum_{i_{M-2}=0}^{n} \sum_{i_{M-3}=0}^{i_{M-2}} \cdots \sum_{i=0}^{i_1} 1 \right) \phi(\ell^e)^{M-1},$$

This can be realized by noting that a product of M terms is also a product of two terms; one term is a product of $M - 1$ terms and the other. Then for any $a \in \mathbb{Z}/m\mathbb{Z}$ we have an element in $\mathbb{Z}/\ell_1^{e_1}\mathbb{Z} \times \mathbb{Z}/\ell_2^{e_2}\mathbb{Z} \times ... \times \mathbb{Z}/\ell_s^{e_S}\mathbb{Z}$ under the natural isomorphism say $(u_1\ell_1^{n_1}, u_2\ell_2^{n_2}, ..., u_s\ell_s^{n_s}) \in \mathbb{Z}/\ell_1^{e_1}\mathbb{Z} \times \mathbb{Z}/\ell_2^{e_2}\mathbb{Z} \times ... \times \mathbb{Z}/\ell_s^{e_S}\mathbb{Z}$, where u_i are units and $0 \leq n_i \leq e_i$. Counting the number of ways of writing a as a product of M terms is equal to the product of the number of ways of writing each coordinate of a as a product of M terms.

The reader may note that the product in (4.4) is always at least 1. In particular, the product is exactly 1 if and only if a is a unit in $\mathbb{Z}/m\mathbb{Z}$.

4.3 Exponential sums for modular forms: the inverse case

One may now ask that for a given prime ℓ and small enough ε, how many primes p are there for which an estimate like (3.2) holds. Our attempt to answer this question is summarized in the following results.

Theorem 4.3.1 (Bajpai, Bhakta, García)**.** *Let $f(z)$ be a newform of weight k, without CM, and with integer Fourier coefficients. Consider the set $\mathcal{P}_k = \{\ell \text{ prime} \mid (k-1, \ell-1) = 1\}$. Then, for any fixed $\varepsilon > 0$ and any large enough $\ell \in \mathcal{P}_k$, the set of primes p satisfying*

$$\max_{\xi \in \mathbb{F}_\ell^*} \left| \sum_{n \leq \tau} \mathbf{e}_\ell \left(\xi a(p^n) \right) \right| \leq \tau \ell^{-\delta}$$

have density at least $1 + O_\varepsilon\left(\frac{1}{\ell^{1-3\varepsilon}}\right)$, where $\delta = \delta(\varepsilon)$ is same as in Theorem 2.2.1.

Intuitively, this theorem can be regarded as the inverse (holding ℓ fixed and varying p) of Theorem 3.0.1, and in this analogy, the following result is the inverse of Theorem 3.0.2. Just for the sake of simplicity, we are assuming $(k-1, \ell-1) = 1$, which can be easily avoided and will be evident from the proof of the following theorem.

Theorem 4.3.2 (Bajpai, Bhakta, García)**.** *If $f(z)$ is a cuspform, and can be written as $\mathbb{Q}$ linear combination of r many newforms without CM and with integer coefficients, such that all of these components satisfy GST hypothesis. Then, for any fixed $\varepsilon > 0$ and large enough ℓ, the set of primes p satisfying*

$$\max_{\xi \in \mathbb{F}_\ell^*} \left| \sum_{n \leq \tau} \mathbf{e}_\ell \left(\xi a(p^n) \right) \right| \leq \tau \ell^{-\delta}$$

have density at least $2^{-r} + O_\varepsilon\left(\frac{1}{\ell^{1-2\varepsilon}}\right)$, where $\delta = \delta(\varepsilon)$ is same as in Theorem 2.2.1.

4.3.1 Proof of Theorem 4.3.1

For any prime p, let us denote the roots of $x^2 - a(p)x + p^{k-1} \pmod{\ell}$ by $\alpha_p^{(\ell)}, \beta_p^{(\ell)}$. Recall that from Deligne-Serre correspondence, we have the associated Galois representation

$$\rho_f^{(\ell)} : \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right) \longrightarrow \mathrm{GL}_2\left(\mathbb{Z}_\ell\right),$$

such that $a(p) = \mathrm{tr}\left(\rho_f^{(\ell)}(\mathrm{Frob}_p)\right)$ for any prime $p \nmid N\ell$. It is clear that the characteristic polynomial of $\rho_f^{(\ell)}(\mathrm{Frob}_p) \pmod{\ell}$ is same as $x^2 - a(p)x + p^{k-1} \pmod{\ell}$. Following Ribet [74, Theorem 3.1], it is known that the image of this representation is $\left\{A \in \mathrm{GL}_2\left(\mathbb{Z}_\ell\right) \mid \det(A) \in \left(\mathbb{Z}_\ell^*\right)^{k-1}\right\}$, except possibly for finitely many primes ℓ.

In particular, the condition $(k-1, \ell-1) = 1$ implies that the induced Galois representation

$$\rho_{f,\ell} : \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right) \longrightarrow \mathrm{GL}_2\left(\mathbb{F}_\ell\right),$$

is surjective for any large prime ℓ, and the eigenvalues of the matrix $\rho_{f,\ell}(\mathrm{Frob}_p) \in \mathrm{GL}_2\left(\mathbb{F}_\ell\right)$ are $\alpha_p^{(\ell)}$ and $\beta_p^{(\ell)}$. From the proof of Theorem 3.0.1, we know that an estimate of type (3.2) holds provided that,

$$\mathrm{ord}\left(\alpha_p^{(\ell)}\right) > \ell^\varepsilon,\ \mathrm{ord}\left(\beta_p^{(\ell)}\right) > \ell^\varepsilon,\ \text{and}\ \ \mathrm{ord}\left(\alpha_p^{(\ell)}(\beta_p^{(\ell)})^{-1}\right) > \ell^\varepsilon.$$

Let us define,

$$C = \left\{ A \in \mathrm{GL}_2(\mathbb{F}_\ell) \mid \mathrm{ord}\left(\lambda_{1,A}\right), \mathrm{ord}\left(\lambda_{2,A}\right), \mathrm{ord}\left(\lambda_{1,A}\lambda_{2,A}^{-1}\right) > \ell^\varepsilon \right\},$$

where $\lambda_{1,A}, \lambda_{2,A}$ are the eigenvalues of A in $\mathbb{F}_{\ell^2}^*$. Now the problem is about computing the density of primes p for which the corresponding $\rho_{f,\ell}\left(\mathrm{Frob}_p\right)$ is in C. Note that C is a subset of $\mathrm{GL}_2(\mathbb{F}_\ell)$ stable under conjugation. Hence, by Chebotarev's density theorem, the required density is at least $\frac{|C|}{|\mathrm{GL}_2(\mathbb{F}_\ell)|}$. For each $a \neq b \in \mathbb{F}_\ell^*$, let $C_{a,b}$ be the conjugacy class of $\left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right)$. It is known that $|C_{a,b}| = (\ell+1)\ell$. For any element λ in $\mathbb{F}_{\ell^2} \setminus \mathbb{F}_\ell$, we denote c_λ to be the conjugacy class of matrices in $\mathrm{GL}_2\left(\mathbb{F}_\ell\right)$ having eigenvalue λ. It is known that $|C_\lambda| = \ell(\ell-1)$. Now, we consider the following sets:

$$S_1 = \left\{ a, b \in \mathbb{F}_\ell^* \mid \mathrm{ord}\left(a\right) > \ell^\varepsilon, \mathrm{ord}\left(b\right) > \ell^\varepsilon, \mathrm{ord}\left(ab^{-1}\right) > \ell^\varepsilon \right\},$$
$$S_2 = \left\{ \lambda \in \mathbb{F}_{\ell^2}^* \setminus \mathbb{F}_\ell^* \mid \mathrm{ord}\left(\lambda\right) = \mathrm{ord}\left(\lambda^\ell\right) > \ell^\varepsilon, \mathrm{ord}\left(\lambda^{\ell-1}\right) > \ell^\varepsilon \right\},$$

and realize that $|C| = \frac{1}{2}((\ell+1)\ell|S_1| + \ell(\ell-1)|S_2|)$. This reduced to the problem of estimating S_1 and S_2. Let us first estimate S_1. Take σ to be a generator of $\mathbb{F}_\ell^*$. For any divisor d of $\ell-1$, the set of all elements of $\mathbb{F}_\ell^*$ having order exactly d is of the form $\sigma^{\frac{\ell-1}{d}i}$ with $(i,d) = 1$. In particular, the number of elements of $\mathbb{F}_\ell^*$ with order greater than ℓ^ε is given by

$$\sum_{\substack{d|\ell-1 \\ d>\ell^\varepsilon}} \phi(d) = \ell + O\left(\sum_{\substack{d|\ell-1 \\ d<\ell^\varepsilon}} \phi(d)\right) = \ell + O\left(\ell^\varepsilon d(\ell-1)\right) = \ell + O_\varepsilon\left(\ell^{2\varepsilon}\right),$$

where $d(\cdot)$ is the divisor function, and here we are using the well-known upper bound on the divisor function (see [71]) for any prime ℓ large enough. Now note that $\mathrm{ord}\left(ab^{-1}\right) < \ell^\varepsilon$ implies that ab^{-1} belongs to a set with only $\sum_{k|\ell-1, k<\ell^\varepsilon} \phi(k)$ many elements. By the argument above, this set has only $O_\varepsilon\left(\ell^{2\varepsilon}\right)$ many elements. This observation implies that

$$|\left\{ a, b \in \mathbb{F}_\ell^* \mid \mathrm{ord}\left(a\right), \mathrm{ord}\left(b\right), \textit{or}\ \mathrm{ord}\left(ab^{-1}\right) < \ell^\varepsilon \right\}| = O_\varepsilon(\ell^{2\varepsilon+1}).$$

In particular, we then have $|S_1| = \ell^2 + O_\varepsilon(\ell^{2\varepsilon+1})$.

Let us now estimate $|S_2|$. Take τ to be a generator of $\mathbb{F}_{\ell^2}^*$, then any $\lambda \in S_2$, of order d, is of the form $\tau^{\frac{\ell^2-1}{d}i}$, with $(i,d)=1$. We also have an order restriction on $\lambda^{\ell-1}$, which implies that $\frac{d}{(d,\ell-1)} > \ell^{\varepsilon}$. Hence,

$$|S_2| = \sum_{\substack{d|\ell^2-1 \\ \frac{d}{(d,\ell-1)}>\ell^{\varepsilon}}} \phi(d) = \ell^2 + O\Big(\sum_{\substack{d|\ell^2-1 \\ \frac{d}{(d,\ell-1)}<\ell^{\varepsilon}}} \phi(d) \Big).$$

Note that, the condition $\frac{d}{(d,\ell-1)} < \ell^{\varepsilon}$ implies that $d < \ell^{\varepsilon+1}$. Therefore,

$$\sum_{\substack{d|\ell^2-1 \\ \frac{d}{(d,\ell-1)}<\ell^{\varepsilon}}} \phi(d) \leq \ell^{\varepsilon+1} d(\ell^2-1) = O_{\varepsilon}\left(\ell^{1+3\varepsilon}\right).$$

Therefore, the required density is at least

$$\frac{1}{2}(\ell-1)\ell\frac{|S_1|}{|\mathrm{GL}_2(\mathbb{F}_\ell)|} + \frac{1}{2}(\ell+1)\ell\frac{|S_2|}{|\mathrm{GL}_2(\mathbb{F}_\ell)|} = 1 + O_{\varepsilon}\left(\frac{1}{\ell^{1-3\varepsilon}}\right).$$

□

4.3.2 Proof of Theorem 4.3.2

Let $\rho_{f,\ell} : \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right) \to \mathrm{GL}_{2r}(\mathbb{F}_\ell)$ be the map defined by

$$\sigma \mapsto \begin{pmatrix} \rho_{f_{1,\ell}}(\sigma) & & & \\ & \rho_{f_{2,\ell}}(\sigma) & & \\ & & \ddots & \\ & & & \rho_{f_{r,\ell}}(\sigma) \end{pmatrix}.$$

It is clear that the image of this representation is contained in $\Delta_r(\ell)$, where

$$\Delta_r(\ell) = \left\{ \begin{pmatrix} g_1 & & & \\ & g_2 & & \\ & & \ddots & \\ & & & g_r \end{pmatrix} \mid \det(g_1) = \det(g_2) = \cdots = \det(g_r) \right\}.$$

It is in fact the case that the image is contained in $\Delta_r^{(k-1)}(\ell)$, where $\Delta_r^{(k-1)}(\ell)$ denotes the set of matrices in $\Delta_r(\ell)$ in which determinant of each block is a $(k-1)^{th}$ power in $\mathbb{F}_\ell^*$. Due to [74, Theorem 3.1], we may assume that for any prime ℓ large enough, the image of each $\rho_{f_{i,\ell}}$ is $\Delta_1^{(k-1)}(\ell)$, which coincides with the set of matrices in $\mathrm{GL}_2(\mathbb{F}_\ell)$ whose determinants are a $(k-1,\ell-1)^{th}$ power in $\mathbb{F}_\ell^*$. If the image of $\rho_{f,\ell}$ is not exactly $\Delta_r^{(k-1)}(\ell)$, then by [63, Lemma 5.1] we get a set of quadratic characters $\{\chi_{i,j,\ell}\}_{1\leq i,j\leq r}$ of $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$ such that

$$\rho_{f_i,\ell}(\mathrm{Frob}_p) \text{ is conjugate to } \chi_{i,j,\ell}(\mathrm{Frob}_p)\,\rho_{f_j,\ell}(\mathrm{Frob}_p) \text{ in } \mathrm{GL}_2(\mathbb{F}_\ell),$$

for all $1 \le i, j \le r$. In particular, $a_i(p) = \pm a_j(p) \pmod{\ell}$, for all $1 \le i, j \le r$, and any prime $p \nmid N\ell$. This implies that $\alpha_\ell^{(i,p)} + \beta_\ell^{(i,p)} = \pm(\alpha_\ell^{(j,p)} + \beta_\ell^{(j,p)})$. Moreover, we also know that

$$\alpha_\ell^{(i,p)}\beta_\ell^{(i,p)} = \alpha_\ell^{(j,p)}\beta_\ell^{(j,p)} = p^{k-1} \pmod{\ell}.$$

In particular, this means that

$$\{\alpha_\ell^{(i,p)}, \beta_\ell^{(i,p)}\} = \pm\{\alpha_\ell^{(j,p)}, \beta_\ell^{(j,p)}\}, \forall 1 \le i, j \le r, \text{and for any prime } p \nmid N\ell. \quad (4.5)$$

Due to GST, for a positive density of primes p, none of these

$$\{\alpha^{(i,p)}\beta^{-(j,p)}\}_{1\le i,j\le 2} \quad \text{or} \quad \pm\{\alpha^{(i,p)}, \alpha^{-(j,p)}\}_{1\le i\ne j\le 2}$$

are roots of unity. For those primes p, following the arguments in the proof of Lemma 3.2.1, and considering the set in (3.12), each element of the set $\{\alpha_\ell^{(i,p)}\beta_\ell^{-(j,p)}\}_{1\le i,j\le 2}$ has order larger than 4 except for finitely many primes ℓ. We then have a contradiction to (4.5), and hence we may assume that the image of $\rho_{f,\ell}$ is indeed $\Delta_r^{(k-1)}(\ell)$ for any prime ℓ large enough.

Hence, the required density is at least $\frac{|C_r^{k-1}(\ell)|}{|\Delta_r^{(k-1)}(\ell)|}$, where $C_r^{k-1}(\ell)$ is the union of conjugacy classes of elements in $\Delta_r^{(k-1)}(\ell)$ whose eigenvalues satisfy the conditions of Theorem 2.2.1. Note that any tuple $(a_1, a_2, \cdots, a_{2r}) \in (\mathbb{F}_\ell^*)^{2r}$ with $\mathrm{ord}\,(a_i) > \ell^\varepsilon$, $\mathrm{ord}\,(a_i a_j^{-1}) > \ell^\varepsilon, \forall i \ne j$ and $a_i a_{i+1} = a_j a_{j+1}, \forall i, j$ odd, satisfies that $\prod_{i,\ \mathrm{odd}} C_{a_i,a_{i+1}} \subseteq C_r^{k-1}(\ell)$. We call these tuples *nice* and we want to count them. First of all note that,

$$\{(a_1, a_2, \cdots, a_{2r}) \in (\mathbb{F}_\ell^*)^{2r} \mid a_i a_{i+1} = a_j a_{j+1}, \forall i, j \text{ odd}\} = \frac{(\ell-1)^{r+1}}{(\ell-1, k-1)}.$$

On the other hand, for any $(k-1)^{th}$ power λ in $\mathbb{F}_\ell^*$, note that $ab = \lambda$ and $\mathrm{ord}\,(ab^{-1}) < \ell^\varepsilon$ imply $\mathrm{ord}\,(a^2\lambda^{-1}) < \ell^\varepsilon$. From the proof of Theorem 4.3.1, for a fixed λ, the number of such a is $O_\varepsilon(\ell^{2\varepsilon})$. Moreover, $\mathrm{ord}\,(a) < \ell^\varepsilon$ or $\mathrm{ord}\,(b) < \ell^\varepsilon$ holds for only $O_\varepsilon(\ell^{2\varepsilon})$ many elements a or b. In particular, the number of tuples that does not come into our consideration is

$$\sum_{\lambda,\ (k-1)^{th}\ \mathrm{power}} O_\varepsilon(\ell^{r-1+2\varepsilon}) = O_\varepsilon\left(\frac{\ell^{r+2\varepsilon}}{(k-1, \ell-1)}\right).$$

In particular, we then have

$$\begin{aligned} |C_r^{k-1}(\ell)| &\ge \sum_{(a_1,a_2,\cdots,a_r)\ \mathrm{nice}} \left(\prod_{i\ \mathrm{odd}} |C_{a_i,a_{i+1}}|\right) \\ &= \left(\frac{\ell(\ell+1)}{2}\right)^r \left(\frac{(\ell-1)^{r+1}}{(\ell-1, k-1)} + O_\varepsilon\left(\frac{\ell^{r+2\varepsilon}}{(k-1, \ell-1)}\right)\right). \end{aligned} \quad (4.6)$$

The extra factor $\left(\frac{\ell(\ell+1)}{2}\right)^r$ is coming because each conjugacy class $C_{a_{i,i+1}}$ has $\ell(\ell+1)$ many elements and taking into consideration that $C_{a_i,a_{i+1}} = C_{a_{i+1},a_i}, \forall i$ odd, the

extra factor $\frac{1}{2}$ is coming for each component. The proof is now complete because $|\Delta_r^{(k-1)}(\ell)| = \left(\frac{|\mathrm{GL}_2(\mathbb{F}_\ell)|}{\ell-1}\right)^r \frac{\ell-1}{(\ell-1,k-1)}$. □

4.4 On a local-global phenomenon

In this section, we shall discuss a special phenomenon of the Galois representations for composite modulus, which we call a local-global property. For example, in the proof of Lemma 4.1.3, we see that the Galois representation modulo composite number m has a certain property if and only if it has the same property modulo any of the prime factors of m. Following the same, we shall discuss other analogous cases in this section.

For any arbitrary number K, we arrange the elliptic curves over K with respect to the usual height $h(E) = ||(a,b)||$, where we consider the usual norm in $\mathbb{R} \otimes \mathcal{O}_K^2 \cong \mathbb{R}^{2[K:\mathbb{Q}]}$. Here E is in the Weierstrass form given by $E_{(a,b)} : y^2 = x^3 + ax + b$ with $a, b \in \mathcal{O}_K$, the ring of integers of K. Denote $S_K(x) = \{(a,b) \in \mathcal{O}_K^2 \mid h(E_{(a,b)}) \leq x\}$. It can be shown that $\#S_K(x) = c_K x^{2[K:\mathbb{Q}]}$, for some constant $c_K > 0$. In this regard, we first prove the following. Throughout the whole section, we say a *property* holds for almost all elliptic curves over K, if the *property* holds for all but $o\left(x^{2[K:\mathbb{Q}]}\right)$ many elliptic curves in $S_K(x)$, as $x \to \infty$.

Theorem 4.4.1 (Bhakta)**.** *Let K be a number field with discriminant d_K and degree D_k over $\mathbb{Q}$. Consider E/K to be an elliptic curve and m be any natural number co-prime to* 30.

(i) The induced Galois representation $\rho_{E,m}$ is surjective if and only if $\rho_{E,\ell}$ is surjective for any prime $\ell | m$, provided that K contains no proper abelian extension of $\mathbb{Q}$, or if m is co-prime to the discriminant D_K.

(ii) Any integer m co-prime to 30*, that is not square-free, is bad. Moreover, for any number field, K_m native to m, almost all the elliptic curves over K_m are exceptional.*

Before proceeding to the proof, let us first shed some light on (ii). We call a natural number m, *bad* if there exists a finite extension K_m of K, and an elliptic curves E over K_m such that $\mathrm{im}(\rho_{E,m}) \neq \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ but $\mathrm{im}(\rho_{E,\ell}) = \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ for any prime $\ell \mid m$. Moreover, we call such a number field as *native* to m and such an elliptic curve as *exceptional elliptic curve* for the pair (m, K_m). This is how we measure the failure of local-global property for Galois representations.

4.4.1 Proof of Theorem 4.4.1

Proof of part (i). Let m be an integer co-prime to 30. If $\rho_{E,m}$ is surjective, then $\rho_{E,\ell} = \mathrm{pr}_{m,\ell} \circ \rho_{E,m}$ is surjective for any $\ell \mid m$, where

$$\mathrm{pr}_{m,\ell} : \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}) \longrightarrow \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}),$$

is the natural projection.

For the converse, it follows from the given hypothesis that $\mathrm{im}(\rho_{E,\ell}) = \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ is a quotient of $\mathrm{im}(\rho_{E,m})$ for any prime $\ell|m$. In particular, $\mathrm{PSL}_2(\mathbb{Z}/\ell\mathbb{Z}) \in \mathrm{Occ(G)}$ for any prime $\ell|m$, where $\mathrm{G} = \mathrm{im}(\rho_{E,m})$. It follows from Lemma 4.1.4 that, $\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})$ is contained in G. We then have that $\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z}) = \mathrm{comm(G)}$, and in particular $[\mathrm{G} : \mathrm{comm(G)}] \mid \phi(m)$. On the other hand, the Weil pairing gives $[K(\zeta_m) : K] \mid [\mathrm{G} : \mathrm{comm(G)}]$. It is now enough to ensure that $[K(\zeta_m) : K] = \phi(m)$. Note that, $[K(\zeta_m) : K] = [\mathbb{Q}(\zeta_m) : K \cap \mathbb{Q}(\zeta_m)]$, and hence it is enough to ensure that $K \cap \mathbb{Q}(\zeta_m) = \mathbb{Q}$. We shall see the imposed conditions on m or K gives us that privilege.[2]

First of all, since $K \cap \mathbb{Q}(\zeta_m)$ is an abelian extension of $\mathbb{Q}$ contained in K, the first imposed condition on K forces the intersection to be trivial. On the other hand, since $K \cap \mathbb{Q}(\zeta_m)$ is an extension of $\mathbb{Q}$ contained in both K and $\mathbb{Q}(\zeta_m)$, it is evident that the condition $(\phi(m), D_K) = 1$ implies $K \cap \mathbb{Q}(\zeta_m) = \mathbb{Q}$. Moreover, the assumption $(m, d_K) = 1$ immediately implies that the discriminant of $K \cap \mathbb{Q}(\zeta_m)$ is only 1. In particular, in all the cases we have $K \cap \mathbb{Q}(\zeta_m) = \mathbb{Q}$, as desired.

Proof of part (ii). Take any integer m that is not square-free. Write $m = \prod_{i=1}^{d} \ell_i^{e_i}$ and without loss of generality let us assume that $e_1 > 1$. Consider F to be an extension of $\mathbb{Q}$ contained in $\mathbb{Q}(\zeta_{\ell_1^{e_1}})$ of degree ℓ_1. We can do that, because $e_1 > 1$ by the assumption. It is evident that, $F \cap \mathbb{Q}(\zeta_{\ell_1}) = \mathbb{Q}$. Now for any $i > 1$, we have $\mathbb{Q}(\zeta_{\ell_i}) \cap \mathbb{Q}(\zeta_{\ell_1^{e_1}}) = \mathbb{Q}$, and in particular, we have $F \cap \mathbb{Q}(\zeta_{\ell_1}) = \mathbb{Q},\ \forall 1 \leq i \leq d$. Hence, for any $1 \leq i \leq d$ we have

$$[F(\zeta_{\ell_i}) : F] = [\mathbb{Q}(\zeta_{\ell_i}) : F \cap \mathbb{Q}(\zeta_{\ell_i})] = \ell_i - 1,$$

where the last implication is true because $F \cap \mathbb{Q}(\zeta_{\ell_i}) = \mathbb{Q}$. Let us now denote $K_m = F$, and show that the pair (m, K_m) satisfies all the necessary conditions for m to be a potentially bad number. First, we need to show that there exists at least one elliptic curve E over K_m, for which

$$\mathrm{im}(\rho_{E,m}) \neq \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}) \text{ but } \mathrm{im}(\rho_{E,\ell_i}) = \mathrm{GL}_2(\mathbb{Z}/\ell_i\mathbb{Z}),\ \forall\ 1 \leq i \leq d.$$

We know from [100, Proposition 2.1] that, there exists at least one elliptic curve E/K_m for which $\mathrm{im}(\rho_{E,\ell_i}) \supset \mathrm{SL}_2(\mathbb{Z}/\ell_i\mathbb{Z}),\ \forall\ 1 \leq i \leq d$. In fact, this holds for almost all elliptic curves over K_m. From the construction, we know that $[K_m(\zeta_{\ell_i}) : K_m] = \ell_i - 1,\ \forall 1 \leq i \leq d$. Now it follows from the argument of part (a) that, i.e., due to the Weil pairing that, $\mathrm{im}(\rho_{E,\ell_i}) = \mathrm{GL}_2(\mathbb{Z}/\ell_i\mathbb{Z}),\ \forall\ 1 \leq i \leq d$.

On the other hand, for any elliptic curve E/K_m, if the image of $\rho_{E,m}$ is $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$, then we must have that $|K_m(\zeta_m) : K_m| = \phi(m)$. This is because, it follows from Weil-pairing that $\zeta_m \in K_m(E[m])$ and $\sigma(\zeta_m) = \zeta_m^{\det(\rho_{E,m}(\sigma))}$, where ζ_m is the primitive m^{th} root of unity. In particular, the fixed field of $\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})$ correspond to $K(\zeta_m)$. This shows that $[K_m(\zeta_m) : K_m] = \phi(m)$. Instead, we have

$$[K_m(\zeta_m) : K_m] = [\mathbb{Q}(\zeta_m) : K_m \cap \mathbb{Q}(\zeta_m)] \leq [\mathbb{Q}(\zeta_m) : K_m] < \phi(m),$$

[2]This is not true in general. For instance, one may consider $K = \mathbb{Q}(\sqrt{-15})$ and then we have $[K(\zeta_{15}) : K] = 4 \neq \phi(15)$.

since K_m is a non-trivial extension of $\mathbb{Q}$ contained in $\mathbb{Q}(\zeta_m)$, a contradiction. $\square$

Remark 4.4.2. In part (b) of Theorem 4.4.1, we assume that m is square-free. Note that this assumption is necessary. Otherwise, we do not have the failure because

$$\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}) = \prod_{\ell,\ \substack{\text{prime}\\ \ell|m}} \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}).$$

Let us now discuss some interesting consequences of Theorem 4.4.1. If one wants to make Proposition 5.7 in [100] effective, one can see the explicit constant is given by $\frac{m^3}{\phi(m)}$. First let us recall the definition of the set $B_{K,m}(x)$ from [100].

Corollary 4.4.3. *For any $m \in \mathbb{N}$ with $(m, 30d_K) = 1$, the explicit constant is given by*

$$\sum_{\ell|m} \frac{\ell^3}{\phi(\ell)}.$$

Proof. It follows from the proof of Proposition 5.7 in [100], that $|B_{K,\ell}(x)| \leq \frac{\ell^3}{\phi(\ell)} \frac{\log x}{x^{\frac{[K:\mathbb{Q}]}{2}}}$. It is now enough to show that

$$B_{K,m}(x) \subseteq \bigcup_{\ell|m} B_{K,\ell}(X).$$

It follows from Theorem 4.4.1 that $\bigcap_{\ell|m} B_{K,\ell}(x)^c \supseteq B_{K,m}(x)^c$, and this completes the proof. $\square$

4.4.2 Local-global for pairs of elliptic curves

Serre introduced a representation associated with the pair of elliptic curves (analogously for the arbitrary tuple as well) as,

$$\rho_{E_1\times E_2,n}(\sigma) = \begin{pmatrix} \rho_{E_1,n}(\sigma) & 0 \\ 0 & \rho_{E_2,n}(\sigma) \end{pmatrix} \text{ for all } \sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}).$$

In this case, Serre showed an analog of his open image theorem. To be more precise, Serre showed that $\mathrm{im}(\rho_{E_1\times E_2,\ell}) = \Delta(\ell)$ for all but finitely many primes ℓ, where the diagonal subgroup $\Delta(\ell)$ is given by,

$$\Delta(\ell) = \left\{ \begin{pmatrix} g_1 & 0 \\ 0 & g_2 \end{pmatrix} \mid \det(g_1) = \det(g_2), \big(g_1, g_2\big) \in \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) \right\}.$$

Jones in [47] considered this topic and proved an asymptotic estimate analogous to Grant's main result in [44]. Grant's work was based on counting rational points on certain modular curves. Jones's approach was by studying the distribution of Frobenius symbols using the multi-dimensional version of Gallagher's large sieve.

Theorem 4.4.4 (Bhakta)**.** *Let K be a number field with discriminant d_K and degree D_k over $\mathbb{Q}$. Consider (E_1, E_2) be any pair of elliptic curves over K, and m be a natural number, and m be any natural number co-prime to 30. The induced Galois representation $\rho_{E_1\times E_2,m}$ has image $\Delta(m)$ if and only if, $\rho_{E,\ell}$ has image $\Delta(\ell)$ for any prime $\ell|m$, provided that K contains no proper abelian extension of $\mathbb{Q}$, or if m is co-prime to the discriminant D_K.*

Proof. One direction is obvious. For the other direction, by Theorem 4.4.1 we have that

$$\mathrm{im}(\rho_{E_1,m}) = \mathrm{im}(\rho_{E_2,m}) = \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}).$$

Let G be $\mathrm{im}(\rho_{E_1\times E_2,m}) \subseteq \Delta(m)$. It follows from the given condition that $\Delta(\ell)$ is a quotient of G, for any prime $\ell \mid m$. Denote $S\Delta(\ell)$ to be the set of elements in $\Delta(\ell)$ whose each block has determinant 1, and $G^{(\ell)}$ be $\ker \circ \pi_{m/\ell^r}(G) \subseteq \Delta(\ell^r)$, where r is the maximum power of ℓ dividing m, and π_{m/ℓ^r} be the natural projection $\Delta(m) \to \Delta(m/\ell^r)$.

Moreover, we consider $G' = \mathrm{pr}_\ell(G^{(\ell)}) \subseteq \Delta(\ell)$, and set

$$G'_1 = \Big\{ g \in \mathrm{GL}_2(\mathbb{F}_\ell) : \begin{pmatrix} I & \\ & g \end{pmatrix} \in G' \Big\},\ G'_2 = \Big\{ g \in \mathrm{GL}_2(\mathbb{F}_\ell) : \begin{pmatrix} g & \\ & I \end{pmatrix} \in G' \Big\}.$$

From the given condition we know that Occ of both G'_1 and G'_2 contains $\mathrm{PSL}_2(\mathbb{F}_\ell)$, for every prime $\ell \mid m$. In particular, it follows from Lemma 4.1.4 that G contains $S\Delta(m)$, which is defined to be the set of elements in $\Delta(m)$ having determinant 1. According to [47, Lemma 3.3], $G \neq \Delta(\mathbb{Z}/m\mathbb{Z})$ implies there exist a set $C_1 \times C_2 \subseteq \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$, closed under conjugation such that $\det(C_1) = \det(C_2) = 1$ with $G \cap (C_1 \times C_2) = \phi$. This contradicts the deduction that G contains $S\Delta(m)$. □

Let E be an elliptic curve over an arbitrary number field K, and consider $A(E) = 30\prod_{\ell\in M_E} \ell$, where M_E is the set of primes $\ell \geq 7$ such that $\rho_{E,\ell}$ is not surjective. Now for a pair of elliptic curves $E_1 \times E_2$ over K, let us consider

$$A(E_1 \times E_2) = 30 \prod_{\ell\in M_{E_1\times E_2}} \ell,$$

and $M_{E_1\times E_2}$ is the set of primes ℓ for which $\mathrm{im}(\rho_{E_1\times E_2,\ell}) \neq \Delta(\ell)$. It is clear that

$$\mathrm{lcm}(A(E_1), A(E_2)) \mid A(E_1 \times E_2).$$

If they are not equal, then there exists a prime ℓ such that $\mathrm{im}(\rho_{E_i,\ell}) = \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ for $i \in \{1, 2\}$, and $\mathrm{im}(\rho_{E_1\times E_2,\ell}) \neq \Delta(\ell)$. Now by [63, Lemma 5.1], $\rho_{E_1,\ell}$ and $\rho_{E_2,\ell}$ are conjugate up-to a quadratic character of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. It follows from [64, Proposition 1] and Theorem 4.4.4 the following.

Corollary 4.4.5. *Let K be any number field satisfying one of the conditions in part (a) of Theorem 4.4.1, and $E_1, E_2/K$ be two elliptic curves without complex multiplication, which are not isogenous over $\overline{\mathbb{Q}}$. then we have the following equality*

$$\mathrm{im}(\rho_{E_1\times E_2,m}) = \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}),$$

for any integer m co-prime to $A(E_1 \times E_2) \ll \max\{h_1, h_2\}^{O(1)}$, where h_1 and h_2 respectively be the heights of E_1 and E_2.

Proof. It follows from Theorem 4.4.4 that $\mathrm{im}(\rho_{E_1 \times E_2, m}) = \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$, for any integer m co-prime to $A(E_1 \times E_2)$. For an upper bound on $A(E_1 \times E_2)$, the reader may look at Proposition 1 in [64]. □

Remark 4.4.6. Jones in [47] showed that almost all pairs of elliptic curves over $\mathbb{Q}$ are pairwise non-isogenous over $\overline{\mathbb{Q}}$.

4.4.3 The modular analog

Let $f(z)$ be any newform of weight k and level N. It is known due to Deligne-Serre correspondence that, for any integer m we have an associated Galois representation

$$\rho_{f,m} : \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right) \longrightarrow \mathrm{GL}_2\left(\mathbb{Z}/m\mathbb{Z}\right),$$

such that $a(p) \pmod m \equiv \mathrm{tr}\left(\rho_{f,m}(\mathrm{Frob}_p)\right)$ for any prime $p \nmid Nm$. When f is without CM, it follows from [74] that, there exists an integer M_f such that for any integer m co-prime to M_f, the image of this representation is given by

$$\Delta_{k,m} = \left\{A \in \mathrm{GL}_2\left(\mathbb{Z}/m\mathbb{Z}\right) \mid \det(A) \in \left((\mathbb{Z}/m\mathbb{Z})^*\right)^{k-1}\right\}.$$

Following the proof of Theorem 4.4.1, one could see that for any integer m co-prime to 30, $\mathrm{im}(\rho_{f,m})$ contains $\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})$ if and only if, $\mathrm{im}(\rho_{f,\ell})$ contains $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$ for any prime $\ell \mid m$. In particular, one could perhaps get a smaller M_f, as long as we want the image to contain only $\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})$. In this direction, we ask the following.

Question 4.4.7. *Is it true that*

$$\mathrm{im}(\rho_{f,m}) = \Delta_{k,m} \text{ if and only if, } \mathrm{im}(\rho_{f,\ell}) = \Delta_{k,\ell},$$

for any prime $\ell \mid m$?

It is not hard to notice that the answer to this question is yes, provided that $\zeta_m^{(k-1,\ \phi(m))}$ is in the field corresponding to $\ker(\rho_{f,m})$.

Moreover, any cuspform $f(z)$ can be uniquely written as $c_1 f_1 + c_2 f_2 + \cdots c_r f_r$, where $c_1, c_2, \cdots, c_r \in \overline{\mathbb{Q}}$. One can attach a Galois representation $\rho_{f,m} : \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right) \to \mathrm{GL}_{2r}\left(\mathbb{Z}/m\mathbb{Z}\right)$ defined by the map

$$\sigma \mapsto \begin{pmatrix} \rho_{f_{1,\ell}}(\sigma) & & & \\ & \rho_{f_{2,\ell}}(\sigma) & & \\ & & \ddots & \\ & & & \rho_{f_{r,\ell}}(\sigma) \end{pmatrix}.$$

In this case, the image is contained in $\Delta_{k_1,k_2,\cdots,k_r}(m)$, where $\Delta_{k_1,k_2,\cdots,k_r}(m)$ denotes the set of all block matrices of size 2×2 in $\mathrm{GL}_2\left(\mathbb{Z}/m\mathbb{Z}\right)$ in which determinant of each block is a $k_i - 1^{th}$ power of some element in the multiplicative group $(\mathbb{Z}/m\mathbb{Z})^*$.

Arguing similarly as in the proof of Theorem 4.4.4 one can see that, $\mathrm{im}(\rho_{f,m})$ contains $\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})^r$ if and only if, $\mathrm{im}(\rho_{f,\ell})$ contains $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})^r$ for any prime $\ell \mid m$. One can show that when $f_1, f_2, \cdots, f_r$ are not pairwise equivalent, $\mathrm{im}(\rho_{f,m})$ contains $\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})^r$ for all but finitely many primes ℓ. In this regard, we again ask the following stronger question.

Question 4.4.8. *Is it true that*

$$\mathrm{im}(\rho_{f,m}) = \Delta_{k_1,k_2,\cdots,k_r,m} \text{ if and only if, } \mathrm{im}(\rho_{f,\ell}) = \Delta_{k_1,k_2,\cdots,k_r,\ell},$$

for any prime $\ell \mid m$?

Chapter 5

Solutions having polynomial-growth

The main goal of this chapter is to extend the main result of Shparlinski [85] for a larger class of cuspforms. In certain cases, we also study the same problem, modulo composite numbers. As already explained in the introduction, the obtained solutions in Chapter 3 could be too large. In this chapter, we aim to achieve solutions of smaller sizes. Let us first discuss the tools that will be used throughout.

5.1 Growth results and exponential sums over finite fields

Let $m, s, \omega \geq 1$ be any given integers, and $A_1, A_2, \cdots, A_\omega$ be some subsets of $\mathbb{Z}/m\mathbb{Z}$ satisfying

$$\prod_{i=1}^{\omega} \#A_i \geq m^{1+\beta}, \tag{5.1}$$

for some $\beta > 0$. For any $a \in \mathbb{Z}/m\mathbb{Z}$, we denote $T_s(a)$ be the number of solutions to the equation

$$\prod_{i=1}^{\omega} a_1^{(i)} + \prod_{i=1}^{\omega} a_2^{(i)} + ... + \prod_{i=1}^{\omega} a_s^{(i)} \equiv a \pmod{m}, \tag{5.2}$$

where $a_j^{(i)} \in A_i,\ \forall 1 \leq j \leq s, 1 \leq i \leq \omega$. Following Section 2.3.1 in Chapter 2, we then have the following counting formula,

$$T_s(a) = \frac{(\#A_1 \#A_2 \cdots \#A_\omega)^s}{m} + O\left(\frac{1}{m}\sum_{\lambda=1}^{m-1}\left|\sum_{a^{(1)}\in A_1,\cdots,a^{(\omega)}\in A_\omega} \mathbf{e}_m\left(\lambda a^{(1)}a^{(2)}\cdots a^{(\omega)}\right)\right|^s\right). \tag{5.3}$$

When $\omega = 2$, an old result mentioned in Exercise 14.a in [98, Chapter 6] says that

$$\max_{\lambda \in \mathbb{Z}/m\mathbb{Z}} \left| \sum_{a_1 \in A_1} \sum_{a_2 \in A_2} \mathbf{e}_m \left(\lambda a_1 a_2\right) \right| \leq \sqrt{m \# A_1 \# A_2}. \tag{5.4}$$

To prove this, the reader may use the same argument as in the proof of Lemma 7 in [21], replacing q by m and taking $a := 1_{A_1}, b := 1_{A_2}$ and $\phi := \mathrm{e}_m$. As an immediate consequence, we obtain the following by the bound at (5.4) in (5.3).

Corollary 5.1.1. *For $\omega = 2$ and any $s > 2/\beta$, the sum*

$$a_1^{(1)} a_1^{(2)} + a_2^{(1)} a_2^{(2)} + \cdots a_s^{(1)} a_s^{(2)}$$

is equidistributed in $\mathbb{Z}/m\mathbb{Z}$, where β is the same constant as in (5.1), and $a_j^{(1)} \in A_1, a_j^{(2)} \in A_2, \forall 1 \leq j \leq s$.

To study (5.2) for $\omega = 3$, we shall use the following bound by Shkredov in [83, Theorem 5].

Theorem 5.1.2. *Let $A_1, A_2, A_3 \subseteq \mathbb{F}_\ell$ be arbitrary sets such that for some $\delta > 0$ the following holds*

$$|A_1||A_2||A_3| \geq \ell^{1+\beta}. \tag{5.5}$$

Then

$$\max_{\lambda \in (\mathbb{Z}/\ell\mathbb{Z})^*} \left| \sum_{a_1 \in A_1} \sum_{a_2 \in A_2} \sum_{a_3 \in A_3} \mathbf{e}_\ell \left(\lambda a_1 a_2 a_3\right) \right| \ll \frac{|A_1||A_2||A_3|}{\ell^{\frac{\beta}{8\log(8/\beta)+4}}}.$$

To treat the case $\omega > 3$, the following bound due to Bourgain, Gilbichuck in [21, Theorem 2] will be handy for us.

Theorem 5.1.3 (Bourgain-Gilbichuck)**.** *Let $3 \leq \omega \ll \log\log \ell$ be a natural number and $\varepsilon > 0$ an arbitrary fixed constant. For any subsets $A_1, A_2, \cdots, A_\omega \subset \mathbb{F}_\ell \setminus \{0\}$ with*

$$|A_1| \cdot |A_2| \cdot (|A_3| \cdots |A_\omega|)^{1/81} > \ell^{1+\beta}, \tag{5.6}$$

there is an estimate

$$\max_{\lambda \in (\mathbb{Z}/\ell\mathbb{Z})^*} \left| \sum_{a_1 \in A_1} \sum_{a_2 \in A_2} \cdots \sum_{a_\omega \in A_\omega} \mathbf{e}_\ell \left(\lambda a_1 a_2 \cdots a_\omega\right) \right| \ll \frac{|A_1||A_2| \cdots |A_\omega|}{\ell^{0.45\beta/2^\omega}}.$$

To study modulo composite numbers, we need to study these exponential sums over arbitrary finite fields $\mathbb{F}_q$. For which, we could use Theorem 4 of Bourgain-Gilbichuck in [21]. With this, we get a non-trivial bound assuming that, for any $d \in \mathbb{F}_q$ and any proper subfield S of $\mathbb{F}_q$, dS has a small intersection with each of the set A_i. However in our case, each of the sets A_i will be in a prime field $\mathbb{F}_\ell$, and hence, we can not use this result. However, Theorem 5.1.2 and Theorem 5.1.3 could be used to study the square-free integers. To be more precise, using these two results, we have the following.

Corollary 5.1.4. *Let m be any square-free integer, and $A_1, A_2, \cdots, A_\omega \subseteq (\mathbb{Z}/m\mathbb{Z})^*$ with*

$$|A_1| \cdot |A_2| \cdot (|A_3| \cdots |A_\omega|)^{1/81} > m^{1+\beta}. \tag{5.7}$$

Then we have the following estimate

$$\max_{\lambda \in (\mathbb{Z}/m\mathbb{Z})^*} \left| \sum_{a_1 \in A_1} \sum_{a_2 \in A_2} \cdots \sum_{a_\omega \in A_\omega} \mathbf{e}_m\left(\lambda a_1 a_2 \cdots a_\omega\right) \right| \ll \frac{|A_1||A_2| \cdots |A_\omega|}{\ell^{0.45\beta/2^\omega}},$$

for some prime factor ℓ of m.

Proof. Note that there exists a prime $\ell \mid m$ for which

$$|A_1^{(\ell)}| \cdot |A_2^{(\ell)}| \cdot (|A_3^{(\ell)}| \cdots |A_\omega^{(\ell)}|)^{1/81} > \ell^{1+\beta},$$

where $A_i^{(\ell)}$ is denoted to be ℓ^{th} component of A_i, $\forall 1 \le i \le \omega$. The proof now follows applying Theorem 5.1.3 for $\{A_i^{(\ell)}\}_{1 \le i \le \omega}$, and trivially estimating the exponential sum associated to the other components. □

5.2 Residue classes over small range

Let $f(z)$ be a cuspform with coefficients in $\mathbb{Q}$, and m be any integer. In this section, we give a lower bound for the number of elements in the set $\{a(n) \pmod m\}_{n \in I}$, where I is some small set. We know from section 4.1 that the set is $\mathbb{Z}/m\mathbb{Z}$, when I is a large set, and $f(z)$ is of a certain type. In this section, we shall consider a small set I. Shparlinski in [85] considered this for the Ramanujan-tau function. Arguing along the same lines, we first have the following generalization.

Lemma 5.2.1. *Let $f(z)$ be any Hecke eigenform, and m be any integer. For any set of primes S, consider*

$$N_{f,m,S}(x) = \#\{a(p), a(p^2) \pmod m \mid p \le \sqrt{x}\}.$$

If S has a positive density, then for any $x \ge 1$,

$$N_{f,m,S}(x) \gg_S x^{1/4+o(1)},$$

provided that $x^{1/2} \le L$, where L is the largest prime factor of m. In particular $N_{f,L,S}(m^{2\varepsilon}) \gg_S m^{\frac{\varepsilon}{2}+o(1)}$, for any $1 > \varepsilon > 0$, provided that $m^\varepsilon \le L$.

The proof is essentially the same as in [85]. It follows from the Hecke relation $a(p^2) = a(p)^2 - p^{k-1}$, and the fact that the number of distinct residue classes $p^{k-1} \pmod m$, $p \le \sqrt{x} \le L$ is $\gg \sqrt{x}$. Given any integer m, the condition $m^\varepsilon \le L$ is, of course, satisfied for any small $\varepsilon > 0$. However if we want to take any $1/2 \le \varepsilon < 1$, we should have that $\nu_L(m) = 1$ and L is sufficiently larger than the other prime factors of m.

Let $f_1, f_2, \cdots, f_r$ be a set of eigenforms of the same weight k and level N, and consider

$$\mathcal{S}_{f_1,f_2,\cdots,f_r,m} = \left\{p \mid a_1(p) \equiv a_2(p) \cdots \equiv a_r(p) \pmod{m},\ p^{k-1} \equiv 1 \pmod{m}\right\}. \tag{5.8}$$

Then we have the following.

Lemma 5.2.2. *If all of the $f_1, f_2, \cdots, f_r$ are newforms without CM, then $\mathcal{S}_{f_1,f_2,\cdots,f_r,m}$ has a positive density of primes, if it is non-empty. Otherwise there exists an integer N_f, such that for any integer m co-prime to N_f,*

$$a_i(p) \equiv \pm a_j(p) \pmod{m},\ p^{k-1} = 1 \pmod{m}\ \forall\ 1 \leq i, j \leq r,$$

for a set of primes p with positive density.

Proof. Let us first start with recalling the Galois representation from (4.2)

$$\rho_{f_1,f_2,\cdots,f_r,m} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_{2r}(\mathbb{Z}/m\mathbb{Z}).$$

Now consider

$$C = \left\{ \begin{pmatrix} A_1 & & & \\ & A_2 & & \\ & & \ddots & \\ & & & A_r \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})^r \;\middle|\; \mathrm{tr}(A_1) = \mathrm{tr}(A_2) = \cdots = \mathrm{tr}(A_r) \right\}.$$

If $\mathcal{S}_{f_1,f_2,\cdots,f_r,m}$ is non-empty, then $C \cap \mathrm{im}(\rho_{f_1,f_2,\cdots,f_r,m})$ is also non-empty, and we have the required positive density due to Chebotarev's density theorem.

On the other hand if $\mathcal{S}_{f_1,f_2,\cdots,f_r,m}$ is empty, then it follows from (4.1) that $\mathrm{G}_{f_1,f_2,\cdots,f_r,m}$ does not contain $\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})^r$. Then Lemma 4.1.3 in Chapter 3, implies that there is more than one equivalence class in the set $\{f_1, f_2, \cdots, f_r\}$. Let $f_{i_1}, f_{i_2}, \cdots, f_{i_{r'}}$ be the representatives from each class. Again applying Lemma 4.1.3, we see that $\mathrm{G}_{f_{i_1},f_{i_2},\cdots,f_{i_{r'}},m}$ contains $\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})^{r'}$. The proof is now complete due to (4.1). Also, note that the condition $p^{k-1} \equiv 1 \pmod{m}$ is satisfied because we are working with the conjugacy classes in $\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})$. □

Let us now consider $f_1, f_2, ..., f_r$ be the Hecke eigenforms with Fourier expansion $f_i(z) = \sum_{n=1}^{\infty} a_i(n) z^n$, and $a_i(n) \in \mathbb{Q},\ \forall 1 \leq i \leq r$. For any homogeneous polynomial $P(x_1, x_2, ..., x_r)$ with $P(\pm 1, \pm 1, ..., \pm 1) \neq 0$, set $a(n) = P(a_1(n), a_2(n), ..., a_r(n))$. Consider the quantity $N_{f,m,S}(x)$ as in Lemma 5.2.1. Since we are assuming that $P(\pm 1, \pm 1, ..., \pm 1) \neq 0$, we can also assume that $P(\pm 1, \pm 1, ..., \pm 1) \neq 0 \pmod{m}$, for any integer m with sufficiently large prime factors.

Corollary 5.2.3. *Suppose that $f_1, f_2, \cdots, f_r$ are all newforms without CM. Let m be any integer with sufficiently large prime factors satisfying that $P(\pm 1, \pm 1, ..., \pm 1) \neq 0 \pmod{m}$, and L be the largest prime factor of m satisfying that $m^{\varepsilon} \leq L$ for some $0 < \varepsilon < 1$. Then we have,*

$$N_{f,L,S}(m^{2\varepsilon}) \gg \frac{m^{\varepsilon/2+o(1)}}{d},\ d = \deg(P).$$

Proof. If the set $\mathcal{S}_{f_1,f_2,\cdots,f_r,m}$ in (5.8) is non-empty, then it follows from Chebotarev's density theorem that for any $n \geq 1$,

$$a(p^n) = P(a_1(p^n), a_1(p^n), \cdots a_1(p^n)) \pmod{m},$$

for a set of primes p with positive density. Since $P(x_1, x_2, \cdots x_r)$ is a homogeneous polynomial, we have

$$P(a_1(p^n), a_1(p^n), \cdots a_1(p^n)) = P(1, 1, \cdots, 1)a_1(p^n)^d \pmod{m},$$

where d is the degree of P. On the other hand for any prime p not in $\mathcal{S}_{f_1,f_2,\cdots,f_r,m}$,

$$a(p^n) = Q(a_1(p^n), a_1(p^n), \cdots a_1(p^n)) \pmod{m},\ \forall n \geq 1$$

for a set of primes p with positive density, where $Q(x_1, x_2, ..., x_r) = P(\pm x_1, \pm x_2, \cdots, \pm x_r)$. Since $P(x_1, x_2, .., x_r)$ is a homogeneous, $Q(x_1, x_2, ..., x_r)$ is a homogeneous polynomial of degree $d = \deg(P)$. Hence we get,

$$Q(a_1(p^n), a_1(p^n), ...a_1(p^n)) = P(\pm 1, \pm 1, \cdots, \pm 1)a_1(p^n)^d \pmod{m}.$$

The proof now follows immediately from Lemma 5.2.1 and by the assumption that $P(\pm 1, \pm 1, \cdots, \pm 1) \neq 0$. Note that the factor $1/d$ is coming because an equation $x^d = a \pmod{L}$ has at most d roots over $\mathbb{F}_L$. □

Remark 5.2.4. Here we are always concerned with when all the c_i are in $\mathbb{Q}$. The number of tuples $(c_1, c_2, \cdots, c_r)$ of height at most H is $\sim (2H/\zeta(2))^r$, see [46, Theorem B.6.2] Among them, the number of tuples $(c_1, c_2, \cdots, c_r)$ with $\sum_{i=1}^{m} \pm c_i = 0$ is $\sim H^{r-1}$. In the sense of heights, we are saying that almost any f in $S_k(\mathbb{Q}, N)$ of the form $\sum_{i=1}^{r} c_i f_i,\ c_i \in \mathbb{Q}$, satisfy the condition in Corollary 5.2.3.

Now to study the case when not all of the f_i are newforms without CM, we need to count the number of points on the intersection of certain hypersurfaces. In this case, we have a weaker lower bound in the sense of a lesser exponent.

Lemma 5.2.5. *Let us consider $a(n) = \sum_{i=1}^{r} a_i(n)$, then for any integer $m \geq 1$, the sum $\sum_{i=1}^{r} a_i(p)^m$ can be written as a linear combination of $a(p^{m'})$, $0 \leq m' \leq m$, where the coefficients are polynomials in p with coefficients in $\mathbb{Q}$. Moreover, the coefficient associated with 1 (resp. $a(p)$) has the highest degree when m is odd (resp. even).*

Proof. By the properties of the Hecke operators, we have

$$a_i(p^{2\beta}) = a_i(p)^{2\beta} - \binom{2\beta-1}{1} p^{12} a_i(p)^{2\beta-2} + \cdots + (-1)^{\beta-1} \binom{\beta+1}{2} p^{12\beta-12} a_i(p)^2 + \\ + (-1)^{\beta} p^{(k-1)\beta},$$

and

$$a_i(p^{2\beta+1}) = a_i(p)^{2\beta+1} - \binom{2\beta}{1}p^{12}a_i(p)^{2\beta-1} + \cdots + (-1)^{\beta-1}\binom{\beta+2}{3}p^{12\beta-12}a_i(p)^3 + \\ + (-1)^{\beta}\binom{\beta+1}{1}p^{(k-1)\beta}a_i(p),$$

for any $\beta \in \mathbb{N}$ and $i \in \{1, 2, \cdots, r\}$. Denoting $\sum_{i=1}^{r} a_i(p)^m = A_m$, we see that $a(p^n)$ can be written as a linear combinaton of $A_1, A_2, \cdots, A_n$, with the coefficients being polynomials in p. The proof now follows inductively, as $A_1 = a(p)$.

□

Lemma 5.2.6. *Let $a_1, a_2, ..., a_r$ be any r real numbers, $s_j = \sum_{i=1}^{r} a_i^j$, and consider $f(x) = x^r + q_1x^{r-1} + q_2x^{r-2} + ... + q_{r-1}x + q_r$ be the polynomial whose roots are $a_1, a_2, a_3, ..., a_r$. Then every coefficient q_k can be written as a polynomial in $\{s_j\}_{j\in\{1,2,...,r\}}$.*

Proof. The proof follows immediately from Newton's identity on the symmetric polynomials. More precisely we have

$$q_k = \frac{(-1)^k}{k!}B_k(-s_1, -1!s_2, \cdots, -(k-1)!s_k),$$

for some polynomial $B_k \in \mathbb{Q}[x_1, x_2, \cdots, x_k]$.

□

Proposition 5.2.7. *Let $f \in S(\mathbb{Q}, N)$ be any arbitrary element of the form $c_1f_1 + c_2f_2 + \cdots c_rf_r$, where $c_i \in \mathbb{Q}$, and all the f_i are Hecke eigenforms. For any set of primes S, and any integer m, let us consider*

$$N_{f,m,S}(x) = \#\{a(p), a(p^2), \cdots a(p^{2r}) \pmod m \mid p \leq x^{\frac{1}{2r}}\}.$$

Suppose that S has positive density. Then for any $\delta > 0$, and any sufficiently large $x \geq 1$, we have

$$N_{f,m,S}(x) \gg_S x^{\frac{1}{4r^2}-\delta},$$

provided that $x^{1/2r} \leq L$, where L is the largest prime factor of m. In particular $N_{f,L,S}(m^{2\varepsilon}) \gg_S m^{\frac{\varepsilon}{2r^2}-\delta}$, for any $\varepsilon > 0$, provided that $m^{\varepsilon/r^2} \leq L$.

Proof. Let $y > 0$ be any given real number for which $N_{f,m,S}(x) \leq y$. In particular, $\#\{a(p) \pmod m : p \leq x^{\frac{1}{2r}}\} < y$, and hence there exists a_1 such that $a(p) \equiv a_1 \pmod m$ for at least $\frac{x^{\frac{1}{2r}+o(1)}}{y}$ primes up-to $x^{\frac{1}{2r}}$. Now consider the set

$$S_{a_1} = \{p : a(p) \equiv a_1 \pmod m,\ p \leq x^{\frac{1}{2r}}\}.$$

We have that $\#\{a(p^2) \pmod m : p \in S_{a_1}(x)\} < y$, then there exists a_2 such that, $a(p^2) \equiv a_2 \pmod m$ for at least $\frac{\#S_{a_1}(x)}{y} = \frac{x^{\frac{1}{2r}+o(1)}}{y^2}$ many primes up-to $x^{\frac{1}{2r}}$. Let us then consider

$$S_{a_1,a_2}(x) = \{p : a(p^2) \equiv a_2 \pmod m,\ p \in S_{a_1}(x)\}.$$

Since $\{a(p^3) \pmod m : p \in S_{a_1,a_2}(x)\} < y$, there exists a_3 such that $a(p^3) \equiv a_3 \pmod m$ for at least $\frac{\#S_{a_1,a_2}(x)}{y} = \frac{x^{\frac{1}{2r}+o(1)}}{y^3}$ many primes up-to $x^{\frac{1}{2r}}$. Arguing recursively, we obtain

$$a(p) = a_1 \pmod m,\ a(p^2) = a_2 \pmod m, \cdots, a(p^{2r}) = a_{2r} \pmod m,$$

for at least $\frac{x^{\frac{1}{2r}+o(1)}}{y^{2r}}$ many primes up-to $x^{\frac{1}{2r}}$, and we denote this set of primes to be $S_{a_1,a_2,\ldots a_{2r}}(x)$.

Now the characteristic polynomial of the sequence $\{a_i(p^n)\}$ is $x^2 - a_i(p)x + p^{k-1}$, and hence $\{a(p^n)\}$ is a linear recurrence sequence with the characteristic polynomial $p(T) = \prod_{i=1}^{r}(T^2 - a_i(p)T + p^{k-1})$.[1] It follows from Lemma 5.2.5 and Lemma 5.2.6 that, the coefficients of $p(x)$ are polynomials in the prime p, for any $p \in S_{a_1,a_2,\ldots a_{2r}}(x)$. Moreover, the polynomial with the highest degree appears only once, with degree $(k-1)r$. In particular, we get a polynomial $g(T)$ of degree $(k-1)r$, which satisfies

$$g(p) = 0 \pmod m,\ \forall p \in S_{a_1,a_2,\ldots a_{2r}}(x).$$

In particular, $g(p) = 0 \pmod L$ for at least $\frac{x^{\frac{1}{2r}+o(1)}}{y^{2r}}$ many primes p up-to $x^{\frac{1}{2r}} \le L$. The proof now follows, taking $y = x^{\frac{1}{4r^2}-\delta}$ since $g(p) = 0 \pmod L$ for only $O_g(1)$ many $p \le L$. □

5.2.1 Sums with Hecke eigenforms

Let m be any given integer, and f be any Hecke eigenform. We then want to show that $\{a(n) \pmod m\}_{n=m^{O(1)}}$ is an additive basis for $\mathbb{Z}/m\mathbb{Z}$. This was proved by Shparlinski when f is given by the Ramanujan-tau function and m is a prime. For any $\gamma > 0$, let us consider

$$N_\gamma = \{m \in \mathbb{N} \mid \ell \text{ prime divides } m \implies m \le \ell^{1+\gamma}\}.$$

Proposition 5.2.8. *Let ω be any integer, and $\gamma, \beta > 0$ be any real numbers. Take any pairwise disjoint set of primes $S_1, S_2, \cdots, S_\omega$ satisfying*

$$\begin{cases} \#A_1\#A_2\cdots\#A_\omega \ge m^{1+\beta},\ \omega = 2,3 \\ \#A_1\#A_2(\#A_3\cdots\#A_\omega)^{\frac{1}{81}} \ge m^{1+\beta},\ \omega \ge 4. \end{cases} \tag{5.9}$$

[1] For a reference, the reader may look at https://math.stackexchange.com/questions/1348838/sum-and-product-of-linear-recurrences.

where $A_i = \{a(p), a(p^2) \pmod m \mid p \in S_i\}$. *Set* $B_\gamma(\ell) = \{m \in N_\gamma$ *is square-free and* $p \mid m \implies p > \ell\}$. *There exists* ℓ_β *such that*

$$\sum_{i=1}^{s} a(n_i) \equiv a \pmod m$$

is solvable for any integer a, *and*

$$s > \begin{cases} \frac{2}{\beta}, & \omega = 2 \\ \frac{(1+\gamma)(8\log(\frac{8}{\beta})+4)}{\beta}, & \omega = 3, \quad m \in B_\gamma(\ell_\beta) \\ \frac{(1+\gamma)2^\omega}{0.45\beta}, & \omega \geq 4, \qquad\quad m \in B_\gamma(\ell_\beta). \end{cases} \tag{5.10}$$

In either of the cases, any such n_i *has prime factors only from* $S_1, S_2, \cdots, S_\omega$.

Proof. The proof for the case $\omega = 2$ follows from Corollary 5.1.1, since $a(\cdot)$ is multiplicative and S_1, S_2 are disjoint set of primes.

For higher values of ω, we assume that m is squarefree. To prove for $\omega = 3$, note that there exists a prime $\ell \mid m$ such that

$$|A_1^{(\ell)}||A_2^{(\ell)}| \cdots |A_3^{(\ell)}| \geq \ell^{1+\beta},$$

where $A_i^{(\ell)}$ is the ℓ^{th} component of A_i. Arguing similarly as in the proof of Corollary 5.1.4, we get the following from Theorem 5.1.2.

$$\max_{\lambda \in (\mathbb{Z}/m\mathbb{Z})^*} \left| \sum_{a_1 \in A_1} \sum_{a_2 \in A_2} \sum_{a_3 \in A_3} \mathbf{e}_m(\lambda a_1 a_2 a_3) \right| \ll \frac{|A_1||A_2||A_3|}{\ell^{\frac{\beta}{8\log(8/\beta)+4}}}.$$

Now note that there exists ℓ_β such that, the following holds for any $m \in B(\ell_\beta)$,

$$O\left(\left(\frac{|A_1||A_2||A_3|}{\ell^{\frac{\beta}{8\log(8/\beta)+4}}}\right)^s\right) = o\left(\frac{(|A_1||A_2||A_3|)^s}{m}\right),$$

since $s\beta > (8\log(8/\beta)+4)(1+\gamma)$ by the assumption. The result follows this case from the formula at (5.3).

For a proof of $\omega \geq 4$,, we follow the same argument as is the previous case and use Corollary 5.1.4 and (5.3).

□

5.2.2 Sums with a larger class

Let us now consider a modular form f with rational coefficients of the form $c_1 f_1 + c_2 f_2 + \cdots + c_r f_r$, where $c_i \in Q$, and f_i are all Hecke eigenforms with rational coefficients. More generally, one can also consider a new sequence $a(n) := P(a_1(n), a_2(n), \cdots, a_r(n))$ for any homogeneous polynomial $P(x_1, x_2, \cdots, x_r)$ with

rational coefficients. The first problem we immediately encounter is that $a(\cdot)$ is not necessarily multiplicative unless $P(\cdot)$ is a monomial. Even in the case of a monomial, to get an analogous result to Proposition 5.2.8, we need to ensure that

$$\#A_1\#A_2\cdots\#A_\omega \geq m^{1+\beta},$$

where

$$A_i = \left\{P(a_1(p),\cdots,a_r(p)),\ P(a_1(p^2),\cdots,a_r(p^2)) \pmod m \mid p\in S_i\right\},$$

for some set of primes S_i. This is easy if P is of the form x_i^e for some i. In general, we have a somewhat weaker result, which shall be discussed in this section. For any r-tuple of signs $\vec{\sigma}$, let us consider

$$\mathcal{S}_{\vec{\sigma},\vec{f},m} = \left\{p \mid \sigma_1 a_1(p) = \cdots = \sigma_r a_r(p) \pmod m,\ p^{k-1}=1 \pmod m\right\},$$

and $\mathcal{S}_{\vec{\text{sign}},\vec{f},m} = \bigcup_{\vec{\sigma}\in\{\pm1\}^r}\mathcal{S}_{\vec{\sigma},\vec{f},m}$. We then have the following.

Corollary 5.2.9. *Let m,ω,γ and $\beta>0$ be as in Proposition 5.2.8. Take any pairwise disjoint set of primes $S_1,S_2,\cdots,S_\omega$ satisfying*

$$\begin{cases}\#A_1\#A_2\cdots\#A_\omega \geq m^{1+\beta}, \omega = 2,3\\ \#A_1\#A_2(\#A_3\cdots\#A_\omega)^{\frac{1}{81}} \geq m^{1+\beta}, \omega\geq 4.\end{cases} \tag{5.11}$$

where $A_i = \{a(p), a(p^2) \pmod m \mid p\in S_i\cap\mathcal{S}_{\vec{\text{sign}},\vec{f},m}\}$. Suppose that $(P(\vec{\sigma}),m)=1$ for any $\vec{\sigma}\in\{\pm1\}^r$. Then there exists $\beta'>0$ (depending on β) such that for $\omega=2$, 3 and $\omega\geq4$ respectively, and for $s>\frac{2}{\beta'}$, $\frac{(1+\gamma)8\log(8/\beta)+4}{\beta'}$, and $\frac{(1+\gamma)2^\omega}{0.45\beta'}$, any $a\in\mathbb{Z}$ can be written as

$$a(n_1)+a(n_2)+\ldots+a(n_s)\equiv a \pmod m,\ n_i\in\mathbb{N},\ i=1,2,\cdots,s,$$

for any sufficiently large m. Moreover any such n_i has prime factors only from $S_1,S_2,\cdots,S_\omega$.

Proof. Note that for any $p\in\mathcal{S}_{\vec{\text{sign}},\vec{f},m}$, we have

$$a_i(p^2)=a_j(p^2),\ \forall\ 1\leq i,j\leq r.$$

In particular, for any such prime p,

$$a(p)=P(\vec{\sigma})a_1(p)^d,\ a(p^2)=P(1,1,\cdots,1)a_1(p^2)^d,$$

for some $\vec{\sigma}\in\{\pm1\}^r$ and d is the degree of P. Since $\#A_1\#A_2\cdots\#A_\omega\geq m^{1+\beta}$, for a particular type of sign-tuple $\vec{\sigma}:=(\sigma_1,\sigma_2,\cdots,\sigma_r)$, we have

$$\#A_1'\#A_2'\cdots\#A_\omega' \geq \frac{m^{1+\beta}}{2^r},\ \omega=2,3$$

$$\#A_1'\#A_2'(\#A_3'\cdots\#A_\omega')^{\frac{1}{81}} \geq \frac{m^{1+\beta}}{2^r},\ \omega\geq4,$$

where $A_i' = \{a(p),\ a(p^2) \pmod m \mid p\in S_i\cap\mathcal{S}_{\vec{\sigma},\vec{f},m}\}$. The proof now follows from Proposition 5.2.8, for any β' and sufficiently large m satisfying $m^{\beta-\beta'}\geq 2^r$. □

5.3 Proof of the main results

To prove Theorem 5.3.1, we need an explicit value of β in (5.9). We shall obtain this by the known explicit bounds for the sum-product problems over finite fields. For instance, suppose that $m := \ell$ is a prime and $A \subset \mathbb{F}_\ell$ is a small set. Then the problem is to find $\beta > 0$ for which

$$\max\{|A + A|, |A \cdot A|\} \gg |A|^{1+\beta}.$$

Garaev in [39] showed that β could be taken to be $1/14$, then Rudnev in [76] improved it to $1/11$ and the most optimal β, according to the best of our knowledge is given by $1/5$. This is a result of Roche-Newton, Shkredov, and Rudnev in [75].

Let us now state and prove the main results of this chapter.

Theorem 5.3.1 (Bhakta, Krishnamoorthy, Muneeswaran)**.** *Let $f(z)$ be any cusp-form, and S_1, S_2 be any set of primes having positive density with $S_1 \cap S_2 = \phi$. Then there exists an integer N_{S_1,S_2} such that for any integer m with all prime factors larger than N_{S_1,S_2}, and $L^{1/77} \geq m/L$, where L is the largest prime factor of m, we have the following.*

(i) If $f(z)$ is a Hecke eigenform then for any $a \in \mathbb{Z}/m\mathbb{Z}$, we can write

$$\sum_{i=1}^{s} a(n_i) \equiv a \pmod{m},\ n_i \leq m^{130/33},\ \forall 1 \leq i \leq s,$$

for some $s \leq 52$. Furthermore, all the prime factors of any such n_i are bounded by $O(m^{65/66})$, and they belong to $S_1 \cup S_2$. Additionally, each n_i has at least one prime factor from both S_1 and S_2.

(ii) In general if $f(z)$ is of the form $\sum_{i=1}^{r} c_i f_i,\ c_i \in \mathbb{Q}, f_i$ are newforms without CM and $\sum \sigma_i c_i \not\equiv 0 \pmod{m}, \sigma_i \in \{\pm 1\}$. If none of the associated Galois representations $\rho_{f_{i_1}, f_{i_2} \cdots, f_{i_s}, m}$ does not have image $\Delta_k^{(s)}(m)$ for any subset $I = \{i_1, i_2, \cdots, i_s\}$ of $\{1, 2, \cdots, r\}$ with $\#I \geq 2$. Then for any $a \in \mathbb{Z}/m\mathbb{Z}$, we can write

$$\sum_{i=1}^{s} a(n_i) \equiv a \pmod{m},\ n_i \leq m^{130/33},\ \forall 1 \leq i \leq s,$$

for some $s \leq 52$. Moreover, all the prime factors of any such n_i are $O(m^{65/66})$, and are in $S_1 \cup S_2$. In addition, each n_i has at least one prime factor from both S_1 and S_2.

Proof of Theorem 5.3.1. For proof of part (i), we take $\varepsilon = 65/66$ in Lemma 5.2.1 and obtain that $\#\{a(p) \pmod{L},\ p \in S_1, p \leq m^{65/66}\}$ or $\#\{a(p^2) \pmod{L},\ p \in S_1, p \leq m^{65/66}\} \gg m^{65/132+o(1)} \geq L^{65/132+o(1)}$. Consider the set with a larger size and set it as A_1. Similarly, $\#\{a(p) \pmod{L},\ p \in S_2, p \leq m^{65/66}\}$ or $\#\{a(p^2) \pmod{L},\ p \in S_2, p \leq m^{65/66}\} \gg m^{65/132+o(1)} \geq L^{65/132+o(1)}$, and denote the larger

one as A_2. Now we use [75, Theorem 6] to both of the sets A_1 and A_2. We have set A_1', which is one of the $A_1 \cdot A_1$ or $A_1 + A_1$, and a set A_2', which is one of the $A_2 \cdot A_2$ or $A_2 + A_2$, satisfying that

$$\#A_1' \gg L^{13/22+o(1)},\ A_2' \gg L^{13/22+o(1)},$$

when L is sufficiently large say $L^{1/77} \geq L'$. Where $L' = \frac{m}{L}$ with $(L, L') = 1$. We have

$$\#A_1'.\ \#A_2' \gg L^{13/11+o(1)} \geq (LL')^{14/12} = m^{1+2/12}$$

On the other hand, realizing A_1' and A_2' as subsets of $\mathbb{Z}/m\mathbb{Z}$ under the natural inclusion $\mathbb{Z}/L\mathbb{Z} \hookrightarrow \mathbb{Z}/m\mathbb{Z}$, the proof now follows from Corollary 5.1.1 for any $s > 12$. This is because any element in $A_1' \cdot A_2'$ is of the form $a(n_1) + a(n_2) + a(n_3) + a(n_4)$, with $n_1, n_2, n_3, n_4 \leq m^{130/33}$, each n_i has at least one prime factor from S_1, and at least one prime factor from S_2.

Now for a proof of part (ii), it follows from Lemma 4.1.5 that all any two f_i, f_j differ by a quadratic character. In particular, the result now follows the same argument as in the proof of Corollary 5.2.9 by taking $d = 1$ and $P = \sum c_i x_i$. □

Theorem 5.3.2 (Bhakta, Krishnamoorthy, Muneeswaran)**.** *Let $f(z)$ be any cusp-form with rational coefficients, $0 < \varepsilon, \gamma < 1$ be any given real numbers, m be a square-free positive integer and $S_1, S_2, \cdots, S_\omega$ be any set of primes of positive density, with $\varepsilon(2 + \frac{\omega-2}{81}) > 2(\gamma + 1)$ and $S_i \cap S_j = \phi,\ i \neq j$. Then there exists an integer $N_{S_1,S_2,\cdots,S_\omega,\varepsilon}$ such that for any integer m with all the prime factors of m are larger than $N_{S_1,S_2,\cdots,S_\omega,\varepsilon}$, $m^{\varepsilon/2} = o(L)$ and $L^\gamma \geq m/L$ for some $\gamma > 0$, we have the following.*

(a) If $f(z)$ is a Hecke eigenform then for any $a \in \mathbb{Z}/m\mathbb{Z}$, we can write

$$\sum_{i=1}^{s} a(n_i) \equiv a \pmod{m},\ n_i \leq m^{2\varepsilon\omega},\ \forall 1 \leq i \leq s,$$

for some computable s depending on $\varepsilon, \omega, \gamma$. Moreover, all the prime factors of any such n_i are less than or equal to m^ε and in $\bigcup_{i=1}^{\omega} S_i$.

(b) In general if $f(z)$ of the form $\sum_{i=1}^{r} c_i f_i, c_i \in \mathbb{Q},\ f_i$ are newforms without CM and $\sum \sigma_i c_i \not\equiv 0 \pmod{m}, \sigma_i \in \{\pm 1\}$. If the associated Galois representation $\rho_{f_1,f_2\cdots,f_r,m}$ does not have image $\Delta_k^{(r)}(m)$, then for any $a \in \mathbb{Z}/m\mathbb{Z}$, we can write

$$\sum_{i=1}^{s} a(n_i) \equiv a \pmod{\ell},\ n_i \leq m^{2\varepsilon\omega},\ \forall 1 \leq i \leq s,$$

for the same s as in (a). Moreover, all the prime factors of any such n_i are less than or equal to m^ε and in $\bigcup_{i=1}^{\omega} S_i$.

Proof of Theorem 5.3.2. Let us first prove (i). Take $\varepsilon > 0$ be any given real, and $S_1, S_2, \cdots, S_\omega$ be any pairwise disjoint set of primes of positive density, with $\varepsilon(1 + \frac{\omega-2}{81}) > 2$. We studied the case $\omega = 2$ in Theorem 5.3.1. The proof for $\omega > 2$ case follows a similar path. It follows from Lemma 5.2.1 that for each $1 \leq i \leq \omega$, we have $\#\{a(p) \pmod L,\ p \in S_i, p \leq m^\varepsilon\}$ or $\#\{a(p^2) \pmod L,\ p \in S_i, p \leq m^\varepsilon\} \gg L^{\varepsilon/2+o(1)}$. Denote A_i to be one of the corresponding sets with larger cardinality, we have

$$\#A_1\#A_2(\prod_{3\leq i\leq\omega} \#A_i)^{1/81} \gg L^{\varepsilon(2+\frac{\omega-2}{81})/2+o(1)}.$$

Denoting $\beta = \varepsilon(2 + \frac{\omega-2}{81})/2 + o(1) - 1$ (which is positive by the assumption on ω) and writing $m = LL'$ with $(L, L') = 1$, we have

$$L^{1+\beta} \geq m^{1+\beta'},$$

for any β' satisfying $L^{\frac{\beta-\beta'}{1+\beta'}} > m/L$. The result now follows from Proposition 5.2.8 for $s = \frac{2^\omega}{0.45\beta'}$, where $\beta' = \frac{\beta-\gamma}{\gamma+1}$.

Proceeding similar to the proof of part (ii) of the previous proof, we get the part (ii) of this theorem. □

Remark 5.3.3. We now list the explicit values in the following table, obtained from Theorem 8.0.6.

ω	ϵ	γ	s
21	0.9	0.005	2^{31}
165	0.5	0.003	2^{180}
1461	0.1	0.0006	2^{1478}
16041	0.1	0.00006	2^{16062}
161841	0.001	0.000006	2^{161866}
1619841	0.0001	0.0000006	$2^{1619894}$
16199841	0.00001	0.00000006	$2^{16199872}$
161999841	0.000001	0.000000006	$2^{161999875}$

Table 1: Required number of terms for a given bound

5.4 Further questions and remarks

5.4.1 Solution with primes

We are having some assumptions on the composite number m in both Theorem 3.2 and Theorem 8.0.6. We would like to see if it is possible to remove them. We also ask if it is possible to obtain a solution to the equation

$$\sum_{i=1}^{O(1)} a(p_i) \equiv a \pmod m,\ p_i \leq m^{O(1)},$$

where each p_i is a prime. Or at least, if $\{a(n) \pmod m\}_{\substack{\omega(n)=1 \\ n\leq m^{O(1)}}}$ is an additive basis for $\mathbb{Z}/m\mathbb{Z}$. Recall that Bajpai, García, and the first author studied this in [10]; however, their method does not give polynomial growth of the solutions. Note that we have obtained solutions with polynomial growth and ω many prime factors for certain m.

5.4.2 Sum of the polynomial values

Following the arguments in Section 5.2 one can study solvability of the equation $\sum_{i=1}^{O(1)} a(n_i)^d \equiv a \pmod m$, as remarked by Shparlinski in [85]. However, Proposition 5.2.7 is giving the hope that it is also possible to study $\sum_{i=1}^{O(1)} p(a(n_i)) \equiv a \pmod m$, for any polynomial $p(x) \in \mathbb{Q}[x]$. The only obstacle is that $p(f(n))$ may not be multiplicative for any multiplicative function $f(n)$. We also ask if there is a way to overcome this. Perhaps the most interesting situation is when P is of degree 1. In that case, $a(n) := P(a_1(n), a_2(n), \cdots, a_r(n))$ is Fourier coefficient of some modular form.

5.4.3 On a larger family of cuspforms

We expect that it is possible to work with a larger class of cuspforms in Proposition 5.2.7, at least when m is a prime ℓ. We covered some other families in Corollary 5.2.3. In this section, we shall discuss our heuristics for extending these families. This is because we expect the following to hold, under some suitable conditions, perhaps.

Question 5.4.1. *Let ℓ be any prime, and L be its any power. Is it true that for any tuples $(c_i)_{1\leq i\leq r} \in \mathbb{F}_L^r$, $(a_i)_{1\leq i\leq r+1} \in \mathbb{F}_L^{r+1}$, the number of solutions to the equations*

$$c_1x_1^i + c_2x_2^i + \cdots c_rx_r^i = a_i, \ \forall 1 \leq i \leq r+1,$$

is at most $O_r(1)$?

For instance, this is easily seen to be true when all the c_i are the same, using Newton's identity. In general, we have a partial answer due to the following.

Lemma 5.4.2. *Let ℓ be any prime, and L be its any power. For any $(c_1, c_2, \cdots, c_r) \in \mathbb{F}_L^r$, consider $f_i = c_1x_1^i + c_2x^i \cdots c_rx_r^i \in \mathbb{F}_L[x_1, x_2, \cdots x_r]$, and V be the projective variety generated by $f_1, f_2, \cdots, f_r$. Then $\dim(V) = 0$ provided that $\sum_{i\in S} c_i \neq 0$ in $\mathbb{F}_\ell$ for any $S \subseteq \{1, 2, \cdots, r\}$.*

Proof. It is enough to prove that there is no non-trivial prime ideal I in the coordinate ring of V. Suppose there is such a non-trivial prime ideal I. It follows from the identity $f_r = \sum_{i=1}^{r} q_i f_{r-i}$ that $(\sum_{i=1}^{r} c_i)x_1x_2\cdots x_r$ in I, where q_i is i^{th} elementary symmetric polynomial in $x_1, x_2, \cdots, x_r$. Since $\sum_{i=1}^{r} c_i \neq 0$, we may assume that $x_r \in I$. Then repeating the same argument, and keeping in mind that any sum $\sum_{i\in S} c_i \neq 0$, we have that $x_1, x_2, \cdots, x_r$ all are in I. In particular, this shows that,

$$I = (f_1, f_2, \cdots, f_r) = (x_1, x_2, \cdots, x_r),$$

which completes the proof. □

Remark 5.4.3. The condition $\sum\limits_{i\in S} c_i \neq 0$ is important. For instance, $\sum\limits_{1\leq i\leq r} c_i = 0$, implies that V contains the variety $(x_1 - x_r, x_2 - x_r, \cdots x_{r-1} - x_r)$. In particular, V is of dimension at least 1.

As a consequence of Lemma 5.4.2, we have a positive answer to Question 5.4.1 when all the a_i are equal. For proof, one may use [61, Theorem 2.1]. We shall now see how helpful it is to have a complete answer to Question 5.4.1. Let $f_1, f_2, \cdots, f_r$ be any set of Hecke eigenforms and set

$$a_{P,\vec{f}}(n) = P(a_1(n), a_2(n), \cdots, a_r(n)),$$

where $P(x_1, x_2, \cdots, x_r)$ is a polynomial with r number of varriables.

Corollary 5.4.4. *Let ℓ be any given prime, then for any set of primes S, consider quantity,*

$$N_{S,P,\vec{f}}(x) = \#\{a_{P,\vec{f}}(n) \pmod{\ell} \mid p \text{ divides } n \implies p \in S,\ n \leq x\}.$$

Suppose that S has positive density, then we have the following estimate for any sufficiently large prime ℓ, and any $\delta > 0$

$$N_{S,P,\vec{f}}(x) \geq \min\left\{\ell^{\frac{1}{2}-\delta}, x^{\frac{1}{4r^2}-\delta}\right\}.$$

Proof. Let us start with writing $a_i(p^n) \pmod{\ell} = c_i\alpha_i^n + d_i\beta_i^n$, where $\alpha_i, \beta_i \in \mathbb{F}_{\ell^2}$, and suppose that P is a homogeneous polynomial of degree d. Then $a_f(p^n)$ is a linear combination of $\left\{\prod_{i=1}^{r} \alpha_i^{nt_i}\beta_i^{n(d_i-t_i)}\right\}_{\substack{0\leq t_i\leq d_i \\ \sum d_i = d}}$. Let $\vec{d} = (d_1, d_2, \cdots, d_r)$ appear as degrees of a monomial in P. For a fixed tuple $(a_1, a_2, \cdots, a_{r+1}) \in \mathbb{F}_\ell^{r+1}$, let us now consider the number of primes p for which

$$(a_{P,\vec{f}}(p), a_{P,\vec{f}}(p^2)\cdots, a_{P,\vec{f}}(p^{r+1})) \pmod{\ell} = (a_1, a_2, \cdots, a_{r+1}).$$

It follows from our expectation in Question 5.4.1 that, $\left\{\prod_{i=1}^{r} \alpha_i^{t_i}\beta_i^{d_i-t_i}\right\}_{\substack{0\leq t_i\leq d_i \\ \sum d_i = d}}$, is $O(1)$. In particular,

$$\prod_{\sum d_i = d} \prod_{i=1}^{r} \prod_{0\leq t_i\leq d_i} \alpha_i^{t_i}\beta_i^{d_i-t_i} = O(1).$$

Recall that $\alpha_i\beta_i = p^{k_i-1} \pmod{\ell}$, and hence

$$\prod_{\sum d_i=d}\prod_{i=1}^{r}\prod_{0\leq t_i\leq d_i}\alpha_i^{t_i}\beta_i^{d_i-t_i} = \prod_{\sum d_i=d}\prod_{i=1}^{r-1}p^{(k_i-1)\frac{d_i(d_i+1)}{2}} \pmod{\ell} = O(1).$$

This is impossible since S is infinite, and any $k_i - 1$ is strictly positive. In particular, this shows that the number of primes p for which

$$(a_{P,\bar{f}}(p), a_{P,\bar{f}}(p^2)\cdots, a_{P,\bar{f}}(p^{r+1})) \pmod{\ell} = (a_1, a_2, \cdots, a_{r+1})$$

is $O(1)$. The proof now follows, arguing similarly as in the proof of Proposition 5.2.7 □

Chapter 6

Admissible Vector-valued automorphic forms and growth

6.1 Fuchsian groups

A Fuchsian group is a discrete subgroup G of $\mathrm{PSL}_2(\mathbb{R})$ for which $\mathrm{G}\backslash\mathbb{H}$ is topologically a Riemann surface with finitely many punctures. For a quick exposition on the theory of Fuchsian groups, we refer the reader to [81, 96]. A group G in $\mathrm{PSL}_2(\mathbb{R})$ is called discrete, if G is a discrete subgroup of $\mathrm{PSL}_2(\mathbb{R})$ with respect to the induced topology of $\mathrm{PSL}_2(\mathbb{R})$. More explicitly, to define the discreteness of a subgroup G of $\mathrm{PSL}_2(\mathbb{R})$, we mean:
given any matrix $A \in \mathrm{G}$*, there is an* $\epsilon_A > 0$ *such that all the matrices* $B(\neq A)$ *in* G *have* $\mathrm{dist}(A, B) > \epsilon_A$*, where*

$$\mathrm{dist}(A, B) = \min\left\{ \sum_{i,j} \mid A_{ij} - B_{ij} \mid, \sum_{i,j} \mid A_{ij} + B_{ij} \mid \right\}.$$

The action of any subgroup of $\mathrm{SL}_2(\mathbb{R})$ on $\mathbb{H}$ is the Möbius action, defined by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \tau = \frac{a\tau + b}{c\tau + d}.$$

Define $\mathbb{H}^* = \mathbb{H} \cup \mathbb{R} \cup \{\infty\}$ to be the extended upper half plane of $\mathrm{PSL}_2(\mathbb{R})$ and this action can be extended to $\mathbb{H}^*$. For any $\gamma = \pm \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{PSL}_2(\mathbb{R})$, the action of γ on ∞ is defined as follows:

$$\gamma \cdot \infty = \lim_{\tau \mapsto \infty} \frac{a\tau + b}{c\tau + d} = \frac{a}{c} \in \mathbb{R} \cup \{\infty\}, \tag{6.1}$$

and for any $x \in \mathbb{R}$, the action is defined similarly by taking the limit $\tau \mapsto x$ in (6.1).

An element $\gamma \in \mathrm{PSL}_2(\mathbb{R})$ is called parabolic, if the absolute value of the trace of γ is equal to 2. A point $\tau \in \mathbb{H}^*$ is said to be a fixed point of $\gamma \in \mathrm{PSL}_2(\mathbb{R})$ if

$\gamma \cdot \tau = \tau$. If $\gamma = \pm \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ is a parabolic element then its fixed point $\tau = \frac{a \mp 1}{c}$ when $a + d = \pm 2$ and $c \neq 0$, in addition $\tau = \infty$ when $c = 0$.

Note 6.1.1. $\mathrm{PSL}_2(\mathbb{R})$ acts on $\mathbb{R} \cup \{\infty\}$. Note that in $\mathbb{H}^*$, there is only one notion of ∞ usually denoted by $i\infty$, but for notational convenience, it will be written ∞. Following (6.1), for any $x \in \mathbb{R}$ it is observed that there exists an element $\gamma = \pm \left(\begin{smallmatrix} x & -1 \\ 1 & 0 \end{smallmatrix}\right)$ such that $\gamma \cdot \infty = x$ which means $\mathrm{PSL}_2(\mathbb{R})$ acts transitively on $\mathbb{R} \cup \{\infty\}$. For any $x \in \mathbb{R}$, such γ is denoted by A_x.

Definition 6.1.2. Let G be a subgroup of $\mathrm{PSL}_2(\mathbb{R})$. A point $\mathfrak{c} \in \mathbb{R} \cup \{\infty\}$ is called a cusp of G if it is fixed by some non-trivial parabolic element of G. Let $\mathfrak{C}_\mathrm{G}$ denote the set of all cusps of G and we define $\mathbb{H}^*_\mathrm{G} = \mathbb{H} \cup \mathfrak{C}_\mathrm{G}$ to be the extended upper half plane of G.

For example: if $\mathrm{G} = \mathrm{PSL}_2(\mathbb{R})$ then $\mathfrak{C}_\mathrm{G} = \mathbb{R} \cup \{\infty\}$ and if $\mathrm{G} = \mathrm{PSL}_2(\mathbb{Z})$ then $\mathfrak{C}_\mathrm{G} = \mathbb{Q} \cup \{\infty\}$ consists of the G-orbit of cusp ∞. For any $\tau \in \mathbb{H}^*_\mathrm{G}$, let $\mathrm{G}_\tau = \{\gamma \in \mathrm{G} | \gamma \cdot \tau = \tau\}$ be the stabilizer subgroup of τ in G. For any $\mathfrak{c} \in \mathfrak{C}_\mathrm{G}$, $\mathrm{G}_\mathfrak{c}$ is an infinite order cyclic subgroup of G. If $\mathfrak{c} = \infty$ then G_∞ is generated by $t_\infty = \pm \left(\begin{smallmatrix} 1 & h_\infty \\ 0 & 1 \end{smallmatrix}\right) = t^{h_\infty}$ for a unique real number $h_\infty > 0$ called the cusp width of the cusp ∞. In case of $\mathfrak{c} \neq \infty$, $\mathrm{G}_\mathfrak{c}$ is generated by $t_\mathfrak{c} = A_\mathfrak{c} t^{h_\mathfrak{c}} A_\mathfrak{c}^{-1}$ for some smallest real number $h_\mathfrak{c} > 0$, called the cusp width of the cusp $\mathfrak{c}$ such that $t_\mathfrak{c} \in \mathrm{G}$ where $A_\mathfrak{c} = \pm \left(\begin{smallmatrix} \mathfrak{c} & -1 \\ 1 & 0 \end{smallmatrix}\right) \in \mathrm{PSL}_2(\mathbb{R})$ so that $A_\mathfrak{c}(\infty) = \mathfrak{c}$, as defined in the Note 6.1.1. From now on, for convenience, h_∞ will be denoted by h. For every $\mathfrak{c} \in \mathfrak{C}_\mathrm{G} \backslash \{\infty\}$, the elements of $\mathrm{G}_\mathfrak{c}$ depend on $\mathfrak{c}$. Since $\mathfrak{c} \in \mathbb{R} \cup \{\infty\}$, there are two possibilities: $\mathfrak{c} \in \mathbb{R}$ or $\mathfrak{c} = \infty$. Consider $\mathfrak{c} \in \mathbb{R}$ and let γ be any element in $\mathrm{G}_\mathfrak{c}$ then $\gamma = (t_\mathfrak{c})^r$ for some integer r, that is, $\gamma = A_\mathfrak{c}(t^{h_\mathfrak{c}})^r A_\mathfrak{c}^{-1}$.

6.1.1 Fuchsian groups of the first kind

The class of all Fuchsian groups is divided into two categories, namely Fuchsian groups of the first and of the second kind. A fundamental domain of Fuchsian groups is defined to distinguish between them and will be denoted by F_G. It exists for any discrete group G acting on $\mathbb{H}$ and is defined as follows.

Definition 6.1.3. Let G be any discrete subgroup of $\mathrm{PSL}_2(\mathbb{R})$. Then a domain (connected open set) F_G in $\mathbb{H}$ is called the fundamental domain of G, if

- no two elements of F_G are equivalent with respect to G,
- any point in $\mathbb{H}$ is equivalent to a point in the closure of F_G in $\mathbb{H}$ with respect to G, that is, any G-orbit in $\mathbb{H}$ intersects with the closure of F_G.

The hyperbolic area of F_G may be finite or infinite. When F_G has finite area then such G is a Fuchsian group of the first kind otherwise of the second kind. A Fuchsian group of the first kind with at least one cusp is often called as non-cocompact Fuchsian group of the first kind. In this article, we are mainly concerned with non-cocompact Fuchsian groups of the first kind. A Fuchsian group G will

have several different fundamental domains but it can be observed that their area will always be the same. Let us write $\widetilde{\mathrm{F}}_{\mathrm{G}}$ and $\widehat{\mathrm{F}}_{\mathrm{G}}$ to denote the closure of the fundamental domain F_{G} in $\mathbb{H}$ and $\mathbb{H}^*_{\mathrm{G}}$ respectively. From F_{G} a (topological) surface Σ_{G} is obtained by identifying the closure $\widehat{\mathrm{F}}_{\mathrm{G}}$ of F_{G} in $\mathbb{H}^*_{\mathrm{G}}$ using the action of G on $\widehat{\mathrm{F}}_{\mathrm{G}}$, i.e. $\Sigma_{\mathrm{G}} = \widehat{\mathrm{F}}_{\mathrm{G}}/\sim$ (equivalently $\Sigma_{\mathrm{G}} = \mathrm{G}\backslash\mathbb{H}^*_{\mathrm{G}}$).

6.1.2 Structure of words in Fuchsian groups

We say that a word in a Fuchsian group is an element of the form $C_1C_2\cdots C_s$, where each $C_i \in \mathrm{G}$. A theorem of Eichler [30, Satz 1] asserts that there exists a finite set $\mathrm{G}_{\mathrm{Eichler}} \subset \mathrm{G}$ such that any γ in G equals to a product $C_1C_2\ldots C_L$ for some $C_1, C_2\ldots, C_L$ so that L is bounded by a linear function of order $\log\|\gamma\|$ and each C_i either belongs to $\mathrm{G}_{\mathrm{Eichler}}$ or is a power of a parabolic element of $\mathrm{G}_{\mathrm{Eichler}}$. However, this result will not be sufficient for our purposes because we need to control the powers of parabolic elements appearing in the Eichler's decomposition.

Similarly, Beardon [12] gave a decomposition where each C_i is written as a product of elements from a geometrically chosen set of generators. Following Beardon's notations, the number of such elements coming in the product is denoted by $|C_i|$. These generators, say G^*, are precisely the side pairings of a convex fundamental domain. Let D_{G} be such a convex fundamental domain of G. We need to understand these C_i's in more details for the work in Section 7.2. It is known that $\widehat{\mathrm{D}}_{\mathrm{G}}$ has finitely many vertices. We say that two vertices v_1, v_2 of $\widehat{\mathrm{D}}_{\mathrm{G}}$ are equivalent, if and only if they differ by an element of G, and denoted by $v_1 \sim v_2$. We call a vertex as parabolic vertex (cusp), if it is a fixed point of a parabolic element of G. It is known that the stabilizer of any parabolic vertex is an infinite cyclic group.

Lemma 6.1.4. *There exists a constant c (possibly depending on G) and a finite subset G_0 of G such that any $C_i \in \mathrm{G}$ with $|C_i| > c$, can be written as a product of a parabolic element with an element of G_0. Here the parabolic element is of the form $t^n_{\mathfrak{c}}$, for some cusp $\mathfrak{c} \in \mathrm{G}$, and integer n.*

Proof. It follows from Theorem 3 of [12] that there exists a constant c (possibly depending on G) such that any $C_i \in \mathrm{G}$ with $|C_i| > c$ can be written as $A_{n_i+1}\cdots A_{n_{i+1}}$ such that

$$\widehat{\mathrm{D}}_{\mathrm{G}}, A_{n_i+1}\widehat{\mathrm{D}}_{\mathrm{G}}, \ldots, A_{n_i+1}\cdots A_{n_{i+1}}\widehat{\mathrm{D}}_{\mathrm{G}}$$

share a common parabolic vertex, say v. Therefore, we get a sequence of vertices $\{v_j\}_{1\le j\le n_{i+1}-n_i}$ in $\widehat{\mathrm{D}}_{\mathrm{G}}$ such that

$$A_{n_i+1}A_{n_i+2}\cdots A_{n_i+j}(v_j) = v,\ \forall\ 1 \le j \le n_{i+1} - n_i.$$

For each pair (v_1, v_2) of equivalent vertices, we fix an element $C_{v_1,v_2} \in \mathrm{G}$ which takes v_1 to v_2. We then have

$$A_{n_i+1}A_{n_i+2}\cdots A_{n_{i+1}}C_{v,v_{n_{i+1}-n_i}}(v) = v.$$

In particular, we can write $A_{n_i+1}A_{n_i+2}\cdots A_{n_{i+1}}C_{v,v_{n_{i+1}-n_i}} = P_v^k$, where P_v is the parabolic element in G^* fixing v. This is because, the stabilizer subgroup (in G)

of any parabolic vertex is a cyclic group. The proof is now complete because $\{C_{(v_1,v_2)} \mid v_1 \sim v_2\}$ is a finite set. Moreover, this parabolic element P_v is a power of $t_{\mathfrak{c}}$ for some cusp $\mathfrak{c}$, because the parabolic vertex v is a cusp by definition. □

6.2 Vector-valued automorphic forms

This section reviews the basics of vector-valued automorphic forms that we need to understand and prove Theorem 1.3.1 and Theorem 1.3.2. Rather recently, the theory of vector-valued modular forms for the modular group has witnessed a fair amount of their development and interest, see the references mentioned in [7]. Hence, a few resources could be used to review the fundamental concepts of vector-valued automorphic forms. However, our treatment of vector-valued automorphic forms in this section closely follows [6, 7, 38, 51, 54].

Let $j : \mathrm{PSL}_2(\mathbb{R}) \times \mathbb{C} \to \mathbb{C}$ be the function such that for every $\gamma = \pm \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ in $\mathrm{PSL}_2(\mathbb{R})$ and $\tau \in \mathbb{C}$, $j(\gamma, \tau) = c\tau + d$, and satisfies the property $j(\gamma_1\gamma_2, \tau) = j(\gamma_1, \gamma_2\tau)j(\gamma_2, \tau)$ for every $\gamma_1, \gamma_2 \in \mathrm{G}$ and $\tau \in \mathbb{C}$ such that $\gamma_2\tau \neq \infty$.

Definition 6.2.1. If $\mathbb{X} : \mathbb{H} \to \mathbb{C}^m$ is a vector-valued holomorphic function, $\gamma \in \mathrm{PSL}_2(\mathbb{R})$ and k is an even integer, we define a vector-valued holomorphic function $\mathbb{X}|_k\gamma$ on $\mathbb{H}$ by setting $\mathbb{X}|_k\gamma(\tau) = j(\gamma, \tau)^{-k}\mathbb{X}(\gamma\tau)$.

It is easy to check that $\mathbb{X}|_k\gamma_1|_k\gamma_2 = \mathbb{X}|_k(\gamma_1\gamma_2)$, so the stroke operator induces a right group action on the space of vector-valued holomorphic functions on $\mathbb{H}$. Moreover, if $T \in \mathrm{GL}_m(\mathbb{C})$, then $T(\mathbb{X}|_k\gamma) = (T\mathbb{X})|_k\gamma$. This plays an important role in our article, as it allows us to relate the behaviors of the automorphic forms when we move from one cusp to another.

Definition 6.2.2. Let $\mathbb{X} : \mathbb{H} \to \mathbb{C}^m$ be a vector-valued holomorphic function. Then, we say that:

- $\mathbb{X}(\tau)$ has *moderate growth at* ∞ when there exist $\nu \in \mathbb{R}$ and $Y > 0$ such that $\|\mathbb{X}(\tau)\| \leq \exp(\nu y)$ when $y > Y$. Recall that we are denoting $y = \mathrm{Im}\tau$, and
- $\mathbb{X}(\tau)$ has *moderate growth at* $\mathfrak{c} \in \mathbb{R}$ with respect to $k \in 2\mathbb{Z}$ when $\mathbb{X}|_k A_{\mathfrak{c}}$ has moderate growth at ∞.

Remark 6.2.3. If $\mathbb{X}(\tau)$ has moderate growth at $\mathfrak{c}$ with respect to k and $\gamma \in \mathrm{PSL}_2(\mathbb{R})$ sends ∞ to $\mathfrak{c}$, then $\mathbb{X}|_k\gamma$ also has moderate growth at ∞. This can be shown by using the equality $\mathbb{X}|_k\gamma = \mathbb{X}|_k A_{\mathfrak{c}}|_k A_{\mathfrak{c}}^{-1}\gamma$ and the fact that $A_{\mathfrak{c}}^{-1}\gamma$ fixes ∞, and it is of the form $\left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right)$.

We now define a vector-valued automorphic form (vvaf) with respect to admissible representation $\rho : \mathrm{G} \to \mathrm{GL}_m(\mathbb{C})$.

Definition 6.2.4. Let $\rho : \mathrm{G} \to \mathrm{GL}_m(\mathbb{C})$ be a representation. We say that ρ is an *admissible representation* of G if $\rho(\gamma)$ is diagonalizable for every parabolic element $\gamma \in \mathrm{G}$. Otherwise, we say that ρ is a *logarithmic representation* .

Remark 6.2.5. For non-trivial vector-valued automorphic form associated to admissible representation, the moderate growth is same as saying that $\mathbb{X}$ is meromorphic at ∞. If all the components of any such $\mathbb{X}$ are non-zero, then we must have that all the eigenvalues of $\rho(t_\infty)$ are unitary. This is because: without loss of generality, assume that $\rho(t_\infty)$ is a diagonal matrix[1] and suppose that $\rho(t_\infty)$ has at least one non-unitary eigenvalue, say of the norm r, then this means that

$$|\mathbb{X}_i(\tau \pm nh)| = r^{\pm n}|\mathbb{X}_i(\tau)|, \ \forall n \in \mathbb{Z}, \tau \in \mathbb{H},$$

and for some component $\mathbb{X}_i$ of $\mathbb{X}$. However for any $n, \tau \pm nh$ and τ have the same imaginary parts and taking $n \to -\infty$ this contradicts the moderate growth condition unless $\mathbb{X}_i$ is zero. Here $+$ (resp. $-$) is used to treat the case $r > 1$ (resp. $r < 1$).

6.2.1 Admissible vector-valued automorphic forms

Definition 6.2.6. Let G be a Fuchsian group of the first kind, k be an even integer, $\rho : \mathrm{G} \to \mathrm{GL}_m(\mathbb{C})$ be an admissible representation and $\mathbb{X} : \mathbb{H} \to \mathbb{C}^m$ be a vector-valued holomorphic function. Then we say that $\mathbb{X}(\tau)$ is an *admissible vvaf* of weight k with respect to ρ if $\mathbb{X}(\tau)$ satisfies the following functional and growth conditions.

- $\mathbb{X}|_k\gamma = \rho(\gamma)\mathbb{X}, \quad \forall \gamma \in \mathrm{G},$
- For any cusp $\mathfrak{c}$ of G, the function $\mathbb{X}$ has moderate growth at $\mathfrak{c}$.

A vvaf is called *holomorphic* if for any cusp $\mathfrak{c}$ of G, the function $\mathbb{X}|_k A_\mathfrak{c}$ is bounded in some half-plane (contained in $\mathbb{H}$). It is called a *vector-valued cusp form* if, for any cusp $\mathfrak{c}$, the function $\mathbb{X}|_k A_\mathfrak{c}(\tau)$ approaches to 0 as $y \to \infty$.

Remark 6.2.7. If $\mathbb{X}$ is an admissible vvaf of weight k for the Fuchsian group G with respect to ρ and $\gamma \in \mathrm{PSL}_2(\mathbb{R})$, then $\mathbb{X}|_k\gamma$ is an admissible vvaf of weight k for $\gamma^{-1}\mathrm{G}\gamma$ with respect to the representation $\gamma^{-1}\delta\gamma \mapsto \rho(\delta)$.

As a consequence of growth condition and functional behavior, $\mathbb{X}(\tau)$ has an infinite series expansion at any cusp $\mathfrak{c} \in \widehat{\mathfrak{C}}_\mathrm{G}$. These expansions, which are essentially Laurent series expansions, will be referred to as "Fourier series expansions" or simply as "Fourier expansions". Often these expansions are also referred to as $\widetilde{q}_\mathfrak{c}$-expansions with respect to $\mathfrak{c} \in \mathfrak{C}_\mathrm{G}$, where $\widetilde{q}_\mathfrak{c} = \exp\left(\frac{2\pi i A_\mathfrak{c}^{-1}\tau}{h_\mathfrak{c}}\right)$. In addition, for notational convenience, we will always use $\widetilde{q}$ to denote $\widetilde{q}_\infty$.

Lemma 6.2.8. *Let $f(\tau)$ be a scalar-valued meromorphic function on $\mathbb{H}$ which has no poles when $y \geq Y$ for some $Y > 0$ and obeys $f(\tau + h) = \exp(2\pi i\Lambda)f(\tau)$ for every $\tau \in \mathbb{H}$ for some $\Lambda \in \mathbb{R}$. Suppose that $f(\tau)$ has moderate growth at ∞. Then*

$$\widetilde{q}^{\ -\Lambda} f(\tau) = \sum_{n=-M}^{\infty} f_{[n]} \ \widetilde{q}^{\ n}, \tag{6.2}$$

for some $f_{[n]} \in \mathbb{C}, M \in \mathbb{Z}$, and this sum converges absolutely in $y > Y$.

[1]The general case will follow from Remark 6.2.7.

Proof. Since $f(\tau)$ has moderate growth at ∞, there is an integer M such that $F(\tau) = \widetilde{q}^{\,M-\Lambda} f(\tau)$ approaches to 0 as $y \to \infty$ for $0 \le x \le h$. Note that $F(\tau + h) = F(\tau)$ therefore $g(\widetilde{q}) = F(\tau)$ is a well-defined and holomorphic function in the punctured disc $0 < |\widetilde{q}| < \exp(-\frac{2\pi Y}{h})$, about $\widetilde{q} = 0$ and is bounded there (because it approaches to 0 as $\widetilde{q}$ goes to 0). This means that $\widetilde{q} = 0$ is a removable singularity thus defining $g(0) = 0$ gives $g(\widetilde{q})$ is holomorphic in the disc $|\widetilde{q}| < \exp(-\frac{2\pi Y}{h})$. This means that $g(\widetilde{q})$ has a Taylor expansion in $\widetilde{q}$, which converges absolutely in that disc. □

For each eigenvalue λ of $\rho(t_\infty)$, we denote $\mu(\lambda)$ to be the unique real number such that $\lambda = \exp(2\pi i \mu(\lambda))$ and $0 \le \mu(\lambda) < 1$.

Proposition 6.2.9. *Let* G *be a Fuchsian group of the first kind with a cusp at* ∞ *and* k *be an even integer. Let* $\mathbb{X}(\tau)$ *be an admissible vvaf of weight* k *with respect to the representation* $\rho : \mathrm{G} \to \mathrm{GL}_m(\mathbb{C})$. *Let* $\rho(t_\infty) = P\mathrm{diag}\,(\lambda_1, \lambda_2, \cdots, \lambda_m)\, P^{-1}$. *Then, at the cusp* ∞,

$$\mathbb{X}(\tau) = P\widetilde{q}^{\Lambda} P^{-1} \sum_{n=-M}^{\infty} \mathbb{X}_{[n]} \widetilde{q}^{n} \tag{6.3}$$

where $\mathbb{X}_{[n]} \in \mathbb{C}^m$ *and* $M \in \mathbb{Z}$. *Here* $\widetilde{q}^{\Lambda}$ *is denoted to be the diagonal matrix* $\mathrm{diag}\left(\widetilde{q}^{\mu(\lambda_1)}, \widetilde{q}^{\mu(\lambda_2)}, \cdots, \widetilde{q}^{\mu(\lambda_m)}\right)$

Proof. We have $P^{-1}\mathbb{X}(\tau + h) = \mathrm{diag}\,(\lambda_1, \lambda_2, \cdots, \lambda_m)\, P^{-1}\mathbb{X}(\tau)$. Hence, each component of the function $\tau \mapsto P^{-1}\mathbb{X}(\tau)$ satisfies the hypotheses of Lemma 6.2.8. Applying this, we get

$$P^{-1}\mathbb{X}(\tau) = \widetilde{q}^{\Lambda} \sum_{n=-M}^{\infty} v_n \widetilde{q}^{n} \tag{6.4}$$

for some vector-valued sequence v_n. Now we multiply both sides of the last equation by P and define $\mathbb{X}_{[n]} = P v_n$. □

Remark 6.2.10. If v is an eigenvector of $\rho(t_\infty)$ with eigenvalue λ, then v is an eigenvector of $P\widetilde{q}^{\Lambda}P^{-1}$ with eigenvalue $\widetilde{q}^{\mu(\lambda)}$. Since the ρ is admissible, the eigenvectors of $\rho(t_\infty)$ span $\mathbb{C}^m$, this implies that the Fourier expansion at (6.4) does not depend on the choice of the diagonalizing matrix.

If $\mathbb{X}$ is a holomorphic vvaf then all terms of the sum (6.3) with $n < 0$ must vanish. Indeed, if some of these terms did not vanish, then the infinite series would grow at least as $\exp(2\pi y/h)$ as $y \to \infty$. So, $\mathbb{X}(\tau)$ would tend to ∞ as $y \to \infty$, contradicting our definition of holomorphic vector-valued automorphic forms. Similarly, if $\mathbb{X}$ is a vector-valued cusp form, we may take $\mu(\lambda)$ such that $0 < \mu(\lambda) \le 1$ for each eigenvalue λ of $\rho(t_\infty)$ (so now $\mu(\lambda)$ might be 1, but not 0). Then all the terms with $n < 0$ vanish. So, for the vector-valued cusp forms, the infinite series in (6.3) is bounded, while the matrix $P\widetilde{q}^{\Lambda}P^{-1}$ approaches to 0 exponentially as $y \to \infty$. Hence $\mathbb{X}(\tau) \to 0$ exponentially as $y \to \infty$.

Definition 6.2.11. The *Fourier expansion of* $\mathbb{X}$ *at* ∞ (with respect to the choice of diag $(\mu(\lambda_1), \mu(\lambda_2), \cdots, \mu(\lambda_m))$ is given by (6.3). The coefficients $\mathbb{X}_{[n]}$ are known as *Fourier coefficients of* $\mathbb{X}(\tau)$. The *Fourier coefficients of* $\mathbb{X}(\tau)$ *at a cusp* $\mathfrak{c} \in \mathbb{R}$ are defined as the Fourier coefficients of $\mathbb{X}|_k A_{\mathfrak{c}}(\tau)$ at ∞.

Let us now state the main result of this chapter.

Theorem 6.2.12 (Bajpai, Bhakta, Finder)**.** *Let* G *be a non-cocompact Fuchsian group of the first kind and* $\rho : \mathrm{G} \to \mathrm{GL}_m(\mathbb{C})$ *be an admissible representation such that all the eigenvalues of the image of each parabolic element have norm* 1*. Let* $\mathfrak{c}$ *be any cusp of* G*. Then there exists a constant* α*, depending on* G*, with the following properties.*

(i) If $\mathbb{X}(\tau)$ *is an admissible holomorphic vector-valued automorphic form of even integer weight* k *with respect to* ρ*, then the sequence of Fourier coefficients of* $\mathbb{X}$ *at the cusp* $\mathfrak{c}$ *is* $O(n^{k+2\alpha})$*.*

(ii) If $\mathbb{X}(\tau)$ *is an admissible vector-valued cusp form, the sequence of Fourier coefficients is* $O(n^{k/2+\alpha})$*.*

(iii) Moreover, if $k + 2\alpha < 0$*, then* $\mathbb{X} \equiv 0$*.*

6.3 Growth for admissible vector-valued automorphic forms

Before proving Theorem 6.2.12, we briefly summarize our strategy. As the cusp may be moved to ∞ using $A_{\mathfrak{c}}$, we may assume that $\mathfrak{c} = \infty$. Applying a theorem of Eichler, we shall show the existence of α such that

$$\|\rho(\gamma)\| = \left\| \rho \begin{pmatrix} a & b \\ c & d \end{pmatrix} \right\| \ll (c^2 + d^2)^{\alpha}$$

when ρ is admissible. We choose a bounded fundamental domain for G. An arbitrary $\tau \in \mathbb{H}$ is picked, with the aim of bounding $\|\mathbb{X}(\tau)\|$. Then we take $\gamma \in \mathrm{G}$ and z in the fundamental domain such that $\tau = \gamma z$. The vectors $\mathbb{X}(\tau)$ and $\mathbb{X}(z)$ are related via the functional equation, in which there appears $\rho(\gamma)$, whose norm will be estimated. Using the Fourier expansion at any cusp of G, one can estimate $\mathbb{X}(z)$ as z approaches to the cusp within the fundamental domain. In addition, $j(\gamma, z)$ appears in the computations, so we need Corollary 6.3.4 to complete the proof. Also, because of this corollary which only holds for cusps inequivalent to ∞, the case of ∞ must be treated separately.

The following lemma is one of the key tools to prove our main result.

Lemma 6.3.1. *[56, Lemma 6] For any* $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ *in* G*, there exists an integer* n *such that the real numbers* $\tilde{a}$ *and* $\tilde{b}$ *defined by* $\gamma = \left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right)^n \left(\begin{smallmatrix} \tilde{a} & \tilde{b} \\ c & d \end{smallmatrix}\right)$ *satisfy* $\tilde{a}^2 + \tilde{b}^2 \leq k_1(c^2 + d^2)$*, where* k_1 *is a constant depending only on* G*.*

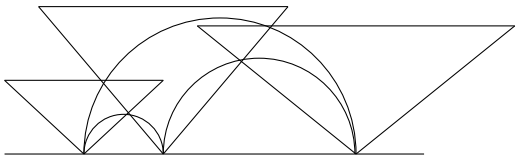

Figure 6.1: Fundamental domain of a Fuchsian group covered by triangles $\mathcal{S}(\mathfrak{c}, v_0, K)$.

Consequently, we have a polynomial-growth of ρ as follows.

Lemma 6.3.2. *For any* $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ *in* G, *we have* $\|\rho(\gamma)\| \ll (c^2+d^2)^{\alpha}$, *where* $\alpha = O\left(\log(M_{\mathrm{G}})\right)$ *and* $M_{\mathrm{G}} = \max\left\{\|\rho(\gamma)\|\right\}_{\gamma \in \mathrm{G}_{\mathrm{Eichler}}}$.

Proof. From the previous lemma we can write $\gamma = \left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right)^n \left(\begin{smallmatrix} \tilde{a} & \tilde{b} \\ c & d \end{smallmatrix}\right)$, such that $\tilde{a}^2+\tilde{b}^2 \leq k_1(c^2+d^2)$, where k_1 is some constant depending on G. The admissibility of ρ implies that the powers of $\left\|\rho\left(\left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right)\right)\right\|$ are uniformly bounded, and in particular, $\|\rho(\gamma)\| \ll \left\|\rho\left(\left(\begin{smallmatrix} \tilde{a} & \tilde{b} \\ c & d \end{smallmatrix}\right)\right)\right\|$. Now applying the result of Eichler on $\left(\begin{smallmatrix} \tilde{a} & \tilde{b} \\ c & d \end{smallmatrix}\right)$, we get $\|\rho(\gamma)\| \ll M_G^L$, where $L \leq C_1 \log(\tilde{a}^2+\tilde{b}^2+c^2+d^2) + C_2 \leq C_1 \log\left((k_1+1)(c^2+d^2)\right) + C_2$, and C_1, C_2 are some constants depending on G. In particular, we then have

$$\|\rho(\gamma)\| \leq M_{\mathrm{G}}^{C_2} \times \left((k_1+1)(c^2+d^2)\right)^{C_1 \log(M_{\mathrm{G}})}.$$

In particular, we can now take $\alpha = C_1 \log(M_{\mathrm{G}})$ to complete the proof. □

Now, we establish the bound for the Fourier coefficients of admissible vector-valued cusp forms as stated in Theorem 6.2.12.

6.3.1 Proof of part (ii) of Theorem 6.2.12

With the polynomial-growth of ρ obtained from the previous lemma (together with the functional equation), we want to relate $\mathbb{X}(\gamma z)$ to $\mathbb{X}(z)$. Denoting $\tau = \gamma z$, $\|\mathbb{X}(\tau)\| = \|(cz+d)^k \rho(\gamma)\mathbb{X}(z)\| \ll |cz+d|^k (c^2+d^2)^{\alpha} \|\mathbb{X}(z)\|$. Let $z = u+iv$. Using the elementary inequality $c^2+d^2 \leq |cz+d|^2(1+4|z|^2)/v^2$, proven by Knopp in [56, lemma 4], one obtains

$$\|\mathbb{X}(\tau)\| \ll |cz+d|^{k+2\alpha}(1+4|z|^2)^{\alpha} v^{-2\alpha} \|\mathbb{X}(z)\|. \tag{6.5}$$

Applying the identity $y = \mathrm{Im}\gamma z = \frac{v}{|cz+d|^2}$, we get

$$y^{k/2+\alpha} \|\mathbb{X}(\tau)\| \ll (1+4|z|^2)^{\alpha} v^{k/2-\alpha} \|\mathbb{X}(z)\|. \tag{6.6}$$

At this point, it is convenient to restrict z to a fundamental domain of G which does not depend on τ. Since G is a Fuchsian group of the first kind, $\mathrm{G}\backslash\mathbb{H}_{\mathrm{G}}^*$ is compact,

and there are only finitely many equivalence classes of cusps, and a bounded fundamental domain that may be partitioned into a finite set of pieces, see Figure 1. More precisely, the constants K, v_0, and a finite set of cusps $\mathfrak{c}_{\mathrm{G}}$ such that each such piece is contained in a triangle of the type $\{z \in \mathbb{H} : v < v_0 \text{ and } |u - \mathfrak{c}| \leq Kv\}$, which we denote by $\mathcal{S}(\mathfrak{c}, v_0, K)$, where $\mathfrak{c} \in \mathfrak{C}_{\mathrm{G}}$. Then, for z in this fundamental domain,

$$y^{k/2+\alpha}\|\mathbb{X}(\tau)\| \ll v^{k/2-\alpha}\|\mathbb{X}(z)\|. \tag{6.7}$$

Since $\mathbb{X}$ is a vector-valued cusp form, if $\mathfrak{c}$ is any cusp, $\mathbb{X}|_k A_{\mathfrak{c}}$ decays exponentially as the imaginary part of its argument goes to infinity. We shall show this implies that, for any real number β, $\|\mathbb{X}(z)\| \ll v^{\beta}$ in $\mathcal{S}(\mathfrak{c}, v_0, K)$. To do so, let $\mathbb{Y}_{\mathfrak{c}} = \mathbb{X}|_k A_{\mathfrak{c}}$. Then

$$\mathbb{X}(z) = \mathbb{Y}_{\mathfrak{c}}|_k A_{\mathfrak{c}}^{-1}(z) = (\mathfrak{c} - z)^{-k}\mathbb{Y}_{\mathfrak{c}}\left(\frac{1}{\mathfrak{c} - z}\right).$$

Since $|\mathfrak{c} - z|$ is comparable to v,

$$\|\mathbb{X}(z)\| \ll v^{-k}\|\mathbb{Y}_{\mathfrak{c}}\left(\frac{1}{\mathfrak{c} - z}\right)\|.$$

Since $\mathbb{Y}_{\mathfrak{c}}$ decays more rapidly than the $(k+\beta)^{\text{th}}$-power of the imaginary part of its argument, we get

$$\|\mathbb{X}(z)\| \ll v^{-k}\left(\mathrm{Im}\frac{1}{\mathfrak{c} - z}\right)^{-k-\beta}.$$

Note that

$$\mathrm{Im}\frac{1}{\mathfrak{c} - z} = \frac{v}{|\mathfrak{c} - z|^2} = \frac{v}{(\mathfrak{c} - u)^2 + v^2},$$

whence, from the definition of $\mathcal{S}(\mathfrak{c}, v_0, K)$,

$$\frac{1}{v} \geq \mathrm{Im}\frac{1}{\mathfrak{c} - z} \geq \frac{v}{K^2 v^2 + v^2} \gg \frac{1}{v}.$$

Therefore,

$$\mathbb{X}(z) \ll v^{-k}v^{k+\beta} = v^{\beta}, \ \forall z \in \mathcal{S}(\mathfrak{c}, v_0, K).$$

Since the fundamental domain we chose is contained in a finite union of these sets, the bound holds in the fundamental domain as well. Taking $\beta = \alpha - k/2$ and using (6.7), we see that $y^{k/2+\alpha}\|\mathbb{X}(\tau)\|$ is bounded in $\mathbb{H}$. Now note that the i^{th}-component of the n^{th}-Fourier coefficient is

$$\mathbb{X}_{[i,n]} = \frac{1}{h}\int_0^h \mathbb{X}_i(x + iy)\widetilde{q}^{(-n-\mu(\lambda_i))}dx.$$

In particular, we then have

$$\mathbb{X}_{[i,n]} \ll y^{-k-2\alpha}e^{2\pi y(n+\mu(\lambda_i)/h}.$$

Taking $y = \frac{1}{n+\mu(\lambda_i)}$ we get the desired result. □

6.3.2 Proof of part (i) and part (iii) of Theorem 6.2.12

We now establish the growth for admissible holomorphic vector-valued automorphic forms. To complete the proof of the theorem, we need the following lemma.

Lemma 6.3.3. *Let* $\mathfrak{c}$ *and* ∞ *be the cusps of the Fuchsian group* G. *Then either* $\mathfrak{c}$ *and* ∞ *are equivalent cusps or* $\inf_{\gamma\in\mathrm{G}} |j(\gamma,\mathfrak{c})| > 0$.

Proof. We begin with the case $\mathfrak{c} = 0$. Note that, if $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, then $j(\gamma, 0) = d$. Now assume that 0 and ∞ are not equivalent cusps of G. Then $d \neq 0$ whenever $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{G}$. Since ∞ is a cusp of G, there is a parabolic element in $\mathrm{G}\backslash\{I\}$ whose lower left entry vanishes. Such an element necessarily equals to $\left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right)$ for some nonzero h. Using that 0 is a cusp of G, we similarly obtain $\left(\begin{smallmatrix} 1 & 0 \\ h' & 1 \end{smallmatrix}\right) \in \mathrm{G}$ for some nonzero h'. For any integer n,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ h' & 1 \end{pmatrix}^n = \begin{pmatrix} a + nh'b & b \\ c + nh'd & d \end{pmatrix}.$$

Since $h'd \neq 0$, there is n such that $|c + nh'd| \leq |h'd|$, namely the integer part of $-c/h'd$. By Lemma 1.7.3 of [67], either $c + nh'd = 0$ or $|c + nh'd| \geq |h|^{-1}$. If $c + nh'd = 0$, by part 2 of Theorem 1.5.4 in [67] with $x = \infty$ and σ equal to the identity, we have $|d| = 1$. If $|c + nh'd| \geq |h|^{-1}$, by our choice of n, we get $|d| \geq |hh'|^{-1}$. So $\inf_{\gamma\in\mathrm{G}} |j(\gamma, 0)| \geq \min\{1, |hh'|^{-1}\} > 0$, as desired.

Now we show the claim for a general $\mathfrak{c}$. We shall move the cusp to the origin by means of the translation $B_{\mathfrak{c}}(\tau) = \tau - \mathfrak{c}$. Observe that 0 is a cusp of the Fuchsian group $B_{\mathfrak{c}}\mathrm{G}B_{\mathfrak{c}}^{-1}$. Indeed, let $\delta \in \mathrm{G}$ be a parabolic element such that $\delta\mathfrak{c} = \mathfrak{c}$. Then $B_{\mathfrak{c}}\delta B_{\mathfrak{c}}^{-1}$ is parabolic and $B_{\mathfrak{c}}\delta B_{\mathfrak{c}}^{-1}0 = B_{\mathfrak{c}}\delta\mathfrak{c} = B_{\mathfrak{c}}\mathfrak{c} = 0$. Similarly, ∞ is a cusp of $B_{\mathfrak{c}}\mathrm{G}B_{\mathfrak{c}}^{-1}$. If 0 and ∞ were equivalent cusps of this new group, there would exist $\delta \in B_{\mathfrak{c}}\mathrm{G}B_{\mathfrak{c}}^{-1}$ such that $\delta 0 = \infty$. Then we would have $B_{\mathfrak{c}}^{-1}\delta B_{\mathfrak{c}} \in \mathrm{G}$ and $B_{\mathfrak{c}}^{-1}\delta B_{\mathfrak{c}}\mathfrak{c} = B_{\mathfrak{c}}^{-1}\delta 0 = B_{\mathfrak{c}}^{-1}\infty = \infty$, so $\mathfrak{c}$ would be equivalent to ∞ as a cusp of G, a contradiction. We have established 0 and ∞ are inequivalent cusps. From the case we have already proven,

$$\inf_{\gamma\in B_{\mathfrak{c}}\mathrm{G}B_{\mathfrak{c}}^{-1}} |j(\gamma, 0)| > 0. \tag{6.8}$$

Now let $\gamma \in \mathrm{G}$ and $\tilde{\gamma} = B_{\mathfrak{c}}\gamma B_{\mathfrak{c}}^{-1}$. Then $\gamma\mathfrak{c} \neq \infty$ and $\tilde{\gamma}B_{\mathfrak{c}} = B_{\mathfrak{c}}\gamma$. Hence, it follows from the definition of j that $j(\tilde{\gamma}, 0) = j(\gamma, \mathfrak{c})$. Combining this with inequality (6.8), we conclude the proof. □

Corollary 6.3.4. *Let* $\mathfrak{c}$ *and* ∞ *be inequivalent cusps of the Fuchsian group* G. *Let* K *and* v_0 *be positive real numbers. Then there exists a constant* $C_{K,\mathfrak{c}} > 0$ *such that* $|j(\gamma, z)| \geq C_{K,\mathfrak{c}}$ *for any* $\gamma \in \mathrm{G}$ *and any* $z \in \mathcal{S}(\mathfrak{c}, v_0, K)$.

Proof. When z varies in $\mathcal{S}(\mathfrak{c}, v_0, K)$, the point $j(\gamma, z) = cz + d$ varies in a similar triangle to $\mathcal{S}(\mathfrak{c}, v_0, K)$, with a vertex at $j(\gamma, \mathfrak{c})$ (see Figure 2). In particular, $j(\gamma, z)$

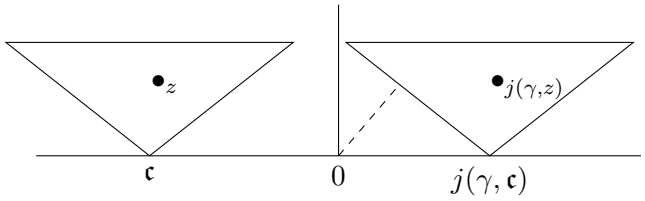

Figure 6.2: If z lies in a given triangle $\mathcal{S}(\mathfrak{c}, v_0, K)$, then $j(\gamma, z)$ lies in a similar triangle, which helps to estimate its distance to the origin.

lies between the straight lines through $j(\gamma, \mathfrak{c})$ with slopes $1/K$ and $-1/K$. So the distance from $j(\gamma, z)$ to the origin is greater than the distance from some of these straight lines to the origin. From trigonometry, the latter is $|j(\gamma, \mathfrak{c})|/\sqrt{K^2+1}$. Therefore

$$|j(\gamma, z)| \geq \frac{|j(\gamma, \mathfrak{c})|}{\sqrt{K^2+1}}.$$

The claim now follows from Lemma 6.3.3, taking $C_{K,\mathfrak{c}} = \frac{\inf_{\gamma \in \mathrm{G}} |j(\gamma,\mathfrak{c})|}{\sqrt{K^2+1}}$. □

We now give proof of the bound of order $O(n^{k+2\alpha})$ in Theorem 6.2.12.

Proof of part (i) of Theorem 6.2.12: holomorphic vvaf

We begin with the case $k + 2\alpha \geq 0$. Let $\mathcal{S}(\mathfrak{c}, v_0, K) = \{u + iv \in \mathbb{H} : v < v_0 \text{ and } |u - \mathfrak{c}| \leq Kv\}$. There exists constants v_0, v_1, K and a fundamental domain $\mathrm{F_G}$ that is contained in a finite union of sets of type $\mathcal{S}(\mathfrak{c}, v_0, K)$, where $\mathfrak{c}$ is a cusp of G that is not equivalent to ∞, and of a set $\{u + iv \in \mathbb{H} : 0 \leq u < h \text{ and } v > v_1\}$. Take τ in $\mathbb{H}$ such that $\mathrm{Im}\tau = y < v_1$. There exists $z = u + iv$ in $\mathrm{F_G}$ such that $\gamma z = \tau$. From inequality (6.5),

$$y^{k+2\alpha} \|\mathbb{X}(\tau)\| \ll |cz + d|^{-k-2\alpha} (1 + 4|z|^2)^{\alpha} v^k \|\mathbb{X}(z)\|.$$

From the fact that $\mathbb{X}|_k A_{\mathfrak{c}}$ is bounded near ∞, one can show that $v^k \|\mathbb{X}(z)\|$ is bounded in any set of type $\mathcal{S}(\mathfrak{c}, v_0, K)$. Therefore, in such a set,

$$y^{k+2\alpha} \|\mathbb{X}(\tau)\| \ll |cz + d|^{-k-2\alpha}.$$

By Corollary 6.3.4, $|cz + d|$ has a lower bound independent of γ and z, for any z in $\mathcal{S}(\mathfrak{c}, v_0, K)$. This implies that $y^{k+2\alpha}\mathbb{X}(\tau)$ is bounded since we are assuming that the exponent $-k - 2\alpha$ is negative.

It remains to consider the case in which $0 \leq u < h$ and $v > v_1$. Now $\frac{1+4|z|^2}{v^2}$ is bounded, so that

$$y^{k+2\alpha} \|\mathbb{X}(\tau)\| \ll \left(\frac{v}{|cz + d|}\right)^{k+2\alpha} \leq |c|^{-k-2\alpha}.$$

By Lemma 1.7.3 of [67] and the hypothesis that the exponent $-k-2\alpha$ is negative, this has an upper bound unless $\gamma = \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}^n$. But $\gamma = \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}^n \implies y = v > v_1$, contradicting our choice of τ. Therefore, $y^{k+2\alpha}\|\mathbb{X}(\tau)\|$ is bounded if y is sufficiently small. As in the proof for vector-valued cusp forms, one obtains the bound for the Fourier coefficients of $\mathbb{X}$.

Proof of part (iii) of Theorem 6.2.12: case $k + 2\alpha < 0$

To treat the case $k + 2\alpha < 0$, we work with a fundamental domain that is contained in a finite union of sets of the type $\mathcal{S}(\mathfrak{c}, v_0, K)$. In such a region, we employ inequality (6.6) together with the bound $\mathbb{X}(z) \ll v^{-k}$, and get

$$y^{k/2+\alpha}\|\mathbb{X}(\tau)\| \ll v^{-k/2-\alpha} \ll 1,$$

since v is bounded. This implies that $\|\mathbb{X}(\tau)\| \to 0$ as $y \to 0$. Therefore, each component of $\mathbb{X}(\tau)$ approaches to 0 as $y \to 0$. Multiplying the i^{th}-component of $\mathbb{X}$ by $\widetilde{q}^{1-\mu(\lambda_i)}$, we get a power series in $\widetilde{q}$ which approaches to 0 as $|\widetilde{q}| \to 1$. By the maximum principle applied to circles with a radius close to 1, we conclude that each component of $\mathbb{X}(\tau)$ vanishes. □

6.4 L-functions and the associated exponential sums

Knopp and Mason remarked [52] that it is possible to attach an L-function to admissible vvmf for the modular group with analytic continuation. In this section, we generalize this notion to the admissible vvaf for Fuchsian groups of the first kind. The proof of functional equation is classical. However, we will briefly discuss the proof to remain self-contained. In this connection, the reader will find the article [50] useful, where the authors discussed the special values of L-function attached to vvmf for the modular group. In this section, we rather focus on the analytic continuation of these L-functions attached in general to the admissible vector-valued automorphic forms.

We assume that $0, \infty$ are cusps of G and $\mathbb{X}$ is an admissible cuspform. Let us define

$$L(\mathbb{X}, \mathfrak{s}) = \sum_{n \geq 0} \frac{\mathbb{X}_{[n]}}{(n+\Lambda)^{\mathfrak{s}}}$$

in $\mathrm{Re}(\mathfrak{s}) > k/2 + \alpha + 1$, where α is the constant as in Theorem 6.2.12, $\mathbb{X}_{[n]}$ is the n^{th}-Fourier coefficient of $\mathbb{X}$ at ∞, and $(n + \Lambda)$ is the matrix

$$\mathrm{diag}\left(n + \mu(\lambda_1), n + \mu(\lambda_2), \cdots, n + \mu(\lambda_m)\right),$$

where each λ_i is an eigenvalue of $\rho(t_\infty)$. We also define the completed L-function

$\widetilde{\Lambda}(\mathbb{X},\mathfrak{s})$ to be $(2\pi)^{-\mathfrak{s}}\Gamma(\mathfrak{s})L(\mathbb{X},\mathfrak{s})$. Recalling that $\Gamma(\mathfrak{s})=\int_0^\infty e^{-y}y^{\mathfrak{s}-1}dy$, we have

$$\begin{aligned}\int_0^\infty \mathbb{X}(ihy)y^{\mathfrak{s}-1}dy &= \int_0^\infty \sum_{n\geq 0}\mathbb{X}_{[n]}e^{-2\pi y(n+\Lambda)}y^{\mathfrak{s}-1}dy\\ &= (2\pi)^{-\mathfrak{s}}\Gamma(s)L(\mathbb{X},\mathfrak{s})=\widetilde{\Lambda}(\mathbb{X},\mathfrak{s}).\end{aligned}$$

Theorem 6.2.12 implies that $\widetilde{\Lambda}(\mathbb{X},\mathfrak{s})$ is analytic in the region $\mathrm{Re}(\mathfrak{s})>k/2+\alpha$. This is because, for each component $\mathbb{X}_j$ of $\mathbb{X}$ we have

$$\begin{aligned}\Big|\int_0^\infty \mathbb{X}_j(ihy)y^{\mathfrak{s}-1}dy\Big| &\leq \int_0^Y \Big|\mathbb{X}_j(ihy)\Big|y^{\mathfrak{s}-1}dy+\int_Y^\infty \Big|\mathbb{X}_j(ihy)\Big|y^{\mathfrak{s}-1}dy\\ &\leq \int_0^Y |hy|^{-k/2-\alpha}y^{\mathfrak{s}-1}dy+\int_Y^\infty \exp(-cy)y^{\mathfrak{s}-1}dy,\end{aligned}$$

where $c\,(>0)$ is coming from the exponential decay of $\mathbb{X}$ in a neighborhood of ∞. In particular, the second integral is bounded for any $\mathfrak{s}$. To bound the first integral it is enough to consider the range only from 0 to 1 and after performing a change of variable we are left with the integral $\int_1^\infty y^{k/2+\alpha-\mathfrak{s}-1}dy$, which converges for $\mathrm{Re}(\mathfrak{s})>k/2+\alpha$.

Consider $S=\left(\begin{smallmatrix}0&-1\\1&0\end{smallmatrix}\right)$ and note that $\mathbb{Y}=\mathbb{X}|_kS$, is an admissible vvaf for the group $S^{-1}\mathrm{G}S$. We now have

$$\begin{aligned}\int_0^\infty \mathbb{Y}(ihy)y^{\mathfrak{s}-1}ds &= (hi)^{-k}\int_0^\infty y^{\mathfrak{s}-k-1}\mathbb{X}(i/hy)dy\\ &= (hi)^{-k}\int_0^\infty \sum_{n\geq 0}\mathbb{X}_{[n]}e^{-2\pi(n+\Lambda)/h^2y}y^{\mathfrak{s}-k-1}dy\\ &= -(hi)^{-k}\int_0^\infty \sum_{n\geq 0}\mathbb{X}_{[n]}e^{-2\pi y(n+\Lambda)/h^2}y^{k-\mathfrak{s}-1}dy\\ &= -(hi)^{-k}h^{2k-2s}\widetilde{\Lambda}(\mathbb{X},k-\mathfrak{s}).\end{aligned}$$

Moreover, since ∞ is a cusp of $S^{-1}\mathrm{G}S$, arguing similarly as before, we get an analytic continuation for $\int_0^\infty \mathbb{Y}(ihy)y^{\mathfrak{s}-1}ds$, to $\mathrm{Re}(\mathfrak{s})>k/2+\alpha$. In particular, the completed L-function $\widetilde{\Lambda}(\mathbb{X},\mathfrak{s})$ has analytic continuation to $\mathrm{Re}(\mathfrak{s})<k/2-\alpha$ as well.

Note 6.4.1. In both cases, we are assuming that 0 and ∞ are cusps of G. In general, let us assume that G has at least one cusp. Since G is a Fuchsian group of the first kind, G has at least two distinct (not necessarily inequivalent) cusps in $\mathbb{P}^1(\mathbb{R})$. Let $\mathfrak{c}_1$ and $\mathfrak{c}_2$ be any two distinct cusps of G. If they are both finite, then we can choose $\gamma:=\left(\begin{smallmatrix}\mathfrak{c}_1 & \frac{\mathfrak{c}_2}{\mathfrak{c}_1-\mathfrak{c}_2}\\ 1 & \frac{1}{\mathfrak{c}_1-\mathfrak{c}_2}\end{smallmatrix}\right)\in \mathrm{PSL}_2(\mathbb{R})$, which satisfies that $\gamma\infty=\mathfrak{c}_1$ and $\gamma 0=\mathfrak{c}_2$. On the other hand, without loss of generality, let us assume that $\mathfrak{c}_1=\infty$ and $\mathfrak{c}_2$ is finite. In that case we can take $\gamma:=\left(\begin{smallmatrix}1&\mathfrak{c}_2\\0&1\end{smallmatrix}\right)$, which again satisfies that $\gamma\infty=\mathfrak{c}_1$ and $\gamma 0=\mathfrak{c}_2$. In both of the cases, $\gamma^{-1}\mathrm{G}\gamma$ contains the cusps 0 and ∞. With this set up, we can now finally define $L_{\mathfrak{c}_1,\mathfrak{c}_2}(\mathbb{X},\mathfrak{s})=L(\mathbb{X}|_k\gamma,\mathfrak{s})$, and this gives us a (non-empty) family of L-functions indexed by pairwise distinct cusps.

6.5 Exponential sums and growth

Studying exponential sums associated to arithmetic functions is of great interest in number theory. When f is a cusp form of weight k and level N, by the standard bound on the Fourier coefficients, one can show that

$$S(f,\theta,X)=\sum_{1\leq n\leq X} f_{[n]}e(n\theta)\ll X^{k/2}\log X, \tag{6.9}$$

where we make use of the standard notation $e(z):=e^{2i\pi z}$ and stick to it throughout the section. The extra log factor in (6.9) was later removed by Jutila [48].

In this section, we shall first consider the analogous exponential sums for holomorphic admissible vector-valued automorphic forms and show how our growth results give a bound of order $X^{\sigma(k/2+\alpha)}\log X$, with $\sigma=2$ for the holomorphic vector-valued automorphic forms and $\sigma=1$ for vector-valued cusp forms. We aim to study the analogous exponential sums associated to Fourier coefficients of holomorphic vector-valued automorphic forms of Fuchsian groups of the first kind.

Consider

$$\mathbb{X}(z)=\Big(\sum_{n=0}^{\infty}\mathbb{X}_{[i,n]}\widetilde{q}^{n+\mu(\lambda_i)}\Big)_{0\leq i\leq m-1}$$

and the exponential sums associated to the components of the Fourier coefficients as

$$S_i(\mathbb{X},\theta,X)=\sum_{0\leq n<X}\mathbb{X}_{[i,n]}e(n\theta),\ 0\leq i\leq m-1.$$

For any $y>0$, we have $\mathbb{X}_{[i,n]}=\frac{1}{h}\int_0^h \mathbb{X}_i(\tau)e\left(-\frac{\tau}{h}(n+\mu(\lambda_i))\right)\,dx$. Therefore

$$S_i(\mathbb{X},\theta,X)=\frac{1}{h}\int_0^h \mathbb{X}_i(\tau)e\left(-\frac{\tau}{h}\lambda_i\right)\sum_{0\leq n<X}e\left(n\left(-\frac{\tau}{h}+\theta\right)\right)\,dx.$$

The sum on the right-hand side is a geometric progression, and this gives us

$$\left|\sum_{0\leq n<X}e\left(n\left(-\frac{\tau}{h}+\theta\right)\right)\right|\ll\left|\frac{1-e\left(X\left(-\frac{\tau}{h}+\theta\right)\right)}{1-e\left(-\frac{\tau}{h}+\theta\right)}\right|.$$

Note that $|e\left(X\left(-\frac{\tau}{h}+\theta\right)\right)|=e^{2\pi Xy/h}$ and also from Theorem 6.2.12 we have $|\mathbb{X}_i(\tau)|\ll y^{-\sigma(k/2+\alpha)}$. In particular,

$$|S_i(\mathbb{X},\theta,X)|\ll y^{-\sigma(k/2+\alpha)}e^{2\pi Xy/h}\frac{1}{h}\int_0^h\frac{1}{\left|1-e\left(-\frac{\tau}{h}+\theta\right)\right|}\,dx.$$

Replacing x by $x+h\theta$ and using the periodicity of $e\left(-\frac{\tau}{h}\right)$,

$$\begin{aligned}\int_0^h \frac{1}{\left|1-e\left(-\frac{\tau}{h}+\theta\right)\right|}\,dx &= \int_{-h\theta}^{h-h\theta} \frac{1}{\left|1-e\left(-\frac{\tau}{h}\right)\right|}\,dx = \int_{-h/2}^{h/2} \frac{1}{\left|1-e\left(-\frac{\tau}{h}\right)\right|}\,dx \\ &\ll \int_0^{h/2} \frac{1}{\left|\frac{\tau}{h}\right|}\,dx = h\left(\int_0^y \frac{1}{|\tau|}\,dx + \int_y^{h/2} \frac{1}{|\tau|}\,dx\right) \\ &\ll h\left(1+\log\frac{h}{y}\right).\end{aligned}$$

Thus,

$$|S_i(\mathbb{X},\theta,X)| \ll y^{-\sigma(k/2+\alpha)} e^{2\pi Xy/h}\left(1+\log\frac{h}{y}\right).$$

One now gets $|S_i(\mathbb{X},\theta,X)| \ll X^{\sigma(k/2+\alpha)}\log X$ by taking $y=h/X$.

Doing a little more delicate analysis, we can obtain a better bound of the Fourier coefficients on average. To be more precise, we shall now give a stronger bound on $\sum_{n\le X}\left\|\sum \mathbb{X}_{[n]}\right\|^2$. Before that, let us first discuss the known results for the scalar case. When f is a (scalar-valued) cusp form of weight k (and of level N, say) then Rankin [72, Theorem 1] showed that

$$\sum_{1\le n\le X} |f_{[n]}|^2 = cX^k + O(x^{k-2/5}),$$

where $c>0$ is a computable constant. Writing $z=x+iy$, we have

$$\begin{aligned}\sum_{0\le n\le X}\left\|\mathbb{X}_{[n]}\right\|^2 e^{-4\pi ny} &\le \sum_{0\le i\le m-1}\int_0^h |\mathbb{X}_i(x+iy)|^2\,dx \\ &= \int_0^h \left\|\mathbb{X}(x+iy)\right\|^2\,dx \\ &\ll y^{-2k-4\alpha},\end{aligned}$$

for any $y>0$. So in particular, taking $y=\frac{1}{X}$ we obtain for holomorphic vector-valued automorphic forms that $\sum_{0\le n\le X}\left\|\mathbb{X}_{[n]}\right\|^2 \ll X^{2k+4\alpha}$. Similarly, for vector-valued cusp forms, we get

$$\sum_{0\le n\le X}\left\|\mathbb{X}_{[n]}\right\|^2 \ll X^{k+2\alpha}. \tag{6.10}$$

Chapter 7

Logarithmic Vector-valued automorphic forms: lifting and growth

In this chapter, we shall generalize the notion of admissible vvaf and study their growth. Following the standard setup, let G be a Fuchsian group of the first kind, k be an even integer, $\rho : \mathrm{G} \to \mathrm{GL}_m(\mathbb{C})$ be a representation, and $\mathbb{X} : \mathbb{H} \to \mathbb{C}^m$ be a vector-valued holomorphic function. Suppose that $\mathbb{X}(\tau)$ satisfies the functional behavior $\mathbb{X}|_k\gamma = \rho(\gamma)\mathbb{X},\ \forall\gamma \in \mathrm{G}$. We are interested in the case when ρ is not necessarily admissible and all the eigenvalues of $\rho(\gamma)$ are unitary for every parabolic element $\gamma \in \mathrm{G}$. Such an associated vvaf $\mathbb{X}(\tau)$ will be called *logarithmic vvaf*.

7.1 Logarithmic vvaf and the Fourier expansion

We shall now discuss the properties and features of logarithmic vvaf, following [53]. Let us first consider the space

$$W = \mathrm{Span}_{\mathbb{C}} \left\{ \mathbb{X}_i(\tau) \mid 0 \leq i \leq m-1 \right\}.$$

Note that W has dimension at most m over $\mathbb{C}$, and it is invariant under the action of t_∞. In other words, we can consider $\rho(t_\infty) : W \to W$ defined by $\mathbb{X}_i(\tau) \mapsto \mathbb{X}_i(\tau + h)$. With respect to the basis $\{\mathbb{X}_i(\tau) \mid 0 \leq i \leq m-1\}_{0 \leq 1 \leq m-1}$, or possibly a subset of this if they are linearly dependent, we may assume that $\rho(t_\infty)$ is in the Jordan canonical form

$$\begin{pmatrix} J_{m(\lambda_1),\lambda_1} & & & \\ & J_{m(\lambda_2),\lambda_2} & & \\ & & \ddots & \\ & & & J_{m(\lambda_k),\lambda_k} \end{pmatrix},$$

where the Jordan block J_{m_i,λ_i} is defined to be

$$\begin{pmatrix} \lambda_i & & & \\ \lambda_i & \ddots & & \\ & \ddots & \ddots & \\ & & \lambda_i & \lambda_i \end{pmatrix},$$

which is conjugate to the canonical Jordan block, and $m(\lambda)$ is the multiplicity of the eigenvalue λ. We shall denote $R(t_\infty)$ to be the set of all eigenvalues of $\rho(t_\infty)$.

Lemma 7.1.1. *Let $\mathbb{X}(\tau)$ be a vector-valued holomorphic function on $\mathbb{H}$ such that $\mathbb{X}(\tau+h) = \rho(t_\infty)\mathbb{X}(\tau)$, then for each eigenvalue λ of $\rho(t_\infty)$ there are $\widetilde{q}$-expansions $h_{\lambda,j}(\tau) = \sum_{n\in\mathbb{Z}} \mathbb{X}_{[\lambda,j,n]}\widetilde{q}^{n+\mu(\lambda)}$, $0 \le j \le m(\lambda)-1$ such that*

$$\mathbb{X}(\tau) = \sum_{\lambda\in R(t_\infty)} \sum_{j=0}^{m(\lambda)-1} (\log \widetilde{q})^j h_{\lambda,j}(\tau). \tag{7.1}$$

Proof. We start by writing

$$\Big\{\mathbb{X}_i(\tau)\Big\}_{0\le i\le m-1} = \bigsqcup_{\substack{\lambda\in R(t_\infty),\\ 0\le i\le m(\lambda)-1}} \Big\{\mathbb{X}_{i,\lambda}(\tau)\Big\},$$

such that for each eigenvalue λ, we have $\rho(t_\infty)$ is the single block $J_{m(\lambda),\lambda}$ when acting on the space generated by $\{\mathbb{X}_{i,\lambda}\}_{0\le i\le m(\lambda)-1}$.

For each λ we can now write,

$$\mathbb{X}_{i,\lambda}(\tau+h) = \lambda(\mathbb{X}_{i,\lambda}(\tau) + \mathbb{X}_{i-1,\lambda}(\tau)),\ 0 \le i \le m(\lambda)-1,$$

where we set $\mathbb{X}_{-1,\lambda} = 0$. Define,

$$\tilde{h}_{i,\lambda}(\tau) = \sum_{j=0}^{i} (-1)^j \binom{\tau/h + j - 1}{j} \mathbb{X}_{i-j,\lambda}(\tau),\ 0 \le i \le m(\lambda)-1.$$

Following the argument of [53, page 265], we see that each $\tilde{h}_{i,\lambda}$ has a convergent $\widetilde{q}$-expansion of type $\sum_{n\in\mathbb{Z}, n+\lambda\ge 0} a_i(n)\widetilde{q}^{n+\mu(\lambda)}, 0 \le i \le m(\lambda)-1$ and

$$\mathbb{X}_{i,\lambda}(\tau) = \sum_{j=0}^{i} \binom{\tau}{j} \tilde{h}_{i-j,\lambda}(\tau),\ 0 \le i \le m(\lambda)-1. \tag{7.2}$$

Now note that,

$$\mathrm{Span}_{\mathbb{C}} \left\{ \binom{\tau}{j} \mid 0 \le j \le m(\lambda)-1 \right\} = \mathrm{Span}_{\mathbb{C}} \left\{ (\log \widetilde{q})^j \mid 0 \le j \le m(\lambda)-1 \right\},$$

because $2\pi i\tau/h = \log \widetilde{q}$. It now follows from (7.2) that there exists a matrix $H_\lambda(\tau)$, whose entries are written in terms of $\tilde{h}_{j,\lambda}$'s, such that

$$\begin{pmatrix} \mathbb{X}_{0,\lambda}(\tau) \\ \mathbb{X}_{1,\lambda}(\tau) \\ \vdots \\ \mathbb{X}_{m(\lambda)-1,\lambda}(\tau) \end{pmatrix} = H_\lambda(\tau) A \begin{pmatrix} 1 \\ (\log \widetilde{q}) \\ \vdots \\ (\log \widetilde{q})^{m(\lambda)-1} \end{pmatrix},$$

for some $A \in \mathrm{GL}_m(\mathbb{C})$. We can therefore write for eigenvalue λ and $i \in \{0, 1, \cdots, m(\lambda)-1\}$ that

$$\mathbb{X}_{i,\lambda}(\tau) = \sum_{j=0}^{m(\lambda)-1} (\log \widetilde{q})^j h_{i,j,\lambda}(\tau),$$

where each $h_{i,j,\lambda}(\tau)$ is of form $\sum_{n\geq 0} \mathbb{X}_{[i,j,\lambda,n]} \widetilde{q}^{n+\mu(\lambda)}$. The result is now proved by taking $h_{\lambda,j}(\tau) = \sum_{0\leq i\leq m(\lambda)-1} h_{i,j,\lambda}(\tau) e_{\lambda,i}$, where $e_{\lambda,i}$ is an element of the canonical basis of $\mathbb{C}^m$. □

Note 7.1.2. The lemma above shows how to get a logarithmic expansion of $\mathbb{X}(\tau)$ at ∞ when $\rho(t_\infty)$ is in the Jordan canonical form. For a general ρ, let $P\rho(t_\infty)P^{-1}$ be in the Jordan canonical form, then $\mathbb{Y} = P\mathbb{X}$ is a logarithmic vvaf for $P\rho P^{-1}$. Since $P\rho(t_\infty)P^{-1}$ is in the Jordan canonical form, we have

$$\mathbb{Y}(\tau) = \sum_{\lambda\in R(t_\infty)} \sum_{j=0}^{m(\lambda)-1} (\log \widetilde{q})^j \sum_{n=-M}^{\infty} \widetilde{q}^{n+\mu(\lambda)} v_{[\lambda,j,n]}$$

where $v_{[\lambda,j,n]}$ denotes a vector. Then we need only to multiply this by P^{-1}. Since multiplying by P^{-1} will mix the components of $v_{[\lambda,j,n]}$, we have $\widetilde{q}^{n+\mu(\lambda)}$ for all the eigenvalues λ.

To get such an expansion around other cusp $\mathfrak{c}$, one needs to get an expansion of $\mathbb{X}|_k A_{\mathfrak{c}}$ around ∞, as we did in the admissible case. Having this in our hands, we are now ready to describe the vector-valued automorphic forms when the corresponding representation is not admissible.

In Lemma 7.1.1 and Note 7.1.2, we have seen how to get a logarithmic expansion of $\mathbb{X}(\tau)$. We are interested in studying the growth when all the components $\mathbb{X}_i(\tau)$ are holomorphic at the cusps in the logarithmic sense which we define below and use in the rest of the article.

Definition 7.1.3. *We say that $\mathbb{X}(\tau)$ is holomorphic at the cusp ∞ if it has an expansion of the form*

$$\mathbb{X}(\tau) = \sum_{\lambda\in R(t_\infty)} \sum_{j=0}^{m(\lambda)-1} (\log \widetilde{q})^j \sum_{n=0}^{\infty} \mathbb{X}_{[\lambda,j,n]} \widetilde{q}^{n+\mu(\lambda)}$$

where each $\mathbb{X}_{[\lambda,j,n]}$ is a vector, and $\mathbb{X}$ is holomorphic at the cusp $\mathfrak{c}$ if $\mathbb{X}|_k A_{\mathfrak{c}}$ is holomorphic at the cusp ∞. If $\mathbb{X}$ is holomorphic at all cusps, then we say that $\mathbb{X}$ is a holomorphic vvaf. Moreover, we say that $\mathbb{X}(\tau)$ vanishes at the cusp ∞ if it has an expansion of the form

$$\mathbb{X}(\tau) = \sum_{\lambda \in R(t_\infty)} \sum_{j=0}^{m(\lambda)-1} (\log \widetilde{q})^j \sum_{n=1}^{\infty} \mathbb{X}_{[\lambda,j,n]} \widetilde{q}^{n+\mu(\lambda)}.$$

In other words, all of the associated $\widetilde{q}$-expansions of $\mathbb{X}(\tau)$ have exponential decay as the imaginary part of τ goes to ∞. Similarly, $\mathbb{X}(\tau)$ vanishes at the cusp $\mathfrak{c}$ if $\mathbb{X}|_k A_{\mathfrak{c}}$ vanishes at the cusp ∞, and therefore we say that $\mathbb{X}(\tau)$ is a vector-valued cusp form if $\mathbb{X}(\tau)$ vanishes at all cusps of G.

7.2 Growth for logarithmic vector-valued automorphic forms

In the previous chapter, we studied the growth of Fourier coefficients of admissible vector-valued automorphic forms. Recall that our definition included moderate growth for this case. We initiated the discussion about the logarithmic vvaf in Section 7.1. Now, we are not imposing the moderate growth condition in this general setting. In this case, we assume that all the eigenvalues of the image of each parabolic element are unitary.

7.2.1 Polynomial-growth of the representation

One of the big advantages of assuming ρ admissible was that, $\|\rho(t_{\mathfrak{c}}^n)\| = O_{\mathfrak{c}}(1)$, for any cusp $\mathfrak{c}$ of G and $n \in \mathbb{Z}$. However, the same may not hold when ρ is not admissible. We have the following lemma to overcome that obstacle.

Lemma 7.2.1. *For any integer $n \neq 0$, and any parabolic element $t_{\mathfrak{c}} \in$ G, we have the following estimate*

$$\|\rho(t_{\mathfrak{c}}^n)\| \ll_{\mathfrak{c},m} |n|^{m-1}.$$

Proof. Due to the assumption, we may assume that $\rho(t_{\mathfrak{c}})$ is conjugate to a matrix in the Jordan canonical form. Now it is enough to bound norms of the corresponding Jordan blocks. Let J_{m_t,λ_t} be one of such blocks. We can write

$$J_{m_t,\lambda_t}^n = \lambda_t^n (I_{m_t} + N)^n = \lambda_t^n \sum_{0 \leq i \leq m_t} \binom{n}{i} N^i,$$

because $N^i = 0$ for any $i \geq m_t$. In particular, we then have

$$\left\| J_{m_t,\lambda_t}^n \right\| \ll_{m_t} n^{m_t - 1},$$

because $|\lambda| = \|N\| = 1$ and $\sum_{0 \leq i \leq m_t - 1} \binom{n}{i} \ll_{m_t} n^{m_t-1}$. The result now follows by varying the Jordran blocks. □

We start with considering the decomposition of γ given by Beardon, as discussed in Section 6.1.2. We say that a parabolic element γ is a *parabolic generator*, if it is of the form $t_{\mathfrak{c}}$ for some cusp $\mathfrak{c}$ of G.

Lemma 7.2.2. *The product of the powers of the parabolic generators coming in the word $\gamma = C_1 C_2 \cdots C_s$ is at most $\|\gamma\|^{\alpha_1}$, for some constant α_1 depending on* G.

Proof. It follows from Lemma 6.1.4 that there exists a constant c such that whenever $|C_i| > c$, we have C_i is a product of a power of $t_{\mathfrak{c}}$, (where $\mathfrak{c}$ is a cusp of G) with an element coming from a finite subset G^* of G. In this case, $\|C_i\| \gg$ the power of $t_{\mathfrak{c}}$ appearing in C_i. On the other hand, the number of C_i with $|C_i| \leq c$ is bounded by $|\mathrm{G}^*|^c = O(1)$. In particular, all of the powers of parabolic elements appearing in such C_i's are also $O(1)$. Therefore, the desired product of the powers of the parabolic elements coming in γ is bounded by $O\left(\prod_{i,|C_i|>c} \|C_i\|\right)$. The proof is now complete by [12, Theorem 2]. □

Consequently, we have the following growth result on ρ. It is not hard to see that we do not have such a nice growth if images of some parabolic element have non-unitary eigenvalues.

Lemma 7.2.3. *Let $\gamma := \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{G}$ be an arbitrary element. Then we have that $\|\rho(\gamma)\| \ll (a^2+b^2+c^2+d^2)^{\alpha'}$, for some constant α' depending on* G.

Proof. We first consider the decomposition $\gamma = \prod_{i=1}^{s} C_i$ as given by Beardon, and obtain $\|\rho(\gamma)\| \leq \prod_{i=1}^{s} \|\rho(C_i)\|$. Once again, since G^* is finite, the terms with $|C_i| < c$ do not contribute much. On the other hand, following Lemma 6.1.4, $|C_i| > c$ implies that there exists a cusp $\mathfrak{c}_i$ of G such that C_i is a product of $t_{\mathfrak{c}_i}^{n_i}$ with an element from G^*. In particular, it follows from Lemma 7.2.1 that

$$\|\rho(C_i)\| \leq M_{\mathrm{G}} \left\|\rho(t_{\mathfrak{c}_i}^{n_i})\right\| \ll_{\mathfrak{c}_i, m} M_{\mathrm{G}} |n_i|^{m-1},$$

where M_{G} is the maximum of $\|\rho(\gamma)\|_{\gamma \in \mathrm{G}^*}$. Now each such $\mathfrak{c}_i$ is in fact a vertex of $\widehat{\mathrm{D}}_{\mathrm{G}}$, and also the rank m is fixed, hence we can actually write $\|\rho(C_i)\| \ll M_{\mathrm{G}} |n_i|^{m-1}$. We then have the following estimate

$$\|\rho(\gamma)\| \leq \prod_{i=1}^{s} \|\rho(C_i)\| \ll \prod_{i,|C_i|>c} \|\rho(C_i)\| \ll M_{\mathrm{G}}^{s} \prod_{\substack{i,|C_i|>c \\ t_{\mathfrak{c}_i}^{n_i} \in C_i}} |n_i|^{m-1}.$$

Now we get the desired bound by applying Lemma 7.2.2 and the bound $s = O(\log(a^2+b^2+c^2+d^2))$ from [12, Theorem 2].

□

7.2.2 Recipe to bridge two certain regions in $\mathbb{H}$

We need another ingredient to finish our preparation for the logarithmic case of Theorem 6.2.12. As in the proof of the admissible case, we shall need a relation between $|cz+d|^2$ and c^2+d^2, where (c,d) is the last row of a matrix in G. However, Lemma 7.2.3 gives a bound in terms of $a^2+b^2+c^2+d^2$. For this reason, it is useful to have an inequality of the form $a^2+b^2 \ll c^2+d^2$. We shall shortly see that there exists a region where vvaf has the desired growth, and the following result gives us an element of G, which serves as a bridge to the region $1 \leq x \leq h, 0 < y < 1$.

Lemma 7.2.4. *Let* $\gamma_0 = \left(\begin{smallmatrix} a_0 & b_0 \\ c_0 & d_0 \end{smallmatrix}\right)$ *with* $c_0 \neq 0$. *Let* $\gamma \in \mathrm{PSL}_2(\mathbb{R})$ *have rows* r_1 *and* r_2. *Let* $\tilde{\gamma} = \gamma_0\gamma$ *have rows* $\tilde{r}_1$ *and* $\tilde{r}_2$. *Then either* $\|r_1\| \leq \max\left\{1, 2\left|\frac{d_0}{c_0}\right|\right\}\|r_2\|$ *or* $\|\tilde{r}_1\| \leq 2\frac{|a_0|+|b_0|}{|c_0|}\|\tilde{r}_2\|$, *where* $\|\cdot\|$ *of the rows are defined as the usual norm in* $\mathbb{R}^2$.

Proof. Assume $\|r_1\| \geq \max\{1, 2\left|\frac{d_0}{c_0}\right|\}\|r_2\|$. From the definition of matrix multiplication, $\tilde{r}_1 = a_0r_1 + b_0r_2$ and $\tilde{r}_2 = c_0r_1 + d_0r_2$. From the triangle inequality,

$$\|\tilde{r}_1\| \leq |a_0| \cdot \|r_1\| + |b_0| \cdot \|r_2\| \leq (|a_0| + |b_0|)\|r_1\|. \tag{7.3}$$

Applying the triangle inequality, the hypothesis $\|r_1\| \geq 2\left|\frac{d_0}{c_0}\right|\|r_2\|$ and (7.3), give us

$$\|\tilde{r}_2\| \geq |c_0| \cdot \|r_1\| - |d_0| \cdot \|r_2\| \geq \frac{|c_0|}{2}\|r_1\| \geq \frac{1}{2} \cdot \frac{|c_0|}{|a_0| + |b_0|}\|\tilde{r}_1\|,$$

which is equivalent to the stated inequality. □

7.2.3 Proof of Theorem 1.3.1: logarithmic case

Let us consider the case when $\mathbb{X}(\tau)$ is a vector-valued cusp form. We claim that there exists $\gamma_0 = \left(\begin{smallmatrix} a_0 & b_0 \\ c_0 & d_0 \end{smallmatrix}\right) \in \mathrm{G}$ such that $c_0 > 0$ and $d_0 > 0$. The existence of a matrix $\gamma_1 = \left(\begin{smallmatrix} a_1 & b_1 \\ c_1 & d_1 \end{smallmatrix}\right)$ such that $c_1 \neq 0$ follows from [67, Theorem 1.5.4] and the assumption that G is a Fuchsian group of the first kind. Since we are in $\mathrm{PSL}_2(\mathbb{R})$ rather than in $\mathrm{SL}_2(\mathbb{R})$, we may assume $c_1 > 0$. Let n be so large that $d_1 + nhc_1 > 0$. Then we can take $\gamma_0 = \gamma_1 t_\infty^n = \left(\begin{smallmatrix} a_1 & b_1+nha_1 \\ c_1 & d_1+nhc_1 \end{smallmatrix}\right)$. From now on let us fix such a γ_0.

Consider $\mathrm{F_G}$ to be a fundamental domain of G that is union of the sets of type $\mathcal{S}(\mathfrak{c}, v_0, K)$,

$$\mathrm{G}_1 = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid \|r_1\| \leq \max\left\{1, 2\left|\frac{d_0}{c_0}\right|\right\}\|r_2\| \right\},$$

and denote $\mathbb{H}_1 = \mathrm{G}_1\mathbb{F}_\mathrm{G}$. The previous lemma, and (6.7) implies that for any $\tau \in \mathbb{H}_1$,

$$y^{k/2+\alpha'}\|\mathbb{X}(\tau)\| \ll v^{k/2-\alpha'}\|\mathbb{X}(z)\|, \tag{7.4}$$

where $\tau = \gamma z$ for some $\gamma \in \mathrm{G}_1$ and z is in the union of $\mathcal{S}(\mathfrak{c}, v_0, K)$'s. Since $\mathbb{X}$ is a vector-valued cusp form, all the $\widetilde{q}_\mathfrak{c}$-expansions associated to $\mathbb{X}|_k A_\mathfrak{c}$ decay

exponentially as the imaginary part of $A_{\mathfrak{c}}^{-1}z = \frac{1}{\mathfrak{c}-z} \to \infty$. On the other hand, $|\log \widetilde{q}_{\mathfrak{c}}|$ grows polynomially, as $\mathrm{Im}\left(\frac{1}{\mathfrak{c}-z}\right) \to \infty$ and $\mathrm{Re}\left(\frac{1}{\mathfrak{c}-z}\right)$ can be taken to be bounded. The maximum power of $\log \widetilde{q}_{\mathfrak{c}}$ appearing in the logarithmic expansion is at most $\dim(\rho)$, and it is clear that an extra polynomial factor does not affect the exponential decay of the logarithmic expansion. In particular, $\mathbb{X}|_k A_{\mathfrak{c}}$ decays exponentially as $y \to \infty$. Now arguing similarly as in Theorem 6.2.12, that is, by comparing $\mathbb{X}$ with $\mathbb{X}|_k A_{\mathfrak{c}}$, we get $y^{\beta}\,\|\mathbb{X}(z)\| = O(1)$ for any $z \in S(\mathfrak{c}, y_0, K)$ and real β. We now get $\|\mathbb{X}(\tau)\| \ll y^{-k/2-\alpha'}$ for any $\tau \in \mathbb{H}_1$ by taking $\beta = \alpha' + \frac{k}{2}$ in (7.4).

Now we compare $\mathbb{X}(\tau)$ with $\mathbb{X}(\gamma_0\tau)$ to see the growth in $\mathbb{H} \setminus \mathbb{H}_1$. Let $\tau = x+iy \in \mathbb{H} \setminus \mathbb{H}_1$, then using the functional equation,

$$\begin{aligned}
\|\mathbb{X}(\tau)\| &= |c_0\tau + d_0|^{-k} \|\rho(\gamma_0)^{-1}\mathbb{X}(\gamma_0\tau)\| \\
&\ll |c_0\tau + d_0|^{-k} (\mathrm{Im}\gamma_0\tau)^{-k/2-\alpha'} \\
&\ll |c_0\tau + d_0|^{-k} \left(\frac{y}{|c_0\tau + d_0|^2}\right)^{-k/2-\alpha'} \\
&\ll |c_0\tau + d_0|^{2\alpha'} y^{-k/2-\alpha'} \\
&\ll y^{-k/2-\alpha'},
\end{aligned}$$

for any $0 \le x \le h$ and $0 < y < 1$. In particular, $|\mathbb{X}_i(\tau)| \ll y^{-k/2-\alpha'}$ for all $0 \le i \le m-1$. Then it follows inductively from (7.2) that $|\widetilde{h}_{\lambda,j}(\tau)| \ll y^{-k/2-\alpha'}$, and in particular

$$|h_{i,j,\lambda}(\tau)|, \|h_{\lambda,j}(\tau)\| \ll y^{-k/2-\alpha'}, \tag{7.5}$$

for all $1 \le j \le m(\lambda)-1$, any eigenvalue λ of $\rho(t_\infty)$, and $0 \le x \le h$. Now note that

$$\left\|\mathbb{X}_{[\lambda,j,n]}\right\| \ll \frac{1}{h}\int_0^h \left\|h_{\lambda,j}(x+iy)\widetilde{q}^{(-n-\mu(\lambda))}\right\| dx,\ \forall\ 0 \le j \le m(\lambda)-1.$$

In particular, we then have

$$\left\|\mathbb{X}_{[\lambda,j,n]}\right\| \ll y^{-k/2-\alpha'} e^{2\pi y(n+\mu(\lambda))/h},\ \forall\ 0 \le j \le m(\lambda)-1.$$

Now, taking $y = \frac{1}{n+\mu(\lambda)}$ and setting α to be α' we get the desired result.

Let us now consider the holomorphic case. Similarly as in the previous case, we shall first show that $\mathbb{X}$ has polynomial-growth in $\mathbb{H}_1$. Consider a fundamental domain that is covered by finitely many sets of type $\mathcal{S}(\mathfrak{c}, y_0, K)$, where $\mathfrak{c}$ is a finite cusp of G not equivalent to ∞, and a region of type $\mathcal{S} = \{z \in \mathbb{H} \mid 0 \le u \le h, v > v_0\}$. From (6.5) we have for any $\tau \in \mathbb{H}_1$ that

$$y^{k+2\alpha'+m}\|\mathbb{X}(\tau)\| \ll |cz+d|^{-k-2\alpha'-2m}(1+4|z|^2)^{\alpha'} v^{k+m}\|\mathbb{X}(z)\| \tag{7.6}$$

where $\tau = \gamma z$, for some $\gamma \in \mathrm{G}$ and $z = u+iv$ lying in one of the sets $\mathcal{S}(\mathfrak{c}, y_0, K)$. Following the arguments given in the previous case, we have $v^{k+m}\|\mathbb{X}(z)\| = O(1)$. This is because, all $\widetilde{q}_{\mathfrak{c}}$-expansions of $\mathbb{X}|_k A_{\mathfrak{c}}$ are bounded near ∞ and the extra log

factor grows like $\mathrm{Im}\left(\frac{1}{\mathfrak{c}-z}\right) \sim v^{-1}$. It now follows immediately from Lemma 6.3.4 that $y^{k+2\alpha}\|\mathbb{X}(\tau)\|$ is bounded whenever z is in one of the sets $\mathcal{S}(\mathfrak{c}, v_0, K)$, where $\alpha = \alpha' + m$. On the other hand if z in $\mathcal{S}$, we have to be a little more careful because of the extra unbounded log factors coming in the Fourier expansion. From (7.6) it follows that

$$\begin{aligned} y^{k+2\alpha'+m}\|\mathbb{X}(\tau)\| &\ll v^{k+m}|cz+d|^{-k-2\alpha'-2m}(1+4|z|^2)^{\alpha'}\|\mathbb{X}(z)\| \\ &\ll v^{k+2m+2\alpha'}|cz+d|^{-k-2\alpha'-2m}v^{-m}\|\mathbb{X}(z)\|, \end{aligned}$$

as $\frac{1+4|z|^2}{v^2}$ is bounded. Now note that $v^{-m}\|\mathbb{X}(z)\| = O(1)$ in $\mathcal{S}$ because the $h_{\lambda,j}$'s from (7.1) are bounded in $\mathcal{S}, |\log z| = O(y)$ and the maximum power of log appearing in the expansion of $\mathbb{X}(\tau)$ goes up to at most m. Thus, if $k + 2\alpha' + 2m \geq 0$ and $y < v_0$, we have $y^{k+2\alpha'+m}\|\mathbb{X}(\tau)\| \ll 1$ as in the admissible case.

We now need to relate $\mathbb{H}_1$ with $\mathbb{H}$, and for that, we are again going to rely on the comparison of $\mathbb{X}(\tau)$ with $\mathbb{X}(\gamma_0\tau)$. Note that we have estimated $\mathbb{X}(\tau)$ only at the points of $\mathbb{H}_1$ with small imaginary part. So we need to ensure that $\mathrm{Im}\gamma_0\tau = \frac{y}{|c_0\tau+d_0|^2}$ is small. This happens when $0 \leq x \leq h$ and y is small, because then $|c_0\tau + d_0| \geq \mathrm{Re}(c_0\tau + d_0) \geq d_0$ by our choice of γ_0. Arguing similarly as in the previous case, we have that for any $\tau = x + iy \in \mathbb{H} \setminus \mathbb{H}_1$,

$$\|\mathbb{X}(\tau)\| \ll y^{-k-2\alpha'-m},$$

provided τ is bounded. Performing the integration, we get the desired result by the same choice of α. This completes the proof of parts (i) and (ii).

For part (iii), we may assume that $k+2\alpha'+m < 0$. If we have also $k+2\alpha'+2m \geq 0$, the previous argument gives $\|\mathbb{X}(\tau)\| \ll y^{-k-2\alpha'-m}$, so $\mathbb{X}(\tau) \to 0$ as $y \to 0$ with $0 \leq x \leq h$. If $k+2\alpha'+2m < 0$, let $\tilde{\alpha}$ solve the equation $k+2\tilde{\alpha}+2m = 0$. Then we can apply the same argument with $\tilde{\alpha}$ instead of α'. We get $\|\mathbb{X}(\tau)\| \ll y^{-k-2\tilde{\alpha}-m} = y^m$, which also approaches to 0 as $y \to 0$. Now we obtain $\mathbb{X} \equiv 0$ as in the admissible case. □

7.3 Growth of the representations

In both admissible and logarithmic cases of Theorem 1.3.1, we required a unitary condition on the eigenvalues to get a Fourier expansion. One of the consequences of this condition is that the corresponding representation has polynomial-growth. By polynomial-growth, we mean: the existence of a constant α such that $\|\rho(\gamma)\| \ll \|\gamma\|^{\alpha}$ for any γ in the group G. In this section, we want to see when a given representation has polynomial-growth, and what happens to the growth of vector-valued holomorphic function $\mathbb{X}$ on $\mathbb{H}$ which satisfies the functional equation $\mathbb{X}|_k\gamma = \rho(\gamma)\mathbb{X}, \forall\gamma \in \mathrm{G}$, for the given representation ρ.

7.3.1 On polynomial-growth

We have the following criteria for polynomial-growth of ρ, which basically says that it is enough to look over only the set of parabolic elements.

Proposition 7.3.1. *Let* G *be a Fuchsian group of the first kind and* $\rho : \mathrm{G} \to \mathrm{GL}_m(\mathbb{C})$ *be a representation. Then* ρ *has polynomial-growth if and only if all the eigenvalues of the image of each parabolic element are unitary.*

Proof. Suppose that all the eigenvalues of the image of each parabolic are unitary, then we get the polynomial-growth immediately from Lemma 7.2.3. Now for the other direction, take $\gamma \in \mathrm{G}$ to be a parabolic element such that at least one eigenvalue of $\rho(\gamma)$ is non-unitary. Note that γ is conjugate to an element of the form $\left(\begin{smallmatrix} 1 & mh \\ 0 & 1 \end{smallmatrix}\right)$ and in particular $\|\gamma^n\| \ll |n|$. It now follows from the computation with Jordan canonical form as in the proof of Lemma 7.2.2 that $\|\rho(\gamma^n)\| \geq r^n$, for any $n \in \mathbb{Z}$, where r can be taken to be the norm of any eigenvalue of $\rho(\gamma)$. This gives a contradiction. □

We now have an interesting consequence: the polynomial-growth is preserved under induction, restriction, and isomorphism.

Corollary 7.3.2. *Let* $\mathrm{H} \subseteq \mathrm{G}$ *be two Fuchsian groups of the first kind and* H *has finite index in* G*. Then* ρ *has polynomial-growth if and only if the induced representation* $\tilde{\rho} := \mathrm{Ind}_{\mathrm{H}}^{\mathrm{G}}(\rho)$ *has polynomial-growth.*

For the definition and the details on induced representation and their associated vector-valued automorphic forms, see Sections 3 and 4 of [7]. Let us recall the definition of $\tilde{\rho}$. Write $\mathrm{G} = \gamma_1\mathrm{H} \cup \gamma_2\mathrm{H} \cup \cdots \cup \gamma_d\mathrm{H}$, where d is the index of H in G. Without loss of generality, we may assume that $\gamma_1 = 1$. The representation $\rho : \mathrm{H} \to \mathrm{GL}_m(\mathbb{C})$ can be extended to a function on all of G, i.e. $\rho : \mathrm{G} \to \mathrm{M}_m(\mathbb{C})$ by setting $\rho(x) = 0, \forall x \notin \mathrm{H}$ where $\mathrm{M}_m(\mathbb{C})$ is the set of all $m \times m$ matrices over $\mathbb{C}$. The induced representation $\tilde{\rho} : \mathrm{G} \to \mathrm{GL}_{dm}(\mathbb{C})$ is defined by

$$\tilde{\rho}(x) = \begin{pmatrix} \rho(\gamma_1^{-1}x\gamma_1) & \rho(\gamma_1^{-1}x\gamma_2) & \dots & \rho(\gamma_1^{-1}x\gamma_d) \\ \rho(\gamma_2^{-1}x\gamma_1) & \rho(\gamma_2^{-1}x\gamma_2) & \dots & \rho(\gamma_2^{-1}x\gamma_d) \\ \vdots & \vdots & \ddots & \vdots \\ \rho(\gamma_d^{-1}x\gamma_1) & \rho(\gamma_d^{-1}x\gamma_2) & \dots & \rho(\gamma_d^{-1}x\gamma_d) \end{pmatrix}, \quad \forall x \in \mathrm{G}. \tag{7.7}$$

Now for any $x \in \mathrm{G}$ and $\forall 1 \leq i \leq m$, there exists a unique $1 \leq j \leq m$ such that $\rho(\gamma_i^{-1}x\gamma_j) \neq 0$. Therefore, exactly one nonzero $m \times m$ block appear in every row and every column of (7.7).

Proof of Corollary 7.3.2. Due to Proposition 7.3.1 we now know that a representation has polynomial-growth if and only if, every eigenvalue of image of each parabolic element is unitary. We shall prove this result with respect to this unitary property.

Restriction invariant is an immediate consequence. Now if ρ_1 and ρ_2 are isomorphic representations, then $\rho_1(\gamma)$ is conjugate to $\rho_2(\gamma)$ for each element $\gamma \in \mathrm{G}$.

In particular, all the eigenvalues of $\rho_1(\gamma)$ are unitary if and only if, all the eigenvalues of $\rho_2(\gamma)$ are unitary.

For the induction invariance, let $\tilde{\rho}$ be the induced representation of ρ with respect to a choice of the coset representatives $\gamma_1, \ldots, \gamma_d$ of H in G, where d is the index of H in G. Let $\gamma \in$ G be a parabolic element. Then, for each i, some non-trivial power of $g_i = \gamma_i^{-1}\gamma\gamma_i$ is in H. This can be shown from the existence of $n_{i,1}$ and $n_{i,2}$ such that $g_i^{n_{i,1}}\mathrm{H} = g_i^{n_{i,2}}\mathrm{H}$, say the n_i^{th}- power. Then $\gamma_i^{-1}\gamma^N\gamma_i \in$ G for each i, where $N = \mathrm{lcm}\{n_i\}$. In particular, $\tilde{\rho}(\gamma^N)$ is a block diagonal matrix whose blocks are of the form $\rho(\gamma_i^{-1}\gamma^N\gamma_i)$. If ρ has polynomial-growth, then each such block consists of the unitary eigenvalues, and in particular all the eigenvalues of $\tilde{\rho}(\gamma^N)$ are unitary. Moreover, the eigenvalues of $\tilde{\rho}(\gamma)$ are N^{th} roots of the eigenvalues of $\tilde{\rho}(\gamma^N)$, as one can see from the Jordan canonical form of $\tilde{\rho}(\gamma)$. Therefore, all the eigenvalues of $\tilde{\rho}(\gamma)$ are unitary, and hence $\tilde{\rho}$ has polynomial-growth.

On the other hand suppose that $\tilde{\rho}$ has polynomial-growth. Take an element $\gamma_0 \in$ H, and it is enough to show that every eigenvalue of $\rho(\gamma_0)$ is unitary. It follows from the discussion in the previous paragraph that, there exists N such that $\tilde{\rho}(\gamma_0^N)$ is a block diagonal matrix. Moreover, one of the block is $\rho(\gamma_0^N)$ since one of the representative can be taken to be the identity element of H. In particular, $\rho(\gamma_0^N)$ has only unitary eigenvalues, and so does $\rho(\gamma_0)$, as desired. □

7.3.2 On a sharp polynomial-growth for finite index subgroups of $\mathrm{PSL}_2(\mathbb{Z})$

In Lemma 7.2.3 we had a polynomial-growth on the representation involving all the entries, while in Lemma 6.3.2 the bound only involved the bottom row. The difference is that, in the admissible case, for any parabolic element $\gamma \in$ G, $\|\rho(\gamma^n)\|$ is bounded irrespective of n. To improve Lemma 7.2.3 we need to control the number of times parabolic elements appear when we decompose an element of G. For example, when we take G to be a finite index subgroup of $\mathrm{PSL}_2(\mathbb{Z})$, we have a better control.

Proposition 7.3.3. *Let* G *be the finite index subgroup of* $\mathrm{PSL}_2(\mathbb{Z})$, *and* ρ *be a representation of* G *such that, any eigenvalue in the image of each parabolic element is unitary. Then we have,*

$$\|\rho(\gamma)\| \ll (c^2+d^2)^{\alpha} \max\left\{[|a/c|]^{m-1}, 1\right\}, \ \forall \gamma \in \mathrm{G}.$$

Proof. First consider the induced representation $\tilde{\rho}$ of ρ to $\mathrm{PSL}_2(\mathbb{Z})$. It follows from the proof of Corollary 7.3.2 that, image of each parabolic element under this induced representation have only unitary eigenvalues. Take an element $\gamma \in \mathrm{G} \subseteq \mathrm{PSL}_2(\mathbb{Z})$. We start with writing $\gamma = (st^{l_{v+1}})(st^{l_v})\cdots(st^{l_1})(st^{l_0})$ with $s = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right), t = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, as in [54, Lemma 3.1]. Using Corollary 3.5 and the estimate of l_v from [54, Lemma 3.1], we get $\|\tilde{\rho}(\gamma)\| \ll (c^2+d^2)^{\alpha} \max\left\{[|a/c|]^{m-1}, 1\right\}$. Since $\|\rho(\gamma)\| \leq \|\tilde{\rho}(\gamma)\|$, the result follows.

□

Therefore we indeed have a better growth for finite index subgroups of $\mathrm{PSL}_2(\mathbb{Z})$ at least when $c \neq 0$, in the sense that the bound does not involve one of the entries

of γ. When $c = 0$, the element γ is parabolic. In that case, one can get a bound from Lemma 7.2.1.

Example of a representation with non polynomial-growth

There exists a G and a representation ρ of it such that ρ does not have polynomial-growth. For instance, consider $\mathrm{G} = \mathrm{PSL}_2(\mathbb{Z})$ and $\rho : \mathrm{G} \to \mathrm{GL}_3(\mathbb{C})$ given by

$$\rho(s) = \begin{pmatrix} a & -(a+1) & 1 \\ a-1 & -a & 1 \\ 0 & 0 & 1 \end{pmatrix}, \ \rho(t) = \mathrm{diag}(\lambda_1, \lambda_2, \lambda_3),$$

where $a, \lambda_1, \lambda_2, \lambda_3$ are yet to be chosen. See [26, Section 2.1] for a proof of ρ being a representation, provided that $\lambda_1\lambda_2 = -\lambda_3^2$, $\frac{\lambda_1\lambda_2}{(\lambda_1-\lambda_2)^2} = -a^2$ and $\frac{1}{\lambda_1\lambda_2(\lambda_1-\lambda_2)} = a$. We can make sure that these conditions hold by taking $\lambda_1, \lambda_2, \lambda_3$ as follows: take $\lambda_3 = 1$ and λ_1, λ_2 in such a way, so that $\lambda_1\lambda_2 = -1$ and $\lambda_1 - \lambda_2 = -\frac{1}{a}$. We want to make one of λ_1 or λ_2 non-unitary, which we can ensure by taking any purely imaginary a.

Example of a representation with polynomial-growth

Consider

$$\mathbb{X}(\tau) = \frac{1}{\eta(\tau)} \begin{pmatrix} \theta_2(\tau) \\ \theta_3(\tau) \\ \theta_4(\tau) \end{pmatrix},$$

where $\theta_2(\tau), \theta_3(\tau), \theta_4(\tau)$ and $\eta(\tau)$ are well known weight $1/2$ scalar-valued modular forms. For a complete description of these functions, the reader may refer to [55]. It turns out that $\mathbb{X}(\tau)$ is a vector-valued modular function of $\mathrm{PSL}_2(\mathbb{Z})$ and representation ρ where $\rho : \mathrm{PSL}_2(\mathbb{Z}) \to \mathrm{GL}_3(\mathbb{C})$ is a rank 3 representation of $\Gamma(1)$ given by

$$\rho(s) = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \text{ and } \rho(t) = \begin{pmatrix} \exp(\frac{\pi \mathrm{i}}{6}) & 0 & 0 \\ 0 & 0 & \exp(-\frac{\pi \mathrm{i}}{12}) \\ 0 & \exp(-\frac{\pi \mathrm{i}}{12}) & 0 \end{pmatrix}.$$

To see whether ρ has polynomial-growth, it is enough to check the eigenvalues of $\rho(t)$. In this case, they are given by $\exp(\frac{\pi \mathrm{i}}{6}), \exp(-\frac{\pi \mathrm{i}}{12})$ and $-\exp(-\frac{\pi \mathrm{i}}{12})$. In particular, ρ has polynomial-growth in this case.

7.3.3 A consequence of polynomial-growth

In Theorem 6.2.12, we achieved polynomial-growth of the Fourier coefficients by showing a bound of the form $\|\mathbb{X}(\tau)\| \ll y^{-k-2\alpha}$ when $\mathbb{X}(\tau)$ is a holomorphic vvaf. In this process, polynomial-growth of the associated representation ρ played a crucial role. We obtained such a growth of ρ assuming that all the images of the parabolic elements have only unitary eigenvalues. However, even if we do not have this assumption, we could still consider a vector-valued holomorphic function $\mathbb{X} : \mathbb{H} \to \mathbb{C}^m$ which satisfies the functional behavior, that is $\mathbb{X}|_k\gamma = \rho(\gamma)\mathbb{X}, \ \forall \gamma \in \mathrm{G}$. In this more general situation, one may naturally ask whether we still have a polynomial-growth for $\mathbb{X}(\tau)$. To answer this question, we prove the following.

Theorem 7.3.4 (Bajpai, Bhakta, Finder)**.** *Let* G *be a non-cocompact Fuchsian group of the first kind,* $\mathbb{X} : \mathbb{H} \to \mathbb{C}^m$ *be a vector-valued holomorphic function, and* $\rho : \mathrm{G} \to \mathrm{GL}_m(\mathbb{C})$ *be a representation. Suppose that* $\mathbb{X}$ *is non-zero, and* $\mathbb{X}(\gamma\tau) = (c\tau + d)^k \rho(\gamma)\mathbb{X}(\tau), \forall \gamma \in \mathrm{G}, \tau \in \mathbb{H}$*, where* $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$*. Then, we have the following.*

(i) If ρ *is irreducible and there exists a constant* $\zeta > 0$ *such that* $\|\mathbb{X}(x+iy)\| \ll y^{-\zeta}$ *for all* $x + iy \in \mathbb{H}$*, then*

$$\|\rho(\gamma)\| \ll \|\gamma\|^{2\zeta - k}, \ \forall \gamma \in \mathrm{G}.$$

(ii) More generally, if ρ *is irreducible and* $\|\mathbb{X}(x+iy)\| \ll \max_{0 \le j \le m-1}\{|x + iy|^j y^{-\zeta}\}$ *for all* $x + iy \in \mathbb{H}$*, then*

$$\|\rho(\gamma)\| \ll \max\{\|\gamma\|^{j+2\zeta-k}\}_{0 \le j \le m-1}, \ \forall \gamma \in \mathrm{G}.$$

(iii) If ρ *is not necessarily irreducible, then some subrepresentation* ρ' *of* ρ *must have a similar growth. In particular, if* ρ *is decomposable, then some of the irreducible components of* ρ *have similar growth.*

Proof of Theorem 7.3.4. Let us first consider the space $\mathcal{W} = \mathrm{Span}_{\mathbb{C}} \{\mathbb{X}(\tau) \mid \tau \in \mathbb{H}\}$. Of course, here in $\mathcal{W}$, we are taking finite linear combinations of $\mathbb{X}(\tau)$ over $\mathbb{C}$. Moreover $\mathcal{W}$ is a non-zero proper vector-subspace of $\mathbb{C}^m$, since $\mathbb{X}$ is a non-zero holomorphic function $\mathbb{H}$. We now want to show that $\mathcal{W}$ is a representation of ρ. For this, we use the functional equation $j(\gamma, \tau)^{-k}\mathbb{X}(\gamma\tau) = \rho(\gamma)\mathbb{X}(\tau)$, and note that $j(\gamma, \tau) \neq 0$ for any $\gamma \in \mathrm{G}, \tau \in \mathbb{H}$. In particular, we have an action of G on $\mathcal{W}$ given by ρ. Therefore, $\mathcal{W}$ can be considered as a subrepresentation of ρ. Let us first prove (i). In this case ρ is irreducible, and $\mathbb{X}(\tau)$ is a non-zero function, therefore $\mathcal{W}$ is isomorphic to $\mathbb{C}^m$. Let us now fix a basis $\{\mathbb{X}(\tau_1), \mathbb{X}(\tau_2), \cdots, \mathbb{X}(\tau_m)\}$ of $\mathcal{W}$. We then have the following estimate for part (i).

$$\begin{aligned}
\|\rho(\gamma)\| \ll \sup\left\{\frac{\|\rho(\gamma)\mathbb{X}(\tau_i)\|}{\|\mathbb{X}(\tau_i)\|}\right\}_{1 \le i \le m} &= \sup\left\{\frac{|c\tau_i + d|^{-k}\,\|\mathbb{X}(\gamma\tau_i)\|}{\|\mathbb{X}(\tau_i)\|}\right\}_{1 \le i \le m} \\
&\ll \sup\left\{\frac{|c\tau_i + d|^{-k}|\mathrm{Im}(\gamma\tau_i)|^{-\zeta}}{\|\mathbb{X}(\tau_i)\|}\right\}_{1 \le i \le m} \\
&\ll \sup\left\{\frac{|c\tau_i + d|^{2\zeta-k}|\mathrm{Im}(\tau_i)|^{-\zeta}}{\|\mathbb{X}(\tau_i)\|}\right\}_{1 \le i \le m} \\
&\ll |c^2 + d^2|^{\zeta - k/2} \ll \|\gamma\|^{2\zeta-k},
\end{aligned}$$

where we are writing $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. On the other hand, for part (ii), using the bound

$\|X(x+iy)\| \ll \max_{0\leq j\leq m-1}\{|x+iy|^j y^{-\zeta}\}$, we have the following estimate

$$\begin{aligned}\|\rho(\gamma)\| \ll \sup\left\{\frac{\|\rho(\gamma)\mathbb{X}(\tau_i)\|}{\|\mathbb{X}(\tau_i)\|}\right\}_{1\leq i\leq m} &= \sup\left\{\frac{|c\tau_i+d|^{-k}\,\|\mathbb{X}(\gamma\tau_i)\|}{\|\mathbb{X}(\tau_i)\|}\right\}_{1\leq i\leq m}\\ &\ll \sup\left\{\frac{|c\tau_i+d|^{-k}|\gamma\tau_i|^j|\mathrm{Im}(\gamma\tau_i)|^{-\zeta}}{\|\mathbb{X}(\tau_i)\|}\right\}_{\substack{0\leq j\leq m-1\\ 1\leq i\leq m}}\\ &\ll \sup\left\{\frac{|c\tau_i+d|^{2\zeta-k}\,\|\gamma\|^j}{\|\mathbb{X}(\tau_i)\|}\right\}_{\substack{0\leq j\leq m-1\\ 1\leq i\leq m}}\\ &\ll \max\{\|\gamma\|^{j+2\zeta-k}\}_{0\leq j\leq m-1}.\end{aligned}$$

Now for part (iii), if $\mathcal{W}=\mathbb{C}^m$, then we are done. If not, then $\mathcal{W}$ is a non-trivial subrepresentation of $\mathbb{C}^m$ because $\mathbb{X}$ is a non-zero function. By the same argument as in part (i), the subrepresentation $\rho|_{\mathcal{W}}$ of ρ has a similar growth.

In particular when ρ is decomposable, we can consider a basis of $\mathbb{C}^m$, of the form $\{\mathbb{X}(\tau_1),\mathbb{X}(\tau_2),\cdots,\mathbb{X}(\tau_{m'}),v_{m'+1},\cdots v_m\}$. Then the block of ρ corresponding to $\{\mathbb{X}(\tau_1),\mathbb{X}(\tau_2),\cdots,\mathbb{X}(\tau_{m'})\}$ has a similar polynomial-growth, following the same argument as in the irreducible case. □

Remark 7.3.5. Part (a) of Theorem 7.3.4 could be considered as a converse statement to the admissible case of Theorem 6.2.12, and part (b) to the general logarithmic case.vTheorem 7.3.4 is meaningful if there exists at least one case where the associated representation does not have polynomial-growth, and a non-trivial holomorphic function on $\mathbb{H}$ satisfies the corresponding functional equation. We could then say such a holomorphic function does not have polynomial-growth. For instance, let us consider $\mathrm{G}=\Gamma(2)$, where

$$\Gamma(2)=\left\langle \gamma_1,\gamma_2,\gamma_3\in \mathrm{PSL}_2(\mathbb{Z}) \;\middle|\; \gamma_1\gamma_2\gamma_3=1\right\rangle$$

and

$$\gamma_1=\pm\begin{pmatrix}3 & 2\\ -2 & -1\end{pmatrix},\ \gamma_2=\pm\begin{pmatrix}1 & 0\\ -2 & 1\end{pmatrix},\ \gamma_3=\begin{pmatrix}1 & 2\\ 0 & 1\end{pmatrix}.$$

Let ρ be a representation for $\Gamma(2)$ defined by

$$\rho(\gamma_3)=\begin{pmatrix}1 & 0\\ 0 & 2\end{pmatrix},\rho(\gamma_2)=\begin{pmatrix}1 & 0\\ 0 & \frac{1}{2}\end{pmatrix},\rho(\gamma_1)=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}.$$

Then consider the vvaf $\mathbb{X}(\tau)=\begin{pmatrix}f\\ 0\end{pmatrix}$, for any modular form f for $\Gamma(2)$ associated to the trivial character.

Given any representation of any Fuchsian group of the first kind without having polynomial-growth, we expect it is possible to construct a vector-valued holomorphic function that satisfies the functional property.

7.4 Properties of the lifted vector-valued automorphic forms

In this section, we shall recall the induction of representations and introduce vvaf associated to them. We closely follow [7] throughout this section and develop the main tools to prove the main results of this article. Let us first recall our setup: G is a Fuchsian group of the first kind, and H is a finite index subgroup, say d, of G.

7.4.1 A special choice of the representatives

Fix any cusp $\mathfrak{c} \in \widehat{\mathfrak{C}}_{\mathrm{G}}$ and let $\mathfrak{c}_1, \cdots, \mathfrak{c}_{\mathfrak{n}_\mathfrak{c}}$ be the representatives of the H-inequivalent cusps which are G-equivalent to the cusp $\mathfrak{c}$, so we have

$$\mathrm{G} \cdot \mathfrak{c} = \bigcup_{i=1}^{\mathfrak{n}_\mathfrak{c}} \mathrm{H} \cdot \mathfrak{c}_i.$$

Therefore, for each i we get an $A_i \in \mathrm{G}$ with $A_i(\mathfrak{c}) = \mathfrak{c}_i$. Let us denote $k_\mathfrak{c}$ be the cusp width of $\mathfrak{c}$ in G and $h_{\mathfrak{c}_i}$ be the cusp width of $\mathfrak{c}_i$ in H. Then a set of coset representatives of H in G can be taken to be $g_{ij} = t_\mathfrak{c}^j A_i^{-1}$ for all $1 \leq i \leq n_\mathfrak{c}$ and $0 \leq j < h_i$, where $h_i = \frac{h_{\mathfrak{c}_i}}{k_\mathfrak{c}} \in \mathbb{Z}$. It turns out that, $\sum_{1 \leq i \leq n_\infty} h_i = d$.

Let ρ be a representation of rank m associated to H, and denote $\widetilde{\rho} := \mathrm{Ind}_{\mathrm{H}}^{\mathrm{G}}(\rho)$ to be the induction of ρ. With the choice of coset representatives $\{g_{i,j}\}$ of H in G as described above, we can write $\widetilde{\rho}(t_\mathfrak{c})$ in the block diagonal form, where each block is of size $mh_i \times mh_i$, $\forall\ 1 \leq i \leq n_\mathfrak{c}$. Moreover, these blocks are in the lower-diagonal form whose right top block is $\rho(t_i)$, and all other blocks are in the lower diagonal entry is $I_{m\times m}$. More precisely, it is of the form

$$\begin{pmatrix} 0 & & & \rho(t_i) \\ I & \ddots & & \\ & \ddots & \ddots & \\ & & I & 0 \end{pmatrix}_{mh_i \times mh_i},$$

where $t_i = A_i t_\mathfrak{c}^{h_i} A_i^{-1}$ is the generator of the stabilizer $\mathrm{H}_{\mathfrak{c}_i}$ in H. For a proof of this, the reader may refer to (4.3) in [7].

7.4.2 Lifting of vector-valued automorphic forms

Let H, G and ρ be as in the previous section, and $\mathbb{X}(\tau)$ be a vvaf associated to (ρ, H). Since H has finite index in G, one can take the similar set of representatives $\{g_{i,j}\}$ of H in G.

Now one may ask for an induced form $\widetilde{X}(\tau)$, which is also a vvaf associated to $\widetilde{\rho}$. Fix a cusp $\mathfrak{c}$ of G and let $\{g_{i,j}\}$ be the set of coset representatives of H in G, as described earlier. We then define the induced function $\widetilde{\mathbb{X}}^{(\mathfrak{c})} : \mathbb{H} \to \mathbb{C}^{dm}$ by setting,

$$\tau \mapsto \left(\mathbb{X}(g_{i,j}^{-1}\tau)\right)^{\mathrm{t}}_{\substack{1 \leq i \leq n_\mathfrak{c} \\ 0 \leq j < h_i}}.$$

The reader can note that, given any cusp $\mathfrak{c}$ of G, we are uniquely lifting the vvaf $\mathbb{X}(\tau)$ to $\widetilde{\mathbb{X}}^{(\mathfrak{c})}(\tau)$, because $g_{i,j}$ are well defined. Of course, $\widetilde{\mathbb{X}}^{(\mathfrak{c})}(\tau)$ is just a vector-valued holomorphic function on $\mathbb{H}$ right now, because $\mathbb{X}(\tau)$ is a vvaf. To make sure that $\widetilde{\mathbb{X}}^{(\mathfrak{c})}(\tau)$ is a vvaf (be it admissible or logarithmic), we first need to check the functional equation with respect to the induced representation $\widetilde{\rho}$. Note that,

$$\widetilde{\mathbb{X}}^{(\mathfrak{c})}(\gamma\tau) = \begin{pmatrix} \mathbb{X}(\gamma_1^{-1}\gamma\tau) \\ \mathbb{X}(\gamma_2^{-1}\gamma\tau) \\ \vdots \\ \mathbb{X}(\gamma_d^{-1}\gamma\tau) \end{pmatrix} = \begin{pmatrix} \mathbb{X}(\gamma_1^{-1}\gamma\gamma_{j_1}\gamma_{j_1}^{-1}\tau) \\ \mathbb{X}(\gamma_2^{-1}\gamma\gamma_{j_2}\gamma_{j_2}^{-1}\tau) \\ \vdots \\ \mathbb{X}(\gamma_d^{-1}\gamma\gamma_{j_d}\gamma_{j_d}^{-1}\tau) \end{pmatrix}$$
$$= \begin{pmatrix} j(\gamma_1^{-1}\gamma\gamma_{j_1},\tau)^k\rho(\gamma_1^{-1}\gamma\gamma_{j_1})\mathbb{X}(\gamma_{j_1}^{-1}\tau) \\ j(\gamma_2^{-1}\gamma\gamma_{j_2},\tau)^k\rho(\gamma_2^{-1}\gamma\gamma_{j_2})\mathbb{X}(\gamma_{j_2}^{-1}\tau) \\ \vdots \\ j(\gamma_d^{-1}\gamma\gamma_{j_d},\tau)^k\rho(\gamma_d^{-1}\gamma\gamma_{j_d})\mathbb{X}(\gamma_{j_d}^{-1}\tau) \end{pmatrix},$$

where $\{\gamma_i | 1 \leq i \leq d\}$ is the set $\{g_{i,j} | 1 \leq i \leq n_{\mathfrak{c}}, 0 \leq j < h_i\}$. To satisfy the functional equation property, we need that

$$j(\gamma_i^{-1}\gamma\gamma_{j_i},\tau)^k = j(\gamma,\tau)^k,\ \forall\ 1 \leq i \leq d, \gamma \in \mathrm{G}.$$

We can make sure this if, $r_2(\gamma_i^{-1}\gamma\gamma_{j_i}) = r_2(\gamma),\ \forall\ 1 \leq i \leq d,\ \gamma \in \mathrm{G}$, or simply if the weight $k = 0$, where $r_2(\cdot)$ denotes the second row of the corresponding matrix. Of course, it is unlikely that $r_2(\gamma_i^{-1}\gamma\gamma_{j_i}) = r_2(\gamma),\ \forall\ 1 \leq i \leq d,\ \gamma \in \mathrm{G}$ would always hold. So to be on the safer side, we simply stick to the weight $k = 0$ case to ensure that the functional equation is satisfied. Before discussing the moderate growth condition, let us define a suitable lift for any arbitrary weight case. Let us first recall a reduction trick introduced in [7]. The idea is to find a scalar-valued cusp form $\Delta_{\mathrm{G}}(\tau)$ of non-zero weight, which is holomorphic on $\mathbb{H}^*_{\mathrm{G}}$ and nonzero everywhere, except at ∞. For instance if G is given by the modular group $\mathrm{PSL}_2(\mathbb{Z})$, then one can take

$$\Delta_{\mathrm{G}}(\tau) = (\eta(\tau))^{24} = q\prod_{n\geq 1}(1-q^n)^{24},$$

where $\eta(\tau)$ is the Dedekind eta function. For the existence in the general case, the reader may look at the exposition in [7, Section 4].

Now given any admissible or logarithmic vvaf $\mathbb{X}(\tau)$ of weight k, let us denote $\mathbb{X}_0(\tau) = \Delta_{\mathrm{H}}^{-k/w_{\mathrm{H}}}(\tau)\mathbb{X}(\tau)$, where w_{H} is the weight of $\Delta_{\mathrm{H}}(\tau)$. It is clear that, $\mathbb{X}_0(\tau)$ is a vvaf of weight 0, associated to the representation $\rho \otimes \nu_{\mathrm{H}}^{-k}$, where ν_{H} is the rank 1 representation associated to $\Delta_{\mathrm{H}}^{1/w_{\mathrm{H}}}(\tau)$. One can then consider a reduction to a weight 0 automorphic form by $\mathbb{X}(\tau) \mapsto \mathbb{X}_0(\tau)$. In particular, we now have a recipe to lift to a vvaf of arbitrary weight, by considering the map

$$\mathbb{X}(\tau) \mapsto \mathbb{X}_0(\tau) \mapsto \widetilde{\mathbb{X}_0}^{(\mathfrak{c})}(\tau)\Delta_{\mathrm{G}}^{k/w_{\mathrm{G}}}(\tau) := \Delta_{\mathrm{G}}^{k/w_{\mathrm{G}}}(\tau)\Big(\mathbb{X}_0(g_{i,j}^{-1}\tau)\Big)^{\mathrm{t}}_{\substack{1\leq i\leq n_{\mathfrak{c}}\\ 0\leq j<h_i}}.$$

Note that $\widetilde{\mathbb{X}_0}^{(\mathfrak{c})}(\tau)\Delta_{\mathrm{G}}^{k/w_{\mathrm{G}}}(\tau)$ satisfies the functional equation with respect to the representation $\widetilde{(\rho\otimes\nu_{\mathrm{H}})}^{-k}\otimes\nu_{\mathrm{G}}^{k}=\widetilde{\rho}$. Therefore, we refine our definition of lift by setting

$$\widetilde{\mathbb{X}}^{(\mathfrak{c})}(\tau):=\widetilde{\mathbb{X}_0}^{(\mathfrak{c})}(\tau)\Delta_{\mathrm{G}}^{k/w_{\mathrm{G}}}(\tau).$$

If ∞ is a cusp of G, then we set $\widetilde{\mathbb{X}}(\tau):=\widetilde{\mathbb{X}}^{(\infty)}(\tau)$ as the definition of lifted form. If not, we pick any cusp $\mathfrak{c}$ of G and set $\widetilde{\mathbb{X}}(\tau):=\widetilde{\mathbb{X}}^{(\mathfrak{c})}|_k A_{\mathfrak{c}}(\tau)$, which satisfies the required functional equation with respect to the representation $A_{\mathfrak{c}}^{-1}\gamma A_{\mathfrak{c}}\mapsto\widetilde{\rho}(\gamma)$.

7.4.3 Preservation of the cuspidal properties

Before studying the behavior at the cusps, we first need to have a better understanding of the representatives of H in G. Suppose that ∞ is a cusp of G and $\{\mathfrak{c}_i|1\leq i\leq n_\infty\}$ are the cusps of H lying under ∞, and $\{g_{i,j}\}$ be the set of coset representatives of H in G as described before, with the important property that, $g_{i,j}(\mathfrak{c}_i)=\infty$. The following lemma is about a comparison with the set of all coset representatives $\{g_{i,j}|1\leq i\leq n_\infty, 0\leq j<h_i\}$ inside G and the set $\{A_{\mathfrak{c}_i}|1\leq i\leq n_\infty\}$ inside $\mathrm{PSL}_2(\mathbb{R})$.

Lemma 7.4.1. *There exists $a_{i,j}$ and $\alpha_{i,j}\in\mathbb{R}$ such that*

$$g_{i,j}\tau=a_{i,j}^2A_{\mathfrak{c}_i}^{-1}\tau+jh_\infty+\alpha_{i,j},\ \forall\ \tau\in\mathbb{H}.$$

Proof. Recall that, $g_{i,j}=t_\infty^jA_i^{-1}$ where $A_i(\infty)=\mathfrak{c}_i$. We also know that $A_{\mathfrak{c}_i}(\infty)=\mathfrak{c}_i$, in particular, $A_i^{-1}A_{\mathfrak{c}_i}(\infty)=\infty$. On the other hand, $A_i^{-1}A_{\mathfrak{c}_i}\in\mathrm{PSL}_2(\mathbb{R})$. In particular, $A_i^{-1}A_{\mathfrak{c}_i}=\left(\begin{smallmatrix}a&\alpha\\0&1/a\end{smallmatrix}\right)$ for some $a,\alpha\in\mathbb{R}$. We then have,

$$g_{i,j}\tau=t_\infty^jA_i^{-1}\tau=t_\infty^j\begin{pmatrix}a&\alpha\\0&1/a\end{pmatrix}A_{\mathfrak{c}_i}^{-1}\tau=a^2A_{\mathfrak{c}_i}^{-1}\tau+jh_\infty+\alpha a.$$

This completes the proof by taking $a_{i,j}:=a$ and $\alpha_{i,j}:=\alpha a$. □

We recall that any classical holomorphic modular form does not have weight 0, unless it is a constant function. In those cases, the representation under consideration has a finite image. However, the same may not be true if the representation does not have a finite image. Consider the representation $\mathbb{I}_0:\mathrm{SL}_2(\mathbb{Z})\to\mathrm{GL}_2(\mathbb{C})$, given by $\gamma\mapsto\gamma$. Now consider the holomorphic function $\mathbb{Y}:\mathbb{H}\to\mathbb{C}^2$ given by $\tau\mapsto(\tau,1)$. We know that $\mathbb{Y}(\tau)$ is a holomorphic logarithmic vvaf of weight -1. Then $\mathbb{Y}'(\tau):=\mathbb{Y}(\tau)\Delta(\tau)^{\frac{1}{12}}$ is a non-constant holomorphic logarithmic vvaf of weight 0 associated to the representation $\rho':=\mathbb{I}_0\otimes\nu_{\mathrm{SL}_2(\mathbb{Z})}$. In fact, given any holomorphic logarithmic vvaf of non-zero weight, one can twist with a suitable power of $\Delta(\tau)$ to get a holomorphic logarithmic vvaf of weight 0. Following [38, Section 4.2], we know that the space of holomorphic logarithmic vvaf is a free module of rank two over the polynomial ring $\mathbb{C}[E_4,E_6]$, generated by $\mathbb{Y}'(\tau)$ and its modular derivative.

Moreover, the representation $\rho' : \mathrm{SL}_2(\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{C})$ indeed have infinite image, because

$$\|\rho'(t^n)\| = \left\|\mathbb{I}_0 \otimes \nu_{\mathrm{SL}_2(\mathbb{Z})}(t^n)\right\| = \|\mathbb{I}_0(t^n)\| = n,$$

which follows from the explicit description of $\nu_{\mathrm{SL}_2(\mathbb{Z})}$, see [7, Page 7]. Gannon in [38] gave an explicit description of the logarithmic representations of rank 2 associated to $\mathrm{SL}_2(\mathbb{Z})$, and they all differ from ρ' by some character of $\mathrm{SL}_2(\mathbb{Z})$.

We are now ready to prove the required cuspidal properties of the lifted forms.

Lemma 7.4.2. *Let $\mathfrak{c}$ be an arbitrary cusp of* G*, and $\{\mathfrak{c}_i | 1 \leq i \leq n_{\mathfrak{c}}\}$ be the set of all inequivalent cusps of* H *lying under $\mathfrak{c}$. Then we have the following.*

(i) If $\mathbb{X}(\tau)$ has moderate growth at all the cusps $\{\mathfrak{c}_i | 1 \leq i \leq n_{\mathfrak{c}}\}$, then the lifted form $\widetilde{\mathbb{X}}^{(\mathfrak{c})}(\tau)$ has moderate growth at $\mathfrak{c}$ as well.

(ii) If $\mathbb{X}(\tau)$ is holomorphic (or vanished) at all the cusps $\{\mathfrak{c}_i | 1 \leq i \leq n_{\mathfrak{c}}\}$, then the lifted form $\widetilde{\mathbb{X}}^{(\mathfrak{c})}(\tau)$ has same properties at the cusp $\mathfrak{c}$, provided that the weight of $\mathbb{X}(\tau)$ is 0.

Proof. For both of the parts, it is enough to prove that $\widetilde{\mathbb{X}}^{(\mathfrak{c})}(\tau)$ satisfy the required cuspidal properties at the cusp ∞.

Let us first prove (i). It is clear that $\mathbb{X}_0(\tau)$ has moderate growth at all the cusps $\{\mathfrak{c}_i | 1 \leq i \leq n_\infty\}$, because any power of $\Delta_{\mathrm{H}}(\tau)$ has the same property. Now we shall show that all the components of $\widetilde{\mathbb{X}}_0(\tau)$ has moderate growth at ∞. Let $\mathbb{Y}(\tau) := \mathbb{X}_0(g_{i,j}^{-1}\tau)$ be such a component. Since $\mathbb{X}_0(\tau)$ has moderate growth at all the cusps $\{\mathfrak{c}_i | 1 \leq i \leq n_\infty\}$ there exists a constant $c \in \mathbb{R}$ such that $\|\mathbb{X}_0(\tau)\| \ll |e^{2\pi i c A_{\mathfrak{c}_i}^{-1}\tau}|$ as $\mathrm{im}(\tau) \to \infty$. It follows from Lemma 7.4.1 that, $\|\mathbb{Y}(\tau)\| \ll |e^{2\pi i c'\tau}|$, for some constant $c \in \mathbb{R}$, as $\mathrm{im}(\tau) \to \infty$. This shows that, $\widetilde{\mathbb{X}}_0(\tau)$ has moderate growth at ∞. On the other hand, any power of $\Delta_{\mathrm{G}}(\tau)$ has moderate growth at ∞ as well, and this completes the proof of part (i).

Let us now prove (ii). To show that $\widetilde{\mathbb{X}}(\tau)$ is holomorphic (or vanishes) at the cusp ∞, we need to show that all the components are bounded (or vanishes) as $\mathrm{im}(\tau) \to \infty$. The constant c appearing in the previous paragraph is 0 when $\mathbb{X}(\tau)$ is holomorphic and negative when $\mathbb{X}(\tau)$ is a cuspform. Moreover, it can also be seen from Lemma 7.4.1 that the constants c and c' from the previous paragraph are a positive multiple of each other. Therefore $\widetilde{\mathbb{X}}(\tau)$ has the similar cuspidal properties as $\mathbb{X}(\tau)$. This shows that the lifted form also shares the same cuspidal properties when the weight is 0. □

7.5 Lifting of logarithmic vector-valued automorphic forms

It was proved, by the first author in [7], that the induction of an admissible representation is admissible. In this section, we shall study the induction of non-admissible, i.e., logarithmic representations. In this regard, we have the following.

Proposition 7.5.1. *Let* $\mathfrak{c}$ *be an arbitrary cusp of* G *and* $\{\mathfrak{c}_i | 1 \leq i \leq n_{\mathfrak{c}}\}$ *be the set of inequivalent cusps of* H *for which* $\mathrm{G} \cdot \mathfrak{c} = \bigcup H \cdot \mathfrak{c}_i$. *Then,*

(i) If $\rho(t_i)$ *is not diagonalizable for some* i, *then* $\widetilde{\rho}(t_{\mathfrak{c}})$ *is not diagonalizable.*

(ii) In particular if ρ *is a logarithmic representation, then* $\widetilde{\rho}$ *is a logarithmic representation as well.*

Proof. Let us start with considering the coset representatives $\{g_{i,j}\}$ of H in G from the previous paragraph. We first claim that, for any pair (i,j), some non-trivial power of $\gamma_{i,j} = g_{i,j}^{-1} t_{\mathfrak{c}} g_{i,j}$ is in H. To prove this, we start by noting that there exists $n_{i,j,1}$ and $n_{i,j,2}$ such that $g_{i,j}^{n_{i,j,1}}\mathrm{H} = g_{i,j}^{n_{i,j,2}}\mathrm{H}$. This is because H has a finite index in G. In particular, for each pair (i,j), there exists some integer $n_{i,j}$ such that $g_{i,j}^{-1} t_{\mathfrak{c}}^{n_{i,j}} g_{i,j} \in \mathrm{H}$. Let us now consider $n = \mathrm{lcm}\,\{n_{i,j} | 1 \leq i \leq n_{\mathfrak{c}}, 1 \leq j \leq h_i\}$. In particular, $g_{i,j}^{-1} t_{\mathfrak{c}}^{n} g_{i,j} \in \mathrm{H}$ for each pair (i,j). Therefore, $\widetilde{\rho}(t_{\mathfrak{c}}^n)$ is a block diagonal matrix where each block is of the form $\rho(g_{i,j}^{-1} t_{\mathfrak{c}}^{n} g_{i,j})$. Note that $g_{i,j}^{-1} t_{\mathfrak{c}}^{n} g_{i,j} \in \mathrm{H}$ and fixes the cusp $\mathfrak{c}_i$, hence it is some non-trivial power of t_i. Let us write $g_{i,j}^{-1} t_{\mathfrak{c}}^{n} g_{i,j} = t_i^m$, where $m \neq 0$ is an integer. By the assumption, there exists some i for which $\rho(t_i)$ can be written in Jordan normal form, with a Jordan block, say J_λ, of size greater than 1. In particular, $\rho(t_i^m)$ can be written in a block diagonal form, where one of the blocks is J_λ^m, which is not diagonalizable for any integer $m \neq 0$. This completes the proof of part (i).

For the proof of part (ii), let $\mathfrak{c}_i$ be a cusp of H for which $\rho(t_i)$ is not diagonalizable. Now $\mathfrak{c}_i$ is a cusp of G as well, with $\mathfrak{c}_i$ itself lying under it as a cusp of H. It the follows from the part (i) that $\widetilde{\rho}(t_{\mathfrak{c}})$ is not diagonalizable, which completes the proof. □

Remark 7.5.2. It is clear that $n_{i,j} \leq d$, for each pair (i,j), where d is the index of H in G. In other words, n is crudely bounded by d^d. However, if H is normal in G, one can always take $n_{i,j}$ to be d. In particular, one can take $n = d$. In fact, the discussion in Section 7.4.1 allows us to take $n = \mathrm{lcm}\,\{h_i | 1 \leq i \leq n_{\mathfrak{c}}\}$.

7.5.1 On the growth of the Fourier coefficients

In [9], the authors studied the growth of any holomorphic vvaf associated to Fuchsian groups of the first kind. More precisely, they showed that, there exists a constant α (depending on the associated representation) such that $\|\mathbb{X}[n]\| \ll_{\mathrm{H},\rho} n^{k+2\alpha}$, where $\mathbb{X}(\tau)$ is a holomorphic vvaf of weight $k \in 2\mathbb{Z}$ associated a representation ρ of H. Moreover, the constant α depends only on H and the exponent $k+2\alpha$ can be divided by 2 for cuspforms. In this section, we shall study the change of this exponent under lifting.

In general, we show that the constant α is multiplied by at most the index of H in G. In particular, the exponent do not change when $\alpha = 0$. In [9], the authors remarked that α can be taken to be 0 when ρ is a unitary representation. To prove the main result of this section, let us start with the following.

Lemma 7.5.3. *Let ρ be a representation of* H *such that* $\|\rho(h)\| \ll_{\mathrm{H}} \|h\|^{\alpha}$, $\forall h \in \mathrm{H}$. *Then the induced representation $\widetilde{\rho}$ associated to a finite extension* G *of* H *has the following growth.*

$$\|\widetilde{\rho}(\gamma)\| \ll_{\mathrm{G}} \|\gamma\|^{\alpha}, \ \forall \gamma \in \mathrm{G}.$$

Proof. It follows from the definition of induced representations that,

$$\|\widetilde{\rho}(\gamma)\| \leq \max_{\substack{1\leq i,j\leq d \\ \gamma_i\gamma\gamma_j^{-1}\in \mathrm{H}}} \left\|\rho(\gamma_i\gamma\gamma_j^{-1})\right\|.$$

On the other hand, it follows from the assumption on ρ, and the semi multiplicative property of $\|\cdot\|$ that $\left\|\rho(\gamma_i\gamma\gamma_j^{-1})\right\| \ll_{\mathrm{G}} \|\gamma\|^{\alpha}$. This completes the proof. □

Let us now recall from Lemma 7.4.2 that if $\mathbb{X}(\tau)$ is a holomorphic vvaf of weight 0, then the lifted form $\widetilde{\mathbb{X}}(\tau)$ is a holomorphic vvaf as well. As a consequence of Lemma 7.5.3, we deduce the following.

Corollary 7.5.4. *Let $\mathbb{X}(\tau)$ be an admissible holomorphic vvaf associated to (H, ρ) of weight* 0. *Then there exists a constant α depending only on* H *and ρ such that the Fourier coefficients of the lifted holomorphic vvaf $\widetilde{\mathbb{X}}(\tau)$ have the following growth*

$$\left\|\widetilde{\mathbb{X}}[n]\right\| \ll_{\mathrm{H},\rho} n^{\alpha},$$

In particular, the growth of the Fourier coefficients of the lifted vector-valued automorphic forms do not depend on G. *However, if $\mathbb{X}(\tau)$ is a holomorphic logarithmic vvaf, then the exponent increases by at most* $\mathrm{rank}(\widetilde{\rho}) := \mathrm{rank}(\rho)|\mathrm{G}/\mathrm{H}|$.

Proof. When ρ is admissible, we can write $\|\widetilde{\rho}(\gamma)\| \ll_{\mathrm{G}} (c^2+d^2)^{\alpha}$ due to Lemma 4.1 in [9]. Since $\mathbb{X}(\tau)$ has even integer weight, it is evident that $\rho(I) = \rho(-I)$. Therefore ρ can be thought of as a representation of H. One can then follow the proof for the admissible case in the same article.

For the logarithmic case, one can follow the argument on page 21 of [9]. The increase in the exponent is coming because of the extra logarithmic terms in the Fourier expansion, and they come with power at most $\mathrm{rank}(\widetilde{\rho})$, which is precisely $\mathrm{rank}(\rho)|\mathrm{G}/\mathrm{H}| = md$. □

Chapter 8

On the elliptic Wieferich primes

Let $E/\mathbb{Q}$ be an elliptic curve given by a Weierstrass equation with coefficients $a_i \in \mathbb{Z}$, and $P \in E(\mathbb{Q})$ be a non-torsion point. Throughout this section we consider E and P as being fixed.

For any integer $n \geq 0$, define the nth division polynomial $\psi_n \in \mathbb{Z}[x, y]$ as follows.

$$\begin{aligned}
&\psi_0 = 0, \quad \psi_1 = 1, \quad \psi_2 = 2y + a_1x + a_3, \\
&\psi_3 = 3x^4 + b_2x^3 + 3b_4x^2 + 3b_6x + b_8, \\
&\psi_4 = \psi_2(2x^6 + b_2x^5 + 5b_4x^4 + 10b_6x^3 + 10b_8x^2 + (b_2b_8 - b_4b_6)x + b_4b_8 - b_2^6)
\end{aligned}$$

where the b_i are defined in [88, Chapter III], with subsequent polynomials given by

$$\begin{aligned}
\psi_{2n+1} &= \psi_{n+2}\psi_n^3 - \psi_{n+1}^3\psi_{n-1}, \quad n \geq 2, \\
\psi_{2n}\psi_2 &= \psi_n(\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2), \quad n \geq 3,
\end{aligned} \tag{8.1}$$

and extend this to negative n by setting $\psi_n = -\psi_{-n}$. These formulas are equivalent to the recurrence relation

$$\psi_{m+n}\psi_{m-n}\psi_r^2 = \psi_{m+r}\psi_{m-r}\psi_n^2 - \psi_{n+r}\psi_{n-r}\psi_m^2 \tag{8.2}$$

for any integers m, n, r. The sequence ψ_n forms a divisibility sequence in $\mathbb{Z}[x, y]$, i.e. $\psi_n \mid \psi_m$ for $n \mid m$. One notion of an *elliptic divisibility sequence (EDS)* in a commutative ring would be a divisibility sequence satisfying (8.2). The study of EDS in $\mathbb{Z}$, in this sense, was begun by Ward [99], and a modern exposition can be found in [36, Ch. 10]. We will use a slightly different kind of EDS considered by Verzobio [97], which is better suited to our purpose.

We can interpret x, y and each ψ_n as rational functions on $E(\mathbb{Q})$. By [88, Ex. III.3.7], multiplication by n is given as a rational map by

$$[n](P) = \left(\frac{x(P)\psi_n^2 - \psi_{n-1}\psi_{n+1}}{\psi_n^2}, \frac{\psi_{n-1}^2\psi_{n+2} - \psi_{n-2}\psi_{n+1}^2}{4y(P)\psi_n^3} \right).$$

In particular ψ_n is the square root of the denominator of the x–coordinate; the problem for us is that in general there may be some common factors between the numerator and denominator, so it will not be in the lowest terms. We want to work with the genuine denominator as it has better p-adic properties (cf. Lemma 8.1.3).

Definition 8.0.1. *Define the sequence e_n by $nP = (a_n/e_n^2, b_n/e_n^3)$ with $\gcd(a_n b_n, e_n) = 1$ and $e_n > 0$. Writing $\operatorname{sign}(t) = t/|t|$ for any $t \neq 0$, set*

$$\beta_0 = 0, \qquad \beta_n = \operatorname{sign}(\psi_n(P))\frac{e_n}{e_1}, \qquad (n \in \mathbb{Z} \setminus \{0\}).$$

Definition 8.0.2. *A prime p is called an elliptic non-Wieferich prime if $\nu_p(\beta_n) = 1$ for some integer n.*

Note that it follows from Lemma 11 in [87] that p is indeed a non-Wieferich prime for a point P in the sense mentioned in the previous section. In particular, the problem is then to study square-free parts of the sequence β_n. It follows from the following conjecture that the number of elliptic non-Wieferich primes at most x is $\gg_{E,P} \log x$.

Conjecture 8.0.3. *Let $E/\mathbb{Q}$ be an elliptic curve in the Weierstrass form. For any $\varepsilon > 0$ there exists a constant c_ε such that*

$$\max\left\{\frac{1}{2}\log|a_P|\log|e_P|\right\} \leq (1+\varepsilon)\log\operatorname{rad}(e_P) + c_\varepsilon$$

for all $P \in E(\mathbb{Q}) \setminus \{O\}$.

Definition 8.0.4. *Let χ be a Dirichlet character with modulus $q(\chi)$. Say a prime p is χ-Wieferich prime if $ord(\chi(p)) \nmid \nu_p(\beta_n)$ for some integer n, and prime $p \nmid q(\chi)$.*

We shall show in the next section that β_n is periodic modulo any prime power and hence modulo any integer. Let π be the period of $\beta_n \bmod q(\chi)$. Suppose that there exists $\alpha \in \mathbb{N}$ such that

$$\gcd(\alpha, \pi) = 1$$

and such that one of the following holds:

$$\begin{aligned}
&\chi(|\beta_\alpha|) \neq 0, 1, \quad \text{or}\\
&\chi(-|\beta_\alpha|) \neq 0, 1 \text{ and } 4 \nmid \pi, \quad \text{or}\\
&\chi(-|\beta_\alpha|) \neq 0, 1 \text{ and } P \in E(\mathbb{R})^0,
\end{aligned}$$

then we say the character χ is *nice*. We shall prove the following in the next section.

Proposition 8.0.5. *Let χ be a nice Dirichlet character with modulus $q(\chi)$. Then*

$$\#\{\text{primes } \ell \leq x : \operatorname{ord}(\chi(p)) \nmid \nu_p(\beta_\ell) \text{ for some prime } p \nmid q(\chi)\} \geq \frac{1}{2\varphi(\pi)}\frac{x}{\log x},$$

as $x \to \infty$.

Consequently, we have the following unconditional lower bound for the χ-Wieferich primes.

Theorem 8.0.6 (Bhakta)**.** *For any nice Dirichlet character χ, we get at least $c_{E,P}\frac{\sqrt{\log x}}{\log\log x}$ many χ-Wieferich primes up-to x, for some constant $c_{E,P} > 0$.*

Proof. We shall show in the next section that β_n is periodic modulo any integer N, with some period π_N, depending on N. Given a Dirichlet character χ, denote $\pi(\chi)$ to be the period of $\beta_n \pmod{q(\chi)}$, and consider

$$S_\chi(x) = \#\left\{\text{primes } \ell \leq x : \operatorname{ord}(\chi(p)) \nmid \nu_p(\beta_\ell) \text{ for some prime } p \nmid q(\chi)\right\}.$$

Let us first note that, for any prime $\ell \in S_\chi(x)$, we have a χ-Wieferich prime p_ℓ. Moreover, the association $\ell \mapsto p_\ell$ is injective due to Lemma 8.1.7, which we shall prove shortly in the next section. On the other hand, it follows from [87, Lemma 8] that $\log(p_\ell) \leq \log|\beta_\ell| = O(\ell^2)$. This completes the proof of Theorem 8.0.6. □

Now we are left with three tasks; first, we shall discuss periodicity, then prove Proposition 8.0.5, and finally, study the proportion of nice characters.

8.1 Periodicity

Let E be an elliptic curve over $\mathbb{Q}_p$ given by a (not necessarily minimal) Weierstrass equation with coefficients in $\mathbb{Z}_p$. In other words, let E be given by

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,\ a_i \in \mathbb{Q}_p,\ \forall i \in \{1,2,3,4,6\}.$$

Denote by $E_0(\mathbb{Q}_p)$ the set of points of $E(\mathbb{Q}_p)$ with non-singular reduction modulo p. We say that $P \in E(\mathbb{Q}_p)$ has *bad reduction* if $P \notin E_0(\mathbb{Q}_p)$. There is a subgroup filtration

$$\cdots \subset E_2(\mathbb{Q}_p) \subset E_1(\mathbb{Q}_p) \subset E_0(\mathbb{Q}_p),\ E_i(\mathbb{Q}_p) = \{P \in E_0(\mathbb{Q}_p) : P \equiv O \bmod p^i\},\ i \geq 1.$$

Definition 8.1.1. *If $P \in E(\mathbb{Q}_p) \setminus E_1(\mathbb{Q}_p)$ we set $\nu_p(P) = 0$. If $P \in E_1(\mathbb{Q}_p)$ we define*

$$\nu_p(P) = \sup\{i : P \in E_i(\mathbb{Q}_p)\}.$$

Definition 8.1.2. *For $P \in E_0(\mathbb{Q}_p)$ and $k \in \mathbb{N}$ we denote by $P \bmod p^k$ the image of P in $E_0(\mathbb{Q}_p)/E_k(\mathbb{Q}_p)$. We denote by $\operatorname{ord}(P \bmod p^k)$ its order.*

Lemma 8.1.3. *Let $P = (x, y) \in E(\mathbb{Q}_p)$. Then $\nu_p(P) = \max\{0, -\nu_p(x)/2\}$.*

Proof. If $\nu_p(x) \geq 0$ then $\nu_p(P) = 0$ so the result holds. So assume $\nu_p(x) < 0$. As the rational function x/y is a uniformising parameter at O, we find that $\nu_p(P) = \nu_p(x/y)$. However, using $\nu_p(x) < 0$ and the Weierstrass equation, one finds that $2\nu_p(y) = 3\nu_p(x)$, and the claim easily follows. □

Lemma 8.1.3 gives a more explicit definition of filtration, which is often used in texts (e.g. [88, Ex. VII.7.4]). We have the following inequality for the valuation of a multiple of a point.

Lemma 8.1.4. *Let $P \in E_1(\mathbb{Q}_p)$. Then $\nu_p(nP) \geq \nu_p(P) + \nu_p(n)$, with equality if $p \nmid n$.*

Proof. Hensel's lemma [23, Lem. 2.1] shows that $|E_i(\mathbb{Q}_p)/E_{i+1}(\mathbb{Q}_p)| = p$ for all $i \geq 1$, thus this quotient is isomorphic to $\mathbb{Z}/p\mathbb{Z}$. The result now easily follows. □

Remark 8.1.5. Using the formal group law on E [88, Thm. IV.6.4(b), Prop. VII.2.2], one can show that equality holds except possibly if $p = 2, \nu_p(P) = 1$ and $p \mid n$. (See also [91, Thm. 3] for a version over number fields.) The hypothesis is required for $p = 2$. Take

$$E : y^2 + xy = x^3 + 4x + 1, \quad P = (15/4, -83/8).$$

Then $v_2(P) = 1$, but one calculates that $v_2(2P) = 4$.

The sequence β_n is *not* in general an elliptic divisibility sequence in the traditional sense, since it need not satisfy the recurrence relation (8.2); differences can occur if P admit primes of bad reduction. In [97], Verzobio calls such sequences EDSB, as opposed to sequences of the form $\psi_n(P)$ which he terms EDSA. He shows in [97, Thm. 1.9] that the following weakened version of (8.2) does hold for an EDSB.

Theorem 8.1.6 (Verzobio, [97])**.** *Set*

$$M = M(P) = \operatorname{lcm}\{ \operatorname{ord}(P + E_0(\mathbb{Q}_p)) : p \text{ prime}\},$$

where $\operatorname{ord}(P + E_0(\mathbb{Q}_p))$ *denotes the order of the image of P in the finite group $E(\mathbb{Q}_p)/E_0(\mathbb{Q}_p)$. Let $n, m, r \in \mathbb{Z}$ of which two are multiples of $M(P)$. Then*

$$\beta_{n+m}\beta_{n-m}\beta_r^2 = \beta_{m+r}\beta_{m-r}\beta_n^2 - \beta_{n+r}\beta_{n-r}\beta_m^2. \tag{8.3}$$

The reader may note that M is the least positive integer such that MP has everywhere good reduction. Verzobio defines β_n for $n \geq 0$ and proves the theorem under the assumption $n \geq m \geq r > 0$; in our notation this can be removed by using $\beta_{-n} = -\beta_n$ and permuting the variables as appropriate.

To illustrate some of the nice p-adic properties of this sequence, we first make explicit Lemma 8.1.3.

Lemma 8.1.7. *For all primes p we have $\nu_p(\beta_n) = \nu_p(nP) - \nu_p(P)$.*

Proof. Immediate from the definition and Lemma 8.1.3. □

Lemma 8.1.8. *For all $n, m \in \mathbb{Z}$ we have* $\gcd(\beta_m, \beta_n) = |\beta_{\gcd(m,n)}|$.

Proof. By Lemma 8.1.7, for any prime p and any $V \in \mathbb{N}$ we have

$$\{n \in \mathbb{Z} : \nu_p(\beta_n) \geq V\} = \{n \in \mathbb{Z} : nP \in E_{V+\nu_p(P)}(\mathbb{Q}_p)\} = q\mathbb{Z}$$

for some $q \in \mathbb{N}$. In particular $p^V \mid \beta_n$ if and only if $q \mid n$. Therefore

$$p^V \mid \gcd(\beta_m, \beta_n) \iff q \mid \gcd(m,n) \iff p^V \mid \beta_{\gcd(m,n)}.$$

□

We emphasize that an EDSA need not have these properties if P admits primes of bad reduction. The elegance of Verzobio's EDSB is that it has both good p-adic properties and comes within a whisker of satisfying the recurrence relation.

8.1.1 Symmetry law

A central part of Ward's work on elliptic divisibility sequences is a *symmetry law* [99, Thm. 8.1] (see [1, Thm. 1.11] for a modern formulation). This says that an integral EDSA modulo a prime forms a periodic sequence of a certain form. We prove a version of this for EDSBs for general prime powers.

Proposition 8.1.9. *Let M be as in Theorem 8.1.6. Let $n, r \in \mathbb{Z}$ with $M \mid r$. Let p be a prime and let $k \in \mathbb{N}$. Suppose that p^k divides $\beta_r / \gcd(\beta_r, \beta_M)$. Then for all $\ell \in \mathbb{Z}$ we have*

$$\beta_{n+\ell r} \equiv \begin{cases} \left(\beta_{M+r}\beta_{M-r}\beta_M^{-2}\right)^{\frac{\ell(\ell+1)}{2}} (\beta_{n+r}\beta_n^{-1})^\ell \beta_n \bmod p^k, & \text{if } p^k \nmid \beta_n, \\ 0 \bmod p^k, & \text{if } p^k \mid \beta_n, \end{cases}$$

where in the first case the quotients $\beta_{M+r}\beta_{M-r}/\beta_M^2$ and β_{n+r}/β_n are p-adic units.

Proof. Lemma 8.1.8 gives us

$$|\beta_{\gcd(n,r)}| = \gcd(\beta_{n+\ell r}, \beta_r) = \gcd(\beta_n, \beta_r) \tag{8.4}$$

for every $\ell \in \mathbb{Z}$. This proves the proposition if $p^k \mid \beta_n$, so assume that $p^k \nmid \beta_n$.

Taking $m = M$ in Theorem 8.1.6, and replacing n by $n + \ell r$, we obtain

$$\beta_{M+r}\beta_{M-r}\beta_{n+\ell r}^2 \equiv \beta_{n+(\ell+1)r}\beta_{n+(\ell-1)r}\beta_M^2 \bmod \beta_r^2, \tag{8.5}$$

for any $\ell \in \mathbb{Z}$. We want to combine this with Lemma 8.1.8. Let

$$C = \frac{\beta_{M+r}\beta_{M-r}}{\beta_M^2}, \qquad a_\ell = \frac{\beta_{n+\ell r}}{\gcd(\beta_n, \beta_r)}. \tag{8.6}$$

Since $M \mid r$, Lemma 8.1.8 shows that $C \in \mathbb{Z}$. Also (8.4) shows that a_ℓ is an integer coprime to $\beta_r / \gcd(\beta_n, \beta_r)$. Hence, dividing both sides of (8.5) by $\beta_{n+\ell r}^2 \beta_M^2$ gives

$$C \equiv \frac{a_{\ell+1}a_{\ell-1}}{a_\ell^2} \bmod \frac{\beta_r^2}{\gcd(\beta_n\beta_M, \beta_r)^2} \quad \text{for all } \ell \in \mathbb{Z}, \tag{8.7}$$

where every a_ℓ is coprime to the modulus. It follows by induction on ℓ from (8.7) that

$$a_\ell \equiv C^{\frac{\ell(\ell+1)}{2}} a_1^\ell a_0^{1-\ell} \bmod \frac{\beta_r^2}{\gcd(\beta_n\beta_M, \beta_r)^2}.$$

Multiplying by $\gcd(\beta_n, \beta_r)$ we obtain

$$a_\ell \gcd(\beta_n, \beta_r) \equiv C^{\frac{\ell(\ell+1)}{2}} (a_1 a_0^{-1})^\ell a_0 \gcd(\beta_n, \beta_r) \bmod \frac{\gcd(\beta_n, \beta_r)\beta_r^2}{\gcd(\beta_n\beta_M, \beta_r)^2}.$$

Here $\beta_r/\gcd(\beta_M, \beta_r)$ divides the modulus, and so the congruence holds modulo p^k. Inserting the definitions (8.6) proves the first case in the proposition.

Finally, since $p^k \mid \beta_r/\gcd(\beta_M, \beta_r)$ and $p^k \nmid \beta_n$, we see that p divides the modulus in (8.7). Since every a_ℓ is coprime to the modulus, we see that C and $\beta_{n+r}\beta_n^{-1} = a_1 a_0^{-1}$ are p-adic units, as claimed in the final part of the proposition. □

We now use the symmetry law to prove that β_n is periodic modulo any prime power and hence modulo any integer. Versions of this appear in the literature for differing definitions of EDS. Ward proved eventual periodicity modulo any prime in [99, Thm. 11.1]. Shipsey proved a version modulo p^2 for primes of good reduction [82, Thm. 3.5.4]. Ayad proved it modulo any integer, but assuming good reduction and avoiding $p = 2$ [5, Thm. D]. Silverman proved a version over finite fields [89, Thm. 1] as well as a version modulo prime powers whenever the curve has good ordinary reduction [89, Thm. 3]. Our version (Proposition 8.1.10) contains none of these technical assumptions and is a general version of periodicity for Verzobio's arguably more elegant EDSB.

Our result is the following, which shows periodicity modulo an arbitrary prime power and gives an upper bound for the period. Note that the Chinese Remainder Theorem then easily shows periodicity modulo an arbitrary integer.

Proposition 8.1.10. *Let M be as in Theorem 8.1.6, let $k \in \mathbb{N}$, and let p be a prime. Let*

$$r(p^k) = M \operatorname{ord}\left(MP \bmod p^{k+\nu_p(MP)}\right) \tag{8.8}$$

and

$$\pi(p^k) = \begin{cases} (p-1)p^{k-1}r(p^k), & \text{if } p \neq 2 \text{ and } \left(\frac{\beta_{M+r(p^k)}\beta_{M-r(p^k)}}{p}\right) = 1, \\ 2(p-1)p^{k-1}r(p^k), & \text{otherwise.} \end{cases} \tag{8.9}$$

Then for every $m \in \mathbb{Z}$ we have

$$m \equiv n \bmod \pi(p^k) \quad \Longrightarrow \quad \beta_m \equiv \beta_n \bmod p^k.$$

In other words, the sequence $\beta_m \bmod p^k$ is periodic with period dividing $\pi(p^k)$.

Proof. For ease of notation, we write $r = r(p^k)$ throughout the proof. We first observe that $rP \equiv O \bmod p^{k+\nu_p(MP)}$ by (8.8). That is we have $k + \nu_p(MP) \leq \nu_p(rP)$, and hence by Lemma 8.1.7 and (8.8) we have

$$p^k \text{ divides } \frac{\beta_r}{\gcd(\beta_M, \beta_r)} \quad \text{and} \quad M \mid r. \tag{8.10}$$

Let $n \in \mathbb{Z}$. By (8.10), the hypotheses of Proposition 8.1.9 are satisfied. If $p^k \mid \beta_n$ then the result follows immediately; suppose therefore that $p^k \nmid \beta_n$. Proposition 8.1.9 shows that

$$\beta_{n+\ell r} \equiv \left(\beta_{M+r}\beta_{M-r}\beta_M^{-2}\right)^{\frac{\ell(\ell+1)}{2}} (\beta_{n+r}\beta_n^{-1})^{\ell}\beta_n \mod p^k,$$

for every $\ell \in \mathbb{Z}$, where $\beta_{M+r}\beta_{M-r}\beta_M^{-2}, \beta_{n+r}\beta_n^{-1}$ are p-adic units. In particular $\gcd(\beta_n, p^k) = \gcd(\beta_{n+\ell r}, p^k) = \gcd(\beta_n, \beta_r, p^k)$.

Now $\#(\mathbb{Z}/p^k\mathbb{Z})^\times = (p-1)p^{k-1}$, and so if $u \in \mathbb{Z}_p^\times$ then

$$2(p-1)p^{k-1} \mid \ell \implies u^{\frac{\ell(\ell+1)}{2}} \equiv 1 \bmod p^k.$$

Moreover if $p \neq 2$ and $\left(\frac{u}{p}\right) = 1$ then $u = v^2$ for $v \in \mathbb{Z}_p^\times$. So

$$(p-1)p^{k-1} \mid \ell,\ p \neq 2,\ \left(\frac{u}{p}\right) = 1 \implies u^{\frac{\ell(\ell+1)}{2}} \equiv 1 \bmod p^k.$$

Thus by definition of $\pi(p^k)$, if $\pi(p^k) \mid \ell r$ then

$$\left(\beta_{M+r}\beta_{M-r}\beta_M^{-2}\right)^{\frac{\ell(\ell+1)}{2}} (\beta_{n+r}\beta_n^{-1})^{\ell} \equiv 1 \bmod p^k,$$

which implies

$$\beta_{n+\ell r} \equiv \beta_n \bmod p^k.$$

Writing $m = n + \ell r$ completes the proof. □

There is a simpler but slightly weaker bound for the period.

Lemma 8.1.11. *Let M be as in Theorem 8.1.6, let $k \in \mathbb{N}$, and let p be a prime. Then the period of $\beta_n \bmod p^k$ divides*

$$\begin{cases} 2M(p-1)p^{2(k-1)} \operatorname{ord}(MP \bmod p), & \text{if } \nu_p(MP) = 0, \\ 2M(p-1)p^{2k-1}, & \text{otherwise.} \end{cases}$$

Proof. Let $Q = MP$. By Proposition 8.1.10, it suffices to show that

$$\operatorname{ord}(Q \bmod p^{k+\nu_p(Q)}) \text{ divides } r_1(p^k) := \begin{cases} p^{k-1}\operatorname{ord}(Q \bmod p), & \text{if } \nu_p(Q) = 0, \\ p^k, & \text{otherwise.} \end{cases}$$

If $\nu_p(Q) = 0$ then Lemma 8.1.4 implies that $\nu_p(p^{k-1}\operatorname{ord}(Q \bmod p)Q) \geq k - 1 + \nu_p(\operatorname{ord}(Q \bmod p)Q) \geq k$. If $\nu_p(Q) > 0$ then Lemma 8.1.4 yields $\nu_p(p^kQ) \geq k + \nu_p(Q)$. In both cases $r_1(p^k)Q \equiv 0 \bmod p^{k+\nu_p(Q)}$, as required. □

Remark 8.1.12. By definition M divides $\prod_p |E(\mathbb{Q}_p)/E_0(\mathbb{Q}_p)|$, hence is bounded uniformly with respect to P. Moreover $\operatorname{ord}(MP \bmod p)$ divides $|E_0(\mathbb{Q}_p)/E_q(\mathbb{Q}_p)|$. Thus Lemma 8.1.11 shows that the period of $\beta_n \bmod N$ can be bounded independently of P for all $N \in \mathbb{N}$, with the bound only depending on E and N.

8.1.2 Signs

Recall from Definition 8.0.1 that the sign of β_n is the sign of the sequence $\psi_n(P)$. The following is [90, Thm. 4] (see also [3] for a generalisation.)

Theorem 8.1.13 (Silverman-Stephens)**.** *There is a sign $\sigma \in \{\pm 1\}$ and an irrational number β such that for all $n \in \mathbb{N}$ we have*

$$\sigma^{n-1}\mathrm{sign}(\beta_n) = \begin{cases} (-1)^{\lfloor n\beta \rfloor}, & \text{if } P \in E(\mathbb{R})^0, \\ (-1)^{\lfloor n\beta \rfloor + \frac{n}{2}}, & \text{if } P \notin E(\mathbb{R})^0 \text{ and } n \text{ is even,} \\ (-1)^{\frac{n-1}{2}}, & \text{if } P \notin E(\mathbb{R})^0 \text{ and } n \text{ is odd.} \end{cases}$$

If $P \in E(\mathbb{R})^0$ then β is defined as follows. We fix an $\mathbb{R}$-analytic group isomorphism $\psi : E(\mathbb{R})^0 \to \mathbb{R}^*_{>0}/e^{\mathbb{Z}}$. Then let $\beta = \log u$ where u is a representative of $\psi(P)$ in $\mathbb{R}^*_{>0}$ with $e^{-1} < u < 1$.

In Silverman and Stephens' original statement of the theorem, there is an isomorphism $E(\mathbb{R}) \to \mathbb{R}^*/q^{\mathbb{Z}}$, which maps $E(\mathbb{R})^0$ to either $\mathbb{R}^*_{>0}/q^{\mathbb{Z}}$ if $q > 0$ or $\mathbb{R}^*_{>0}/q^{2\mathbb{Z}}$ otherwise. Without loss of generality we can assume that $E(\mathbb{R})^0$ is mapped to $\mathbb{R}^*_{>0}/e^{\mathbb{Z}}$, or else we can compose our isomorphism with $v \mapsto v^{-1/\log q}$ or $v^{-1/2\log q}$. When $P \in E(\mathbb{R})^0$ their choice of u then satisfies $e^{-1} < u < 1$ as above.

We want to say something about the Diophantine approximation properties of the irrational number β from the theorem. Let $\exp_E : \mathbb{C} \to E(\mathbb{C})$ be the usual parametrisation of E using the Weierstrass $\wp$-function, see for example [88, Corollary 5.1.1]. The usual convention would be to normalize so that, in a certain sense, the derivative of $\exp_E$ at the origin is the identity. This is not necessary for our purposes, however. We only use the fact that $\exp_E$ is an $\mathbb{R}$-analytic surjective additive group homomorphism, and Theorem 1.2 of Bosser and Gaudron [18], which states:

Theorem 8.1.14 (Bosser-Gaudron)**.** *Let $z \in \mathbb{C}$ such that $\exp_E(z) \in E(\mathbb{Q}) \setminus \{O\}$. Then we have*

$$\log|z| \gg_E 1 - \widehat{h}(\exp_E(z)),$$

where $\widehat{h}$ is the canonical height on $E(\mathbb{Q})$.

We use this to prove

Lemma 8.1.15. *Suppose the point P from the start of this section satisfies $P \in E(\mathbb{R})^0$. Let β be as in Theorem 8.1.13, and let $N \in \mathbb{Z} \setminus \{0\}$. Then*

$$\min_{M \in \mathbb{Z}} \log|N\beta - M| \gg_E 1 - \widehat{h}(NP).$$

Proof. Let $w \in \mathbb{C}^*$ such that $\exp_E(w) = P$, so that $\exp_E(w\mathbb{R}) = E(\mathbb{R})^0$ and $\psi(\exp_E(tw)) = e^{t\beta+\mathbb{Z}}$ for any $t \in \mathbb{R}$. For any $M \in \mathbb{Z}$ we deduce that

$$\exp_E(N + \beta^{-1}M) = \phi^{-1}(e^{N\beta+M+\mathbb{Z}}).$$

By the definition of β we deduce $\exp_E(N+\beta^{-1}M) = \phi^{-1}(u^N e^{\mathbb{Z}})$ which is NP by definition of u. That is,

$$\exp_E^{-1}(NP) \supseteq \{(N+\beta^{-1}M)w : M \in \mathbb{Z}\}.$$

Now by Theorem 8.1.14, any t such that $tw \in \exp_E^{-1}(NP)$ has $\log|t| \gg_E 1-h(NP)$, and so

$$\min_{M\in\mathbb{Z}} \log|N\beta - M| \gg_E 1 - \widehat{h}(NP).$$

□

8.2 Controlling the valuations with Dirichlet characters

We now provide the main technical input required to prove the main results of this chapter. Under certain assumptions, it stipulates the existence of many prime-numbered elements of the sequence β_n which are divisible by primes that are non-trivial with respect to a given Dirichlet character with a certain valuation. We require the following effective version of uniform distribution modulo 1 for primes in an arithmetic progression multiplied by an irrational.

Proposition 8.2.1. *Suppose the point P from the start of this section satisfies $P \in E(\mathbb{R})^0$. Let $s,t \in \mathbb{N}$ with $\gcd(s,t)=1$ and let β be as in Theorem 8.1.13. For any $0 \le a < b \le 1$ and any $\epsilon > 0$ we have*

$$\#\{\textit{primes } \ell \le x : \ell \equiv s \bmod t, \{\ell\beta/2\} \in [a,b)\} = \left(\frac{b-a}{\varphi(t)} + o(1)\right)\frac{x}{\log x},$$

where we write $\{\cdot\}$ for the fractional part. In particular for any $\epsilon > 0$ we have

$$\#\{\textit{primes } \ell \le x : \ell \equiv s \bmod t, (-1)^{\lfloor \ell\beta \rfloor} = 1\} = \left(\frac{1}{2\varphi(t)} + o(1)\right)\frac{x}{\log x}$$

Before proving this, let us firsr recall the following Erdős–Turán inequality [33, Theorem III]:

Lemma 8.2.2 (Erdős–Turán)**.** *For any $0 \le a < b \le 1$, any real sequence t_m, any $M \in \mathbb{N}$ and any $H > 0$ we have*

$$\left|(b-a)M - \sum_{m=1}^{M} \mathbf{1}_{\{t_m\}\in[a,b)}\right| \ll \frac{M}{H} + \sum_{1\le j\le H}\frac{1}{j}\left|\sum_{m=1}^{M} e(jt_m)\right|,$$

where we write $\{\cdot\}$ for the fractional part, and $\mathbf{1}_{\{t_m\}\in[a,b)} = 1$ if $\{t_m\} \in [a,b)$ and 0 otherwise.

Proof of Proposition 8.2.1. For the second part, we note that $(-1)^{\lfloor \ell\beta \rfloor} = 1$ if and only if $0 \le \{\ell(\beta/2)\} < 1/2$. So it suffices to prove the first claim in the proposition. Then we apply Lemma 8.2.2 with M, t_m as follows. Denote the primes $\ell \equiv s \bmod t, \ell \le x$ by $\ell_1, \dots, \ell_M$ and let $t_m = \{\ell_m \beta/2\}$. There is $c > 0$ such that for each $B > 0$ with $t \le (\log x)^B$, we have

$$M = \frac{x}{\varphi(t)\log x} + O\left(\frac{x}{\varphi(t)(\log x)^2}\right) + O_B(x\exp(-c\sqrt{\log x})),$$

by the Siegel-Walfisz theorem [68, Corollary 11.21, see also p5]. In particular, we have the follwing as $x \to \infty$.

$$M = \frac{x}{\varphi(t)\log x} + O\left(\frac{x}{\varphi(t)(\log x)^2}\right),$$

We substitute this into Lemma 8.2.2 to obtain

$$\begin{aligned} &\#\big\{m \le M : \{\ell_m\beta/2\} \in [a,b)\big\} - \frac{(b-a)x}{\varphi(t)\log x} \\ &\qquad \ll \frac{x}{H\varphi(t)\log x} + \frac{x}{\varphi(t)(\log x)^2} + \sum_{1\le j\le H} \frac{1}{j} \left| \sum_{\substack{\ell\le x \\ \ell\equiv s \bmod t \\ \ell \text{ prime}}} e(j\ell\beta/2) \right|. \end{aligned} \tag{8.11}$$

Our goal is to estimate the last sum above. As often happens, it is convenient to count primes weighted by the von Mangoldt function. By partial summation,

$$\begin{aligned} \sum_{\substack{\ell\le x \\ \ell\equiv s \bmod t \\ \ell \text{ prime}}} e(j\ell\beta/2) = \frac{1}{\log x} \sum_{\substack{\ell\le x \\ \ell\equiv s \bmod t \\ \ell \text{ prime}}} (\log \ell) e(j\ell\beta/2) + \\ \int_1^x \frac{1}{y(\log y)^2} \sum_{\substack{\ell\le y \\ \ell\equiv s \bmod t \\ \ell \text{ prime}}} (\log \ell) e(j\ell\beta/2)\,\mathrm{d}y. \end{aligned} \tag{8.12}$$

Below we will show that

$$\sum_{\substack{\ell\le y \\ \ell\equiv s \bmod t \\ \ell \text{ prime}}} (\log \ell) e(j\ell\beta/2) \ll_E y \cdot tj\sqrt{\frac{\widehat{h}(P)}{\log y}} \log\log\log y \tag{8.13}$$

for all $y \ge 1, j \in \mathbb{N}$. It follows from (8.12) that for each non-zero integer j we have

$$\sum_{\substack{\ell\le x \\ \ell\equiv s \bmod t \\ \ell \text{ prime}}} e(j\ell\beta/2) \ll_E \frac{x}{\log x} \cdot tj\sqrt{\frac{\widehat{h}(P)}{\log x}} \log\log\log x.$$

Together with (8.11) and the choice

$$H = \left(\frac{\log x}{\widehat{h}(P)}\right)^{1/4} (t\varphi(t)\log\log\log x)^{-1/2},$$

we have the desired asymptotic formula. □

Lemma 8.2.3. *Let β be as in Theorem 8.1.13. Then for any integer t, we have the following estimate as $y \to \infty$.*

$$\sum_{\substack{\ell \le y \\ \ell \equiv s \bmod t \\ \ell \text{ prime}}} e(j\ell\beta/2) \ll_E y \cdot tj\sqrt{\frac{\widehat{h}(P)}{\log y}}\log\log\log y.$$

Proof. We use the formula

$$\frac{1}{t}\sum_{m \in \mathbb{Z}/t\mathbb{Z}} e(m(n-s)/t) = \begin{cases} 1, & n \equiv s \bmod t, \\ 0, & \text{otherwise,} \end{cases}$$

which is valid for all integers n. This gives

$$\sum_{\substack{\ell \le y \\ \ell \equiv s \bmod t \\ \ell \text{ prime}}} (\log \ell) e(j\ell\beta/2) = \frac{1}{t}\sum_{m \in \mathbb{Z}/t\mathbb{Z}} e(-ms/t) \sum_{\ell \le y} (\log \ell) e((m/t + j\beta/2)\ell).$$

To estimate the inner sum, we now use two standard results on exponential sums in primes, which appear as Theorem 3.1 and Lemma 3.1 in Vaughan [95].

Theorem 8.2.4 (Vinogradov)**.** *If $\alpha \in \mathbb{R}, a \in \mathbb{Z}, q \in \mathbb{N}$ with $\gcd(a,q) = 1, q \le y$, and $|\alpha - a/q| \le q^{-2}$ then*

$$\sum_{\substack{p \le y \\ p \text{ prime}}} (\log p) e(\alpha p) \ll (\log y)^4 (yq^{-1/2} + y^{4/5} + y^{1/2}q^{1/2}).$$

Lemma 8.2.5. *Let $B > 0$. If $\alpha \in \mathbb{R}, a \in \mathbb{Z}, q \in \mathbb{N}$ with $\gcd(a,q) = 1, q \le (\log y)^B$ and $|\alpha - a/q| \le (\log y)^B/y$ then there is $C_B > 0$ such that*

$$\sum_{\substack{p \le y \\ p \text{ prime}}} (\log p) e(\alpha p) = \frac{\mu(q)}{\varphi(q)} v(\alpha - a/q) + O_B(y\exp(-C_B\sqrt{\log p}))$$

where μ is the Möbius function, φ is the Euler totient function and $v(\beta) = \sum_{m=1}^{y} e(\beta m)$.

Suppose that $\alpha \in \mathbb{R}, a \in \mathbb{Z}, q \in \mathbb{N}$ with $\gcd(a,q) = 1, q \le y$, and $|\alpha - a/q| \le 1/qy$. If $q \le (\log y)^B$ we apply Lemma 8.2.5; otherwise we apply Theorem 8.2.4. Recalling the standard bound $\varphi(q) \gg \frac{q}{\log\log q}$, we have

$$\sum_{\substack{\ell \le y \\ \ell \text{ prime}}} (\log \ell) e(\alpha \ell) \ll_B y(\log y)^{4-B} + \frac{y \log\log q}{q}.$$

To complete the proof of Lemma 8.2.3, we take $B = 5$ and $\alpha = m/t + j\beta/2$, and find a and q satisfying the assumptions above using Dirichlet's approximation theorem. This gives us $a \in \mathbb{Z}, q \in \mathbb{N}$ with $\gcd(a,q) = 1$ and $q \le y$ such that $|(m/t + j\beta/2) - a/q| \le 1/qy$ holds, and we then have

$$\sum_{\substack{\ell \le y \\ \ell \text{ prime}}} (\log \ell) e((m/t + j\beta/2)\ell) \ll \frac{y}{\log y} + \frac{y \log\log q}{q}. \tag{8.14}$$

To apply this, we need a lower bound on q. For that we use Lemma 8.1.15 with $N = tjq$, which gives

$$\min_{M \in \mathbb{Z}} \log |2tjq\beta - M| \gg_E 1 - \widehat{h}(2tjqP).$$

By our choice of q we have

$$\min_{M \in \mathbb{Z}} \log |2tjq\beta - M| \le \log |2tjq\beta - 2tj + 2qm| \le \log(2t/y),$$

which gives us

$$1 + \log(y/t) \ll_E \widehat{h}(2tjqP).$$

Recalling that h is a quadratic form on $E(\mathbb{Q}) \otimes \mathbb{R}$, we have $1 + \log(y/t) \ll_E (tjq)^2 h(P)$ and hence either $y \ll t$ or

$$q \ge \frac{\log y}{tj\sqrt{h(P)}}.$$

We substitute this into (8.14) to show that either

$$\sum_{\substack{\ell \le y \\ \ell \text{ prime}}} (\log \ell) e(\ell(m/t + j\beta/2)) \ll_E y(\log y)^{-1} + \frac{ytj\sqrt{h(P)} \log\log\log y}{\log y} \quad \text{or} \quad y \ll t.$$

In the latter case we have $\sum_{\ell \le y} (\log \ell) e(\ell(m/t + j\beta/2)) \ll t$ by the Prime Number Theorem. So in any case

$$\sum_{\substack{\ell \le y \\ \ell \text{ prime}}} (\log \ell) e(\ell(m/t + j\beta/2)) \ll_E t + y(\log y)^{-1} + \frac{ytj\sqrt{h(P)} \log\log\log y}{\log y},$$

and this completes the proof of the lemma. □

With this, we are now finally ready to prove the main result of this section.

Proof of Proposition 8.0.5. From the assumptions on χ, there exists $\tau \in \{\pm 1\}$ such that $\chi(\tau|\beta_\alpha|) \neq 0, 1$. We separate into two cases depending on the real properties of P.

Case 1. $P \in E(\mathbb{R})^0$:

From Theorem 8.1.13 we have $\text{sign}(\beta_n) = \sigma^{n-1}(-1)^{\lfloor n\beta \rfloor}$ for some $\sigma \in \{\pm 1\}$ and some irrational number β. Now consider the set of primes

$$\Lambda = \{\ell \text{ prime} : \ell \equiv \alpha \bmod \pi, \text{sign}(\beta_\ell) = \tau\text{sign}(\beta_\alpha)\}\}.$$

Let $\ell \in \Lambda$. Then by periodicity we have $\beta_\ell \equiv \beta_\alpha \bmod q(\chi)$, so $\chi(\beta_\ell) = \chi(\beta_\alpha)$ as χ is periodic modulo $q(\chi)$. Moreover, we have arranged signs so that $\chi(|\beta_\ell|) = \chi(\tau|\beta_\alpha|) \neq 0, 1$. Hence as χ is multiplicative we deduce the existence of a prime factor p of $|\beta_\ell|$ with $p \nmid q(\chi)$ and $\text{ord}\,(\chi(p)) \nmid \nu_p(\beta_\ell)$. It thus suffices to note that $\{\ell \in \Lambda : \ell \leq x\}$ satisfies the required lower bound by Proposition 8.2.1.

Case 2. $P \notin E(\mathbb{R})^0$:

In order to handle a number of sub-cases simultaneously, we show that there is $\iota \in \{0, 1, 2, 3\}$ such that $\alpha + \iota\pi$ is odd and

$$(-1)^{(\alpha+\iota\pi-1)/2} = \begin{cases} \tau\text{sign}(\beta_\alpha), & \text{if } \alpha \text{ is even,} \\ \tau(-1)^{(\alpha-1)/2}, & \text{if } \alpha \text{ is odd.} \end{cases} \tag{8.15}$$

Case 2.1. α is even

Here π is odd since $(\alpha, \pi) = 1$. Choosing $\iota \in \{1, 3\}$ we can arrange for $\frac{\alpha+\iota\pi-1}{2}$ to be odd or even, and hence $(-1)^{(\alpha+\iota\pi-1)/2} = -1$ or 1 to satisfy (8.15).

Case 2.2. $2 \nmid \alpha$ and $4 \mid \pi$

In this case we have $\tau = 1$. Let $\iota = 0$ and then $(-1)^{(\alpha-1)/2} = \tau(-1)^{(\alpha-1)/2}$ as required for (8.15).

Case 2.3. $2 \nmid \alpha$ and $4 \nmid \pi$

We can choose $\iota \in \{0, 2\}$ so that $\iota\pi/2$ is odd or even as needed. So we arrange $(-1)^{\iota\pi/2} = \tau$ which gives (8.15).

We now let $q = \text{lcm}\,(4, \pi)$ and consider primes ℓ of the form $\ell \equiv \alpha + \iota\pi \bmod q$. By Theorem 8.1.13 and (8.15) we then have $\text{sign}(\beta_\ell) = \tau\text{sign}(\beta_\alpha)$. But $\beta_\ell \equiv \beta_\alpha \bmod q(\chi)$ by periodicity, so $\chi(|\beta_\ell|) = \chi(\tau|\beta_\alpha|) \neq 0, 1$, as χ is periodic modulo $q(\chi)$. We are now in a similar situation to Case 1. Note that $\alpha + \iota\pi$ is odd implies

that $\gcd(\alpha + \iota\pi, q) = 1$, and so by the Siegel-Walfisz Theorem, the set under consideration has size $\geq \left(\frac{1}{2\varphi(\pi)} + o(1)\right) \frac{x}{\log x}$, as desired.

□

8.3 On the proportion of nice characters

To find nice characters, we study the characters χ for which there exists $\alpha \in \mathbb{N}$ such that $\gcd(\alpha, \pi) = 1$ and $\chi(\beta_\alpha) \neq 0, \pm 1$, where $\pi := \pi(\chi)$ be the period of $\beta_n \pmod{q(\chi)}$. Then considering the arithmetic progression $\alpha \bmod \pi$ shows that there exists such an α with α prime, and there are infinitely many such primes. In addition $\chi(\beta_\alpha) = 0$ implies $\alpha = \mathrm{ord}(P \pmod p)$ for some prime $p \mid q(\chi)$, whenever α is a prime.

We can ignore this situation for large enough prime α, because $\mathrm{ord}(P \pmod p)$ is finite. In particular, it is now equivalent to look for χ for which there exists infinitely many primes ℓ such that $\chi(\beta_\ell) \neq \pm 1$. Note that, given any prime ℓ we have

$$\frac{\#\{\chi \text{ modulus } p : \chi(\beta_\ell) \in \{\pm 1\}\}}{\#\{\chi \text{ modulus } p\}} = \frac{2}{\mathrm{ord}(\beta_\ell)}, \tag{8.16}$$

where $\mathrm{ord}(\beta_\ell)$ denotes the corresponding order in the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^*$.

Now given a prime ℓ, we say a Dirichlet character χ is a ℓ-pseudo nice character if $\chi(\beta_\ell) \neq \pm 1$. We then have the following results applying the main theorems in [32].

Proposition 8.3.1. *Let ℓ be any prime for which $\beta_\ell \neq \pm 1$, then we have the following.*

(i) For all but $o(x/\log x)$ many primes p up-to x, the number of not ℓ-pseudo nice Dirichlet characters of prime modulus p is at most $2p^{1/2}\log p$.

(ii) Let $\varepsilon : \mathbb{N} \to \mathbb{R}$ be any unbounded sufficiently slow growing function. Then under the assumption of GRH, the number of ℓ-pseudo nice Dirichlet characters of prime modulus p is at most $\varepsilon(p)$, for all but $o(x/\log x)$ many primes p up-to x.

Proof. Part (i) follows the introduction in [32], and part (ii) follows from [32, Theorem 4]. □

Furthermore, we say a that Dirichlet character χ is a ℓ-nice character if

$$\chi(\beta_\ell) \neq 0, \pm 1, \text{ and } \ell \nmid \pi.$$

In particular, we now need to take care of those primes p for which

$$\ell = \mathrm{ord}(P \pmod p), \text{ or } \ell \mid \pi.$$

It follows from Lemma 8.1.11, assuming $(\ell, M) = 1$ that

$$\ell \mid p - 1 \text{ or, } \ell \mid \mathrm{ord}(P \pmod p), \text{ or } \ell \mid \mathrm{ord}(MP \pmod p).$$

To eliminate those primes, we use the following lemma.

Lemma 8.3.2. *Let $P \in E(\mathbb{Q})$ be any point, and ℓ be a prime such that the ℓ-adic Galois representation for E $\rho_\ell : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ is surjective. Then the set of primes p for which $\ell \mid \mathrm{ord}(P \pmod p)$ has density at most $\frac{\ell}{\ell^2-1}$.*

Proof. Let P be a prime unramified in $\mathbb{Q}(E[\ell])$ such that $\ell \mid \mathrm{ord}\,(P \bmod P)$. This implies that $E(\mathbb{F}_P)[\ell] \neq 0$, which is equivalent to

$$\det(I_2 - \rho_\ell(\mathrm{Frob}_p)) = 0. \tag{8.17}$$

There are $\ell(\ell+1)(\ell-1)^2$ elements in $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$, and among them there are $\ell^3 - \ell^2$ many elements $x \in \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ that satisfy the equation $\det(I_2 - x) = 0$. Thus, by the Chebotarev's density theorem, the proportion of primes p that satisfy (8.17) is

$$\frac{\ell^3 - \ell^2}{\ell(\ell+1)(\ell-1)^2} = \frac{\ell}{\ell^2 - 1}.$$

□

Let us now note the following facts due to Siegel's theorem on the finiteness of integral points on an elliptic curve.

Lemma 8.3.3. *(i) For any integer f, there exists ℓ_f such that for any prime $\ell > \ell_f$, $\beta_\ell^f \neq 1$.*

(i) Under the ABC conjecture, for any sufficiently large f, we have *$\beta_\ell^f \neq 1$ for any prime ℓ.*

Proof. Proof of part (i) follows from [34, Theorem 1] and part (ii) from from [34, Remark 1.2]. In fact, the reader may also look at Theorem 1.3 and Corollary 1.7 in [60]. □

In particular, we now obtain the following.

Theorem 8.3.4 (Bhakta)**.** *Let $E/\mathbb{Q}$ be any elliptic curve without CM, and then we have the following for all but finitely many primes ℓ:*

(i) For a set of primes p of density at least $1 - O(\frac{1}{\ell})$, the number of not ℓ-nice Dirichlet characters of prime modulus p is at most $2p^{1/2}\log p$.

(ii) Let $\varepsilon : \mathbb{N} \to \mathbb{R}$ be any unbounded slow growing function. Then under the assumption of GRH, for a set of primes p of density at least $1 - O(\frac{1}{\ell})$, the number of not ℓ-nice Dirichlet characters of prime modulus p is at most $\varepsilon(p)$.

Remark 8.3.5. Note that both parts in Theorem 8.3.4 are valid for a set of primes having positive density, and in fact, the density is close to 1 as long as ℓ is large. So what about other primes? in the exceptional cases, do we get at least one nice character? It follows from (8.16) that For any prime ℓ, $|\beta_\ell|$ has order $\geq d$ in $(\mathbb{Z}/p\mathbb{Z})^*$ if and only if, the number of not ℓ-nice characters modulo p is at most $\frac{2\phi(p)}{d}$. In

particular, for any prime p, there must exist at least one nice Dirichlet character modulo p, provided that $\phi(p) - \frac{2\phi(p)}{d} > 0$, or equivalently if $d > 2$. For that we can use Lemma 8.3.3. In particular, the ABC conjecture implies that given any prime ℓ, there exists p_ℓ such that for any prime $p > p_\ell$ there exists a Dirichlet character χ of modulus p for which $\chi(\beta_\ell) \neq \pm 1$.

The hard part is to ensure that χ is indeed a nice character, i.e. we need that $\chi(\beta_\ell) \neq 0$ and $(\ell, \pi) = 1$, where π is the period of (β_n) modulo $q := q(\chi)$. Then we see from Lemma 8.1.11 that we might face problems when $p \equiv 1 \pmod{\ell}$.

8.4 Associated character sums and exponential sums

Let us recall from Theorem 8.1.6 that the sequence (β_n) is an elliptic divisibility sequence provided that $M = 1$, or equivalently if P has good reduction any every prime. In this section, we shall study character sums associated to any such elliptic divisibility sequence.

Definition 8.4.1. *The discriminant of an elliptic divisibility sequence sequence (β_n) is defined to be*

$$\mathrm{disc}(\beta_n) = \beta_4\beta_2^{15} - 3\beta_4^2\beta_2^{10} + 3\beta_4^2\beta_2^{10} - 20\beta_4\beta_3^3\beta_2^7 + 3\beta_4^3\beta_2^5 + 16\beta_3^6\beta_2^4 + 8\beta_4^2 4\beta_3^3\beta_2^2 + \beta_4^4.$$

The elliptic divisibility sequence (β_n) is said to be nonsingular if

$$\beta_2 \neq 0,\ \beta_3 \neq 0,\ \mathrm{disc}(\beta_n) \neq 0.$$

Ward in [99] proves that any nonsingular elliptic divisibility sequences are equivalent to the division polynomials of an elliptic curve. Moreover, a singular sequence, up to equivalence, is either the trivial sequence $\mathbb{I}_n = n$ or a Lucas sequence $s_n = \frac{a^n - b^n}{a-b}$. In the next section, we shall study some associated character sums and exponential sums.

Characters sums associated to the division polynomials were considered by Shparlinski and Stange in [86]. They considered the quadratic case and remarked that their result could be generalized for any character. In this section, we first prove that generalization. For any integer π, any prime power q, and any Dirichlet character χ modulo q, let us consider

$$S_{\chi,\pi}(P) = \sum_{\substack{(n,\pi)=1 \\ 1 \leq n \leq R}} \chi(\beta_n),$$

where R is the order of $P \pmod{q}$. Then we have the following.

Proposition 8.4.2. *Suppose that (β_n) is non-singular, and χ has order d, then we have the following estimate*

$$S_{\chi,\pi}(P) = O(\omega(\pi)\phi(d)^{1/3} R^{1/2} q^{5/12} (\log q)^{4/3}).$$

Proof. For each prime $\ell' \mid \pi$, it is enough to prove that

$$\sum_{\substack{\ell' \mid n \\ 1 \leq n \leq R}} \chi(\beta_n) = O(\phi(d)^{1/3} R^{1/2} q^{5/12} (\log q)^{4/3}).$$

We know that $\beta_n = \Psi_n(P_0)$, for some non-torsion point $P_0 \in E'(\mathbb{Q})$, and for some elliptic curve $E'/\mathbb{Q}$. Now we proceed as in the proof of Theorem 6 in [86], and for any large parameter L consider the set of primes $S_L = \{R \leq \ell \leq L \mid \ell = 1 \pmod d\}$. We choose any L for which $\#S_L \sim \frac{1}{\phi(d)} \frac{L}{\log L}$. Denoting $W = \sum_{\ell \in S_L} \sum_{\substack{\ell' \mid n \\ 1 \leq n \leq R}} \chi(\Psi_{\ell n}(P_0))$, we argue as in [86], and get

$$|W|^2 \leq \sum_{\ell_1 \neq \ell_2 \in S_L} \sum_{\substack{\ell' \mid n \\ 1 \leq n \leq R}} \chi(\Psi_{\ell_1}(nP)\Psi_{\ell_2}(nP)) + O\left(qR \frac{1}{\phi(d)} \frac{L}{\log L}\right).$$

To bound the summation above, for each $\ell_1 \neq \ell_2$, apply Lemma 5 in [86] for the subgroup $H = \{nP \mid n \leq R,\ \ell' \text{ divides } n\}$, and obtain the following.

$$\sum_{\substack{\ell' \mid n \\ 1 \leq n \leq R}} \chi(\beta_n) \ll q^{1/2} R^{1/2} \phi(d)^{1/2} L^{-1/2} (\log L) + q^{1/4} R^{1/2} L.$$

The proof now follows taking $L \sim q^{1/6} (\log q)^{1/3} \phi(d)^{1/3}$. □

Now we study the singular (β_n), let us first consider the case when $\beta_n = c^{n^2-1} n$. Let χ be any Dirichlet character modulo prime p. Then for any prime ℓ of the form $1 + (p-1)k$ we have

$$\chi(\beta_\ell) = \chi(1-k) \neq 0, \pm 1,$$

for any infinitely many integers k. Therefore, we are now left to consider the case of Lucas sequences. The result may not necessarily be true for the arbitrary Lucas sequences. For example one may consider $s_{n+2} - ps_{n+1} + ps_n = 0$, and then $\chi(s_n) = 0$ for any Dirichlet character χ of modulus p. In this regard, one may ask the following stronger question.

Question 8.4.3. *Given a Lucas sequence s_n over $\mathbb{Q}$, for how many primes p we have $\{s_n \pmod p\} = \mathbb{F}_p$? and if that happens, how are all the residue classes distributed?*

Of course for any such prime p, we have $\chi(s_n) \neq 0, \pm 1$ for some n. We do not know any positive answer to the question above. We already discussed a weaker result in Theorem 2.3.2 in Chapter 2, as long as the characteristic polynomial for s_n is irreducible and monic in $\mathbb{Z}[x]$.

Let us now get back to the discussion on Proposition 8.4.2. First of all, a non-trivial estimate to $S_{\chi,\pi}(P)$ shows that if χ is even, then χ also must be a nice character. This is essentially because, if χ is even and not nice, then $\chi(|\beta_n|) = \chi(\beta_n)$,

and in particular $\chi(\beta_n)$ can only be 1 for any $(n, \pi\text{ord}(P \pmod q))) = 1$. Now the bound at Proposition 8.4.2 is non-trivial provided that

$$d^{2/3}q^{5/6} \ll R^{1-\varepsilon},$$

for some $\varepsilon > 0$. For this, roughly we need $d \ll q^{1/4-\varepsilon}$ and $R > q^{1-\varepsilon}$. In particular, the bound is non-trivial uniformly for all characters of not so large order, provided that $R > q^{1-\varepsilon}$. In this regard, we have the following when q is a prime.

Lemma 8.4.4. *Given any $\varepsilon > 0$, for all but $o_\varepsilon(x/\log x)$ many primes p up-to x, we have the following*

$$\text{ord}(P \pmod p) \gg p^{1/3-\varepsilon}.$$

Proof. Let us first recall the sequence (D_n) from Section 2 in [87]. Then it follows from (11) that we need to know the prime factors of (D_n). To prove the lemma, we need to show that

$$\#\{p, \text{ prime} \leq x \mid \text{ord}(P \pmod p) \leq x^{1/3-\varepsilon}\} = O_\varepsilon(x/\log x).$$

This is equivalent to show that $\omega\left(\prod_{n=1}^{1/3-\varepsilon} D_n\right) = O_\varepsilon(x/\log x)$. It follows from Lemma 8 in [87] that $\log D_n \ll_P n^2$. In particular, $\omega\left(\prod_{n=1}^{1/3-\varepsilon} D_n\right) = O_P(x^{1-\varepsilon})$,which completes the proof. □

We now ask the following.

Question 8.4.5. *Let $P \in E(\mathbb{Q})$ be any non-torsion point. Given any $\varepsilon > 0$, how often it is true that* $\text{ord}(P \pmod p) > p^{1-\varepsilon}$*?, when we vary over all the primes p.*

This is an analog of [32, Theorem 4], and could be considered as a weaker version of *elliptic analog of Artin's primitive root conjecture*. In other words, the conjecture is asking for the proportion of primes p for which $\text{ord}(P \pmod p) = \#E(\mathbb{F}_p) \sim p$. Gupta and Murty [45] showed under the assumption on GRH that we have a positive density when E is without CM, and $2, 3$ are inert in $\mathbb{Q}(\sqrt{-11})$. We are asking for a weaker result in Question 8.4.5. The reader may note that our question is an elliptic analog of [32, Theorem 4]. Recently Akbary, Ghioca, and Murty in [2] show under GRH and ARH (Artin's holomorphy conjecture) that the answer to Question 8.4.5 is positive as long as we consider the subgroups of $E(\mathbb{Q})$ with large enough rank.

8.4.1 On a multilinear version

As an application to the unconditional result in Lemma 8.4.4 we can use Theorem 5.1.3 to get non-trivial multilinear (with more than 83-fold products) exponential sums associated with (β_n), for almost all the prime fields. To be more precise, for any tuple of integers $\vec{n} = (n_1, n_2, \cdots, n_r)$, set $\beta_{\vec{n}} = \beta_{n_1}\beta_{n_2}\cdots\beta_{n_r}$. First of all note that, if $\chi(\beta_{\vec{n}}) \neq 0, \pm 1$ for some tuple $\vec{n}$ whose all the co-ordinates are co-prime to π, then $\chi(\beta_n) \neq 0, \pm 1$ for some some n co-prime. In particular, χ is a nice character. However, a converse of this phenomenon may not be true in general because

$\chi(\beta_m) \neq 0, \pm 1$ and $\chi(\beta_n) \neq 0, \pm 1$ does not imply $\chi(\beta_m \beta_n) \neq 0, \pm 1$. Therefore, it may be helpful with work with this product version. Combining Lemma 8.4.4 and Theorem 5.1.3, we obtain the following.

Proposition 8.4.6. *Almost all the primes p have the following property: for any $r \geq 83$, any element in $\mathbb{F}_p$ can be written sum of at $O(1)$-elements of the form $\beta_{\vec{n}}$, where $\vec{n} \in \mathbb{Z}^r$.*

Regarding this, we ask the following.

Question 8.4.7. *Does there exist an r such that for almost all primes p, any element in $\mathbb{F}_p$ can be written as $\beta_{\vec{n}}$?*

Bibliography

[1] A. Akbary, J. Bleaney, and S. Yazdani. On symmetries of elliptic nets and valuations of net polynomials. *J. Number Theory*, 158:185–216, 2016.

[2] A. Akbary, D. Ghioca, and V. K. Murty. Reductions of points on elliptic curves. *Math. Ann.*, 347(2):365–394, 2010.

[3] A. Akbary, M. Kumar, and S. Yazdani. The signs in elliptic nets. *New York J. Math.*, 23:1237–1264, 2017.

[4] E. Aksoy Yazici, B. Murphy, M. Rudnev, and I. Shkredov. Growth estimates in positive characteristic via collisions. *Int. Math. Res. Not. IMRN*, (23):7148–7189, 2017.

[5] M. Ayad. Périodicité (mod q) des suites elliptiques et points S-entiers sur les courbes elliptiques. *Ann. Inst. Fourier (Grenoble)*, 43(3):585–618, 1993.

[6] J. Bajpai. *On vector valued automorphic forms*. Ph.D. Thesis (Advisor: Terry Gannon), University of Alberta, (2015), 2014.

[7] J. Bajpai. Lifting of modular forms. *Publications Mathématiques de Besançon*, (1):5–20, 2019.

[8] J. Bajpai and S. Bhakta. Lifting of vector-valued automorphic forms. *arXiv:2203.14937*, 2022.

[9] J. Bajpai, S. Bhakta, and R. Finder. Growth of Fourier coefficients of vector-valued automorphic forms. *J. Number Theory*, 249:237–273, 2023.

[10] J. Bajpai, S. Bhakta, and V. C. García. Exponential sums in prime fields for modular forms. *Res. Number Theory*, 8(1):Paper No. 18, 32, 2022.

[11] T. Barnet-Lamb, D. Geraghty, M. Harris, and R. Taylor. A family of Calabi-Yau varieties and potential automorphy II. *Publ. Res. Inst. Math. Sci.*, 47(1):29–98, 2011.

[12] A. F. Beardon. The structure of words in discrete subgroups of SL(2, C). *J. London Math. Soc. (2)*, 10:201–211, 1975.

[13] S. Bhakta. Distribution of non-wieferich primes in certain algebraic groups under abc. *2002.11941*, 2020.

[14] S. Bhakta. Galois representations and composite moduli. *arXiv:2105.11230*, 2023.

[15] S. Bhakta, S. Krishnamoorthy, and R. Muneeswaran. Congruence classes for modular forms over small sets. *arXiv:2302.02725*, 2023.

[16] S. Bhakta, D. Loughran, S. Myerson, and M. Nakahara. The elliptic sieve and brauer groups. *arXiv:2109.03746*, 2021.

[17] V. Blomer and F. Brumley. The role of the Ramanujan conjecture in analytic number theory. *Bull. Amer. Math. Soc. (N.S.)*, 50(2):267–320, 2013.

[18] V. Bosser and E. Gaudron. Logarithmes des points rationnels des variétés abéliennes. *Canad. J. Math.*, 71(2):247–298, 2019.

[19] J. Bourgain. Mordell's exponential sum estimate revisited. *J. Amer. Math. Soc.*, 18(2):477–499, 2005.

[20] J. Bourgain and M.-C. Chang. A Gauss sum estimate in arbitrary finite fields. *C. R. Math. Acad. Sci. Paris*, 342(9):643–646, 2006.

[21] J. Bourgain and A. Glibichuk. Exponential sum estimates over a subgroup in an arbitrary finite field. *J. Anal. Math.*, 115:51–70, 2011.

[22] J. Bourgain, A. A. Glibichuk, and S. V. Konyagin. Estimates for the number of sums and products and for exponential sums in fields of prime order. *J. London Math. Soc. (2)*, 73(2):380–398, 2006.

[23] T. Browning and D. Loughran. Sieving rational points on varieties. *Trans. Amer. Math. Soc.*, 371(8):5757–5785, 2019.

[24] J. Brüdern, K. Matomäki, R. Vaughan, and T. Wooley. *Analytic Number Theory*. Oberwolfach Report, 2019.

[25] F. Campagna. Cyclic reduction of elliptic curves. *ALGANT Master Thesis*, 2018.

[26] L. Candelori, T. Hartland, C. Marks, and D. Yépez. Indecomposable vector-valued modular forms and periods of modular curves. *Res. Number Theory*, 4(2):Paper No. 17, 24, 2018.

[27] A. C. Cojocaru. On the surjectivity of the Galois representations associated to non-CM elliptic curves. *Canad. Math. Bull.*, 48(1):16–31, 2005. With an appendix by Ernst Kani.

[28] P. Deligne. La conjecture de Weil. I. *Inst. Hautes Études Sci. Publ. Math.*, (43):273–307, 1974.

[29] F. Diamond and J. Shurman. *A first course in modular forms*, volume 228 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2005.

[30] M. Eichler. Grenzkreisgruppen und kettenbruchartige Algorithmen. *Acta Arith.*, 11:169–180, 1965.

[31] M. Eichler and D. Zagier. *The theory of Jacobi forms*, volume 55 of *Progress in Mathematics*. Birkhäuser Boston Inc., Boston, MA, 1985.

[32] P. Erdős and M. R. Murty. On the order of $a \pmod p$. In *Number theory (Ottawa, ON, 1996)*, volume 19 of *CRM Proc. Lecture Notes*, pages 87–97. Amer. Math. Soc., Providence, RI, 1999.

[33] P. Erdös and P. Turán. On a problem in the theory of uniform distribution. I. *Nederl. Akad. Wetensch., Proc.*, 51:1146–1154 = Indagationes Math. 10, 370–378 (1948), 1948.

[34] G. Everest, J. Reynolds, and S. Stevens. On the denominators of rational points on elliptic curves. *Bull. Lond. Math. Soc.*, 39(5):762–770, 2007.

[35] G. Everest, A. van der Poorten, I. Shparlinski, and T. Ward. *Recurrence sequences*, volume 104 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 2003.

[36] G. Everest, A. van der Poorten, I. Shparlinski, and T. Ward. *Recurrence sequences*, volume 104 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 2003.

[37] A. Ferraguti. Galois representation attached to type $(1, \chi)$ modular forms. 2011.

[38] T. Gannon. The theory of vector-valued modular forms for the modular group. In *Conformal field theory, automorphic forms and related topics*, volume 8 of *Contrib. Math. Comput. Sci.*, pages 247–286. Springer, Heidelberg, 2014.

[39] M. Z. Garaev. An explicit sum-product estimate in $\mathbb{F}_p$. *Int. Math. Res. Not. IMRN*, (11):Art. ID rnm035, 11, 2007.

[40] M. Z. Garaev. Sums and products of sets and estimates for rational trigonometric sums in fields of prime order. *Uspekhi Mat. Nauk*, 65(4(394)):5–66, 2010.

[41] M. Z. Garaev, V. C. García, and S. V. Konyagin. The Waring problem with Ramanujan's τ-function. *Izv. Ross. Akad. Nauk Ser. Mat.*, 72(1):39–50, 2008.

[42] V. C. García. On the distribution of sparse sequences in prime fields and applications. *J. Théor. Nombres Bordeaux*, 25(2):317–329, 2013.

[43] V. C. García and F. Nicolae. Additive bases with coefficients of newforms. *Forum Math.*, 30(5):1079–1087, 2018.

[44] D. Grant. A formula for the number of elliptic curves with exceptional primes. *Compositio Math.*, 122(2):151–164, 2000.

[45] R. Gupta and M. R. Murty. Primitive points on elliptic curves. *Compositio Math.*, 58(1):13–44, 1986.

[46] M. Hindry and J. H. Silverman. *Diophantine geometry: an introduction*, volume 201. Springer Science & Business Media, 2013.

[47] N. Jones. Pairs of elliptic curves with maximal Galois representations. *J. Number Theory*, 133(10):3381–3393, 2013.

[48] M. Jutila. On exponential sums involving the Ramanujan function. *Proc. Indian Acad. Sci. Math. Sci.*, 97(1-3):157–166 (1988), 1987.

[49] N. M. Katz. *Gauss sums, Kloosterman sums, and monodromy groups*, volume 116 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 1988.

[50] B. Kim and S. Lim. L-series for vector-valued modular forms. *Taiwanese J. Math.*, 20(4):705–722, 2016.

[51] M. Knopp and G. Mason. On vector-valued modular forms and their Fourier coefficients. *Acta Arith.*, 110(2):117–124, 2003.

[52] M. Knopp and G. Mason. Vector-valued modular forms and Poincaré series. *Illinois J. Math.*, 48(4):1345–1366, 2004.

[53] M. Knopp and G. Mason. Logarithmic vector-valued modular forms. *Acta Arith.*, 147(3):261–282, 2011.

[54] M. Knopp and G. Mason. Logarithmic vector-valued modular forms and polynomial-growth estimates of their Fourier coefficients. *Ramanujan J.*, 29(1-3):213–223, 2012.

[55] M. I. Knopp. *Modular functions in analytic number theory*. Markham Publishing Co., Chicago, Ill., 1970.

[56] M. I. Knopp. Some new results on the Eichler cohomology of automorphic forms. *Bull. Amer. Math. Soc.*, 80:607–632, 1974.

[57] N. M. Korobov. The distribution of non-residues and of primitive roots in recurrence series. *Doklady Akad. Nauk SSSR (N.S.)*, 88:603–606, 1953.

[58] N. M. Korobov. *Exponential sums and their applications*, volume 80 of *Mathematics and its Applications (Soviet Series)*. Kluwer Academic Publishers Group, Dordrecht, 1992. Translated from the 1989 Russian original by Yu. N. Shakhov.

[59] E. Kowalski. *Exponential sums over finite fields: elementary methods*. `https://people.math.ethz.ch/~kowalski/exponential-sums-elementary.pdf`, 2021.

[60] U. Kühn and J. S. Müller. A height inequality for rational points on elliptic curves implied by the *abc*-conjecture. *Funct. Approx. Comment. Math.*, 52(1):127–132, 2015.

[61] G. Lachaud and R. Rolland. On the number of points of algebraic sets over finite fields. *J. Pure Appl. Algebra*, 219(11):5117–5136, 2015.

[62] R. Lidl and H. Niederreiter. *Introduction to finite fields and their applications*. Cambridge University Press, Cambridge, 1986.

[63] D. W. Masser and G. Wüstholz. Galois properties of division fields of elliptic curves. *Bull. London Math. Soc.*, 25(3):247–254, 1993.

[64] D. W. Masser and G. Wüstholz. Galois properties of division fields of elliptic curves. *Bull. London Math. Soc.*, 25(3):247–254, 1993.

[65] L. Mathewson. The class equation of gl2 (fq). 2012.

[66] W. McCallum, W. Stein, and J. Voight. *Rational and Integral Points on Higher Dimensional Varieties*. Lecture notes for ARCC workshop held at AIM in Palo Alto, December 11-20, 2002.

[67] T. Miyake. *Modular forms*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, english edition, 2006. Translated from the 1976 Japanese original by Yoshitaka Maeda.

[68] H. L. Montgomery and R. C. Vaughan. *Multiplicative number theory. I. Classical theory*, volume 97 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2007.

[69] J. S. Morrow. Composite images of Galois for elliptic curves over $\mathbf{Q}$ and entanglement fields. *Math. Comp.*, 88(319):2389–2421, 2019.

[70] M. R. Murty. Oscillations of Fourier coefficients of modular forms. *Math. Ann.*, 262(4):431–446, 1983.

[71] M. R. Murty. *Problems in analytic number theory*, volume 206 of *Graduate Texts in Mathematics*. Springer, New York, second edition, 2008. Readings in Mathematics.

[72] R. A. Rankin. Contributions to the theory of Ramanujan's function $\tau(n)$ and similar arithmetical functions. I. The zeros of the function $\sum_{n=1}^{\infty} \tau(n)/n^s$ on the line $\mathrm{Re}(s) = 13/2$. II. The order of the Fourier coefficients of integral modular forms. *Proc. Cambridge Philos. Soc.*, 35:351–372, 1939.

[73] K. A. Ribet. Galois action on division points of Abelian varieties with real multiplications. *Amer. J. Math.*, 98(3):751–804, 1976.

[74] K. A. Ribet. On l-adic representations attached to modular forms. II. *Glasgow Math. J.*, 27:185–194, 1985.

[75] O. Roche-Newton, M. Rudnev, and I. D. Shkredov. New sum-product type estimates over finite fields. *Adv. Math.*, 293:589–605, 2016.

[76] M. Rudnev. An improved sum-product inequality in fields of prime order. *Int. Math. Res. Not. IMRN*, (16):3693–3705, 2012.

[77] P. Sarnak. *Some applications of modular forms*, volume 99 of *Cambridge Tracts in Mathematics*. Cambridge University Press, Cambridge, 1990.

[78] A. Selberg. On the estimation of Fourier coefficients of modular forms. In *Proc. Sympos. Pure Math., Vol. VIII*, pages 1–15. Amer. Math. Soc., Providence, R.I., 1965.

[79] J.-P. Serre. Divisibilité de certaines fonctions arithmétiques. In *Séminaire Delange-Pisot-Poitou, 16e année (1974/75), Théorie des nombres, Fasc. 1, Exp. No. 20*, page 28. 1975.

[80] J.-P. Serre. *Abelian l-adic representations and elliptic curves*, volume 7 of *Research Notes in Mathematics*. A K Peters, Ltd., Wellesley, MA, 1998. With the collaboration of Willem Kuyk and John Labute, Revised reprint of the 1968 original.

[81] G. Shimura. *Introduction to the arithmetic theory of automorphic functions*. Publications of the Mathematical Society of Japan, No. 11. Iwanami Shoten, Publishers, Tokyo, 1971. Kanô Memorial Lectures, No. 1.

[82] R. Shipsey. *Elliptic Divisibility Sequences,*. Ph.D. Thesis, Goldsmiths College, London University., 2000.

[83] I. D. Shkredov. On asymptotic formulae in some sum-product questions. *Trans. Moscow Math. Soc.*, 79:231–281, 2018.

[84] I. E. Shparlinski. Bounds of Gauss sums in finite fields. *Proc. Amer. Math. Soc.*, 132(10):2817–2824, 2004.

[85] I. E. Shparlinski. On the value set of the Ramanujan function. *Arch. Math. (Basel)*, 85(6):508–513, 2005.

[86] I. E. Shparlinski and K. E. Stange. Character sums with division polynomials. *Canad. Math. Bull.*, 55(4):850–857, 2012.

[87] J. H. Silverman. Wieferich's criterion and the *abc*-conjecture. *J. Number Theory*, 30(2):226–237, 1988.

[88] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1992. Corrected reprint of the 1986 original.

[89] J. H. Silverman. p-adic properties of division polynomials and elliptic divisibility sequences. *Math. Ann.*, 332(2):443–471, 2005.

[90] J. H. Silverman and N. Stephens. The sign of an elliptic divisibility sequence. *J. Ramanujan Math. Soc.*, 21(1):1–17, 2006.

[91] K. E. Stange. Integral points on elliptic curves and explicit valuations of division polynomials. *Canad. J. Math.*, 68(5):1120–1158, 2016.

[92] P. Stevenhagen and H. W. Lenstra, Jr. Chebotarëv and his density theorem. *Math. Intelligencer*, 18(2):26–37, 1996.

[93] K. Takeuchi. Arithmetic triangle groups. *J. Math. Soc. Japan*, 29(1):91–106, 1977.

[94] J. Thorner. Effective forms of the Sato–Tate conjecture. *arXiv*, 2020.

[95] R. C. Vaughan. *The Hardy-Littlewood method*, volume 125 of *Cambridge Tracts in Mathematics*. Cambridge University Press, Cambridge, second edition, 1997.

[96] A. B. Venkov. *Spectral theory of automorphic functions and its applications*, volume 51 of *Mathematics and its Applications (Soviet Series)*. Kluwer Academic Publishers Group, Dordrecht, 1990. Translated from the Russian by N. B. Lebedinskaya.

[97] M. Verzobio. A recurrence relation for elliptic divisibility sequences. *arXiv:2102.07573*, 2021.

[98] I. M. Vinogradov. *Elements of number theory*. Dover Publications, Inc., New York, 1954. Translated by S. Kravetz.

[99] M. Ward. Memoir on elliptic divisibility sequences. *Amer. J. Math.*, 70:31–74, 1948.

[100] D. Zywina. Elliptic curves with maximal Galois action on their torsion points. *Bull. Lond. Math. Soc.*, 42(5):811–826, 2010.

[101] D. Zywina. On the surjectivity of mod ℓ representations associated to elliptic curves. *arXiv*, 2015.