Ramanujan Mathematical Society

Lecture Notes Series

Number 26

Topics in Number Theory

Proceedings of a Conference Organised by the Institute of Mathematical Sciences, Chennai and IIT Ropar during 22–25th December, 2017

On the Occasion of the 130th Birth Anniversary of Srinivasa Ramanujan

Volume Editors

Tapas Chatterjee

Department of Mathematics,
Indian Institute of Technology,
Ropar Nangal Road, Rupnagar,
Punjab 140 001, India

Sanoli Gun

Department of Mathematics,
The Institute of Mathematical Sciences,
CIT Campus Taramani,
Chennai 600 113, Tamil Nadu, India

Published by

Ramanujan Mathematical Society
2020

ISBN: 978-81-936684-1-2

Published by Ramanujan Mathematical Society, India

For Ordering Contact:

The Managing Editor
Dr. E. Sampathkumar
RMS-LNS Office, 8/1, 13th Cross, Adipampa Road,
V. V. Mohalla, Mysore 570 002, India.
Phone: +91 821 2511006, Mobile: +91 9448978303
Email: esampathkumar@gmail.com
Visit us at **http://www.ramanujanmathsociety.org**

Typeset in LaTeX by Krishtel eMaging Solutions Pvt. Ltd.,
Door No. 3/2, Plot No. 68, Ist Floor, Kadamban Street, M.S.M. Nagar,
Valasaravakkam, Chennai 600 087, Tamil Nadu, India.
Phone: +91 44 2486 1316, Mobile: 9444116242.
E-mail: nss@krishtelemaging.com
website: www.krishtelemaging.com

Printed at Image Screens, # 262, Triplicane High Road,
Chennai 600 005, Tamilnadu, India. Phone: +91 8122216899
E-mail: imagescreens@gmail.com

RMS Lecture Notes Series in Mathematics

Lecture Notes Series in Mathematics (LNSM) is published by the Ramanujan Mathematical Society (RMS). The type of material considered for publication in LNSM includes (1) High-level research monographs covering a broad spectrum of topics (2) Proceedings of Conferences (3) "Collected Works" and "Selected Works" of eminent mathematicians (4) Current research oriented summer schools and intensive courses.

Editorial Board

Editorial Policy

The Editors invite well-written monograph length manuscripts on any topic in mathematics. Excellent expositions of known topics, accessible expositions of emerging topics, or proceedings of conferences on topics of current activity are especially welcome.

Authors are encouraged to contact editors with their manuscript ideas at an early stage so as to get feedback about appropriateness. In the case of a proceedings volume, the organizers are asked to submit the title of the conference, names of all members of the organizing committee, and the list of speakers along with the titles and abstracts of their talks.

All submitted monographs should include a table of contents, an introduction with historical background and motivation, a discussion of open problems and research directions for future work, a subject index and a sufficiently extensive bibliography so as to guide readers in the literature.

In the case of a proceedings volume, submissions should include the articles and referee reports as well as the list of participants.

Submissions should be electronic, in pdf format, and sent by email to the Managing Editors who will forward them to the appropriate Editor for scientific review. Manuscripts may be sent to esampathkumar@gmail.com

All submitted manuscripts will undergo a review for mathematical accuracy, quality of exposition and interest to the community. The decision of the Editorial Board regarding the suitability of a submission for publication in this series will be final.

Preface

December 22, 2017 marked the 130 birth anniversary of Srinivasa Ramanujan. To commemorate this occasion, the Institute of Mathematical Sciences (Chennai) and the Indian Institute of Technology (Ropar) organized an international conference on Number Theory. The conference was held at IIT Ropar during December 22–25, 2017. It featured a very diverse group of speakers and correspondingly, the talks covered many different areas of Number Theory. In particular, there were talks on L-functions, Automorphic forms, Abelian varieties and Transcendence.

We are thankful to the participants of the conference who provided a vibrant intellectual atmosphere amidst the verdant surroundings in Ropar. We had a rewarding and fulfilling experience as organisers, and we take this opportunity to thank our institutes IMSc, Chennai and IIT Ropar for their unfailing and continuous support for this conference.

To enable young researchers an opportunity to glimpse the state-of-the-art in these important areas of Number Theory, it was decided to publish the proceedings of the conference. We are really grateful to the speakers who kindly agreed to give us their articles and were patient with the refereeing process.

Finally, we would like to thank the editorial board members and the technical staff of the RMS Lecture Notes Series without whose support this proceedings would not have seen the light of day.

Tapas Chatterjee and Sanoli Gun

Members of the Advisory Board

LIST OF PARTICIPANTS

Speakers

(1) S. D. Adhikari, HRI Allahabad
(2) S. Baier, JNU Delhi
(3) A. Bhand, IISER Bhopal
(4) A. Bharadwaj, CMI Chennai
(5) T. Chatterjee, IIT Ropar
(6) S. Das, IISc Bangalore
(7) T. Dalal , IIT Hyderabad
(8) P. Darbar, IMSc Chennai
(9) S. David, University of Paris VI, France
(10) P. K. Dey, ISI Delhi
(11) S. Dhillon, IIT Ropar
(12) Anup Dixit, University of Toronto, Canada
(13) Atul Dixit, IIT Gandhinagar
(14) S. Eliahou, Université du Littoral Cote d' Opale, France
(15) E. Ghate, TIFR Mumbai
(16) S. Gun, IMSc Chennai
(17) R. Gupta, IIT Gandhinagar
(18) S. Jha, IIT Kanpur
(19) S. Khanduja, IISER Mohali
(20) S. S. Khurana, IIT Ropar
(21) A. Kumar, HRI Allahabad
(22) B. Kumar, IMSc Chennai
(23) M. Kumar, IIT Ropar
(24) N. Kumar, IIT Hyderabad
(25) R. Kumar, IIT Gandhinagar
(26) M. Kumari, NISER Bhubaneswar

(27) S. Laishram, ISI Delhi
(28) B. Maji, IIT Gandhinagar
(29) M. Manickam, KSOM Kozhikode
(30) K. Matsumoto, Nagoya University, Japan
(31) J. Meher, NISER Bhubaneswar
(32) N. K. Meher, HRI Allahabad
(33) R. Murty, Queens University, Canada
(34) K. Murty, University of Toronto, Canada
(35) J. Oesterlé, University of Paris VI, France
(36) F. Pazuki, The University of Copenhagen, Denmark
(37) P. Akhilesh, IMSc Chennai
(38) S. Pathak, Queens University, Canada
(39) B. Paul, IMSc Chennai
(40) P. Philippon, CNRS, France
(41) G. Prakash, HRI Allahabad
(42) C. S. Rajan, TIFR Mumbai
(43) B. Ramakrishnan, HRI Allahabad
(44) P. Rath, CMI Chennai
(45) S. Jyothsnaa, IMSc Chennai
(46) E. Saha, TIFR Mumbai
(47) B. Saha, TIFR Mumbai
(48) B. Sahu, NISER Bhubaneswar
(49) A. Sankaranarayanan, TIFR Mumbai
(50) K. Deo Shankhadhar, IISER Bhopal
(51) K. Sinha, IISER Pune
(52) D. Suryaramana, HRI Allahabad
(53) A. Vatwani, IIT Ghandinagar

Contents

Topics in Number Theory, RMS-Lecture Notes Series No. 26, 2020, pp. 1–20.

On the Non-Vanishing of Periodic Dirichlet Series

Abhishek T. Bharadwaj

Chennai Mathematical Institute, H1 Sipcot IT Park, Siruseri, Kellambakkam,
Chennai 603 103, India.
e-mail: abhitvt@cmi.ac.in

Abstract. The article describes the state of the art on the question of non-vanishing of $L(1, f)$ for periodic arithmetic functions f. En-route, we also have some supplementary results for odd periodic arithmetic functions f. The methods used here build upon purely algebraic conditions.

Keywords. Dirichlet L functions, linear forms in logarithms, Erdős conjecture.

Subject Classification: 11M06, 11J86

1. Introduction

A complex number α is said to be an algebraic number if it is a root of a non-zero polynomial equation with integer entries. The complex numbers which do not satisfy any such polynomial equation are called transcendental numbers. The first example of a transcendental number was found by Liouville in the year 1844, where he proved that $\sum_{n=1}^{\infty} \frac{1}{10^{n!}}$ is transcendental. Hermite went on to prove that e is transcendental in 1873. Shortly after that, Lindemann proved the transcendence of π and stated the linear independence of exponentials of algebraic numbers over the field of algebraic numbers $\overline{\mathbb{Q}}$. This was rigorously proved by Weierstrass in 1885.

We are interested in the special values of the Dirichlet series defined by

$$L(s, f) := \sum_{n=1}^{\infty} \frac{f(n)}{n^s} \quad \text{for } \Re(s) > 1,$$

where $f : \mathbb{N} \to \mathbb{C}$ is an arithmetic function of period $q \geq 1$ i.e. $f(n+q) = f(n)$ for all integers n. The Hurwitz zeta functions evaluated at the rational numbers a/q for $1 \leq a \leq q$ are the building blocks for these periodic Dirichlet series. The Hurwitz zeta function is defined by the series :

$$\zeta(s, x) := \sum_{n=0}^{\infty} \frac{1}{(n+x)^s} \qquad \text{for } \Re(s) > 1 \quad \text{and} \quad 0 < x \leq 1.$$

Hurwitz had proved that $\zeta(s, x)$ extends analytically to the entire complex plane, apart from $s = 1$, where it has a simple pole with residue 1. Note that $\zeta(s, 1)$ is the classical Riemann zeta function $\sum_{n=1}^{\infty} \frac{1}{n^s}$.

It is a standard result that for a non-zero complex valued function f, there exists a real number σ such that $L(s, f)$ does not attain a zero whenever $\Re(s) > \sigma$. However, we cannot conclude that $L(s, f)$ has finitely many zeros. In fact, $\zeta(s, x)$ does have infinitely many zeros in $\Re(s) > 1$ when $x \neq 1, 1/2$. This was shown by Davenport and Heilbronn [12] for rational as well as transcendental x and by Cassels [8] when x is an irrational algebraic number.

However, in this article, our primary focus will be on the transcendental nature of $L(s, f)$ at $s = 1$ for periodic arithmetic function f, whenever it exists. We would like to make a remark that $L(s, f)$ cannot be evaluated at $s = 1$ for all periodic arithmetic functions f. When the sum $\sum_{n\geq 1} \frac{f(n)}{n}$ converges, then the function $L(s, f)$ can be extended beyond $\Re(s) > 1$ and it turns out that the value $L(1, f)$ is nothing but $\sum_{n\geq 1} \frac{f(n)}{n}$. Hence we freely use the notation $L(1, f)$ to denote $\sum_{n\geq 1} \frac{f(n)}{n}$.

The first non-trivial and important examples of Dirichlet series are $L(s, \chi)$ for a character χ of conductor f_χ. The proof of infinitude of primes in arithmetic progression $an + b$ with $(a, b) = 1$, boils down to non-vanishing of $L(1, \chi)$ for non-principal characters χ of period a and hence such non-vanishing question is of great interest. One of the interesting aspects about these numbers is that they are transcendental numbers. The proof of the above involves Baker's theory of linear form in logarithms. When f is periodic, we mention the criteria for the convergence of the sum $L(s, f)$ at $s = 1$ along with the explicit expression of $L(1, \chi)$ for Dirichlet Characters χ in Section 2.

We now look at the result by replacing characters with certain algebraic valued arithmetic functions f. More generally, we want to address the question of non-vanishing of $L(1, f)$ by removing the property of Euler product. In relation to this, Chowla had asked the following question in 1969 in a number theory conference:

Question 1.1. *Does there exist a rational valued arithmetic function f, periodic with prime period p such that $L(1, f) = 0$ whenever it converges?*

Baker, Birch and Wirsing generalized this question and answered it by using Baker's theory of linear forms in logarithms in 1973. Their proof involves the non-vanishing of $L(1, \chi)$. However, for odd rational valued arithmetic functions of prime period, the proof can be simplified. We present it in Section 3.

One of the long standing conjectures in this topic is Erdős Conjecture. In a written communication with Livingston [15], Paul Erdős had made the following conjecture which we quote verbatim.

Conjecture 1.2. *If q is a positive integer and f is a number theoretic function with period q and $f(n) \in \{-1, 1\}$ when $n = 1, 2, \ldots q - 1$ and $f(n) = 0$ whenever $n \equiv 0 \bmod q$ then $\sum \frac{f(n)}{n} \neq 0$.*

From now on, we call such functions Erdősian. Questions of this type were discussed by Chowla in his earlier works ([10] and [11]) for a prime period p. This will be discussed in detail along with Okada's criterion. Okada gave a necessary and sufficient condition for the vanishing of the periodic Dirichlet series at $s = 1$. Since then, the general philosophy is the following: find conditions on the function f such that $L(1, f)$ doesn't vanish, and check whether certain 'classes' of Erdősian functions satisfy the condition. In fact, some of the attempts to solve Conjecture 1.2 revolves around the criterion given by Okada. This is discussed in detail in Sections 4, 5 and 6.

A criterion for non-vanishing of $L(1, f)$ requires looking at the odd parts and even parts of f respectively (these are defined in Section 4.3). While $L(1, f)$ is an algebraic multiple of π when f is odd, for even f, the non-vanishing of $L(1, f)$ is more delicate. This involves Ramchandra units and a classification by H. Bass. This will be discussed in Section 7.

This conjecture has been settled by M. Ram Murty and N. Saradha [21] when the period q is in the equivalence class 3 mod 4. In the end, we extend their arguments to some more general cases. In particular, these methods are applicable to odd functions f. For instance, we give a necessary and sufficient condition for a $\mathbb{Z}$-linear combination of cotangents

$$\sum_{i=1}^{(p-1)/2} a_i \frac{1+\zeta_p^i}{1-\zeta_p^i}$$

with integer coefficients a_i, to be an algebraic integer. Such conditions arise naturally when $L(1, f) = 0$ for odd rational valued periodic arithmetic function f. This will be discussed in Section 8.

2. Periodic Dirichlet series

2.1 *Convergence of $L(1, f)$ and the value at $s = 1$*

Let $f : \mathbb{N} \to \mathbb{C}$ be an arithmetic function of period q. The function $L(s, f)$ converges absolutely and uniformly on compact subsets of the complex plane for $\Re(s) > 1$ and hence is a holomorphic function there. Following [20], we write

$$L(s, f) = q^{-s} \sum_{a=1}^{q} f(a)\zeta\left(s, \frac{a}{q}\right). \tag{1}$$

To evaluate the function at $s = 1$, we shall use the following fact:

$$\lim_{s\to 1^+} \zeta(s, x) - \frac{1}{s-1} = -\frac{\Gamma'(x)}{\Gamma(x)} = -\Psi(x) \tag{2}$$

where $\Gamma(x) := \int_0^\infty e^{-t} t^{x-1} dt$ denotes the gamma function. Using (2), we can write (1) as

$$L(s, f) = q^{-s} \sum_{a=1}^{q} f(a)\left(\zeta\left(s, \frac{a}{q}\right) - \frac{1}{s-1}\right) + \frac{q^{-s}}{s-1} \sum_{a=1}^{q} f(a). \tag{3}$$

Hence evaluating the limit at $s = 1$, we get the following theorem.

Theorem 2.1. *The limit of $L(s, f)$ at $s = 1$ exists if and only if $\sum_{a=1}^{q} f(a) = 0$. When the function f satisfies this condition, we have*

$$L(1, f) = -\frac{1}{q} \sum_{a=1}^{q} f(a) \frac{\Gamma'}{\Gamma}\left(\frac{a}{q}\right). \tag{4}$$

Remark 2.2. The necessary and sufficient condition for the existence of $L(s, f)$ at $s = 1$ can also be obtained by partial summation formula. We proceeded in this manner to obtain an expression of $L(1, f)$ whenever it exists.

For the remainder of the Section, we will assume that f is a $\overline{\mathbb{Q}}$-valued arithmetic function with period q and $\sum_{a=1}^{q} f(a) = 0$.

2.2 *Baker's theory of linear forms in Logarithms*

We start by mentioning the Lindemann Weierstrass theorem which helps us to observe the transcendence of logarithms of algebraic numbers.

Theorem 2.3. *If $a_1, \ldots a_n$ are non-zero algebraic numbers and $\alpha_1, \ldots, \alpha_n$ are distinct algebraic numbers then we have*

$$a_1 e^{\alpha_1} + \ldots a_n e^{\alpha_n} \neq 0.$$

Corollary 2.4. *Let $\alpha \in \overline{\mathbb{Q}}$, and $\alpha \neq 0, 1$. Then $\log(\alpha)$ is transcendental.*

Among the list of twenty three problems posed by Hilbert, the seventh question asks about the transcendence of α^{β} given $\alpha \neq 1$ is non-zero algebraic number and β is an algebraic irrational. This was proved in affirmative by Gelfond and Schneider independently around 1934. In particular, the result states that the ratio of logarithms of two non-zero algebraic numbers is either rational or transcendental. In his ground breaking work, Baker had given a similar analogue. Following [6], we state the qualitative version of Baker's theorem on linear forms in logarithms.

Theorem 2.5. *If $\alpha_1, \ldots, \alpha_m$ are non-zero algebraic numbers such that $\log(\alpha_1), \ldots, \log(\alpha_m)$ are linearly independent over $\mathbb{Q}$, then*

$$1, \log(\alpha_1), \ldots, \log(\alpha_m) \text{ are linearly independent over } \overline{\mathbb{Q}}.$$

Remark 2.6. The above theorem holds for any branch of logarithm.

Using the above theorem, we illustrate a simple observation about linear forms in logarithms of algebraic numbers over $\overline{\mathbb{Q}}$.

Lemma 2.7. *If $\alpha_1, \ldots, \alpha_m$ and $\beta_1, \ldots, \beta_m$ are algebraic with α_i non-zero, then the sum*

$$\beta_1 \log(\alpha_1) + \cdots + \beta_m \log(\alpha_m).$$

is either zero or transcendental.

The proof follows by induction on m. For $m = 1$, the theorem holds true by Corollary 2.4. We assume that the lemma holds for $m < n$ and does not hold for n that is,

$$\beta_1 \log(\alpha_1) + \cdots + \beta_m \log(\alpha_m) = \beta_0,$$

where $\beta_0 \neq 0$ and $\beta_0 \in \overline{\mathbb{Q}}^*$. From Theorem 2.5, we note that $\log(\alpha_1), \ldots, \log(\alpha_m)$ are linear dependent over $\mathbb{Q}$. We obtain a contradiction by reducing the equation to $m < n$ by the cancellation of coefficients.

2.3 *Another expression of $L(1, f)$ and its transcendental nature*

Now as shown in [1], we obtain another expression for $L(1, f)$ using fast Fourier transform.

Definition 2.8. *Let f be an arithmetic function of period q. The fast Fourier transform of f is denoted by*

$$\widehat{f}(n) := \frac{1}{q}\sum_{m=1}^{q} f(m)e^{-2\pi imn/q}.$$

With the above definition, the authors [1] showed that,

$$\sum_{n=1}^{\infty}\frac{f(n)}{n} = -\sum_{m=1}^{q-1}\widehat{f}(m)\log(1-e^{2\pi im/q}). \tag{5}$$

This is a linear form in logarithm of non-zero algebraic numbers with algebraic coefficients, and hence should be zero or transcendental whenever f takes algebraic values. Under the same conditions, we also have the following theorem.

Theorem 2.9. *If* $\sum_{m=1}^{q-1}\widehat{f}(m)\log(1-e^{2\pi im/q}) = 0$*, then*

$$\sum_{m=1}^{q-1}\sigma(\widehat{f}(m))\log(1-e^{2\pi im/q}) = 0 \quad \textit{for all } \sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}).$$

For proving the same, Baker, Birch and Wirsing [1] considered a maximal subset S of $\{\log(1-e^{2\pi im/q})\}_{m=1}^{q-1}$, which is linearly independent over $\mathbb{Q}$. Then, they apply the Baker's theorem on linear forms in logarithms of algebraic numbers to show that all the coefficients of linear combinations of $\{\alpha_i\}_{\alpha_i\in S}$ are zero. The result is obtained on applying the automorphism σ to these coefficients and rearranging the terms.

2.4 *Decomposition using $L(1, \chi)$ for Dirichlet type functions*

Definition 2.10. *An arithmetic function f of period q is said to be of Dirichlet type if $f(a) = 0$ whenever $(a, q) > 1$.*

Moreover, for an arithmetic function f of period q, we say that f is odd if $f(q-n) = -f(n)$, and f is even if $f(q-n) = f(n)$.

We state a decomposition result about the Dirichlet type functions.

Proposition 2.11. *Let f be a Dirichlet type arithmetic function of period q satisfying $\sum_{a=1}^{q} f(a) = 0$. Then $L(1, f) = \sum_{\chi\neq 1} a_\chi L(1, \chi)$ where χ runs over the non-trivial characters modulo q. Moreover if f is odd (resp. even) then f can be written as a linear combination of odd (resp. even) characters of modulus q.*

Proof. If $f(n) = \sum_\chi a_\chi \chi(n)$, then we have

$$L(s, f) = a_1\zeta(s) + \sum_{\chi\neq 1} a_\chi L(s, \chi).$$

Since $\sum_{a=1}^{q} f(a) = 0$, we can evaluate $L(s, f)$ at $s = 1$, but since $\zeta(s)$ has a pole at $s = 1$, we conclude that $a_1 = 0$ as the limit of $L(s, \chi)$ at $s = 1$ exists by Theorem 2.1. From the orthogonality relations we have,

$$\sum_n f(n)\overline{\chi}_j(n) = \sum_n \sum_\chi a_\chi \chi(n)\overline{\chi}_j(n) = \sum_\chi a_\chi \sum_n \chi(n)\overline{\chi}_j(n) = \phi(q)a_{\chi_j}.$$

Hence $L(1, f) = \sum_{\chi \neq 1} a_\chi L(1, \chi)$. To prove the second part, suppose f is odd. Then $f(-n) = -f(n)$. Therefore

$$\begin{aligned} 2f(n) &= f(n) - f(-n) \\ &= \sum_{\chi \text{ even}} a_\chi(\chi(n)) - \sum_{\chi \text{ even}} a_\chi(\chi(-n)) + \sum_{\chi \text{ odd}} a_\chi(\chi(n)) - \sum_{\chi \text{ odd}} a_\chi(\chi(-n)). \end{aligned}$$

Hence $f(n) = \sum_{\chi \text{ odd}} a_\chi \chi(n)$ and this implies $L(1, f) = \sum_{\chi_i \text{ odd}} a_i L(1, \chi_i)$.

A similar proof holds true when f is an even arithmetic function of period q. □

In the proof of the above Proposition, we can also see that if the values of f are in a number field K, then the coefficients a_χ belong to the field $K(\zeta_{\phi(q)})$ where ζ_n denotes the primitive n^{th} root of unity. Using this decomposition, we note that the non-vanishing of $L(1, f)$ for odd Dirichlet type function f depends on the linear relation of the values of Dirichlet L functions $L(1, \chi)$ where χ is an odd Dirichlet character. We end by mentioning the expressions of $L(1, \chi)$ for even and odd characters respectively. Throughout, we set $\zeta_N = e^{2\pi i/N}$.

2.5 *Value of the Dirichlet L function at $s = 1$*

For a Dirichlet character χ mod N, we denote the Gauss sum as

$$\tau(\chi) = \sum_{a=1}^{N} \chi(a)\zeta_N^{-a}.$$

It is a standard result that for a primitive character χ of conductor N, we have $|\tau(\chi)| = \sqrt{N}$. We follow [29] for the explicit expression of $L(1, \chi)$.

Theorem 2.12. *Let χ be a non-principal primitive Dirichlet character of conductor N. We then have:*

$$L(1, \chi) = \begin{cases} \pi i \frac{\tau(\chi)}{N} B_{1,\overline{\chi}} & \text{if } \chi(-1) = -1, \\ -\frac{\tau(\chi)}{N} \sum_{a=1}^{N-1} \overline{\chi}(a) \log|1 - \zeta_N^a| & \text{if } \chi(-1) = 1, \end{cases} \tag{6}$$

where the generalised Bernoulli number $B_{1,\chi}$ is given by the following expression.

$$B_{1,\chi} = \frac{1}{N} \sum_{a=1}^{N} \chi(a)a.$$

Note that the non-vanishing of $L(1, \chi)$ for an odd character χ implies that $B_{1,\chi}$ is non-zero.

3. The question of Chowla and the theorem of Baker, Birch and Wirsing

We now proceed to the solution of Question 1.1 for odd rational valued arithmetic functions f.

3.1 *Chowla's question*

When f is odd of period 2, then $f \equiv 0$ and therefore $L(1, f) = 0$. So the interesting case is when the period of f is an odd prime. The question can be solved when f is odd by using the cotangent function as mentioned in [16]. We record an alternate proof with the following proposition. Before proceeding to the proof, we fix a generator g of $(\mathbb{Z}/p\mathbb{Z})^*$ and enumerate the characters of $(\mathbb{Z}/p\mathbb{Z})^*$ as $\{\chi_k\}_{k=0}^{p-2}$, such that

$$\chi_k(g) = \zeta_{p-1}^k.$$

Proposition 3.1. *Let p be an odd prime. The Gauss sums corresponding to the Dirichlet character modulo p, $\{\tau(\chi_i)\}_{i=0}^{p-2}$ form a basis of $\mathbb{Q}(\zeta_p, \zeta_{p-1})$ over $\mathbb{Q}(\zeta_{p-1})$.*

Proof. Let $\sum_i a_i \tau(\chi_i) = 0$, for $a_i \in \mathbb{Q}(\zeta_{p-1})$. After the substitution of $\tau(\chi_i)$, we obtain

$$\sum_{j=1}^{p-1} \left(\sum_{i=0}^{p-2} a_i \chi_i(j) \right) \zeta_p^{-j} = 0.$$

Since $\{\zeta_p^i\}_{i=1}^{p-1}$ is a basis of $\mathbb{Q}(\zeta_{p(p-1)})/\mathbb{Q}(\zeta_{p-1})$, we have

$$\sum_{i=0}^{p-2} a_i \chi_i(j) = 0, \qquad \text{for all } 1 \le j \le p-1.$$

By the linear independence of characters, we have $a_i = 0$ for all i and hence the Gauss sums are linearly independent over $\mathbb{Q}(\zeta_{p-1})$. □

Proof of Question 1.1 for odd functions f. Since the Gauss sums $\{\tau(\chi_i)\}_{i=0}^{p-2}$ form a basis of $\mathbb{Q}(\zeta_p, \zeta_{p-1})/\mathbb{Q}(\zeta_{p-1})$ and $B_{1,\chi}$ is a non-zero element of $\mathbb{Q}(\zeta_{p-1})$, from (6), we note that the set $\{L(1, \chi)/\pi i\}_{\chi \text{ odd}}$ is linearly independent over $\mathbb{Q}(\zeta_{p-1})$. Hence by Proposition 2.11, we obtain the result. □

The above proposition was also observed by R Ayoub in [5]. However, with this manipulation we avoid the expression of $\cot 2\pi n/p$ in terms of the Gauss sums. Before proceeding to the main theorem of [1], we define the Dedekind determinant and its evaluation. We refer the reader to [20] for the proof of Proposition 3.3 and Theorem 3.4.

3.2 *Dedekind determinant*

Definition 3.2. *Let G be a finite abelian group of order n and $F : G \to \mathbb{C}$ be any complex valued function on G. The determinant of the $n \times n$ matrix $[F(xy^{-1})]_{x,y \in G}$ is called the Dedekind determinant.*

For a square matrix A with entries in a field K, let $|A|$ denote its determinant. With the same notations as above we have,

Proposition 3.3. *Let $F : G \to K$ where K is a field of characteristic 0. Then,*

(a) $|[F(xy^{-1})]_{x,y\in G}| = \prod_{\chi\in\widehat{G}} \left(\sum_{x\in G} \chi(x)F(x)\right)$,
(b) $|[F(xy^{-1}) - F(x)]_{x,y\neq 1}| = \prod_{\substack{\chi\neq 1\\ \chi\in\widehat{G}}} \sum_{\sigma\in G} \chi(\sigma)F(\sigma)$,
(c) If $\sum_{\sigma\in G} F(\sigma) = 0$, *then* ,

$$|[F(xy^{-1})]_{x,y\neq 1}| = |G|^{-1} \prod_{\substack{\chi\in\widehat{G}\\ \chi\neq 1}} \sum_{\sigma\in G} \chi(\sigma)F(\sigma).$$

Here $\widehat{G}$ denotes the character group of G.

3.3 *The proof of Baker Birch and Wirsing*

The theorem below answers to a more generalised version of Question 1.1 as mentioned in [1].

Theorem 3.4. *Let f be a non-zero arithmetic function of period q satisfying $f(n) = 0$ whenever $1 < (n, q) < q$, and that the cyclotomic polynomial $\Phi_q(x)$ is irreducible over $\mathbb{Q}(f(1), \dots, f(q))$. Then $L(1, f) \neq 0$ whenever the sum converges.*

The first condition enables us to write $L(1, f)$ as a linear form of $\Psi(a/q) + \gamma$ for a coprime to q. Here γ denotes the Euler's constant. The idea of the proof to construct arithmetic functions $f_h(n) := f(hn)$ of same period q using automorphisms such that $L(1, f_h) = 0$. This is done using the second condition, we choose automorphisms $\sigma : \zeta_q \to \zeta_q^h$ fixing $\mathbb{Q}(f(1), \dots, f(q))$ and apply Theorem 2.9. So, we get that $f(a)$ satisfies a system of equations of the form $AX = 0$, A is the coefficient matrix $\Psi(ab/q)+\gamma$ where a and b varies over the co-prime residue classes modulo q. Hence it would be enough to show the matrix is invertible for which we invoke the Dedekind determinant. The non-vanishing of the determinant involves the non-vanishing of $L(1, \chi)$. We label the following condition as (A) for the future references.

$$\Phi_q(x) \text{ is irreducible over } \mathbb{Q}(f(1), \dots, f(q)). \qquad (A)$$

4. Vanishing of periodic Dirichlet series at $s = 1$

Now let us consider some examples of vanishing of Dirichlet series $L(s, f)$ at $s = 1$ for algebraic periodic functions f. We first analyze the two given conditions in Theorem 3.4. In the case when the period is a prime, it was observed that $L(1, f) \neq 0$ for all non-zero rational valued functions f.

Example 4.1. Consider the Dirichlet series

$$L(s,g) := \left(1 - \frac{p}{p^s}\right)^2 \zeta(s) \qquad \text{where } \Re(s) > 1.$$

Note that at $s = 1$, $\zeta(s)$ has a simple pole, and $\left(1 - \frac{p}{p^s}\right)$ has a zero. Hence, $L(s,g)$ has a zero at $s = 1$. We also observe that g is of period p^2.

Alternatively, we see that the linear combination of all such Dirichlet series also vanish at $s = 1$. Hence, one can ask the following question.

Question 4.2. *Given an arithmetic function f of period N such that $L(1, f) = 0$, does there exist integers k_i dividing N, and arithmetic functions g_i of period $\frac{N}{k_i}$ such that*

$$L(s,f) = \sum_{k_i|N} \left(1 - \frac{k_i}{k_i^s}\right) L(s, g_i), \tag{7}$$

hold whenever $\Re(s) > 1$?

This was answered by T. Okada in [23]. We begin with the notations.

4.1 *Notations*

Let $F(N)$ denote the set of arithmetic functions of period N with algebraic values. For $f \in F(N)$, we define $R(f) := \sum_{n=1}^{N} f(n)$ and we denote $A(N) := \{f \in F(N) | R(f) = 0\}$. For a positive divisor d of N and $g \in F\left(\frac{N}{d}\right)$, we define $g^{(d)} \in F(N)$ as follows:

$$g^{(d)}(n) = \begin{cases} g(n/d) & \text{if } d \mid n, \\ 0 & \text{otherwise} \end{cases}.$$

Also we define $g^{(d)} \in F(N)$ as follows:

$$g^{[d]}(n) := g(n) - dg^{(d)}(n).$$

We have $L(s, g^{(d)}) = d^{-s} L(s,g)$ and $L(s, g^{[d]}) = (1 - d^{1-s}) L(s,g)$. To obtain the value at $s = 1$ for $L(s, g^{[d]})$, we note the following,

$$\lim_{s \to 1} L(s, g^{[d]}) = \lim_{s \to 1} \frac{1 - d^{1-s}}{s - 1} \big((s-1) L(s,g)\big) = \log(d) R(g).$$

Hence,

$$L(1, g^{[d]}) = R(g) \log d.$$

So if $g \in A(N/d)$, then $L(1, g^{[d]}) = 0$. Question 4.2 asks the converse. We now proceed to the main result.

Theorem 4.3. *Suppose $f \in F(N)$ satisfies condition (A). Then $L(1, f) = 0$ if and only if there exists $g_l \in A(N/l)$ such that*

$$f = \sum_{l|N} g_l^{[l]},$$

where l runs over all the prime divisors of N.

The proof of this theorem hinges on the construction of the Dirichlet type function g and functions g_l for each prime divisor l of N such that $f = g + \sum_{l|N} g_l^{[l]}$. Then using Theorem 2.5, T. Okada [23] shows that $g \equiv 0$. In the process, he also showed that g, g_l and f have the same parity i.e. if f is odd (resp. even) then g, g_l are also odd (resp. even).

4.2 *Odd functions satisfying* $L(1, f) = 0$

On examining the odd Dirichlet characters, the authors in [1] made a remark that we require the condition (A). Indeed, this should be expected, as $L(1, \chi)$ is an algebraic multiple of π whenever χ is odd. Since for $q \geq 5$, we have more than one odd character χ mod q, we can obtain a linear combination of odd Dirichlet characters χ's of a fixed modulus q over $\overline{\mathbb{Q}}$ (say f) such that $L(1, f) = 0$. The following example was mentioned in [1].

Example 4.4. Consider the quadratic characters χ and χ' of conductors 3 and 4 respectively and consider the function $f = 2\chi - \sqrt{3}\chi'$. Since

$$L(1, \chi) = \frac{\pi}{2\sqrt{3}} \text{ and } L(1, \chi') = \frac{\pi}{3},$$

it follows that $L(1, f) = 0$.

In fact, a complete classification of the vanishing of the odd functions was made. They proved the redundancy of condition (A) when f is not odd. More precisely,

Theorem 4.5. *All algebraically valued functions f, periodic with period q, in which $L(1, f) = 0$ and $f(a) = 0$ for all $1 < (a, q) < q$ holds, are odd.*

With the above theorem, they immediately deduce the linear independence of $L(1, \chi)$ over $\overline{\mathbb{Q}}$ as χ varies over non-trivial distinct primitive even characters.

Corollary 4.6. *If $\chi_1, \ldots, \chi_k$ are even characters for which the associated primitive characters are distinct, then $L(1, \chi_1), \ldots, L(1, \chi_k)$ are linearly independent over the field of all algebraic numbers.*

4.3 *The odd and the even parts of* $L(1, f)$

From Theorem 2.9, if we have $L(1, f) = 0$, then $L(1, f_a) = 0$ where $f_a(n) := f(an)$ for all $1 \leq a \leq q$ with $(a, q) = 1$, provided condition (A) holds. In particular, if we denote $f_e(n) := \frac{f(n)+f(-n)}{2}$ (referred as the even part of f), then

$$L(1, f) = 0 \implies L(1, f_e) := \frac{L(1, f) + L(1, f_{q-1})}{2} = 0.$$

Similarly, if we denote $f_o(n) := \frac{f(n)-f(-n)}{2}$ (referred as the odd part of f), we obtain $L(1, f_o) = 0$. It is natural to ask the same when we do not have any restrictions on f. In [9], the authors proved the following:

Theorem 4.7. $L(1, f) = 0$ *if and only if* $L(1, f_e) = 0$ *and* $L(1, f_o) = 0$.

5. A conjecture of Erdős and Okada's Criterion

We begin by making a few preliminary observations on Conjecture 1.2. Let the period q be an even number. For convergence, we need to have $\sum_{a=1}^{q} f(a) = 0$. But this is not possible as $\sum_{a=1}^{q} f(a) \equiv 1 \bmod 2$. Hence the statement is vacuously true when the period q is even.

When the period q is a prime, the question is the special case of the Chowla's problem mentioned in the Section 3, and hence the conjecture is true for this case.

T. Okada [22] had given a necessary and sufficient condition on f satisfying condition (A) and such that $L(1, f) = 0$. We start by mentioning some of the notations used in the theorem.

5.1 *Notations*

Let

$$J = \{a \in \mathbb{Z} : 1 \le a \le q \text{ and } (a, q) = 1\},$$

$$L = \{r \in \mathbb{Z} : 1 \le r \le q \text{ and } 1 < (r, q) < q\},\ L' = L \cup \{q\}.$$

Let P denote the set of primes dividing q. For $r \in L'$ and $p \in P$,

$$\epsilon(r, p) = \begin{cases} \upsilon_p(q) + \frac{1}{p-1} \text{ if } \upsilon_p(r) \ge \upsilon_p(q), \\ \upsilon_p(r) \text{ otherwise .} \end{cases}$$

5.2 *Okada's Theorem*

T. Okada gave an equivalent criteria for $L(1, f) = 0$ using the Baker's theory of linear forms in logarithms. He observed that for $L(1, f) = 0$, $f(1), \ldots, f(q)$ has to satisfy a set of homogeneous linear equations. More precisely,

Theorem 5.1. *If* $\Phi_q(x)$ *is irreducible over* $\mathbb{Q}(f(1), \ldots, f(q))$*, then* $L(1, f) = 0$ *holds if and only if* $(f(1), \ldots, f(q))$ *is a solution of the following system of* $\phi(q) + t(q)$ *homogeneous linear equations with rational coefficients*

$$f(a) + \sum_{r \in L} f(r)A(r, a) + \frac{f(q)}{\phi(q)} = 0 \quad \textit{for } a \in J,$$

$$\sum_{r \in L'} f(r)\epsilon(r, p) = 0 \quad \textit{for } p \in P,$$

where $t(q)$ *denotes the number of primes* p *dividing* q.

The numbers $A(r, a)$ are rational numbers and are rather technical to state here. We refer the reader to [22] for further details. Using the above theorem, we now state a corollary which Okada had used to prove Conjecture 1.2 when the period is a prime power or product of two primes.

Corollary 5.2. *If f satisfies the above conditions, then*

$$|f(a)| \leq \left(\frac{q-1}{\phi(q)} - 1\right)M + \frac{1}{\phi(q)}|f(q)| \text{ where } M := \max_{r \in L} |f(r)|.$$

The corollary is proved by rearrangement of terms and using well known fact about Euler Phi function namely, $\sum_{d|q} \phi(d) = q$.

Corollary 5.3. *If $2\phi(q) + 1 > q$, then Conjecture 1.2 is true for q.*

This is the case when $q = p_1 p_2$, and when $q = p^k$. Hence Conjecture 1.2 is true for prime powers and product of two primes. N. Saradha had improved this condition in [28].

6. Variation of Okada Criterion

N. Saradha and R. Tijdeman [4] modified the first condition in Theorem 5.1. We directly state their result using the same notations as mentioned earlier.

6.1 *Modification of Okada's Criterion*

Proposition 6.1. *Let $M(q) := \{\prod_{i=1}^{k} p_i^{n_i} : n_i \geq 0$ and $p_i \mid q\}$ and suppose $f \in F(q)$ satisfies condition (A). Then $L(1, f) = 0$ if and only if*

$$\sum_{m \in M(q)} \frac{f(am)}{m} = 0 \text{ for every } a \text{ with } 1 \leq a \leq q, (a, q) = 1$$

and for all primes $p \mid q$,

$$\sum_{\substack{r=1 \\ (r,q)>1}}^{q} f(r)\epsilon(r, p) = 0.$$

Corollary 6.2. *Let $f \in F(q)$ be completely multiplicative, or multiplicative with $|f(p^k)| < p - 1$ for all prime divisors p of q and every positive integer k. Further assume that f satisfies condition (A). Then $L(1, f) \neq 0$.*

The authors also applied Okada's criterion to investigate sums of the form

$$\sum_{n=0}^{\infty} \frac{(-1)^n(\alpha n + \beta)}{(qn + s_1)(qn + s_2)} \tag{8}$$

with $\alpha, \beta \in \overline{\mathbb{Q}}, s_1, s_2 \in \mathbb{Z}$.

Theorem 6.3. *Consider the sum above with* $|\alpha| + |\beta| > 0$*. Let* Φ_{2q} *be irreducible over* $\mathbb{Q}(\alpha, \beta)$ *and* s_1, s_2 *be distinct integers such that* $qn + s_1, q_n + s_2$ *do not vanish for* $n \geq 0$*. Assume that* $\alpha \neq 0$ *if* $s_1 \equiv s_2 \bmod q$*. Then the sum is transcendental.*

Remark 6.4. We note that the sum mentioned above can be written as $L(1, f)$ for arithmetic function f of period $2q$. Hence we need to consider the cyclotomic polynomial Φ_{2q}.

Meanwhile, M. Ram Murty and T. Chatterjee [2] also modified the second condition mentioned in Theorem 5.1.

Theorem 6.5.

$$\sum_{b \in M(q)} \frac{(f_b, \chi_0)}{b} \log b = 0 \text{ if and only if}$$

$$\sum_{r \in L'} f(r)\epsilon(r, p) = 0 \qquad \text{for } p \in P,$$

where f_b *is the arithmetic function defined by* $f_b(n) = f(bn)$ *and for two functions* $f, g \in F(q)$*;* (f, g) *denotes the inner product*

$$(f, g) = \frac{1}{\phi(q)} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} f(a)\overline{g(a)}.$$

The authors [3] also used Proposition 6.1 for a density theoretic approach to Conjecture 1.2.

6.2 *Density Theoretic Approach to Conjecture 1.2*

Proposition 6.6. *If Conjecture 1.2 is false for a periodic function* f *of period* q *with* q *odd, then*

$$1 \leq \sum_{\substack{d|q \\ d \geq 3 \\ d \neq q}} \frac{1}{\varphi(d)}.$$

Using the above proposition the cases originally solved by Okada were retrieved.

Corollary 6.7. *If* $q = p^k$ *or* $q = p_1 p_2$*, then Conjecture 1.2 is true for period* q*.*

In addition, if we denote $d(n)$ as the number of divisors of n, we have

Corollary 6.8. *If the smallest prime factor of* q *is at least* $d(q)$*, then Conjecture 1.2 is true for* q*.*

Proof. Let l be the smallest prime factor of q. If Conjecture 1.2 is false, then

$$1 \leq \sum_{\substack{d|q \\ d \geq 3}} \frac{1}{\varphi(d)} \leq \frac{1}{\varphi(l)} \sum_{\substack{d|q \\ d \geq 3 \\ d \neq q}} 1 = \frac{d(q) - 2}{l - 1}.$$

Here, we are assuming that q has at least two prime factors and we get $d(q) - 2$ because the sum runs over the proper divisors of q. Hence, we get a strict inequality. Thus $l < d(q)$. □

It was proved in the same paper that Conjecture 1.2 is true for at least 78%. The functions of period $q \equiv 1 \bmod 4$. The bound was increased to 82% by higher moments. However, a remark was made that we can find a small density of numbers q which does indeed satisfy the condition mentioned in Proposition 6.6, and hence the above methods is not sufficient to prove the conjecture. In a recent work, S. Pathak [25] has shown that Conjecture 1.2 holds with "probability" 1.

7. A Question of Milnor

Throughout the Section, for an integer $1 < s \leq n/2$ with $(s, n) = 1$ we denote u_s as

$$u_s := \frac{\zeta_n^s - 1}{\zeta_n - 1}.$$

Milnor, in a private communication to K. G. Ramanathan, had raised the following question about the multiplicative units of the cyclotomic Field $\mathbb{Q}(\zeta_n)$:

Question 7.1. *Does the units u_s along with ζ_n form a basis of a subgroup of the unit group of $\mathbb{Q}(\zeta_n)$?*

K. Ramachandra [27], along with giving a counter-example for the above question, also gave a natural set of multiplicatively independent units. Following [17], let $n = \prod_{i \in I} p_i^{a_i}$ and for each proper subset $J \subseteq I$, we define

$$n_J := \prod_{i \in J} p_i^{a_i}, \qquad \zeta_J = \zeta_n^{n_J}.$$

Theorem 7.2. *The units*

$$v_s = \prod_{\substack{J \subseteq I \\ J \neq I}} \frac{1 - \zeta_J^s}{1 - \zeta_n} \qquad 1 < s \leq n/2 \textit{ with } (s, n) = 1$$

are multiplicatively independent and the group generated by these units form a subgroup of finite index over the full group of units of the ring of integers of $\mathbb{Q}(\zeta_n)$.

Dedekind determinant was used to prove that the units are multiplicatively independent. Using these units, the following theorem was proved in [18].

Theorem 7.3. *For a fixed $q > 1$, the elements $L(1, \chi)$ where χ runs over all the non-trivial even characters modulo q are linearly independent over $\overline{\mathbb{Q}}$.*

Milnor also conjectured that

Conjecture 7.4. *All the multiplicative relations of the numbers $\{1 - \zeta_n^j\}_{j=1}^{n-1}$ are consequences of the following two relations:*

$$1 - \zeta_k^{-1} = -\zeta_k^{-1}(1 - \zeta_k), \tag{9}$$

$$1 - \zeta_n^k = \prod_{\eta^k = 1} (1 - \zeta\eta). \tag{10}$$

The above conjecture was made precise by H. Bass [7], and soon Ennola [13] gave a counter-example of the same. However, he had shown that the above conjecture is true “upto a factor of 2”. Coming back to the case on the non-vanishing of $L(1, f)$ when f is an even function, $L(1, f)$ is a linear combination of logarithms of algebraic numbers $|1-\zeta_q^i|$. A more recent paper of Chatterjee, et al. [9] gives another classification of the same for even functions f such that $L(1, f) = 0$ using the above result.

8. Conjecture 1.2 for the case $q \equiv 3 \bmod 4$

Before proceeding to the proof, we note if α_i are multiplicatively independent positive real numbers, then by Theorem 2.5, the numbers π and $\log \alpha_i$ are linearly independent over $\mathbb{Q}$. When we express $L(1, f)$ as linear combination of logarithms, it is possible to find the coefficient of π using the fast Fourier transform.

Theorem 8.1. *Let $f : \mathbb{Z}/q\mathbb{Z} \to \overline{\mathbb{Q}}$ be an algebraic valued function which is not identically zero, and ζ_q a primitive q-th root of unity. Further suppose that $\sum_{a=1}^{q} f(a) = 0$. If*

$$\frac{f(q)}{2q} + \frac{1}{q}\sum_{b=1}^{q-1} \frac{f(b)}{1-\zeta_q^b} \neq 0, \tag{11}$$

then $L(1, f)$ is transcendental.

If f is an arithmetic function of period q taking algebraic values, and also satisfies $\sum_{a=1}^{q} f(a) = 0$, then

$$L(1, f) = S_f \pi i + \sum_i a_i \log \alpha_i,$$

where α_i are positive real numbers, and S_f denotes the expression mentioned in (11).

We record the proof of Conjecture 1.2 for the case of 3 mod 4 as mentioned in [21]. The crux of the proof is to observe that the coefficient of π doesn’t vanish for Erdősian functions by using the congruence conditions. However, one should also note that the non-vanishing of π is not a necessary condition for non-vanishing of $L(1, f)$. A simple example to see this is to construct an even function f. Assume $q = 5$ $f(5) = 0$, $f(1) = f(4) = 1$, $f(2) = f(3) = -1$. The sum mentioned in (11) is 0, but by Theorem 3.4, we know that $L(1, f) \neq 0$.

Theorem 8.2. *Conjecture 1.2 is true when $q \equiv 3 \bmod 4$.*

Proof. Let us denote the sum in (11) as S. We show that $S \neq 0$. Consider the sum qS and $K = \mathbb{Q}(\zeta_q)$. As qS is an element of the ring of integers O_K of K, we note that

$$qS \equiv q\sum_{b=1}^{q-1} \frac{1}{1-\zeta_q^b} \bmod 2O_K.$$

So it suffices to show that

$$q\sum_{b=1}^{q-1} \frac{1}{1-\zeta_q^b} \neq 0 \bmod 2O_K.$$

By logarithmic differentiation of the expression

$$\sum_{i=0}^{q-1} x^i = \prod_{b=1}^{q-1} (x - \zeta_q^b).$$

and substituting $x = 1$, we obtain

$$\sum_{b=1}^{q-1} \frac{1}{1 - \zeta_q^b} = \frac{q-1}{2}.$$

If $q \equiv 3 \bmod 4$, then the above sum is 1 mod $2O_K$ and hence the theorem is proved. □

Remark 8.3. We can replace the above cyclotomic computation by a 'parity' argument in the following way: for every pair of elements $\frac{q}{1-\zeta_q^k}$ and $\frac{q}{1-\zeta_q^{-k}}$, we replace it

$$\frac{a_k}{1-\zeta_q^k} + \frac{a_{-k}}{1-\zeta_q^{-k}} \equiv q\frac{1+\zeta_q^k}{1-\zeta_q^k} \bmod 2O_K \equiv 1 \bmod 2O_K. \tag{12}$$

In the above $a_k, a_{-k} \in \{\pm q\}$. Since there are only $\frac{q-1}{2}$ elements $\frac{1+\zeta_q^k}{1-\zeta_q^k}$, we obtain $S \equiv 1 \bmod 2O_K$.

We end the section by proving some new results by appealing to elementary results from cyclotomic fields.

8.1 *Some Supplementary results*

We note that $1/(1-\zeta_p)$ is not an algebraic integer and $p/(1-\zeta_p) \in \overline{\mathbb{Z}}$, the ring of algebraic integers. We also recall that if n has at least two odd distinct prime factors, then for $(a, n) = 1$, $(1+\zeta_n^a)/(1-\zeta_n^a) \in \overline{\mathbb{Z}}$.

Proposition 8.4. *Let n be an odd squarefree number greater than 1 and $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}$ be an odd function. For every divisor d of n, $d \neq n$, we set*

$$\alpha_d := \sum_{\substack{i=1 \\ (i,\frac{n}{d})=1}}^{[n/2d]} f(di)\frac{1+\zeta_n^{di}}{1-\zeta_n^{di}}.$$

If $\alpha_{n/p} \notin \overline{\mathbb{Z}}$ for some prime p dividing n, then $L(1, f) \neq 0$.

Proof. Since $\alpha_{n/p} \notin \overline{\mathbb{Z}}$ for some prime p dividing n, we note that $n/p(\alpha_{n/p}) \notin \overline{\mathbb{Z}}$ as $(n/p, p) = 1$. Therefore,

$$\frac{n}{p}L(1, f) = \frac{n}{p}\frac{\pi i}{n}\sum_{a=1}^{[n/2]} f(a)\frac{1+\zeta_n^a}{1-\zeta_n^a} = \frac{\pi i}{n}\Big(\frac{n}{p}\Big(\sum_{\substack{k|n \\ k\neq p}} \alpha_{n/k}\Big) + \frac{n}{p}\alpha_{n/p}\Big).$$

Note that $n/p(\alpha_{n/p}) \notin \bar{\mathbb{Z}}$ and $n/p(\alpha_{n/k}) \in \bar{\mathbb{Z}}$ for all $k|n, k \neq p$. Therefore, $L(1, f) \neq 0$. □

Remark 8.5. The above proposition can be extended to all natural numbers n by replacing the condition $\alpha_{n/p} \notin \overline{\mathbb{Z}}$ with the following condition: there exists a prime $p \mid n$ such that $\sum_{k=1}^{v_p(n)} \alpha_{n/p^k} \notin \overline{\mathbb{Z}}$. Here $v_p(n)$ denotes the highest power of p dividing n.

The above proposition can be applied to construct odd Erdősian functions f such that $L(1, f) \neq 0$. The following notion would be convenient for our future purpose.

Definition 8.6. *An algebraic number $\alpha \in \mathbb{Q}(\zeta_n)$ is said to be Erdősian if α can be expressed as*

$$\sum_{i=1}^{[n/2]} a_i \frac{1+\zeta_n^i}{1-\zeta_n^i},$$

where $a_i \in \{\pm 1\}$. We say that α is Erdősian number of level n, if n is the smallest integer for which the above expression holds. If such a number is also an algebraic integer, then we call it an Erdősian integer of level n.

In fact, given a prime number p, there exists Erdősian numbers in $\mathbb{Q}(\zeta_p)$ which are not algebraic integers. Indeed, given an Erdősian integer $\alpha = \sum_{i=1}^{\frac{p-1}{2}} a_i(1+\zeta_p^i)/(1-\zeta_p^i)$ of level p, there exists at least $(p-1)/2$ combinations $\alpha - 2sgn(a_i)(1+\zeta_p^i)/(1-\zeta_p^i)$ which are not algebraic integers. Here $sgn(x)$ denotes the sign function. For the sake of brevity, we didn't include the higher powers in the above calculation. But however, it is not immediately clear that Erdősian integers of level p exist. We invoke a lemma which helps us in constructing such numbers.

Lemma 8.7. *Let p be a prime. We can express $\frac{1+\zeta_p}{1-\zeta_p}$ as the following:*

$$\frac{1+\zeta_p}{1-\zeta_p} = -1 - \frac{2}{p}\sum_{i=1}^{p-1} i\zeta_p^i. \tag{13}$$

Proof. Since $\{\zeta_p^i\}_{i=1}^{p-1}$ form a normal basis of $\mathbb{Q}(\zeta_p)$ over $\mathbb{Q}$, we write

$$\frac{1}{1-\zeta_p} = \sum_{i=1}^{p-1} a_i\zeta_p^i. \tag{14}$$

Moreover, we obtain

$$\frac{\zeta_p}{1-\zeta_p} = \frac{1}{1-\zeta_p} - 1 = \sum_{i=1}^{p-1}(a_i+1)\zeta_p^i.$$

Therefore, we have another expression for (14) namely

$$\frac{1}{1-\zeta_p} = \sum_{i=1}^{p-2}(a_{i+1}-1)\zeta_p^i + (a_1+1) = \sum_{i=1}^{p-2}(a_{i+1}-a_1)\zeta_p^i - (a_1+1)\zeta_p^{p-1}. \tag{15}$$

Comparing the coefficients of (14) and (15), we have

$$a_i = a_{i+1} - a_1 \qquad \text{for all } 1 \le i \le p-2 \quad \text{and} \qquad a_{p-1} = -a_1 - 1. \tag{16}$$

From the above, we obtain $a_i = i a_1$ for all $1 \le i \le p-1$ and substituting in (16), we obtain $a_1 = \frac{-1}{p}$ and therefore $a_i = \frac{-i}{p}$. Hence, we have

$$\frac{1}{1-\zeta_p} = \frac{-1}{p}\sum_{i=1}^{p-1} i\zeta_p^i.$$

We get the lemma by noting that $\frac{1+\zeta_p}{1-\zeta_p} + 1 = 2\frac{1}{1-\zeta_p}$. □

Moreover, applying the automorphism $\zeta_p \to \zeta_p^j$, on (13) we obtain,

$$\frac{1+\zeta_p^j}{1-\zeta_p^j} = -1 - \frac{2}{p}\sum_{i=1}^{p-1}(ij^{-1}|p)\zeta_p^i, \tag{17}$$

where $(x|p)$ denotes the representative of x mod p in the set $\{1, 2, \ldots, p\}$. Hence we have the following result:

Proposition 8.8. *Let $a_i \in \mathbb{Z}$. Then $\sum_{i=1}^{p-1/2} a_i \frac{1+\zeta_p^i}{1-\zeta_p^i}$ is an algebraic integer if and only if $\sum_i a_i(i^{-1}|p) \equiv 0 \bmod p$.*

We end by using the above proposition to prove that there exists algebraic integers of the above form for $p > 5$, p not a Fermat prime. For $p = 3, 5$, there does not exist any Erdősian integer of level p. Hence by Proposition 8.4, Conjecture 1.2 is true for odd arithmetic functions f of squarefree period n having 3 or 5 as a prime divisor.

Lemma 8.9. *Let p be a prime number which is not a Fermat prime. There exists an Erdősian integer of level p.*

Proof. Let $G := (\mathbb{Z}/p\mathbb{Z})^*$. Let H be a non-trivial subgroup of G such that $|H|$ is odd. Now consider $S := \sum_{[i]\in H} \frac{1+\zeta_p^i}{1-\zeta_p^i}$, where naturally for $[i] \in H$, ζ_p^i means ζ_p^k for any representative k of $[i]$. Note that for $j \neq 1$ and $j \in H$, we have

$$\sum_{i\in H} i = \sum_{i\in H} ji = j\sum_{i\in H} i \implies \sum_{i\in H} i = 0 \bmod p.$$

Hence by the above proposition, S is an algebraic integer. We associate G with $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ and H is identified as a subgroup of G accordingly. Now note that for $a_i \in \mathbb{Z}$, the sum $\alpha := \sum_{[\sigma_i]\in G/\{\pm 1\}H} a_i\sigma_i(S)$ is an algebraic integer. For $a_i \in \{\pm 1\}$, the element α is an Erdősian integer of level p. □

9. Concluding remarks

(1) The non-vanishing of periodic Dirichlet series has been reduced to the linear relations between the linear forms in logarithms of non-zero algebraic numbers.

In order to prove Conjecture 1.2; Livingston had conjectured a linear independence of $\{\log 2 \sin \frac{\pi a}{q}\}_{a=1}^{q-1}$ over $\overline{\mathbb{Q}}$ which was disproved by S. Pathak [24].

(2) Modifications of Conjecture 1.2 can be asked in general. For instance, Conjecture 1.2 is not true if the last condition (that is $f(n) = 0$ for $q \mid n$) is removed. Such a function f has been constructed by R. Tengeley for $q = 36$ and a proof using Digamma function has been presented by Pilerud et al. [26].

(3) For $p = 17$, using SAGE, it was observed that there exists only 16 Erdősian integers of level p, that is only one Erdősian integer up-to conjugate. We give its explicit value below:

$$\alpha = \sum_{i=1}^{8} a_i \frac{1+\zeta_{17}^i}{1-\zeta_{17}^i} \text{ where } (a_1, \ldots, a_8) = (1, -1, -1, 1, 1, -1, -1, -1).$$

The constructions in Lemma 8.9 was purely group theoretic and we expect a similar construction to work for Fermat primes. However, the question about counting Erdősian integers of level p upto conjugates seems to be hard at the moment. It is however interesting to point out that for $p = 13$, we do not have any Erdősian integer of level p which are of degree 12 over $\mathbb{Q}$ and all the Erdősian integers of level p are of degree 4 over $\mathbb{Q}$.

(4) The variant of Conjecture 1.2 when applied to integers $k > 1$ is true. Indeed, for an Erdősian function f, we note that if we have

$$L(k, f) = \sum_{n=1}^{\infty} \frac{f(n)}{n^k} = 0 \implies 1 + |f(1)| \leq \zeta(k).$$

Then $k < 2$. Hence, this makes the question more interesting for the case $k = 1$.

(5) T. Okada had proved the equivalence of vanishing of $L(1, f)$ with the p-adic L function $L_p(1, f)$ for even periodic arithmetic functions f. The theme of non-vanishing of Dirichlet series at $s = 1$ can be applied to other settings as mentioned in [14] and [19].

Acknowledgement

The author would like to thank Purusottam Rath for suggesting the topic and Himalaya Senapati, Jyothsnaa Sivaraman, Biplab Paul and the referee for going through the paper, pointing out some oversights and giving suggestions that improved the presentation of the paper. The author also thanks the INFOSYS for the generous funding.

References

[1] A. Baker, B. J. Birch, and E. A. Wirsing, On a problem of Chowla, *J. Number Theory*, **5** (1973) 224–236.

[2] T. Chatterjee and M. R. Murty, Non-vanishing of Dirichlet series with periodic coefficients, *J. Number Theory*, **145** (2014) 1–21.

[3] T. Chatterjee and M. R. Murty, On a conjecture of Erdos and certain Dirichlet series, *Pacific J. Math.*, **275(1)** (2015) 103–113.

[4] N. Saradha and R. Tijdeman, On the transcendence of infinite sums of values of rational functions, *J. London Math. Soc. (2)*, **67(3)** (2003) 580–592.

[5] R. Ayoub, On a theorem of S. Chowla, *J. Number Theory*, **7** (1975) 105–107.

[6] A. Baker, Linear forms in the logarithms of algebraic numbers, I, II, III, *Mathematika*, **13** (1966) 204–216; ibid. **14** (1967), 102–107; ibid., **14** (1967) 220–228.

[7] H. Bass, Generators and relations for cyclotomic units, *Nagoya Math. J.*, **27** (1966) 401–407.

[8] J. W. S. Cassels, Footnote to a note of Davenport and Heilbronn, *J. London Math. Soc.*, **36** (1961) 177–184.

[9] T. Chatterjee, M. R. Murty and S. Pathak, A vanishing criterion for Dirichlet series with periodic coefficients. In Number theory related to modular curves—Momose memorial volume, *Contemp. Math., Amer. Math. Soc.*, Providence, RI, **701** (2018) 69–80.

[10] S. Chowla, The Riemann zeta and allied functions, *Bull. Amer. Math. Soc.*, **58** (1952) 287–305.

[11] S. Chowla, The nonexistence of nontrivial linear relations between the roots of a certain irreducible equation, *Journal of Number Theory*, **2(1)** (1970) 120–123.

[12] H. Davenport and H. Heilbronn, On the Zeros of Certain Dirichlet Series, *J. London Math. Soc.*, **11(3)** (1936) 181–185.

[13] V. Ennola, On relations between cyclotomic units, *J. Number Theory*, **4** (1972) 236–247.

[14] S. Gun, M. R. Murty and P. Rath, Linear independence of Hurwitz zeta values and a theorem of Baker-Birch-Wirsing over number fields, *Acta Arith.*, **155(3)** (2012) 297–309.

[15] A. E. Livingston, The series $\sum_1^\infty f(n)/n$ for periodic f, *Canad. Math. Bull.*, **8** (1965) 413–432.

[16] M. R. Murty, Some remarks on a problem of Chowla, *Ann. Sci. Math. Québec*, **35(2)** (2011) 229–237.

[17] M. R. Murty, The work of K. Ramachandra in algebraic number theory, *Hardy-Ramanujan J.*, **34/35** (2013) 11–19.

[18] M. R. Murty and V. K. Murty, A problem of Chowla revisited, *J. Number Theory*, **131(9)** (2011) 1723–1733.

[19] M. R. Murty and V. K. Murty, Transcendental values of class group L-functions, *Math. Ann.*, **351(4)** (2011) 835–855.

[20] M. R. Murty and P. Rath, Transcendental numbers, Springer, New York, (2014).

[21] M. R. Murty and N. Saradha, Euler-Lehmer constants and a conjecture of Erdős, *J. Number Theory*, **130(12)** (2010) 2671–2682.

[22] T. Okada, On a certain infinite series for a periodic arithmetical function, *Acta Arith.*, **40(2)** (1981/82) 143–153.

[23] T. Okada, Dirichlet series with periodic algebraic coefficients, *J. London Math. Soc. (2)*, **33(1)** (1986) 13–21.

[24] S. Pathak, On a conjecture of Livingston, *Canad. Math. Bull.*, **60(1)** (2017) 184–195.

[25] S. Pathak, Distribution and non-vanishing of special values of L-series attached to Erdős functions, *Int. J. Number Theory.*, **15(7)** (2019) 1449–1462.

[26] T. K. Pilerud and Kh. K. Pilerud, On a conjecture of Erdős, *Mat. Zametki*, **83(2)** (2008) 312–315.

[27] K. Ramachandra, On the units of cyclotomic fields, *Acta Arith.*, **12** (1966/1967) 165–173.

[28] N. Saradha, Chowla's problem on the non-vanishing of certain infinite series and related questions, In Number theory & discrete geometry, Ramanujan Math. Soc. Lect. Notes Ser., *Ramanujan Math. Soc.*, Mysore, **6** (2008) 171–179.

[29] L. C. Washington, Introduction to cyclotomic fields, Graduate Texts in Mathematics, Springer-Verlag, New York, second edition, **83** (1997).

Topics in Number Theory, RMS-Lecture Notes Series No. 26, 2020, pp. 21–42.

On the Selberg Class of L-Functions

Anup B. Dixit

Department of Mathematics and Statistics, Queen's University, Jeffery Hall, 48 University Ave, Kingston, Canada, ON, K7L 3N6.
e-mail: anup.dixit@queensu.ca

Abstract. The Selberg class of L-functions, $\mathbb{S}$, introduced by A. Selberg in 1989, has been extensively studied in the past few decades. In this article, we give an overview of the structure of this class followed by a survey on Selberg's conjectures and the value distribution theory of elements in $\mathbb{S}$. We also discuss a larger class of L-functions containing $\mathbb{S}$, namely the Lindelöf class, introduced by V. K. Murty. The Lindelöf class forms a ring and its value distribution theory surprisingly resembles that of the Selberg class.

Keywords. Dirichlet series, Selberg class.

2010 Subject Classification: 11M41

1. Introduction

The most basic example of an L-function is the Riemann zeta-function, which was introduced by B. Riemann in 1859 as a function of one complex variable. It is defined on $\Re(s) > 1$ as

$$\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

It can be meromorphically continued to the whole complex plane $\mathbb{C}$ with a pole at $s = 1$ with residue 1. The unique factorization of natural numbers into primes leads to another representation of $\zeta(s)$ on $\Re(s) > 1$, namely the Euler product

$$\zeta(s) = \prod_{p \text{ prime}} \left(1 - \frac{1}{p^s}\right)^{-1}.$$

The study of zeta-function is vital to understanding the distribution of prime numbers. For instance, the prime number theorem is a consequence of $\zeta(s)$ having a simple pole at $s = 1$ and being non-zero on the vertical line $\Re(s) = 1$.

In pursuing the analogous study of distribution of primes in an arithmetic progression, we consider the Dirichlet L-function,

$$L(s, \chi) := \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s},$$

for $\Re(s) > 1$, where χ is a Dirichlet character modulo q, defined as a group homomorphism $\chi : (\mathbb{Z}/q\mathbb{Z})^* \to \mathbb{C}^*$ extended to $\chi : \mathbb{Z} \to \mathbb{C}$ by periodicity and setting $\chi(n) = 0$ if $(n, q) > 1$.

Attached to a number field $K/\mathbb{Q}$, we have the Dedekind zeta-function defined for $\Re(s) > 1$ as

$$\zeta_K(s) := \sum_{\mathfrak{a} \subseteq \mathcal{O}_K} \frac{1}{(N_{K/\mathbb{Q}}(\mathfrak{a}))^s},$$

where $\mathcal{O}_K$ denotes the ring of integers of K and $\mathfrak{a}$ runs over all non-zero ideals of $\mathcal{O}_K$.

All the above L-functions capture valuable information about the underlying structure of the associated arithmetic objects. The general philosophy is to expect a relation between "motivic" L-functions and automorphic L-functions. Such relations are called reciprocity laws. One of the most significant reciprocity laws of today is the modularity theorem (formerly known as the Taniyama-Shimura conjecture), which associates to every elliptic curve over $\mathbb{Q}$, a modular form through an L-function. This must be viewed as a tip of the iceberg of the more challenging Langland's reciprocity conjecture. In an attempt to understand this theory, Selberg defined a class of L-functions, $\mathbb{S}$, which is expected to satisfy all familiar properties of an automorphic L-function. His motivation was to study the value distribution of linear combinations of L-functions in this class.

Since then, there has been significant progress in the study of the Selberg class. An overview of the recent results and conjectures regarding the structure of $\mathbb{S}$ can be found in several expositions, such as excellent surveys by A. Perelli [34], [33] and J. Kaczorowski [15]. In this article, we outline some results and highlight certain open problems and unexplored avenues for future study. The emphasis is on Selberg's conjectures and the value distribution theory of the Selberg class. The last section is devoted to the Lindelöf class of L-functions $\mathbb{M}$, defined by V. K. Murty [27]. This class $\mathbb{M}$ is closed under addition and enjoys a richer algebraic structure than $\mathbb{S}$. Moreover, the value distribution theory of $\mathbb{M}$ closely resembles that of $\mathbb{S}$.

2. The Selberg class

Definition 2.1. *The Selberg class $\mathbb{S}$ consists of meromorphic functions $F(s)$ satisfying the following properties.*

(1) **Dirichlet series** – *It can be expressed as a Dirichlet series*

$$F(s) = \sum_{n=1}^{\infty} \frac{a_F(n)}{n^s},$$

which is absolutely convergent in the region $\Re(s) > 1$. We also normalize the leading coefficient as $a_F(1) = 1$.

(2) **Analytic continuation** – *There exists a non-negative integer k, such that $(s-1)^k F(s)$ is an entire function of finite order.*

(3) **Functional equation** – *There exist real numbers* $Q > 0$, $\alpha_i \geq 0$, *complex numbers* β_i *for* $0 \leq i \leq k$ *and* $w \in \mathbb{C}$, *with* $\Re(\beta_i) \geq 0$ *and* $|w| = 1$, *such that*

$$\Phi(s) := Q^s \prod_i \Gamma(\alpha_i s + \beta_i) F(s) \tag{1}$$

satisfies the functional equation

$$\Phi(s) = w\overline{\Phi}(1 - \overline{s}).$$

(4) **Euler product** – *There is an Euler product of the form*

$$F(s) = \prod_{p \text{ prime}} F_p(s), \tag{2}$$

where

$$\log F_p(s) = \sum_{k=1}^{\infty} \frac{b_{p^k}}{p^{ks}}$$

with $b_{p^k} = O(p^{k\theta})$ *for some* $\theta < 1/2$.

(5) **Ramanujan hypothesis** – *For any* $\epsilon > 0$,

$$|a_F(n)| = O_\epsilon(n^\epsilon). \tag{3}$$

The Euler product implies that the coefficients $a_F(n)$ are multiplicative, i.e., $a_F(mn) = a_F(m)a_F(n)$ when $(m, n) = 1$. Moreover, each Euler factor also has a Dirichlet series representation

$$F_p(s) = \sum_{k=0}^{\infty} \frac{a_F(p^k)}{p^{ks}},$$

which is absolutely convergent on $\Re(s) > 0$ and non-vanishing on $\Re(s) > \theta$, where θ is as in (2).

We mention a few examples of elements in $\mathbb{S}$.

(i) The Riemann zeta-function $\zeta(s) \in \mathbb{S}$.

(ii) Dirichlet L-functions $L(s, \chi)$ and their vertical shifts $L(s+i\theta, \chi)$ are in $\mathbb{S}$, where χ is a primitive Dirichlet character and $\theta \in \mathbb{R}$. Note that $\zeta(s+i\theta) \notin \mathbb{S}$ for $\theta \neq 0$, since it has a pole at $s = 1 - i\theta$.

(iii) For a number field $K/\mathbb{Q}$, the Dedekind zeta functions $\zeta_K(s)$ is an element in $\mathbb{S}$.

(iv) Let L/K be a Galois extension of number fields, with Galois group G. Let $\rho : G \to GL_n(\mathbb{C})$ be a representation of G. The associated Artin L-function is defined as

$$L(s, \rho, L/K) := \prod_{\mathfrak{p} \in K} \det\left(I - (N\mathfrak{p})^{-s} \rho(\sigma_{\mathfrak{q}})\Big|_{V^{I_{\mathfrak{q}}}}\right)^{-1}$$

where $\mathfrak{q}$ is a prime ideal in L lying over prime ideal $\mathfrak{p}$ in K, $\sigma_{\mathfrak{q}}$ is the Frobenius automorphism associated to $\mathfrak{q}$ and $V^{I_{\mathfrak{q}}}$ is the complex vector space fixed by the inertia subgroup $I_{\mathfrak{q}}$.

A conjecture of Artin states that for non-trivial irreducible representation ρ of $Gal(L/K)$, the associated Artin L-function $L(s, \rho, L/K)$ is entire. If the Artin conjecture is true, then these functions lie in the Selberg class.

(v) Let f be a holomorphic newform of weight k to some congruence subgroup $\Gamma_0(N)$. Suppose its Fourier expansion is given by

$$f(z) = \sum_{n=1}^{\infty} c(n) \exp(2\pi i n z).$$

Then its normalized Dirichlet coefficients are given by

$$a(n) := c(n) n^{(1-k)/2},$$

and the associated L-function given by $L(s, f) := \sum_{n=1}^{\infty} a(n)/n^s$ for $\Re(s) > 1$ is an element in the Selberg class. It is also believed that the normalized L-function associated to a non-holomorphic newform is an element in the Selberg class, but the Ramanujan hypothesis is yet to be proven in this case.

(vi) The Rankin-Selberg L-function of any normalized eigenform is in the Selberg class.

3. Invariants in $\mathbb{S}$

The constants in the functional equation (1) depend on F, and although the functional equation may not be unique, we have some well-defined invariants, such as the degree d_F of F, which is defined as the finite sum

$$d_F := 2 \sum_{i=1}^{k} \alpha_i.$$

The factor Q in the functional equation gives rise to another invariant referred to as the conductor q_F, which is defined as

$$q_F := (2\pi)^{d_F} Q^2 \prod_{i=1}^{k} {\alpha_i}^{2\alpha_i}. \tag{4}$$

A natural question in this context is to understand how unique the functional equation is for $F \in \mathbb{S}$. Given a gamma-factor for F in $\mathbb{S}$, one can produce new gamma-factors using the Gauss-Legendre multiplication formula for the Γ-function,

$$\Gamma(s) = m^{s-1/2} (2\pi)^{(1-m)/2} \prod_{k=0}^{m-1} \Gamma\left(\frac{s+k}{m}\right), \tag{5}$$

for any integer $m > 2$. One could also use the functional equation

$$\Gamma(z+1) = z\Gamma(z) \tag{6}$$

to produce new gamma-factors for F. It turns out that the functional equation of $F \in \mathbb{S}$ is unique up to the transformations (5) and (6) (see [17]).

It is an interesting conjecture that both the degree and the conductor for elements in the Selberg class are non-negative integers (see [9], [17]).

Conjecture 1. If $F \in \mathbb{S}$, then d_F and q_F are non-negative integers.

There is recent progress towards the degree conjecture. In 1993, it was shown by J. B. Conrey and A. Ghosh [9] that

Theorem 3.1 (Conrey-Ghosh). *If $F(s) \in \mathbb{S}$, then $F = 1$ or $d_F \geq 1$.*

This was proved using the fact that any non-trivial element in the Selberg class must satisfy a certain growth on $\sigma + it$ for $\sigma < 0$ and t sufficiently large. This growth consequently is captured by the degree, which can be seen using the functional equation.

Conrey and Ghosh [9] also conjectured that the functions of degree one in the Selberg class are precisely given by the Riemann zeta-function $\zeta(s)$, Dirichlet L-functions $L(s,\chi)$ and their shifts $L(s+i\theta,\chi)$, where χ is non-principal primitive and $\theta \in \mathbb{R}$. This conjecture was later proved by Kaczorowski and Perelli [16]. No such classification is known for the higher degrees in the Selberg class.

However, there are known examples of elements in the Selberg class with higher degrees. Dedekind zeta-function attached to a number field $K/\mathbb{Q}$ has degree equal to the degree of the field extension $[K : \mathbb{Q}]$. L-functions associated to holomorphic newforms (see Example v) have degree 2. Moreover, L-functions associated to non-holomorphic newforms, if in the Selberg class, would also have degree 2. The Rankin-Selberg L-function of normalized eigenforms are elements of the Selberg class of degree 4.

For elements $F \in \mathbb{S}$ with $d_F > 1$, it is significantly more difficult to show that d_F is an integer. In this direction, Kaczorowski and Perelli [20] established the following.

Theorem 3.2 (Kaczorowski-Perelli). *For $F \in \mathbb{S}$, if $1 \leq d_F < 2$ then $d_F = 1$.*

The key ingredient in this result is the study of non-linear twists of L-functions. The standard non-linear twist of a Dirichlet series $F(s) = \sum_{n\geq 1} a_n/n^s$ is defined as

$$F_d(s,\alpha) = \sum_{n=1}^{\infty} \frac{a_n}{n^s} e(-n^{1/d}\alpha),$$

where $e(x) = e^{2\pi i x}$ and $\alpha > 0$ is a real number. Kaczorowski and Perelli studied the generalization of such non-linear twists, replacing α with a real vector-valued function $f(\vec{\alpha})$. They showed that these non-linear twists can be written as a linear combination of some familiar holomorphic functions to establish their result.

In general, we are far from showing any partial result on the elements of $\mathbb{S}$ with degree > 2. We also do not know the complete classification of elements of $\mathbb{S}$ with degree 2.

4. Growth and number of zeros

For $F \in \mathbb{S}$, the Euler product ensures that $F(s)$ has no zeros on the right half plane $\Re(s) > 1$. Using the functional equation, one gets a sequence of zeroes in the left half plane $\Re(s) < 0$ corresponding to the poles arising from the Γ-factors. The more interesting case is to understand the zero-distribution in the strip $0 < \Re(s) < 1$. This region is called the critical strip of an L-function in $\mathbb{S}$. From the discussion above, it is clear that for $F \in \mathbb{S}$, the zeros of $F(s)$ are concentrated in the critical strip. Due to the symmetric nature of the functional equation, Riemann conjectured that all the zeros of the ζ-function must lie on the $1/2$-line. This is known as the famous Riemann hypothesis and is considered to be one of the most challenging open questions in number theory. The same statement is also expected to hold for elements in $\mathbb{S}$. This is often referred to as the generalized Riemann hypothesis or the grand Riemann hypothesis.

Conjecture 2 (Generalized Riemann hypothesis). Let $F \in \mathbb{S}$. If $F(s) = 0$ for $0 < \Re(s) < 1$, then $\Re(s) = 1/2$.

Although we are far from proving the Riemann hypothesis, a lot is known about the number of zeros of functions in $\mathbb{S}$ in the critical strip. In this direction, it is important to discuss the growth of an L-function in vertical strips. For any analytic function, counting the number of zeros in a region is often tackled by its values on the boundary using Jensen's theorem. Therefore, in order to capture the number of zeros of $F(s) \in \mathbb{S}$ in the strip $0 < \Re(s) < 1$ and $|\Im(s)| < T$, we need to understand the growth of $F(\sigma + it)$ for σ fixed and t growing large. For $F(s) \in \mathbb{S}$, define

$$\mu_F(\sigma) := \limsup_{|t|\to\infty} \frac{\log F(\sigma + it)}{\log |t|}.$$

We clearly have $\mu_F(\sigma) = 0$ for $\sigma > 1$. Moreover, on the left half plane $\sigma < 0$, $\mu_F(\sigma)$ is obtained using the functional equation

$$F(s) = \frac{\gamma(1-\overline{s})}{\gamma(s)} \overline{F(1-\overline{s})},$$

where the gamma-factor is given by

$$\gamma(s) = Q^s \prod_{j=1}^{k} \Gamma(\alpha_j s + \beta_j).$$

Applying Stirling's formula, we get for $t \geq 1$, uniformly in σ,

$$\frac{\gamma(1-\overline{s})}{\gamma(s)} = \left(\alpha Q^2 t^{d_F}\right)^{1/2-\sigma-it} \exp\left(itd_F + \frac{i\pi(\beta - d_F)}{4}\right)\left(\omega + O\left(\frac{1}{T}\right)\right), \quad (7)$$

where

$$\alpha := \prod_{j=1}^{k} \alpha_j^{2\alpha_j} \text{ and } \beta := 2\sum_{j=1}^{k}(1 - 2\beta_j).$$

Recall the Phragmén-Lindelöf theorem given by

Theorem 4.1 (Phragmén-Lindelöf). *Let $f(s)$ be analytic in the strip $\sigma_1 \leq \Re(s) \leq \sigma_2$ with $f(s) \ll \exp(\epsilon|t|)$. If*

$$|f(\sigma_1 + it)| \ll |t|^{c_1} \quad \text{and}$$

$$|f(\sigma_2 + it)| \ll |t|^{c_2},$$

then

$$|f(\sigma + it)| \ll |t|^{c(\sigma)},$$

uniformly in $\sigma_1 \leq \sigma \leq \sigma_2$, where $c(\sigma)$ is linear in σ with $c(\sigma_1) = c_1$ and $c(\sigma_2) = c_2$.

Using the Phragmén-Lindelöf theorem and (7), we get the following upper bounds on the growth of an element in $\mathbb{S}$.

Proposition 4.2. *Let $F \in \mathbb{S}$. Uniformly in σ, as $|t| \to \infty$,*

$$F(\sigma + it) \sim |t|^{(1/2-\sigma)d_F}|F(1 - \sigma + it)|,$$

where d_F denotes the degree of F. We also have

$$\mu_F(\sigma) \leq \begin{cases} 0 & \text{if } \sigma > 1, \\ \frac{1}{2}d_F(1-\sigma) & \text{if } 0 \leq \sigma \leq 1, \\ d_F\left(\frac{1}{2} - \sigma\right) & \text{if } \sigma < 0. \end{cases}$$

Using the functional equation, it is possible to show that for $F \in \mathbb{S}$,

$$d_F = \limsup_{\sigma < 0} \frac{\mu_F(\sigma)}{1/2 - \sigma}. \tag{8}$$

This gives a characterization of degree in terms of the growth of $F(s)$ in the left half plane $\Re(s) < 0$.

Lindelöf conjectured that the order of growth of the Riemann zeta-function is much smaller than what the Phragmén-Lindelöf theorem gives. In fact, he predicted that $\zeta(s)$ is bounded on $\sigma > 1/2$ (see [24]). This statement is known to be false. But, a weaker version would state that $\mu_\zeta(1/2) = 0$. In other words,

$$\left|\zeta\left(\frac{1}{2} + it\right)\right| \ll |t|^{\epsilon},$$

for any $\epsilon > 0$. This is known as the Lindelöf hypothesis. Note that, the Phragmén-Lindelöf theorem only implies that $|\zeta(1/2 + it)| \ll_\epsilon |t|^{1/4+\epsilon}$ for any $\epsilon > 0$. Any improvement on the constant $1/4$ is called the phenomena of "breaking convexity". The best known improvement on this constant is replacing $1/4$ with $9/56$. This is due to E. Bombieri and H. Iwaniec [8] using Weyl's method of estimating exponential sums, which was earlier incorporated by G. H. Hardy and J. E. Littlewood to attack the same problem.

A more general statement of the Lindelöf hypothesis on the Selberg class is given by

Conjecture 3 (Generalized Lindelöf hypothesis). For $F \in \mathbb{S}$ and any $\epsilon > 0$,

$$\left| F\left(\frac{1}{2} + it\right) \right| \ll |t|^{\epsilon}.$$

It is known due to Littlewood that the Riemann hypothesis implies the Lindelöf hypothesis. By the same argument, one can show that the generalized Riemann hypothesis implies the generalized Lindelöf hypothesis. Moreover, the Lindelöf hypothesis itself has many interesting consequences. The most prominent one is in the context of value distribution of L-functions.

For $F \in \mathbb{S}$, let $N_F(\sigma, T)$ denote the number of zeros of $F(s)$ in the region

$$\left\{ s \in \mathbb{C} : \Re(s) > \sigma, |\Im(s)| < T \right\}.$$

The Lindelöf hypothesis for Riemann zeta-function implies the density hypothesis, which states that for $\sigma > 1/2$,

$$N_{\zeta}(\sigma, T) \ll T^{2(1-\sigma)}.$$

In case of the Selberg class, the generalized Lindelöf hypothesis implies a statement regarding the zero-distribution of L-functions, which we call the zero hypothesis. The classical result on zero density estimate due to Bohr and Landau [6] states that most of the zeroes of $\zeta(s)$ are clustered near the 1/2-line, i.e.,

$$N_{\zeta}(\sigma, T) \ll T^{4\sigma(1-\sigma)+\epsilon}, \tag{9}$$

for $\sigma > 1/2$. More recently, we have the following density theorem due to Kaczorowski and Perelli [19] for the Selberg class.

Theorem 4.3 (Density theorem). *For $F \in \mathbb{S}$,*

$$N_F(\sigma, T) \ll_{\epsilon} T^{c(1-\sigma)+\epsilon},$$

for $\sigma > 1/2$ and $c = 4d_F + 12$.

The above zero-density estimate suggests that the number of zeros close to the vertical line $\Re(s) = 1$ is very small. In general, we formulate the zero hypothesis, which claims that for $F \in \mathbb{S}$ all the zeros are clustered near the 1/2-line.

Conjecture 4 (Zero hypothesis). For $F \in \mathbb{S}$, there is a positive constant c such that for $\sigma > 1/2$,

$$N_F(\sigma, T) \ll T^{1-c(\sigma-1/2)+\epsilon}.$$

Using Riemann-von Mongoldt-type formula, it is possible to count the number of zeros of $F \in \mathbb{S}$ more precisely. (see [35])

Proposition 4.4. *For $F \in \mathbb{S}$, we have*

$$N_F(0, T) = \frac{d_F}{\pi} T \log T + c_F T + O(\log T), \tag{10}$$

where d_F is the degree of F and c_F is a constant depending on F.

Thus, we get another characterization of degree for $F \in \mathbb{S}$ using the number of zeros of F in the critical strip. We have for $F(s) \in \mathbb{S}$

$$d_F = \limsup_{T \to \infty} \frac{N_F(0, T)}{T \log T} \pi. \tag{11}$$

In the above proposition, we could replace counting zeros with counting any a-value and get the exact same result. Define

$$N(F, a, T) := \#\{F(s) = a : 0 < \Re(s) < 1, |\Im(s)| < T\},$$

counted with multiplicity. Then, we have

$$N(F, a, T) = \frac{d_F}{\pi} T \log T + c_F T + O(\log T).$$

5. Selberg's Conjectures

The elements in the Selberg class are not closed under linear combination. But, the Selberg class is closed under multiplication and forms a semi-group with respect to multiplication i.e., if $F, G, H \in \mathbb{S}$, then $FG \in \mathbb{S}$ and $F(GH) = (FG)H$. The fundamental elements with respect to multiplication in $\mathbb{S}$ are called the primitive elements.

Definition 5.1. *$F \in \mathbb{S}$ is said to be a primitive element if any factorization $F = F_1 F_2$ with $F_1, F_2 \in \mathbb{S}$ implies that either $F_1 = 1$ or $F_2 = 1$.*

In other words, an element in $\mathbb{S}$ is primitive if it cannot be further factorized into non-trivial elements in $\mathbb{S}$. Using the characterization of degree in (11), we have that if $F \in \mathbb{S}$ has a factorization $F = F_1 F_2$, with $F_1, F_2 \in \mathbb{S}$, then

$$N(T, F) = N(T, F_1) + N(T, F_2).$$

Taking $T \to \infty$, we conclude that

$$d_F = d_{F_1} + d_{F_2}.$$

We also know from Theorem 3.1 that non-trivial elements in $\mathbb{S}$ cannot have degree < 1. Therefore, we cannot factorize an element $F \in \mathbb{S}$ indefinitely.

Proposition 5.2. *Every element $F \in \mathbb{S}$ can be factorized into primitive elements in $\mathbb{S}$.*

It is still unknown whether the above factorization is unique.

Conjecture 5 (Unique factorization in $\mathbb{S}$). Every element $F \in \mathbb{S}$ can be uniquely factorized into primitive elements.

From the above discussion, it is clear that every element $F \in \mathbb{S}$ with degree $d_F = 1$ is a primitive element. Thus, the Riemann zeta-function and Dirichlet L-functions are all primitive elements in the Selberg class. We know very little about the primitive elements of higher degrees. In [29], M. R. Murty showed that if π is an irreducible cuspidal representation of $GL_2(\mathbb{A}_{\mathbb{Q}})$, then $L(s, \pi)$ is primitive if the Ramanujan conjecture is true.

Selberg's conjectures claim that distinct elements in $\mathbb{S}$ do not interact with each other. Vaguely speaking, distinct primitive elements are orthogonal to each other.

Conjecture 6 (Selberg's conjectures). In [35], Selberg made the following conjectures.

(1) Conjecture A – Let $F \in \mathbb{S}$. There exists a constant n_F such that

$$\sum_{p \leq x} \frac{|a_F(p)|^2}{p} = n_F \log\log x + O(1). \tag{12}$$

(2) Conjecture B – Let $F, G \in \mathbb{S}$ be primitive elements. Then

$$\sum_{p \leq x} \frac{a_F(p)\overline{a_G(p)}}{p} = \begin{cases} \log\log x + O(1), & \text{if } F = G, \\ O(1) & \text{otherwise.} \end{cases}$$

Conjecture B is known as the Selberg's orthogonality conjecture.

It is easy to verify Conjecture A in particular cases. For instance, Conjecture A clearly holds for the Riemann zeta-function and Dirichlet L-functions. Conjecture B can also be verified in the case of Dirichlet L-functions using the orthogonality relations for characters.

In view of Proposition 5.2, it is easy to see that Conjecture B implies Conjecture A. Indeed, if $F \in \mathbb{S}$ has a factorization into primitive elements given by

$$F(s) = F_1(s)F_2(s) \cdots F_m(s),$$

where $F_k(s)$ is primitive for all $1 \leq k \leq m$, then,

$$\sum_{p \leq x} \frac{|a_F(p)|^2}{p} = \sum_{1 \leq j \leq k \leq m} \sum_{p \leq x} \frac{a_{F_j}(p)\overline{a_{F_k}(p)}}{p}.$$

By Conjecture B, the above sum is of the form

$$m \log\log x + O(1),$$

where m is the number of factors in the factorization of $F(s)$ into primitive elements.

Selberg [35] noted that there are connections between these conjectures and several other conjectures like the Sato-Tate conjecture, Langlands conjectures etc. It is not difficult to see that Conjecture B implies unique factorization in $\mathbb{S}$. This was perhaps known to Selberg, but was shown in the work of J. B. Conrey and A. Ghosh [9].

Proposition 5.3. *Conjecture B implies that every element $F \in \mathbb{S}$ has unique factorization into primitive elements.*

Proof. Suppose $F \in \mathbb{S}$ has two different factorizations into primitives, say,

$$F(s) = \prod_{j=1}^{m} F_j(s) = \prod_{k=1}^{r} G_k(s).$$

We can further assume that no F_j is same as G_k. Since

$$\sum_{j=1}^{m} a_{F_j}(p) = \sum_{k=1}^{r} a_{G_k}(p),$$

multiplying both sides by $\overline{a_{F_1}(p)}/p$ and summing over $p \leq x$, we get

$$\sum_{j=1}^{m} \sum_{p \leq x} \frac{a_{F_j}(p)\overline{a_{F_1}(p)}}{p} = \sum_{k=1}^{r} \sum_{p \leq x} \frac{a_{G_k}(p)\overline{a_{F_1}(p)}}{p}. \tag{13}$$

Now, Conjecture B implies that the LHS of (13) is unbounded where as the RHS is bounded as x tends to infinity, which leads to a contradiction. □

By a similar argument as above, we also conclude the following.

Proposition 5.4. *An element $F \in \mathbb{S}$ is a primitive element if and only if $n_F = 1$, where n_F is given by* (12).

In [28], M.R. Murty proved that Conjecture B implies Artin's conjecture.

Theorem 5.5 (M. R. Murty). *For any irreducible representation ρ of $Gal(L/K)$ of degree n, the Artin L-function $L(s, \rho, L/K)$ is entire if Conjecture B holds.*

In fact, he showed something stronger. Langland's reciprocity conjecture states that for any irreducible representation ρ of $Gal(L/K)$ of degree n, there exists an irreducible cuspidal automorphic representation π of $GL_n(\mathbb{A}_{\mathbb{Q}})$, such that $L(s, \rho, L/K) = L(s, \pi)$. Since $L(s, \pi)$ are known to be entire, Artin's conjecture is a consequence of this statement. In [28], M. R. Murty showed that if $K/\mathbb{Q}$ is solvable, then Conjecture B implies Langlands reciprocity conjecture.

In this direction, M. R. Murty [29] initiated the study of Selberg's conjectures over number fields. For any number field K, the idea is to consider functions, given by

$$F(s) = \sum_{\mathfrak{n} \subset \mathcal{O}_K} \frac{a_{\mathfrak{n}}}{\mathbb{N}(\mathfrak{n})^s} \tag{14}$$

on $\Re(s) > 1$, where $\mathfrak{n}$ runs over all non-zero integral ideals of K. The expected functional equation and the Euler product were modified analogously. This new class of functions denoted $\mathbb{S}_K$ could be considered as the Selberg class over a number field K. It is not difficult to see that $\mathbb{S}_K$ is a subset of $\mathbb{S}$. He introduced the notion of K-primitives in $\mathbb{S}_K$ analogous to the primitive elements in $\mathbb{S}$ and made conjectures analogous to the Selberg's conjectures for $\mathbb{S}_K$ discussing its applications to Langland's conjectures (see [29]). This front of study seems to have a lot of potential for future exploration.

There are many more interesting consequences of Conjecture B. Using a similar argument as in Proposition 5.3, one can prove that the Conjecture B implies that if $F \in \mathbb{S}$ has a pole at $s = 1$, it must come from the Riemann-zeta function. More precisely,

Lemma 5.6. *If $F(s) \in \mathbb{S}$ has a pole of order m at $s = 1$, then Conjecture B implies that $F(s) = \zeta(s)^m L(s)$, where $L \in \mathbb{S}$.*

Proof. Since Conjecture B implies unique factorization into primitive elements in $\mathbb{S}$, it suffices to show that if $F \in \mathbb{S}$ is a primitive element with a pole at $s = 1$, then it is $\zeta(s)$. From Proposition 5.4 we know that $n_\zeta = 1$ and $n_F = 1$. If $F \neq \zeta$, then Conjecture B implies that

$$\sum_{p \leq x} \frac{a_F(p)}{p} \ll 1,$$

which is a contradiction. □

This expectation that every pole comes from $\zeta(s)$ can be thought of as the amelioration of Dedekind's conjecture, which states that every Dedekind zeta-function $\zeta_K(s)$ must factorize through $\zeta(s)$.

The Selberg class is designed to model the class of L-functions satisfying the Riemann hypothesis. So, one might ask whether the analogue of prime number theorem is true for the elements in $\mathbb{S}$. Recall that the prime number theorem for natural numbers follows from the fact that $\zeta(s)$ does not vanish on the vertical line $\Re(s) = 1$. It was shown by Kaczorowski and Perelli [19] that prime number theorem for any $F \in \mathbb{S}$ is equivalent to the non-vanishing of $F(s)$ on $\Re(s) = 1$. Thus, one can formulate the prime number theorem in the Selberg class as follows.

Conjecture 7 (Generalized prime number theorem). If $F \in \mathbb{S}$, then $F(s) \neq 0$ for $s = 1 + it$ for any $t \in \mathbb{R}$.

This is still open. But, the above conjecture can be shown assuming Conjecture B. In fact, Kaczorowski and Perelli [19] proved the Conjecture 7 with an assumption weaker than Conjecture A. This weaker assumption is often called the normality conjecture, which is similar to Conjecture A, but with a weaker error term. Here, we present an argument showing that Conjecture B implies Conjecture 7. We use the following lemma.

Lemma 5.7. *If $F \in \mathbb{S}$ has a pole or a zero at $s = 1 + i\theta$ for $\theta \in \mathbb{R}$, then*

$$\sum_{p \leq x} \frac{a_F(p)}{p^{1+i\theta}}$$

is unbounded as x tends to ∞.

Proof. If $F(s)$ has a pole or zero of order $m \neq 0$ at $1 + i\theta$, then we have

$$F(s) \sim c(s - (1 + i\theta))^m,$$

near $1 + i\theta$. Writing $s = \sigma + it$ and taking log, we get

$$\log F(s) \sim m \log(\sigma - 1)$$

near $s = 1 + i\theta$. Moreover, from the Euler product, we have for $\sigma > 1$,

$$\log F(s) = \sum_p \frac{a_F(p)}{p^s} + O(1).$$

Thus, we get

$$\sum_p \frac{a_F(p)}{p^s} \sim m \log(\sigma - 1),$$

as $\sigma \to 1^+$. Assume the function

$$S(x) = \sum_{p \le x} \frac{a_F(p)}{p^{1+i\theta}}$$

is bounded. Then, we have

$$\sum_p \frac{a_F(p)}{p^s} = \int_1^\infty x^{1-\sigma} dS(x)$$
$$= (\sigma - 1) \int_1^\infty S(x) x^{-\sigma}\, dx \ll 1,$$

which is a contradiction. □

We are now ready to prove the following proposition.

Proposition 5.8. *Conjecture B implies Conjecture 7.*

Proof. Since Conjecture B implies unique factorization, it is enough to show the non-vanishing of $F(s)$ on $\Re(s) = 1$ for primitive elements $F \in \mathbb{S}$. Since $\zeta(s)$ does not vanish on $\Re(s) = 1$, using Lemma 5.6, we can further assume that $F(s)$ is entire. This implies that $F(s + i\alpha) \in \mathbb{S}$ for any $\alpha \in \mathbb{R}$.

Now, if F has a zero at $s = 1 + i\theta$, Lemma 5.7 implies that

$$\sum_{p \le x} \frac{a_F(p)}{p^{1+i\theta}}$$

is unbounded as $x \to \infty$. But the Conjecture B applied to $\zeta(s)$ and $F(s + i\theta)$ yields

$$\sum_{p \le x} \frac{a_F(p)}{p^{1+i\theta}} \ll 1,$$

which leads to a contradiction. □

It was observed by Selberg in [35] and Bombieri-Hejhal in [7] that distinct elements in the Selberg class are linearly independent. For an explicit argument, the reader may refer to [10, Lemma 3.5.5]. A natural question that arises is whether distinct primitive elements in $\mathbb{S}$ are algebraically independent. G. Molteni [26] showed that this is a consequence of Conjecture B.

Proposition 5.9. *Conjecture B implies that distinct primitive elements in $\mathbb{S}$ are algebraically independent.*

Proof. Selberg's orthonormality conjecture implies that the factorization into primitive elements in the Selberg class is unique. Suppose, $F_1, F_2, \dots, F_n$ are distinct primitive elements in $\mathbb{S}$ satisfying a polynomial $P(x_1, x_2, \dots, x_n) \in \mathbb{C}[x_1, x_2, \dots, x_n]$. By linear independence of distinct elements in $\mathbb{S}$, we conclude that not all terms in the polynomial expansion of $P(F_1, \dots, F_n)$ are distinct. Thus, we have relations of the form

$$F_1^{a_1} F_2^{a_2} \dots F_n^{a_n} = F_1^{b_1} F_2^{b_2} \dots F_n^{b_n}, \tag{15}$$

where not all the a_i's are the same as the b_i's. But, both the left hand side and the right hand side in (15) are elements in the Selberg class. This contradicts the unique factorization. □

6. Uniqueness results for elements in $\mathbb{S}$

Selberg's orthogonality conjecture implies that for $F, G \in \mathbb{S}$, if $a_F(p) = a_G(p)$ for all but finitely many primes p, then $F = G$. Such uniqueness results are called strong multiplicity one theorems for the Selberg class. Unconditionally, it was shown by M. R. Murty and V. K. Murty [30] that

Theorem 6.1 (Murty-Murty). *For $F, G \in \mathbb{S}$, if $a_F(p) = a_G(p)$ and $a_F(p^2) = a_G(p^2)$ for all but finitely many primes p, then $F = G$.*

As an immediate consequence, we have that if $F, G \in \mathbb{S}$ satisfy the property that the Euler factors $F_p(s) = G_p(s)$ for all but finitely many primes p, then $F = G$. It is expected that the condition $a_F(p) = a_G(p)$ for all but finitely many primes p uniquely characterizes the function in $\mathbb{S}$. But a proof of this fact is still unknown. However, if we further impose the condition that $F(s)$ and $G(s)$ have polynomial Euler product, i.e. an Euler product of the form

$$F(s) = \prod_p \prod_{j=1}^{k} \left(1 - \frac{\alpha_p(j)}{p^s}\right)^{-1},$$

with $|\alpha_p(j)| < 1$, then it was shown by J. Kaczorowski and A. Perelli [18] that for $F, G \in \mathbb{S}$ if $a_F(p) = a_G(p)$ for all but finitely many p, then $F = G$. It is worth noting that the elements in the Selberg class are expected to have polynomial Euler product. As a token of evidence, note that the Riemann zeta-function, Dedekind zeta-functions, Hecke L-functions, L-functions attached to holomorphic cusp forms and in fact all automorphic L-functions have polynomial Euler product.

Another aspect to the uniqueness of elements in the Selberg class arises from the a-value distribution. If $F, G \in \mathbb{S}$ take the same value at sufficiently many points in the critical strip, then $F = G$.

For any two meromorphic functions f and g, we say that they share a value 'a' ignoring multiplicity if $f^{-1}(a)$ is same as $g^{-1}(a)$ as sets. We further say that f and g share a value 'a' counting multiplicity if the zeroes of $f(x) - a$ and $g(x) - a$ are the same with multiplicity. Nevanlinna theory [32] establishes that any two meromorphic functions of finite order sharing five values ignoring multiplicity must be the same. Moreover, if they share four values counting multiplicity, then one must be a Möbius transform of the other. The numbers four and five are the best possible for meromorphic functions.

One can get much stronger results for L-functions. For $F, G \in \mathbb{S}$, define

$$D_{F,G}(T) = \sum_{\rho} |m_F(\rho) - m_G(\rho)|,$$

where ρ runs over all the non-trivial zeroes of F and G with $|\Im(\rho)| < T$ and $m_F(\rho)$ denotes the order of the zero of F at ρ. Then, M. R. Murty and V. K. Murty [30] showed that if $D_{F,G}(T) = o(T)$, then $F = G$. In other words, if F, G share sufficiently many zeros counting multiplicity, then they must be the same. It is possible to show the above result for any a-values.

Proposition 6.2. *For $F, G \in \mathbb{S}$, if F, G share a complex value 'a' counting multiplicity for all but finitely many points, then $F = G$.*

Proof. Since F and G have only one possible pole at $s = 1$, we define H as

$$H := \frac{F - a}{G - a} Q,$$

where $Q(s) = (s - 1)^k p(s)$ is a rational function and $p(s)$ a polynomial such that H has no poles or zeros. Since, F and G have complex order 1, we conclude that H has order at most 1 and hence is of the form

$$H(s) = e^{ms+n}.$$

This immediately leads to $m = 0$, since F and G are absolutely convergent on $\Re(s) > 1$ and taking $s \to \infty$, $F(s)$ and $G(s)$ approach their leading coefficient 1. Similarly, we also get $Q(s) = 1$. This forces

$$F(s) = cG(s) + d.$$

for some constants $c, d \in \mathbb{C}$. Since, F and G have leading coefficient 1, we conclude that $F = G$. □

It is possible to prove stronger results than above using similar techniques used by M. R. Murty and V. K. Murty in [30] to show that if $F, G \in \mathbb{S}$ satisfy $D_{F-a,G-a}(T) = o(T)$, then $F = G$.

In this context, a natural question of interest would be to investigate how many values can two distinct elements in $\mathbb{S}$ share ignoring multiplicity. Clearly, $F(s)$ and $F^2(s)$ share zeros ignoring multiplicity. So the best one could expect is that $F, G \in \mathbb{S}$ sharing two distinct values ignoring multiplicity must be the same. J. Steuding [36] proved this with some extra conditions. In 2010, B. Q. Li [23] gave a proof dropping the additional conditions.

Theorem 6.3 (B. Q. Li). *Let a, b be two distinct complex numbers. If $F, G \in \mathbb{S}$ share values a and b ignoring multiplicity, then $F = G$.*

The main idea in such uniqueness results was to introduce Nevanlinna theory to the study of value distribution theory. In a previous paper, B. Q. Li [22] also showed the following.

Theorem 6.4 (B. Q. Li). *Let $F \in \mathbb{S}$ and f be a meromorphic function with finitely many poles. Suppose F and f share a value 'a' counting multiplicity and another value 'b' ignoring multiplicity, then $F = f$.*

For stronger versions of the above results, the reader may refer to [11]. One can show all the above results by dropping the Euler product and the Ramanujan hypothesis. The question still remains of how large can the error $D_{F,G}(T)$ be. When sharing values ignoring multiplicity, there is no known satisfactory answer to this question.

7. Limit theorems and universality

In the early twentieth century, Harald Bohr introduced geometric and probabilistic methods to the study of the value distribution of the Riemann zeta-function. In this section, the probabilistic methods will be of significance.

For the Riemann zeta-function $\zeta(s)$, we know that if $\sigma_0 > 1$, then

$$|\zeta(s)| \leq \zeta(\sigma_0)$$

in the right half plane $\Re(s) \geq \sigma_0$. In other words, $\zeta(s)$ is bounded on any right half plane $\Re(s) > 1+\epsilon$. The natural question to consider is what happens as σ_0 approaches 1 from the right. In this regard, Bohr [2] proved that in any strip $1 < \Re(s) < 1+\epsilon$, $\zeta(s)$ takes any non-zero complex value infinitely often. The main tool used by Bohr was the Euler product of $\zeta(s)$. Similar study in the critical strip is much more difficult. To tackle this problem, Bohr studied truncated Euler products

$$\zeta_M(s) := \prod_{p \leq M} \left(1 - \frac{1}{p^s}\right)^{-1}.$$

The functions $\zeta_M(s)$ do not converge in the critical strip as M tends to ∞. However, Bohr showed that in the critical strip, for large M, $\zeta_M(s)$ approximates $\zeta(s)$ well in the following sense.

$$\int_T^{2T} \iint_D \left| \frac{\zeta(s+i\tau)}{\zeta_M(s+i\tau)} - 1 \right|^2 d\sigma\, dt\, d\tau \ll \epsilon T, \quad \text{for all } \epsilon > 0,$$

where $D := \{s = \sigma + it : 1/2 + \delta < \sigma \le 2, |t| \le 1\}$. This remarkable idea plays a key role in many interesting discoveries of Bohr.

In [3], Bohr showed that for any $\sigma_0 \in (1/2, 1)$, the image of the vertical line $\{\Re(s) = \sigma_0\}$ given by

$$\Big\{\zeta(s) : s = \sigma_0 + it, t \in \mathbb{R}\Big\}$$

is dense in $\mathbb{C}$. Later, Bohr and Jessen [4], [5] improved these results using probabilistic methods to prove the following limit theorem.

Theorem 7.1 (Bohr, Jessen). *Let R be any rectangle in $\mathbb{C}$ with sides parallel to the real and imaginary axis. Let G be the half plane $\{\Re(s) > 1/2\}$ except for points $z = x + iy$ such that there is a zero of $\zeta(s)$ given by $\rho = \alpha + iy$ with $x \le \alpha$. For any $\sigma > 1/2$, the limit*

$$\lim_{T\to\infty} \frac{1}{T} meas\Big\{\tau \in [0, T] : \sigma + i\tau \in G,\ \log\zeta(\sigma + i\tau) \in R\Big\}$$

exists.

Here the measure is the usual Lebesgue measure. Later, Hattori and Matsumoto [13] identified the probability distribution given by the above limit theorem. It is reasonable to hope that Bohr-Jessen type results can be shown for general automorphic L-functions.

In 1972, Voronin [38] proved the following generalization of Bohr's limit theorem.

Theorem 7.2 (Voronin). *For any fixed distinct numbers $s_1, s_2, \ldots, s_n$ with $1/2 < \Re(s_j) < 1$ for $1 \le j \le n$, the set*

$$\Big\{(\zeta(s_1 + it), \ldots, \zeta(s_n + it)) : t \in \mathbb{R}\Big\}$$

is dense in $\mathbb{C}^n$. Moreover, for any fixed number s with $1/2 < \Re(s) < 1$,

$$\Big\{(\zeta(s + it), \zeta'(s), \ldots, \zeta^{(n-1)}(s + it)) : t \in \mathbb{R}\Big\}$$

is dense in $\mathbb{C}^n$.

Analogous limit and density theorems for other L-functions were obtained by Matsumoto [25], Laurinčikas [21], Šleževičienė [40] et al.

It is interesting to note that despite the density theorems, we do not understand the value distribution of $\zeta(s)$ on $\Re(s) = 1/2$. A folklore, yet unsolved conjecture is that the set of values of $\zeta(s)$ on $\Re(s) = 1/2$ is dense in $\mathbb{C}$. In this direction, Selberg showed that "up to some normalization" of $\zeta(s)$, the values on the 1/2-line satisfy the Gaussian distribution (see Joyner [14]).

In 1975, Voronin [39] proved a fascinating theorem for the Riemann zeta-function, which roughly says that any non-vanishing analytic function is approximated uniformly by shifts of the zeta-function in the critical strip. This is called the Voronin's universality theorem. More precisely,

Theorem 7.3 (Voronin). *Let $0 < r < \frac{1}{4}$ and suppose that $g(s)$ is a non-vanishing continuous function on the disc $\{s : |s| \leq r\}$, which is analytic in its interior. Then, for any $\epsilon > 0$,*

$$\liminf_{T\to\infty} \frac{1}{T}\, meas \left\{ |\tau| < T : \max_{|s|<r} \left| \zeta\left(s + \frac{3}{4} + i\tau\right) - g(s) \right| < \epsilon \right\} > 0.$$

After the result of Voronin, Bagchi [1] gave a proof of universality for the Riemann zeta-function $\zeta(s)$ and some other L-functions using probabilistic methods. Using Bagchi's technique, the universality property for many L-functions has been established, mainly due to the work of Laurančikas, Matsumoto, Steuding et al. In particular, we know that the universality property holds for elements in the Selberg class $\mathbb{S}$ satisfying a condition analogous to the prime number theorem (see [31]).

Theorem 7.4 (Steuding, Nagoshi). *Let $L(s) \in \mathbb{S}$ with degree d_L satisfying the condition*

$$\lim_{x\to\infty} \frac{1}{\pi(x)} \sum_{p\leq x} |a_L(p)|^2 = \kappa_L,$$

where κ_L is a constant depending on L. Let K be a compact subset of the strip

$$1 - \frac{1}{2d_L} < \Re(s) < 1,$$

with connected complement. Suppose $g(s)$ is any non-vanishing continuous function on K, which is analytic in the interior of K. Then, for any $\epsilon > 0$,

$$\liminf_{T\to\infty} \frac{1}{T}\, meas \left\{ |\tau| < T : \max_{s\in K} |L(s + i\tau) - g(s)| < \epsilon \right\} > 0$$

It is important to note that the L-functions for which the universality property has been established is much larger than the Selberg class. In fact, L-functions such as the Hurwitz zeta-function, Lerch zeta-function or Matsumoto zeta-functions are all known to be universal in a certain strip. In view of this, Linnik and Ibragimov conjectured the following.

Conjecture 8 (Linnik, Ibragimov). Let $F(s)$ have a Dirichlet series representation, absolutely convergent on $\Re(s) > 1$ and suppose $F(s)$ can be analytically continued to $\mathbb{C}$ except for a possible pole at $s = 1$ satisfying some "growth conditions", then $F(s)$ is universal in a certain strip.

Although the universality property for elements in $\mathbb{S}$ is conditionally known, the study is far from complete. In particular, for $F \in \mathbb{S}$, the strip for which the universality property has been established is given by $1 - 1/2d_F < \Re(s) < 1$. But the expected strip of universality is $1/2 < \Re(s) < 1$ (see [37], [10]). This is, in fact a consequence of the Lindelöf hypothesis.

Another front to investigate is the following: for a given non-vanishing analytic function $g(s)$ on a compact subset K inside the strip of universality and a given $\epsilon > 0$, for what value of T_0 is the universality property realized? In other words, how large must T_0 be such that for any $T > T_0$, $F(s)$ approximates $g(s)$ up to ϵ, δT number of times, where $\delta > 0$. Unfortunately, there are no known results in this direction. It would be interesting to explicitly describe T when g is a polynomial or a Dirichlet polynomial.

8. Lindelöf class: A generalization

Despite its generality, the Selberg class has several limitations. For instance, it is not closed under addition. This is because of the rigidity of functional equation and the Euler product. Thus, the zero distribution of linear combination of L-functions in the Selberg class, which appears in the work of Bombieri and Hejhal [7] is not addressed by studying the value distribution theory of elements in $\mathbb{S}$. Moreover, some naturally occurring L-functions such as the Hurwitz zeta-function or Lerch zeta-function are not members of the Selberg class. Furthermore, functions such as the Epstein zeta-function, which satisfy a functional equation of the Riemann-type may not always have an Euler product and hence are not members of the Selberg class. This motivated V. K. Murty [27] to introduce a larger class of L-functions $\mathbb{M}$ which contains $\mathbb{S}$, is closed under linear combination and also captures many familiar L-functions, which are not in $\mathbb{S}$. This new class $\mathbb{M}$ forms a ring and the value distribution of elements in $\mathbb{M}$ is very similar to that of the Selberg class. In order to define $\mathbb{M}$, we start by introducing some growth parameters.

Let $F(s)$ be an entire function of order ≤ 1, which is given by the Dirichlet series $F(s) = \sum_n a_n/n^s$ on $\Re(s) > 1$. Define $\mu_F(\sigma)$ as

$$\mu_F(\sigma) := \begin{cases} \inf\Big\{\lambda \in \mathbb{R} : |F(s)| \leq (|s|+2)^{\lambda}, \text{ for all } s \text{ with } \Re(s) = \sigma\Big\}, \\ \\ \infty, \text{ if the infimum does not exist.} \end{cases} \tag{16}$$

Also define:

$$\mu_F^*(\sigma) := \begin{cases} \inf\Big\{\lambda \in \mathbb{R} : |F(\sigma+it)| \ll_{\sigma} (|t|+2)^{\lambda}\Big\}, \\ \\ \infty, \text{ if the infimum does not exist.} \end{cases} \tag{17}$$

If $F(s)$ has a pole of order k at $s = 1$, consider the function

$$G(s) := \left(1 - \frac{2}{2^s}\right)^k F(s). \tag{18}$$

Now define, $\mu_F(\sigma) := \mu_G(\sigma)$ and $\mu_F^*(\sigma) := \mu_G^*(\sigma)$. Intuitively, $\mu_F^*(\sigma)$ does not see how $F(s)$ behaves close to the real axis. It is only dependent on the growth of $F(s)$ on $\Re(s) = \sigma$ and $\Im(s) \gg T$ for arbitrary large T. On the other hand, $\mu_F(\sigma)$ captures an absolute bound for $F(s)$ on the entire vertical line $\Re(s) = \sigma$. It follows from the definition that

$$\mu_F^*(\sigma) \leq \mu_F(\sigma)$$

for any σ.

Definition 8.1. The class $\mathbb{M}$. *Define the class $\mathbb{M}$ (see [27, sec.2.4]) to be the set of functions $F(s)$ satisfying the following conditions.*

(1) **Dirichlet series** – *$F(s)$ is given by a Dirichlet series*

$$\sum_{n=1}^{\infty} \frac{a_F(n)}{n^s},$$

which is absolutely convergent in the right half plane $\Re(s) > 1$.

(2) **Analytic continuation** – *There exists a non-negative integer k such that $(s-1)^k F(s)$ is an entire function of order ≤ 1.*

(3) **Growth condition** – *The quantity $\frac{\mu_F(\sigma)}{(1-2\sigma)}$ is bounded for $\sigma < 0$.*

(4) **Ramanujan hypothesis** – *$|a_F(n)| = O_\epsilon(n^\epsilon)$ for any $\epsilon > 0$.*

Examples of elements in $\mathbb{M}$ include Dirichlet polynomials, all Dirichlet series which are convergent on the whole complex plane, all elements in the Selberg class and their linear combinations, translates of Epstein zeta-functions etc. From the observation (8), we define the following invariants for $\mathbb{M}$, which would play the role of degree in $\mathbb{S}$.

Definition 8.2. *For $F \in \mathbb{M}$, define*

$$c_F := \limsup_{\sigma < 0} \frac{2\mu_F(\sigma)}{1-2\sigma},$$
$$c_F^* := \limsup_{\sigma < 0} \frac{2\mu_F^*(\sigma)}{1-2\sigma}.$$

By the growth condition, c_F and c_F^* are well-defined in $\mathbb{M}$. Furthermore, these invariants satisfy an ultrametric inequality. For $F, G \in \mathbb{M}$,

$$c_{FG} \leq c_F + c_G \quad \text{and} \quad c_{F+G} \leq \max(c_F, c_G).$$

Similarly,

$$c_{FG}^* \leq c_F^* + c_G^* \quad \text{and} \quad c_{F+G}^* \leq \max(c_F^*, c_G^*).$$

In fact, if $c_F > c_G$ (resp. $c_F^* > c_G^*$), then

$$c_{F+G} = c_F \ (\text{resp. } c_{F+G}^* = c_F^*).$$

This ensures that $\mathbb{M}$ is closed under addition.

If $F \in \mathbb{S}$, then $c_F = c_F^* = d_F$. Since the degree in the Selberg class is conjectured to be a non-negative integer, one may wonder if the same is expected to be true for the invariants c_F and c_F^* in $\mathbb{M}$. It turns out that c_F can take non-integer values. In fact, one can manufacture functions in $\mathbb{M}$ with any arbitrary non-negative value c_F. However, we expect c_F^* to take non-negative integer values. In this direction, we have the following partial result (see [27], [12]).

Proposition 8.3. *Suppose $F(s) \in \mathbb{M}$. Then $c_F^* < 1$ implies $c_F^* = 0$.*

It is also possible to classify all elements with $c_F^* = 0$. These are essentially given by all Dirichlet series, which are convergent on the whole of $\mathbb{C}$. There are many more interesting algebraic properties of $\mathbb{M}$. For instance, $\mathbb{M}$ is non-Noetherian. This is interesting because $\mathbb{C}[\mathbb{S}]$ is a subring of $\mathbb{M}$ and Selberg's conjectures imply that $\mathbb{C}[\mathbb{S}]$ is non-Noetherian. Furthermore, the uniqueness result 6.3 and 6.4, and a weaker version of the universality theorem 7.4 can be established for the class $\mathbb{M}$. We refer the reader to [10] for details.

One may wonder if there is some underlying topology on $\mathbb{M}$. Perhaps, understanding the geometry and learning to interpolate between L-functions may hold the key to new discoveries in this fascinating field of mathematics.

9. Acknowledgement

I would like to thank Prof. M. Ram Murty for suggesting me to write this article and several helpful comments. I am grateful to the referee for comments which helped in significantly improving the exposition.

References

[1] B. Bagchi, The statistical behaviour and universality properties of the Riemann zeta-function and other allied Dirichlet series. Indian Statistical Institute, Calcutta, (1981) PhD Thesis.

[2] H. Bohr. Über das verhalten von . (s) in der halbebene . = 1, Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen, *Mathematisch-Physikalische Klasse*, 1911 (1911) 409–428.

[3] H. Bohr, Über eine quasi-periodische Eigenschaft Dirichletscher Reihen mit Anwendung auf die Dirichletschen L-Funktionen, *Math. Ann.*, **85(1)** (1922) 115–122.

[4] H. Bohr and B. Jessen, Über die Werteverteilung der Riemannschen Zetafunktion, *Acta Math.*, **54(1)** (1930) 1–35.

[5] H. Bohr and B. Jessen, Über die Werteverteilung der Riemannschen Zetafunktion, *Acta Math.*, **58(1)** 1–55 (1932).

[6] H. Bohr and E. Landau, Sur les zeros de la fonction $\zeta(s)$ de riemann, *Comptes Rendus Acad. Sci. Paris*, **158** (1914) 106–110.

[7] E. Bombieri and D. A. Hejhal, On the distribution of zeros of linear combinations of Euler products, *Duke Math. J.*, **80(3)** (1995) 821–862.

[8] E. Bombieri and H. Iwaniec. Some mean-value theorems for exponential sums, *Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4)*, **13(3)** (1986) 473–486.

[9] J. B. Conrey and A. Ghosh, On the Selberg class of Dirichlet series: small degrees, *Duke Math. J.*, **72(3)** (1993) 673–693.

[10] A. B. Dixit, The Lindelöf class of L-functions, University of Toronto, 2018. PhD Thesis.

[11] A. B. Dixit, Uniqueness results for a class of l-functions. In A. Akbary and S. Gun, editors, *Geometry, Algebra, Number Theory, and Their Information Technology Applications*, pages 163–181. Springer International Publishing, (2018).

[12] A. B. Dixit and V. K. Murty, The Lindelf class of L-functions, II, *International Journal of Number Theory*, **15(10)**, (2019) 2201–2221.

[13] T. Hattori and K. Matsumoto, A limit theorem for Bohr-Jessen's probability measures of the Riemann zeta-function, *J. Reine Angew. Math.*, **507** (1999) 219–232.

[14] D. Joyner, *Distribution theorems of L-functions*. Harlow, Essex, England: Longman Scientific & Technical; New York: Wiley, (1986). Includes index.

[15] J. Kaczorowski, Axiomatic theory of L-functions: the Selberg class. In Analytic number theory, *Lecture Notes in Math.*, Springer, Berlin, **1891** (2006) 133–209.

[16] J. Kaczorowski and A. Perelli, On the structure of the Selberg class. I. $0 \leq d \leq 1$, *Acta Math.*, **182(2)** 207–241 (1999).
[17] J. Kaczorowski and A. Perelli, On the structure of the Selberg class. II. Invariants and conjectures, *J. Reine Angew. Math.*, **524** 73–96 (2000).
[18] J. Kaczorowski and A. Perelli, Strong multiplicity one for the Selberg class, *C. R. Acad. Sci. Paris Sér. I Math.*, **332(11)** (2001) 963–968.
[19] J. Kaczorowski and A. Perelli, On the prime number theorem for the Selberg class, *Arch. Math. (Basel)*, **80(3)** (2003) 255–263.
[20] J. Kaczorowski and A. Perelli, On the structure of the Selberg class, VII: $1 < d < 2$, *Ann. of Math. (2)*, 173(3) (2011) 1397–1441.
[21] A. Laurinchikas, A limit theorem for Dirichlet L-series, *Mat. Zametki*, **25(4)** 635 (1979) 481–485.
[22] B. Q. Li, A result on value distribution of L-functions, *Proc. Amer. Math. Soc.*, **138(6)** (2010) 2071–2077.
[23] B. Q. Li, A uniqueness theorem for Dirichlet series satisfying a Riemann type functional equation, *Adv. Math.*, **226(5)** (2011) 4198–4211.
[24] E. Lindelöf, Quelques remarques sur la croissance de la fonction $\zeta(s)$, *Bull. Sci. Math.*, **32** (1908) 341–356.
[25] K. Matsumoto, Value-distribution of zeta-functions. In Analytic number theory (Tokyo, 1988), *Lecture Notes in Math.*, Springer, Berlin, **1434** (1990) 178–187.
[26] G. Molteni, On the algebraic independence in the Selberg class, *Arch. Math. (Basel)*, **79(6)** (2002) 432–438.
[27] K. Murty, The Lindelöf class of L-functions. In The Conference on L-Functions, *World Sci. Publ.*, Hackensack, NJ, 165–174 (2007).
[28] M. R. Murty, Selberg's conjectures and Artin L-functions, *Bull. Amer. Math. Soc. (N.S.)*, **31(1)** (1994) 1–14.
[29] M. R. Murty, Selberg's conjectures and Artin L-functions, II. In Current trends in mathematics and physics, Narosa, New Delhi, (1995) 154–168.
[30] M. R. Murty and V. K. Murty, Strong multiplicity one for Selberg's class, *C. R. Acad. Sci. Paris Sér. I Math.*, **319(4)** (1994) 315–320.
[31] H. Nagoshi and J. Steuding, Universality for L-functions in the Selberg class, *Lith. Math. J.*, **50(3)** (2010) 293–311.
[32] R. Nevanlinna, Einige Eindeutigkeitssätze in der Theorie der Meromorphen Funktionen, *Acta Math.*, **48(3–4)** (1926) 367–391.
[33] A. Perelli, A survey of the Selberg class of L-functions. II, *Riv. Mat. Univ. Parma (7)*, **3*** (2004) 83–118.
[34] A. Perelli, A survey of the Selberg class of L-functions. I, *Milan J. Math.*, **73** (2005) 19–52.
[35] A. Selberg, Old and new conjectures and results about a class of Dirichlet series. In *Proceedings of the Amalfi Conference on Analytic Number Theory (Maiori, 1989)*, Univ. Salerno, Salerno, (1992) 367–385.
[36] J. Steuding, How many values can L-functions share? *Fiz. Mat. Fak. Moksl. Semin. Darb.*, **7** (2004) 70–81.
[37] J. Steuding, Value-distribution of L-functions, *Lecture Notes in Mathematics*, Springer, Berlin, **1877** (2007).
[38] S. M. Voronin, The distribution of the nonzero values of the Riemann ζ-function, *Trudy Mat. Inst. Steklov.*, **128** 260 (1972) 131–150. Collection of articles dedicated to Academician Ivan Matveevič Vinogradov on his eightieth birthday. II.
[39] S. M. Voronin, A theorem on the "universality" of the Riemann zeta-function, *Izv. Akad. Nauk SSSR Ser. Mat.*, **39(3)** 703 (1975) 475–486.
[40] R. Šleževičienė, The joint universality for twists of Dirichlet series with multiplicative coefficients by characters. In *Analytic and probabilistic methods in number theory (Palanga, 2001)*, TEV, Vilnius, (2002) 303–319.

Topics in Number Theory, RMS-Lecture Notes Series No. 26, 2020, pp. 43–50.

Nonvanishing of Symmetric Square L-Functions of Cusp Forms

Balesh Kumar

Department of Mathematics, Indian Institute of Technology Ropar, Rupnagar, Punjab 140 001, India.
e-mail: baleshkumar@iitrpr.ac.in, baleshmaths@gmail.com

Abstract. In this article, we prove nonvanishing results for symmetric square L-functions associated to primitive forms of integral weight on average (over an orthogonal basis of Hecke eigenforms) inside the critical strip. This extends a result of Kohnen and Sengupta to forms of level $D > 1$ (an odd fundamental discriminant) with real primitive character modulo D.

Keywords. Symmetric square L-functions, Nonvanishing.

2010 Subject Classification: 11F11, 11F66

1. Introduction

Let N be any positive integer and χ be a primitive Dirichlet character modulo N. We denote by $S_k(N, \chi)$ the space of cusp forms of weight k, level N and character χ. When $N = 1$, we denote the space by S_k. Given a normalised Hecke eigenform f in S_k, the L-function $L(f, s)$ associated to f has an analytic continuation to the whole complex plane and the completed L-function $L^*(f, s)$ satisfies the functional equation. More precisely, the functional equation of $L^*(f, s)$ relates its value at s to its value at $k - s$. The critical strip for such L-function is $(k-1)/2 < \Re(s) < (k+1)/2$. One of the classical problem regarding L-functions is to understand the nonvanishing in the critical strip and the knowledge about the existence of zero-free region is a question of great interest.

The Generalised Riemann Hypothesis (GRH) predicts that any zero of $L(f, s)$ in the critical strip actually lies on the critical line $\Re(s) = k/2$. For a given L-function $L(f, s)$, the GRH is an open problem. However, one naturally asks the above question on an average (over an orthogonal basis of Hecke eigenforms). In this direction, the nonvanishing of the average of L-functions inside the critical strip is due to Kohnen [6]. It is worth noting that the work of Kohnen [6] has been generalised to various L-functions associated to other types of modular forms: L-functions associated to normalised Hecke eigenforms with arbitrary level and primitive character with respect to both the level and weight aspect by Raghuram [9], L-functions of cusp forms twisted by primitive Dirichlet character by Schwagenscheidt [11], L-functions of half-integral weight cusp forms by Ramakrishnan and Shankhadhar [10], Koecher-Maass series of Siegel cusp forms by

Das and Kohnen [4], L-functions of half-integral weight cusp forms in the plus space by Kohnen and Raji [8] and L-functions associated to Hilbert cusp forms by Hamieh and Raji [5].

Given a normalised Hecke eigenform f in $S_k(N,\chi)$, one can define various L-functions associated to f. The most commonly used L-function of degree 3 is symmetric square L-function $L(\mathrm{sym}^2 f, s)$. The aim of this article is to study the nonvanishing of $L(\mathrm{sym}^2 f, s)$ inside the critical strip. Before we state our theorems, we fix the following notations.

Let $D > 1$, $D \equiv 1 \pmod 4$ be a square-free integer, and $\chi_D = \left(\frac{D}{\cdot}\right)$ a real primitive character modulo D and $k > 2$ an even integer. Since χ_D is primitive, we see that the space $S_k(D,\chi_D)$ is the full space of newforms. Therefore, we can choose an orthogonal basis of $S_k(D,\chi_D)$, denoted by $H_k(D,\chi_D)$ which consists of normalised Hecke eigenforms for all Hecke operators. Let $f \in H_k(D,\chi_D)$ be a form with the Fourier expansion

$$f(z) = \sum_{n=1}^{\infty} \lambda_f(n) e^{2\pi i n z}.$$

For $\Re(s) > 1$, the symmetric square L-function associated to f is given by

$$L(\mathrm{sym}^2 f, s) = \prod_p (1-\alpha_p^2 p^{-s})^{-1}(1-\chi_D(p)\alpha_p\bar{\alpha}_p p^{-s})^{-1}(1-\bar{\alpha}_p^2 p^{-s})^{-1},$$

where the product runs over all primes and α_p, $\bar{\alpha}_p$ are defined by

$$\alpha_p + \chi_D(p)\bar{\alpha}_p = \lambda_f(p), \quad \alpha_p\bar{\alpha}_p = p^{k-1}.$$

By the works of Shimura [12], Asai [3, p. 58, Corollary], the completed function (after using the Legendre's duplication formula for Gamma functions in [3, p. 58])

$$\Lambda(\mathrm{sym}^2 f, s) = D^{s/2} 2^{-s} \pi^{-3s/2} \Gamma(s) \Gamma\left(\frac{s-k+2}{2}\right) L(\mathrm{sym}^2 f, s) \tag{1}$$

can be analytically continued to the whole complex plane and satisfies the functional equation

$$\Lambda(\mathrm{sym}^2 f, s) = \Lambda(\mathrm{sym}^2 f, 2k-1-s). \tag{2}$$

In [7], Kohnen and Sengupta has obtained the nonvanishing of $L(\mathrm{sym}^2 f, s)$ associated to a normalised Hecke eigenform of *level one* in the critical region. By using the methods of Kohnen and Sengupta, we prove the following theorem.

Theorem 1. *Let $D > 1$ be an odd fundamental discriminant and t_0 be a real number and $0 < \epsilon < \frac{1}{2}$. Then there exists a positive constant $C_1 = C_1(t_0, \epsilon)$ depending only on t_0 and ϵ such that for $k > C_1$, the function*

$$\sum_{f \in H_k(D,\chi_D)} \frac{1}{\langle f, f\rangle} \Lambda(sym^2 f, s)$$

does not vanish at any point $s = \sigma + it_0$, $k-1 < \sigma < k - \frac{1}{2} - \epsilon$, $k - \frac{1}{2} + \epsilon < \sigma < k$.

We also prove the following theorem which is an analogue of Sun's result [13, Corollary 1.2] where the nonvanishing of $L(\mathrm{sym}^2 f, s)$ for the level aspect on the critical line is obtained. However, we deduce the nonvanishing of $L(\mathrm{sym}^2 f, s)$ in the critical region but off the critical line.

Theorem 2. *Let $k > 6$ be an even integer and t_0 be a real number and $0 < \epsilon < \frac{1}{2}$. Then there exists a positive constant $C_2 = C_2(k, t_0, \epsilon)$ depending only on k, t_0 and ϵ such that for D an odd fundamental discriminant with $D > C_2$, the function*

$$\sum_{f \in H_k(D,\chi_D)} \frac{1}{\langle f, f\rangle} \Lambda(sym^2 f, s)$$

does not vanish at any point $s = \sigma + it_0$, $k-1 < \sigma < k - \frac{1}{2} - \epsilon$, $k - \frac{1}{2} + \epsilon < \sigma < k$.

As a consequence of Theorem 1 and 2, we deduce the following corollary on the nonvanishing of $L(\mathrm{sym}^2 f, s)$ in the critical region with respect to the weight and level aspect.

Corollary 3. *Let $s = \sigma + it$ be a complex number fixed with $k - 1 < \sigma < k$, $\sigma \neq \frac{k}{2}$. If either weight k or level D is large enough where $D > 1$ runs over odd fundamental discriminants then there exists a normalised Hecke eigenform $f \in H_k(D, \chi_D)$ such that $\Lambda(sym^2 f, s) \neq 0$.*

In order to prove the above theorems, we basically use Zagier's kernel and certain analytic estimates. In the next section, we describe kernel function for $L(\mathrm{sym}^2 f, s)$ obtained by Zagier [14]. Then in the subsequent sections, we prove the theorems.

2. The kernel function for $L(\mathrm{sym}^2 f, s)$

In [14, Theorem 4, p. 153], Zagier constructed the kernel function for $L(\mathrm{sym}^2 f, s)$, where f is a normalised Hecke eigenform in $S_k(D, \chi_D)$ with $D > 1$ an odd fundamental discriminant of a real quadratic field. To state the kernel function of $L(\mathrm{sym}^2 f, s)$, we need to define few notations.

Let Δ be a discriminant, that is, $\Delta \equiv 0, 1 \pmod 4$. If $\Delta \neq 0$ then we write $\Delta = D_0 f^2$ with $f \in \mathbb{N}$ and D_0 is the discriminant of $\mathbb{Q}(\sqrt{\Delta})$. For $\Re(s) > 1$, we denote by $L_{D_0}(s)$ the associated L-function defined by analytic continuation of the series $\sum_{n\geq 1} \left(\frac{D_0}{n}\right) n^{-s}$, where $\left(\frac{D_0}{\cdot}\right)$ is the Kronecker symbol. For $\Re(s) > 1$, we put

$$L(s, \Delta) = \begin{cases} \zeta(2s-1) & \text{if } \Delta = 0, \\ L_{D_0}(s) \sum_{d \mid f, d>0} \mu(d) \left(\frac{D_0}{d}\right) d^{-s} \sigma_{1-2s}\left(\frac{f}{d}\right) & \text{if } \Delta \neq 0, \end{cases}$$

where μ is the Möbius function and for $m \in \mathbb{N}$, $\nu \in \mathbb{C}$, we have $\sigma_\nu(m) = \sum_{d\mid f, d>0} d^\nu$.

Furthermore, for an integer t with $\Delta < t^2$ and $s \in \mathbb{C}$ with $1/2 < \Re(s) < k$, we define

$$I_k(\Delta, t; s) = \frac{\Gamma\left(k - \frac{1}{2}\right)\Gamma(1/2)}{\Gamma(k)} \int_0^\infty \frac{y^{k+s-2}}{\left(y^2 + ity - \frac{1}{4}\Delta\right)^{k-1/2}} dy$$

where the above integral converges absolutely for $1-k < \Re(s) < k$ if $\Delta \neq 0$. For $\Delta = 0$, $\pm t > 0$ one has

$$I_k(0,t;s) = e^{\operatorname{sign} t \cdot \frac{\pi i}{2}(s-k)} \sqrt{\pi}\,\frac{\Gamma(s-1/2)\Gamma(k-s)}{\Gamma(k)}|t|^{s-k}. \tag{3}$$

For the above function and its detailed properties, we refer to [14, Proposition 4, p. 132]. Now we state Zagier's kernel function for $L(\mathrm{sym}^2 f, s)$.

Theorem 4 (Zagier). *Let* $D \equiv 1 \pmod 4$*,* $D > 1$*, be a square-free integer and* $k > 2$ *an even integer. For* $m = 1, 2, \ldots$ *and* $2-k < \Re(s) < k-1$*, set*

$$\begin{aligned} c_{m,D}(s) &= m^{k-1} D^{\frac{1}{2}-s} \sum_{\substack{t\in\mathbb{Z} \\ t^2 \equiv 4m \pmod D}} (I_k(t^2-4m, t; s) + I_k(t^2-4m, -t; s)) L\left(s, \frac{t^2-4m}{D}\right) \\ &+ \begin{cases} (-1)^{k/2} \frac{\Gamma(s+k-1)\zeta(2s)}{2^{2s+k-3}\pi^{s-1}\Gamma(k)} u^{k-s-1} & \text{if } m = u^2,\ u > 0, \\ 0 & \text{if } m \text{ is not a perfect square.} \end{cases} \end{aligned} \tag{4}$$

Then the function

$$\phi_{s,D}(z) = \sum_{m=1}^{\infty} c_{m,D}(s) e^{2\pi i m z}$$

is a cusp form on $\Gamma_0(D)$ *of weight* k *and character* χ_D*. Furthermore, for a normalised Hecke eigenform* f *in* $S_k(D, \chi_D)$*, we have*

$$\langle \phi_{s,D}, f\rangle = C_k \frac{\Gamma(s+k-1)}{(4\pi)^{s+k-1}} L(sym^2 f, s+k-1)$$

where $C_k = \frac{(-1)^{k/2}\pi}{2^{k-3}(k-1)}$.

3. Proof of Theorem 1 and 2

The proof of both the theorems are essentially based on the same line of arguments as Kohnen and Sengupta [7] and differ from each other in the last step. Before going into the steps of the proof, we briefly explain the idea behind the proof. We first write the kernel function for $\Lambda(\mathrm{sym}^2 f, s)$ in terms of the basis element in $H_k(D, \chi_D)$, for suitable values of s. Then by comparing the first Fourier coefficients on both the sides, we get an identity for the average of L-functions $\Lambda(\mathrm{sym}^2 f, s)$. Next we proceed the proof by the method of contradiction. We assume, on the contrary, the average of L-functions vanishes at some point in the critical region but off the critical line. Then using certain analytic estimates of the terms involved in the identity and asymptotics for the ratio of Gamma functions, we derive a contradiction as the weight k is sufficiently large. Now we give the detailed proof.

By Theorem 4, we see that

$$\langle \phi_{s,D}, f\rangle = \frac{C_k}{D^{s+k-1}} \frac{\pi^{\frac{1}{2}(s+k-1)}}{2^{s+k-1}\Gamma\left(\frac{s+1}{2}\right)} \Lambda(\mathrm{sym}^2 f, s+k-1).$$

Again, by Theorem 4, we know that $\phi_{s,D}$ is a cusp form in $S_k(D, \chi_D)$, for $2-k < \Re(s) < k-1$. Therefore, writing $\phi_{s,D}$ in terms of the basis elements in $H_k(D, \chi_D)$, we get

$$\phi_{s,D}(z) = \frac{C_k}{D^{s+k-1}} \frac{\pi^{\frac{1}{2}(s+k-1)}}{2^{s+k-1}\Gamma\left(\frac{s+1}{2}\right)} \sum_{f\in H_k(D,\chi_D)} \frac{\Lambda(\mathrm{sym}^2 f, s+k-1)}{\langle f, f\rangle} f(z).$$

Comparing the first Fourier coefficients on both the sides, we get

$$c_{1,D}(s) = \frac{C_k}{D^{s+k-1}} \frac{\pi^{\frac{1}{2}(s+k-1)}}{2^{s+k-1}\Gamma(\frac{s+1}{2})} \sum_{f\in H_k(D,\chi_D)} \frac{1}{\langle f, f\rangle} \Lambda(\mathrm{sym}^2 f, s+k-1), \qquad (5)$$

for $2-k < \Re(s) < k-1$. By using the functional equation (2), it suffices to prove the theorem in the region $k-\frac{1}{2}+\epsilon < \sigma < k$. Suppose that the right-hand side of (5) vanishes at $s = \frac{1}{2}+\delta+it_0$ where $\epsilon < \delta < \frac{1}{2}$. Then from the definition of $c_{1,D}(s)$, we obtain

$$D^{-\delta-it_0} \sum_{\substack{t\in\mathbb{Z}\\ t^2\equiv 4 \pmod D}} \left(I_k\left((t^2-4, t; \frac{1}{2}+\delta+it_0\right) + I_k\left((t^2-4, -t; \frac{1}{2}+\delta+it_0\right)\right)$$
$$\times L\left(\frac{1}{2}+\delta+it_0, \frac{t^2-4}{D}\right) + (-1)^{k/2} \frac{\Gamma\left(k-\frac{1}{2}+\delta+it_0\right)\zeta(1+2\delta+2it_0)}{2^{k-2+2\delta+2it_0}\pi^{-\frac{1}{2}+\delta+it_0}\Gamma(k)} = 0.$$

The above identity can also be written as

$$\frac{(-1)^{\frac{k}{2}-1}2^k\Gamma(k)}{\Gamma\left(k-\frac{1}{2}+\delta+it_0\right)} D^{-\delta-it_0}$$
$$\times \sum_{\substack{t\in\mathbb{Z}\\ t^2\equiv 4 \pmod D}} \left(I_k\left(t^2-4, t; \frac{1}{2}+\delta+it_0\right) + I_k\left(t^2-4, -t; \frac{1}{2}+\delta+it_0\right)\right)$$
$$\cdot L\left(\frac{1}{2}+\delta+it_0, \frac{t^2-4}{D}\right) = \frac{\zeta(1+2\delta+2it_0)}{2^{2\delta-2+2it_0}\pi^{-\frac{1}{2}+\delta+it_0}}. \qquad (6)$$

Note that the right-hand side of (6) does not depend on k and D and is never zero for $\epsilon \le \delta \le \frac{1}{2}$. We will show that the left-hand side of (6) goes to zero uniformly for $\epsilon < \delta < \frac{1}{2}$ as weight k or level D tends to infinity, which gives a contradiction.

In order to do this, we find suitable bounds for the summands in left-hand side of (6). We need to consider the cases $t = \pm 2$ and $\pm t \ge 3$ separately because of the variation of the definition of $I_k(\Delta, t; s)$ and $L(s, \Delta)$ that depends on wheather $\Delta = 0$ or $\Delta \neq 0$.

For $t = \pm 2$, by Equation (3) and the estimate of [7, p. 1645, Equation (8)], we have

$$\begin{aligned} 2&\left(I_k\left(0, 2; \frac{1}{2} + \delta + it_0\right) + I_k\left(0, -2; \frac{1}{2} + \delta + it_0\right)\right) \\ &= 2\left(e^{\frac{\pi i}{2}\left(\frac{1}{2} - k + \delta + it_0\right)} + e^{-\frac{\pi i}{2}\left(\frac{1}{2} - k + \delta + it_0\right)}\right)\sqrt{\pi} \\ &\cdot \frac{\Gamma(\delta + it_0)\Gamma(k - 1/2 - \delta - it_0)}{\Gamma(k)} 2^{-k+1/2+\delta+it_0} \\ &\ll_{t_0,\epsilon} \frac{\left|\Gamma\left(k - \frac{1}{2} - \delta - it_0\right)\right|}{2^k \Gamma(k)}, \end{aligned} \tag{7}$$

where the implied constant in $\ll_{t_0,\epsilon}$ depends only on t_0 and ϵ. For $\pm t \geq 3$, by Equation (7) of [7, p. 1645], we get

$$\begin{aligned} &\left(I_k\left(t^2 - 4, t; \frac{1}{2} + \delta + it_0\right) + I_k\left(t^2 - 4, -t; \frac{1}{2} + \delta + it_0\right)\right) \\ &\ll_{t_0} (t^2 - 4)^{-\frac{1}{4} + \frac{\delta}{2}} \left(\frac{|t| - \sqrt{t^2 - 4}}{|t| + \sqrt{t^2 - 4}}\right)^{\frac{k-1}{2}} \\ &\cdot \frac{\left|\Gamma\left(k - \frac{1}{2} + \delta + it_0\right)\Gamma\left(k - \frac{1}{2} - \delta - it_0\right)\right|}{2^k \Gamma(k)^2}. \end{aligned} \tag{8}$$

Now, we obtain the estimates for $L\left(\frac{1}{2} + \delta + it_0, \frac{t^2-4}{D}\right)$ on the left-hand side of (6). For $|t| = 2$, we have by definition

$$L\left(\frac{1}{2} + \delta + it_0, 0\right) = \zeta(2\delta + 2it_0)$$

which is a continuous function in the range $\epsilon \leq \delta \leq 1/2$ (provided $t_0 \neq 0$) and hence is bounded. If $t_0 = 0$, then we consider the function

$$2i^k \cos\left(\frac{\pi}{2}\left(\frac{1}{2} + \delta + it_0\right)\right) \cdot \zeta(2\delta + 2it_0),$$

where

$$2i^k \cos\left(\frac{\pi}{2}\left(\frac{1}{2} + \delta + it_0\right)\right) = e^{\frac{\pi i}{2}\left(\frac{1}{2} - k + \delta + it_0\right)} + e^{-\frac{\pi i}{2}\left(\frac{1}{2} - k + \delta + it_0\right)}$$

is the second factor on the right hand side of Equation (7). The previous argument implies that the above function is also bounded for $\epsilon \leq \delta \leq 1/2$.

On the other hand, if $|t| \neq 2$, then for all $\delta \geq 0$ and all $\epsilon' > 0$, one has

$$L\left(\frac{1}{2} + \delta + it_0, \frac{t^2 - 4}{D}\right) \ll_{t_0,\epsilon'} \left|\frac{t^2 - 4}{D}\right|^{\frac{1}{2} + \epsilon'}. \tag{9}$$

which follows from [2, Chapter 12, Exercise 22(*b*)].

Since $D > 1$ is an odd fundamental discriminant, therefore for $t \in \mathbb{Z}$ with $|t| \le 2$, the congruence $t^2 \equiv 4 \pmod{D}$ has only solutions for $t = \pm 2$. Denote the left-hand side of (6) by L_{k,D,δ,t_0}. Then by using the bounds from (7), (8) and (9) (fixing any ϵ' in (9)) and the absolute bound for $L\left(\frac{1}{2} + \delta + it_0, 0\right)$, we deduce that

$$|L_{k,D,\delta,t_0}| \ll_{t_0,\epsilon} D^{-\delta} \frac{\left|\Gamma\left(k - \frac{1}{2} - \delta - it_0\right)\right|}{\left|\Gamma\left(k - \frac{1}{2} + \delta + it_0\right)\right|}$$

$$+ \frac{\left|\Gamma\left(k - \frac{1}{2} - \delta - it_0\right)\right|}{D^{\frac{1}{2}+\delta+\epsilon'}\Gamma(k)} \sum_{\substack{t \ge 3 \\ t^2 \equiv 4 \pmod{D}}} (t^2 - 4)^{\frac{1}{4}+\frac{\delta}{2}+\epsilon'} \left(\frac{|t| - \sqrt{t^2-4}}{|t| + \sqrt{t^2-4}}\right)^{\frac{k-1}{2}}.$$

Now we first show that the sum over $t \ge 3$ on the right hand side of the above converges for $k \ge 7$ and is bounded by an absolute constant independent of k. In fact, for $t \ge 3$, we have

$$t^2 - 4 \ge t^2 + \frac{9}{t^2} - 6 = \left(t - \frac{3}{t}\right)^2,$$

and hence

$$t - \sqrt{t^2-4} \le \frac{3}{t} \le 1, \quad \text{for } t \ge 3.$$

Moreover, for $t \ge 3$, we also have

$$t + \sqrt{t^2-4} \ge 2\sqrt{t^2-4} \quad \text{and } \sqrt{t^2-4} \ge \frac{t}{2}.$$

Thus, using the above elementary estimates, we have

$$\sum_{\substack{t \ge 3 \\ t^2 \equiv 4 \pmod{D}}} (t^2 - 4)^{\frac{1}{4}+\frac{\delta}{2}+\epsilon'} \left(\frac{|t| - \sqrt{t^2-4}}{|t| + \sqrt{t^2-4}}\right)^{\frac{k-1}{2}} \le \frac{1}{2^{1/2+\delta+2\epsilon'}} \sum_{t \ge 3} \left(\frac{1}{t}\right)^{k/2-1-\delta-2\epsilon'}.$$

The sum on the right hand side of the above converges absolutely for $k \ge 7$, $\epsilon' < \delta < 1/2$ and bounded by an absolute constant.

Using the fact that (see [1, 6.1.46])

$$\lim_{x \to \infty} x^{b-a} \frac{\Gamma(x+a)}{\Gamma(x+b)} = 1 \quad (a, b \in \mathbb{C}\backslash\mathbb{R}; x \to \infty)$$

and the explicit asymptotics of $x^{b-a}\frac{\Gamma(x+a)}{\Gamma(x+b)}$ for $x \to \infty$ given in [1, 6.1.47], we see that for Theorem 1, by fixing D, we obtain that $L_{k,D,\delta,t_0} \to 0$ uniformly in δ (since $\delta > \epsilon > 0$) as the weight k goes to infinity.

For Theorem 2, we fix the weight k and let the level $D \to \infty$ over odd fundamental discriminant, then also $L_{k,D,\delta,t_0} \to 0$. This proves the theorems. □

Acknowledgements

The author would like to thank the organizers for giving me an opportunity to talk in the conference "Number Theory: Arithmetic, Diophantine and Transcendence" jointly organised by IIT Ropar and IMSc, Chennai, India, on the occasion of 130th birthday of Srinivasa Ramanujan, during December 22–25, 2017 at IIT Ropar, India. We also thank Sanoli Gun and Purusottam Rath for the helpful discussions. The author thanks IMSc, Chennai for providing excellent working facilities during his Post Doctoral Fellow position. The author also thanks the referee for going through the article carefully and for many suggestion and comments which improves the presentation of the article.

References

[1] N. Abramowitz and I. Stegun, Handbook of mathematical functions, Dover, New York (1965).

[2] T. Apostal, Introduction to Analytic Number Theory, Springer, Berlin-Heidelberg-Newyork (1976).

[3] T. Asai, On the Fourier coefficients of automorphic forms at various cusps and some applications to Rankin's convolution, *J. Math. Soc. Japan*, **28** (1976), 48–61.

[4] S. Das and W. Kohnen, Nonvanishing of Koecher-Maass series attached to Siegel cusp forms, *Adv. Math.*, **281** (2015) 624–669.

[5] A. Hamieh and W. Raji, Non-vanishing of L-functions of Hilbert modular forms inside the critical strip, *Acta Arith.*, **185(4)** (2018) 333–346.

[6] W. Kohnen, Nonvanishing of Hecke L-functions associated to cusp forms inside the critical strip, *J. Number Theory*, **67(2)** (1997) 182–189.

[7] W. Kohnen and J. Sengupta, Nonvanishing of symmetric square L-functions of cusp forms inside the critical strip, *Proc. Amer. Math. Soc.*, **128(6)** (2000) 1641–1646.

[8] W. Kohnen and W. Raji, Nonvanishing of L-functions associated to cusp forms of half-integral weight in the plus space, *Res. Number Theory*, **3** (2017), Art. 6, pp. 8.

[9] A. Raghuram, Nonvanishing of L-functions of cusp forms inside the critical strip, Number theory, *Ramanujan Math. Soc. Lect. Notes Ser., Ramanujan Math. Soc.*, Mysore, **1** (2005) 97–105.

[10] B. Ramakrishnan and K. D. Shankhadhar, Nonvanishing of L-functions associated to cusp forms of half-integral weight. Automorphic forms, *Springer Proc. Math. Stat.*, Springer, Cham, **115** (2014) 223–231.

[11] M. Schwagenscheidt, Nonvanishing and central critical values of twisted L-functions of cusp forms on average, *Funct. Approx. Comment. Math.*, **55(1)** (2016) 45–58.

[12] G. Shimura, On the holomorphy of certain Dirichlet series, *Proc. London Math. Soc.*, **31** (1975) 79–98.

[13] Q. Sun, The symmetric-square L-function on the critical line, *J. Number Theory*, **140** (2014) 196–214.

[14] D. Zagier, Modular forms whose Fourier coefficients involve zeta-functions of quadratic fields, in: Modular Functions of One Variable VI, J.-P. Serre and D. Zagier (eds.), *Lecture Notes in Math.*, Springer, Berlin, **627** (1976) 105–169.

Simultaneous Sign Changes of Fourier Coefficients of Half-Integral Weight Newforms

Biplab Paul

Chennai Mathematical Institute, H1, SIPCOT IT Park, Siruseri, Kelambakkam 603 103, India.
e-mail: bpaul@cmi.ac.in

Abstract. Let f, g be distinct newforms of half-integral weights $k_1 + 1/2$ and $k_2 + 1/2$ having real Fourier coefficients $a_f(n)$ and $a_g(n)$ respectively. If $k_1 \neq k_2$, Gun, Kohnen and Rath [4] showed the existence of an infinite set S of primes p such that the sequence $\{a_f(tp^{2m})a_g(tp^{2m})\}_{m\in\mathbb{N}}$ changes sign infinitely often, where t is a square-free integer such that $a_f(t)a_g(t) \neq 0$. In this article, we remove the assumption $k_1 \neq k_2$ and show that the set S of primes has natural density one.

Keywords. Half-integral weight newform, sign changes of Fourier coefficients, Hecke eigenform, Sato-Tate distribution.

2010 Subject Classification: 11F30, 11F37

1. Introduction

Let N, k be positive integers and χ be a Dirichlet character $\bmod 4N$. Denote by $S_{k+1/2}(4N, \chi)$ the space of cusp forms of weight $k+1/2$ for the congruence subgroup $\Gamma_0(4N)$ with Nebentypus character χ. Also let $S^{\text{new}}_{k+1/2}(4N, \chi)$ be the subspace of newforms in the space $S_{k+1/2}(4N, \chi)$. For each $f \in S_{k+1/2}(4N, \chi)$, we have the Fourier expansion

$$f(z) := \sum_{n=1}^{\infty} a_f(n)q^n,$$

where $q := e^{2\pi iz}$ and z is in the complex upper half-plane $\mathcal{H} := \{z \in \mathbb{C} \mid \Im(z) > 0\}$. Owing to various reasons, when the Fourier coefficients $a_f(n)$ are real, the problems of sign change of the Fourier coefficients of integral and half-integral weight cusp forms have been studied by several mathematicians. For any two newforms $f \in S^{\text{new}}_{k_1+1/2}(4N_1, \chi_1)$ and $g \in S^{\text{new}}_{k_2+1/2}(4N_2, \chi_2)$ having real Fourier coefficients, in this article, we study the problem of sign changes of the sequence $\{a_f(m)a_g(m)\}_{m\in\mathbb{N}}$ when $f \neq g$. Throughout the article, $f \in S^{\text{new}}_{k+1/2}(4N, \chi)$ will be called a newform if it is an eigenfunction of all Hecke operators.

By a celebrated work of Shimura [17], one knows that for any square-free integer $t \in \mathbb{N}$, there exists a lifting from the space of cusp forms of half-integral weight $k + 1/2$ to the space of cusp forms of integer weight $2k$. This lift is determined by the Fourier coefficients $a_f(tn^2)$ of f for all $n \in \mathbb{N}$. Motivated by the study of sign changes of Fourier coefficients of integral weight cusp forms, Bruinier and Kohnen [2], assuming Chowla's conjecture, showed that the sequence $\{a_f(tm^2)\}_{m\in\mathbb{N}}$ changes sign infinitely often for a fixed square-free integer $t \in \mathbb{N}$ such that $a_f(t) \neq 0$. Later, Kohnen [8] made the above result unconditional. Further, for a Hecke eigenform $f \in S_{k+1/2}(4N, \chi)$ with χ real, Bruinier and Kohnen unconditionally showed that for all but finitely many primes p coprime to $4N$, the sequence $\{a_f(tp^m)\}_{m\in\mathbb{N}}$ changes sign infinitely often when $a_f(t) \neq 0$. The last result was generalized by Gun, Kohnen and Rath [4]. More precisely, they proved the following theorem.

Theorem 1 (Gun, Kohnen and Rath). *Let $N_1, N_2 \in \mathbb{N}$ be odd and square-free and $k_1, k_2 \geq 2$ be integers such that $k_1 \neq k_2$. Also let*

$$f(z) := \sum_{n\geq 1} a_f(n)q^n \in S^{\text{new}}_{k_1+1/2}(4N_1, \chi_1)$$

$$\text{and} \quad g(z) := \sum_{n\geq 1} a_g(n)q^n \in S^{\text{new}}_{k_2+1/2}(4N_2, \chi_2)$$

be distinct Hecke eigenforms where χ_1, χ_2 are real characters $\bmod 4N_1$ and $\bmod 4N_2$ respectively. Also assume that the Fourier coefficients $a_f(n), a_g(n) \in \mathbb{R}$ for all $n \in \mathbb{N}$ and there exists a square-free $t \in \mathbb{N}$ such that $a_f(t)a_g(t) \neq 0$. If S denotes the set of primes p such that the sequence $\{a_f(tp^{2m})a_g(tp^{2m})\}_{m\in\mathbb{N}}$ changes sign infinitely often, then the set S is infinite.

The proof of this theorem uses Rankin-Selberg theory, a classical theorem of Landau on the oscillation of the coefficients of a Dirichlet series having real coefficients and a result of D. Ramakrishnan [13]. Here we remove the condition $k_1 \neq k_2$ and show that the natural density of the set S of primes is one. More precisely, we have the following theorem.

Theorem 2. *Let $k_1, k_2 > 1$ be natural numbers, N_1, N_2 be odd square-free positive integers and χ_1, χ_2 be real characters modulo $4N_1$ and $4N_2$ respectively. Suppose that*

$$f(z) := \sum_{n\geq 1} a_f(n)q^n \in S^{\text{new}}_{k_1+1/2}(4N_1, \chi_1)$$

$$\text{and} \quad g(z) := \sum_{n\geq 1} a_g(n)q^n \in S^{\text{new}}_{k_2+1/2}(4N_2, \chi_2)$$

are distinct Hecke eigenforms. Also let the Fourier coefficients $a_f(n), a_g(n)$ be real for all $n \geq 1$ and there exists a square-free integer $t \in \mathbb{N}$ with $a_f(t)a_g(t) \neq 0$. If S denotes the set of primes p such that the sequence $\{a_f(tp^{2m})a_g(tp^{2m})\}_{m\in\mathbb{N}}$ changes sign infinitely often, then the set S has natural density one.

Remark 1.1. Theorem 2 can be proved for newforms lying in Kohnen's plus space. The proof will be similar to that of Theorem 2.

In order to prove Theorem 2, we follow the method of Gun, Kohnen and Rath [4]. To find the natural density of the set S of primes, we shall use a consequence of the joint Sato-Tate distributions of two distinct integral weight newforms.

This article is divided in three sections. In the next section, we shall list notations of the paper and recall some of the preliminaries. In the last section, we give the proof of the theorem.

2. Notation and Preliminaries

Throughout the paper, we use following notations. Unless otherwise stated p denotes a prime number. Let $\mathcal{P}$ be the set of all prime numbers. We say a subset A of $\mathcal{P}$ has natural density $d(A)$ if for any real number $x \geq 2$, we have

$$d(A) = \lim_{x\to\infty} \frac{\#\{p \leq x \mid p \in A\}}{\#\{p \leq x \mid p \in \mathcal{P}\}}.$$

We shall also use the following notion of uniform distribution frequently.

Definition 1 ([9, page 171]). *Let μ be a non-negative regular Borel measure on a compact Hausdorff space X such that $\mu(X) = 1$. A sequence $\{x_n\}_{n\in\mathbb{N}} \subset X$ is said to be μ-uniformly distributed in X if for any continuous function $f : X \to \mathbb{R}$, one has*

$$\lim_{N\to\infty} \frac{1}{N} \sum_{1\leq n\leq N} f(x_n) = \int_X f d\mu.$$

In order to prove the theorem stated in the introduction, we need the following classical theorem of Landau.

Theorem 3 (Landau). *Let $f(s) := \sum_{n=1}^{\infty} a(n)n^{-s}$ be a Dirichlet series such that $a(n) \geq 0$ for all $n \geq n_0$. Also assume that the abscissa of convergence σ_0 of the series $f(s)$ is finite. Then the function f has a singularity at $s = \sigma_0$.*

The proof of this theorem can be found in several books. For example, one can look at Montgomery and Vaughan [11, p. 16].

2.1 *Modular forms of integral weight*

Let k, N be positive integers and

$$\Gamma_0(N) := \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid c \equiv 0 \bmod N \right\}.$$

Also let $S_k(N)$ be the space of cusp forms of weight k for the congruence subgroup $\Gamma_0(N)$ and $S_k^{\mathrm{new}}(N)$ be the subspace of newforms of the space $S_k(N)$. Any $f \in S_k(N)$ has a Fourier expansion as follows:

$$f(z) := \sum_{n\geq 1} a_f(n)q^n. \tag{1}$$

For $f \in S_k(N)$ and a Dirichlet character χ mod D, one defines a function, denoted by $f \otimes \chi$, on the upper half-plane $\mathcal{H}$ as follows:

$$(f \otimes \chi)(z) := \sum_{n=1}^{\infty} a_f(n)\chi(n)q^n.$$

It is known [16, Proposition 3.64] that $f \otimes \chi$ is a cusp form of weight k for the congruence subgroup $\Gamma_0(ND^2)$ with the Nebentypus χ^2. In fact, by the work of Ribet [15, Theorem 3.9], one knows the following.

Theorem 4 (Ribet). *Let $N \in \mathbb{N}$ be a square-free and $f \in S_k^{\text{new}}(N)$ be a normalized Hecke eigenform. Let χ be a non-trivial Dirichlet character and*

$$g(z) := \sum_{n=1}^{\infty} a_g(n) q^n$$

be a newform such that $a_g(p) = a_f(p)\chi(p)$ for almost all $p \in \mathcal{P}$. Then the level of g is not square-free.

Now we introduce the notion of CM forms or forms having complex multiplication in the sense of Ribet [14].

Definition 2. *Let χ be a non-trivial Dirichlet character. Then a normalized Hecke eigenform $f \in S_k^{\text{new}}(N)$ is said to be a CM form or a form having complex multiplication by χ if*

$$a_f(p) = \chi(p) a_f(p)$$

for all primes $p \in \mathcal{P}$ in a set of primes of density one. Further, the form f is said to be a non-CM form or does not have complex multiplication if it is not a CM form.

Using Theorem 4, one can now conclude that there are no CM forms of square-free levels.

Let $f \in S_k^{\text{new}}(N)$ be a normalized Hecke eigenform with the Fourier expansion as in (1). Then we define

$$\lambda_f(n) := \frac{a_f(n)}{n^{(k-1)/2}}.$$

From the theory of Hecke operators, we have

$$\lambda_f(1) = 1 \quad \text{and} \quad \lambda_f(m)\lambda_f(n) = \sum_{\substack{d|(m,n),\\ (d,N)=1}} \lambda_f\left(\frac{mn}{d^2}\right).$$

Also by a celebrated work of Deligne, we have

$$|\lambda_f(n)| \le d(n) \quad \text{for all} \quad (n, N) = 1,$$

where $d(n)$ denotes the number of positive divisors of n. Thus for $(p, N) = 1$, one can write

$$\lambda_f(p) := 2\cos\theta_f(p) \quad \text{for} \quad 0 \le \theta_f(p) \le \pi.$$

If $f \in S_k^{\text{new}}(N)$ is a normalized Hecke eigenform which is a non-CM form, then the celebrated Sato-Tate conjecture predicts that the values of $\theta_f(p)$ is uniformly distributed in the interval $[0, \pi]$ with respect to the Sato-Tate measure $d\mu := (2/\pi)\sin^2\theta d\theta$. This is now a theorem due to the work of Barnet-Lamb, Geraghty, Harris and Taylor [1].

Sato-Tate conjecture can be generalized as follows: if f and g are two distinct newforms which are non-CM forms and neither of them is quadratic twist of other, then the sequence $\{(\theta_f(p), \theta_g(p))\}_{p\in\mathcal{P}}$ is uniformly distributed in $[0, \pi] \times [0, \pi]$ with respect to the product Sato-Tate measure $(4/\pi^2)\sin^2\theta \sin^2\beta d\theta d\beta$. As an application of the work of Harris [6] on joint Sato-Tate conjecture, one can derive the following theorem.

Theorem 5. *Let $f \in S_{k_1}^{\mathrm{new}}(N_1)$ and $g \in S_{k_2}^{\mathrm{new}}(N_2)$ be normalized Hecke eigenforms and at least one of f, g is a non-CM form. For any prime p with $(p, N_1N_2) = 1$, write*

$$\lambda_f(p) := 2\cos\theta_f(p) \quad \textit{and} \quad \lambda_g(p) := 2\cos\theta_g(p),$$

where $\theta_f(p), \theta_g(p) \in [0, \pi]$. For any fixed α, if

$$\limsup_{x\to\infty} \frac{\#\{p \le x \mid \theta_f(p) \pm \theta_g(p) = \alpha\}}{x/\log x} > 0,$$

then $f = g \otimes \chi$ for some Dirichlet character χ.

The above theorem has been proved in a recent joint work by Gun and the author [5].

2.2 *Modular forms of half-integral weight*

In this subsection, we shall recall the definition of half-integral weight modular forms and list some basic facts we shall use to prove Theorem 2. For more details see [7, 10, 17].

The theta function $\theta(z)$ is defined on the upper half plane $\mathcal{H}$ by

$$\theta(z) := 1 + 2\sum_{n=1}^{\infty} q^{n^2},$$

for any $z \in \mathcal{H}$ and $q := e^{2\pi i z}$. Since the theta function $\theta(z)$ does not vanish on $\mathcal{H}$, we can define the theta multiplier as follows: for any $\gamma \in \Gamma_0(4)$ and $z \in \mathcal{H}$, let

$$j(\gamma, z) := \frac{\theta(\gamma z)}{\theta(z)}.$$

It is known that

$$j(\gamma, z)^2 = \left(\frac{-1}{d}\right)(cz + d),$$

where $\gamma = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \Gamma_0(4)$. The symbol $\left(\frac{c}{d}\right)$ for $c, d \in \mathbb{Z}$ with $d \neq 0$ is as in [17]. With these notations in place, we are now ready to define half-integral weight modular forms.

Definition 3. *Let k and N be positive integers and χ be a Dirichlet character modulo $4N$. A holomorphic function $f(z)$ on the upper half plane $\mathcal{H}$ is called a* *half-integral weight modular form of weight* $k + 1/2$ *and with Nebentypus* χ *if it is holomorphic at the cusps of* $\Gamma_0(4N)$ *and satisfies*

$$f(\gamma z) = \chi(d) j(\gamma, z)^{2k+1} f(z)$$

for all $\gamma = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \Gamma_0(4N)$. *Further, if* f *vanishes at the cusps of* $\Gamma_0(4N)$, *then it is called a cusp form.*

For any positive integers k, N, let the space of all cusp forms of weight $k + 1/2$ and Nebentypus χ for the group $\Gamma_0(4N)$ be denoted by $S_{k+1/2}(4N, \chi)$. Any $f \in S_{k+1/2}(4N, \chi)$ has a Fourier expansion as follows:

$$f(z) := \sum_{n=1}^{\infty} a_f(n) q^n. \tag{2}$$

On the space $S_{k+1/2}(4N, \chi)$, the action of Hecke operators is given by:

$$f(z) \mid T(p^2, k, \chi)$$
$$:= \sum_{n=1}^{\infty} \left(a_f(p^2 n) + \chi^*(p) \left(\frac{n}{p}\right) p^{k-1} a_f(n) + \chi^*(p^2) p^{2k-1} a_f(n/p^2) \right) q^n,$$

where χ^* is the Dirichlet character defined by $\chi^*(n) := \left(\frac{(-1)^k}{n}\right) \chi(n)$ and $a_f(n/p^2) = 0$ if $p^2 \nmid n$. It is known that the space of cusp forms $S_{k+1/2}(4N, \chi)$ is stable under the action of the Hecke operators. We also need the following operator on the space of cusp forms of half-integral weight modular forms. For any integer $m \in \mathbb{N}$, one defines

$$\left(\sum_{n \geq 1} a(n) q^n \right) | U(m) := \sum_{n \geq 1} a(mn) q^n.$$

Definition 4. *A cusp form* $f \in S_{k+1/2}(4N, \chi)$ *is said to be a Hecke eigenform if it is an eigen function of* $T(p^2, k, \chi)$ *for all primes* p *with* $(p, 4N) = 1$.

We can now state the famous result of Shimura [17] which lifts half-integral weight cusp forms to integral weight cusp forms. More precisely, by the works of Shimura [17] and Niwa [12], one has the following theorem.

Theorem 6 (Shimura correspondence). *Let* $k, N \in \mathbb{N}$ *and* χ *be a Dirichlet character* $\bmod 4N$. *Also let* $f \in S_{k+1/2}(4N, \chi)$ *be a Hecke eigenform having the Fourier expansion as in* (2). *For any square-free integer* $t \in \mathbb{N}$, *define*

$$A_t(n) := \sum_{d \mid n} \chi_{t,N}(d) d^{k-1} a_f\left(\frac{n^2 t}{d^2}\right),$$

where $\chi_{t,N}$ *is a Dirichlet character defined by*

$$\chi_{t,N}(d) := \chi(d) \left(\frac{(-1)^k t}{d}\right). \tag{3}$$

Then the function F defined on the upper half-plane $\mathcal{H}$ by

$$F(z) := \sum_{n\geq 1} A_t(n)q^n$$

is a cusp form in $S_{2k}(2N, \chi^2)$ provided $k \geq 2$.

For any square-free odd integer $N \geq 1$ and any quadratic character $\chi \bmod N$, let $\chi(-1) = \epsilon$ and $\psi_1 := \left(\frac{4\epsilon}{\cdot}\right)\chi$. In [7], Kohnen defined a canonical subspace $S^+_{k+1/2}(4N, \psi_1)$ of the space of cusp forms $S_{k+1/2}(4N, \psi_1)$, as follows:

$$S^+_{k+1/2}(4N, \psi_1) := \left\{ f \in S_{k+1/2}(4N, \psi_1) \mid a_f(n) = 0 \text{ if } \epsilon(-1)^k n \equiv 2, 3 \bmod 4 \right\}.$$

The space $S^+_{k+1/2}(4N, \psi_1)$ is known as Kohnen's plus space. He studied the newforms theory in the space $S^+_{k+1/2}(4N, \psi_1)$. In particular, he defined the subspace of newforms $S^{+,\mathrm{new}}_{k+1/2}(4N, \psi_1) \subset S^+_{k+1/2}(4N, \psi_1)$ as follows: the subspace $S^{+,\mathrm{old}}_{k+1/2}(4N, \psi_1)$ of oldforms is defined by

$$S^{+,\mathrm{old}}_{k+1/2}(4N, \psi_1) := \sum_{d|N, d<N} \left[S^+_{k+1/2}(4d, \psi_1) + S^+_{k+1/2}(4d, \psi_1)|U(N^2/d^2) \right].$$

and define the subspace of newforms $S^{+,\mathrm{new}}_{k+1/2}(4N, \psi_1)$ to be the orthogonal complement of the subspace $S^{+,\mathrm{old}}_{k+1/2}(4N, \psi_1)$ of oldforms with respect to the Petersson inner product in the Kohnen plus space $S^+_{k+1/2}(4N, \psi_1)$. Recall that the Petersson inner product $\langle f, g\rangle$ of $f, g \in S_{k+1/2}(4N, \chi)$ is defined as

$$\langle f, g\rangle := \frac{1}{[\Gamma_0(4) : \Gamma_0(4N)]} \int_{\Gamma_0(4N)\backslash\mathcal{H}} f(z)\overline{g(z)} y^{k+1/2} \frac{dxdy}{y^2},$$

where $x := \Re(z)$, $y := \Im(z)$. The space $S^{+,\mathrm{new}}_{k+1/2}(4N, \psi_1)$ of newforms is known as Kohnen's newform space. He established the correspondence between the Kohnen's newform space and the newform space of integral weight cusp forms. More precisely, he proved the following.

Theorem 7 (Kohnen). *One has*

$$S^+_{k+1/2}(4N, \psi_1) = \oplus_{\substack{r,d\geq 1,\\ rd|N}} S^{+,\mathrm{new}}_{k+1/2}(4d, \psi_1)|U(r^2).$$

Further, the space $S^{+,\mathrm{new}}_{k+1/2}(4N, \psi_1)$ has a basis consists of eigenvectors of all the operators $T(p^2, N, \psi_1)$ for all $p \nmid N$ and $U(p^2)$ for all $p|N$. If $f \in S^{+,\mathrm{new}}_{k+1/2}(4N, \psi_1)$ is such that $f|T(p^2, N, \psi_1) = \lambda_f(p)f$ for all $p \nmid N$ and $f|U(p^2) = \lambda_f(p)f$, then there exists $F \in S^{\mathrm{new}}_{2k}(N)$ such that F is a Hecke eigenform having p-th eigenvalue $\lambda_f(p)$. Further, there is a finite linear combination of Shimura correspondence which is an isomorphism between $S^{+,\mathrm{new}}_{k+1/2}(4N, \psi_1)$ and $S^{\mathrm{new}}_{2k}(N)$ as Hecke modules.

For any odd square-free positive integer N and a quadratic character χ, Manickam, Ramakrishnan and Vasudevan [10], studied the theory of newforms of half-integral weight cusp forms. In particular, they defined the subspace of oldforms as follows:

$$S^{\mathrm{old}}_{k+1/2}(4N, \psi_1) := \sum_{d|N, d<N} \left[S_{k+1/2}(4d, \psi_1) + S_{k+1/2}(4d, \psi_1)|U(N^2/d^2)\right]$$
$$+ S^{+}_{k+1/2}(4N, \psi_1) + S^{+}_{k+1/2}(4N, \psi_1)|U(4).$$

Now define the subspace $S^{\mathrm{new}}_{k+1/2}(4N, \psi_1)$ of newforms as the orthogonal complement of the space $S^{\mathrm{old}}_{k+1/2}(4N, \psi_1)$ of oldforms with respect to the Petersson inner product in the space $S_{k+1/2}(4N, \psi_1)$. Then they proved the existence of an linear isomorphism between the space of newforms of half-integral weight and the space of newforms of integral weight as follows.

Theorem 8 (Manickam, Ramakrishnan and Vasudevan). *The space $S^{\mathrm{new}}_{k+1/2}$ $(4N, \psi_1)$ has a basis consists of eigenvectors of all the operators $T(p^2, N, \psi_1)$ for all $p \nmid N$ and $U(p^2)$ for all $p|N$. Further, the space $S^{\mathrm{new}}_{k+1/2}(4N, \psi_1)$ is isomorphic to the space $S^{\mathrm{new}}_{2k}(2N)$ under a suitable linear combination of Shimura lift. In particular, the image of half-integral weight newform in $S^{\mathrm{new}}_{k+1/2}(4N, \psi_1)$ is a newform in $S^{\mathrm{new}}_{2k}(2N)$ with the same set of eigenvalues.*

One can also define another canonical subspace similar to that of Kohnen's plus space of $S_{k+1/2}(4N)$ which maps to the space $S_{2k}(N)$ of cusp forms under original Shimura lift. For more details see Gun, Manickam and Ramakrishnan [3].

3. Proof of Theorem 2

Let $p \in \mathcal{P}$ be an odd prime such that $(p, N_1N_2) = 1$. Also let $\lambda_f(p)$ and $\lambda_g(p)$ be complex numbers such that

$$f(z)|T(p^2, N_1, \chi_1) = \lambda_f(p)f(z) \quad \text{and} \quad g(z)|T(p^2, N_2, \chi_2) = \lambda_g(p)g(z).$$

By Theorem 8, one knows that there exist newforms $F \in S^{\mathrm{new}}_{2k_1}(2N_1)$ and $G \in S^{\mathrm{new}}_{2k_2}(2N_2)$ such that F and G are the eigenfunctions for the Hecke operator $T(p)$ with eigenvalues $\lambda_f(p)$ and $\lambda_g(p)$ respectively. Since $F \in S^{\mathrm{new}}_{2k_1}(2N_1)$ and $G \in S^{\mathrm{new}}_{2k_2}(2N_2)$, hence $\lambda_f(p)$ and $\lambda_g(p)$ both are real. By hypothesis, $a_f(t)a_g(t) \neq 0$ for some square-free $t \in \mathbb{N}$. Now for any $s \in \mathbb{C}$ with $\Re(s) \gg 1$, by Shimura correspondence, we have

$$\sum_{m\geq 0} \frac{a_f(tp^{2m})}{p^{ms}} = a_f(t)\frac{1 - \chi_{t,N_1}(p)p^{k_1-1-s}}{1 - \lambda_f(p)p^{-s} + p^{2k_1-1-2s}}$$

$$\text{and} \quad \sum_{m\geq 0} \frac{a_g(tp^{2m})}{p^{ms}} = a_g(t)\frac{1 - \chi_{t,N_2}(p)p^{k_2-1-s}}{1 - \lambda_g(p)p^{-s} + p^{2k_2-1-2s}},$$

where χ_{t,N_1} and χ_{t,N_2} are as in (3). Write

$$1 - \lambda_f(p)p^{-s} + p^{2k_1-1-2s} = (1-\alpha_p p^{-s})(1-\overline{\alpha_p} p^{-s})$$
$$\text{and} \quad 1 - \lambda_g(p)p^{-s} + p^{2k_2-1-2s} = (1-\beta_p p^{-s})(1-\overline{\beta_p} p^{-s}),$$

where

$$\alpha_p + \overline{\alpha_p} = \lambda_f(p),\ \beta_p + \overline{\beta_p} = \lambda_g(p) \quad \text{and} \quad \alpha_p\overline{\alpha_p} = p^{2k_1-1},\ \beta_p\overline{\beta_p} = p^{2k_2-1}. \tag{4}$$

Now consider the Dirichlet series

$$D_p(s) := \sum_{m\geq 0} \frac{a_f(tp^{2m})a_g(tp^{2m})}{p^{ms}}.$$

Using partial fractions, we have

$$D_p(s) = \frac{a_f(t)a_g(t)H(p^{-s})}{(1-\alpha_p\beta_p p^{-s})(1-\alpha_p\overline{\beta_p}p^{-s})(1-\overline{\alpha}_p\beta_p p^{-s})(1-\overline{\alpha}_p\overline{\beta}_p p^{-s})},$$

where H is a polynomial of degree ≤ 3. Hence $D_p(s)$ has poles. Consider the set

$$X := \{p \in \mathcal{P} \mid (p, 2N_1N_2) = 1, \alpha_p\beta_p \notin \mathbb{R} \text{ and } \alpha_p\overline{\beta}_p \notin \mathbb{R}\}. \tag{5}$$

If $p \in X$ then by Theorem 3, the sequence $\{a_f(tp^{2m})a_g(tp^{2m})\}_{m\in\mathbb{N}}$ changes sign infinitely often. Now, recall that S is the set of primes p such that the sequence $\{a_f(tp^{2m})a_g(tp^{2m})\}_{m\in\mathbb{N}}$ changes sign infinitely often. Hence X is a subset of S. Since the expressions involving α_p and β_p in (4) and (5) are symmetric with respect to complex conjugation, without loss of generality we can write $\alpha_p = p^{k_1-1/2}e^{i\theta_f(p)}$ and $\beta_p = p^{k_2-1/2}e^{i\theta_g(p)}$ with $0 \leq \theta_f(p), \theta_g(p) \leq \pi$. Now observe that $\alpha_p\beta_p \in \mathbb{R}$ precisely when $\theta_f(p) + \theta_g(p) = m\pi$ for $m = 0, 1, 2$. Similarly, $\alpha_p\overline{\beta}_p \in \mathbb{R}$ if and only if $\theta_f(p) - \theta_g(p) = l\pi$ for $l = -1, 0, 1$ respectively. Thus we have

$$X = \{p \in \mathcal{P} \mid (p, 2N_1N_2) = 1, \theta_f(p) + \theta_g(p) \neq m\pi,$$
$$m = 0, 1, 2 \quad \text{and} \quad \theta_f(p) - \theta_g(p) \neq l\pi, l = -1, 0, 1\}.$$

By (4), we have $\lambda_F(p) := \lambda_f(p)/p^{k_1-1/2} = 2\cos\theta_f(p)$ and $\lambda_G(p) := \lambda_g(p)/p^{k_2-1/2} = 2\cos\theta_g(p)$. Since N_1, N_2 are square-free by Theorem 4, we conclude that neither F nor G is a twist of other. Now we use Theorem 5 to conclude that the natural density of the set X is 1. Hence the set S has natural density 1. This completes the proof. □

Acknowledgements

The author would like to thank Sanoli Gun for some useful discussions and her continuous encouragement. The author would also like to thank the referee for his/her comments on an earlier version which improved the readability of the paper.

References

[1] 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** no. 1, (2011) 29–98.

[2] J. H. Bruinier and W. Kohnen, Sign changes of coefficients of half-integral weight modular forms, *In: Modular forms on Schiermonnikoong* (eds. B. Edixhoven et al.), 57–66, Cambridge Univ. Press (2008).

[3] S. Gun, M. Manickam and B. Ramakrishnan, A canonical subspace of modular forms of half-integral weight, *Math. Ann.*, **347** (2010) 899–916.

[4] S. Gun, W. Kohnen and P. Rath, Simultaneous sign change of Fourier-coefficients of two cusp forms, *Arch. Math. (Basel)* **105** no. 5, (2015) 413–424.

[5] S. Gun and B. Paul, Sign changes of Fourier coefficients of newforms and multiplicity one theorem, Submitted.

[6] M. Harris, Galois representations, automorphic forms, and the Sato-Tate conjecture, *Indian J. Pure Appl. Math.*, **45** no. 5, (2014) 707–746.

[7] W. Kohnen, Newforms of half-integral weight, *J. Reine Angew. Math.*, **333** (1982) 32–72.

[8] W. Kohnen, A short note on Fourier coefficients of half-integral weight modular forms, *Int. J. Number Theory*, **6** no. 6, (2010) 1255–1259.

[9] L. Kuipers and H. Niederreiter, Uniform Distribution of Sequences, Wiley, New York (1974).

[10] M. Manickam, B. Ramakrishnan and T. C. Vasudevan, On the theory of newforms of half-integral weight, *J. Number Theory*, **34** (1990) 210–224.

[11] H. Montgomery and R. Vaughan, Multiplicative number theory I. Classical theory, *Cambridge Studies in Advanced Mathematics*, Cambridge University Press, Cambridge, **97** (2007).

[12] S. Niwa, Modular forms of half-integral weight and the integral of certain theta functions, *Nagoya Math. J.*, **56** (1975) 147–161.

[13] D. Ramakrishnan, Recovering modular forms from squares, Appendix of A problem of Linnik for elliptic curves and mean-value estimates for automorphic representations by W. Duke and E. Kowalski, *Invent. Math.*, **139** (2000) 29–39.

[14] K. A. Ribet, Galois representations attached to eigenforms with Nebentypus, In: Modular functions of one variable, V (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976), *Lecture Notes in Math.*, Springer, Berlin, **601** (1977) 17–51.

[15] K. A. Ribet, Twists of modular forms and endomorphisms of abelian varieties, *Math. Ann.*, **253** no. 1, (1980) 43–62.

[16] G. Shimura, Introduction to the arithmetic theory of Automorphic forms, Publications of the Mathematical Society of Japan, No. 11. Princeton University Press, Princeton, N.J., (1971).

[17] G. Shimura, On modular forms of half integral weight, *Ann. of Math (2)*, **97** (1973) 440–481.

Topics in Number Theory, RMS-Lecture Notes Series No. 26, 2020, pp. 61–70.

Kaprekar Phenomena

Dinesh S. Thakur

Department of Mathematics, University of Rochester, Rochester, NY 14627, USA.
e-mail: dinesh.thakur@rochester.edu

Abstract. We generalize results of D. Kaprekar, H. Hasse and G. Prichett from 3 and 4 digits (with base 10 or general base respectively), to 5, 7, 9 digit numbers (in any base) characterizing all Kaprekar constants in these cases. For a fixed base, and any number of digits, we reduce the infinite computation needed, a priori, to a finite effective computation. We also give several other results and conjectures for general bases and digits, and mention some interesting open questions.

Keywords. Kaprekar constant, dynamical system, digit expansions, discrete

Dedicated to the memory of my father.

1. Introduction

D. R. Kaprekar (1905–1986), after his BA in 1929 from University of Bombay, worked as a school-teacher in Maharashtra, India. He loved numbers and in addition to the typical fascination with primes, factorizations, identities, he was also fascinated by (decimal) digit expansions, digit sums, palindromes, reversal symmetries etc.

When Srinivasan, who knew Hardy-Ramanujan's famous 'taxi-cab number' story of $1729 = 12^3 + 1^3 = 10^3 + 9^3$, tested him by asking what he sees in 1729, his reply was that it is $19 * 91$, 19 is its sum of digits and also its first-last digits, and from its digits, you get primes 17, 71; 79, 97.

He made several discoveries. The one beautiful discovery [K49, K55] from 1946 (see [D08]) related to this paper is that any number of four (decimal) digits, not all the same, will lead to 6174 (now called the Kaprekar constant), after (at most 7) repetitions [K55] of the (Kaprekar) process of 'Order, Reverse and Subtract'.

For example, 0132 leads first to $3210 - 0123 = 3087$, then to $8730 - 0378 = 8352$ and then to $8532 - 2358 = 6174$.

To explore how rare this beautiful phenomenon is among the infinite number of scenarios that you get, as you change the base and the number of digits, various authors [T72, ES88, DG04, M17] studied such systems, which are really (infinitely many) finite dynamical systems. It was shown that for decimals (i.e., base 10), for 3 digits, the constant is 495, and there is no such behavior in any other (than 3 and 4) number of digits, but sometimes weaker behavior with longer cycles, or sometimes with more or no fixed points. In other direction, Helmut Hasse and Gordon Prichett [HP78] explored 4 digit numbers for any base. We recall their results below.

In this article, we generalize these results (to different kind of results) for 5, 7, 9 digit numbers. It is interesting to note that Hasse-Prichett or Jordan paper has no citations listed on Math Sci Net, so only much later after announcing these results at the December 2017 conference, the author found out that [P78] had already settled the 5 digit case. In contrast to the 3, 4, 5 digit cases, where infinitely many bases (arithmetically, exponentially, arithmetically distributed (eventually) respectively) exhibit Kaprekar phenomena, in the 7 or 9 digit cases, only one base (each) has this property.

In this article, we explore any base and number of digits, giving a complete answer for 5, 7, 9 digits (see Section 4), and various partial results and guesses (see Section 5) in general situation, reducing the 'fixed base, any number of digits' case to a finite effective computation.

2. Notation and Basic dynamics of Kaprekar process

2.1 *Fixed digit expansions*

We fix a base $B > 1$ and number of digits $D > 1$, and look at all non-negative integers n of D digits (where we allow leading zeros) in base B. We write $n = \sum_{i=0}^{D-1} n_i B^i$ $(0 \leq n_i < B)$ also as $[n_{D-1}, \ldots, n_0]$, or even sometimes by dropping brackets and commas. We also use the short-form $(a)_k$ for the digit a repeated k times. We write $S = S_{(B,D)}$ for the set of all B^D numbers of D digits in base B, and $\overline{S}$ for the subset of $B^D - B$ numbers, with all digits not the same.

2.2 *Kaprekar process*

Given such n, let $\overrightarrow{n}$ (respectively $\overleftarrow{n}$) be the number obtained by arranging the digits of n in descending (respectively ascending) order, so that Kaprekar process $\kappa : S \to S$ leads from n to $\kappa(n) := \overrightarrow{n} - \overleftarrow{n}$, we denote its result by $n \Rightarrow \kappa(n)$.

2.3 *Examples*

For $(B, D) = (10, 4)$, $\kappa(0132) = 3087$, $\kappa(6174) = 6174$, the fixed point for κ. Kaprekar's result says that the 7-th iteration of κ applied to any n of 4 digits, not all the same, is $\kappa^{(7)}(n) = 6174$.

2.4 *Fixed points*

Since numbers with all digits the same get mapped to zero by κ, we ignore this trivial fixed point zero of κ. We will see below that for $D > 2$, κ restricts to $\overline{S} \to \overline{S}$. By $FP(B, D)$ we denote the set of nonzero fixed points of κ.

2.5 *Kaprekar constants*

We say that (B, D) is Kaprekar tuple (showing Kaprekar phenomena), with Kaprekar constant $K(B, D) \in FP(B, D)$, if every element $n \in \overline{S}$ is mapped to $K(B, D)$ after some number of iterations of κ.

Since $\overline{S}$ is a finite set, every element eventually enters some cycle under iterations of κ. We see that the tuple is Kaprekar, exactly when there is a unique cycle (which means all the elements in $\overline{S}$ reach the same cycle eventually) which is (the unique) fixed point. Thus, if $FP(B, D)$ is empty, or has more than one element, or if there is a cycle of length more than one, (B, D) cannot be Kaprekar.

2.6 *Remarks on effectivity and size reductions*

For a fixed (B, D) the problem is, of course, finite and effective, though computationally expensive. One has to check $B^D - B$ numbers a priori, much less, in fact, as the order of digits of the initial number is unimportant. But right after the first application of κ, the answer only depends on about $D/2$ ordered differences which are monotonically decreasing, as we will see below, thus getting about square-root reduction. This size is still huge for B, D of moderate size, because of the exponential nature of these simple bounds.

2.7 *Differences and subtraction possibilities*

Let $D = 2n$ or $2n + 1$. Let $\overrightarrow{N} = [a_1, \dots a_D] \in \overline{S}$, and consider differences $d_i = a_i - a_{D-(i-1)}$ for $1 \leq i \leq n = \lfloor D/2 \rfloor$. Then $d_1 \geq d_2 \geq \cdots d_n \geq 0$ and $d_1 > 0$.

Then $\kappa(N) = \overrightarrow{N} - \overleftarrow{N}$ equals

$$[d_1, \dots, d_{n-1}, d_n - 1, B - 1, B - d_n - 1, \dots B - d_2 - 1, B - d_1],$$

if $d_n > 0$, (with 'central' $B - 1$ absent for D even) and it equals

$$[d_1, \dots, d_{k-2}, d_{k-1} - 1, B - 1, \dots, B - 1, B - d_n - 1, \dots, B - d_2 - 1, B - d_1],$$

when $d_{k-1} > 0, d_k = \cdots = d_n = 0$.

Observe that $\kappa(N)$ only depends on the differences d_i's, and the sum of digits of $\kappa(N)$ is $r(B - 1)$ where $D/2 \leq r \leq D - 1$.

2.8 *S versus $\overline{S}$*

For $(B, D) = (2j + 1, 2)$, we have $\kappa([2j, j - 1]) = [j, j]$, so $\overline{S}$ is not preserved under κ. (In particular, this is not a Kaprekar tuple). We now show that $\overline{S}$ is preserved under κ for other (B, D), by deriving a contradiction from the assumption that the image of some element in $\overline{S}$ under κ has all digits the same. For $D = 2$, if $a - b = d > 0$, then $\kappa([a, b]) = [d - 1, B - d]$, which does not have equal digits for even B. For $D > 2$, we use the calculation of differences in the previous subsection: For

$D > 3$, in the first case (namely $d_n > 0$), we have $n > 1$, and we get $d_1 = d_n - 1$, contradicting with $d_1 \geq d_n$, whereas in the second case, we get $d_{k-1} - 1 = B - 1$, contradicting $d_i \leq B - 1$. For $D = 3$, we have $n = 1$ and a similar contradiction $d_1 - 1 = B - 1$.

So we can always restrict to $\overline{S}$, when $D > 2$, for the iterations of κ.

3. Kaprekar phenomena for $D \leq 4$

3.1 $D = 2$

(This seems to be folklore). If $a > b$, $[a, b] - [b, a] = [b, a]$ leads to $2a = b + B$, $a = 2b+1$, thus $FP(B, 2)$ non-empty implies $B = 3b+2$, in which case $FP(B, 2) = \{[b, 2b + 1]\}$. In other words, $n = 3b^2 + 4b + 1$ is the unique (non-trivial) fixed point then. We saw above that Kaprekar phenomena implies that B is even, so that $B = 6m + 2$. Now $(2, 2)$ is clearly Kaprekar, with $K(2, 2) = [0, 1]$. But for $m > 0$, we do not get Kaprekar phenomena: Note $\kappa([a, b]) = [d - 1, B - d]$, for $|a - b| = d > 0$, so that the difference $|B - 2d + 1|$ in the image of κ is odd. The difference for the the fixed point $[2m, 4m + 1]$ is $2m + 1$. But $|B - 2d + 1| = 2m + 1$, for odd d implies $d = 2m+1$. Thus, if you start with a tuple in the image of κ, with $d \neq 2m+1$, Kaprekar process iterations will never lead to the fixed point. For example, if you start with 1, its κ-image being $[0, B - 1]$, it will not lead to the fixed point.

3.2 $D = 3$

Theorem 1 (See [J64]). *The tuple* $(B, 3)$ *is Kaprekar, if and only if B is even. We have* $K(2m, 3) = [m - 1, 2m - 1, m]$*, and it is reached in at most m iterations.*

Proof. We give the short proof from [J64]. When $a \geq b \geq c$, with not all digits the same, we have $\kappa([a, b, c]) = [a - c - 1, B - 1, B - a + c]$. So one digit of the image is $B - 1$ and the other 2 add to $B - 1$. When $B = 2m$, it leads to (ordered) $[2m - 1, n, 2m - 1 - n]$, with $n \geq m$. For $n > m$, the next step leads to $[2m - 1, n - 1, 2m - n]$ and so after $n - m$ iterations one reaches the fixed point. In other direction, if $B = 2m + 1$, existence of fixed point with digits $2m, n, 2m - n$, with $n \geq m$, leads to $\kappa([2m, n, 2m - n]) = [n - 1, 2m, 2m - n + 1]$, giving $n - 1 = 2m - n$, parity contradiction. □

3.3 $D = 4$

The complexity increases a lot with one more digit.

Theorem 2 (See [HP78]). *The set* $FP(B, 4)$ *is non-empty, if and only if B is* $2, 4$ *or* $5k$*, with* (d_1, d_2) *being* $(1, 0)$, $(1, 1)$; $(3, 1)$; $(3k, k)$ *respectively. The respective fixed points are* $[0, 1, 1, 1]$, $[1, 0, 0, 1]$, $[3, 0, 2, 1]$ *and* $[3k, k - 1, 4k - 1, 2k]$*. The tuple* $(B, 4)$ *is Kaprekar, if and only if* $B = 2^n * 5$*, with* $n = 0$ *or n odd.*

4. Kaprekar phenomena for 5, 7, 9 digits

4.1 $D = 5$

Theorem 3. *The set* $FP(B, 5)$ *is non-empty, if and only if* $B = 2$ *(in which case, it has 2 elements) or* $B = 3k$ *(in which case, it is singleton). The tuple* $(B, 5)$ *is Kaprekar, if and only if* $B = 3k$*, with* $k = 1$ *or* $k \geq 5$ *odd. In this case,* $K(B, 5) = [2k, k-1, 3k-1, 2k-1, k]$*, corresponding to* $(d_1, d_2) = (2k, k)$*.*

Proof. We refer to [P78] for the full proof, giving only the proof for the first claim and of the 'easier half' of the second, omitting author's (a little different, but not any simpler) proof of the other half.

First we solve for all fixed points N. We use the 'differences' calculation and the notation as above, with cases (i) $d_1 > d_2 > 0$, (ii) $d_1 = d_2 > 0$ and (iii) $d_2 = 0$.

For a fixed point N, if $M = \overrightarrow{N} - \overleftarrow{N}$, then $\overrightarrow{M} = \overrightarrow{N}$.

The inequalities applied to this easily give that in case (i) $\overrightarrow{N} = [B-1, d_1, B-d_2-1, B-d_1, d_2-1]$, so that $d_1 = (B-1) - (d_2-1)$, and $d_2 = d_1 - (B-d_1)$. Solving these we get $B = 3d_2$ and $d_1 = 2d_2$, giving the fixed point $[2k, k-1, 3k-1, 2k-1, k]$ for $B = 3k$. In case (ii), writing $d_1 = d_2 = d$, we get $\overrightarrow{N} = [B-1, B-d, d, d-1, B-d-1]$, with $B-1 = B-d$ and $d-1 = B-d-1$, leading to $B = 2d = 2$ corresponding to fixed point $[1, 0, 1, 0, 1]$ for $B = 2$. In the remaining case (iii), writing $d_1 = d$, we get $\overrightarrow{N} = [B-1, B-1, B-1, B-d, d-1]$. (This is because, the other option $\overrightarrow{N} = [B-1, B-1, B-1, d-1, B-d]$ leads to the contradiction $d = (B-1) - (B-d)$.). Since $d_2 = 0$, we get $B - 1 = B - d$ implying $d = 1$. So $d = (B-1) - (d-1) = B - 1$. Hence, in this case $B = 2$ and the fixed point is $[0, 1, 1, 1, 1]$. This proves the first claim of the Theorem.

Next we rule out $B = 6k$ and $B = 9$ from candidates for Kaprekar phenomena, as they have (straight-forward to check) respectively a 2-cycle starting from $[6k-1, 3k, 3k, 3k, 3k-2]$, and a 5-cycle starting from $[8, 8, 4, 3, 1]$ (with (d_1, d_2) pair cycling through $(7, 5)$, $(6, 4)$, $(5, 3)$, $6, 1)$, $(8, 4)$ while the fixed point corresponds to $(6, 3)$). This finishes the proof of the 'only if' part of the second statement. □

4.2 $D = 7$

Theorem 4. *For* $D = 7$*, Kaprekar phenomena happens, if and only if* $B = 4$*, in which case* $[3, 2, 0, 3, 2, 1, 1]$ *is the fixed point.*

Proof. Let $n \geq 0$. We rule out $B = 9 + 4n, 18 + 4n, 23 + 4n, 24 + 4n$ by exhibiting respectively a 2-cycle, 4-cycle, 8-cycle, 19-cycle.

For $B = 9 + 4n$, $\overrightarrow{N} = [8 + 4n, 6 + 3n, 6 + 3n, 5 + 2n, 3 + 2n, 3 + n, 1 + n]$ corresponding to differences $(7 + 3n, 3 + 2n, 3 + n)$ leads to a 2-cycle with $\kappa(\overrightarrow{N}) = [7 + 3n, 3 + 2n, 2 + n, 8 + 4n, 5 + 3n, 5 + 2n, 2 + n]$ corresponding to differences $(6 + 3n, 5 + 2n, 2 + n)$. (Note that if we put $n = -1$, $3 + 2n < 3 + n$ and the ordering and the calculation is not valid).

For $B = 18 + 4n$, $\overrightarrow{N} = [17 + 4n, 14 + 3n, 13 + 3n, 9 + 2n, , 8 + 2n, 5 + n, 2 + n]$ with differences $(15 + 3n, 9 + 2n, 5 + n)$ leads to a 4-cycle, as the reader can verify directly.

For $B = 23 + 4n$, $\overrightarrow{N} = [22 + 4n, 18 + 3n, 16 + 3n, 11 + 2n, 11 + 2n, 5 + n, 5 + n]$, with differences $(17 + 3n, 13 + 2n, 5 + n)$ leads to a 8-cycle.

For $B = 24 + 4n$, we have a 19-cycle, starting with N with $\overrightarrow{N} = [23 + 4n, 19+3n, 17+3n, 12+2n, 11+2n, 7+n, 3+n]$ with differences $(20+3n, 12+2n, 6+n)$. (Alternate way to rule out this arithmetic progression for the Kaprekar phenomenon is to note that we have 2 fixed points from families mentioned in Section 5.3: Put $k = 4$, $m = 6 + n$ in the first family there and $r = 4, n = 1, k = 6 + n$ in the second).

For $B = 4$, it is easy to verify directly that it leads to the Kaprekar phenomenon with $K(4, 7) = 14565$, which is $[3, 2, 0, 3, 2, 1, 1]$.

For $B = 2$, we see below that there are 2 non-trivial fixed points.

So one is left to consider $B = 3, 5, 6, 7, 8, 10, 11, 12, 14, 15, 16, 19, 20$. If we start with $N = 1$, these exhibit n-cycles respectively for n being 2, 4, 2, 6, 7, 8, 14, 9, 8, 10, 11, 14, 13. □

4.3 *Remark*

Note that as B increases by 4, the differences change by (3, 2, 1). For $D = 5$, it was (2, 1) for increase by 2, and for $D = 3$ it was 1 for 1. This leads to a guess that for $D = 2m + 1$, and for large enough B, (after entering a cycle) the differences change of $(m, m - 1, \dots 1)$, for the increase of $m + 1$ in the base, leads to the same cycle structure. In fact, the vector $\overrightarrow{N}$ increases by $[m + 1, m, m, m - 1, m - 1, \dots, 1, 1]$ in such a step.

If this is true, it is probably possible to prove it, even with an explicit lower bound on B, without too much effort. Then for a given odd D, with only finitely many corresponding B's giving the Kaprekar phenomenon, we can prove this finiteness effectively. We have not tried this, except in the next simplest case below.

4.4 $D = 9$

Theorem 5. *For $D = 9$, Kaprekar phenomena occurs if and only if $B = 5$, in which case* $[4, 3, 2, 0, 4, 3, 2, 1, 1]$ *is the fixed point.*

Proof. Let $D = 9$.

For $B = 5n + 13$, for $n \geq 4$, we get two-cycle, starting from $\overrightarrow{N} = [12 + 5n, 12 + 4n, 8 + 4n, 9 + 3n, 4 + 3n, 8 + 2n, 3 + 2n, 3 + n, 1 + n]$.

For $B = 5n + 12$, $n \geq 3$, we get two cycle, starting from $\overrightarrow{N} = [11 + 5n, 11 + 4n, 7 + 4n, 8 + 3n, 4 + 3n, 7 + 2n, 3 + 2n, 3 + n, 1 + n]$.

For $B = 39 + 5n$, $n \geq 0$, we have a two-cycle, starting from $\overrightarrow{N} = [38 + 5n, 33 + 4n, 29 + 4n, 25 + 3n, 19 + 3n, 19 + 2n, 13 + 2n, 8 + n, 6 + n]$.

For $B = 65 + 5n$, $n \geq 0$, we have a four-cycle, starting from $\overrightarrow{N} = [64 + 5n, 54 + 4n, 52 + 4n, 39 + 3n, 38 + 3n, 26 + 2n, 25 + 2n, 11 + n, 11 + n]$.

For $B = 41 + 5n$, $n \geq 0$, we have a six-cycle, starting from $\overrightarrow{N} = [40 + 5n, 32 + 4n, 32 + 4n, 25 + 3n, 22 + 3n, 18 + 2n, 15 + 2n, 9 + n, 7 + n]$.

The left-over finitely many cases, all for $5 \neq B \leq 60$, are ruled out and $B = 5$ is directly verified, just as in the proof of the previous theorem. □

We just mention one short-cut, or alternate to elimination: For $B = 10+5n$, $n \geq 0$, we have a fixed point $[8+4n, 6+3n, 4+2n, 1+n, 9+5n, 7+4n, 5+3n, 3+2n, 2+n]$, and for n even, another one $[(B/2)_2, B/2-1, (B-1)_3, (B/2-1)_2, B/2]$, where we use the short-from notation introduced in 2.1 for the repeated digits.

5. Kaprekar phenomena for fixed bases

5.1 $B = 2, 3$

Theorem 6. *(i) The set $FP(2, D)$ is never empty. It is singleton, if and only if $D = 2, 3$, if and only if $(2, D)$ is Kaprekar.*

(ii) The set $FP(3, D)$ empty if and only if $D = 2, 3, 4, 6$. It is singleton if and only if $D = 5, 7, 8, 9, 10, 12$. The tuple $(3, D)$ is Kaprekar if and only if $D = 5, 8$.

Proof. (i) follows from the immediately verified fact that for $n > 1$, $[1_{n-1}, 0, 1, 0_{n-1}, 1]$, $[0, 1_{2n}] \in FP(2, 2n+1)$, and $[1_{n-1}, 0_n, 1]$, $[0, 1_{2n-1}] \in FP(2, 2n)$, and the direct check (or using 3.1, 3.2) for $D = 2, 3$ (corresponding to $n = 1$, when the two points coincide).

For $B = 3$, it's easy to verify that for $m > k > 0$, $[2_k, 1_{m-k-1}, 0, 2_{m-k}, 1_{m-k}, 0_{k-1}, 1] \in FP(3, 3m-k)$. If $D \geq 15$, we can write $D = 3m-k = 3(m+1)-(k+3)$, with $k = 1, 2$ or 3, so that $m \geq 6$, $m > k$, $m+1 \geq 7 > k+3$. Hence there are at least two (non-trivial) fixed points for such $(3, D)$. The same works for $D = 14, 13, 11$ by using $14 = 3*5-1 = 3*6-4$, $13 = 3*5-2 = 3*6-5$, $11 = 3*4-1 = 3*5-4$. For $D = 12$, $D \leq 10$, the rest of the claims can be easily checked by straight-forward computer exhaustive check (which, with a little patience, can easily be done also by hand in this case) for existence and uniqueness of fixed point. In more details, this can be done by checking for the solutions to the corresponding equations, then in singleton list, all except $D = 5, 8$ can be ruled out for Kaprekar phenomena. (There are several short-cuts, for example, for $D = 5n - 3$, we get a 2-cycle, starting from $[2_{3n-2}, 1_{2n-2}, 0]$. Often iterations starting with $n = 1$ exhibits eventually a cycle of length more than one). Finally, $D = 5, 8$ can be directly verified for Kaprekar phenomena. Thus (ii) follows. □

5.2 *General Base* $B \geq 4$

Theorem 7. *For a given base $B > 1$, there are only finitely many D such that $FP(B, D)$ is singleton or empty, and in particular, such that there is Kaprekar phenomena for (B, D). In fact, if $B \geq 3$, then for $D > 4B - 6$, there is at least one element in $FP(B, D)$, and for $D > 8B - 12$, there are at least two elements in $FP(B, D)$. For even $B \geq 4$ and $D \geq B(B-1)$, there are at least 2 elements in $FP(B, D)$*

Proof. Now let $B \geq 3$, and consider $D = 2b(B-2) + 2a + b$, with $a, b \geq 1$. We exhibit a fixed point p, with $\overrightarrow{p} = [(B-1)_a, (B-1)_b, (B-2)_{2b}, \ldots, 1_{2b}, 0_a]$. Here, p is given by (again with obvious modifications for $B = 3$)

$$[(B-1)_a, (B-2)_b, \ldots, 2_b, 1_{b-1}, 0, (B-1)_b, \ldots, 1_b, 0_{a-1}, 1].$$

Now we use the standard fact from elementary number theory that given relatively prime m, n, any $D > mn - m - n$ can be written as $ma + nb$, with integers $a, b \geq 0$, so with $a, b \geq 1$ for $D > mn$ and with $a \geq 1, b > 2$ for $D > mn + 2n$. We use this with $m = 2, n = 2(B-2)+1$. In the last case, we have $D = 2a + b(2(B-2)+1) = 2(a + 2(B-2)+1) + (b-2)(2(B-2)+1)$ giving the two fixed points and proving the first part.

For the second part, with a slightly better bound for small B, we proceed as follows. Let $B \geq 4$ be even, and $D \geq B(B-1)$. Write $D = n(B-1) + r$, with $0 \leq r \leq B-2$, so that $r + 2 \leq B \leq n$. We exhibit two fixed points (straight-forward to verify) p, q, with $\overrightarrow{p} = [(B-1)_n, \ldots, 1_n, 0_r]$ and $\overrightarrow{q} = [(B-1)_{n-1}, (B-2)_n, \ldots, 1_n, 0_{r+1}]$. In fact, for $r \geq 1$ and for $r = 0$ respectively, we have

$$p = [(B-1)_r, (B-2)_{n-r}, \ldots, 3_r, 2_{n-r}, 1_{r-1}, 0, (B-1)_{n-r},$$
$$(B-2)_r, \ldots, 1_{n-r} 0_{r-1}, 1],$$
$$p = [(B-2)_n, \ldots, 2_{n-1}, 1, (B-1)_n, \ldots, 3_n, 1_{n-1}, 2],$$

with first portion up to digit 2 dropped for $B = 4$. Also, q is given by (with commas dropped to save space),

$$[(B-1)_{r+1}(B-2)_{n-r-2}(B-3)_{r+2} \ldots 2_{n-r-2} 1_{r+1} 0$$
$$\times (B-1)_{n-r-2}(B-2)_{r+2} \ldots 1_{n-r-2} 0_r 1],$$

with obvious modifications for $B = 4$. □

5.3 *Fixed point families*

We now give a few other general fixed point families, which once observed, are straight-forward and easy to verify.

Jordan gives ordered form $[km-1, (k-1)m, (k-1)m-1, (k-2)m, \ldots, m, m-1]$ of an element in $FP(km, 2k-1)$. (See [J64]).

For $D \geq 6$ even, Jordan gives a congruence class for moduli $105, 255, 257$ such that for B in it, there are at least 2 elements in $FP(B, D)$.

Here is a more general situation. We claim that

$$[((r-1)k)_n, ((r-2)k)_n, \ldots (2k)_n, k_{n-1}, k-1, (rk-1)_n, ((r-1)k-1)_n, \ldots (2k-1)_n,$$

$(k-1)_{n-1}, k] \in FP(rk, (2r-1)n)$, for $r > 1$. This is easy to verify, once observed. This gives fixed points not only in odd number of digits, but in any non 2-power number of digits, for basis which are multiples of certain number. If D has 2 distinct odd factors greater than 1, we get more than one fixed point for basis which are multiples of certain numbers. Thus, for such families of (B, D)'s, there is no unique cycle, and in particular, no Kaprekar phenomena.

Combining, we see that for D a non-trivial odd multiple of 3, we have at least 2 non-trivial fixed points for tuples $(2km, D)$'s, where we write $D = 2k - 1 > 3$. Also, we see at least 2 non-trivial fixed points for $(6k, 15n)$.

For D an even multiple of 3, we get arithmetic progressions of B, with the constant difference 30, with at least 2 non-trivial fixed points for such (B, D)'s. Jordan [J64] has already obtained for such D, arithmetic progressions of B with at least 2 non-trivial fixed points. In our case, we just get better density of such B's.

5.4 *Some data and guesses*

(1) The B showing Kaprekar phenomena are (i) For $D = 6$, only $B = 13, 17$ (with respectively at most 22, 40 steps needed to reach the fixed point) among $B \leq 39$, (ii) For $D = 7$, only $B = 4$ (with at most 6 steps) among $B \leq 24$, we have proved this above except for the bound on the number of steps which can be directly verified, (iii) For $D = 8$, only $B = 3$ (at most 6 steps) among $B \leq 17$, (iv) For $D = 9$, only $B = 5$ (at most 14 steps) among $B \leq 17$. In most of the cases, just looking at the iterations starting from 1, and observing them entering cycle of length more than 1 ruled out Kaprekar phenomena. Rarely, seeing a fixed point instead, we changed the initial point.

The data suggests that probably the examples we found are the only ones, even if we drop the bounds on B that we checked.

(2) For $6 \leq D \leq 13$, and $B \leq 100$, we ran program to see if iterations of the process starting with initial point $N = 1$ reaches a fixed point in about 100 (or 400 for larger B) steps, in rare cases when it did, whether those survive with $N = 2, 3, 12$ etc. Only Kaprekar phenomena found (other than that mentioned in one and proved for $D = 7$) corresponded to $\kappa(3, 8) = 5332$ (6 steps), $\kappa(5, 9) = 1831056 = [4, 3, 2, 0, 4, 3, 2, 1, 1]$ (14 steps), and $\kappa(7, 11) = 19222633344 = [0, 1_2, 2, 3_2, 4, 5_2, 6_2]$ (18 or 19 steps at most). (The last one was checked only for $N < 3^{12}$ and some random other checks).

Writing more sophisticated cycle-detection program it should be easy to prove (or disprove) that the examples we found are the only ones for the range of B, D's we consider, and to even extend this range.

(3) For $D = 2, 7, 9$ we have proved there is, and for $D = 8, 11$ there seems to be, only one Kaprekar base each. For $D = 6$, there seem to be 2 Kaprekar bases. For $D = 4$, there are (eventually) exponentially spread Kaprekar bases, while for $D = 3, 5$ they are spread (eventually) in arithmetic progression and there seem to be none for $D = 10, 12, 13$.

5.5 *Open questions*

Some interesting open questions and projects, less ambitious than (0) the complete understanding of all cycle structures for all (B, D), or even (i) characterization of all Kaprekar constants, but for which I would love to know the answer are (ii) Characterization of (B, D) such that $FP(B, D)$ is non-empty, or singleton, or when there is unique (length more than one) cycle, (iii) What are (are there infinitely many) D's such that for some B (or for infinitely many B's) there is a Kaprekar phenomena? (iv) What are good estimates for the maximum number of iterations needed to reach the Kaprekar constant, when the Kaprekar phenomenon happens, and what are (some of) the numbers which need the maximum number of iterations?

Acknowledgments

I am grateful to Shashikant Katre, who told me about the Hasse-Prichett result in Summer 2017. These results were presented at the International conference at Pune in December 2017, on the occasion of Katre's retirement. Katre has been instrumental in helping several batches of graduate, undergraduate and school students in India, teaching and inspiring them to do mathematics research. We are grateful for his dedication and selfless service over the years. I thank the organizers of the Ropar conference for their invitation, and also for inviting the article, even though I could not attend the conference at the last moment. I thank Alejandro Lara Rodriguez, who provided me the basic digit expansion related sage commands. Online SAGE math cell was used interactively for the computations needed. I am very grateful to the referee for many helpful suggestions.

References

[D08] S. P. Deshpande, Ganitanandi Kaprekar (in Marathi), Narendra Prakashan, Pune, India (2008).

[DG04] D. Deutsch and B. Goldman, Kaprekar's constant, *Math. Teacher*, **98** No. 4 (2004) 234–242.

[ES88] K. Eldridge and S. Sagong, The determination of Kaprekar convergence and loop convergence of all three-digit numbers, *Amer. Math. Monthly*, **95** No. 2 (1988) 105–112.

[HP78] H. Hasse and G. D. Prichett, Determination of all 4-digit Kaprekar constants, *J. Reine Angew (Crelle's Journal)* **299–300** (1978) 113–124.

[J64] J. H. Jordan, Self Producing Sequences of Digits, *Amer. Math. Month.*, **71** (1964) 61–64.

[K49] D. R. Kaprekar, Another Solitaire Game, *Scripta Math.*, **15** (1949) 244–245.

[K55] D. R. Kaprekar, An Interesting Property of the Number 6174, *Scripta Math.*, **21** (1955) 304.

[M17] M. Moreira, Dihedral symmetry in Kaprekar's problem, *Math. Mag.*, **90** (2017) 39–47.

[P78] G. D. Prichett, Terminating cycles for iterated difference values of five digit integers, *J. Reine Angew (Crelle's Journal)*, **303–304** (1978) 379–388.

[T72] C. Trigg, Kaprekar's routine with five-digit integers, *Math. Mag.*, **45** No. 3 (1972) 121–129.

Topics in Number Theory, RMS-Lecture Notes Series No. 26, 2020, pp. 71–107.

p-Adic Rankin Product *L*-Functions

Eknath Ghate and Ravitheja Vangala

School of Mathematics, TIFR, Homi Bhabha Road, Mumbai 400 005, India.
e-mail: eghate@math.tifr.res.in, ravithej@math.tifr.res.in

Abstract. We describe Panchishkin's construction of the p-adic Rankin product L-function.

Keywords. p-adic L-functions, Kummer congruences, Rankin-Selberg method, Nearly holomorphic modular forms

2010 Subject Classification: Primary 11F67, Secondary 11F30, 11F85

Let p be an odd prime. In this article we give a construction of the p-adic Rankin product L-function which interpolates p-adically the special values of the convolution of two cusp forms on the complex upper half plane. The argument given here closely follows Panchishkin's original argument [Pan88] where the S-adic non-archimedean L-function associated to the Rankin product of two modular forms was constructed, for S any set of finite primes including p. In this exposition we will specialize the argument given in [Pan88] to the case $S = \{p\}$. We correct a sign error in the original argument without which it does not seem possible to glue together the individual measures constructed by Panchishkin at each point in the critical strip into a single p-adic L-function, and also provide some background details along the way.

1. Introduction

1.1 *Rankin product L-functions*

Let N be an arbitrary natural number. We consider a cusp form f of weight $k \geq 2$ for the congruence subgroup $\Gamma_0(N)$ and nebentypus ψ. We suppose that f is a primitive cusp form, i.e., it is a normalized newform of some level C_f dividing N; C_f is called the conductor of f. Let g be another primitive cusp form of conductor C_g and weight $2 \leq l < k$ for $\Gamma_0(N)$ and nebentypus ω. We set $e(z) = e^{2\pi i z}$ and let

$$f(z) = \sum_{n=1}^{\infty} a(n)e(nz), \quad g(z) = \sum_{n=1}^{\infty} b(n)e(nz) \tag{1.1}$$

be the Fourier expansions of f and g. The Rankin convolution of the modular forms f and g is defined by means of the equality

$$\mathcal{D}(s, f, g) := L_N(2s + 2 - k - l, \psi\omega)L(s, f, g), \tag{1.2}$$

where

$$L(s, f, g) = \sum_{n=1}^{\infty} a(n)b(n)n^{-s},$$

and $L_N(2s+2-k-l, \psi\omega)$ denotes the Dirichlet L-series with character $\psi\omega$, and the subscript N indicates that the factors corresponding to the prime divisors of N are omitted from the Euler product. A classical method of Rankin and Selberg [Ran39] enables one to construct an analytic continuation of the function $\mathcal{D}(s, f, g)$ to the whole complex plane and prove that it satisfies a functional equation. Let

$$f^{\rho}(z) := \sum_{n=1}^{\infty} \overline{a(n)}e(nz), \quad g^{\rho}(z) := \sum_{n=1}^{\infty} \overline{b(n)}e(nz).$$

Further, define

$$\Psi(s, f, g) = \gamma(s)\mathcal{D}(s, f, g), \tag{1.3}$$

where $\gamma(s) = (2\pi)^{-2s}\Gamma(s)\Gamma(s-l+1)$ consists of Γ-functions. Though we do not use it here, $\Psi(s, f, g)$ has a well-known functional equation. For instance, if ψ, ω and $\psi^{-1}\omega$ all have conductor N and $C_f = C_g = N$, then the functional equation is (see [Hid93, §9.5, Theorem 1]):

$$\Psi(s, f^{\rho}, g) = W(f^{\rho}, g)N^{3(-s+(k+l-1)/2)}\Psi(k+l-1-s, f, g^{\rho}), \tag{1.4}$$

where

$$W(f^{\rho}, g) = (-1)^{l}\Lambda(f^{\rho})\Lambda(g)\frac{G(\psi^{-1}\omega)}{|G(\psi^{-1}\omega)|},$$

$G(\psi^{-1}\omega)$ is the Gauss sum associated to $\psi^{-1}\omega$ and $\Lambda(f^{\rho})$, $\Lambda(g)$ are the root numbers associated to f^{ρ}, g respectively (defined in §2). Shimura [Shi77] established the following algebraicity result for the special values of $\mathcal{D}(s, f, g)$ (see [Hid93, §10.2, Theorem 1]): the numbers

$$\Psi(s, f, g)(\pi^{1-l}\langle f, f\rangle_{C_f})^{-1} \in \overline{\mathbb{Q}}, \tag{1.5}$$

for all integers $l \le s \le k-1$. Here $\langle f, f\rangle_{C_f}$ is the Petersson inner product defined by

$$\langle f, f\rangle_{C_f} := \int_{\mathcal{H}/\Gamma_0(C_f)} |f(z)|^2 y^{k-2}\, dxdy, \quad z = x+iy,$$

where $\mathcal{H}/\Gamma_0(C_f)$ is a fundamental domain for the upper half plane $\mathcal{H}$ modulo the action of $\Gamma_0(C_f)$. The integers $s = l, \ldots, k-1$ in (1.5) are "critical" in the sense of Deligne [Del79]. They are precisely the values of s for which neither of the functions $\gamma(s)$ and $\gamma(k+l-1-s)$ in the functional equation have poles.

1.2 *Main theorem*

Let $\mathbb{C}_p = \widehat{\overline{\mathbb{Q}}}_p$ be the completion of the algebraic closure of $\mathbb{Q}_p$. Let $|\cdot|_p$ be the norm on $\mathbb{C}_p$, normalized so that $|p|_p = 1/p$. For any topological group G, let $X(G)$ denote the group of continuous homomorphisms from G to $\mathbb{C}_p^\times$. The domain of definition of p-adic L-functions is the $\mathbb{C}_p$-analytic Lie group $X_p = X(\mathbb{Z}_p^\times)$, where $\mathbb{Z}_p^\times$ is the group of units of $\mathbb{Z}_p$. We put $X_p^{\mathrm{tors}} = \{\chi \in X_p \mid \chi \text{ has finite order}\}$. Let x_p denote the embedding $\mathbb{Z}_p \hookrightarrow \mathbb{C}_p$. For a precise statement of the results we introduce the notation

$$g(\chi) := \sum_{n=1}^{\infty} \chi(n)b(n)e(nz),$$

for the cusp form g twisted by the Dirichlet character χ. We fix an embedding of $\overline{\mathbb{Q}}$ into $\mathbb{C}$ and an embedding $i_p : \overline{\mathbb{Q}} \hookrightarrow \mathbb{C}_p$. Then every Dirichlet character χ whose conductor C_χ is a power of p can be identified with an element of X_p^{tors} and vice versa. By Theorem 2.6, with $g(\chi)$ replaced by $g^\rho(\overline{\chi})$, the numbers

$$\frac{\Psi(l+r, f, g^\rho(\overline{\chi}))}{\pi^{1-l}\langle f, f\rangle_{C_f}} \in \overline{\mathbb{Q}},$$

for $r = 0, 1, \ldots, k-l-1$. In this article we construct a $\mathbb{C}_p$-analytic function on X_p which interpolates the numbers

$$i_p\left(\frac{\Psi(l+r, f, g^\rho(\overline{\chi}))}{\pi^{1-l}\langle f, f\rangle_{C_f}}\right),$$

for all $\chi \in X_p^{\mathrm{tors}}$ and $r = 0, 1, \ldots, k-l-1$. We work under the assumption that f is a p-ordinary form, i.e., $a(p)$ is a unit in $\mathbb{C}_p$. In other words

$$|i_p(a(p))|_p = 1. \tag{1.6}$$

In addition, we suppose that

$$(C_f, C_g) = 1, \quad (p, C_f) = (p, C_g) = 1, \tag{1.7}$$

and we set $C = C_f C_g$. Let $\alpha(p)$ denote the root of the Hecke polynomial $X^2 - a(p)X + \psi(p)p^{k-1}$ for which $|i_p(\alpha(p))|_p = 1$ and let $\alpha'(p)$ be the other root. For every prime $q \nmid N$, let

$$X^2 - a(q)X + \psi(q)q^{k-1} = (X - \alpha(q))(X - \alpha'(q)),$$

$$X^2 - b(q)X + \omega(q)q^{l-1} = (X - \beta(q))(X - \beta'(q)). \tag{1.8}$$

We extend the definition of $\alpha(n)$ to all natural numbers of the form p^r by setting $\alpha(p^r) := \alpha(p)^r$.

Theorem 1.1 (Main theorem). *Under the assumptions* (1.6) *and* (1.7), *there exists a unique measure μ on $\mathbb{Z}_p^\times$ satisfying the following interpolation property: for all* *characters* $\chi \in X_p^{\mathrm{tors}}$ *and all integers* r *with* $0 \le r \le k-l-1$, *the value of the function* $x_p^r\chi$ *under the measure* μ

$$\int_{\mathbb{Z}_p^\times} x_p^r \chi \, d\mu$$

is given by the image under i_p *of the following algebraic number*

$$(-1)^r \omega(C_\chi) \frac{G(\chi)^2 C_\chi^{l+2r-1}}{\alpha(C_\chi^2)} \cdot \frac{\Psi(l+r, f, g^\rho(\overline{\chi}))}{\pi^{1-l}\langle f, f\rangle_{C_f}}.$$

This is exactly[1] [Pan88, Thm. 1.4], noting that the extra Euler factors $A(r,\chi)$ there do not appear here because $S = \{p\}$. Finally we remark that if μ is a $\mathbb{C}_p$-valued measure on $\mathbb{Z}_p^\times$, as in the main theorem above, then the function L_μ (the p-adic L-function attached to μ) defined by

$$L_\mu(\chi) = \mu(\chi) = \int_{\mathbb{Z}_p^\times} \chi \, d\mu, \quad \forall\, \chi \in X_p, \tag{1.9}$$

always turns out to be a $\mathbb{C}_p$-analytic function $L_\mu : X_p \longrightarrow \mathbb{C}_p$.

To make sense of the last statement we briefly recall the $\mathbb{C}_p$-analytic structure on $X_p = X(\mathbb{Z}_p^\times)$. We set

$$U = \{x \in \mathbb{Z}_p^\times \mid x \equiv 1 \bmod p\},$$

units of $\mathbb{Z}_p$ congruent to 1 mod p. Then we have the following decomposition

$$X_p = X((\mathbb{Z}/p\mathbb{Z})^\times) \times X(U).$$

Therefore every $\chi \in X_p$ can be written as $\chi_0\chi_1$ with $\chi_0 \in X((\mathbb{Z}/p\mathbb{Z})^\times)$ and $\chi_1 \in X(U)$. The characters χ_0 and χ_1 are called the tame part and the wild part of the character χ respectively.

We claim the function φ defined by $\varphi(\chi) := \chi(1+p)$, where $1+p$ is a topological generator of the group U, induces an isomorphism of groups

$$\varphi : X(U) \xrightarrow{\sim} T := \{t \in \mathbb{C}_p^\times \mid |t-1|_p < 1\}.$$

This isomorphism defines an analytic structure on $X(U)$, which can easily be checked to be independent of the choice of generator $1+p$. We first check that φ is well defined, i.e., φ takes values in T. Let $\chi \in X(U)$. Since $(1+p)^{p^n} \to 1$ as $n \to \infty$, by the continuity of χ we have $(\chi(1+p))^{p^n} \to 1$. Hence, $|\chi(1+p)|_p = 1$ and $|\chi(1+p)-1|_p \le \max\{|\chi(1+p)|_p, 1\} \le 1$. We now claim that $|\chi(1+p)-1|_p < 1$. Suppose not, then $|\chi(1+p)-1|_p = 1$. Therefore

$$\begin{aligned} 1 &= |(\chi(1+p)-1)^{p^n}|_p \\ &= \left|\sum_{k=1}^{p^n} \binom{p^n}{k} (\chi(1+p)-1)^k\right|_p \quad \left(\text{as } p \,\middle|\, \binom{p^n}{k}(\chi(1+p)-1)^k, \ \forall\, 1 \le k < p^n\right) \end{aligned}$$

[1] Except that we have added the sign $(-1)^r$ which we feel is necessary (see subsequent footnotes).

$$= |(\chi(1+p) - 1 + 1)^{p^n} - 1|_p$$
$$= |(\chi(1+p))^{p^n} - 1|_p.$$

This contradicts $(\chi(1+p))^{p^n} \to 1$. Hence $|\chi(1+p) - 1|_p < 1$. We now show that φ is an isomorphism. Every character $\chi \in X_p$ is uniquely determined by $\chi(1+p)$, since $1+p$ is a topological generator of U, hence φ is injective. For $t \in T$, define $\chi_t((1+p)^n) = t^n$, for all $n \in \mathbb{Z}$. Extending χ_t to all of $1 + p\mathbb{Z}_p$ by continuity we get an element of $X(U)$ which maps to t under φ. Hence φ is also surjective. A function $F : T \to \mathbb{C}_p$ is said to be analytic if $F(t)$ can be expressed as a power series, i.e., $F(t) = \sum_{i=0}^{\infty} a_i (t-1)^i,\ a_i \in \mathbb{C}_p$, which converges absolutely for all $t \in T$. The isomorphism $\varphi : X(U) \simeq T$ allows us to define an analytic structure on $X(U)$. Finally the notion of analyticity can be extended to all of X_p by translation.

In closing this introduction, we remark that Hida [Hid88] subsequently constructed a more general measure interpolating the critical Rankin product L-values of two cusp forms which themselves vary in p-adic families,[2] and in a different direction, Vienney [Vie00] has generalized Panchishkin's argument to cases where $a(p)$ is not a p-adic unit.[3]

1.3 *Outline of the paper*

We recall notation and results from the theory of modular forms in §2. In §3 we recall generalities about distributions and measures and state a criterion for a distribution whose values are known on a specific set of functions to be a measure in terms of the abstract Kummer congruences. The measure in Theorem 1.1 is obtained from certain complex-valued distributions Ψ_s, which we construct in §4 using the definition of the convolution (1.2). The distributions Ψ_s take values in $\overline{\mathbb{Q}}$ on X_p^{tors} for integers $l \le s \le k-1$. In §5 we obtain an integral representation for these distribution values using the Rankin-Selberg method and holomorphic projection. In §6 we prove that the $\mathbb{C}_p$-valued distributions $i_p(\Psi_s)$ satisfy the abstract Kummer congruences to finish the proof of Theorem 1.1.

2. Background on Modular forms

In this section we recall a few results from the theory of classical modular forms. Most of the material covered here is well known. In this section f and g are arbitrary functions which need not satisfy the assumptions of §1 unless otherwise stated. Also, χ, ψ, ω denote Dirichlet characters. Let $\mathrm{M}_2(\mathbb{Z})$ denote the set of 2×2 matrices with entries in $\mathbb{Z}$. Let $\mathrm{SL}_2(\mathbb{Z})$ denote the set of matrices with determinant 1 in $\mathrm{M}_2(\mathbb{Z})$. Let $\mathbb{C}$ denote the complex plane. We write an element $z \in \mathbb{C}$ as $x + iy$, where $x, y \in \mathbb{R}$ and $i^2 = -1$. For $z = x + iy \in \mathbb{C}$, sometimes we denote x and y by $\mathrm{Re}(z)$ and $\mathrm{Im}(z)$ respectively.

[2] The sign mentioned in the previous footnote is consistent with the sign in [Hid88, Theorem I].

[3] Again, the author remarks that it is necessary to add a sign, see just below [Vie00, Defintion 4.1].

2.1 *Classical modular forms*

Let $\mathcal{H} = \{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\}$ denote the complex upper half plane, on which the group $\mathrm{GL}_2^+(\mathbb{R})$ of real 2×2 matrices with positive determinant acts by fractional linear transformations. For any natural number k, we have a weight k action of $\mathrm{GL}_2^+(\mathbb{R})$ on functions $f : \mathcal{H} \to \mathbb{C}$ given by:

$$(f|_k\gamma)(z) = (\det\gamma)^{k/2}(cz+d)^{-k} f\left(\frac{az+b}{cz+d}\right), \quad \forall\, \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2^+(\mathbb{R}).$$

For any natural number N, we have the following subgroups:

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

$$\Gamma_1(N) = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N) \mid a \equiv d \equiv 1 \mod N\right\},$$

$$\Gamma(N) = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_1(N) \mid b \equiv 0 \mod N\right\}.$$

Definition 2.1. *A subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$ is called a congruence subgroup if $\Gamma(N) \subset \Gamma$ for some $N > 0$. The smallest N satisfying this condition is called the level of the congruence subgroup.*

If Γ is a congruence group, then $M_k(\Gamma)$ denotes the complex vector space of modular forms of weight k for Γ. These consist of holomorphic functions $f : \mathcal{H} \to \mathbb{C}$ which satisfy $f|_k\gamma = f$, for all $\gamma \in \Gamma$, and a holomorphicity condition at the cusps of Γ. Let $S_k(\Gamma)$ denote the subspace of cusp forms consisting of those f which in addition vanish at the cusps.

Notation. Throughout the article we use the following notation:

(i) For every integer M, let $S(M)$ denote the set of primes dividing M.
(ii) For every $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{M}_2(\mathbb{Z})$, and Dirichlet character ψ we put $\psi(\gamma) = \psi(d)$.
(iii) Let χ_0 denote the principal character on $\mathbb{Z}$. It is given by $\chi_0(n) = 1,\ \forall\, n \in \mathbb{Z}$.

If ψ is a Dirichlet character mod N, we set

$$M_k(N, \psi) = \{f \in M_k(\Gamma_1(N)) \mid f|_k\gamma = \psi(\gamma) f,\ \forall\, \gamma \in \Gamma_0(N)\},$$

$$S_k(N, \psi) = S_k(\Gamma_1(N)) \cap M_k(N, \psi).$$

For an arbitrary modular form $h \in M_k(N, \psi)$ and a cusp form $f \in S_k(N, \psi)$ with $k \geq 1$, the Petersson inner product is defined by the integral

$$\langle f, h\rangle_N = \int_{\mathcal{H}/\Gamma_0(N)} \overline{f(z)} h(z) y^{k-2}\, dx dy, \tag{2.1}$$

where $\mathcal{H}/\Gamma_0(N)$ is a fundamental domain for the upper half plane $\mathcal{H}$ modulo the action of $\Gamma_0(N)$. Observe that if $\gamma \in \mathrm{GL}_2^+(\mathbb{R})$ normalizes $\Gamma_0(N)$ and γ^2 is a scalar matrix, then (see [Miy89, Theorem 2.8.2])

$$\langle f|_k\gamma, h\rangle_N = \langle f, h|_k\gamma\rangle_N. \tag{2.2}$$

For the rest of this subsection assume that M, N are positive integers such that $S(NM) = S(N)$. Since $S(NM) = S(N)$ it can be checked that $[\Gamma_0(N) : \Gamma_0(NM)] = M$ and

$$\left\{\beta_u = \begin{pmatrix} 1 & 0 \\ uN & 1 \end{pmatrix} \middle| u = 1, \ldots, M\right\}$$

is a set of coset representatives for $\Gamma_0(NM)\backslash\Gamma_0(N)$. Therefore, for every $\gamma \in \Gamma_0(N)$ and β_u, there exists unique $\gamma_u \in \Gamma_0(NM)$ and $\beta_{u'}$ such that $\beta_u\gamma = \gamma_u\beta_{u'}$. Since β_u, $\beta_{u'} \equiv \mathrm{I}_2 \bmod N$ we have

$$\gamma \equiv \beta_u\gamma = \gamma_u\beta_{u'} \equiv \gamma_u \bmod N.$$

For a Dirichlet character ψ modulo N and $h \in M_k(NM, \psi)$ we have

$$\left(\sum_{u=1}^{M} h|_k\beta_u\right)|_k\gamma = \sum_{u=1}^{M} h|_k\gamma_u\beta_{u'} = \sum_{u=1}^{M} \psi(\gamma_u)\cdot h|_k\beta_{u'} = \psi(\gamma)\cdot\sum_{u=1}^{M} h|_k\beta_u.$$

Therefore $\sum_{u=1}^{M} h|_k\beta_u \in M_k(N, \psi)$. For M, N positive integers such that $S(NM) = S(N)$ and a Dirichlet character ψ modulo N, define the trace operator $Tr_N^{NM} : M_k(NM, \psi) \to M_k(N, \psi)$ by the equality

$$Tr_N^{NM}(h) = \sum_{u=1}^{M} h|_k\beta_u = \sum_{u=1}^{M} h|_k \begin{pmatrix} 1 & 0 \\ uN & 1 \end{pmatrix}. \tag{2.3}$$

Remark 2.2. The definition of the trace above depends on the choice of coset representatives $\{\beta_1, \ldots, \beta_M\}$ of $\Gamma_0(NM)\backslash\Gamma_0(N)$. In the computations below, we always use this choice.

Lemma 2.3. *Let ψ be a Dirichlet character modulo N. Let $f \in S_k(N, \psi)$ and $h \in M_k(NM, \psi)$. If $S(M) \subset S(N)$, then $\langle f, h\rangle_{NM} = \langle f, Tr_N^{NM}(h)\rangle_N$.*

Proof. Let $\{\beta_1, \ldots, \beta_M\}$ be as above. If $\mathcal{D}$ is a fundamental domain for $\Gamma_0(N)$, then $\coprod_{u=1}^{M} \beta_u\mathcal{D}$ is a fundamental domain for $\Gamma_0(NM)$. Therefore

$$\begin{aligned}
\langle f, h\rangle_{NM} &= \int_{\mathcal{H}/\Gamma_0(NM)} \overline{f(z)}h(z)y^{k-2}\,dxdy \\
&= \sum_{u=1}^{M}\int_{\beta_u\mathcal{D}} \overline{f(z)}h(z)y^{k-2}\,dxdy \\
&= \sum_{u=1}^{M}\int_{\mathcal{D}} \overline{(f|_k\beta_u)(z)}(h|_k\beta_u)(z)y^{k-2}\,dxdy \\
&= \sum_{u=1}^{M}\int_{\mathcal{D}} \overline{f(z)}\,(h|_k\beta_u)(z)y^{k-2}\,dxdy \\
&= \langle f, Tr_N^{NM}(h)\rangle_N.
\end{aligned}$$

□

For any integer k, complex number s and Dirichlet characters χ, ψ modulo L, M respectively, we define (see [Miy89, Chapter 7]) the non-holomorphic Eisenstein series of weight k by

$$E_k(z, s; \chi, \psi) = y^s \sum_{c,d=-\infty}^{\infty}{}' \chi(c)\psi(d)(cz+d)^{-k}|cz+d|^{-2s}, \ \forall\, z \in \mathcal{H}, \tag{2.4}$$

where the prime means that the sum is over all $(c, d) \in \mathbb{Z}^2 \backslash \{(0, 0)\}$. The series converges for $\mathrm{Re}(k + 2s) > 2$ and can be continued meromorphically to the whole complex plane as a function of s. Further, if $k \geq 3$, then $E_k(z, 0; \chi, \chi_0) \in M_k(L, \chi)$ [Miy89, Lemma 7.1.4, Lemma 7.1.5].

2.2 *Operators acting on modular forms*

Let $f \in S_k(N, \psi)$ be a cusp form with the Fourier expansion

$$f(z) = \sum_{n=1}^{\infty} a(n)e(nz).$$

If d is a natural number, then define

$$\begin{aligned}
f|U_d &= \sum_{n=1}^{\infty} a(dn)e(nz) \ = \ d^{k/2-1} \sum_{u \bmod d} f|_k \begin{pmatrix} 1 & u \\ 0 & d \end{pmatrix}, \\
f|V_d &= f(dz) \ = \ d^{-k/2} f|_k \begin{pmatrix} d & 0 \\ 0 & 1 \end{pmatrix} \in S_k(Nd, \psi), \\
f^{\rho}(z) &= \overline{f(-\overline{z})} \ = \ \sum_{n=1}^{\infty} \overline{a(n)} e(nz) \in S_k(N, \overline{\psi}), \\
f|w_d &= (\sqrt{d}z)^{-k} f\left(\frac{-1}{dz}\right) \ = \ f|_k \begin{pmatrix} 0 & -1 \\ d & 0 \end{pmatrix}, \ f|w_N \in S_k(N, \overline{\psi}).
\end{aligned}$$

Also, the Hecke operators $T_n : M_k(N, \psi) \to M_k(N, \psi)$ are defined by $(T_n f)(z) = \sum_{m=0}^{\infty} a(m, T_n f)e(mz)$, where $a(m, T_n f) = \sum_{0<d|(m,n)} \psi(d)d^{k-1}a(mn/d^2)$.

When $S(NM) = S(N)$, we have the following identity, which will be used for explicit computations:

$$Tr_N^{NM}(f) = (-1)^k M^{1-k/2} \ f|w_{NM}U_M w_N, \ \forall\, f \in S_k(N, \psi). \tag{2.5}$$

The above identity follows from the definitions and the matrix identity:

$$\begin{pmatrix} 1 & 0 \\ uN & 1 \end{pmatrix} = -(NM)^{-1} \begin{pmatrix} 0 & -1 \\ NM & 0 \end{pmatrix} \begin{pmatrix} 1 & -u \\ 0 & M \end{pmatrix} \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix}.$$

Lemma 2.4. *Let $f(z) = \sum_{n=1}^{\infty} a(n)e(nz) \in S_k(N, \psi)$ and U_d, V_d, T_n be as above.*

(1) *If $d^2 \mid N$ and ψ is a Dirichlet character mod N/d, then $f|U_d \in S_k(N/d, \psi)$.*

(2) *For* $n \geq 1$, *we have* $T_n(f) = \sum_{ad=n} \psi(d)d^{k-1} f|U_a V_d$. *Hence,* $T_p = U_p$ *if* $p \mid N$ *is a prime.*

Proof. Let $\begin{pmatrix} x & y \\ z & w \end{pmatrix} \in \Gamma_0(N/d)$ and $0 \leq u, u' < d$. Then

$$\begin{pmatrix} 1 & u \\ 0 & d \end{pmatrix} \begin{pmatrix} x & y \\ z & w \end{pmatrix} \begin{pmatrix} 1 & u' \\ 0 & d \end{pmatrix}^{-1} = \begin{pmatrix} x + uz & \frac{y+uw-(x+uz)u'}{d} \\ dz & w - zu' \end{pmatrix}.$$

We observe that if $d^2 \mid N$, then $d \mid z$ and $(x, d) = 1$. So $x + uz$ is a unit in $\mathbb{Z}/d\mathbb{Z}$. Hence, for every $0 \leq u < d$, there exists unique u' mod d such that $d \mid (y + uw - (x + uz)u')$. This implies that for every u mod d there exist unique u' mod d such that

$$\begin{pmatrix} x_u & y_u \\ z_u & w_u \end{pmatrix} := \begin{pmatrix} x + uz & \frac{y+uw-(x+uz)u'}{d} \\ dz & w - zu' \end{pmatrix} \in \Gamma_0(N).$$

Therefore

$$\begin{aligned} (f|U_d)|_k \begin{pmatrix} x & y \\ z & w \end{pmatrix} &= \sum_{u \bmod d} f|_k \begin{pmatrix} x_u & y_u \\ z_u & w_u \end{pmatrix} \begin{pmatrix} 1 & u' \\ 0 & d \end{pmatrix} \\ &= \sum_{u' \bmod d} \psi(w_u) f|_k \begin{pmatrix} 1 & u' \\ 0 & d \end{pmatrix} \\ &= \psi(w) \sum_{u' \bmod d} f|_k \begin{pmatrix} 1 & u' \\ 0 & d \end{pmatrix} \quad (\because \ \ w_u \equiv w \bmod (N/d)) \\ &= \psi(w)(f|U_d). \end{aligned}$$

Hence (1) follows. For the second statement we compare the Fourier expansion of both sides. From the definition of U_a, V_d it follows that

$$\begin{aligned} \sum_{ad=n} \psi(d)d^{k-1} f|U_a V_d(z) &= \sum_{d|n} \psi(d)d^{k-1} (f|U_{n/d})(dz) \ \ (\text{substituting } \ a = n/d) \\ &= \sum_{d|n} \psi(d)d^{k-1} \sum_{m=1}^{\infty} a(mn/d)e(mdz) \\ &= \sum_{d|n, d|m} \psi(d)d^{k-1} \sum_{m=1}^{\infty} a(mn/d^2)e(mz) \\ &= \sum_{m=1}^{\infty} \left(\sum_{d|(m,n)} \psi(d)d^{k-1} a(mn/d^2) \right) e(mz) \\ &= (T_n f)(z). \end{aligned}$$

□

Definition 2.5. *We call an element $f \in S_k(N, \psi)$ a primitive cusp form of conductor N if the following conditions are satisfied:*

(1) *f is an eigenform, i.e., $f(z)$ is an eigenvector for the Hecke operators T_n, for all $n \in \mathbb{N}$,*
(2) *$a(1) = 1$, where $f(z) = \sum_{n=1}^{\infty} a(n)e(nz)$,*
(3) *f is a newform, i.e., it is orthogonal to all (old)forms lying in the images of the maps $V_d : S_k(N/d, \psi) \to S_k(N, \psi)$, for $d \mid N$, $C_\psi \mid (N/d)$, under $\langle\, , \,\rangle_N$.*

If $f \in S_k(N, \psi)$ is a primitive cusp form, then $T_q(f) = a(q)f$ and $f|U_{q'} = T_{q'}(f) = a(q')f$ for all $q \nmid N$ and $q' \mid N$ respectively. Hence, f is uniquely determined by the eigenvalues of the Hecke operators T_n. Further, we also have the following:

Euler Product $L(s, f) = \displaystyle\sum_{n=1}^{\infty} a(n)e(nz) = \prod_q (1 - a(q)q^{-s} + \psi(q)q^{k-1-2s})$.

Functional Equation $\Lambda_N(s; f) = i^k \Lambda_N(k - s; f|w_N)$, where $\Lambda_N(s; f) = (2\pi/\sqrt{N})^{-s}\Gamma(s)L(s, f)$.

From the theory of newforms (see [Miy89, Theorem 4.6.15]) it follows that if $f \in S_k(N, \psi)$ is a primitive cusp form of conductor C_f, then

$$f|w_{C_f} = \Lambda(f) f^\rho, \tag{2.6}$$

where $\Lambda(f)$ is called the root number associated to f.

Let $g \in S_k(N, \omega)$ be a primitive cusp form of conductor C_g. If the conductor C_χ of the primitive Dirichlet character χ is coprime to C_g, then the twisted cusp form $g(\chi) \in S_k(C_g C_\chi^2, \omega\chi^2)$ [Miy89, Lemma 4.3.10 (2)] is primitive, and

$$\Lambda(g(\chi)) = \omega(C_\chi)\chi(C_g)\frac{G(\chi)^2}{C_\chi}\Lambda(g), \tag{2.7}$$

where

$$G(\chi) = \sum_{u \bmod C_\chi} \chi(u) e^{2\pi i u/C_\chi},$$

is the Gauss sum [Miy89, Theorem 4.3.11].

2.3 *Rankin-Selberg convolution*

The proof of Theorem 1.1 makes constant use of the classical Rankin-Selberg method (see [Ran39], [Ran52]). For the sake of completeness, we recall a few consequences of the Rankin-Selberg method in this section. Let $f \in S_k(N, \psi)$, $g \in S_l(N, \omega)$ be primitive cusp forms. Let $\alpha(q)$, $\alpha'(q)$, $\beta(q)$, $\beta'(q)$ be as in (1.8) for all $q \nmid N$. Put

$\alpha(q) = a(q)$ and $\beta(q) = b(q)$ and $\alpha'(q) = \beta'(q) = 0$ for all $q \mid N$. Then the L-function associated to f and g has the Euler product

$$L(s, f) = \sum_{n=1}^{\infty} a(n)n^{-s} = \prod_q [(1 - \alpha(q)q^{-s})(1 - \alpha'(q)q^{-s})]^{-1},$$

$$L(s, g) = \sum_{n=1}^{\infty} b(n)n^{-s} = \prod_q [(1 - \beta(q)q^{-s})(1 - \beta'(q)q^{-s})]^{-1}. \tag{2.8}$$

Before we state the result we introduce another class of Eisenstein series which are different from (2.4). For every Dirichlet character ψ mod N, we set

$$E_{k,N}(z, s, \psi) = y^s \sum_{c,d=-\infty}^{\infty}{}' \psi(d)(cNz + d)^{-k}|cNz + d|^{-2s}. \tag{2.9}$$

Let $f \in S_k(N, \psi)$ and $g \in S_l(N, \omega)$ be primitive cusp forms as in the Introduction (so $l < k$) and let $\mathcal{D}(s, f, g)$ be as in (1.2). Then the Rankin-Selberg method states that

(1) The Rankin product L-function has the Euler product

$$\mathcal{D}(s, f, g) = \prod_q [(1 - \alpha(q)\beta(q)q^{-s})(1 - \alpha(q)\beta'(q)q^{-s}) \times (1 - \alpha'(q)\beta(q)q^{-s})(1 - \alpha'(q)\beta'(q)q^{-s})]^{-1}. \tag{2.10}$$

(2) For $s \in \mathbb{C}$ with $\mathrm{Re}(s) > 1 + \frac{k+l}{2}$, the Rankin product L-function $\mathcal{D}(s, f, g)$ has the integral representation given by

$$2(4\pi)^{-s}\Gamma(s)\mathcal{D}(s, f, g) = \langle f^{\rho}, gE_{k-l,N}(z, s - k + 1, \psi\omega)\rangle_N. \tag{2.11}$$

We now state an algebraicity result for the Rankin product L-function which is crucial for the construction of the p-adic Rankin product L-function, due to Shimura.

Theorem 2.6. ([Shi77, Theorem 4], [Hid93, §10.2, Corollary 1]) *Let $f \in S_k(N, \psi)$ and $g \in S_l(N, \omega)$ be primitive cusp forms of conductor C_f and C_g respectively. Then for every Dirichlet character χ and for all integers s with $l \le s \le k - 1$, we have*

$$\frac{\Psi(s, f, g(\chi))}{\pi^{1-l}\langle f, f\rangle_{C_f}} \in \overline{\mathbb{Q}}. \tag{2.12}$$

2.4 *Nearly holomorphic modular forms*

In this section we recall some facts about nearly holomorphic modular forms due to Shimura (see [Hid93, §10.1]).

The Maass-Shimura differential operator of weight $k \in \mathbb{C}$ on C^∞-functions on $\mathcal{H}$ is the operator:

$$\delta_k = \frac{1}{2\pi i}\left(\frac{k}{2iy} + \frac{\partial}{\partial z}\right), \quad \text{where } z = x + iy, \ \frac{\partial}{\partial z} = \frac{1}{2}\left(\frac{\partial}{\partial x} - i\frac{\partial}{\partial y}\right). \tag{2.13}$$

For every positive integer r, we define $\delta_k^r := \delta_{k+2r-2} \circ \cdots \circ \delta_{k+2} \circ \delta_k$ and $\delta_k^0 f = f$. Let $d := \frac{1}{2\pi i}\frac{\partial}{\partial z}$. The Maass-Shimura differential operator satisfies the following properties:

(1) $\delta_{k+s}(fg) = (\delta_k f)g + f(\delta_s g) = (\delta_s f)g + f(\delta_k g), \ \forall\, s, k \in \mathbb{C}$,
(2) $\delta_k(f) = y^{-k} d(y^k f), \ \forall\, k \in \mathbb{C}$,
(3) $\delta_k^r = \delta_{k+2}^{r-1} \circ \delta_k$,
(4) $\delta_k^r(f) = \sum_{j=0}^r \binom{r}{j} \frac{\Gamma(r+k)}{\Gamma(j+k)} (-4\pi y)^{j-r} d^j f, \ \forall\, k \in \mathbb{C}, \ r \in \mathbb{N}$.

Definition 2.7. *Let k, r be non-negative integers. A function $f : \mathcal{H} \to \mathbb{C}$ is said to be a nearly holomorphic modular form of weight k and depth less than or equal to r for the congruence subgroup Γ, if the following hold:*

(1) *f is smooth as a function of x and y,*
(2) *$f|_k\gamma = f$, for all $\gamma \in \Gamma$,*
(3) *there exist holomorphic functions $f_0, \ldots, f_r$ on $\mathcal{H}$ such that $f(z) = \sum_{j=0}^r (4\pi y)^{-j} f_j(z)$,*
(4) *f is slowly increasing, i.e., for every $\alpha \in \mathrm{SL}_2(\mathbb{Z})$, there exists positive real numbers A and B such that $|(f|_k\alpha)(z)| \leq A(1 + y^{-B})$ as $y \to \infty$.*

The space of nearly holomorphic modular forms of weight k and depth less than or equal to r for the congruence subgroup Γ is denoted by $\mathcal{N}_k^r(\Gamma)$. It is clear that for $r = 0$ we obtain the space of (holomorphic) modular forms $M_k(\Gamma)$. Let $\mathcal{N}_k(\Gamma) = \cup_{r=0}^\infty \mathcal{N}_k^r(\Gamma)$, then $\oplus_{k=0}^\infty \mathcal{N}_k(\Gamma)$ is a graded $\mathbb{C}$-algebra. Further, let $\mathcal{N}_k^r(N, \chi) = \{f \in \mathcal{N}_k^r(\Gamma_1(N)) \mid (f|_k\gamma)(z) = \chi(\gamma) f(z), \forall\, \gamma \in \Gamma_0(N)\}$.

We say a function $h \in \mathcal{N}_k^r(\Gamma)$ is rapidly decreasing if for every $B \in \mathbb{R}$ and $\alpha \in \mathrm{SL}_2(\mathbb{Z})$, there exists a positive constant A such that $|(h|_k\alpha)(z)| \leq A(1 + y^B)$ as $y \to \infty$. We denote the subspace of rapidly decreasing functions in $\mathcal{N}_k^r(\Gamma)$, $\mathcal{N}_k^r(N, \chi)$ and $\mathcal{N}_k(\Gamma)$ by $\mathcal{NS}_k^r(\Gamma)$, $\mathcal{NS}_k^r(N, \chi)$ and $\mathcal{NS}_k(\Gamma)$ respectively (cf. Lemma 2.15).

Lemma 2.8. *If $h : \mathcal{H} \to \mathbb{C}$ is a C^∞-function, then $(\delta_k^r h)|_{k+2r}\gamma = \delta_k^r(h|_k\gamma)$, for all $\gamma \in \mathrm{GL}_2^+(\mathbb{R})$.*

Proof. By induction on r, it is enough to prove the lemma for $r = 1$ and for all $k \in \mathbb{C}$, that is,

$$(\delta_k h)|_{k+2}\gamma = \delta_k(h|_k\gamma).$$

For $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2^+(\mathbb{R})$, the left hand side is given by

$$((\delta_k h)|_{k+2}\gamma)(z) = \frac{1}{2\pi i}\left(\left(\frac{kh}{2i\,\mathrm{Im}(z)} + \frac{\partial h}{\partial z}\right)\Big|_{k+2}\gamma\right)(z)$$

$$= \frac{1}{2\pi i}\left((cz+d)^{-k-2}\frac{k}{2i\mathrm{Im}(\gamma z)}h(\gamma z) + (cz+d)^{-k-2}\frac{\partial h}{\partial z}(\gamma z)\right)$$
$$= \frac{1}{2\pi i}\left((cz+d)^{-k-2}|cz+d|^2\frac{k}{2iy}h(\gamma z) + (cz+d)^{-k-2}\frac{\partial h}{\partial z}(\gamma z)\right).$$

The right hand side is given by

$$\begin{aligned}
&\delta_k(h|_k\gamma)(z)\\
&= \delta_k((cz+d)^{-k}h(\gamma z))\\
&= \frac{1}{2\pi i}\left(\frac{k}{2iy} + \frac{\partial}{\partial z}\right)((cz+d)^{-k}h(\gamma z))\\
&= \frac{1}{2\pi i}\left(\frac{k}{2iy}(cz+d)^{-k}h(\gamma z) - ck(cz+d)^{-k-1}h(\gamma z) + (cz+d)^{-k-2}\frac{\partial h}{\partial z}(\gamma z)\right)\\
&= \frac{1}{2\pi i}\left(\frac{k}{2iy}(cz+d)^{-k-1}h(\gamma z)(cx+ciy+d-2ciy) + (cz+d)^{-k-2}\frac{\partial h}{\partial z}(\gamma z)\right)\\
&= \frac{1}{2\pi i}\left(\frac{k}{2iy}(cz+d)^{-k-2}|cz+d|^2h(\gamma z) + (cz+d)^{-k-2}\frac{\partial h}{\partial z}(\gamma z)\right),
\end{aligned}$$

which proves that $(\delta_k h)|_{k+2}\gamma = \delta_k(h|_k\gamma)$ and completes the proof. □

Let $h : \mathcal{H} \to \mathbb{C}$ be a holomorphic function with $h(z) = \sum_{n=0}^{\infty} a(n)e(nz/N)$. Then $e(-z/N)(h(z) - a_0)$ is holomorphic on $\mathcal{H} \cup \{\infty\}$. Thus, there exists a positive real number C such that

$$|h(z)| \le |h(\infty)| + Ce^{-2\pi y/N} \text{ as } y \to \infty. \tag{2.14}$$

Proposition 2.9. *For $k, r \in \mathbb{N}$, the operator δ_k^r induces a linear map of $\mathbb{C}$-vector spaces $\delta_k^r : M_k(\Gamma) \to \mathcal{N}_{k+2r}^r(\Gamma)$.*

Proof. Clearly δ_k^r is $\mathbb{C}$-linear. So it is enough to show $\delta_k^r(f) \in \mathcal{N}_{k+2r}^r(\Gamma)$, $\forall f \in M_k(\Gamma)$. Let $f \in M_k(\Gamma)$. Recall that

$$\delta_k^r(f) = \sum_{j=0}^{r}\binom{r}{j}\frac{\Gamma(r+k)}{\Gamma(j+k)}(-4\pi y)^{j-r}d^j f.$$

Clearly $d^j f$ is holomorphic and y^{j-r} is smooth. Hence, $\delta_k^r(f)$ satisfies (1) and (3) of Definition 2.7. By Lemma 2.8, it follows that

$$(\delta_k^r f)|_{k+2r}\gamma = \delta_k^r(f|_k\gamma) = \delta_k^r(f), \quad \text{for all } \gamma \in \Gamma, \tag{2.15}$$

hence (2) also holds. It remains to check that $\delta_k^r f$ is slowly increasing. If $\alpha \in \mathrm{SL}_2(\mathbb{Z})$, then $f|_k\alpha$ is also C^∞, so

$$(\delta_k^r f)|_{k+2r}\alpha = \delta_k^r(f|_k\alpha) = \sum_{j=0}^{r}\binom{r}{j}\frac{\Gamma(r+k)}{\Gamma(j+k)}(-4\pi y)^{j-r}d^j(f|_k\alpha).$$

Note that the $(-4\pi y)^{j-r}$ are bounded as $y \to \infty$ and the $d^j(f|_k\alpha)$ are holomorphic. It follows from (2.14) that, for every $0 \le j \le r$, there exists positive numbers A_j, B_j such that $|(-4\pi y)^{j-r} d^j(f|_k\alpha)| \le A_j(1 + e^{-2\pi y/B_j})$ as $y \to \infty$. Since e^{-y} decays faster than y^{-n} for any $n \ge 0$ as $y \to \infty$, we have $|(\delta_k^r f)|_{k+2r}\alpha| \le A_\alpha(1 + y^{-B_\alpha})$ as $y \to \infty$ for some positive numbers A_α, B_α. □

Now we will show that $E_k(z, s; \chi, \chi_0)$ is a nearly holomorphic modular form if χ is a Dirichlet character modulo N and $s \le 0$ is an integer such that $k + 2s > 2$. To prove this, we need to consider the action of the Maass-Shimura operator on Eisenstein series. Observe that for k, r positive integers and $s \le 0$ an integer such that $k+2s > 2$, we have

$$\begin{aligned}
\delta_k^r(y^s) &= \sum_{j=0}^{r} \binom{r}{j} \frac{\Gamma(k+r)}{\Gamma(k+j)} (-4\pi y)^{j-r} d^j y^s \\
&= \sum_{j=0}^{r} \binom{r}{j} \frac{\Gamma(k+r)}{\Gamma(k+j)} (-4\pi y)^{j-r} \left(\frac{-1}{4\pi}\right)^j \frac{\Gamma(s+1)}{\Gamma(s-j+1)} y^{s-j} \\
&= (-4\pi)^{-r} y^{s-r} r! \sum_{j=0}^{r} \binom{k+r-1}{r-j} \binom{s}{j} \\
&= (-4\pi)^{-r} \frac{\Gamma(s+k+r)}{\Gamma(s+k)} y^{s-r},
\end{aligned} \tag{2.16}$$

where the last equality follows by comparing the coefficient of X^r in $(1+X)^s(1+X)^{k+r-1}$ and $(1+X)^{s+k+r-1}$.

For $(c, d) \in \mathbb{Z}^2 \backslash \{(0, 0)\}$, let $\gamma = \left(\begin{smallmatrix} d & -c \\ c & d \end{smallmatrix}\right)$. Since $y^s|_k\gamma = (cz+d)^{-k}|cz+d|^{-2s} y^s$, we have

$$\begin{aligned}
&\delta_k^r((cz+d)^{-k}|cz+d|^{-2s} y^s) \\
&\quad = \delta_k^r(y^s|_k\gamma) = \delta_k^r(y^s)|_{k+2r}\gamma \qquad \text{(By Lemma 2.8)} \\
&\quad \overset{(2.16)}{=} (-4\pi)^{-r} \frac{\Gamma(s+k+r)}{\Gamma(s+k)} (y^{s-r})|_{k+2r}\gamma \\
&\quad = (-4\pi)^{-r} \frac{\Gamma(s+k+r)}{\Gamma(s+k)} (cz+d)^{-k-2r} |cz+d|^{-2(s-r)} y^{s-r}.
\end{aligned}$$

Let χ be a Dirichlet character modulo N. Multiplying both sides of the equation above by $\chi(c)$ and then taking the sum over all $(c, d) \in \mathbb{Z}^2 \backslash \{(0, 0)\}$ (ignoring convergence issues) we get

$$(-4\pi)^r \frac{\Gamma(s+k)}{\Gamma(s+k+r)} \delta_k^r(E_k(z, s; \chi, \chi_0)) = E_{k+2r}(z, s-r; \chi, \chi_0). \tag{2.17}$$

From [Miy89, Chapter 7] we know that if $k \ge 3$, $E_k(z, 0; \chi, \chi_0) = \sum'_{c,d} \chi(c)(cz+d)^{-k}$ is a usual holomorphic modular form in $M_k(N, \chi)$. It follows from (2.17) and Proposition 2.9 that for all integers $r \geq 0$ and $k \geq 3$:

$$E_{k+2r}(z, -r; \chi, \chi_0) \in \mathcal{N}^r_{k+2r}(N, \chi).$$

A similar argument for the Eisenstein series $E_{k,N}(z, 0, \overline{\chi}) \in M_k(N, \chi)$, $k \geq 3$ (cf. (2.9)), gives:

Proposition 2.10. *Let k, r be integers such that $0 \leq r < k/2 - 1$. If χ is a Dirichlet character mod N, then $E_k(z, -r; \chi, \chi_0)$, $E_{k,N}(z, -r, \overline{\chi}) \in \mathcal{N}^r_k(N, \chi)$.*

Theorem 2.11. ([Hid93, §10.1, Theorem 1]) *Suppose that $r \geq 0$ and $k \geq 1$. If $f \in \mathcal{N}^r_{k+2r}(N, \chi)$, then*

$$f = \sum_{j=0}^{r} \delta^j_{k+2r-2j} h_j, \text{ where } h_j \in M_{k+2r-2j}(N, \chi). \tag{2.18}$$

More precisely,

$$\mathcal{N}^r_{k+2r}(N, \chi) \cong \oplus^r_{j=0} M_{k+2r-2j}(N, \chi),$$

$$\mathcal{N}S^r_{k+2r}(N, \chi) \cong \oplus^r_{j=0} S_{k+2r-2j}(N, \chi),$$

and the isomorphism is obtained via $f \mapsto (h_j)$, where h_j are as in (2.18). *Moreover these isomorphisms are equivariant under the $|_k$ action of* $\mathrm{GL}_2^+(\mathbb{R})$.

The projection $f \mapsto h_0$ induces a map

$$\mathcal{H}ol : \mathcal{N}^r_{k+2r}(N, \chi) \to M_{k+2r}(N, \chi), \tag{2.19}$$

which is called the holomorphic projection.

Lemma 2.12. *Let $f \in S_k(N, \psi)$ and let $g : \mathcal{H} \to \mathbb{C}$ be a smooth function which is slowly increasing such that $g|_k\gamma = \psi(\gamma)g$ for every $\gamma \in \Gamma_0(N)$. Then $\langle f, g\rangle_N := \int_{\mathcal{H}/\Gamma_0(N)} \overline{f(z)} g(z) y^{k-2} dxdy$ converges.*

Proof. This follows from Lemma 2.15 (1) below and [Hid93, §9.3, (6)]. □

Lemma 2.13. *Suppose $f \in S_k(N, \chi)$ and $g \in \mathcal{N}^r_k(N, \chi)$. If $r < k/2$, then $\langle f, g\rangle_N = \langle f, \mathcal{H}ol(g)\rangle_N$. Further, if $g \in \mathcal{N}S^r_k(N, \chi)$, then $\mathcal{H}ol(g)$ is the unique cusp form with the property $\langle f, g\rangle_N = \langle f, \mathcal{H}ol(g)\rangle_N$, $\forall\, f \in S_k(N, \chi)$.*

Proof. The first part follows from [Hid93, §10.1, Corolllary 1]. By Theorem 2.11, we have $\mathcal{H}ol(g) \in S_k(N, \chi)$. Now the first part shows that $\mathcal{H}ol(g)$ satisfies the required property. From Lemma 2.12, we have $f \mapsto \langle f, g\rangle_N$ defines an anti-linear functional on $S_k(N, \chi)$. The uniqueness statement follows from the fact that Petersson inner product induces a non-degenerate pairing $\langle\ ,\ \rangle_N : S_k(N, \chi) \times S_k(N, \chi) \to \mathbb{C}$. □

Lemma 2.14. (Holomorphic Projection lemma) [Zag92, Appendix C] *Let Γ be a congruence subgroup and let $\Phi : \mathcal{H} \to \mathbb{C}$ be a smooth function satisfying:*

(1) $\Phi|_k\gamma = \Phi$, $\forall\, \gamma \in \Gamma$ *and* $\forall\, z \in \mathcal{H}$,
(2) $\Phi(z) = c_0 + O(y^{-\epsilon})$ *as* $y = \mathrm{Im}(z) \to \infty$,

for some integer $k > 2$ *and numbers* $c_0 \in \mathbb{C}$ *and* $\epsilon > 0$. *If* $\Phi(z) = \sum_{n=0}^{\infty} c_n(y)e(nx)$, *then the function* $\phi(z) := \sum_{n=0}^{\infty} c_n e(nz)$ *with*

$$c_n = \frac{(4\pi n)^{k-1}}{(k-2)!} \int_0^{\infty} c_n(y) e^{-2\pi n y} y^{k-2} dy$$

for $n > 0$ *belongs to* $M_k(\Gamma)$ *and satisfies* $\langle f, \phi\rangle_\Gamma = \langle f, \Phi\rangle_\Gamma$, $\forall\, f \in S_k(\Gamma)$.

Any rapidly decreasing function $\Phi : \mathcal{H} \to \mathbb{C}$ which satisfies hypothesis (1) of Lemma 2.14, automatically satisfies hypothesis (2) with $c_0 = 0$. For such Φ, we set

$$\mathcal{H}ol(\Phi) := \phi,$$

where ϕ is as defined in Lemma 2.14. It is easy to see that ϕ is a cusp form. Recall that the elements of $\mathcal{N}S_k^r(N, \chi)$ are rapidly decreasing. The definition of $\mathcal{H}ol$ given just above in fact extends the definition of the holomorphic projection $\mathcal{H}ol$ given in (2.19), by the uniqueness part of Lemma 2.13.

We now state a result which will enable one to apply the lemma above.

Lemma 2.15. *Let* k, N *be a positive integers and* χ *a Dirichlet character mod* N. *Then*

(1) *If* $h \in S_k(N, \chi)$, *then* $|(h|_k\gamma)(z)| = O(y^{-B})$, *for all positive real numbers* B *and all* $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, *as* $y \to \infty$. *In particular* h *is rapidly decreasing.*
(2) *For any compact set* $T \subset \mathbb{R}$ *and* $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, *there exists positive real numbers* A *and* B *such that if* $\chi \neq \chi_0$

$$|E_k(z, s; \chi, \chi_0)|_k\gamma| \le A(1 + y^{-B}), \quad \text{as } y \to \infty \text{ as long as } \mathrm{Re}(z) \in T.$$

Proof. Observe that if $h \in S_k(N, \chi)$, then h vanishes at the cusps. Now the first part of the lemma follows from (2.14). For the second part see [Hid93, §9.3, Lemma 3]. □

It follows from Lemma 2.15 that if h is a (holomorphic) cusp form of weight $2 \le l < k$ (in our application below h will be the slash of a twist of g from the Introduction), then $h(z)E_{k-l}(z, s; \chi, \chi_0)$ has weight $k > 2$ and satisfies the hypotheses of Lemma 2.14, with $c_0 = 0$. So $\mathcal{H}ol(h(z)E_{k-l}(z, s; \chi, \chi_0))$ is defined, and we can calculate its Fourier expansion using Lemma 2.14 if we know the Fourier expansion of $h(z)E_{k-l}(z, s; \chi, \chi_0)$.

3. Distributions and Measures

In this section, we define distributions and measures following [Pan88]. Most of the material covered in this section can also be found in [Was97, MSD74]. Finally, we state the abstract Kummer congruences which is the key tool used in the construction of the p-adic L-function.

3.1 *Distributions*

Let Y be a compact, Hausdorff and totally disconnected topological space. Then Y is a projective limit of finite discrete spaces Y_i,

$$Y = \varprojlim Y_i, \tag{3.1}$$

with respect to transition maps $\pi_{ij} : Y_i \to Y_j$, for $i \geq j$, i, j in some directed set I. We assume that the π_{ij} are surjections, so the canonical maps $\pi_i : Y \to Y_i$ are projections. Let R be a commutative ring and let $\mathrm{Step}(Y, R)$ be the set of R-valued locally constant functions on Y.

Definition 3.1. *A distribution on Y with values in an R-module $\mathcal{A}$ is a homomorphism of R-modules*

$$\mu : \mathrm{Step}(Y, R) \to \mathcal{A}.$$

We use the notation

$$\mu(\varphi) = \int_Y \varphi \, d\mu = \int_Y \varphi(y) \, d\mu(y),$$

for $\varphi \in \mathrm{Step}(Y, R)$. Any distribution μ can be given by a system of functions $\{\mu^{(i)} : Y_i \to \mathcal{A}\}$, satisfying the following finite additivity condition:

$$\mu^{(j)}(y) = \sum_{x \in \pi_{ij}^{-1}(y)} \mu^{(i)}(x), \ \forall\, y \in Y_j, \ x \in Y_i, \ i \geq j. \tag{3.2}$$

Indeed, given such a system of functions $\{\mu^{(i)} : Y_i \to \mathcal{A} \mid i \in I\}$, if $\delta_{i,x}$ is the characteristic function of the inverse image $\pi_i^{-1}(x) \subset Y$, for $x \in Y_i$, define

$$\mu(\delta_{i,x}) = \mu^{(i)}(x)$$

and extend the definition of μ to all of $\mathrm{Step}(Y, R)$ by linearity. Conversely, given a distribution μ, in order to construct such a system, set $\mu^{(i)}(x) = \mu(\delta_{i,x}) \in \mathcal{A}$, $\forall\, x \in Y_i$.

It can be checked that a system of functions $\{\mu^{(i)} : Y_i \to \mathcal{A}\}$ satisfies (3.2) if and only if for all $j \in I$ and all $\varphi_j : Y_j \to R$,

$$\text{the sum } \sum_{x \in Y_i} \varphi_i(x)\mu^{(i)}(x) \text{ does not depend on } i, \ \forall\, i \geq j, \tag{3.3}$$

where $\varphi_i := \varphi_j \circ \pi_{ij} : Y_i \to R$. If μ is the corresponding distribution and $\varphi = \varphi_j \circ \pi_j \in \mathrm{Step}(Y, R)$, then $\mu(\varphi)$ is just the sum above. If $Y = G = \varprojlim G_i$ is a profinite abelian group and R is an integral domain containing all roots of unity of order dividing the cardinality of G (perhaps a transfinite cardinal, in which case R contains all roots of unity), then one needs to verify (3.3) only for all characters of finite order $\chi : G \to R^\times$, since the orthogonality relations imply that their linear span over $R \otimes \mathbb{Q}$ coincides with $\mathrm{Step}(Y, R \otimes \mathbb{Q})$ (see [MSD74]).

Example 3.2. Let p be an odd prime. Then $\mathbb{Z}_p^\times = \varprojlim (\mathbb{Z}/p^n\mathbb{Z})^\times$. We consider

$$X_p = X(\mathbb{Z}_p^\times) = \mathrm{Hom}_{\mathrm{cont}}(\mathbb{Z}_p^\times, \mathbb{C}_p^\times), \; \mathcal{B} = \{\chi \in X(\mathbb{Z}_p^\times) \mid \chi \text{ has finite order}\}.$$

We claim that $\mathcal{B}$ is a basis for Step $(\mathbb{Z}_p^\times, \mathbb{C}_p)$ as a $\mathbb{C}_p$-vector space. For every $x \in (\mathbb{Z}/p^n\mathbb{Z})^\times$, let $\delta_{n,x}$ be the characteristic function of the basic open set $\{a \in \mathbb{Z}_p^\times \mid a \equiv x \bmod p^n\}$. Then, by the orthogonality relations, we have

$$\delta_{n,x} = \frac{1}{\varphi(p^n)} \sum_{\chi \in X((\mathbb{Z}/p^n\mathbb{Z})^\times)} \bar{\chi}(x)\, \chi .$$

Since every locally constant function $\mathbb{Z}_p^\times \to \mathbb{C}_p$ is a $\mathbb{C}_p$-linear combination of characteristic functions, we see that $\mathcal{B}$ spans Step$(\mathbb{Z}_p^\times, \mathbb{C}_p)$. For linear independence, let $\chi_1, \ldots, \chi_n \in \mathcal{B}$ and suppose $\sum_{i=1}^n a_i \chi_i = 0$, with $a_i \in \mathbb{C}_p$. By choosing m sufficiently large we may assume $\chi_i \in X((\mathbb{Z}/p^m\mathbb{Z})^\times)$, for all i. By linear independence of characters, we have $a_i = 0$, for all i.

3.2 *Measures*

Let R be a topological ring with topology induced by a norm. Let $\mathcal{C}(Y, R)$ denote the R-module of continuous R-valued functions on Y and equip $\mathcal{C}(Y, R)$ with the corresponding sup norm topology. In this article we will take $R = \mathbb{C}$ (or) $\mathbb{C}_p$ (or) $\mathcal{O}_p := \{x \in \mathbb{C}_p \mid |x|_p \le 1\}$.

Definition 3.3. *A measure on Y with values in a topological R-module $\mathcal{A}$ is a continuous homomorphism of R-modules $\mu : \mathcal{C}(Y, R) \to \mathcal{A}$.*

The restriction of a measure μ to the R-submodule Step$(Y, R) \subset \mathcal{C}(Y, R)$ is a distribution, which we denote by the same symbol. Since Y is compact, we have Step(Y, R) is dense in $\mathcal{C}(Y, R)$. So every measure is uniquely determined by its values on Step(Y, R). We take for R a closed subring of $\mathbb{C}_p$, and let $\mathcal{A}$ be a complete R-module with topology induced by a norm $|\cdot|_{\mathcal{A}}$ on $\mathcal{A}$. We further assume that $|\cdot|_{\mathcal{A}}$ is compatible with $|\cdot|_p$, i.e., $|ra|_{\mathcal{A}} = |r|_p |a|_{\mathcal{A}}$, for all $r \in R$ and $a \in \mathcal{A}$. Then the condition that a distribution $\{\mu^{(i)} : Y_i \to \mathcal{A}\}$ gives rise to an $\mathcal{A}$-valued measure on Y is equivalent to the condition that the $\mu^{(i)}$ are bounded, i.e., there is a uniform constant $B > 0$ such that for all $i \in I$ and all $x \in Y_i$, we have $|\mu^{(i)}(x)|_{\mathcal{A}} < B$. The proof of this fact is easy using the non-archimedean property and completeness of the norm $|\cdot|_{\mathcal{A}}$ (see [Was97, Proposition 12.1]). In particular, if $\mathcal{A} = R = \mathcal{O}_p = \{x \in \mathbb{C}_p \mid |x|_p \le 1\}$ is the ring of integers of $\mathbb{C}_p$, then distributions are the same as measures. The most important tool in the construction of the p-adic L-function is the following criterion for the existence of a measure with prescribed properties.

Theorem 3.4. (The abstract Kummer congruences) ([Kat78, Proposition 4.0.6], [CP04]) *Let $\{f_i\}$ be a system of continuous $\mathcal{O}_p$-valued functions on Y such that the $\mathbb{C}_p$-linear span of $\{f_i\}$ is dense in $\mathcal{C}(Y, \mathbb{C}_p)$. Let $\{a_i\}$ be any system of* *elements with $a_i \in \mathcal{O}_p$. Then the existence of an $\mathcal{O}_p$-valued measure μ on Y (i.e., $\mu(\mathcal{C}(Y, \mathcal{O}_p)) \subset \mathcal{O}_p$) with the property that*

$$\int_Y f_i \, d\mu = a_i$$

is equivalent to the following: for an arbitrary choice of elements $b_i \in \mathbb{C}_p$, almost all of which vanish, and any $n \geq 0$, we have the following implication of congruences:

$$\sum_i b_i f_i(y) \in p^n \mathcal{O}_p, \ \forall \, y \in Y \implies \sum_i b_i a_i \in p^n \mathcal{O}_p. \tag{3.4}$$

Proof. The necessity is obvious. Indeed if $\sum_i b_i f_i(y) \in p^n \mathcal{O}_p$, then

$$\sum_i b_i a_i = \sum_i \int_Y b_i f_i \, d\mu$$
$$= p^n \int_Y \left(p^{-n} \sum_i b_i f_i \right) d\mu \ \in p^n \mathcal{O}_p.$$

In order to prove the sufficiency we need to construct a measure μ from the numbers a_i. For a function $f \in \mathcal{C}(Y, \mathcal{O}_p)$ and a positive integer n, there exists $b_i \in \mathbb{C}_p$ such that $b_i = 0$ for almost all i, and

$$f - \sum_i b_i f_i \in \mathcal{C}(Y, p^n \mathcal{O}_p)$$

by the density of the $\mathbb{C}_p$-span of the $\{f_i\}$ in $\mathcal{C}(Y, \mathbb{C}_p)$. We now claim that the value $\sum_i b_i a_i$ belongs to $\mathcal{O}_p$ and is well defined modulo p^n, i.e., it doesn't depend on the choice of b_i. Since $f \in \mathcal{C}(Y, \mathcal{O}_p)$, clearly $\sum_i b_i f_i \in \mathcal{C}(Y, \mathcal{O}_p)$. Therefore, by (3.4), we have $\sum_i b_i a_i \in \mathcal{O}_p$. Let $c_i \in \mathbb{C}_p$ be another set of numbers with $c_i \neq 0$ only for finitely many i such that $f - \sum_i c_i f_i \in \mathcal{C}(Y, p^n \mathcal{O}_p)$. Then

$$\sum_i (c_i - b_i) f_i = \left(f - \sum_i b_i f_i \right) - \left(f - \sum_i c_i f_i \right) \in \mathcal{C}(Y, p^n \mathcal{O}_p).$$

By (3.4), we have $\sum_i c_i a_i \equiv \sum_i b_i a_i \mod p^n \mathcal{O}_p$. Therefore, $\sum_i b_i a_i$ is well defined modulo p^n. We denote this value by $\int_Y f d\mu \mod p^n$. Further, the above argument shows $(\int_Y f d\mu \mod p^{n+1}) \equiv (\int_Y f d\mu \mod p^n) \mod p^n \mathcal{O}_p$. So we may define μ on $\mathcal{C}(Y, \mathcal{O}_p)$ by

$$\int_Y f \, d\mu = \left\{ \left(\int_Y f \, d\mu \bmod p^n \right) \right\}_{n \geq 1} \in \varprojlim \mathcal{O}_p / p^n \mathcal{O}_p = \mathcal{O}_p.$$

Since every element of $\mathcal{C}(Y, \mathbb{C}_p)$ is bounded, by rescaling, the above definition of μ extends to all of $\mathcal{C}(Y, \mathbb{C}_p)$. A check shows $\mu : \mathcal{C}(Y, \mathbb{C}_p) \to \mathbb{C}_p$ is a continuous linear map, so μ is an $\mathcal{O}_p$-valued measure. Clearly $\int_Y f_i \, d\mu = a_i$. □

Recall that $X_p = \mathrm{Hom}_{\mathrm{cont}}(\mathbb{Z}_p^\times, \mathbb{C}_p^\times)$ has an analytic structure described in the Introduction. If $\mu : \mathcal{C}(\mathbb{Z}_p^\times, \mathbb{C}_p) \to \mathbb{C}_p$ is a measure, then the non-archimedean Mellin transform of μ, defined by

$$L_\mu(\chi) = \mu(\chi) = \int_{\mathbb{Z}_p^\times} \chi \, d\mu, \ \forall \chi \in X_p, \tag{3.5}$$

gives a bounded $\mathbb{C}_p$-analytic function $L_\mu : X_p \longrightarrow \mathbb{C}_p$ (see [MSD74, §7.4], [Man73, Theorem 8.7]). Here 'analytic' means that the integral (3.5) depends analytically on the parameter $\chi \in X_p$. The converse is also true: any bounded $\mathbb{C}_p$-analytic function on X_p is the Mellin transform of some measure μ. These measures with the convolution operation form an algebra, which essentially coincides with the Iwasawa algebra (see [CP04, §(1.4.3), §(1.5.2)]).

4. Construction of Complex-valued Distributions

From now on, let f and g be the primitive cusp forms as in the Introduction. In this section we define two complex-valued distributions associated to f and g and compare them.

Let p be a prime as in the Introduction. The p-stabilization of f is defined by

$$f_0(z) = f(z) - \alpha'(p) f(pz) = f(z) - \alpha'(p)(f|V_p)(z), \tag{4.1}$$

where as before $f(z) = \sum_{n=1}^{\infty} a(n, f)e(nz) \in S_k(C_f, \psi)$. Let $f_0(z) = \sum_{n=1}^{\infty} a(n, f_0)e(nz)$ be the Fourier expansion of f_0. Comparing the Fourier coefficients in (4.1), we get $a(n, f_0) = a(n, f) - \alpha'(p)a(n/p, f)$. Hence, we have the following identity for the corresponding Dirichlet series:

$$\begin{aligned} L(s, f_0) &= \sum_{n=1}^{\infty} a(n, f_0) n^{-s} \\ &= (1 - \alpha'(p)p^{-s}) \left(\sum_{n=1}^{\infty} a(n, f) n^{-s} \right) = (1 - \alpha'(p)p^{-s}) L(s, f). \end{aligned} \tag{4.2}$$

From (4.1), it follows that $f_0 \in S_k(pC_f, \psi)$ and from (2.8) and (4.2), we have

$$\begin{aligned} L(s, f_0) &= (1 - \alpha'(p)p^{-s}) \left(\prod_{q \text{ prime}} (1 - \alpha(q)q^{-s})^{-1} (1 - \alpha'(q)q^{-s})^{-1} \right) \\ &= (1 - \alpha(p)p^{-s})^{-1} \left(\sum_{\substack{n=1 \\ p \nmid n}}^{\infty} a(n, f) n^{-s} \right). \end{aligned} \tag{4.3}$$

Thus we have the following multiplicative relation

$$a(p^r n, f_0) = \alpha(p^r) a(n, f_0) = \alpha(p)^r a(n, f_0), \ \forall\, r, n \geq 0. \tag{4.4}$$

Hence, f_0 is a U_p-eigenvector with eigenvalue $\alpha(p)$, i.e., $f_0|U_p = \alpha(p) f_0$.

Recall $g \in S_l(N, \omega)$. From the definition of the operators w_d and V_d given in Section 2.2, one checks that

$$g|w_{AB} = A^{l/2} g|w_B V_A, \tag{4.5}$$

where A, B are positive integers.

Recall that complex valued Dirichlet characters χ of p-power conductor are the same as finite order characters $\chi : \mathbb{Z}_p^\times \to \mathbb{C}^\times$. As in Example 3.2, we have $\mathcal{B} = \{\chi : \mathbb{Z}_p^\times \to \mathbb{C}^\times \text{ of finite order}\}$ forms a basis of $\mathrm{Step}(\mathbb{Z}_p^\times, \mathbb{C})$. Therefore every complex-valued function on $\mathcal{B}$ extends to a complex-valued distribution on $\mathbb{Z}_p^\times$.

Let $\chi : \mathbb{Z}_p^\times \to \mathbb{C}^\times$ be a Dirichlet character of conductor C_χ. Then $g(\chi) = \sum_{n=1}^{\infty} \chi(n) b(n) e(nz)$ lies in $S_l(C_g C_\chi^2, \omega\chi^2)$, where here and below we use the convention that $\chi(n) = 0$ if $n \in p\mathbb{Z}$.

For every $s \in \mathbb{C}$, define a quantity $\Psi_s^{(M')}(\chi)$ as follows:

$$\Psi_s^{(M')}(\chi) = \frac{(pM')^{s-l/2} C_f^{s-l/2} \overline{\chi}(C_g)}{\Lambda(g)\alpha(pM')} \cdot \frac{\Psi(s, f_0|V_{C_f}, g(\chi)|w_{C_0 M'})}{\pi^{1-l}\langle f, f\rangle_{C_f}}, \tag{4.6}$$

where C_0, M' are natural numbers satisfying:

$$C_0 = pC = pC_f C_g, \;\; p^2 C_\chi^2 | M' \text{ and } S(M') = \{p\}. \tag{4.7}$$

A priori, the definition of $\Psi_s^{(M')}(\chi)$ depends on M', though we show below that it does not, whence $\Psi_s^{(M')}$ extends to a (well-defined) complex-valued distribution on $\mathbb{Z}_p^\times$. To do this, for each $s \in \mathbb{C}$, consider the complex-valued distribution Ψ_s on $\mathbb{Z}_p^\times$ whose value on the Dirichlet character $\chi : \mathbb{Z}_p^\times \to \mathbb{C}^\times$ is given by:

$$\Psi_s(\chi) := \frac{\omega(C_\chi) G(\chi)^2 C_\chi^{2s-l-1}}{\alpha(C_\chi)^2} \cdot \frac{\Psi(s, f, g^\rho(\overline{\chi}))}{\pi^{1-l}\langle f, f\rangle_{C_f}}. \tag{4.8}$$

Proposition 4.1. *Let p be an odd prime for which f is a p-ordinary form. Then for every Dirichlet character $\chi : \mathbb{Z}_p^\times \to \mathbb{C}^\times$ and positive integer M' such that $p^2 C_\chi^2 \mid M'$ and $S(M') = \{p\}$, we have*

$$\Psi_s^{(M')}(\chi) = \Psi_s(\chi).$$

In particular, $\Psi_s^{(M')}$ does not depend on M'.

Proof. First we simplify the right side of (4.6). From (1.2) and (1.3) it follows that

$$\Psi(s, f_0|V_{C_f}, g(\chi)|w_{C_0 M'}) = (2\pi)^{-2s}\Gamma(s)\Gamma(s-l+1) L_{pC}(2s+2-k-l, \overline{\psi\omega\chi^2})$$
$$\times L(s, f_0|V_{C_f}, g(\chi)|w_{C_0 M'}), \tag{4.9}$$

noting that $S(pC) = S(C_0 M')$, for the joint level $C_0 M'$ of the forms $f_0|V_{C_f}$ and $g(\chi)|w_{C_0 M'}$. We define $A(n)$ and $B(n)$ to be the coefficients in the Dirichlet series

$$L(s, f_0) = \sum_{n=1}^{\infty} A(n) n^{-s},$$

$$L(s, g(\chi)|w_{p^2C_gC_\chi^2}) = \sum_{n=1}^{\infty} B(n)n^{-s}. \tag{4.10}$$

Then, by the multiplicative property (4.4), we have

$$A(Mn) = \alpha(M)A(n), \quad \text{for all } M \text{ such that } S(M) = \{p\}. \tag{4.11}$$

Let M_1 be such that $M' = pC_\chi^2 M_1$. Applying (4.5) with $A = M_1C_f$ and $B = p^2C_gC_\chi^2$, we get

$$\begin{aligned} g(\chi)|w_{C_0M'} = g(\chi)|w_{M_1C_fp^2C_gC_\chi^2} &= (M_1C_f)^{l/2}g(\chi)|w_{p^2C_gC_\chi^2}V_{M_1C_f} \\ &= (M_1C_f)^{l/2}\sum_{n=1}^{\infty} B(n)e(M_1C_fnz). \end{aligned} \tag{4.12}$$

We transform the last L-function in (4.9) as follows:

$$\begin{aligned} L(s, f_0|V_{C_f}, g(\chi)|w_{C_0M'}) &\overset{(4.12)}{=} (M_1C_f)^{l/2}\sum_{n=1}^{\infty} A(nC_f^{-1})B(nM_1^{-1}C_f^{-1})n^{-s} \\ &= (M_1C_f)^{l/2}\sum_{n=1}^{\infty} A(nM_1)B(n)(nM_1C_f)^{-s} \\ &\overset{(4.11)}{=} (M_1C_f)^{l/2-s}\alpha(M_1)\sum_{n=1}^{\infty} A(n)B(n)n^{-s} \\ &= (M_1C_f)^{l/2-s}\alpha(M_1)L(s, f_0, g(\chi)|w_{p^2C_gC_\chi^2}) \\ &= \frac{\alpha(M')}{\alpha(pC_\chi^2)} \cdot \left(\frac{M'C_f}{pC_\chi^2}\right)^{l/2-s} L(s, f_0, g(\chi)|w_{p^2C_gC_\chi^2}). \end{aligned} \tag{4.13}$$

If we substitute (4.13) in (4.6), we see that (4.6) does not depend on M'. In order to obtain the more precise expression given by (4.8), it is enough to establish the following equality:

$$\Psi(s, f_0, g(\chi)|w_{p^2C_gC_\chi^2}) = \alpha(p)^2p^{l-2s}\Lambda(g(\chi))\Psi(s, f, g^\rho(\overline{\chi})), \tag{4.14}$$

where $\Lambda(g(\chi))$ is the root number associated to $g(\chi)$, i.e., $g(\chi)|w_{C_gC_\chi^2} = \Lambda(g(\chi))g^\rho(\overline{\chi})$, since by (2.7), we have $\Lambda(g(\chi)) = \omega(C_\chi)\chi(C_g)G(\chi)^2C_\chi^{-1}\Lambda(g)$.

To derive (4.14) we find an appropriate expression for $g(\chi)|w_{p^2C_gC_\chi^2}$. Applying (4.5) once more with $A = p^2$ and $B = C_gC_\chi^2$, we get

$$g(\chi)|w_{p^2C_gC_\chi^2} = p^lg(\chi)|w_{C_gC_\chi^2}V_{p^2} = p^l\Lambda(g(\chi))g^\rho(\overline{\chi})|V_{p^2},$$

so that

$$L(s, f_0, g(\chi)|w_{p^2 C_g C_\chi^2}) = p^l \Lambda(g(\chi)) L(s, f_0, g^\rho(\overline{\chi})|V_{p^2}).$$

A computation similar to that of (4.13) shows that

$$\begin{aligned} L(s, f_0, g^\rho(\overline{\chi})|V_{p^2}) &= p^{-2s} L(s, f_0|U_{p^2}, g^\rho(\overline{\chi})) \\ &= \alpha(p^2) p^{-2s} L(s, f_0, g^\rho(\overline{\chi})), \end{aligned}$$

where we used $f_0|U_p = \alpha(p) f_0$ in the last step. Therefore

$$\Psi(s, f_0, g(\chi)|w_{p^2 C_g C_\chi^2}) = \alpha(p)^2 \Lambda(g(\chi)) p^{l-2s} \Psi(s, f_0, g^\rho(\overline{\chi})).$$

Substituting this in (4.14) we are reduced to proving

$$\Psi(s, f_0, g^\rho(\overline{\chi})) = \Psi(s, f, g^\rho(\overline{\chi})).$$

From (4.1), it follows that

$$\begin{aligned} L(s, f_0, g^\rho(\overline{\chi})) &= L(s, f, g^\rho(\overline{\chi})) - \alpha'(p) L(s, f|V_p, g^\rho(\overline{\chi})) \\ &= L(s, f, g^\rho(\overline{\chi})) \quad (\because \chi(p) = 0). \end{aligned} \tag{4.15}$$

Further, for every character $\chi : \mathbb{Z}_p^\times \to \mathbb{C}^\times$, we have $S(pC_f C_g C_\chi^2) = S(CC_\chi^2)$ (except if χ is the trivial character) so that

$$L_{pC_f C_g C_\chi^2}(2s + 2 - k - l, \overline{\psi\omega\chi^2}) = L_{CC_\chi^2}(2s + 2 - k - l, \overline{\psi\omega\chi^2}) \tag{4.16}$$

in all cases (since if χ is the trivial character, $\chi(p) = 0$). From (4.15) and (4.16), it follows that $\Psi(s, f_0, g^\rho(\overline{\chi})) = \Psi(s, f, g^\rho(\overline{\chi}))$. Thus we obtain (4.14). □

We conclude this section by making an observation on the algebraicity of $\Psi_s^{(M')}$, which will be used in later sections.

Corollary 4.2. *Let $\chi : \mathbb{Z}_p^\times \to \mathbb{C}^\times$ be a finite order character and M' as in Proposition 4.1. Then for every integer s with $l \le s \le k - 1$, we have $\Psi_s^{(M')}(\chi) \in \overline{\mathbb{Q}}$.*

Proof. By Theorem 2.6, we have $\Psi_s(\chi)$ is algebraic for every integer s with $l \le s \le k - 1$. Hence, by the previous proposition, we have $\Psi_s^{(M')}$ is also algebraic for every integer s in the interval $[l, k - 1]$. □

Dirichlet characters actually take values in $\overline{\mathbb{Q}} \subset \mathbb{C}$. Via our fixed embedding $i_p : \overline{\mathbb{Q}} \hookrightarrow \mathbb{C}_p$, we may think of them as $\mathbb{C}_p$-valued. Moreover, by the corollary above we may similarly think of $\Psi_s^{(M')}$ as $\mathbb{C}_p$-valued for $s \in [l, k - 1]$. Thus, for such s, all the measures in this section can (and later will be) thought of as p-adic entities.

5. Integral representation for Distributions

In this section we obtain an integral expression for the distribution $\Psi_s^{(M')}$ given by (4.6) involving the Petersson inner product of certain cusp forms. We also compute the Fourier expansion of one of these cusp forms. This will be needed in the last section in order to explicitly verify the Kummer congruences.

Recall the following classical integral formula of Rankin (cf. (2.11)). For $F \in S_k(N, \psi)$ and $G \in M_l(N, \omega)$, we have

$$\Psi(s, F, G) = 2^{-1}\Gamma(s - l + 1)\pi^{-s}\langle F^\rho, GE(s - k + 1)\rangle_N, \tag{5.1}$$

where

$$F^\rho(z) = \overline{F(-\overline{z})} \in S_k(N, \overline{\psi}),$$

$$E(z, s) = E_{k-l,N}(z, s, \psi\omega) = y^s \sum_{c,d=-\infty}^{\infty}{}' \psi\omega(d)(cNz + d)^{-(k-l)}|cNz + d|^{-2s}.$$

Let $\chi : \mathbb{Z}_p^\times \to \mathbb{C}_p^\times$ be a finite order character. Let M' be as in (4.7), i.e., $p^2C_\chi^2 \mid M'$ and $S(M') = \{p\}$. We apply (5.1) with

$$N = C_0C_fM',$$

$$F = f_0|V_{C_f} \in S_k(pC_f^2, \psi) \subset S_k(C_0C_fM', \psi),$$

$$G = g(\chi)|w_{C_0M'} \in S_l(C_0M', \overline{\omega\chi^2}) \subset S_l(C_0C_fM', \overline{\omega\chi^2}).$$

For every integer s such that $l \leq s \leq k - 1$, we transform the definition of the distribution (4.6) by means of the equality

$$\Psi(s, f_0|V_{C_f}, g(\chi)|w_{C_0M'}) = 2^{-1}\Gamma(s - l + 1)\pi^{-s}\langle f_0^\rho|V_{C_f}, GE(s - k + 1)\rangle_{C_0C_fM'},$$

where $E(z, s - k + 1) = E_{k-l,C_0C_fM'}(z, s - k + 1, \psi\overline{\omega\chi^2})$. If we set

$$K(s) = G \cdot E(z, s),$$

then the formula for the values of the distribution (4.6) takes the form

$$\Psi_s^{(M')}(\chi) = (pM')^{s-l/2}C_f^{s-l/2}\overline{\chi}(C_g)\Lambda(g)^{-1}\alpha(pM')^{-1}$$
$$\times 2^{-1}\Gamma(s - l + 1)\pi^{-s}\frac{\langle f_0^\rho|V_{C_f}, K(s - k + 1)\rangle_{C_0C_fM'}}{\pi^{1-l}\langle f, f\rangle_{C_f}}. \tag{5.2}$$

By Lemma 2.3 (with $N = C_0C_f$, $M = M'$, $f = f_0^\rho|V_{C_f}$ and $g = K(s)$), we obtain

$$\langle f_0^\rho|V_{C_f}, K(s)\rangle_{C_0C_fM'} = \langle f_0^\rho|V_{C_f}, Tr_{C_0C_f}^{C_0C_fM'}(K(s))\rangle_{C_0C_f}$$
$$\overset{(2.5)}{=} (-1)^k M'^{1-k/2}\langle f_0^\rho|V_{C_f}, K'(s)|U_{M'}w_{C_0C_f}\rangle_{C_0C_f},$$

where $K'(s) = K(s)|w_{C_0 C_f M'}$. Hence

$$\Psi_s^{(M')}(\chi) = (-1)^k p^{s-l/2} M'^{(2s-l-k+2)/2} C_f^{s-l/2} \overline{\chi}(C_g)\Lambda(g)^{-1}\alpha(pM')^{-1}$$
$$\times 2^{-1}\Gamma(s-l+1)\pi^{-s} \frac{\langle f_0^\rho | V_{C_f}, K'(s-k+1)|U_{M'} w_{C_0 C_f}\rangle_{C_0 C_f}}{\pi^{1-l}\langle f, f\rangle_{C_f}}. \tag{5.3}$$

Now we compute the Fourier coefficients of $K'(s)$ for special values of s (more precisely, for $l-k+1 \le s \le 0$, $s \in \mathbb{Z}$). We rewrite $K'(s)$ as

$$K'(s) = g' \cdot E'(z, s),$$

where

$$g' = g(\chi)|w_{C_0 M'} w_{C_0 C_f M'} \quad \text{and} \quad E'(z, s) = E(z, s)|w_{C_0 C_f M'}.$$

It follows from the definition of $w_{C_0 M'}$, $w_{C_0 C_f M'}$ that

$$g' = (-1)^l C_f^{l/2} g(\chi)|V_{C_f}. \tag{5.4}$$

The Fourier expansion of the Eisenstein series $E'(z, s)$ will be computed in the next section, from which we will obtain the Fourier expansion of $K'(s)$.

5.1 *Fourier expansion of Eisenstein series*

Here we follow [Miy89, §7.2] to compute the Fourier expansion of $E'(z, s)$. The procedure given in [Miy89] describes the Fourier expansion of more general Eisenstein series. Let $\mathcal{H}' = \{z \in \mathbb{C} \mid \mathrm{Re}(z) > 0\}$ denote the right half plane. For $\alpha \in \mathbb{C}$ and $\beta, z \in \mathcal{H}'$, the Whittaker function $W(z; \alpha, \beta)$ is defined by the following integral:

$$W(z; \alpha, \beta) = \Gamma(\beta)^{-1} \int_0^\infty (u+1)^{\alpha-1} u^{\beta-1} e^{-zu}\, du. \tag{5.5}$$

The convergence of the above integral follows from [Miy89, Lemma 7.2.1 (2)].

Lemma 5.1. *The function $W(z; \alpha, \beta)$ can be continued analytically to a holomorphic function on $\mathcal{H}' \times \mathbb{C} \times \mathbb{C}$ satisfying:*

(1) $W(z; \alpha, \beta) = z^{1-\alpha-\beta} W(z; 1-\beta, 1-\alpha)$, $\forall\, (z, \alpha, \beta) \in \mathcal{H}' \times \mathbb{C} \times \mathbb{C}$.
(2) $W(z; \alpha, 0) = 1$, $\forall\, (z, \alpha) \in \mathcal{H}' \times \mathbb{C}$.
(3) $W(y; \alpha, \beta) = \sum_{i=0}^{r} (-1)^i \binom{r}{i} y^{r-i} \frac{\Gamma(\alpha)}{\Gamma(\alpha-i)} W(y; \alpha-i, \beta+r)$, $\forall\, r \ge 0$, $y \in \mathbb{R}^+$, $(\alpha, \beta) \in \mathbb{C} \times \mathbb{C}$.

Proof. Note that $\omega(z; \alpha, \beta)$ defined by [Miy89, (7.2.31)] equals to $z^\beta W(z; \alpha, \beta)$ for all $(z, \alpha, \beta) \in \mathcal{H}' \times \mathbb{C} \times \mathcal{H}'$. The lemma now follows from [Miy89, Theorem 7.2.4 (1)], [Miy89, Lemma 7.2.6] and [Miy89, (7.2.40)]. □

By part (3) of Lemma 5.1, with $\beta = -r$, and by part (2), we obtain for all $y > 0$ that

$$W(y;\alpha,-r) = \sum_{i=0}^{r}(-1)^i\binom{r}{i}\frac{\Gamma(\alpha)}{\Gamma(\alpha-i)}y^{r-i}W(y;\alpha-i,0)$$
$$= \sum_{i=0}^{r}(-1)^i\binom{r}{i}\frac{\Gamma(\alpha)}{\Gamma(\alpha-i)}y^{r-i}. \tag{5.6}$$

Recall that the Eisenstein series $E_k(z,s;\theta,\varphi)$ for θ and φ Dirichlet characters mod L and M respectively is defined by (cf. (2.4))

$$E_k(z,s;\theta,\varphi) = y^s \sum_{c,d=-\infty}^{\infty}{}' \theta(c)\varphi(d)(cz+d)^{-k}|cz+d|^{-2s}.$$

We now state a result about the Fourier expansion of Eisenstein series.

Theorem 5.2. *Let θ and φ be Dirichlet characters mod L and mod M, respectively, satisfying $\theta(-1)\varphi(-1) = (-1)^k$. Then for any integer k, the Eisenstein series $E_k(z,s;\theta,\varphi)$ can be analytically continued to a meromorphic function on the whole s-plane and has the Fourier expansion*

$$\begin{aligned}E_k(z,s;\theta,\varphi) &= C(s)y^s + D(s)y^{1-k-s}\\ &\quad + A(s)y^s\sum_{n=1}^{\infty}a_n(s)(4\pi/M)^s e(nz/M)W(4\pi yn/M;k+s,s)\\ &\quad + B(s)y^s\sum_{n=1}^{\infty}a_n(s)(4\pi/M)^{s+k}e(-n\bar{z}/M)W(4\pi yn/M;s,k+s),\end{aligned}$$

where

$$C(s) = \begin{cases} 2L_M(2s+k,\varphi), & \text{if } \theta = \chi_0,\\ 0, & \text{otherwise,}\end{cases}$$

$$D(s) = \begin{cases} 2\sqrt{\pi}i^{-k}\prod_{p|M}(1-p^{-1})\Gamma(s)^{-1}\Gamma(s+k)^{-1} & \\ \quad\times\Gamma\left(\frac{2s+k-1}{2}\right)\Gamma\left(\frac{2s+k}{2}\right)L_L(2s+k-1,\theta), & \text{if } \varphi \text{ is the trivial character mod } M,\\ 0, & \text{otherwise,}\end{cases}$$

$$A(s) = 2^{k+1}i^{-k}G(\varphi^0)(\pi/M)^{s+k}\Gamma(s+k)^{-1},$$

$$B(s) = 2^{1-k}i^{-k}\varphi(-1)G(\varphi^0)(\pi/M)^s\Gamma(s)^{-1},$$

$$a_n(s) = \sum_{0<c|n}\theta(n/c)c^{k+2s-1}\sum_{0<d|(l,c)}d\mu(l/d)\varphi^0(l/d)\overline{\varphi^0}(c/d).$$

Here φ^0 denotes the primitive character associated with φ of conductor $m_\varphi = M/l$ and μ is the Möbius function.

Proof. This is [Miy89, Theorem 7.2.9], noting that $E_k(z, s; \theta, \varphi)$ differs from the one defined in [Miy89, (7.2.1)] by a factor of y^s and $\omega(y; \alpha, \beta)$ equals $y^\beta W(y; \alpha, \beta)$, $\forall\, (\alpha, \beta) \in \mathbb{C} \times \mathbb{C}$. □

We apply the above theorem to compute the Fourier expansion of $E'(z, s)$. Recall

$$\begin{aligned} E'(z, s) &= E(z, s)|w_{C_0 C_f M'} = E_{k-l, C_0 C_f M'}(z, s, \overline{\psi\omega\chi^2})|w_{C_0 C_f M'} \\ &= (C_0 C_f M')^{-(k-l+2s)/2} E_{k-l}(z, s; \psi\overline{\omega\chi^2}, \chi_0) \quad \text{(by direct computation).} \end{aligned} \tag{5.7}$$

For convenience we introduce the normalized Eisenstein series

$$G^*(z, s) = \frac{(C_0 C_f M')^{(k-l+2s)/2} \Gamma(k-l+s)}{(-2\pi i)^{k-l} \pi^s} E'(z, s) \tag{5.8}$$

$$\overset{(5.7)}{=} \frac{\Gamma(k-l+s)}{(-2\pi i)^{k-l} \pi^s} E_{k-l}(z, s; \psi\overline{\omega\chi^2}, \chi_0). \tag{5.9}$$

If s is an integer such that $s \leq 0$ and $k - l + s > 0$, then from (5.9) and Theorem 5.2, we have

$$\begin{aligned} G^*(z, s) &= \varepsilon(k-l, y, s, \psi\overline{\omega\chi^2}) \\ &\quad + 2(4\pi y)^s \sum_{n=1}^{\infty} \sum_{0<c|n} \psi\overline{\omega\chi^2}(n/c) c^{k-l+2s-1} W(4\pi y n; k-l+s, s) e(nz) \\ &= \varepsilon(k-l, y, s, \psi\overline{\omega\chi^2}) \\ &\quad + 2(4\pi y)^s \sum_{n=1}^{\infty} \sum_{dd'=n} \psi\overline{\omega\chi^2}(d') d^{k-l+2s-1} W(4\pi y n; k-l+s, s) e(nz), \end{aligned} \tag{5.10}$$

where here and below we take $d, d' > 0$ and

$$\varepsilon(k-l, y, s, \psi\overline{\omega\chi^2}) = \frac{\Gamma(k-l+s)}{(-2\pi i)^{k-l} \pi^s} (C(s) y^s + D(s) y^{1-k+l-s}),$$

with $C(s)$, $D(s)$ denoting the same constants as in Theorem 5.2 (corresponding to $\theta = \psi\overline{\omega\chi^2}$, $\varphi = \chi_0$). The term with $\overline{z}$ doesn't appear as for such s we have $B(s) = 0$ because the Gamma function $\Gamma(s)$ in the denominator of $B(s)$ has a pole at $s \leq 0$ and the function $a_n(s) W(4\pi y n/M; k+s, s)$ is holomorphic in s.

5.2 *Integral representation via holomorphic projection*

Taking s equal to $s-k+1 \le 0$ in (5.8), we get[4]

$$E'(z, s-k+1) = (C_0 C_f M')^{-(2s+2-k-l)/2}(-1)^{k-l} i^{k-l} 2^{k-l} \pi^{s-l+1} \times \Gamma(s-l+1)^{-1} G^*(z, s-k+1). \tag{5.11}$$

Substituting (5.11) and (5.4) into (5.3), and substituting $C_0 = pC = pC_f C_g$, we get

$$\begin{aligned}\Psi_s^{(M')}(\chi) &= \frac{2^{k-l-1} i^{k-l} p^{k/2-1} \overline{\chi}(C_g) C_f^{(k+l-2)/2}}{\alpha(pM')\Lambda(g) C^{(2s+2-k-l)/2}} \\ &\quad \cdot \frac{\langle f_0^\rho | V_{C_f}, (g(\chi)|V_{C_f} G^*(z, s-k+1))|U_{M'} w_{C_0 C_f}\rangle_{C_0 C_f}}{\langle f, f\rangle_{C_f}} \\ &= \gamma(M')\langle f, f\rangle_{C_f}^{-1} \langle f_0^\rho |_{V_{C_f}}, K^*(s-k+1)|U_{M'} w_{C_0 C_f}\rangle_{C_0 C_f},\end{aligned} \tag{5.12}$$

in which we have set

$$\begin{aligned}\gamma(M') &= 2^{k-l-1} i^{k-l} p^{k/2-1} C_f^{l-1} C_g^{(l-k)/2} \alpha(pM')^{-1} \Lambda(g)^{-1}, \\ K^*(s) &= C_f^{-s} C_g^{-s} \overline{\chi}(C_g) g(\chi)|V_{C_f} G^*(z, s).\end{aligned} \tag{5.13}$$

Observe that $\gamma(M')$ is an algebraic number. Moreover, $i_p(\gamma(M'))$ is p-integral if $i_p(\Lambda(g))$ is a p-adic unit. One can check this last fact using explicit formulas for the root number in terms of Gauss sums when the automorphic representation attached to g has no supercuspidal local factors; it is apparently also true in general [Hid88, (5.4a), (5.4b)]. In any case $i_p(\gamma(M'))$ is bounded independent of M', which is all we shall need later.

It follows from (5.10) that for integers $l-k < s \le 0$ we have

$$K^*(s) = \sum_{n=1}^{\infty} \sum_{C_f n_1 + n_2 = n} d(n_1, n_2; y, s) e(nz), \tag{5.14}$$

where for $p \mid n$, the Fourier coefficients are given by[5]

$$d(n_1, n_2; y, s) = C_f^{-s} C_g^{-s} \overline{\chi}(C_g) \chi(n_1) b(n_1) \times 2(4\pi y)^s \sum_{n_2 = dd'} \psi\overline{\omega\chi^2}(d') d^{2s+k-l-1} W(4\pi n_2 y, s-l+k, s). \tag{5.15}$$

[4]This formula differs from [Pan88, (4.22)] by $(-1)^{s-k+1}$ and is the source of the sign discrepancy in Theorem 1.1 mentioned in the first footnote. With the sign as in (5.11), it becomes difficult to verify the abstract Kummer congruences needed to prove [Pan88, (5.6)]. Instead, we shall later verify that (6.8) below holds.

[5]The formula differs from [Pan88, (4.27)] by $(-1)^s$ due to the sign error mentioned in the previous footnote.

Here we used that if $p \mid n$, then there is no contribution to the coefficient of $e(nz)$ in $K^*(s)$ from the constant ($n_2 = 0$) term of Eisenstein series $G^*(z,s)$, because the coefficient of $e(C_f n_1 z)$ in $g(\chi)|V_{C_f}$ is zero for $p \mid n_1$ since $\chi(n_1) = 0$.

The expression (5.12) for $\Psi_s^{(M')}(\chi)$ involves $K^*(s-k+1)$ whose Fourier coefficients contain Whittaker functions which are difficult to handle. To get rid of the Whittaker functions we consider its holomorphic projection. We first check that $\mathcal{H}ol(K^*(s-k+1))$ is defined. From Proposition 2.10, it follows that if $(k+l)/2 < s \leq k-1$, then $E_{k-l}(z, s-k+1; \overline{\psi\omega\chi^2}, \chi_0)$ belongs to $\mathcal{N}_{k-l}^{-s+k-1}(C_0C_fM', \overline{\psi\omega\chi^2})$, hence so does $G^*(z, s-k+1)$, by (5.9). Thus $K^*(s-k+1) \in \mathcal{N}S_k^{-s+k-1}(C_0C_fM', \psi)$ if $s > (k+l)/2$. So for such s one can define the holomorphic projection $\mathcal{H}ol(K^*(s-k+1))$ of $K^*(s-k+1)$ in the sense of Theorem 2.11. However, for $l \leq s \leq (k+l)/2$ it is not clear (to us) that $K^*(s-k+1)$ is a nearly holomorphic form. So we cannot use Theorem 2.11 to define the holomorphic projection of $K^*(s-k+1)$ for $l \leq s \leq (k+l)/2$. Nevertheless, by the discussion at the end of §2, we know that $K^*(s)$ is rapidly decreasing and satisfies the hypotheses of Lemma 2.14, with $c_0 = 0$. Thus one can define the holomorphic projection of $K^*(s-k+1)$ for any integer $l \leq s \leq k-1$.

We now study:

$$\widetilde{K}_{M'}(s) := \mathcal{H}ol(K^*(s))|U_{M'},$$

for integers $l-k+1 \leq s \leq 0$. We begin by computing the level and nebentypus of $\widetilde{K}_{M'}(s)$. Since $K^*(s)|_k\gamma = \psi(\gamma)K^*(s)$ for all $\gamma \in \Gamma_0(C_0C_fM')$, we have $\mathcal{H}ol(K^*(s)) \in S_k(C_0C_fM', \psi)$, by the remarks after Lemma 2.14. As $p^2 \mid M'$ we have $\mathcal{H}ol(K^*(s))|U_p \in S_k(C_0C_fM'/p, \psi)$, by Lemma 2.4 (1). Repeatedly applying Lemma 2.4 (1) we get $\mathcal{H}ol(K^*(s))|U_{M'} \in S_k(C_0C_f, \psi)$.

We now state the main result of this section.

Proposition 5.3. *Let the notation be as above. For $s \in \mathbb{Z}$ with $l \leq s \leq k-1$ one has following equality*

$$\Psi_s^{(M')}(\chi) = \gamma(M')\langle f, f\rangle_{C_f}^{-1}\langle f_0^\rho|V_{C_f}, \widetilde{K}_{M'}(s-k+1)|\omega_{C_0C_f}\rangle_{C_0C_f}. \qquad (5.16)$$

Moreover, for $s \in \mathbb{Z}$ with $l-k+1 \leq s \leq 0$ we have

$$\widetilde{K}_{M'}(s) = \sum_{n=1}^{\infty}\sum_{C_f n_1 + n_2 = M'n} d(n_1, n_2; s, \chi)e(nz) \in S_k(C_0C_f, \psi) \qquad (5.17)$$

is a cusp form with algebraic Fourier coefficients given by[6]

$$\begin{aligned} &d(n_1, n_2; s, \chi) \\ &\quad = 2C_f^{-s}C_g^{-s}\overline{\chi}(C_g)\chi(n_1)b(n_1)\sum_{n_2=dd'}\overline{\psi\omega\chi^2}(d')d^{2s+k-l-1}P_s(n_2, M'n) \end{aligned} \qquad (5.18)$$

[6]The formula differs from [Pan88, (4.29)] by the same sign as in the previous footnote.

and

$$P_s(x,y)=\sum_{i=0}^{-s}(-1)^i\binom{-s}{i}\frac{\Gamma(s+k-l)\Gamma(k-i-1)}{\Gamma(s+k-l-i)\Gamma(k-1)}x^{-s-i}y^i$$
$$=x^{-s}+\frac{y}{\Gamma(k-1)}Q_s(x,y),\ \textit{where}\ s\le 0\ \textit{and}\ Q_s(x,y)\in\mathbb{Z}[x,y]. \tag{5.19}$$

Proof. The proof of the lemma is an application of the holomorphic projection lemma (Lemma 2.14). We first note that $\mathcal{H}ol$ commutes with the action of the w_N-operator. Indeed, by Lemma 2.14 and (2.2), we have

$$\langle h,\mathcal{H}ol(\Phi|w_N)\rangle_N=\langle h,\Phi|w_N\rangle_N=\langle h|w_N,\Phi\rangle_N$$
$$=\langle h|w_N,\mathcal{H}ol(\Phi)\rangle_N=\langle h,\mathcal{H}ol(\Phi)|w_N\rangle_N,$$

for all modular rapidly decreasing Φ and all cusp forms h of weight k and level $N\ge 1$, whence $\mathcal{H}ol(\Phi|w_N)=\mathcal{H}ol(\Phi)|w_N$. A similar argument shows that $\mathcal{H}ol$ commutes with the U_p-operator. Thus, by Lemma 2.13 and Lemma 2.14, we have

$$\langle f_0^\rho|V_{C_f},K^*(s-k+1)|U_{M'}w_{C_0C_f}\rangle_{C_0C_f}$$
$$=\langle f_0^\rho|V_{C_f},\mathcal{H}ol(K^*(s-k+1)|U_{M'}w_{C_0C_f})\rangle_{C_0C_f}$$
$$=\langle f_0^\rho|V_{C_f},\mathcal{H}ol(K^*(s-k+1))|U_{M'}w_{C_0C_f}\rangle_{C_0C_f}$$
$$=\langle f_0^\rho|V_{C_f},\widetilde{K}_{M'}(s-k+1)|w_{C_0C_f}\rangle_{C_0C_f}.$$

Substituting the above expression in (5.12), we obtain (5.16). It follows from (5.14), (5.15) that

$$K^*(s)|U_{M'}=M'^{k/2-1}\sum_{u \bmod M'}K^*(s)|\begin{pmatrix}1&u\\0&M'\end{pmatrix}$$
$$\overset{(5.14)}{=}M'^{-1}\sum_{u \bmod M'}\sum_{n=1}^{\infty}\sum_{C_fn_1+n_2=n}d(n_1,n_2;y/M',s)e(n(z+u)/M')$$
$$=\sum_{n=1}^{\infty}\sum_{C_fn_1+n_2=n}d(n_1,n_2;y/M',s)e(nz/M')M'^{-1}\sum_{u \bmod M'}e(un/M')$$
$$=\sum_{n=1}^{\infty}\sum_{C_fn_1+n_2=M'n}d(n_1,n_2;y/M',s)e(nz). \tag{5.20}$$

Now we use Lemma 2.14 to compute the Fourier coefficients of $\widetilde{K}_{M'}(s-k+1)=\mathcal{H}ol(K^*(s-k+1)|U_{M'})$ for $l\le s\le k-1$. Let $s'=s-k+1$ then $l-k+1\le s'\le 0$.

From (5.20) and Lemma 2.14 it follows that

$$\widetilde{K}_{M'}(s') = \sum_{n=1}^{\infty} \sum_{C_f n_1 + n_2 = M'n} \frac{(4\pi n)^{k-1}}{\Gamma(k-1)} \times \left(\int_0^{\infty} d(n_1, n_2; y/M', s') e^{-2\pi n y} e^{-2\pi n y} y^{k-2}\, dy \right) e(nz). \qquad (5.21)$$

Note that if $C_f n_1 + n_2 = M'n$, the quantity $d(n_1, n_2; y/M', s)$ is as in (5.15), with y replaced by y/M', because $p \mid M'n$, since $p \mid M'$. We get

$$\begin{aligned} d(n_1, n_2; s', \chi) &:= \frac{(4\pi n)^{k-1}}{\Gamma(k-1)} \int_0^{\infty} d(n_1, n_2; y/M', s') e^{-4\pi n y} y^{k-2} dy, \\ &= 2(C_f C_g)^{-s'} \overline{\chi}(C_g) \chi(n_1) b(n_1) \sum_{n_2 = dd'} \psi\overline{\omega\chi^2}(d') d^{2s'+k-l-1} \\ &\times \frac{(4\pi n)^{k-1}}{\Gamma(k-1)} \int_0^{\infty} \left(\frac{4\pi y}{M'} \right)^{s'} W\left(\frac{4\pi n_2 y}{M'}, s' + k - l, s' \right) e^{-4\pi n y} y^{k-2} dy. \qquad (5.22) \end{aligned}$$

Since $l - k + 1 \le s' \le 0$, we can use (5.6) to compute $W(4\pi n_2 y/M', s' + k - l, s')$. We obtain

$$\begin{aligned} &\frac{(4\pi n)^{k-1}}{\Gamma(k-1)} \int_0^{\infty} \left(\frac{4\pi y}{M'} \right)^{s'} W\left(\frac{4\pi n_2 y}{M'}, s' + k - l, s' \right) e^{-4\pi n y} y^{k-2} dy \\ &= \sum_{i=0}^{-s'} (-1)^i \binom{-s'}{i} \frac{\Gamma(s' + k - l)}{\Gamma(s' + k - l - i)\Gamma(k-1)} \\ &\quad \times \int_0^{\infty} (4\pi n)^{k-1} \left(\frac{4\pi y}{M'} \right)^{s'} \left(\frac{4\pi n_2 y}{M'} \right)^{-s'-i} e^{-4\pi n y} y^{k-2} dy \\ &= \sum_{i=0}^{-s'} (-1)^i \binom{-s'}{i} \frac{\Gamma(s' + k - l)}{\Gamma(s' + k - l - i)\Gamma(k-1)} n_2^{-s'-i} M'^i \\ &\quad \times \int_0^{\infty} (4\pi n y)^{k-1} (4\pi y)^{-i} e^{-4\pi n y} \frac{dy}{y} \\ &= \sum_{i=0}^{-s'} (-1)^i \binom{-s'}{i} \frac{\Gamma(s' + k - l)}{\Gamma(s' + k - l - i)\Gamma(k-1)} n_2^{-s'-i} (M'n)^i \int_0^{\infty} y^{k-1} y^{-i} e^{-y} \frac{dy}{y} \end{aligned}$$

$$= \sum_{i=0}^{-s'} (-1)^i \binom{-s'}{i} \frac{\Gamma(s'+k-l)\Gamma(k-i-1)}{\Gamma(s'+k-l-i)\Gamma(k-1)} n_2^{-s'-i} (M'n)^i$$

$$= P_{s'}(n_2, M'n).$$

Therefore, for every n_1, n_2 such that $C_f n_1 + n_2 = M'n$, (5.22) becomes

$$d(n_1, n_2; s', \chi)$$
$$= 2(C_f C_g)^{-s'} \overline{\chi}(C_g)\chi(n_1)b(n_1) \sum_{n_2 = dd'} \psi\overline{\omega\chi^2}(d')d^{2s'+k-l-1} P_{s'}(n_2, M'n).$$

Substituting the above expression in (5.21) finishes the proof. □

6. Kummer congruences for the distributions

In this section, we show that the distributions in (4.6) for $s = l + r$, where $0 \leq r \leq k-l-1$ patch together into a measure, by verifying the abstract Kummer congruences.

By Proposition 5.3, with $s = l + r$, where $0 \leq r \leq k - l - 1$, we have

$$\Psi_{l+r}^{(M')}(\chi) = \gamma(M')\langle f, f\rangle_{C_f}^{-1} \langle f_0^\rho | V_{C_f}, \widetilde{K}_{M'}(r-k+l+1)|w_{C_0C_f}\rangle_{C_0C_f}$$

$$\overset{(2.2)}{=} \gamma(M')\langle f, f\rangle_{C_f}^{-1} \langle f_0^\rho | V_{C_f} w_{C_0C_f}, \widetilde{K}_{M'}(r-k+l+1)\rangle_{C_0C_f}. \quad (6.1)$$

By Corollary 4.2 and (5.13), we have $\Psi_s^{(M')}(\chi)$ and $\gamma(M')$ are algebraic numbers. Hence

$$\langle f, f\rangle_{C_f}^{-1} \langle f_0^\rho | V_{C_f}, \widetilde{K}_{M'}(r-k+l-1)|w_{C_0C_f}\rangle_{C_0C_f} \in \overline{\mathbb{Q}}. \quad (6.2)$$

Further, note that the cusp form $\widetilde{K}_{M'}(r-k+l+1)$ has algebraic Fourier coefficients. Let

$$S_k(C_0C_f, \psi; \overline{\mathbb{Q}}) = \{h \in S_k(C_0C_f, \psi) \mid h \text{ has algebraic Fourier coeffecients}\}.$$

We now claim that $f_0^\rho | V_{C_f} w_{C_0C_f} \in S_k(C_0C_f, \psi; \overline{\mathbb{Q}})$. Clearly $f_0^\rho | V_{C_f} w_{C_0C_f}$ belongs to $S_k(C_0C_f, \psi)$. So it is enough to show that the Fourier coefficients of $f_0^\rho | V_{C_f} w_{C_0C_f}$ are algebraic. Observe that

$$f_0^\rho | V_{C_f} w_{C_0C_f}$$

$$\overset{(4.1)}{=} f^\rho | V_{C_f} w_{C_0C_f} - \alpha'(p) f^\rho | V_p V_{C_f} w_{C_0C_f}$$

$$= C_f^{-k/2} f^\rho | w_{C_0} - \alpha'(p)(pC_f)^{-k/2} f^\rho | w_{C_fC_g}$$

(from the definition of $V_p, V_{C_f}, w_{C_0C_f}$)

$$\overset{(4.5)}{=} (pC_gC_f^{-1})^{k/2} f^\rho | w_{C_f} V_{pC_g} - \alpha'(p)(pC_fC_g^{-1})^{-k/2} f^\rho | w_{C_f} V_{C_g}$$

$$\stackrel{(2.6)}{=} (pC_gC_f^{-1})^{k/2}\Lambda(f^\rho)f^\rho|V_{pC_g} - \alpha'(p)(pC_fC_g^{-1})^{-k/2}\Lambda(f^\rho)f^\rho|V_{C_g}.$$

Since f is primitive, it follows that $f_0^\rho|V_{C_f}w_{C_0C_f}$ has algebraic Fourier coefficients. Define the linear functional $\mathcal{L} : S_k(C_0C_f, \psi) \longrightarrow \mathbb{C}$, by

$$\mathcal{L}(K) = \frac{\langle f_0^\rho|V_{C_f}w_{C_0C_f}, K\rangle_{C_0C_f}}{\langle f, f\rangle_{C_f}}. \tag{6.3}$$

We note from (6.1) and (6.3) that, for every finite order character $\chi : \mathbb{Z}_p^\times \to \mathbb{C}^\times$,

$$\Psi_{l+r}^{(M')}(\chi) = \gamma(M')\mathcal{L}(\widetilde{K}_{M'}(r-k+l+1)). \tag{6.4}$$

Lemma 6.1. *Let $\mathcal{L}$ be defined as above. Then*

(1) *$\mathcal{L}$ is defined over $\overline{\mathbb{Q}}$, i.e., $\mathcal{L}(S_k(C_0C_f, \psi; \overline{\mathbb{Q}})) \subset \overline{\mathbb{Q}}$.*
(2) *Let $K(z) = \sum_{n=1}^\infty a(n, K)e(nz)$ be an element of $S_k(C_0C_f, \psi; \overline{\mathbb{Q}})$. Then there exists $m \in \mathbb{N}$ and $\xi_1, \ldots, \xi_m \in \overline{\mathbb{Q}}$ such that*

$$\mathcal{L}(K) = \sum_{n=1}^m \xi_n a(n, K). \tag{6.5}$$

Proof. Choose an orthogonal basis $f_1, \ldots, f_d$ of $S_k(C_0C_f, \psi; \overline{\mathbb{Q}})$ such that $f_1 = f_0^\rho|V_{C_f}w_{C_0C_f}$. By Proposition 5.3, we know that $\widetilde{K}_{M'}(r-k+l+1) \in S_k(C_0C_f, \psi; \overline{\mathbb{Q}})$ for all integers $0 \le r \le k-l-1$. Let $\widetilde{K}_{M'}(r-k+l+1) = \sum_{i=1}^d c_i f_i$, for some $c_i \in \overline{\mathbb{Q}}$. It follows from (6.2) and orthogonality that

$$\mathcal{L}(\widetilde{K}_{M'}(r-k+l+1)) = c_1\mathcal{L}(f_0^\rho|V_{C_f}w_{C_0C_f}) \in \overline{\mathbb{Q}}.$$

Choose r, χ such that $\Psi_{l+r}^{(M')}(\chi) = \gamma(M')\mathcal{L}(\widetilde{K}_{M'}(r-k+l+1)) \neq 0$. Such a choice exists, otherwise all the twisted L-values of the Rankin product L-function vanish by (4.8) and Proposition 4.1, so the p-adic Rankin product L-function, or more precisely the measure μ in Theorem 1.1, can be taken to be identically zero. Hence, $c_1 \neq 0$ and $\mathcal{L}(f_0^\rho|V_{C_f}w_{C_0C_f}) \in \overline{\mathbb{Q}}$. Therefore $\mathcal{L}(S_k(C_0C_f, \psi; \overline{\mathbb{Q}})) = \overline{\mathbb{Q}}\mathcal{L}(f_0^\rho|V_{C_f}w_{C_0C_f}) = \overline{\mathbb{Q}}$. This finishes the proof of the first part.

Let $\mathbb{T}_k(C_0C_f, \psi)$ denote the $\overline{\mathbb{Q}}$-subalgebra of $\mathrm{End}_{\mathbb{C}}(M_k(C_0C_f, \psi))$ generated by the Hecke operators T_n, for all $n \in \mathbb{N}$. Clearly $\mathbb{T}_k(C_0C_f, \psi)$ is a finite dimensional $\overline{\mathbb{Q}}$-vector space. By [Miy89, Theorem 4.5.13] and [Miy89, (4.5.27)] we obtain that $\{T_n\}_{n\in\mathbb{N}}$ spans $\mathbb{T}_k(C_0C_f, \psi)$ as a $\overline{\mathbb{Q}}$-vector space. Hence, by finite dimensionality, there exists m such that $T_1, \ldots, T_m$ span $\mathbb{T}_k(C_0C_f, \psi)$ as a $\overline{\mathbb{Q}}$-vector space. There is an isomorphism of $\overline{\mathbb{Q}}$-vector spaces given by (see [Gha02, Lemma 2])

$$\begin{aligned} \mathbb{T}_k(C_0C_f, \psi) &\longrightarrow \mathrm{Hom}_{\overline{\mathbb{Q}}}(S_k(C_0C_f, \psi; \overline{\mathbb{Q}}), \overline{\mathbb{Q}}) \\ T &\mapsto a(1, Tf). \end{aligned}$$

By the first part of the lemma we know that $\mathcal{L} \in \mathrm{Hom}_{\overline{\mathbb{Q}}}(S_k(C_0C_f, \psi; \overline{\mathbb{Q}}), \overline{\mathbb{Q}})$. Therefore, $\mathcal{L}(K) = a(1, TK)$, for some $T \in \mathbb{T}_k(C_0C_f, \psi)$. Since $T_1, \cdots, T_m$ span $\mathbb{T}_k(C_0C_f, \psi)$ as $\overline{\mathbb{Q}}$-vector space, there exists $\xi_1, \ldots, \xi_m \in \overline{\mathbb{Q}}$ such that, $T = \sum_{n=1}^m \xi_n T_n$. So $\mathcal{L}(K) = \sum_{n=1}^m \xi_n a(1, T_n K) = \sum_{n=1}^m \xi_n a(n, K), \forall\ K \in S_k(C_0C_f, \psi; \overline{\mathbb{Q}})$. □

As mentioned earlier, every complex-valued Dirichlet character χ on $\mathbb{Z}_p^\times$ takes values in $\overline{\mathbb{Q}} \subset \mathbb{C}$. From now on we think of such character as taking values in $\mathbb{C}_p$ via our fixed embedding $i_p : \overline{\mathbb{Q}} \to \mathbb{C}_p$. Since $\Psi_{l+r}(\chi) \in \overline{\mathbb{Q}}$, for $0 \le r \le k - l - 1$, by Corollary 4.2, we have $i_p(\Psi_{l+r}(\chi)) \in \mathbb{C}_p$. Thus we may think of the complex distribution Ψ_{l+r}, as a $\mathbb{C}_p$-valued distribution. We shall denote these distributions by $i_p(\Psi_{l+r})$, for $0 \le r \le k - l - 1$.

We now define a candidate for the measure in Theorem 1.1, namely we take

$$\mu := i_p(\Psi_l). \tag{6.6}$$

By Proposition 4.1 and (6.4), we have

$$\begin{aligned}\Psi_{l+r}(\chi) &= \gamma(M')\mathcal{L}(\widetilde{K}_{M'}(r - k + l + 1)) \\ &= \gamma(M') \sum_{n=1}^{m} \xi_n\, a(n, \widetilde{K}_{M'}(r - k + l + 1)) \quad \text{(by Lemma 6.1 (2))} \\ &= \gamma(M') \sum_{n=1}^{m} \xi_n \sum_{C_f n_1 + n_2 = M'n} d(n_1, n_2; r - k + l + 1, \chi),\end{aligned} \tag{6.7}$$

by Proposition 5.3, where M' is a sufficiently large power of p chosen depending on χ, and $\gamma(M')$ is as defined in (5.13). As remarked earlier, $\gamma(M')$ is p-integral in many cases (apparently in all), but in any case has bounded denominator, coming from $\Lambda(g)$, since $\alpha(pM')$ is a p-adic unit. Similarly, the $\xi_n \in \overline{\mathbb{Q}}$ have bounded denominators. Finally the $d(n_1, n_2; s, \chi)$ also have denominators at worst $\Gamma(k - 1)$ by (5.18), (5.19). Hence multiplying $i_p(\Psi_{l+r})$ by a suitable (fixed) power of p we may and do assume that $i_p(\Psi_{l+r}(\chi))$ lies in $\mathcal{O}_p$ for all χ. Proving that this rescaled distribution is an $\mathcal{O}_p$-valued measure will imply that $i_p(\Psi_{l+r})$ is a (not necessarily $\mathcal{O}_p$-valued) measure.

Proposition 6.2. *For all integers* $0 \le r \le k - l - 1$, *we have*

(1) *The* $\mathbb{C}_p$*-valued distributions* $i_p(\Psi_{l+r})$ *are bounded. Hence,* $i_p(\Psi_{l+r})$ *are measures on* $\mathbb{Z}_p^\times$.

(2) *Moreover, with* μ *as in* (6.6), *the following equality holds*[7]

$$\int_{\mathbb{Z}_p^\times} \chi x_p^r \, d\mu = (-1)^r \int_{\mathbb{Z}_p^\times} \chi \, d i_p(\Psi_{l+r}). \tag{6.8}$$

[7] The formula (6.8) differs from [Pan88, (5.6)] by the factor $(-1)^r$. This factor is forced on us in view of the sign corrections mentioned in the previous footnotes. Moreover, this sign has theoretical significance: (6.8) matches with a general expectation about measures attached to L-functions of motives [CP89, (4.16)].

Proof. Fix an integer $0 \le r \le k-l-1$. Recall that the linear span of $\mathcal{B} = \{\chi \mid \chi : \mathbb{Z}_p^\times \to \mathbb{C}_p^\times$ has finite order$\}$ is dense in $\mathcal{C}(\mathbb{Z}_p^\times, \mathbb{C}_p)$. We claim that the distribution $i_p(\Psi_{l+r})$ satisfies the abstract Kummer congruences (3.4) with $\mathcal{B}$ as the system of functions. We need to prove that for every finite set of characters $\chi_1, \ldots, \chi_t \in \mathcal{B}$, constants $c_1, \ldots, c_t \in \mathbb{C}_p$ and $m \ge 0$,

$$\text{if } \sum_{i=1}^{t} c_i \chi_i \equiv 0 \pmod{p^m}, \text{ then } \sum_{i=1}^{t} c_i \, i_p(\Psi_{l+r}(\chi_i)) \equiv 0 \pmod{p^m}.$$

Choose M' sufficiently large so that (6.7) holds for each of the χ_i. By (6.7), this is equivalent to proving

$$\text{if } \sum_{i=1}^{t} c_i \chi_i \equiv 0 \pmod{p^m}, \text{ then } \sum_{i=1}^{t} c_i \, d(n_1, n_2; r-k+l+1, \chi) \equiv 0 \pmod{p^m} \tag{6.9}$$

for each n, and each n_1, n_2 satisfying $C_f n_1 + n_2 = M'n$.

If $p \mid n_1$, then $d(n_1, n_2; r-k+l+1, \chi_i) = 0$, by (5.18), since $\chi_i(n_1) = 0$. So, the relation (6.9) is trivially true. Hereafter, we assume $p \nmid n_1$. Since $p \nmid C_f$, $p \mid M'$ and $C_f n_1 + n_2 = M'n$, we have $p \mid n_1$ if and only if $p \mid n_2$. So we have $p \nmid n_2$ and $d/d'C$ is a p-adic unit, for $dd' = n_2$. Let $s = r-k+l+1$. We may also assume M' has been chosen large enough so that $p^m \mid M'/\Gamma(k-1)$. From (5.19) and the equality $C_f n_1 + n_2 = M'n$, it follows that

$$\begin{aligned} P_s(n_2, M'n) &\equiv n_2^{k-l-1-r} \equiv (dd')^{k-l-1-r} \pmod{p^m}, \\ \chi(n_1) &= \overline{\chi}(-C_f)\chi(n_2) = \overline{\chi}(-C_f)\chi(dd'). \end{aligned} \tag{6.10}$$

By (5.18) and (6.10), we have the congruence

$$\begin{aligned} &d(n_1, n_2; r-k+l+1, \chi) \\ &\quad \equiv 2\overline{\chi}(-C)C^{k-l-r-1} b(n_1) \sum_{n_2 = dd'} \psi\overline{\varpi}\overline{\chi}(d')\chi(d)(d')^{k-l-r-1} d^r \pmod{p^m}. \end{aligned}$$

Therefore,

$$\begin{aligned} &(-1)^r \sum_{i=1}^{t} c_i \, d(n_1, n_2; r-k+l+1, \chi_i) \\ &\quad \equiv 2b(n_1) \sum_{n_2 = dd'} \psi\overline{\varpi}(d')(d'C)^{k-l-1} \sum_{i=1}^{t} c_i \chi_i \left(\frac{-d}{d'C}\right) \left(\frac{-d}{d'C}\right)^r \pmod{p^m}. \end{aligned} \tag{6.11}$$

By assumption, $\sum_i c_i \chi_i \equiv 0 \pmod{p^m}$, so $\sum_i c_i \chi_i(-d/d'C) \equiv 0 \pmod{p^m}$. Since each $-d/d'C$ is a p-adic unit, we obtain $\sum_{i=1}^{t} c_i \, d(n_1, n_2; r-k+l+1, \chi_i) \equiv 0 \pmod{p^m}$. Thus (6.9) holds and this finishes the proof of (1).

For (2), we claim there exists a $\mathbb{C}_p$-valued measure ν such that

$$\int_{\mathbb{Z}_p^\times} \chi x_p^r \, d\nu = (-1)^r \int_{\mathbb{Z}_p^\times} \chi \, di_p(\Psi_{l+r}), \quad \forall \; 0 \le r \le k-l-1.$$

Let $\mathcal{B}' = \{\chi x_p^r \mid \chi \in \mathcal{B} \text{ and } 0 \le r \le k-l-1\}$. To prove the existence of this measure, it is enough to verify the abstract Kummer congruences hold for $\mathcal{B}'$ as the system of functions. As in (1), we need to prove for every finite set of characters $\chi_i \in \mathcal{B}'$ and $c_{i,r} \in \mathbb{C}_p$,

$$\text{if } \sum_{i,r} c_{i,r} \chi_i x_p^r \equiv 0 \pmod{p^m}, \text{ then}$$

$$\sum_{i,r} (-1)^r c_{i,r} \, d(n_1, n_2; r-k+l+1, \chi_i) \equiv 0 \pmod{p^m}. \tag{6.12}$$

As observed above, if $p \mid n_1$, then $d(n_1, n_2; r-k+l+1, \chi_i) = 0$, so (6.12) holds. For $p \nmid n_1$, it follows from (6.11) that

$$\sum_{i,r} (-1)^r c_{i,r} \, d(n_1, n_2; r-k+l+1, \chi_i)$$

$$\equiv \sum_{n_2 = dd'} 2b(n_1) \psi\overline{\omega}(d')(d'C)^{k-l-1} \left(\sum_{i,r} c_{i,r} \chi_i \left(\frac{-d}{d'C}\right) \left(\frac{-d}{d'C}\right)^r \right) \pmod{p^m}.$$

By the assumption in (6.12), the inner sum is congruent to 0 (mod p^m). Thus

$$\sum_{i,r} (-1)^r c_{i,r} \, d(n_1, n_2; r-k+l+1, \chi_i) \equiv 0 \pmod{p^m},$$

so again (6.12) holds. This proves that ν as claimed above exists. Further μ and ν agree on $\mathcal{B}$ (take $r = 0$) which spans $\mathrm{Step}(\mathbb{Z}_p^\times, \mathbb{C}_p)$. Hence $\mu = \nu$. This completes the proof of (2). □

Let μ be the distribution in (6.6). By Proposition 6.2 (1) with $r = 0$, we see that μ is a measure. By (6.8), and (4.8) with $s = l + r$, we see that μ satisfies the interpolation property[8] of Theorem 1.1. This completes the proof of Theorem 1.1.

Acknowledgements

We thank B. Balasubramanyam, D. Benois, D. Loeffler and S. Kobayashi for helpful conversations.

[8]The sign $(-1)^r$ in (6.8) contributes to the corrected sign $(-1)^r$ in Theorem 1.1.

References

[CP89] J. Coates and B. Perrin-Riou, p-adic L-functions attached to motives over $\mathbb{Q}$, Algebraic Number Theory – in honor of K. Iwasawa, J. Coates, R. Greenberg, B. Mazur and I. Satake, eds. (Tokyo: Mathematical Society of Japan), (1989) 23–54.

[CP04] M. Courtieu and A. A. Panchishkin, Non-Archimedean L-functions and arithmetical Siegel modular forms, *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, Second edition, Vol. 1471 (2004).

[Del79] P. Deligne, Valeurs de fonctions L et périodes d'intégrales, *Proc. Sympos. Pure Math.*, **33(2)** (1979) 313–346.

[Gha02] E. Ghate, An introduction to congruences between modular forms, Current trends in number theory (Allahabad 2000), Hindustan Book Agency, New Delhi, (2002) 39–58.

[Hid88] H. Hida, A p-adic measure attached to the zeta functions associated with two elliptic modular forms II, *Ann. Inst. Fourier* (Grenoble), **38(3)** (1988) 1–83.

[Hid93] H. Hida, Elementary theory of L-functions and Eisenstein series, London Mathematical Society Student Texts, Cambridge University Press, Cambridge, Vol. 26 (1993).

[Kat78] N. M. Katz, p-adic L-functions for CM fields, *Invent. Math.*, **49(3)** (1978) 199–297.

[Man73] Ju. I. Manin, Periods of cusp forms, and p-adic Hecke series, *Mathematics of the USSR-Sbornik*, **92(134)** (1973) 378–401, 503.

[Miy89] T. Miyake, Modular forms, Translated from the Japanese by Yoshitaka Maeda, Springer-Verlag, Berlin (1989).

[MSD74] B. Mazur and P. Swinnerton-Dyer, Arithmetic of Weil curves, *Invent. Math.*, **25** (1974) 1–61.

[Pan88] A. A. Panchishkin, Non-archimedean Rankin L-functions and their functional equations, *Izv. Akad. Nauk SSSR Ser. Mat.*, **52(2)** (1988) 336–354, 447.

[Ran39] 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 $\Re s = 13/2$ II. The order of the Fourier coefficients of integral modular forms, *Proc. Cambridge Philos. Soc.*, **35** (1939) 351–372.

[Ran52] R. A. Rankin, The scalar product of modular forms, *Proc. London Math. Soc. (3)*, **2** (1952) 198–217.

[Shi77] G. Shimura, On the periods of modular forms, *Math. Ann.*, **229(3)** (1977) 211–221.

[Vie00] M. Vienney, A new construction of p-adic Rankin convolutions in the case of positive slope, *Int. J. Number Theory*, **6(8)** (2010) 1875–1900.

[Was97] L. Washington, Introduction to Cyclotomic fields, Graduate Texts in Mathematics. Springer-Verlag, New York, Second edition, Vol. 83 (1997).

[Zag92] D. Zagier, Introduction to modular forms. In From number theory to physics (Les Houches, 1989). Springer, Berlin, (1992) 238–291.

Topics in Number Theory, RMS-Lecture Notes Series No. 26, 2020, pp. 109–131.

Heights, Ranks and Regulators of Abelian Varieties

Fabien Pazuki*

Department of Mathematical Sciences, University of Copenhagen, Universitetsparken 5, 2100 Copenhagen Ø, Denmark, and Institut de Mathématiques de Bordeaux, Université de Bordeaux, 351, cours de la Libération, 33405 Talence, France.
e-mail: fabien.pazuki@math.u-bordeaux.fr

Abstract. We give a lower bound on the Faltings height of an abelian variety over a number field by the sum of its injectivity diameter and the norm of its bad reduction primes. It leads to an unconditional explicit upper bound on the rank of Mordell-Weil groups. Assuming the height conjecture of Lang and Silverman, we then obtain a Northcott property for the regulator on the set of polarized simple abelian varieties defined over a fixed number field K, of dimension g and rank m_K bounded from above and with dense K-rational points. We remove the simplicity assumption in the principally polarized case by giving a refined version of the Lang-Silverman conjecture.

Keywords. Heights, abelian varieties, regulators, Mordell-Weil.

Subject Classification: 11F11, 11F66

Hauteurs, rangs et régulateurs des variétés abéliennes.

Résumé. On minore la hauteur de Faltings d'une variété abélienne sur un corps de nombres par la somme de son diamètre d'injectivité et de la norme de ses premiers de mauvaise réduction. Cela entraîne une majoration explicite inconditionnelle du rang des groupes de Mordell-Weil. On obtient alors comme conséquence d'une conjecture de Lang et Silverman une propriété de Northcott pour le régulateur sur l'ensemble des variétés abéliennes simples, polarisées et définies sur un corps de nombres, à dimension et rang bornés et dont les points rationnels sont denses. On montre comment se passer de l'hypothèse de simplicité dans le cas de polarisation principale en proposant une version raffinée de la conjecture de Lang-Silverman.

Mots-Clefs: Hauteurs, variétés abéliennes, régulateurs, Mordell-Weil.

1. Introduction

Let K be a number field of degree d over $\mathbb{Q}$ and let M_K stand for the set of all places of K. We denote by M_K^∞ the set of archimedean places. For any place $v \in M_K$, we denote by K_v the completion of K with respect to the valuation $|.|_v$. One fixes $|p|_v = p^{-1}$ as a normalization for any finite place v above a rational prime p. The local degree will be denoted by $d_v = [K_v : \mathbb{Q}_v]$.

Let A be an abelian variety of dimension g defined over the number field K. The set of rational points of A over K is finitely generated by the Mordell-Weil Theorem, and

*Many thanks to Pascal Autissier, Marc Hindry, Robin de Jong, Qing Liu, Gaël Rémond and Martin Widmer for exchanging ideas concerning this article. The author is supported by the DNRF Niels Bohr Professorship of Lars Hesselholt, ANR-14-CE25-0015 Gardio and ANR-17-CE40-0012 Flair.

the aim of this article is to study links between the rank of the Mordell-Weil group, the regulator of the Mordell-Weil lattice and the Faltings height of the abelian variety A.

We first give an inequality between the Faltings height $h_{\mathrm{F}^+}(A/K)$ of Definition 2.2 and the norm of the bad reduction primes of A, interesting in itself and useful for the following results.

Theorem 1.1. *Let $g \geq 1$ be an integer. Let K be a number field of degree d. There exist two quantities $c = c(g) > 0$, $c_0 = c_0(g) \in \mathbb{R}$, such that for any abelian variety A of dimension g, defined over K, one has*

$$h_{\mathrm{F}^+}(A/K) \geq c\frac{1}{d}\log N^0_{A/K} + c_0$$

where $N^0_{A/K}$ is the product of the norms of the primes of K of bad reduction for A. The explicit values $c = (12g)^{-12g^{12g^{4g}}}$ and $c_0 = -1/c$ are valid.

We believe this inequality will be useful in different contexts. We believe furthermore that some steps in the proof presented here could be useful as well (explicit Bertini, reduction to the jacobian case by quotient with explicit bounds on their heights, *etc*). See Proposition 3.2 for a detailed description of the argument. A similar statement (for the semi-stable case) was obtained in [HiPa16] independently. They show the result in details over function fields and with different arguments. The main difference is the fact that the quantities c and c_0 here don't depend on the base field K, but only on the dimension g. Their strategy of proof seems to work over number fields as well, based on rigid uniformization of abelian varieties. Remark that their lower bound (at least in the case of function fields) is given in terms of Tamagawa numbers. To obtain Tamagawa numbers with our strategy would require a better understanding of the variation of component groups of Néron models within isogeny classes of abelian varieties. Another difference is that the quantities c and c_0 here are given explicitly, and are not too extreme in the case of jacobian varieties, where $c = 1/12^{4g^2+1}$ and $c_0 = 0$, see Proposition 3.2 and Proposition 3.6 below. Unfortunately, it is unlikely that the explicit expressions we obtain could be improved in a significant way using the strategy we follow here. The main reason is the use of Theorem 1.3 page 760 of [Rém10] where one already has a tower with three levels of exponents, plus the fact that the control given in [CaTa12] on the genus of the curve constructed by the Bertini argument is (more than) exponential: the combination of these inequalities is forcing our c and our c_0 to behave like a four levels exponential function in the dimension of A, and the aforementioned results both seem difficult to improve on.

Whenever a polarization is given on A, one can obtain a richer lower bound. Let (A, L) be a polarized abelian variety of dimension g defined over the number field K. We give an inequality between the Faltings height $h_{\mathrm{F}^+}(A/K)$ of Definition 2.2, the norm of the bad reduction primes of A over K and the injectivity diameter of $(A(\mathbb{C}), L)$. As a direct corollary of Theorem 1.1 and of the Matrix Lemma (see Theorem 3.1 below) we obtain:

Corollary 1.2. *Let $g \geq 1$ be an integer. Let K be a number field of degree d. There exist three explicit quantities $c_1 = c_1(g) > 0$, $c_2 = c_2(g) > 0$, $c_3 = c_3(g) \in \mathbb{R}$, such that for any abelian variety A of dimension g, defined over K, for any ample line bundle L carrying a polarization on A, one has*

$$h_{\mathrm{F}^+}(A/K) \geq c_1 \frac{1}{d} \log N^0_{A/K} + c_2 \frac{1}{d} \sum_{v \in M_K^\infty} d_v \rho(A_v, L_v)^{-2} + c_3$$

where $N^0_{A/K}$ is the product of the norms of the primes of K of bad reduction for A and $\rho(A_v, L_v)$ is the injectivity diameter of $A_v(\mathbb{C})$ polarized by L_v. The explicit values $c_1 = (12g)^{-12g^{12g^{4g}}}/17$, $c_2 = 1/17$ and $c_3 = -1/c_1$ are valid.

Note that the polarization is not required to be principal here. As for Theorem 1.1, the explicit values given here are not expected to be optimal. Nevertheless in the case where A is the semi-stable jacobian of a curve, one can take $c_1 = 1/204$, $c_2 = 1/17$ and $c_3 = -39g/17$.

One obtains the following result as another corollary of Theorem 1.1 and preexisting bounds on the Mordell-Weil rank.

Corollary 1.3. *Let A be an abelian variety of dimension g defined over a number field K of degree d and discriminant Δ_K. Let m_K be the Mordell-Weil rank of $A(K)$. There exists a quantity $c_4 = c_4(d, g) > 0$ such that*

$$m_K \leq c_4 \max\{1, h_{\mathrm{F}^+}(A/K), \log |\Delta_K|\},$$

and the explicit value $c_4 = (12g)^{12g^{12g^{4g}}} d^3$ is valid.

Let us add another remark, namely if $A = J_C$ is the jacobian of a curve C of genus $g \geq 2$ (not necessarily semi-stable) over a number field K of degree d and discriminant Δ_K, one has the explicit

$$m_K \leq 48 g^3 d^3 2^{8g^2} 12^{4g^2} \max\{1, h_{\mathrm{F}^+}(J_C/K)\} + g d 2^{8g^2} \log |\Delta_K| + g^3 d^3 2^{8g^2} \log 16,$$

as given in the proof of Corollary 1.3. The case of elliptic curves is given in Lemma 4.7 of [Paz14]. Corollary 1.3 will be used in the proof of Lemma 5.3. [1]

We then focus on the regulator of $A(K)$. We show that it satisfies a Northcott property for simple abelian varieties under a conjecture of Lang and Silverman, as proposed in [Paz16a].[2]

Theorem 1.4. *Assume the Lang-Silverman Conjecture 4.1. The set of $\overline{\mathbb{Q}}$-isomorphism classes of simple abelian varieties A, equipped with an ample and symmetric line bundle L, defined over a fixed number field K, of dimension g and rank m_K bounded from above, with $A(K)$ Zariski dense in A and with $\mathrm{Reg}_L(A/K)$ bounded from above is finite.*

[1] The reader will see that Lemma 5.3 is stronger than what is needed for the sequel, but we keep Remark 4.4 in mind.

[2] Note that a version of Theorem 1.4 for elliptic curves without the requirement that the rank is bounded from above is given in [Paz14] with an incorrect proof, see [Paz16b].

In this special case one restricts to simple abelian varieties where the Zariski density of $A(K)$ is equivalent to having positive Mordell-Weil rank. Using a stronger height conjecture one obtains the following general statement, without any simplicity assumption, on the moduli space of principally polarized abelian varieties.

Theorem 1.5. *Assume the stronger Lang-Silverman Conjecture 5.1. The set of $\overline{\mathbb{Q}}$-isomorphism classes of principally polarized abelian varieties A, defined over a fixed number field K, of dimension g and rank m_K bounded from above, with $A(K)$ Zariski dense in A and regulator bounded from above is finite.*

As explained in [Paz16a], if one restricts to $g = 1$ one can replace the Lang-Silverman conjecture by the ABC conjecture in the statements of Theorem 1.4 and Theorem 1.5.

We divide the work as follows. In section 2 we give the definitions of the regulator and of the Faltings height of an abelian variety. In section 3 we prove Theorem 1.1: it relies on the core of the work, namely Proposition 3.2, which gives the semi-stable version. The final step is then given in Proposition 3.6. The rest of the work is of a more prospective nature, but still concerning the arithmetic of Mordell-Weil groups. In section 4 we use the conjecture of Lang and Silverman to deduce Theorem 1.4. In section 5 we discuss how a stronger conjecture of Lang and Silverman type imply Theorem 1.5. We conclude in section 6 with a comparaison with number fields, extending the dictionary of [Paz14].

2. Definitions

Let S be a set. We will say that a function $f : S \to \mathbb{R}$ satisfies a Northcott property on S if for any real number B, the set $\{P \in S \mid f(P) \leq B\}$ is finite.

Notation. the function denoted log is the reciprocal of the classical exponential function, so $\log e = 1$ (we do not use the notation ln). We will denote by $\mathcal{O}_K$ the ring of integers of the number field K. If K' is a finite extension of a number field K, we denote by $\mathcal{N}_{K'/K}$ the relative norm. If $\mathfrak{p}'$ is a prime ideal in $\mathcal{O}_{K'}$ above the prime ideal $\mathfrak{p}$ in $\mathcal{O}_K$, then $e_{\mathfrak{p}'/\mathfrak{p}}$ is the ramification index and $f_{\mathfrak{p}'/\mathfrak{p}}$ stands for the residual degree.

2.1 *Regulators of abelian varieties*

Let A/K be an abelian variety over a number field K polarized by an ample and symmetric line bundle L. Let m_K be the Mordell-Weil rank of $A(K)$. Let $\widehat{h}_{A,L}$ be the Néron-Tate height associated with the pair (A, L). Let $\langle ., . \rangle$ be the associated bilinear form, given by

$$\langle P, Q \rangle = \frac{1}{2}\Big(\widehat{h}_{A,L}(P+Q) - \widehat{h}_{A,L}(P) - \widehat{h}_{A,L}(Q)\Big)$$

for any $P, Q \in A(\overline{\mathbb{Q}})$. This pairing on $A \times A$ depends on the choice of L.

Definition 2.1. *Let $P_1, \ldots, P_{m_K}$ be a basis of the lattice $A(K)/A(K)_{\text{tors}}$, where $A(K)$ is the Mordell-Weil group. The regulator of A/K is defined by*

$$\text{Reg}_L(A/K) = |\det(\langle P_i, P_j\rangle_{1\le i,j\le m_K})|,$$

where by convention an empty determinant is equal to 1.

As for the height, the regulator of an abelian variety depends on the choice of an ample and symmetric line bundle L on A.

There is a more intrinsic way of defining a regulator, that doesn't depend on the choice of L. Start with the natural pairing on the product of A with its dual abelian variety $\check{A}$ given by the Poincaré line bundle $\mathcal{P}$: for any $P \in A(\overline{\mathbb{Q}})$ and any $Q \in \check{A}(\overline{\mathbb{Q}})$, define $\langle P, Q\rangle = \widehat{h}_{A\times\check{A},\mathcal{P}}(P, Q)$. Next choose a base $P_1, \ldots, P_{m_K}$ of $A(K)$ modulo torsion and a base $Q_1, \ldots, Q_{m_K}$ of $\check{A}(K)$ modulo torsion. Then define

$$\text{Reg}(A/K) = |\det(\langle P_i, Q_j\rangle_{1\le i,j\le m_K})|.$$

Let us recall how these two regulators are linked (see for instance [Hin07]). Let $\Phi_L : A \to \check{A}$ be the isogeny given by $\Phi_L(P) = t_P^* L \otimes L^{-1}$. One has the formula

$$\widehat{h}_{A,L}(P) = \frac{1}{2}\langle P, \Phi_L(P)\rangle.$$

Hence if u is the index of the subgroup $\Phi_L(\mathbb{Z}P_1 \oplus \cdots \oplus \mathbb{Z}P_{m_K})$ in $\check{A}(K)$ modulo torsion, one has

$$\text{Reg}_L(A/K) = u2^{-m_K}\text{Reg}(A/K). \tag{1}$$

Let us remark that when L induces a principal polarization, the index u is equal to 1. Thus Theorem 1.5 is valid with both regulators.

2.2 *The Faltings height*

Let A be an abelian variety defined over a number field K, of dimension $g \ge 1$. Recall that $\mathcal{O}_K$ is the ring of integers of K and let $\pi : \mathcal{A} \longrightarrow \text{Spec}(\mathcal{O}_K)$ be the Néron model of A over $\text{Spec}(\mathcal{O}_K)$. Let ε: $\text{Spec}(\mathcal{O}_K) \longrightarrow \mathcal{A}$ be the zero section of π and let $\omega_{\mathcal{A}/\mathcal{O}_K}$ be the maximal exterior power (the determinant) of the sheaf of relative differentials

$$\omega_{\mathcal{A}/\mathcal{O}_K} := \varepsilon^\star\Omega^g_{\mathcal{A}/\mathcal{O}_K} \simeq \pi_\star\Omega^g_{\mathcal{A}/\mathcal{O}_K}\ .$$

For any archimedean place v of K, let σ be an embedding of K in $\mathbb{C}$ associated to v. The associated line bundle

$$\omega_{\mathcal{A}/\mathcal{O}_K,\sigma} = \omega_{\mathcal{A}/\mathcal{O}_K} \otimes_{\mathcal{O}_K,\sigma} \mathbb{C} \simeq H^0(\mathcal{A}_\sigma(\mathbb{C}), \Omega^g_{\mathcal{A}_\sigma}(\mathbb{C}))$$

is equipped with a natural L^2-metric $\|.\|_v$ given by

$$\|s\|_v^2 = \frac{i^{g^2}}{(2\pi)^{2g}}\int_{\mathcal{A}_\sigma(\mathbb{C})} s \wedge \overline{s}\ .$$

The $\mathcal{O}_K$-module $\omega_{\mathcal{A}/\mathcal{O}_K}$ is of rank 1 and together with the hermitian norms $\|.\|_v$ at infinity it defines an hermitian line bundle $\overline{\omega}_{\mathcal{A}/\mathcal{O}_K} = (\omega_{\mathcal{A}/\mathcal{O}_K}, (\|.\|_v)_{v\in M_K^\infty})$ over $\mathcal{O}_K$. It has a well defined Arakelov degree $\widehat{\deg}(\overline{\omega}_{\mathcal{A}/\mathcal{O}_K})$. Recall that for any hermitian line bundle $\overline{\mathcal{L}}$ over Spec$(\mathcal{O}_K)$ the degree of $\overline{\mathcal{L}}$ in the sense of Arakelov is defined as

$$\widehat{\deg}(\overline{\mathcal{L}}) = \log \#(\mathcal{L}/s\mathcal{O}_K) - \sum_{v\in M_K^\infty} d_v \log \|s\|_v \ ,$$

where s is any non zero section of $\mathcal{L}$. The resulting number does not depend on the choice of s in view of the product formula on the number field K.

The Arakelov degree of this metrized bundle will give a translate of the classical Faltings height.

Definition 2.2. *The height of A/K is defined as*

$$h_{\mathrm{F}^+}(A/K) := \frac{1}{[K:\mathbb{Q}]}\widehat{\deg}(\overline{\omega}_{\mathcal{A}/\mathcal{O}_K}) \ .$$

This non-negative real number doesn't depend on any choice of polarization on A. When A/K is semi-stable, this height only depends on the $\overline{\mathbb{Q}}$-isomorphism class of A. It is just a translate of the classical Faltings height $h_F(A/K)$, we have $h_{\mathrm{F}^+}(A/K) = h_F(A/K) + \frac{g}{2}\log(2\pi^2)$. If A/K is not semi-stable, one may use Chai's base change conductor as in the formula (15) in the sequel as a complementary definition. See [Fa83] Satz 1, page 356 and 357 for its basic properties, and for a comparison with the theta height in [Paz12] (based on ideas of Bost and David). We prefer to use this translate because it gives cleaner inequalities (see the jacobian case in Proposition 3.2 for instance). We recall here four classical properties: firstly, if $A = A_1 \times A_2$ is a product of abelian varieties, one has $h_{\mathrm{F}^+}(A/K) = h_{\mathrm{F}^+}(A_1/K) + h_{\mathrm{F}^+}(A_2/K)$. Secondly, the dual abelian variety of A has the same height as A by a result of Raynaud. Thirdly, if K'/K is a number field extension, one has $h_{\mathrm{F}^+}(A/K') \leq h_{\mathrm{F}^+}(A/K)$. Finally if A/K is semi-stable, one defines the stable height by $h_{\mathrm{F}^+}(A/\overline{\mathbb{Q}}) := h_{\mathrm{F}^+}(A/K)$, which is invariant by number field extension.

At finite places we focus on the bad reduction locus with the following quantity.

Definition 2.3. *Let A be an abelian variety over a number field K. Let $\mathcal{A} \to$ Spec$(\mathcal{O}_K)$ be its Néron model. Let $\mathfrak{p}$ be a prime of $\mathcal{O}_K$. If the special fiber $\mathcal{A}_\mathfrak{p}$ is an abelian variety, we say that $\mathfrak{p}$ is a prime of good reduction for A, otherwise the prime is of bad reduction. We define*

$$N^0_{A/K} = \prod_{\substack{\mathfrak{p}\subset\mathcal{O}_K,\\ \mathfrak{p}\text{ bad for } A}} \mathcal{N}_{K/\mathbb{Q}}(\mathfrak{p}).$$

Regarding archimedean places, let us recall what the injectivity diameter is.

Definition 2.4. *Let A be a complex abelian variety. Let L be a polarization on A. Let T_A be the tangent space of A, let Γ_A be its period lattice and H_L the* *associated Riemann form on T_A. The injectivity diameter is the positive number $\rho(A, L) = \min_{\gamma \in \Gamma \setminus \{0\}} \sqrt{H_L(\gamma, \gamma)}$, i.e. the first minimum in the successive minima of the period lattice of A.*

3. A lower bound for the Faltings height

We start by recalling Masser's Matrix Lemma in Bost version (later precised by Autissier and Gaudron-Rémond). We then give a lower bound for the Faltings height by the norm of the bad reduction primes in the semi-stable case, then we obtain the result in the general case by base change, hence deriving a proof of Theorem 1.1 and Corollary 1.2. This implies an upper bound on the Mordell-Weil rank of abelian varieties over number fields in terms of the Faltings height.

3.1 *Archimedean places*

Let us start by the Matrix Lemma given in Théorème 1.1 page 345 of Gaudron and Rémond [GaRe14b] (see also Autissier's [Aut13] for good explicit constants if the polarization is principal; the first version was given by Bost for principally polarized abelian varieties, as stated in Autissier's paper). We give it here with the height $h_{\mathrm{F}^+}(A/K) = h_F(A/K) + \frac{g}{2}\log(2\pi^2)$.

Theorem 3.1 (Matrix Lemma). *Let K be a number field such that A is defined over K, polarized by an ample line bundle L. For any archimedean place v of K, denote by $\rho(A_v, L_v)$ the injectivity diameter of the complex polarized abelian variety (A_v, L_v), then*

$$\frac{1}{d} \sum_{v \in M_K^\infty} d_v \rho(A_v, L_v)^{-2} \leq 16\, h_{\mathrm{F}^+}(A/\overline{\mathbb{Q}}) + 39g.$$

The Matrix Lemma is true for the stable height $h_{\mathrm{F}^+}(A/\overline{\mathbb{Q}})$, and we always have $h_{\mathrm{F}^+}(A/K) \geq h_{\mathrm{F}^+}(A/\overline{\mathbb{Q}})$. Here the polarization is not necessarily principal.

3.2 *Bad reduction places*

We compare the height and the size of the bad primes of A over the base field K. We first give a proof of the inequality in the semi-stable case and then obtain the general result using base change properties given in the next paragraph. The following proposition gives the result in the semi-stable case. Let us first recall the case of elliptic curves, studied in [Paz14], where the argument is direct and produces easy constants. Let $A = E$ be an elliptic curve. One has the exact formula

$$h_{\mathrm{F}^+}(E/K) = \frac{1}{12d}\left[\log \mathcal{N}_{K/\mathbb{Q}}(\Delta_E) - \sum_{v \in M_K^\infty} d_v \log\Big(|\Delta(\tau_v)|(2\,\mathrm{Im}\,\tau_v)^6\Big)\right],$$

where Δ_E is the minimal discriminant of the curve, τ_v is a period in the fundamental domain such that $E(\overline{K}_v) \simeq \mathbb{C}/\mathbb{Z}+\tau_v\mathbb{Z}$ and $\Delta(\tau_v) = q\prod_{n=1}^{+\infty}(1-q^n)^{24}$ is the modular discriminant, with $q = \exp(2\pi i \tau_v)$. A direct analytic estimate using $\operatorname{Im}\tau_v \geq \sqrt{3}/2$ provides us with

$$h_{\mathrm{F}^+}(E/K) \geq \frac{1}{12d}\log N^0_{E/K}. \tag{2}$$

Let's move on to higher dimension.

Proposition 3.2. *Let A/K be a semi-stable abelian variety of dimension g and defined over a number field K of degree d. Then there exists quantities $c_5 = c_5(g) > 0$ and $c_6 = c_6(g) \in \mathbb{R}$ such that*

$$h_{\mathrm{F}^+}(A/K) \geq c_5\frac{1}{d}\log N^0_{A/K} + c_6.$$

The explicit values $c_5 = (12g)^{-12g^{12g^{3.5g}}}$ and $c_6 = -1/c_5$ are valid. If A is the jacobian of a curve of genus $g \geq 1$, then one can even take $c_5 = \frac{1}{12}$ and $c_6 = 0$.

Proof. The proof is divided into six steps: we start by the case of jacobians in Step 1. Then for general abelian varieties, we reduce to the case of principally polarized abelian varieties in Step 2 by Zarhin's trick. We make use of several projective heights (theta height, height *à la* Philippon, ...) to work on the inequality in Step 3. Then we explain in Step 4 how to find a curve of small height on a principally polarized abelian variety (by a Bertini Theorem) with the extra constraint that it is defined over a finite extension of K with controlled ramification, that will help us reduce the general case to the first case of jacobians. We show that the abelian variety we started with is a quotient of the jacobian of this curve (by classical arguments) in Step 5 and we can finally conclude (via Néron-Ogg-Shafarevich) by putting everything together in Step 6. As A/K is semi-stable, its Faltings height is invariant by number field extension, this will be used in the sequel.

Step 1. We start by proving the result for jacobians of curves. If $A = J_C$ is the jacobian of a curve C, the argument may be presented as follows. By the arithmetic Noether's formula of [MB89] Théorème 2.5 page 496 one has for a curve C of genus $g \geq 1$ (with semi-stable jacobian J_C) over a number field K of degree d,

$$12d\, h_{\mathrm{F}^+}(J_C/K) = (\omega_C\cdot\omega_C) + \sum_{\substack{\mathfrak{p}\ \mathrm{prime}\\ \mathfrak{p}\subset\mathcal{O}_K}} \delta_{\mathfrak{p}}(C)\log\mathcal{N}_{K/\mathbb{Q}}(\mathfrak{p})$$

$$+ \sum_{\sigma:K\hookrightarrow\mathbb{C}} \delta(C_\sigma) + dg\log(2^2\pi^8),$$

where the auto-intersection $(\omega_C\cdot\omega_C)$ is non-negative, $\delta(C_\sigma)$ is the delta invariant of Faltings of the complex curve C_σ and $\delta_{\mathfrak{p}}(C)$ is the number of singular points in the fiber $C_{\mathfrak{p}}$. It is zero if and only if $\mathfrak{p}$ is a prime ideal in $\mathcal{O}_K$ of good reduction for C. A remark is that the quantity

$$\frac{1}{d}\sum_{\mathfrak{p}\ \mathrm{prime}} \delta_{\mathfrak{p}}(C)\log\mathcal{N}_{K/\mathbb{Q}}(\mathfrak{p}) \tag{3}$$

is invariant by number field extension of the base field K. Indeed, if one proceeds with a base change from $\mathcal{O}_K$ to $\mathcal{O}_{K'}$, each double point in the fiber over a prime $\mathfrak{p}$ of C/K becomes singular in the fiber over primes $\mathfrak{p}'|\mathfrak{p}$ of C/K' with thickness equal to the ramification index $e_{\mathfrak{p}'/\mathfrak{p}}$, so the number of double points gets multiplied by $e_{\mathfrak{p}'/\mathfrak{p}}$ by passing from $\mathfrak{p}$ to $\mathfrak{p}'$, see the proof of Lemma 1.12 in [DeMu69].

One has $(\omega_C \cdot \omega_C) \geq 0$ and $\delta(C_\sigma) \geq -2g \log 2\pi^4$ by [Wil17], hence

$$(\omega_C \cdot \omega_C) + \sum_{\sigma : K \hookrightarrow \mathbb{C}} \delta(C_\sigma) \geq d \cdot c_7(g)$$

where one can take $c_7(g) = -2g \log 2\pi^4$. (Note that using the second inequality of Proposition 2.4.8 page 102 of [Java14] we would get $(\omega_C \cdot \omega_C) + \sum_{\sigma:K\hookrightarrow\mathbb{C}} \delta(C_\sigma) \geq -4dg^2$.)

It proves that the height of J_C satisfies

$$h_{\mathrm{F}^+}(J_C/K) \geq \frac{1}{12d} \sum_{\mathfrak{p}\ prime} \delta_{\mathfrak{p}}(C) \log \mathcal{N}_{K/\mathbb{Q}}(\mathfrak{p}) + c_8(g), \tag{4}$$

for $c_8(g) = g \log(2^2\pi^8) - 2g \log 2\pi^4 = 0$. This completes the statement for jacobians, because any bad prime for J_C is also a bad prime for C, so we have $\delta_{\mathfrak{p}}(C) \geq 1$ for any bad prime of J_C. We now look for a way to reduce to the case of jacobians.

Step 2. We may assume, using Zarhin's trick, that the abelian variety is principally polarized. Indeed if $\check{A}$ stands for the dual of A, the abelian variety $Z(A) = A^4 \times \check{A}^4$ carries a principal polarization, $h_{\mathrm{F}^+}(Z(A)/K) = 8\, h_{\mathrm{F}^+}(A/K)$ and $N^0_{Z(A)/K} = N^0_{A/K}$. It will have a little cost on the value of the quantities c_5 and c_6. Let us now fix a principal polarization L_{pri} on A.

Step 3. We will use the theory of Mumford theta coordinates as in the article of [DaPh02] pages 646–652, provided we do a field extension K'/K that enables us to choose a Mumford theta structure of level 4. The choice $K' = K[A[16]]$ is valid (and implies that A is semi-stable over K'), and Lemma 4.7 page 2078 of [GaRe14a] implies

$$[K' : K] \leq 16^{4g^2}. \tag{5}$$

We choose an embedding $\Theta_{16} : A \to \mathbb{P}^{16^g-1}$ given by the theta sections of $L = L_{pri}^{\otimes 16}$, where L_{pri} is the principal polarization and we define the theta height of (A, L) by $h_\Theta(A, L) = h(\Theta_{16}(O_A))$. We will in fact show the lower bound for the theta height of A: by virtue of the following inequality given in [Paz12]

$$|h_\Theta(A, L) - \frac{1}{2} h_{\mathrm{F}^+}(A/\overline{\mathbb{Q}})| \leq 6 \cdot 4^{2g} \log(4^{2g}) \log(h_\Theta(A, L) + 2), \tag{6}$$

it will lead to the lower bound we seek for the Faltings height of A as explained in Step 6.

By Proposition 3.9 of [DaPh02] page 665, one has for any algebraic subvariety $V \subset A$ the inequality (where $N = 16^g - 1$)

$$|\widehat{h}_{\mathbb{P}^N}(V) - h_{\mathbb{P}^N}(V)| \leq c_9(g, \dim V, \deg V, h_\Theta(A, L)),$$

where $h_{\mathbb{P}^N}(V)$ is the height of the variety V as defined in [DaPh02] page 644, the height $\widehat{h}_{\mathbb{P}^N}(V)$ is defined in [Phi91] in Proposition 9 and the quantity $c_9(g, \dim V, \deg V, h_\Theta(A, L)) > 0$ can be taken to be $(4^{g+1}h_\Theta(A, L) + 3g\log 2)\cdot(\dim V + 1)\cdot \deg V$. Picking $V = A$, one gets $\widehat{h}_{\mathbb{P}^N}(A) = 0$, $\dim A = g$, $\deg_L A = 16^g g!$ and

$$h_{\mathbb{P}^N}(A) \leq c_{10}(g)(h_\Theta(A, L) + 1), \tag{7}$$

where $c_{10}(g) > 0$ only depends on the dimension of A, and one can take $c_{10}(g) = 4^{3g+1}(g!)(g+1)$. Hence giving a lower bound on the height $h_{\mathbb{P}^N}(A)$ will imply a lower bound on the theta height, which in turn will imply a lower bound on the Faltings height by (6).

By Theorem 1.3 page 760 of [Rém10] and Proposition 1.1 page 760 of [Rém10] one has that for any curve C in $\mathbb{P}^N$ of genus g_0 and degree $\deg C$ there exists a quantity $c_{11}(g_0, \deg C) > 0$ such that

$$h_\Theta(J_C, L_\Theta) \leq c_{11}(g_0, \deg C)(h_{\mathbb{P}^N}(C) + 1), \tag{8}$$

where L_Θ is the polarization associated to the theta divisor on J_C. As C is embedded into its jacobian by a theta embedding, one has $\deg(C) = g_0$ and one can even take $c_{11} = (6g_0)^{121 g_0 8^{g_0}}$.

Step 4. The next goal is now to find an algebraic curve C on A of genus $g_0 \leq c_{12}(g)$ such that $h_{\mathbb{P}^N}(C) \leq c_{12}(g)h_{\mathbb{P}^N}(A)$. The proposition is already proved for $g = 1$, we may well suppose that $g \geq 2$ from now on. We will cut A by $g - 1$ hyperplanes $H_1, \dots, H_{g-1}$ in general position of height $h(H_i) \leq c_{13}(g)h_{\mathbb{P}^N}(A)$. Using Bertini's Theorem given in Theorem II.8.18 of [Har06] page 179, there exists a dense open subset U such that for any hyperplane H in U, the intersection $A \cap H$ is non-singular and connected. As $\overline{\mathbb{Q}}$ is algebraically closed, one has $U(\overline{\mathbb{Q}}) \neq \emptyset$, so there exist hyperplanes H with coordinates in $\overline{\mathbb{Q}}$ and $A \cap H$ a geometrically connected non-singular variety in $\mathbb{P}^N$. To be able to choose hyperplans H_i with height $h(H_i) \leq c_{13}(g)h_{\mathbb{P}^N}(A)$, we use the following argument: assume we have an infinite set S_M of algebraic numbers of height less that M, where $M \geq 0$ is a fixed real number. This set can be infinite because we don't impose an upper bound on the degree of these algebraic numbers. Consider the infinite set of all lines in the dual projective space $\check{\mathbb{P}}^N$ with coefficients in S_M. As U is an open dense subset, its complement can't contain all these lines, so there exists infinitely many lines intersecting U. Pick one of these lines. It provides us with the desired hyperplane H_i in $\mathbb{P}^N$. Repeat the argument $g - 1$ times to obtain a smooth curve C, geometrically connected on A, of genus g_0. Furthermore, we would like to ensure that the resulting field extension used to define C will remain as little ramified as possible. The choice of the set S_M is then crucial, we will now take the time to explain how it is done.

Classical existence theorems for infinite unramified extensions of a given number field often come from the application of the Golod-Shafarevich inequality (see [GoSha64]). A quadratic field with at least 5 different prime factors generally admits such an extension. The following result is of a similar spirit. Let $k = \mathbb{Q}(\sqrt{-643 \cdot 1318279381})$. By Maire [Mai00], the quadratic field k admits an infinite everywhere unramified extension $k^\dagger$, which is a tower of unramified

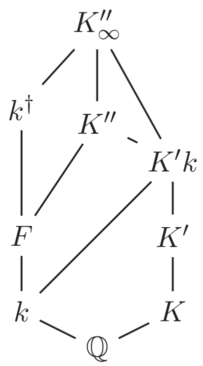
2-extensions. Recall $K' = K(A[16])$. Let $K'k$ be the compositum of K' and k over $\mathbb{Q}$ and let $K''_\infty = k^\dagger K'k$ be the compositum of $k^\dagger$ and $K'k$ over k. Then $K''_\infty/K'k$ is unramified (classical, see Proposition B.2.4 page 592 of [BoGu07] for instance). We want to find small algebraic numbers in this infinite extension.

Let $F \subset k^\dagger$ be a finite extension of k. By applying Minkowski's convex body Theorem as in the proof of Theorem B.2.14 page 595 of [BoGu07][3], there exists a non-zero algebraic number α_F in $\mathcal{O}_F$ generating F over $\mathbb{Q}$ (this is important) and with logarithmic absolute Weil height less than $\log|\Delta_{F/\mathbb{Q}}|^{1/[F:\mathbb{Q}]}$. Now $|\Delta_{F/\mathbb{Q}}|^{1/[F:\mathbb{Q}]} = |\Delta_{k/\mathbb{Q}}|^{1/2}$ because F/k is unramified and $[k:\mathbb{Q}] = 2$, and $\log|\Delta_{k/\mathbb{Q}}|^{1/2}$ is bounded from above by $\log 10^6 < 14$. Varying F along the tower, we get infinitely many α_F because each α_F is primitive in F, hence they are pairwise distincts. We gather all these α_F to define the set $S_M \subset K''_\infty$, for $M = 14$, and thus get a curve C defined over a finite[4] extension $K'' \subset K''_\infty$ unramified over $K'k$ and with $c_{13}(g) = 14$.

Note that $[K'k:\mathbb{Q}] \leq [k:\mathbb{Q}][K':\mathbb{Q}] = 2[K':\mathbb{Q}]$, and $[K'k:\mathbb{Q}] = [K'k:K'][K':\mathbb{Q}]$, hence

$$[K'k : K'] \leq 2. \tag{9}$$

Here is a picture to help the reader follow the construction.



We end by a last field extension to be able to use the theta height of Jac(C), we pose $K^\diamond = K''(\mathrm{Jac}(C)[16])$. The jacobian of C is now semi-stable and Lemma 4.7 page 2078 of [GaRe14a] implies

$$[K^\diamond : K''] \leq 16^{4g_0^2}. \tag{10}$$

The control on the height of the intersection defining C and on the degree of the intersection is provided by Proposition 2.3 page 765 of [Rém10] which gives in our situation, as $\deg A = 16^g g!$ and $h(H_i) \leq c_{13}(g)h_{\mathbb{P}^N}(A)$,

$$h_{\mathbb{P}^N}(C) \leq h_{\mathbb{P}^N}(A \cap H_1 \cap \cdots \cap H_{g-1}) \leq c_{14}(g)(h_{\mathbb{P}^N}(A) + 1), \tag{11}$$

where one can take $c_{14}(g) = g(16^g g!) + 14$. We also need to control the genus g_0 of the curve C. Using calculations on the successive Hilbert polynomials of

[3]See also [VaWi13] for better bounds in some cases.

[4]In the end the curve is defined with a finite number of coefficients in S_M and K'.

$A \cap H_1 \cap \cdots \cap H_i$, one can take the explicit bound $g_0 \leq 6^g g! g^2 = c_{12}(g)$, see [CaTa12] for the details[5].

Step 5. The conjunction of (8), (11), (7) and the fact that $g_0 \leq c_{12}(g)$ imply that over the finite extension $K^\diamond/K$ there exists a curve C on A such that

$$h_\Theta(J_C, L_\Theta) \leq c_{15}(g)(h_\Theta(A, L) + 1) \tag{12}$$

where one can take $c_{15}(g) = (12g)^{12g^{12g^{2g}}}$, and by the last section of [CaTa12] we have a closed immersion $A \to J_C$. By the Poincaré Reducibility Theorem, this implies that there exists an abelian variety B such that J_C is isogenous to $A \times B$. Isogenous abelian varieties share the same bad reduction primes by the Néron-Ogg-Shafarevich criterion, because they have the same Tate modules (see Theorem 1 page 493 of [SeTa68] and Corollary 2 page 22 of [Fa86]). Thus, if we denote $d^\diamond = [K^\diamond : \mathbb{Q}]$, we get that

$$\frac{1}{d^\diamond} \sum_{\mathfrak{p}^\diamond \text{ bad for } A} \delta_{\mathfrak{p}^\diamond}(C) \log \mathcal{N}_{K^\diamond/\mathbb{Q}}(\mathfrak{p}^\diamond) \leq \frac{1}{d^\diamond} \sum_{\mathfrak{p}^\diamond \subset O_{K^\diamond}} \delta_{\mathfrak{p}^\diamond}(C) \log \mathcal{N}_{K^\diamond/\mathbb{Q}}(\mathfrak{p}^\diamond). \tag{13}$$

Step 6. Let us show that we have reduced the proof to the case of jacobians of curves. Following the previous steps we get

$$\begin{aligned} \frac{1}{d^\diamond} \sum_{\mathfrak{p}^\diamond \subset O_{K^\diamond}} \delta_{\mathfrak{p}^\diamond}(C) \log \mathcal{N}_{K^\diamond/\mathbb{Q}}(\mathfrak{p}) &\underset{\text{(i)}}{\leq} h_{\mathrm{F}^+}(J_C/K^\diamond) \underset{\text{(ii)}}{\ll} h_\Theta(J_C, L_\Theta) \\ &\underset{\text{(iii)}}{\ll} h_\Theta(A, L) \underset{\text{(iv)}}{\ll} h_{\mathrm{F}^+}(A/K^\diamond), \end{aligned}$$

where the implied constants (multiplicative and additive) depend only on g and the successive inequalities are

- (i) is the case of curves given by inequality (4),
- (ii) is the comparison between the theta height and the Faltings height of [Paz12] as recalled in (6),
- (iii) is inequality (12),
- (iv) is again (6).

If the curve C was defined over K, we could use on the far left side the invariance property (3). In the general case we have nevertheless inequality (13), and we get from there

$$\frac{1}{d^\diamond} \sum_{\substack{\mathfrak{p}^\diamond \subset \mathcal{O}_{K^\diamond} \\ \text{bad for } A}} \delta_{\mathfrak{p}^\diamond}(C) \log \mathcal{N}_{K^\diamond/\mathbb{Q}}(\mathfrak{p}^\diamond) \geq \frac{1}{d} \sum_{\substack{\mathfrak{p} \subset \mathcal{O}_K \\ \text{bad for } A}} \Big(\sum_{\mathfrak{p}^\diamond | \mathfrak{p}} \frac{f_{\mathfrak{p}^\diamond/\mathfrak{p}}}{[K^\diamond : K]} \Big) \log \mathcal{N}_{K/\mathbb{Q}}(\mathfrak{p}) \tag{14}$$

[5] Let us also remark that one can embed the curve in $\mathbb{P}^3$, then using a theorem of Castelnuovo for curves in $\mathbb{P}^3$ given in Theorem 6.4 page 351 of [Har06], one has $g_0 \leq \deg_{\mathbb{P}^3}(C)^2$.

where $f_{\mathfrak{p}^\diamond/\mathfrak{p}}$ is the residual degree. Indeed, if $\mathfrak{p}^\diamond$ is a bad prime for A, it is also a bad prime for $\mathrm{Jac}(C)$, hence also a bad prime for C (the converse statement is wrong), hence $\delta_{\mathfrak{p}^\diamond}(C) \geq 1$. Using

$$[K^\diamond : K] = \sum_{\mathfrak{p}^\diamond|\mathfrak{p}} e_{\mathfrak{p}^\diamond/\mathfrak{p}} f_{\mathfrak{p}^\diamond/\mathfrak{p}} \leq \Big(\max_{\mathfrak{p}^\diamond|\mathfrak{p}} e_{\mathfrak{p}^\diamond/\mathfrak{p}}\Big) \sum_{\mathfrak{p}^\diamond|\mathfrak{p}} f_{\mathfrak{p}^\diamond/\mathfrak{p}},$$

one gets in (14)

$$\frac{1}{d^\diamond} \sum_{\mathfrak{p}^\diamond \text{ bad for } A} \delta_{\mathfrak{p}^\diamond}(C) \log \mathcal{N}_{K^\diamond/\mathbb{Q}}(\mathfrak{p}^\diamond) \geq \frac{1}{d} \sum_{\mathfrak{p} \text{ bad for } A} \frac{1}{\max_{\mathfrak{p}^\diamond|\mathfrak{p}} e_{\mathfrak{p}^\diamond/\mathfrak{p}}} \log \mathcal{N}_{K/\mathbb{Q}}(\mathfrak{p})$$

and

$$\frac{1}{d} \sum_{\mathfrak{p} \text{ bad for } A} \frac{1}{\max_{\mathfrak{p}^\diamond|\mathfrak{p}} e_{\mathfrak{p}^\diamond/\mathfrak{p}}} \log \mathcal{N}_{K/\mathbb{Q}}(\mathfrak{p}) \geq \frac{1}{2 \cdot 16^{4(g^2+g_0^2)} d} \log N^0_{A/K}$$

where this last inequality holds because the ramification index is controlled by

$$e_{\mathfrak{p}^\diamond/\mathfrak{p}} \leq [K^\diamond : K''][K'' : K'k][K'k : K'][K' : K] \leq 2 \cdot 16^{4g^2} \cdot 16^{4g_0^2}$$

as $K''/K'k$ is unramified and as one has (5), (9) and (10).

One concludes by $h_{\mathrm{F}^+}(A/K^\diamond) = h_{\mathrm{F}^+}(A/K)$ on the far right side because A/K is already semi-stable. At each and every step an explicit constant is provided, an easy calculation leads to $c_5 = (12g)^{-12g^{12g^{3.5g}}}$ and $c_6 = -1/c_5$ for the general case. □

3.3 *Reducing to the semi-stable case*

We explain in this section how to use base change properties to derive the general case from the semi-stable case. Let us start by the following definition.

Definition 3.3. *Let A be an abelian variety defined over a discrete valuation field $K_\mathfrak{p}$ and let $K'_{\mathfrak{p}'}$ be a finite extension of $K_\mathfrak{p}$ where A has semi-stable reduction, with ramification index $e_{\mathfrak{p}'/\mathfrak{p}}$, where $\mathfrak{p}'$ is a prime above $\mathfrak{p}$, and $\omega_{A/K_\mathfrak{p}}$ the determinant of differentials. Let $h_\mathfrak{p} : \mathcal{A}_{\mathcal{O}_{K_\mathfrak{p}}} \times_{\mathcal{O}_{K_\mathfrak{p}}} \mathcal{O}_{K'_{\mathfrak{p}'}} \to \mathcal{A}_{\mathcal{O}_{K'_{\mathfrak{p}'}}}$ be the canonical base change morphism. Let* $\mathrm{Lie}(h_\mathfrak{p})$ *be the induced injective morphism on differentials. Let*

$$c(A, \mathfrak{p}, \mathfrak{p}') = \frac{1}{e_{\mathfrak{p}'/\mathfrak{p}}} \mathrm{length}_{\mathcal{O}_{K'_{\mathfrak{p}'}}} \mathrm{coker}(\mathrm{Lie}(\mathrm{h}_\mathfrak{p}))$$

be the base change conductor, where if $\Gamma(.,.)$ *stands for global sections one has*

$$\mathrm{coker}(\mathrm{Lie}(\mathrm{h}_\mathfrak{p})) = \frac{\Gamma(\mathrm{Spec}(\mathcal{O}_{K_\mathfrak{p}}), \omega_{A/K_\mathfrak{p}}) \otimes \mathcal{O}_{K'_{\mathfrak{p}'}}}{\Gamma(\mathrm{Spec}(\mathcal{O}_{K'_{\mathfrak{p}'}}), \omega_{A/K'_{\mathfrak{p}'}})}.$$

This conductor was defined by Chai in [Cha00], see also the reference [HaNi12] pages 90–98. It satisfies in particular the two following key properties.

Proposition 3.4. *Let A be an abelian variety defined over a discrete valuation field $K_{\mathfrak{p}}$ and let $K'_{\mathfrak{p}'}$ be a finite extension of $K_{\mathfrak{p}}$ where A has semi-stable reduction with base change conductor $c(A, \mathfrak{p}, \mathfrak{p}')$. Then one has*

(1) $c(A, \mathfrak{p}, \mathfrak{p}') = 0$ if and only if $A/K_{\mathfrak{p}}$ has semi-stable reduction,
(2) if A is not semi-stable at $\mathfrak{p}$, then $c(A, \mathfrak{p}, \mathfrak{p}') \geq 1/e_{\mathfrak{p}'/\mathfrak{p}}$.

Proof. The proof goes along the same lines as Proposition 4.3 of [Paz14] which deals with elliptic curves. As it is relatively short, we give it here for abelian varieties. Let us start by assuming that $A/K_{\mathfrak{p}}$ has semi-stable reduction. Denote by $\mathcal{A}^0_{\mathcal{O}_{K_{\mathfrak{p}}}}$ the identity component of the Néron model of A over $K_{\mathfrak{p}}$, one then has $\mathcal{A}^0_{\mathcal{O}_{K_{\mathfrak{p}}}} \otimes \mathcal{O}_{K'_{\mathfrak{p}'}} \simeq \mathcal{A}^0_{\mathcal{O}_{K'_{\mathfrak{p}'}}}$ by Corollaire 3.3 page 348 of SGA 7.1 [SGA72], hence the differentials are the same, so $c(A, \mathfrak{p}, \mathfrak{p}') = 0$.

Reciprocally, one still has a map $\Phi : \mathcal{A}^0_{\mathcal{O}_{K_{\mathfrak{p}}}} \otimes \mathcal{O}_{K'_{\mathfrak{p}'}} \to \mathcal{A}^0_{\mathcal{O}_{K'_{\mathfrak{p}'}}}$. As $c(A, \mathfrak{p}, \mathfrak{p}') = 0$, the Lie algebras are the same and as Φ is an isomorphism on the generic fibers, Φ is birational. On the special fiber, Φ has finite kernel and is thus surjective because the dimensions are equal, here again because $c(A, \mathfrak{p}, \mathfrak{p}') = 0$.

We have that Φ is quasi-finite and birational. As $\mathcal{A}_{\mathcal{O}_{K'_{\mathfrak{p}'}}}$ is normal, by Zariski's Main Theorem found in Corollary 4.6 page 152 of [Liu02] for instance, Φ is an open immersion. So Φ is surjective and is also an open immersion, hence an isomorphism. This implies that $A/K_{\mathfrak{p}}$ is semi-abelian, and proves part (1). Part (2) is easier, if A is not semi-stable then the length in the definition of $c(A, \mathfrak{p}, \mathfrak{p}')$ is a positive integer, hence bigger than 1. □

We need a lemma.

Lemma 3.5. *Let Uns denote the set of unstable primes of A over K. Let K' be a number field extension of K over which A has semi-stable reduction everywhere. Then one has*

$$h_{\mathrm{F}^+}(A/K) - h_{\mathrm{F}^+}(A/K') \geq \frac{1}{[K' : \mathbb{Q}]} \sum_{\mathfrak{p} \in Uns} \log \mathcal{N}_{K/\mathbb{Q}}(\mathfrak{p}). \tag{15}$$

Proof. For a field F, we denote by $\mathcal{A}_{\mathcal{O}_F}$ the Néron model of A over the base Spec $\mathcal{O}_F$. As K' is a finite extension of K, we have

$$h_{\mathrm{F}^+}(A/K) - h_{\mathrm{F}^+}(A/K') = \frac{1}{[K : \mathbb{Q}]} \deg(\omega_{\mathcal{A}_{\mathcal{O}_K}}) - \frac{1}{[K' : \mathbb{Q}]} \deg(\omega_{\mathcal{A}_{\mathcal{O}_{K'}}}), \tag{16}$$

i.e. the archimedean parts cancel out. Let $\phi : K \to K'$ be the inclusion, we have a morphism $\omega_{\mathcal{A}_{\mathcal{O}_{K'}}} \to \phi^* \omega_{\mathcal{A}_{\mathcal{O}_K}}$, taking degrees (see also the proof of Lemme 1.23 page 35 of [Del85]) one obtains

$$[K' : K] \deg(\omega_{\mathcal{A}_{\mathcal{O}_K}}) = \deg(\phi^* \omega_{\mathcal{A}_{\mathcal{O}_K}}),$$

and

$$\deg(\phi^* \omega_{\mathcal{A}_{\mathcal{O}_K}}) = \deg(\omega_{\mathcal{A}_{\mathcal{O}_{K'}}}) + \sum_{\mathfrak{p} \subset \mathcal{O}_K} \sum_{\mathfrak{p}' | \mathfrak{p}} \mathrm{length}_{\mathcal{O}_{K'_{\mathfrak{p}'}}} (\mathrm{coker} \phi) \log \mathcal{N}_{K'/\mathbb{Q}}(\mathfrak{p}'),$$

hence using Proposition 3.4 we obtain

$$[K':K]\deg(\omega_{\mathcal{A}_{\mathcal{O}_K}}) \geq \deg(\omega_{\mathcal{A}_{\mathcal{O}_{K'}}}) + \sum_{\mathfrak{p}\in Uns}\sum_{\mathfrak{p}'|\mathfrak{p}} \frac{[K':K]}{e_{\mathfrak{p}'/\mathfrak{p}}}\log \mathcal{N}_{K/\mathbb{Q}}(\mathfrak{p}),$$

hence dividing by $[K':\mathbb{Q}] = [K':K][K:\mathbb{Q}]$, and using $e_{\mathfrak{p}'/\mathfrak{p}} \leq [K':K]$

$$\frac{1}{[K:\mathbb{Q}]}\deg(\omega_{\mathcal{A}_{\mathcal{O}_K}}) \geq \frac{1}{[K':\mathbb{Q}]}\deg(\omega_{\mathcal{A}_{\mathcal{O}_{K'}}}) + \frac{1}{[K':\mathbb{Q}]}\sum_{\mathfrak{p}\in Uns}\log \mathcal{N}_{K/\mathbb{Q}}(\mathfrak{p}),$$

which gives the result by using (16). □

We are now ready to perform a base change on the inequality of Proposition 3.2, which will be the completion of the proof of Theorem 1.1.

Proposition 3.6 (Final step in the proof of Theorem 1.1). *Let $g \geq 1$ be an integer and K a number field of degree d. There exists $c_{16}(g) > 0$ and $c_{17}(g) \in \mathbb{R}$ such that for any abelian variety (not necessarily semi-stable) A defined over K, with dimension g, one has*

$$h_{\mathrm{F}^+}(A/K) \geq c_{16}\frac{1}{d}\log N^0_{A/K} + c_{17},$$

and one can take $c_{16} = c_5/12^{4g^2}$ and $c_{17} = c_6$. If A is the jacobian of a curve, one can take $c_{16} = 1/12^{4g^2+1}$ and $c_{17} = 0$.

Proof. Let $N^{st}_{A/K}$ be the product of the norms of primes where A has semi-stable bad reduction. Let $N^{uns}_{A/K}$ be the product of the norms of primes where A has unstable bad reduction. By definition one has $N^0_{A/K} = N^{st}_{A/K}N^{uns}_{A/K}$. Let K' be a number field extension of K such that A acquires semi-stable reduction everywhere over K'. Using equality (15), one gets

$$h_{\mathrm{F}^+}(A/K) \geq h_{\mathrm{F}^+}(A/K') + \frac{1}{[K':\mathbb{Q}]}\log N^{uns}_{A/K}.$$

As A/K' has semi-stable reduction everywhere, one obtains by Proposition 3.2 that

$$h_{\mathrm{F}^+}(A/K') \geq c_5(g)\frac{1}{d'}\log N^{st}_{A/K'} + c_6(g).$$

Recall (use Theorem 6.2 page 413 of [SiZa95]) that one may choose the explicit extension $K' = K[A[12]]$, hence the degree $d' = [K':\mathbb{Q}]$ is controlled by the degree $d = [K:\mathbb{Q}]$ and by the dimension of A; for instance, apply Lemma 4.7 page 2078 of [GaRe14a] to obtain $d' = [K[A[12]]:K] \leq 12^{4g^2}$. Now one has (with sums taken over semi-stable bad primes of A)

$$\begin{aligned}\frac{1}{d'}\log N^{st}_{A/K'} &= \frac{1}{d'}\sum_{\mathfrak{p}'\subset\mathcal{O}_{K'}}\log\mathcal{N}_{K'/\mathbb{Q}}(\mathfrak{p}') \\ &\geq \frac{1}{d}\sum_{\mathfrak{p}\subset\mathcal{O}_K}\frac{1}{\max\limits_{\mathfrak{p}'|\mathfrak{p}} e_{\mathfrak{p}'/\mathfrak{p}}}\log\mathcal{N}_{K/\mathbb{Q}}(\mathfrak{p}) \geq \frac{1}{12^{4g^2}d}\log N^{st}_{A/K}\end{aligned}$$

because $e_{\mathfrak{p}'/\mathfrak{p}} \leq [K' : K]$ and so gathering the estimates we obtain

$$h_{\mathrm{F}^+}(A/K) \geq c_{18}\frac{1}{d}\log N_{A/K}^{st} + c_{19}\frac{1}{d}\log N_{A/K}^{uns} + c_{17} \geq \min\{c_{18}, c_{19}\}\frac{1}{d}\log N_{A/K}^{0} + c_{17},$$

where the quantities c_{17}, c_{18}, c_{19} only depend on g. □

Note that for $g = 1$, Proposition 3.6 is an improvement on Proposition 4.4 page 57 of [Paz14], both in the result and in the presentation: an equality of prime norms is incorrect in *loc. cit.* because of possible ramification of stable primes of K'/K, but the proof fortunately led to a weaker inequality in the end, so the result stated in *loc. cit.* still holds, and anyhow the new result given here is better.

We obtain an easy proof of Corollary 1.2 as the sum of Theorem 3.1 and Proposition 3.6. Apply Proposition 3.6 to get $h_{\mathrm{F}^+}(A/K) \geq c_{16}\log N_{A/K}^{0} + c_{17}$ and Theorem 3.1 to get

$$16\,h_{\mathrm{F}^+}(A/K) \geq 16\,h_{\mathrm{F}^+}(A/\overline{\mathbb{Q}}) \geq \frac{1}{d}\sum_{v\in M_K^\infty} d_v\,\rho(A_v, L_v)^{-2} - 39g,$$

then sum these two inequalities.

We can now derive Corollary 1.3.

Proof of Corollary 1.3. We will use as a pivot the quantity $N_{A/K}^{0}$. Applying Theorem 5.1 of [Rém10] page 775, there exists quantities $c_{20} = c_{20}(K, g) > 0$ and $c_{21} = c_{21}(K, g) \geq 0$ such that $m_K \leq c_{20}(K, g)\log N_{A/K}^{0} + c_{21}(K, g)$. The quantities depend on the degree and the discriminant of the base field here. This last inequality doesn't require semi-stability of A. Applying Proposition 3.6 of the present text one obtains $\log N_{A/K}^{0} \leq c_{22}(K, g)\max\{h_{\mathrm{F}^+}(A/K), 1\}$, also valid in general. Use the explicit quantities (valid in general) of Theorem 5.1 of [Rém10] page 775, it leads to $m_K \leq 4g^3d^2 2^{8g^2}\log N_{A/K}^{0} + gd2^{8g^2}(\log|\Delta_K| + g^2d^2\log 16)$, and combine with Proposition 3.6. It proves the corollary. In the case of jacobians combine with Proposition 3.2 which gives $h_{\mathrm{F}^+}(J_C/K) \geq \frac{1}{12d}\log N_{J_C/K}^{0}$ in the semi-stable case and Proposition 3.6 which gives $h_{\mathrm{F}^+}(J_C/K) \geq \frac{1}{12d12^{4g^2}}\log N_{J_C/K}^{0}$ for the general case. □

4. Lang-Silverman conjecture and regulators

We give here a conjecture of Lang and Silverman ([Si84b] page 396[6] or [Paz12][7]). Throughout this section, we will use the notation $\overline{\mathrm{End}(A)\cdot P} = A$ to say that the set $\mathrm{End}(A)\cdot P$ is Zariski dense in A.

[6]This first version of the conjecture is known to be wrong, consider for instance the point $(P, 0)$ on a variety $A_1 \times A_2$ where P is non-torsion and let the height of A_2 tend to infinity. However the philosophy of the conjecture is clearly the same as the original statement, a generic point can't have too small height.

[7]This stronger version is also known to be wrong, see Remark 4.2 and section 5 of the present article for a clarification.

Conjecture 4.1 (Lang-Silverman). *Let $g \geq 1$ be an integer. For any number field K, there exists a positive quantity $c_{23} = c_{23}(K, g)$ such that for any abelian variety A/K of dimension g and any ample symmetric line bundle L on A, for any point $P \in A(K)$, one has:*

$$\left(\overline{\mathrm{End}(A)\cdot P} = A\right) \Rightarrow \left(\widehat{h}_{A,L}(P) \geq c_{23} \max\left\{h_{\mathrm{F}^+}(A/K),\ 1\right\}\right),$$

where $\widehat{h}_{A,L}(.)$ is the Néron-Tate height associated to the line bundle L and $h_{\mathrm{F}^+}(A/K)$ is the (relative) Faltings height of the abelian variety A/K.

Remark 4.2. We only require the condition $\mathrm{End}(A)\cdot P$ Zariski dense, not necessarily $\mathbb{Z}\cdot P$ Zariski dense. Let us consider the following situation: let A_1 be a simple abelian variety over K and let $A = A_1 \times A_1$. Choose $P = ([n]P_1, P_1) \in A(K)$. If P_1 is non-torsion, then $\overline{\mathbb{Z}\cdot P}$ is a strict abelian subvariety (of degree growing with n), whereas $\overline{\mathrm{End}(A)\cdot P} = A$. As one has $\widehat{h}_{A,L}(P) = (n^2+1)\widehat{h}_{A_1,L_1}(P_1)$ for the product polarization L, and as $h_{\mathrm{F}^+}(A/K) = 2\,h_{\mathrm{F}^+}(A_1/K)$, the point P satisfies the expected lower bound if the point P_1 does.

Proposition 4.3. *Assume the Lang-Silverman Conjecture 4.1. Let K be a number field and $g, m \geq 1$ be integers. There exists a quantity $c_{24} = c_{24}(K, g, m) > 0$ such that for any simple abelian variety A defined over K of dimension g, of rank m over K, polarized by an ample and symmetric line bundle L,*

$$\mathrm{Reg}_L(A/K) \geq \Big(c_{24} \max\{h_{\mathrm{F}^+}(A/K),\ 1\}\Big)^m.$$

Proof. Let us denote $h = \max\{h_{\mathrm{F}^+}(A/K),\ 1\}$ and for any $i \in \{1, \ldots, m\}$, the Minkowski ith-minimum $\lambda_i = \lambda_i(A(K)/A(K)_{\mathrm{tors}})$. Apply Minkowski's successive minima inequality to the Mordell-Weil lattice,

$$\lambda_1 \cdots \lambda_m \leq m^{m/2}(\mathrm{Reg}_L(A/K))^{1/2}.$$

Now, as A is simple, any non-torsion point satisfies $\overline{\mathrm{End}(A)\cdot P} = A$, so using m times the inequality of Conjecture 4.1 one gets

$$\mathrm{Reg}_L(A/K) \geq \frac{c_{23}^m h^m}{m^m}, \tag{17}$$

which gives the result. □

We thus obtain Theorem 1.5 as a corollary of Proposition 4.3. Indeed if the rank is non zero, as soon as the regulator, the rank and the dimension are bounded from above, the height will be bounded from above, hence the claimed finiteness. This may be expressed in other words by: the Lang-Silverman conjecture implies that the regulator $\mathrm{Reg}_L(A/K)$ satisfies a Northcott property on the set of polarized simple abelian varieties (modulo isomorphisms) of dimension g defined over a fixed number field K with $A(K)$ Zariski dense and Mordell-Weil rank bounded from above.

Remark 4.4. Back to inequality (17), in view of Corollary 1.3, we have $h \gg m$. Any improvement of the form $h \gg m^{1+\varepsilon}$ (for a fixed $\varepsilon > 0$) would lead to a stronger Northcott property, without assuming that the rank is bounded from above. See also the addendum [Paz16b].

5. A stronger lower bound conjecture

We would like to refine the conjecture[8] of Lang and Silverman to take care of the exceptional points in Conjecture 4.1: what can be said about the points P satisfying $\overline{\mathrm{End}(A)\cdot P} \subsetneq A$?

Conjecture 5.1 (Lang-Silverman, new strong version). *Let $g \geq 1$ be an integer. For any number field K, there exists two positive quantities $c_{33} = c_{33}(K, g)$ and $c_{34} = c_{34}(K, g)$ such that for any abelian variety A/K of dimension g and any ample symmetric line bundle L on A, for any point $P \in A(K)$, one has:*

- *either there exists an abelian subvariety $B \subset A$, $B \neq A$, of degree $\deg_L(B) \leq c_{34}\deg_L(A)$ and such that the order of the point P modulo B is bounded from above by c_{34},*
- *or one has $\mathrm{End}(A)\cdot P$ is Zariski dense and*

$$\widehat{h}_{A,L}(P) \geq c_{33}\max\left\{h_{\mathrm{F}^+}(A/K),\ 1\right\},$$

where $\widehat{h}_{A,L}(.)$ is the Néron-Tate height associated to the line bundle L and $h_{\mathrm{F}^+}(A/K)$ is the (relative) Faltings height of the abelian variety A/K.

This is a strong statement. It implies the strong torsion conjecture for example. Indeed, any torsion point $P \in A(K)_{\mathrm{tors}}$ falls into the first case because its canonical height is zero. Hence the order of P is bounded from above solely in terms of K and g and of the cardinality of the torsion subgroup of a strict abelian subvariety B. An easy induction on the dimension of A gives a bound on the order of P solely in terms of K and g, hence on the exponent of the torsion group as well, hence on the cardinal of the torsion group $A(K)_{\mathrm{tors}}$ as well.

This strong form of the conjecture is motivated by Théorème 1.4 page 511 of [Da93] and Théorèmes 1.8 and 1.13 of [Paz13]. Remark that in both of these works, the abelian varieties considered are principally polarized, hence the dependance in the degree of A is only through the dimension g.

Let us see now how this statement can help in understanding the link between the Mordell-Weil group $A(K)$ and the abelian subvarieties of A. The following quantity will play a key role in this paragraph.

Definition 5.2. *Let A be an abelian variety over a number field K. Let m_K denote the Mordell-Weil rank of $A(K)$. Define*

$$m_0 = \sup\{\mathrm{rank}(B(K)) \mid B \text{ strict abelian subvariety of } A\}.$$

We will call the relative quantity $m_K - m_0$ the Zariski rank *of the Mordell-Weil group $A(K)$.*

[8] Such an attempt has been proposed in Conjecture 1.8 of [Paz12], but it unfortunately fails because of situations similar to the one described in Remark 4.2 where certain points fall in the first case but should fall in the second instead. This was communicated to the author by the referee of another project, may he be warmly thanked here. We fix the problem by changing the condition given there as $\overline{\mathbb{Z}\cdot P} = A$ by the weaker $\overline{\mathrm{End}(A)\cdot P} = A$. We also add a dependance in $\deg_L(A)$ in the attempt to control the degree of B thanks to a remark of Gaël Rémond.

Note that $m_K - m_0 > 0$ is equivalent to $A(K)$ being Zariski dense in A. This Zariski rank could be compared with the following quantity for a number field K. If r_K is the rank of units in K, let r_0 denote the maximal rank of units in a strict subfield of K. As already noticed in [Paz14] in the easier case of elliptic curves, the Zariski rank $m_K - m_0$ plays the same role (at least when one gives lower bounds on the regulator in both contexts) as the relative rank of units $r_K - r_0$ for number fields.

The next lemma studies the size of the successive minima of the Mordell-Weil lattice modulo torsion, where the square of the norm is implicitly given by the Néron-Tate height. We believe this version could lead in the future to some improvements in Theorem 1.5.

Lemma 5.3. *Assume Conjecture 5.1. Let (A, L) be a polarized abelian variety of dimension g defined over a number field K. For any $i \in \{1, \dots, m_K\}$, let λ_i be the i-th successive minima of the lattice $A(K)/A(K)_{tors}$. Then there is a quantity $c_{35} = c_{35}(K, g, \deg_L(A)) > 0$ such that*

$$\begin{cases} \text{for any } i, & \lambda_i^2 \geq c_{35}\, i, \\ \text{if } i > m_0, & \lambda_i^2 \geq c_{35} \max\{1, h_{\mathrm{F}^+}(A/K)\}. \end{cases}$$

Proof. Within the proof, we will use the symbol c_* for a positive quantity only depending on g, on K and on $\deg_L(A)$. We allow the value of this quantity c_* to vary at some steps within the proof, as long as it depends only on g, on K and on $\deg_L(A)$ and stays positive. If $c_{34}(K, g)$ denotes the quantity appearing in Conjecture 5.1, denote by $\overline{c_{34}} = \max\{1, \max_{1 \leq i \leq g} c_{34}(K, i)\}$, the field K being fixed.

Let $\mathcal{B}$ denote the set of all abelian subvarieties B in A of degree bounded from above by $\overline{c_{34}}^g \deg_L(A)$: it contains the subvarieties appearing in the first case of Conjecture 5.1, and we raise $\overline{c_{34}}$ to the power g to be able to use an induction on the dimension g towards the end. This is a finite set with cardinal bounded from above by a quantity depending only on g, on K (because $\overline{c_{34}}$ only depends on g and K) and on $\deg_L(A)$. The reader interested in an explicit upper bound for the cardinal of this set can refer to Proposition 4.1 page 529 of [Rém00].

Choose an integer $i \in \{1, \dots, m_K\}$ and define

$$Z_i = \bigcup_{\substack{B \in \mathcal{B} \\ \mathrm{rank}(B(K)) < i}} B(K).$$

The set $A(K) \backslash Z_i$ is non-empty, because the rank of the lattices in the finite union is always strictly smaller than m_K. Let P_i be a non-torsion point of minimal height lying in $A(K) \backslash Z_i$. Apply the "Lemme d'évitement" of Gaudron-Rémond given in Théorème 1.1 page 125 of [GaRe12] to obtain $\widehat{h}_{A,L}(P_i) \leq M \lambda_i(A(K))^2$, where M is positive and bounds from above the cardinality of $\mathcal{B}$, which can be chosen depending only on g, on K and on $\deg_L(A)$ in view of Conjecture 5.1.

On the one hand if $\mathrm{End}(A) \cdot P_i$ is dense in A, by Conjecture 5.1 one has $\widehat{h}_{A,L}(P_i) \geq c_* \max\{1, h_{\mathrm{F}^+}(A/K)\}$. We add that $\max\{1, h_{\mathrm{F}^+}(A/K)\} \geq c_* m_K$ by applying the Corollary 1.3, and $m_K \geq i$ by definition.

On the other hand if $\mathrm{End}(A)\cdot P_i$ is not dense in A, by Conjecture 5.1 there exists an abelian variety $B \in \mathcal{B}$ such that the order of P_i is less than c_{34} modulo B, then by definition of m_0 one has $\mathrm{rank}(B(K)) \leq m_0$ and by choice of P_i one has $\mathrm{rank}(B(K)) \geq i$, hence $m_0 \geq i$.

Apply Conjecture 5.1 to $P_i \in B(K)$ (modulo torsion in A). If $\mathrm{End}(B)\cdot P_i$ is dense in B one obtains

$$\widehat{h}_{A,L}(P_i) = \widehat{h}_{B,L}(P_i) \geq c_* \max\{1, h_{\mathrm{F}^+}(B/K)\},$$

then again using Corollary 1.3 one gets $\widehat{h}_{A,L}(P_i) \geq c_*\mathrm{rank}(B(K)) \geq c_* i$. If $\mathrm{End}(B)\cdot P_i$ is not dense in B, we are reduced to the case of a strict abelian subvariety of A. There exists an abelian subvariety $B_1 \subset B$ of degree bounded from above by $c_{34}\deg_L(B)$ such that P_i has order bounded from above by $\overline{c_{34}}$ modulo B_1. As $\deg_L(B) \leq \overline{c_{34}}\deg_L(A)$, one has $\deg_L(B_1) \leq \overline{c_{34}}^2\deg_L(A)$, hence $\deg_L(B_1) \leq \overline{c_{34}}^g\deg_L(A)$ so $B_1 \in \mathcal{B}$. As P_i avoids Z_i one has again $\mathrm{rank}(B_1(K)) \geq i$. If $\mathrm{End}(B_1)\cdot P_i$ is dense in B_1, then

$$\widehat{h}_{A,L}(P_i) \geq c_* \max\{1, h_{\mathrm{F}^+}(B_1/K)\} \geq c_*\mathrm{rank}(B_1(K)) \geq c_* i.$$

If $\mathrm{End}(B_1)\cdot P_i$ is not dense in B_1, one continues by induction until one reaches a strict abelian subvariety B_n such than $\mathrm{End}(B_n)\cdot P_i$ is dense in B_n, which will eventually be the case when B_n is simple for instance. It gives the lemma. □

Proposition 5.4. *Assume Conjecture 5.1. Let K be a number field, let $g \geq 1$ be an integer, let $m \geq 0$ be an integer. There exists a quantity $c_{36} = c_{36}(K, g, m) > 0$ such that for any principally polarized abelian variety A defined over K of dimension g, equipped with an ample and symmetric line bundle L, with $A(K)$ of rank m,*

$$\mathrm{Reg}_L(A/K) \geq \Big(c_{36}\max\{h_{\mathrm{F}^+}(A/K),\ 1\}\Big)^{m-m_0}.$$

Proof. Let us denote $h = \max\{h_{\mathrm{F}^+}(A/K),\ 1\}$ and $m = \mathrm{rank}(A(K))$, and for any $i \in \{1,\dots,m\}$, $\lambda_i = \lambda_i(A(K)/A(K)_{\mathrm{tors}})$.

The inequality is trivial for $m = 0$. From now on, let us assume $m \neq 0$. Apply Minkowski's successive minima inequality to the Mordell-Weil lattice,

$$\lambda_1^2\cdots\lambda_m^2 \leq m^m\mathrm{Reg}_L(A/K).$$

Now apply lemma 5.3 with $\deg_L(A) = g!$ to get

$$\mathrm{Reg}_L(A/K) \geq \frac{c_{35}^{m-m_0}h^{m-m_0}\lambda_1^2\cdots\lambda_{m_0}^2}{m^m}, \tag{18}$$

If $m_0 = 0$, the inequality is the one claimed. Let us suppose that $m_0 \neq 0$. Apply again Lemma 5.3 to get

$$\mathrm{Reg}_L(A/K) \geq m^{-m}(c_{35})^{m_0}(m_0!)\,(c_{35}h)^{m-m_0}. \tag{19}$$

Hence the claimed inequality, as $1 \leq m_0 \leq m$. □

Theorem 1.5 follows directly from Proposition 5.4, because the set of principally polarized abelian varieties defined over a fixed number field K, of fixed dimension g such that $A(K)$ is Zariski dense in A and with regulator and rank bounded from above is also a set of bounded height under Conjecture 5.1. Note that in view of (1), one can replace $\mathrm{Reg}_L(A/K)$ by $\mathrm{Reg}(A/K)$ in Theorem 1.5 because the polarization is principal.

6. Conclusion

We generalize here the last section of [Paz14] to abelian varieties, extending the dictionary given in [Hin07] as well.

	Number field K		Abelian variety A/K	
zeta function	$\zeta_K(s)$	$\leftrightarrow$	$L(A,s)$	L function
log of discriminant	$\log\|D_K\|$	$\leftrightarrow$	$h_{\mathrm{F}^+}(A)$	Faltings height
regulator	R_K	$\leftrightarrow$	$\mathrm{Reg}(A/K)$	regulator
class number	h_K	$\leftrightarrow$	$\|Ш(A/K)\|$	Tate-Shafarevitch group
torsion	$(U_K)_{\mathrm{tors}}$	$\leftrightarrow$	$(A\times\check{A})(K)_{\mathrm{tors}}$	torsion of A and dual $\check{A}$
degree	d	$\leftrightarrow$	g	dimension
max sub rank of units	r_0	$\leftrightarrow$	m_0	max rank of ab. subvar.
relative unit ranks	r_K-r_0	$\leftrightarrow$	m_K-m_0	Zariski rank of $A(K)$
CM field	$r_K=r_0$	$\leftrightarrow$	$m_K=m_0$	$A(K)$ non Z. dense
non-CM field	$r_K>r_0$	$\leftrightarrow$	$m_K>m_0$	$A(K)$ Zariski dense

Remark 6.5. One could prefer to put in link the property "$A(K)$ Zariski dense in A" with "K generated by units". Let us remark that $A(K)$ Zariski dense is equivalent to $m_K>m_0$, but on the number field side there exists some CM fields K that are generated by units, so K generated by units is not equivalent to $r_K>r_0$. However, regarding the finiteness property obtained from giving an upper bound for the regulator, one may replace the property of being non-CM by the property of being generated by units because there are only finitely many CM fields generated by units with regulator bounded from above. This property of generation, rather than being non-CM, could be seen as a better match to the density property of $A(K)$ on the abelian side.

References

[Aut13] P. Autissier, Un lemme matriciel effectif. *Mathematische Zeitschrift*, **273** (2013) 355–361.

[BoGu07] E. Bombieri and W. Gubler, Heights in Diophantine Geometry. *New Mathematical Monographs*, Cambridge University Press 2006 (reprint 2007) **4** (2007).

[Cha00] C.-L. Chai, Néron models for semiabelian varieties: congruence and change of base field. *Asian J. Math.*, **4** (2000) 715–736.

[CaTa12] A. Cadoret and A. Tamagawa, Notes on the torsion conjecture. In Groupes de Galois Géométriques et differentiels, P. Boalch and J.-M. Couveignes eds., Séminaires et Congrès, S.M.F. **27** (2012) 57–68.

[Da93] S. David, Minorations de hauteurs sur les variétés abéliennes. *Bull. Soc. Math. France*, **121** (1993) 509–544.

[DaPh02] S. David and P. Philippon, Minorations des hauteurs normalisées des sous–variétés de variétés abeliennes. II. *Comment. Math. Helv.*, **77** (2002) 639–700.

[Del85] P. Deligne, Preuve des conjectures de Tate et de Shafarevitch. *Séminaire N. Bourbaki*, **616** (1983–1984) 25–41.

[DeMu69] P. Deligne and D. Mumford, The irreducibility of the space of curves of given genus. *Publ. Math. IHES*, **36** (1969) 75–109.

[Fa83] G. Faltings, Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Invent. Math.*, **73** (1983) 349–366.

[Fa86] G. Faltings, Finiteness theorems for abelian varieties over number fields. *Arithmetic Geometry*, Cornell and Silverman (editors), Springer-Verlag, (1986) 9–27.

[GaRe12] E. Gaudron and G. Rémond, Lemmes de Siegel d'évitement. *Acta Arith.*, **154.2** (2012) 125–136.

[GaRe14a] E. Gaudron and G. Rémond, Polarisations et isogénies. *Duke Math. J.*, **163(11)** (2014) 2057–2108.

[GaRe14b] E. Gaudron and G. Rémond, Théorème des périodes et degrés minimaux d'isogénies. *Comment. Math. Helv.*, **89** (2014) 343–403.

[GoSha64] E. S. Golod and I. R. Shafarevich, On the class field tower (Russian). *Izv. Akad Nauk SSSR Ser. Mat.*, **28** (1964) 261–272.

[HaNi12] L. H. Halle and J. Nicaise, Néron models and base change, *Lecture Notes in Math.*, **2156** (2016).

[Har06] R. Hartshorne, Algebraic Geometry. *Graduate Texts in Mathematics*, Springer-Verlag, **52** (2006).

[Hin07] M. Hindry, Why is it difficult to compute the Mordell-Weil group? Diophantine geometry, *CRM Series, Ed. Norm.*, Pisa **4** (2007) 197–219.

[HiPa16] M. Hindry and A. Pacheco, An analogue of the Brauer-Siegel theorem for abelian varieties in positive characteristic, *Mosc. Math. J.*, **16** (2016) 45–93.

[Java14] A. Javanpeykar, Polynomial bounds for Arakelov invariants of Belyi curves. *Algebra and Number Theory*, **8.1** (2014) 89–140.

[Liu02] Q. Liu, Algebraic Geometry and Arithmetic Curves. *Oxford Graduate Texts in Mathematics*, Oxford Science Publications **6** (2002).

[Mai00] C. Maire, On infinite unramified extensions. *Pacific J. of Math.*, **192.1** (2000) 135–142.

[Mil08] J.-S. Milne, Abelian varieties. www.jmilne.org/math/**2.0** (2008).

[MB89] L. Moret-Bailly, La formule de Noether pour les surfaces arithmétiques. *Invent. Math.*, **98** (1989) 491–498.

[Paz10] F. Pazuki, Remarques sur une conjecture de Lang. *Journal de Théorie des Nombres de Bordeaux*, **22(1)** (2010) 161–179.

[Paz12] F. Pazuki, Theta height and Faltings height. *Bull. Soc. Math. France*, **140.1** (2012) 19–49.

[Paz13] F. Pazuki, Minoration de la hauteur de Néron-Tate sur les surfaces abéliennes. *Manuscripta Math.*, **142** (2013) 61–99.

[Paz14] F. Pazuki, Heights and regulators of number fields and elliptic curves. *Publ. Math. Besançon*, **2014/2** (2014) 47–62.

[Paz16a] F. Pazuki, Northcott property for the regulators of number fields and abelian varieties. *Oberwolfach Rep.*, **13** (2016).

[Paz16b] F. Pazuki, Erratum and addendum to "Heights and regulators of number fields and elliptic curves". *Publ. Math. Besançon*, **2016** (2016) 81–83.

[Phi91] P. Philippon, Sur les hauteurs alternatives I. *Math. Annalen*, **289** (1991) 255–283.

[Ray85] M. Raynaud, Hauteurs et isogénies. Seminar on arithmetic bundles: the Mordell conjecture (Paris, 1983/84), Astérisque, **127** (1985) 199–234.

[Rém00] G. Rémond, Décompte dans une conjecture de Lang. *Invent. Math.*, **142** (2000) 513–545.

[Rém05] G. Rémond, Inégalité de Vojta généralisée. *Bull. Soc. Math. France*, **133.4** (2005) 459–495.

[Rém10] G. Rémond, Nombre de points rationnels des courbes. *Proc. Lond. Math. Soc.*, **101.3** (2010) 759–794.

[SeTa68] J.-P. Serre and J. Tate, Good reduction of abelian varieties. *Annals of Math.*, **88.3** (1968) 492–517.

[SGA72] A. Grothendieck, Groupes de monodromie en géométrie algébrique. SGA 7.1, *Lecture Notes in Mathematics*, Springer-Verlag, **288** (1972).

[SiZa95] A. Silverberg and Yu. Zarhin, Semistable reduction and torsion subgroups of abelian varieties. *Ann. Inst. Fourier*, **45** (1995) 403–420.

[Si84b] J. H. Silverman, Lower bounds for height functions. *Duke Math. J.*, **51** (1984) 395–403.

[VaWi13] J. D. Vaaler and M. Widmer, A note on small generators of number fields. Diophantine methods, lattices and arithmetic theory of quadratic forms, *Contemp. Math.*, **587** (2013) 214–225.

[Wil17] R. Wilms, New explicit formulas for Faltings delta invariant. *Invent. Math.*, **209.2** (2017) 481–539.

Topics in Number Theory, RMS-Lecture Notes Series No. 26, 2020, pp. 133–146.

Some Examples of Higher Depth Vector-Valued Quantum Modular Forms

Kathrin Bringmann[1], Jonas Kaszian[2] and Antun Milas[3]

[1]Mathematical Institute, University of Cologne, Weyertal 86-90, 50931 Cologne, Germany.
e-mail: kbringma@math.uni-koeln.de

[2]Mathematical Institute, University of Cologne, Weyertal 86-90, 50931 Cologne, Germany.
e-mail: jkaszian@math.uni-koeln.de

[3]Department of Mathematics and Statistics, SUNY-Albany, Albany, NY 12222, U.S.A.
e-mail: amilas@albany.edu

Abstract. In this note, we continue our study of generalized quantum modular forms initiated in [4, 5]. We construct further examples of depth two quantum modular forms generalizing several results in [4]. In a special case (corresponding to $p = 2$) we present a more detailed analysis. In particular, a rank two higher depth quantum modular form for the full modular group is constructed.

Keywords. Quantum modular forms, false theta functions

2020 Subject Classification: 11F27, 11F37

1. Introduction and statement of results

For $p \in \mathbb{N}$, define the following $\mathfrak{sl}_3$ false theta function

$$F(q) := \sum_{\substack{m_1,m_2\geq 1\\ m_1\equiv m_2 \pmod 3}} \min(m_1,m_2) q^{\frac{p}{3}\left(m_1^2+m_2^2+m_1m_2\right)-m_1-m_2+\frac{1}{p}} \left(1-q^{m_1}\right)\left(1-q^{m_2}\right)\left(1-q^{m_1+m_2}\right).$$

This function was introduced in [3] as the numerator of the character of a certain W-algebra associated to $\mathfrak{sl}_3$. A more direct connection between the series and Lie theory can be readily seen from its coefficient $\min(m_1, m_2)$ – the value of Kostant's partition function of $\mathfrak{sl}_3$.

In [4] we decomposed F as

$$F(q) = \frac{2}{p} F_1\left(q^p\right) + 2F_2\left(q^p\right), \tag{1.1}$$

where F_1 and F_2 are generalizations of quantum modular forms. Roughly speaking Zagier [12] defined *quantum modular forms* to be function $f : \mathcal{Q} \to \mathbb{C}$ ($\mathcal{Q} \subset \mathbb{Q}$) such that the "obstruction to modularity"

$$f(\tau) - (c\tau + d)^{-k} f(M\tau) \qquad M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$$

is "nice". One can show quantum modular properties of the F_j by using two-dimensional Eichler integrals. For instance, as $\tau \to \frac{h}{k} \in \mathbb{Q}$, F_1 agrees with an integral of the shape ($q := e^{2\pi i\tau}$)

$$\int_{-\overline{\tau}}^{i\infty} \int_{w_1}^{i\infty} \frac{f(\boldsymbol{w})}{\sqrt{-i(w_1+\tau)}\sqrt{-i(w_2+\tau)}} dw_2 dw_1,$$

where $f \in S_{\frac{3}{2}}(\chi_1, \Gamma) \otimes S_{\frac{3}{2}}(\chi_2, \Gamma)$ (χ_j are certain multipliers and $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$). Throughout we write vectors in bold letters and their components with subscripts. The modular properties of the integral in (1.1) follow from the modularity of f which in turn gives quantum modular properties of F_1. We call the resulting functions higher depth quantum modular forms. Roughly speaking, *depth two quantum modular forms* satisfy, in the simplest case, the modular transformation property with $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$

$$f(\tau) - (c\tau + d)^{-k} f(M\tau) \in \mathcal{Q}_\kappa(\Gamma)\mathcal{O}(R) + \mathcal{O}(R), \tag{1.2}$$

where $\mathcal{Q}_\kappa(\Gamma)$ is the space of quantum modular forms of weight κ and $\mathcal{O}(R)$ the space of real-analytic functions defined on $R \subset \mathbb{R}$. In [5], we proved that F_1 and F_2 are components of vector-valued quantum modular forms of depth two, generalizing (1.2).

A natural question that arises is what the other components of the vector-valued forms are as q-series. To investigate this, we define, for $1 \le s_1, s_2 \le p \in \mathbb{N}$,

$$\mathbb{F}_{\boldsymbol{s}}(q) := \sum_{\substack{m_1,m_2 \ge 1 \\ m_1 \equiv m_2 \pmod 3}} \min(m_1, m_2) q^{\frac{p}{3}\left(\left(m_1 - \frac{s_1}{p}\right)^2 + \left(m_2 - \frac{s_2}{p}\right)^2 + \left(m_1 - \frac{s_1}{p}\right)\left(m_2 - \frac{s_2}{p}\right)\right)}$$
$$\times \left(1 - q^{m_1 s_1} - q^{m_2 s_2} + q^{m_1 s_1 + (m_1+m_2)s_2} + q^{m_2 s_2 + (m_1+m_2)s_1} - q^{(m_1+m_2)(s_1+s_2)}\right).$$

Note that $\mathbb{F}_{(1,1)}(q) = F(q)$. As discussed in [3] these series are in fact parametrized by dominant integral weights $(s_1-1)\omega_1+(s_2-1)\omega_2$ for $\mathfrak{sl}_3$, where ω_j are fundamental weights (dual to simple roots α_1 and α_2).

We may decompose $\mathbb{F}_{\boldsymbol{s}}$ as in (1.1) (see Lemma 2.1). The corresponding functions $\mathbb{F}_{1,\boldsymbol{s}}$ and $\mathbb{F}_{2,\boldsymbol{s}}$ are again generalized quantum modular forms. More precisely, we have.

Theorem 1.1. *The functions* $\mathbb{F}_{1,\boldsymbol{s}}$ *and* $\mathbb{F}_{2,\boldsymbol{s}}$ *are depth two quantum modular forms (with respect to some subgroup) of weights one and two, respectively.*

To prove Theorem 1.1, we show that $\mathbb{F}_{1,\boldsymbol{s}}(\tau)$ asymptotically agrees to infinite order with a certain Eichler integral $\mathcal{E}_{1,\boldsymbol{s}}(\frac{\tau}{p})$ defined in (2.1). Similarly, $\mathbb{F}_{2,\boldsymbol{s}}(\tau)$ asymptotically agrees with an Eichler integral $\mathcal{E}_{2,\boldsymbol{s}}(\frac{\tau}{p})$ given in (2.2).

We next restrict to the special case $p = 2$. It turns out (see Lemma 2.2) that for $p = 2$ all $\mathbb{F}_{2,\boldsymbol{s}}$ vanish. Thus we only need to consider $\mathbb{F}_{1,\boldsymbol{s}}$.

Theorem 1.2. *For* $p = 2$*, the space spanned by* $\mathcal{E}_{1,(1,1)}$ *and* $\mathcal{E}_{1,(1,2)}$ *is essentially invariant under modular transformations. By this we mean that the only terms appearing in the modular transformations which do not lie in the space are simpler (see* (2.6) *and* (2.7) *for the case of inversion).*

Motivated by representation theory of the W-algebra $W^0(p)_{A_2}$ studied in [3, 8], we raise the following.

Conjecture. *After multiplication with η^2, the characters of $W^0(p)_{A_2}$ given in [3, Section 5] (which also includes the series $\mathbb{F}_{\boldsymbol{s}}$) combine into a vector-valued quantum modular form of depth two.*

The second goal of this paper is to determine the asymptotic behavior of $\mathcal{E}_{1,\boldsymbol{s}}(it)$ as $t \to 0^+$. It is well-known that asymptotic behaviors of vector-valued modular forms (as $t \to 0^+$) can be computed by applying the S-transformation $\tau \mapsto -\frac{1}{\tau}$, and then analyzing the dominating term. This method is widely used for studying quantum dimensions of modules of vertex algebras (and affine Lie algebras) as their characters often transform invariantly under $\mathrm{SL}_2(\mathbb{Z})$. In this paper we work with functions (coming also from characters) that transform with higher depth error terms so their asymptotics are more interesting and harder to analyze. We show that asymptotic behavior of double Eichler integrals can be also analyzed by using a similar approach. We do this directly from the integral representation of the error function. In the body of the paper, we show that it is enough to study

$$\mathbb{E}_{1,(1,1)}(\tau) := 4I_{(1,3)}(\tau) \quad \text{and} \quad \mathbb{E}_{1,(1,2)}(\tau) := 2I_{(1,1)}(\tau) + 2I_{(1,5)}(\tau), \tag{1.3}$$

where the theta integrals $I_{\boldsymbol{k}}$ are defined in (2.3). We prove the following.

Theorem 1.3. *We have, as $t \to 0^+$,*

$$\mathbb{E}_{1,(1,1)}(it) \sim \frac{1}{4}, \qquad \mathbb{E}_{1,(1,2)}(it) \sim \frac{3}{4}.$$

Note that the asymptotics in Theorem 1.3 agree with the answer which one obtains from [5] by using two-dimensional false theta functions.

Acknowledgements

The research of the first author is supported by the Alfried Krupp Prize for Young University Teachers of the Krupp foundation and the research leading to these results receives funding from the European Research Council under the European Union's Seventh Framework Programme (FP/2007–2013)/ERC Grant agreement n. 335220 - AQSER. The research of the second author is supported by the European Research Council under the European Union's Seventh Framework Programme (FP/2007–2013)/ERC Grant agreement n. 335220 - AQSER. The third author was partially supported by the NSF Grant DMS-1601070.

We thank Caner Nazaroglu for helping with numerical calculations and the referee for many helpful comments.

2. Proof of Theorem 1.1 and Theorem 1.2

To prove Theorem 1.1 and Theorem 1.2, we let

$$\mathbb{F}_{1,s}(q) := \sum_{\boldsymbol{\alpha}\in\mathscr{S}_s} \varepsilon_{\boldsymbol{s}}(\alpha) \sum_{\boldsymbol{n}\in\mathbb{N}_0^2} q^{pQ(\boldsymbol{n}+\boldsymbol{\alpha})},$$

where $Q(x_1, x_2) := 3x_1^2 + 3x_1x_2 + x_2^2$ and where

$$\begin{aligned}\mathscr{S}_{\boldsymbol{s}} := \Bigg\{ &\left(\frac{s_2 - s_1}{3p}, 1 - \frac{s_2}{p}\right), \left(1 - \frac{s_2 - s_1}{3p}, 1 - \frac{s_1}{p}\right), \left(\frac{2s_1 + s_2}{3p}, 1 - \frac{s_1 + s_2}{p}\right), \\ &\left(\frac{2s_2 + s_1}{3p}, 1 - \frac{s_1 + s_2}{p}\right), \left(1 - \frac{s_1 + 2s_2}{3p}, \frac{s_2}{p}\right), \left(1 - \frac{s_2 + 2s_1}{3p}, \frac{s_1}{p}\right), \\ &\left(\frac{2s_1 + s_2}{3p}, 1 - \frac{s_1}{p}\right), \left(\frac{2s_2 + s_1}{3p}, 1 - \frac{s_2}{p}\right), \left(1 - \frac{s_1 + 2s_2}{3p}, \frac{s_1 + s_2}{p}\right), \\ &\left(1 - \frac{s_2 + 2s_1}{3p}, \frac{s_1 + s_2}{p}\right), \left(\frac{s_2 - s_1}{3p}, \frac{s_1}{p}\right), \left(1 - \frac{s_2 - s_1}{3p}, \frac{s_2}{p}\right)\Bigg\},\end{aligned}$$

$$\varepsilon_{\boldsymbol{s}}(\boldsymbol{\alpha}) := \begin{cases} s_2 & \text{if } \boldsymbol{\alpha} \in \left\{ \left(\frac{s_2-s_1}{3p}, 1 - \frac{s_2}{p}\right), \left(1 - \frac{s_1+2s_2}{3p}, \frac{s_2}{p}\right), \right. \\ & \qquad \left. \left(\frac{2s_2+s_1}{3p}, 1 - \frac{s_2}{p}\right), \left(1 - \frac{s_2-s_1}{3p}, \frac{s_2}{p}\right) \right\}, \\ s_1 & \text{if } \boldsymbol{\alpha} \in \left\{ \left(1 - \frac{s_2-s_1}{3p}, 1 - \frac{s_1}{p}\right), \left(1 - \frac{s_2+2s_1}{3p}, \frac{s_1}{p}\right), \right. \\ & \qquad \left. \left(\frac{2s_1+s_2}{3p}, 1 - \frac{s_1}{p}\right), \left(\frac{s_2-s_1}{3p}, \frac{s_1}{p}\right) \right\}, \\ -(s_1 + s_2) & \text{if } \boldsymbol{\alpha} \in \left\{ \left(\frac{2s_1+s_2}{3p}, 1 - \frac{s_1+s_2}{p}\right), \left(\frac{2s_2+s_1}{3p}, 1 - \frac{s_1+s_2}{p}\right), \right. \\ & \qquad \left. \left(1 - \frac{s_1+2s_2}{3p}, \frac{s_1+s_2}{p}\right), \left(1 - \frac{s_2+2s_1}{3p}, \frac{s_1+s_2}{p}\right) \right\} \end{cases}$$

and

$$\mathbb{F}_{2,\boldsymbol{s}}(q) := \sum_{\boldsymbol{\alpha} \in \mathscr{S}_{\boldsymbol{s}}} \eta_{\boldsymbol{s}}(\boldsymbol{\alpha}) \sum_{\boldsymbol{n} \in \mathbb{N}_0^2} (n_2 + \alpha_2)\, q^{Q(\boldsymbol{n}+\boldsymbol{\alpha})},$$

where

$$\eta_{\boldsymbol{s}}(\boldsymbol{\alpha}) := \begin{cases} 1 & \text{if } \boldsymbol{\alpha} \in \left\{ \left(\frac{s_2-s_1}{3p}, 1 - \frac{s_2}{p}\right), \left(1 - \frac{s_2-s_1}{3p}, 1 - \frac{s_1}{p}\right), \left(\frac{2s_1+s_2}{3p}, 1 - \frac{s_1}{p}\right), \right. \\ & \qquad \left. \left(\frac{2s_2+s_1}{3p}, 1 - \frac{s_2}{p}\right), \left(1 - \frac{s_1+2s_2}{3p}, \frac{s_1+s_2}{p}\right), \left(1 - \frac{s_2+2s_1}{3p}, \frac{s_1+s_2}{p}\right)\right\}, \\ -1 & \text{if } \boldsymbol{\alpha} \in \left\{ \left(\frac{2s_1+s_2}{3p}, 1 - \frac{s_1+s_2}{p}\right), \left(\frac{2s_2+s_1}{3p}, 1 - \frac{s_1+s_2}{p}\right), \left(1 - \frac{s_1+2s_2}{3p}, \frac{s_2}{p}\right), \right. \\ & \qquad \left. \left(1 - \frac{s_2+2s_1}{3p}, \frac{s_1}{p}\right), \left(\frac{s_2-s_1}{3p}, \frac{s_1}{p}\right), \left(1 - \frac{s_2-s_1}{3p}, \frac{s_2}{p}\right)\right\}. \end{cases}$$

Remark. We have

$$\mathbb{F}_{(p,p)}(q) = 1.$$

Thus we may throughout assume that $\boldsymbol{s} \neq (p, p)$.

Similarly as in the case $\boldsymbol{s} = (1, 1)$, a lengthy calculation gives.

Lemma 2.1. *We have*

$$\mathbb{F}_{\boldsymbol{s}}(q) = \frac{1}{p}\mathbb{F}_{1,\boldsymbol{s}}\left(q^p\right) + \mathbb{F}_{2,\boldsymbol{s}}\left(q^p\right).$$

The following theorem states quantum modular properties of the functions $\mathbb{F}_{1,s}$ and $\mathbb{F}_{2,s}$, using the method of [4]. Let

$$\mathcal{E}_{1,s}(\tau) := \sum_{\boldsymbol{\alpha}\in\mathscr{S}_s^*} \varepsilon_s(\boldsymbol{\alpha})\mathcal{E}_{1,\boldsymbol{\alpha}}(p\tau), \tag{2.1}$$

where

$$\mathscr{S}_s^* := \left\{\left(\frac{s_2-s_1}{3p}, 1-\frac{s_2}{p}\right), \left(1-\frac{s_2-s_1}{3p}, 1-\frac{s_1}{p}\right), \left(\frac{2s_1+s_2}{3p}, 1-\frac{s_1}{p}\right),\right.$$
$$\left.\left(\frac{2s_2+s_1}{3p}, 1-\frac{s_2}{p}\right), \left(1-\frac{s_1+2s_2}{3p}, \frac{s_1+s_2}{p}\right)\left(1-\frac{s_2+2s_1}{3p}, \frac{s_1+s_2}{p}\right)\right\}.$$

Moreover, the Eichler integrals $\mathcal{E}_{1,\boldsymbol{\alpha}}$ are given as

$$\mathcal{E}_{1,\boldsymbol{\alpha}}(\tau) := -\frac{\sqrt{3}}{4}\int_{-\overline{\tau}}^{i\infty}\int_{w_1}^{i\infty} \frac{\theta_1(\boldsymbol{\alpha};\boldsymbol{w})+\theta_2(\boldsymbol{\alpha};\boldsymbol{w})}{\sqrt{-i(w_1+\tau)}\sqrt{-i(w_2+\tau)}}dw_2dw_1$$

with

$$\theta_1(\boldsymbol{\alpha};\boldsymbol{w}) := \sum_{\boldsymbol{n}\in\boldsymbol{\alpha}+\mathbb{Z}^2} (2n_1+n_2)n_2 e^{\frac{3\pi i}{2}(2n_1+n_2)^2w_1+\frac{\pi i n_2^2 w_2}{2}},$$

$$\theta_2(\boldsymbol{\alpha};\boldsymbol{w}) := \sum_{\boldsymbol{n}\in\boldsymbol{\alpha}+\mathbb{Z}^2} (3n_1+2n_2)n_1 e^{\frac{\pi i}{2}(3n_1+2n_2)^2w_1+\frac{3\pi i n_1^2 w_2}{2}}.$$

Finally let

$$\mathcal{E}_{2,s}(\tau) := \sum_{\boldsymbol{\alpha}\in\mathscr{S}_s^*} \mathcal{E}_{2,\boldsymbol{\alpha}}(p\tau). \tag{2.2}$$

Here

$$\mathcal{E}_{2,\boldsymbol{\alpha}}(\tau) := \frac{\sqrt{3}}{8\pi}\int_{-\overline{\tau}}^{i\infty}\int_{w_1}^{i\infty} \frac{2\theta_3(\boldsymbol{\alpha};\boldsymbol{w})-\theta_4(\boldsymbol{\alpha};\boldsymbol{w})}{\sqrt{-i(w_1+\tau)}(-i(w_2+\tau))^{\frac{3}{2}}}dw_2dw_1$$
$$+\frac{\sqrt{3}}{8\pi}\int_{-\overline{\tau}}^{i\infty}\int_{w_1}^{i\infty} \frac{\theta_5(\boldsymbol{\alpha};\boldsymbol{w})}{(-i(w_1+\tau))^{\frac{3}{2}}\sqrt{-i(w_2+\tau)}}dw_2dw_1$$

with

$$\theta_3(\boldsymbol{\alpha};\boldsymbol{w}) := \sum_{\boldsymbol{n}\in\boldsymbol{\alpha}+\mathbb{Z}^2} (2n_1+n_2) e^{\frac{3\pi i}{2}(2n_1+n_2)^2w_1+\frac{\pi i n_2^2 w_2}{2}},$$

$$\theta_4(\boldsymbol{\alpha};\boldsymbol{w}) := \sum_{\boldsymbol{n}\in\boldsymbol{\alpha}+\mathbb{Z}^2} (3n_1+2n_2) e^{\frac{\pi i}{2}(3n_1+2n_2)^2w_1+\frac{3\pi i n_1^2 w_2}{2}},$$

$$\theta_5(\boldsymbol{\alpha};\boldsymbol{w}) := \sum_{\boldsymbol{n}\in\boldsymbol{\alpha}+\mathbb{Z}^2} n_1 e^{\frac{\pi i}{2}(3n_1+2n_2)^2w_1+\frac{3\pi i n_1^2 w_2}{2}}.$$

Furthermore define, for $\nu \in \{0,1\}$, $h \in \mathbb{Z}$, $N, A \in \mathbb{N}$ with $A|N$ and $N|hA$, the theta function studied, for example, by Shimura [11]

$$\Theta_\nu(A,h,N;\tau) := \sum_{\substack{m\in\mathbb{Z}\\ m\equiv h \pmod{\mathrm{N}}}} m^\nu q^{\frac{Am^2}{2N^2}}.$$

We are now ready to prove Theorem 1.1.

Proof of Theorem 1.1 (Sketch). We start with $\mathbb{F}_{1,s}$. Write

$$\mathbb{F}_{1,s}\left(e^{2\pi i \frac{h}{k}-t}\right) \sim \sum_{m\geq 0} A_{s,h,k}(m)t^m \quad \left(t\to 0^+\right).$$

Using the Euler-Maclaurin summation formula (in the shape stated in (28) of [4]) one can prove, following the proof of Theorem 7.1 of [4], that

$$\mathbb{E}_{1,s}\left(\frac{it}{2\pi}-\frac{h}{k}\right) \sim \sum_{m\geq 0} A_{s,h,k}(m)(-t)^m \quad \left(t\to 0^+\right).$$

Here

$$\mathbb{E}_{1,s}(\tau) := \frac{1}{2}\sum_{\boldsymbol{\alpha}\in\mathscr{S}_s^*} \varepsilon_s(\boldsymbol{\alpha}) \sum_{\boldsymbol{n}\in\boldsymbol{\alpha}+\mathbb{Z}^2} M_2\left(\sqrt{3};\sqrt{v}\left(2\sqrt{3}n_1+\sqrt{3}n_2,n_2\right)\right) q^{-Q(\boldsymbol{n})},$$

where $\boldsymbol{w}\in\mathbb{R}^2$ and $\kappa\in\mathbb{R}$ with $w_2,\ w_1-\kappa w_2\neq 0$, we set

$$M_2(\kappa;\boldsymbol{w}) := -\frac{1}{\pi^2}\int_{\mathbb{R}^2-i\boldsymbol{w}} \frac{e^{-\pi t_1^2-\pi t_2^2-2\pi i(t_1w_1+t_2w_2)}}{t_2(t_2-\kappa t_1)}\,dt_1dt_2.$$

In particular, $\mathbb{E}_{1,s}$ agrees with $\mathbb{F}_{1,s}$ on $\mathbb{Q}$. Proceeding as in the proof of Lemma 6.1 of [4] one can then show that

$$\mathbb{E}_{1,s}(\tau) = \mathcal{E}_{1,s}\left(\frac{\tau}{p}\right).$$

To determine the transformation behaviour, we rewrite the theta functions in $\mathcal{E}_{1,s}$ in terms of Shimura theta functions to obtain, as in the proof of Proposition 5.2 of [4]

$$3p\mathcal{E}_{1,s}\left(\frac{\tau}{p}\right) = (2s_1+s_2)J_{(s_2,s_2+2s_1)}(\tau)+(2s_2+s_1)J_{(s_1,s_1+2s_2)}(\tau)+(s_2-s_1)J_{(s_1+s_2,s_1-s_2)}(\tau),$$

where

$$J_{\boldsymbol{k}}(\tau) := \sum_{\delta\in\{0,1\}} I_{(k_1+\delta p,k_2+3\delta p)}(\tau) \quad \text{with}$$

$$I_{\boldsymbol{k}}(\tau) := -\frac{\sqrt{3}}{4p} I_{\Theta_1(2p,k_1,2p;\cdot),\Theta_1(6p,k_2,6p,\cdot)}(\tau). \tag{2.3}$$

Here, for modular forms f and g of weights κ_1 and κ_2, respectively,

$$I_{f,g}(\tau) := \int_{-\overline{\tau}}^{i\infty} \int_{w_1}^{i\infty} \frac{f(w_1)g(w_2)}{(-i(w_1+\tau))^{2-\kappa_1}(-i(w_2+\tau))^{2-\kappa_2}} dw_2 dw_1.$$

Now the transformation properties follow as in the proof of Proposition 5.2 of [5].

For the function $\mathbb{F}_{2,\boldsymbol{s}}$, we proceed in the same way. Writing

$$\mathbb{F}_{2,\boldsymbol{s}}\left(e^{2\pi i \frac{h}{k} - t}\right) \sim \sum_{m\geq 0} B_{\boldsymbol{s},h,k}(m) t^m \qquad \left(t \to 0^+\right)$$

we may show in a similar manner as in the proof of Theorem 7.2 of [4], using the Euler-Maclaurin summation formula, that

$$\mathbb{E}_{2,\boldsymbol{s}}\left(\frac{it}{2\pi} - \frac{h}{k}\right) \sim \sum_{m\geq 0} B_{\boldsymbol{s},h,k}(m)(-t)^m.$$

Here

$$\mathbb{E}_2(\tau) = \mathbb{E}_{2,\boldsymbol{s}}(\tau) := \frac{1}{4\pi i}$$
$$\times \sum_{\boldsymbol{\alpha}\in\mathscr{S}_{\boldsymbol{s}}^*} \sum_{\boldsymbol{n}\in\boldsymbol{\alpha}+\mathbb{Z}^2} \left[\frac{\partial}{\partial z}\left(M_2\left(\sqrt{3}; \sqrt{3v}(2n_1+n_2), \sqrt{v}\left(n_2 - \frac{2\operatorname{Im}(z)}{v}\right)\right) e^{2\pi i n_2 z}\right)\right]_{z=0} q^{-Q(\boldsymbol{n})}.$$

Following the proof of Lemma 6.2 of [4], one may then prove that

$$\mathbb{E}_{2,\boldsymbol{s}}(\tau) = \mathcal{E}_{2,\boldsymbol{s}}\left(\frac{\tau}{p}\right).$$

To finish the proof one may show that, proceeding as in the proof of Proposition 5.2 of [4].

$$\mathbb{E}_{2,\boldsymbol{s}}(\tau) = \frac{2}{p}\left(-\mathcal{J}_{(s_1+s_2,s_1-s_2)}(\tau) + \mathcal{J}_{(s_2,2s_1+s_2)}(\tau) + \mathcal{J}_{(s_1,2s_2+s_1)}(\tau)\right),$$

where

$$\mathcal{J}_{\boldsymbol{k}}(\tau) := \sum_{\delta\in\{0,1\}} \mathcal{I}_{(k_1+p\delta,k_2+3p\delta)}(\tau), \quad \text{with}$$

$$\mathcal{I}_{\boldsymbol{k}}(\tau) := -\frac{\sqrt{3}}{8\pi} I_{\Theta_1(2p,k_1,2p;\cdot),\Theta_0(6p,k_2,6p;\cdot)}(\tau).$$

Again the transformation properties follow as in the proof of Proposition 5.5 of [5]. □

We now restrict to $p=2$. The following lemma shows the vanishing of $\mathbb{F}_{2,\boldsymbol{s}}$ in this case.

Lemma 2.2. *For $p=2$, the functions $\mathbb{F}_{2,\boldsymbol{s}}$ and $\mathbb{E}_{2,\boldsymbol{s}}$ vanish identically.*

Proof. We start by proving that $\mathbb{F}_{2,\boldsymbol{s}} = 0$. It is enough to consider $\boldsymbol{s} \in \{(1,1),(1,2)\}$. The claim for $\boldsymbol{s} = (1,1)$ follows directly by plugging in the definition of $\mathbb{F}_{2,(1,1)}$ and canceling terms.

We next consider $\mathbb{F}_{2,(1,2)}$. By definition

$$\mathbb{F}_{2,(1,2)}(q) = \sum_{\boldsymbol{\alpha}\in\mathscr{S}_{(1,2)}} \eta_{(1,2)}(\boldsymbol{\alpha}) \sum_{\boldsymbol{n}\in\mathbb{N}_0^2} (n_2+\alpha_2)\, q^{Q(\boldsymbol{n}+\boldsymbol{\alpha})},$$

where

$$\eta_{(1,2)}(\boldsymbol{\alpha}) := \begin{cases} 1 & \text{if } \boldsymbol{\alpha} \in \left\{\left(\frac16,0\right),\left(\frac56,\frac12\right),\left(\frac23,\frac12\right),\left(\frac56,0\right),\left(\frac16,\frac32\right),\left(\frac13,\frac32\right)\right\},\\ -1 & \text{if } \boldsymbol{\alpha} \in \left\{\left(\frac23,-\frac12\right),\left(\frac56,-\frac12\right),\left(\frac16,1\right),\left(\frac13,\frac12\right),\left(\frac16,\frac12\right),\left(\frac56,1\right)\right\}. \end{cases}$$

Note that

$$\begin{aligned} H_{\boldsymbol{\alpha}}(q) &:= \sum_{\boldsymbol{n}\in\mathbb{N}_0^2} (n_2+\alpha_2)\, q^{Q(\boldsymbol{n}+\boldsymbol{\alpha})} - \sum_{\boldsymbol{n}\in\mathbb{N}_0^2} (n_2+\alpha_2-1)\, q^{Q(\boldsymbol{n}+(\alpha_1,\alpha_2-1))}\\ &= (1-\alpha_2)\, q^{\frac14(\alpha_2-1)^2} \sum_{n\in\alpha_1+\frac{\alpha_2-1}{2}+\mathbb{N}_0} q^{3n^2}. \end{aligned}$$

Thus

$$\begin{aligned} &\mathbb{F}_{2,(1,2)}(q)\\ &= -H_{\left(\frac16,1\right)}(q) + H_{\left(\frac56,\frac12\right)}(q) + H_{\left(\frac23,\frac12\right)}(q) - H_{\left(\frac56,1\right)}(q) + H_{\left(\frac16,\frac32\right)}(q) + H_{\left(\frac13,\frac32\right)}(q)\\ &= \frac12 q^{\frac1{16}} \sum_{n\in\frac7{12}+\mathbb{N}_0} q^{3n^2} + \frac12 q^{\frac1{16}} \sum_{n\in\frac5{12}+\mathbb{N}_0} q^{3n^2} - \frac12 q^{\frac1{16}} \sum_{n\in\frac5{12}+\mathbb{N}_0} -\frac12 q^{\frac1{16}} \sum_{n\in\frac7{12}+\mathbb{N}_0} q^{3n^2} = 0. \end{aligned}$$

To see that $\mathbb{E}_{2,\mathbf{s}} = 0$, it is sufficient to prove

$$-\mathcal{J}_{(s_1+s_2,s_1-s_2)} + \mathcal{J}_{(s_2,2s_1+s_2)} + \mathcal{J}_{(s_1,2s_2+s_1)} = 0,$$

which is a straightforward computation with theta series.

We are now ready to prove Theorem 1.2.

Sketch of proof of Theorem 1.2. We write

$$\mathbb{E}_{1,\boldsymbol{s}}(\tau) = -\frac{\sqrt3}{2}\int_{-\overline{\tau}}^{i\infty}\int_{w_1}^{i\infty} \frac{\sum_{\boldsymbol{\alpha}\in\mathscr{S}_{\boldsymbol{s}}^*} \varepsilon(\boldsymbol{\alpha})\left(\theta_1(\boldsymbol{\alpha};2\boldsymbol{w})+\theta_2(\boldsymbol{\alpha};2\boldsymbol{w})\right)}{\sqrt{-i(w_1+\tau)}\sqrt{-i(w_2+\tau)}} dw_2 dw_1.$$

We next show the identities in (1.3). We start with $\boldsymbol{s} = (1,1)$. We use the theta relation

$$\begin{aligned} &\frac12 \sum_{\boldsymbol{\alpha}\in\mathscr{S}_{(1,1)}^*} \varepsilon(\boldsymbol{\alpha})\left(\theta_1(\boldsymbol{\alpha};2\boldsymbol{w})+\theta_2(\boldsymbol{\alpha};2\boldsymbol{w})\right)\\ &\qquad = \frac12 \Theta_1(4,1,4;w_1)\Theta_1(12,3,12;w_2). \end{aligned} \tag{2.4}$$

Equation (2.4) yields

$$\mathbb{E}_{1,(1,1)}(\tau) = -\frac{\sqrt{3}}{2} \int_{-\overline{\tau}}^{i\infty} \int_{w_1}^{i\infty} \frac{\Theta_1(4,1,4;w_1)\Theta_1(12,3,12;w_2)}{\sqrt{-i(w_1+\tau)}\sqrt{-i(w_2+\tau)}} dw_2 dw_1$$
$$= 4I_{(1,3)}(\tau),$$

which is the first identity in (1.3).

We next consider $\mathbb{E}_{1,(1,2)}$ and use that

$$\sum_{\boldsymbol{\alpha}\in\mathscr{S}^*_{(1,2)}} \varepsilon(\boldsymbol{\alpha}) \left(\theta_1(\boldsymbol{\alpha}; 2\boldsymbol{w}) + \theta_2(\boldsymbol{\alpha}; 2\boldsymbol{w})\right)$$
$$= \frac{1}{2}\Theta_1(4,1,4;w_1) \left(\Theta_1(12,1,12;w_2) + \Theta_1(12,5,12;w_2)\right). \qquad (2.5)$$

Thus

$$\mathbb{E}_{1,(1,2)}(\tau)$$
$$= -\frac{\sqrt{3}}{4} \int_{-\overline{\tau}}^{i\infty} \int_{w_1}^{i\infty} \frac{\Theta_1(4,1,4;w_1) \left(\Theta_1(12,1,12;w_2) + \Theta_1(12,5,12;w_2)\right)}{\sqrt{-i(w_1+\tau)}\sqrt{-i(w_2+\tau)}} dw_2 dw_1$$
$$= 2(I_{(1,1)}(\tau) + I_{(1,5)}(\tau)),$$

which is the second identity in (1.3).

We next use Lemma 5.1 of [5], to obtain

$$I_{\boldsymbol{k}}(\tau) = (-i\tau)^{-1} \frac{1}{\sqrt{3}} \sum_{k=1}^{5} \sin\left(\frac{\pi k k_2}{6}\right) I_{(k_1,k)}\left(-\frac{1}{\tau}\right) + \mathbb{A}_{\boldsymbol{k}}(\tau),$$

where $\mathbb{A}_{\boldsymbol{k}}$ contributes the simpler terms mentioned in Theorem 1.2, and is explicitly given by

$$\mathbb{A}_{\boldsymbol{k}}(\tau) := -\frac{\sqrt{3}}{8} \int_0^{i\infty} \int_{w_1}^{i\infty} \frac{\Theta_1(4,k_1,4;w_1)\Theta_1(12,k_2,12;w_2)}{\sqrt{-i(w_1+\tau)}\sqrt{-i(w_2+\tau)}} dw_2 dw_1$$
$$- \frac{\sqrt{3}}{8} I_{\Theta_1(4,k_1,4;\cdot)}(\tau) r_{\Theta_1(12,k_2,12;\cdot)}(\tau) + \frac{\sqrt{3}}{8} r_{\Theta_1(4,k_1,4;\cdot)}(\tau) r_{\Theta_1(12,k_2,12;\cdot)}(\tau),$$

where, for f a holomorphic modular form of weight k,

$$r_f(\tau) := \int_0^{i\infty} f(w)(-i(w+\tau))^{k-2} dw.$$

In particular

$$\mathbb{E}_{1,(1,1)}(\tau) = \frac{1}{\sqrt{3}(-i\tau)} \left(2\mathbb{E}_{1,(1,2)}\left(-\frac{1}{\tau}\right) - \mathbb{E}_{1,(1,1)}\left(-\frac{1}{\tau}\right)\right) + 4\mathbb{A}_{(1,3)}(\tau),$$
$$\mathbb{E}_{1,(1,2)}(\tau) = \frac{1}{\sqrt{3}(-i\tau)} \left(\mathbb{E}_{1,(1,1)}\left(-\frac{1}{\tau}\right) + \mathbb{E}_{1,(1,2)}\left(-\frac{1}{\tau}\right)\right) + 2\mathbb{A}_{(1,1)}(\tau) + 2\mathbb{A}_{(1,5)}(\tau).$$

Inverting and reordering gives

$$\mathbb{E}_{1,(1,1)}\left(-\frac{1}{\tau}\right) = -\frac{i\tau}{\sqrt{3}}\big(2\mathbb{E}_{1,(1,2)}(\tau) - \mathbb{E}_{1,(1,1)}(\tau)\big) - \frac{4i\tau}{\sqrt{3}}\left(\mathbb{A}_{(1,3)}(\tau) - \mathbb{A}_{(1,1)}(\tau) - \mathbb{A}_{(1,5)}(\tau)\right), \tag{2.6}$$

$$\mathbb{E}_{1,(1,2)}\left(-\frac{1}{\tau}\right) = -\frac{i\tau}{\sqrt{3}}\big(\mathbb{E}_{1,(1,2)}(\tau) + \mathbb{E}_{1,(1,1)}(\tau)\big) + \frac{2i\tau}{\sqrt{3}}\left(\mathbb{A}_{(1,1)}(\tau) + \mathbb{A}_{(1,5)}(\tau) + 2\mathbb{A}_{(1,3)}(\tau)\right). \tag{2.7}$$

The claim follows using that

$$\mathbb{E}_{1,(1,1)}(\tau+1) = -\mathbb{E}_{1,(1,1)}(\tau), \quad \mathbb{E}_{1,(1,2)}(\tau+1) = e^{-\frac{\pi i}{6}}\mathbb{E}_{1,(1,2)}(\tau). \qquad \square$$

3. The asymptotic behavior of $H_{1,\boldsymbol{\alpha}}$

To prove Theorem 1.3 we need to compute

$$H_{\boldsymbol{\alpha}} := \lim_{t\to 0^+} \frac{H_{1,\boldsymbol{\alpha}}\left(\frac{i}{t}\right)}{t},$$

where, for $\boldsymbol{\alpha} \in \mathbb{R}^2$,

$$H_{1,\boldsymbol{\alpha}}(\tau) := -\sqrt{3}\int_0^{i\infty}\int_{w_1}^{i\infty} \frac{\theta_1(\boldsymbol{\alpha};\boldsymbol{w}) + \theta_2(\boldsymbol{\alpha};\boldsymbol{w})}{\sqrt{-i(w_1+\tau)}\sqrt{-i(w_2+\tau)}} dw_2 dw_1.$$

Proposition 3.1. *Assume that α_1, α_2 are not both in $\mathbb{Z}$. We have*

$$H_{\boldsymbol{\alpha}} = \begin{cases} \frac{2}{\sqrt{3}}\frac{\sin(2\pi\alpha_1)\sin(2\pi\alpha_2)}{(1-\cos(2\pi\alpha_1))(1-\cos(2\pi\alpha_2))} & \text{if } \alpha_1,\alpha_2 \notin \mathbb{Z}, \\ \frac{2\sqrt{3}}{1-\cos(2\pi\alpha_2)} & \text{if } \alpha_1 \in \mathbb{Z}, \alpha_2 \notin \mathbb{Z}, \\ \frac{2}{(1-\cos(2\pi\alpha_1))\sqrt{3}} & \text{if } \alpha_1 \notin \mathbb{Z}, \alpha_2 \in \mathbb{Z}. \end{cases}$$

Proof. We first rewrite $H_{1,\boldsymbol{\alpha}}(\tau)$. By Theorem 1.2 of [5], we have

$$H_{1,\boldsymbol{\alpha}}(\tau) = \int_{\mathbb{R}^2} g_{1,\boldsymbol{\alpha}}(\boldsymbol{w}) e^{2\pi i\tau Q(\boldsymbol{w})} dw_1 dw_2.$$

Here we define

$$g_{1,\boldsymbol{\alpha}}(\boldsymbol{w}) := \begin{cases} 2\mathcal{G}_{\alpha_1}(w_1)\mathcal{G}_{\alpha_2}(w_2) - 2\mathcal{F}_{\alpha_1}(w_1)\mathcal{F}_{\alpha_2}(w_2) & \text{if } \alpha_1,\alpha_2 \notin \mathbb{Z}, \\ -2\mathcal{F}_0(w_1)\mathcal{F}_{\alpha_2}(w_2) + \frac{2}{\pi w_1}\mathcal{F}_{\alpha_2}\left(w_2 + \frac{3w_1}{2}\right) & \text{if } \alpha_1 \in \mathbb{Z},\ \alpha_2 \notin \mathbb{Z}, \\ -2\mathcal{F}_{\alpha_1}(w_1)\mathcal{F}_0(w_2) + \frac{2}{\pi w_2}\mathcal{F}_{\alpha_1}\left(w_1 + \frac{w_2}{2}\right) & \text{if } \alpha_1 \notin \mathbb{Z},\ \alpha_2 \in \mathbb{Z}, \end{cases}$$

setting

$$\mathcal{F}_\alpha(x) := \frac{\sinh(2\pi x)}{\cosh(2\pi x) - \cos(2\pi\alpha)}, \qquad \mathcal{G}_\alpha(x) := \frac{\sin(2\pi\alpha)}{\cosh(2\pi x) - \cos(2\pi\alpha)}.$$

Applying the two-dimensional saddle point method gives that

$$H_{\boldsymbol{\alpha}} = \frac{g_{1,\boldsymbol{\alpha}}(0,0)}{\sqrt{3}}.$$

Explicitly computing $g_{1,\boldsymbol{\alpha}}(0,0)$ yields the claim of Proposition 3.1.

4. Proof of Theorem 1.3.

Inverting (2.6) and (2.7) gives

$$\begin{aligned}\mathbb{E}_{1,(1,1)}(\tau) &= \frac{1}{\sqrt{3}(-i\tau)}\left(2\mathbb{E}_{1,(1,2)}\left(-\frac{1}{\tau}\right) - \mathbb{E}_{1,(1,1)}\left(-\frac{1}{\tau}\right)\right)\\ &\quad + \frac{4}{\sqrt{3}(-i\tau)}\left(\mathbb{A}_{(1,3)}\left(-\frac{1}{\tau}\right) - \mathbb{A}_{(1,1)}\left(-\frac{1}{\tau}\right) - \mathbb{A}_{(1,5)}\left(-\frac{1}{\tau}\right)\right),\\ \mathbb{E}_{1,(1,2)}(\tau) &= \frac{1}{\sqrt{3}(-i\tau)}\left(\mathbb{E}_{1,(1,2)}\left(-\frac{1}{\tau}\right) + \mathbb{E}_{1,(1,1)}\left(-\frac{1}{\tau}\right)\right)\\ &\quad - \frac{2}{\sqrt{3}(-i\tau)}\left(\mathbb{A}_{(1,1)}\left(-\frac{1}{\tau}\right) + \mathbb{A}_{(1,5)}\left(-\frac{1}{\tau}\right) + 2\mathbb{A}_{(1,3)}\left(-\frac{1}{\tau}\right)\right).\end{aligned}$$

We next rewrite the first summand of $\mathbb{A}_{(1,j)}$, denoting it by $\mathbb{B}_{(1,j)}$. For this, we again use the theta relations (2.4) and (2.5). This yields

$$\mathbb{B}_{(1,3)}(\tau) = \frac{1}{16}\sum_{\boldsymbol{\alpha}\in\mathscr{S}^*_{(1,1)}} \varepsilon(\boldsymbol{\alpha})H_{1,\boldsymbol{\alpha}}(2\tau),\ \mathbb{B}_{(1,1)}(\tau)+\mathbb{B}_{(1,5)}(\tau) = \frac{1}{8}\sum_{\boldsymbol{\alpha}\in\mathscr{S}^*_{(1,2)}} \varepsilon(\boldsymbol{\alpha})H_{1,\boldsymbol{\alpha}}(2\tau).$$

Thus

$$\begin{aligned}\mathbb{E}_{1,(1,1)}(\tau) &= \frac{1}{\sqrt{3}(-i\tau)}\left(2\mathbb{E}_{1,(1,2)}\left(-\frac{1}{\tau}\right) - \mathbb{E}_{1,(1,1)}\left(-\frac{1}{\tau}\right)\right)\\ &\quad + \frac{1}{2\sqrt{3}(-i\tau)}\left(\frac{1}{2}\sum_{\boldsymbol{\alpha}\in\mathscr{S}^*_{(1,1)}} \varepsilon(\boldsymbol{\alpha})H_{1,\boldsymbol{\alpha}}\left(-\frac{2}{\tau}\right) - \sum_{\boldsymbol{\alpha}\in\mathscr{S}^*_{(1,2)}} \varepsilon(\boldsymbol{\alpha})H_{1,\boldsymbol{\alpha}}\left(-\frac{2}{\tau}\right)\right)\\ &\quad - \frac{1}{2(-i\tau)}\left(I_{\Theta_1(4,1,4)}\left(-\frac{1}{\tau}\right) - r_{\Theta_1(4,1,4)}\left(-\frac{1}{\tau}\right)\right)\\ &\quad \times\left(r_{\Theta_1(12,3,12)}\left(-\frac{1}{\tau}\right) - r_{\Theta_1(12,1,12)}\left(-\frac{1}{\tau}\right) - r_{\Theta_1(12,5,12)}\left(-\frac{1}{\tau}\right)\right),\end{aligned}$$

$$\mathbb{E}_{1,(1,2)}(\tau)=\frac{1}{\sqrt{3}(-i\tau)}\left(\mathbb{E}_{1,(1,2)}\left(-\frac{1}{\tau}\right)+\mathbb{E}_{1,(1,1)}\left(-\frac{1}{\tau}\right)\right)$$
$$-\frac{1}{4\sqrt{3}(-i\tau)}\left(\sum_{\boldsymbol{\alpha}\in\mathscr{S}^*_{(1,1)}}\varepsilon(\boldsymbol{\alpha})H_{1,\boldsymbol{\alpha}}\left(-\frac{2}{\tau}\right)+\sum_{\boldsymbol{\alpha}\in\mathscr{S}^*_{(1,2)}}\varepsilon(\boldsymbol{\alpha})H_{1,\boldsymbol{\alpha}}\left(-\frac{2}{\tau}\right)\right)$$
$$+\frac{1}{4(-i\tau)}\Bigg(I_{\Theta_1(4,1,4,1)}\left(-\frac{1}{\tau}\right)-r_{\Theta_1(4,1,4)}\left(-\frac{1}{\tau}\right)\Bigg(2r_{\Theta_1(12,3,12;\,\cdot\,)}\left(-\frac{1}{\tau}\right)$$
$$+r_{\Theta_1(12,1,12;\,\cdot\,)}\left(-\frac{1}{\tau}\right)+r_{\Theta_1(12,5,12;\,\cdot\,)}\left(-\frac{1}{\tau}\right)\Bigg)\Bigg).$$

Letting $\tau=it\to 0$ yields

$$\mathbb{E}_{1,(1,1)}(it)\sim\frac{1}{8\sqrt{3}}\left(\sum_{\boldsymbol{\alpha}\in\mathscr{S}^*_{(1,1)}}\varepsilon(\boldsymbol{\alpha})H_{\boldsymbol{\alpha}}-2\sum_{\boldsymbol{\alpha}\in\mathscr{S}^*_{(1,2)}}\varepsilon(\boldsymbol{\alpha})H_{\boldsymbol{\alpha}}\right)+\frac{1}{2}(h_3-h_1-h_5),\tag{4.1}$$

$$\mathbb{E}_{1,(1,2)}(it)\sim-\frac{1}{8\sqrt{3}}\left(\sum_{\boldsymbol{\alpha}\in\mathscr{S}^*_{(1,1)}}\varepsilon(\boldsymbol{\alpha})H_{\boldsymbol{\alpha}}+\sum_{\boldsymbol{\alpha}\in\mathscr{S}^*_{(1,2)}}\varepsilon(\boldsymbol{\alpha})H_{\boldsymbol{\alpha}}\right)-\frac{1}{4}(2h_3+h_1+h_5),\tag{4.2}$$

where

$$h_j:=\lim_{t\to 0}\frac{1}{t}r_{\Theta_1(4,1,4;\,\cdot\,)}\left(\frac{i}{t}\right)r_{\Theta_1(12,j,12;\,\cdot\,)}\left(\frac{i}{t}\right).$$

We have

$$\sum_{\boldsymbol{\alpha}\in\mathscr{S}^*_s}\varepsilon(\boldsymbol{\alpha})H_{\boldsymbol{\alpha}}=s_2H_{\left(\frac{s_2-s_1}{6},1-\frac{s_2}{2}\right)}+s_1H_{\left(1-\frac{s_2-s_1}{6},1-\frac{s_1}{2}\right)}$$
$$+s_1H_{\left(\frac{2s_1+s_2}{6},1-\frac{s_1}{2}\right)}+s_2H_{\left(\frac{2s_2+s_1}{6},1-\frac{s_2}{2}\right)}$$
$$-(s_1+s_2)H_{\left(1-\frac{s_1+2s_2}{6},\frac{s_1+s_2}{2}\right)}-(s_1+s_2)H_{\left(1-\frac{s_2+2s_1}{6},\frac{s_1+s_2}{2}\right)}.$$

In particular, using Proposition 1.1, we evaluate

$$\sum_{\boldsymbol{\alpha}\in\mathscr{S}^*_{(1,1)}}\varepsilon(\boldsymbol{\alpha})H_{\boldsymbol{\alpha}}=\frac{2}{\sqrt{3}},\qquad\sum_{\boldsymbol{\alpha}\in\mathscr{S}^*_{(1,2)}}\varepsilon(\boldsymbol{\alpha})H_{\boldsymbol{\alpha}}=\frac{16}{\sqrt{3}}.\tag{4.3}$$

To compute $\lim_{t\to 0}t^{-\frac{1}{2}}r_{\Theta_1(N,a,N;\,\cdot\,)}(\frac{i}{t})$ we employ Lemma 3.2 of [5] to obtain

$$r_{\Theta_1(N,a,N;\,\cdot\,)}\left(\frac{i}{t}\right)=\frac{i\sqrt{N}}{2}\sin\left(\frac{2\pi a}{N}\right)\int_{\mathbb{R}}\frac{e^{-\frac{\pi N}{t}x^2}}{\sinh\left(\pi x+\frac{\pi ia}{N}\right)\sinh\left(\pi x-\frac{\pi ia}{N}\right)}dx.$$

The saddle point method then yields that

$$r_{\Theta_1(N,a,N;\,\cdot)}\left(\frac{i}{t}\right) = i\sqrt{t}\cot\left(\frac{\pi a}{N}\right).$$

Thus

$$h_j = \cot\left(\frac{\pi j}{12}\right).$$

In particular

$$h_1 = -\cot\left(\frac{\pi}{12}\right), \qquad h_3 = -1, \qquad h_5 = -\cot\left(\frac{5\pi}{12}\right).$$

Plugging this and (4.3) into (4.1) and (4.2) gives the claim.

5. Simplification for $p = 2$

We first recall the one-dimensional situation for $p = 2$. There is a unique false theta function

$$\sum_{n\in\mathbb{Z}} \operatorname{sgn}\left(n+\frac{1}{2}\right) q^{2\left(n+\frac{1}{4}\right)^2},$$

whose corresponding Eichler integral is (see [3])

$$F_{1,2}^*(\tau) := -2i\int_{-\bar{\tau}}^{i\infty} \frac{\Theta_1(4,1,4;w)}{\sqrt{-i(w+\tau)}}dw.$$

Noting that

$$\Theta_1(4,1,4;\tau) = \eta(\tau)^3, \tag{5.1}$$

this integral transforms as a scalar-valued quantum modular form of weight $\frac{1}{2}$.

In the two-dimensional case, a similar "higher depth" picture emerges. Observing (5.1) and

$$\Theta_1(12,3,12;\tau) = 3\eta(3\tau)^3,$$

$$\Theta_1(12,1,12;\tau) + \Theta_1(12,5,12;\tau) = 3\eta(3\tau)^3 + \eta\left(\frac{\tau}{3}\right)^3$$

we obtain that the space spanned by $\mathbb{E}_{1,(1,1)}(\tau)$ and $\mathbb{E}_{1,(1,2)}(\tau)$ is also spanned by

$$\int_{-\overline{\tau}}^{i\infty}\int_{w_1}^{i\infty} \frac{\eta(w_1)^3\eta(3w_2)^3}{\sqrt{-i(w_1+\tau)}\sqrt{-i(w_2+\tau)}}dw_2dw_1,$$

$$\int_{-\overline{\tau}}^{i\infty}\int_{w_1}^{i\infty} \frac{\eta(w_1)^3\eta\left(\frac{w_2}{3}\right)^3}{\sqrt{-i(w_1+\tau)}\sqrt{-i(w_2+\tau)}}dw_2dw_1. \tag{5.2}$$

The next result can be found in [10, Corollary 6.6] (it can be also derived by using representation theory of $\widehat{\mathfrak{sl}}_3$ as discussed in [2]).

Proposition 5.1. *We have*

$$\eta(\tau) \sum_{m,n\in\mathbb{Z}} q^{m^2+n^2-mn} = 3\eta(3\tau)^3 + \eta\left(\frac{\tau}{3}\right)^3,$$

$$\eta(\tau) q^{\frac{1}{3}} \sum_{m,n\in\mathbb{Z}} q^{m^2+n^2-mn+n} = 3\eta(3\tau)^3.$$

According to [9], $\sum_{m,n\in\mathbb{Z}} q^{m^2+n^2-mn}$ and $q^{\frac{1}{3}} \sum_{m,n\in\mathbb{Z}} q^{m^2+n^2-mn+n}$ are numerators of two characters of irreducible highest weight $\widehat{\mathfrak{sl}}_3$-modules of level one. Therefore modular properties of the double Eichler integrals in (5.2), modulo correction factors, are identical to modular transformation properties of the span of characters of the level one simple affine vertex algebra of $\widehat{\mathfrak{sl}}_3$. It would be interesting to understand a possible connection from a purely representation theoretic perspective. This is closely related to a conjecture of Creutzig and the third author [8] pertaining to quantum modular properties of characters of $W^0(p)_{A_2}$, representations of affine Lie algebras, and representations of quantum groups at a root of unity (see also [1, 6, 7] for other appearances of this and related vertex algebras).

References

[1] D. Adamovic, A realization of certain modules for the $N = 4$ superconformal algebra and the affine Lie algebra $A_2^{(1)}$, *Transform. Groups*, **21** (2016) 299–327.
[2] D. Adamovic and A. Milas, On some vertex algebras related to $V_{-1}(\mathfrak{sl}(n))$ and their characters, arXiv:1805.09771.
[3] K. Bringmann and A. Milas, W-algebras, higher rank false theta functions, and quantum dimensions, *Selecta Math.*, **23** (2017) 1–30.
[4] K. Bringmann, J. Kaszian and A. Milas, Higher depth quantum modular forms, multiple Eichler integrals, and $\mathfrak{sl}_3$ false theta functions, arXiv:1704.06891.
[5] K. Bringmann, J. Kaszian and A. Milas, Vector-valued higher depth quantum modular forms and higher Mordell integrals, arXiv:1803.06261.
[6] T. Creutzig, W-algebras for Argyres-Douglas theories, *Europ. Jour. Math.*, **3** (2017) 659–690.
[7] T. Creutzig and D. Gaiotto, Vertex Algebras for S-duality, arXiv:1708.00875.
[8] T. Creutzig and A. Milas, Higher rank partial and false theta functions and representation theory, *Adv. Math.*, **314** (2017) 203–227.
[9] I. Frenkel and V. Kac, Basic representations of affine Lie algebras and dual resonance models, *Invent. Math.*, **62** (1980) 23–66.
[10] D. Schultz, Cubic theta functions, *Adv. Math.*, **248** (2013) 618–697.
[11] G. Shimura, On modular forms of half-integral weight, *Ann. Math.*, **97** (1973) 440–481.
[12] D. Zagier, Quantum modular forms, *Quanta Math.*, **11** (2010) 659–75.

Topics in Number Theory, RMS-Lecture Notes Series No. 26, 2020, pp. 147–167.

On the Value-Distribution of Symmetric Power L-Functions

Kohji Matsumoto[1] and Yumiko Umegaki[2]

[1]Graduate School of Mathematics, Nagoya University, Chikusa-ku, Nagoya 464-8602, Japan.
e-mail: kohjimat@math.nagoya-u.ac.jp

[2]Department of Mathematical and Physical Sciences, Nara Women's University, Kitauoya-nishimachi, Nara 630-8506, Japan.
e-mail: ichihara@cc.nara-wu.ac.jp

Abstract. We first briefly survey the value-distribution theory of L-functions of the Bohr-Jessen flavor (or the theory of "M-functions"). Limit formulas for the Riemann zeta-function, Dirichlet L-functions, automorphic L-functions etc. are discussed. Then we prove new results on the value-distribution of symmetric power L-functions, which are limit formulas involving associated M-functions.

Keywords. Symmetric power L-function, automorphic L-function, value-distribution, density function, M-function.

2010 Subject Classification: Primary 11F66, Secondary 11M41

1. The Bohr-Jessen limit theorem

We begin with the classical result of Bohr and Jessen [3] on the value-distribution of the Riemann zeta-function $\zeta(s)$.

Let R be a rectangle in the complex plane $\mathbb{C}$ with the edges parallel to the axes. Let $s = \sigma + it$ be a complex variable. By μ_1 we mean the 1-dimensional Lebesgue measure. For $\sigma > 1/2$ and $T > 0$, we define

$$V_\sigma(T, R; \zeta) = \mu_1\{t \in [-T, T] \mid \log\zeta(\sigma + it) \in R\}, \tag{1.1}$$

where the rigorous definition of $\log\zeta(\sigma + it)$ will be given later (in Section 2). Then the result of Bohr and Jessen can be stated as follows.

Theorem 1.1 (Bohr and Jessen [3]).

(i) There exists the limit

$$W_\sigma(R; \zeta) = \lim_{T\to\infty} \frac{1}{T} V_\sigma(T, R; \zeta). \tag{1.2}$$

(ii) This limit can be written as

$$W_\sigma(R; \zeta) = \int_R \mathcal{F}_\sigma(z, \zeta)|dz|, \tag{1.3}$$

where $z = x + iy \in \mathbb{C}$, $|dz| = dxdy/2\pi$, and $\mathcal{F}_\sigma(z, \zeta)$ is a continuous non-negative, explicitly constructed function defined on $\mathbb{C}$.

The limit $W_\sigma(R;\zeta)$ may be regarded as the probability of how many values of $\log\zeta(\sigma+it)$ on the line $\Re s=\sigma$ belong to the given rectangle R, and $\mathcal{F}_\sigma(z,\zeta)$ may be called the density function of this probability. Theorem 1.1 is now called the Bohr-Jessen limit theorem.

Remark 1.2. A reformulation of this type of results in terms of weak convergence of probability measures was given by Laurinčikas (see [21]).

The original proof of Bohr and Jessen is of some geometric flavor. Their proof starts with the expression

$$\log\zeta(\sigma+it)=-\sum_{n=1}^{\infty}\log(1-p_n^{-\sigma-it}), \tag{1.4}$$

where p_n is the nth prime, which is valid for $\sigma>1$. They consider the truncation

$$f_N(\sigma+it)=-\sum_{n=1}^{N}\log(1-p_n^{-\sigma-it})=-\sum_{n=1}^{N}\log(1-p_n^{-\sigma}e^{-it\log p_n}), \tag{1.5}$$

which, even in the case $1/2<\sigma\le 1$, approximates $\log\zeta(\sigma+it)$ in a certain mean value sense. A key idea of Bohr and Jessen is to introduce the auxiliary mapping $S_N:\mathbb{T}^N\to\mathbb{C}$ associated with $f_N(\sigma+it)$ (where $\mathbb{T}^N\simeq[0,1)^N$ is the N-dimensional unit torus) defined by

$$S_N(\theta_1,\ldots,\theta_N;\zeta)=-\sum_{n=1}^{N}\log(1-p_n^{-\sigma}e^{2\pi i\theta_n}) \qquad (0\le\theta_n<1). \tag{1.6}$$

Let $z_n(\theta;\zeta)=-\log(1-p_n^{-\sigma}e^{2\pi i\theta})$. Then each term $z_n(\theta_n;\zeta)$ on the right-hand side of (1.6) describes a planar convex curve when θ_n varies from 0 to 1. Therefore $S_N(\theta_1,\ldots,\theta_N;\zeta)$ is a kind of geometric "sum" of convex curves. Bohr and Jessen [4] developed a detailed theory on such sums of convex curves, and applied it to the proof of their Theorem 1.1.

Later Jessen and Wintner [16] published an alternative proof of Theorem 1.1, which is more analytic (Fourier theoretic). In their proof they used a certain inequality (the Jessen-Wintner inequality), which is also related with convex properties of curves.

We also note that the analogue of Theorem 1.1 for $(\zeta'/\zeta)(s)$ was shown by Kershner and Wintner [20]. As for the explicit construction of the density function, see van Kampen and Wintner [18].

2. A generalization of the Bohr-Jessen limit theorem

It is a natural question to ask how to generalize Theorem 1.1, the Bohr-Jessen limit theorem, to more general zeta and L-functions. An obstacle is that, in more general situation, the geometry of corresponding curves becomes more complicated; especially, the convexity is not valid in general.

Still, however, the part (i) of Theorem 1.1 can be generalized to a fairly general class of zeta-functions.

Let $\mathbb{N}$ be the set of positive integers. For any $n \in \mathbb{N}$, let $g(n) \in \mathbb{N}$, $f(k,n) \in \mathbb{N}$ and $a_n^{(k)} \in \mathbb{C}$ $(1 \le k \le n)$. Using the polynomials given by

$$A_n(X) = \prod_{k=1}^{g(n)} \left(1 - a_n^{(k)} X^{f(k,n)}\right),$$

we define the zeta-function $\varphi(s)$ by the Euler product

$$\varphi(s) = \prod_{n=1}^{\infty} A_n(p_n^{-s})^{-1}. \tag{2.1}$$

Assume

$$g(n) \le C_0 p_n^{\alpha}, \qquad |a_n^{(k)}| \le p_n^{\beta} \tag{2.2}$$

with constants $\alpha, \beta \ge 0$, $C_0 > 0$. Then (2.1) is convergent absolutely in the region $\Re s > \alpha + \beta + 1$.

Let $\mathscr{M}_{\alpha\beta}$ be the set of all functions $\varphi(s)$ defined as above, satisfying (2.2) and the following:

(i) $\varphi(s)$ can be continued meromorphically to $\sigma \ge \sigma_0$, where $\alpha + \beta + 1/2 \le \sigma_0 < \alpha+\beta+1$, and all poles in this region are included in a compact subset of $\{s \mid \sigma > \sigma_0\}$,
(ii) $\varphi(\sigma + it) = O((|t| + 1)^{C'_0})$ for any $\sigma \ge \sigma_0$, with a constant $C'_0 > 0$,
(iii) It holds that

$$\int_{-T}^{T} |\varphi(\sigma_0 + it)|^2 dt = O(T). \tag{2.3}$$

The class

$$\mathscr{M} = \bigcup_{\alpha,\beta \ge 0} \mathscr{M}_{\alpha\beta}$$

was first introduced by the first author [23]. For $\sigma > \sigma_0$, define

$$V_\sigma(T, R; \varphi) = \mu_1\{t \in [-T, T] \mid \log \varphi(\sigma + it) \in R\}, \tag{2.4}$$

where the definition of $\log \varphi(s)$ (for $\varphi \in \mathscr{M}$) is as follows. First, when $\sigma > \alpha+\beta+1$ define

$$\log \varphi(s) = -\sum_{n=1}^{\infty} \sum_{k=1}^{g(n)} \operatorname{Log}\left(1 - a_n^{(k)} p_n^{-f(k,n)s}\right),$$

where Log means the principal branch. Next, let

$$G(\varphi) = \{s \mid \sigma \ge \sigma_0\} \Big\backslash \bigcup_{\rho} \{\sigma + i\Im\rho \mid \sigma_0 \le \sigma \le \Re\rho\},$$

where ρ runs over all zeros and poles ρ with $\Re\rho \geq \sigma_0$. For any $s \in G(\varphi)$, define $\log\varphi(s)$ by the analytic continuation along the horizontal path from the right.

In this general situation, the corresponding mapping is

$$S_N(\theta_1, \ldots, \theta_N; \varphi) = \sum_{n=1}^{N} z_n(\theta_n; \varphi) \qquad (0 \leq \theta_n < 1), \tag{2.5}$$

where

$$z_n(\theta_n; \varphi) = -\sum_{k=1}^{g(n)} \log(1 - a_n^{(k)} p_n^{-f(k,n)\sigma} e^{2\pi i f(k,n)\theta_n}). \tag{2.6}$$

In [23], the following generalization of Theorem 1.1 (i) was shown.

Theorem 2.1 ([23]). *If $\varphi \in \mathscr{M}$, then for any $\sigma > \sigma_0$, the limit*

$$W_\sigma(R; \varphi) = \lim_{T\to\infty} \frac{1}{2T} V_\sigma(T, R; \varphi) \tag{2.7}$$

exists.

It can be seen that the class $\mathscr{M}$ includes a lot of important zeta and L-functions. The reason why such general statement can be shown is that, for the proof of this theorem, geometric properties of corresponding curves (2.6) are not necessary. In fact, the proof of Theorem 2.1 is just based on (besides simple arithmetic facts) Prokhorov's theorem in probability theory.

An alternative proof is given in [24] in the case of Dedekind zeta-functions of algebraic number fields. The method in [24] is to use Lévy's convergence theorem, again in probability theory. This method can also be applied to general $\varphi \in \mathscr{M}$, which is pointed out in [25] and a sketch of the argument in the general case is described in [28].

Therefore, now we can say that the part (i) of Theorem 1.1 has been sufficiently generalized. However Theorem 1.1 includes the part (ii). The part (ii) gives an explicit expression of the limit value in terms of the density function, so it is highly desirable to generalize the part (ii) also, in order to study the behavior of the limit $W_\sigma(R; \varphi)$ more closely.

However this part is related with the geometry of corresponding curves, and its generalization is much more difficult. Joyner [17] discussed the properties of density functions in the case of Dirichlet L-functions, and the first author [24] studied the density functions for Dedekind zeta-functions of Galois number fields, but both of them are the cases when the corresponding curves (2.6) are convex.

In the case of automorphic L-functions, the corresponding (2.6) is not always convex. The study in this case will be given in later sections.

3. *M*-functions

The theorems of Bohr-Jessen type consider the situation when $t = \Im s$ varies. That is, Theorems 1.1 and 2.1 are results in t-aspect. When we consider more general zeta and L-functions, it is also important to study the value-distribution in some different aspect. For example, it is possible to consider the modulus aspect for Dirichlet or Hecke L-functions.

Let χ be a certain character, and $L(s, \chi)$ be the associated L-function (over a certain number field or function field). Ihara [10] studied the behavior of $(L'/L)(s, \chi)$ from this aspect, and proved the limit formula of the form

$$\mathrm{Avg}_\chi \Phi\left(\frac{L'}{L}(s, \chi)\right) = \int_{\mathbb{C}} M_\sigma(z)\Phi(z)|dz| \tag{3.1}$$

for a certain average (specified below) with respect to χ, where Φ is a test function, and $M_\sigma : \mathbb{C} \to \mathbb{R}$ is an explicitly constructed density function, which is non-negative, and belongs to the class C^∞. Ihara called this M_σ the "M-function" associated with the value-distribution of $L(s, \chi)$.

When $\sigma > 1$, Ihara proved (3.1) for any continuous test function Φ. In the function field case, using the (proved) Riemann hypothesis, Ihara proved (3.1) even in some subregion in the critical strip for more restricted class of Φ (e.g. $\sigma > 3/4$ when $\Phi \in L^1 \cap L^\infty$ and moreover its Fourier transform has compact support).

As for the meaning of Avg_χ, Ihara considered several types of averages, but when the ground field is the rational number field $\mathbb{Q}$, the meaning is one of the following: The first type is

$$\mathrm{Avg}_\chi \phi(\chi) = \lim_{m\to\infty} \frac{1}{\pi(m)} \sum_{2<p\le m} \frac{1}{p-2} \sum_{\chi \pmod p}{}^{*} \phi(\chi) \tag{3.2}$$

for a complex-valued function ϕ of χ, where $\pi(m)$ denotes the number of primes up to m, p runs over primes, and $\sum^*$ stands for the sum over primitive Dirichlet characters of modulus p. The second type is considered for the character $\chi_\tau(p) = p^{-i\tau}$. Then the Euler product of the associated L-function is

$$\prod_p (1 - \chi_\tau(p)p^{-s})^{-1} = \prod_p (1 - p^{-s-i\tau})^{-1} = \zeta(s + i\tau),$$

and the meaning of the average is given by

$$\mathrm{Avg}_\chi \phi(\chi) = \lim_{T\to\infty} \frac{1}{2T} \int_{-T}^{T} \phi(\chi_\tau)d\tau. \tag{3.3}$$

The second type of average actually implies a limit formula for the Riemann zeta-function in t-aspect. In particular, the formula (3.1) for this second type of average, with Φ being the characteristic function of R, coincides with the formulation of Kershner and Wintner [20]. An important discovery in Ihara [10] is that the same function M_σ can be used in the formula (3.1) for both of the meanings of average.

Now we restrict ourselves to the case when the ground field is $\mathbb{Q}$, so the meaning of the average is (3.2) or (3.3). We also consider the value-distribution of $\log L(s, \chi)$, so the corresponding limit formula is of the form

$$\mathrm{Avg}_\chi \Phi(\log L(s, \chi)) = \int_{\mathbb{C}} \mathcal{M}_\sigma(z)\Phi(z)|dz| \tag{3.4}$$

with the density function $\mathcal{M}_\sigma$.

Theorem 3.1 (Ihara and Matsumoto [12] [14]). *For any $\sigma > 1/2$, and for the average* (3.2) *or* (3.3)*, both* (3.1) *and* (3.4) *hold with explicitly constructed density functions ("M-functions") M_σ and $\mathcal{M}_\sigma$, for any test function Φ which is* (i) *any bounded continuous function, or* (ii) *the characteristic function of either a compact subset of $\mathbb{C}$ or the complement of such a subset.*

In the number field case the Riemann hypothesis is surely not yet proved, but instead, we can apply certain mean value estimates to obtain the above theorem. Therefore Theorem 3.1 is unconditional. In particular, this theorem includes the Bohr-Jessen limit theorem, and its ζ'/ζ analogue due to Kershner and Wintner, as special cases.

If we assume the Riemann hypothesis (for Dirichlet L-functions), even stronger result can be shown. In [13], the average

$$\mathrm{Avg}_\chi \phi(\chi) = \lim_{p\to\infty} \frac{1}{p-2} \sum_{\chi \pmod{p}}{}^{*} \phi(\chi) \tag{3.5}$$

was considered, and for this average, both (3.1) and (3.4) were proved for more general class of test functions (that is, (i) of Theorem 3.1 is replaced by any continuous function with at most exponential growth) under the assumption of the Riemann hypothesis.

The corresponding study for M-functions in the function field case was done in [11, 13].

Here we mention several further researches in the theory of M-functions. Let D a fundamental discriminant, and χ_D the associated real character. Mourtada and Murty [33] studied the value-distribution of $(L'/L)(\sigma, \chi_D)$ (where $\sigma > 1/2$) in D-aspect, and proved a limit formula similar to (3.1) under the assumption of the Riemann hypothesis. Akbary and Hamieh [1] proved an analogous result for the cubic character case, without the assumption of the Riemann hypothesis.

As for the value-distribution of $(\zeta'/\zeta)(s)$ in t-aspect, there is another approach due to Guo [7] [8]. Inspired by the idea of Guo, Mine [29] proved the existence (and the explicit construction) of the M-function for $(\zeta_K'/\zeta_K)(s)$ in t-aspect, where $\zeta_K(s)$ denotes the Dedekind zeta-function of an algebraic number field K (including the non-Galois case), with an explicit error estimate in the limit formula of the form (3.1). In [31], he extended the result to the case of more general L-functions, belonging to a certain subclass of $\mathscr{M}$.

In his another paper [30], Mine treated the limit theorem of Bohr-Jessen type (but without taking logarithm) for Lerch zeta-functions, and proved a refinement, written in terms of the associated M-function. This paper of Mine implies that the theory of M-functions works for zeta-functions without Euler products.

Suzuki [39] discovered that certain M-function appears even in a rather different context. He studied the zeros of the real or imaginary part of

$$\xi(s) = \frac{1}{2}s(s-1)\pi^{-s/2}\Gamma(s/2)\zeta(s),$$

and proved that the distribution of spacings of the second-order normalization of imaginary parts of those zeros can be represented by an integral involving the M-function for $(\zeta'/\zeta)(s)$.

4. The value-distribution of automorphic L-functions (the modulus and level aspects)

At the end of the preceding section we saw that M-functions have been studied for various zeta and L-functions. Since one of the most important classes of L-functions is the class of automorphic L-functions, it is natural to ask how is the theory of M-functions associated with automorphic L-functions.

First we fix the notation. Let k be an even integer and N positive integer, and let $S_k(N)$ be the set of holomorphic cusp forms of weight k for $\Gamma_0(N)$. We write the Fourier expansion of $f \in S_k(N)$ as

$$f(z) = \sum_{n=1}^{\infty} \lambda_f(n) n^{(k-1)/2} e^{2\pi i n z},$$

and define the attached L-function by

$$L(f, s) = \sum_{n=1}^{\infty} \lambda_f(n) n^{-s}$$

for $\Re s = \sigma > 1$. Now we assume that $f \in S_k(N)$ is a primitive form, that is, a normalized Hecke-eigen newform. Then $L(s, f)$ has the Euler product

$$\begin{aligned} L(f, s) &= \prod_{p \mid N} (1 - \lambda_f(p) p^{-s})^{-1} \prod_{p \nmid N} (1 - \lambda_f(p) p^{-s} + p^{-2s})^{-1} \\ &= \prod_{p \mid N} (1 - \lambda_f(p) p^{-s})^{-1} \prod_{p \nmid N} (1 - \alpha_f(p) p^{-s})^{-1} (1 - \beta_f(p) p^{-s})^{-1} \end{aligned}$$

for $\sigma > 1$, where $|\alpha_f(p)| = 1$, $\beta_f(p) = \overline{\alpha_f(p)}$, and $\alpha_f(p) + \beta_f(p) = \lambda_f(p)$ (for $p \nmid N$).

First consider the modulus aspect. Let χ be a Dirichlet character. The twisted L-function $L(f \otimes \chi, s)$ is defined by replacing p^{-s} by $\chi(p) p^{-s}$ on each local factor. Lebacque and Zykin [22] developed the theory similar to [13] for $L(f \otimes \chi, s)$, and proved the limit formulas corresponding to (3.1) and (3.4).

More difficult is the case of the level aspect. So far there are two attempts in this direction, the aforementioned paper of Lebacque and Zykin [22], and an article of the authors [27]. Here we briefly mention the results proved in [27].

Let $\gamma \in \mathbb{N}$, and define the (partial) γth symmetric power L-function attached to f by

$$L_N(\mathrm{Sym}_f^{\gamma}, s) = \prod_{p \nmid N} \prod_{h=0}^{\gamma} (1 - \alpha_f^{\gamma - h}(p) \beta_f^h(p) p^{-s})^{-1} \tag{4.1}$$

for $\sigma > 1$.

Here we consider the situation $N = q^m$, where q is a prime number. Then the form of the right-hand side of (4.1) is the same for all m, which we denote by

$$L_q(\mathrm{Sym}_f^\gamma, s) = \prod_{p \neq q} \prod_{h=0}^{\gamma} (1 - \alpha_f^{\gamma-h}(p)\beta_f^h(p)p^{-s})^{-1} \tag{4.2}$$

for $\sigma > 1$. Let $\mu, \nu \in \mathbb{N}$, $\mu - \nu = 2$. By $Q(\mu)$ we denote the smallest prime number satisfying $2^\mu/\sqrt{Q(\mu)} < 1$. The main results in [27] is the limit formula for the value-distribution of the difference

$$\log L_q(\mathrm{Sym}_f^\mu, \sigma) - \log L_q(\mathrm{Sym}_f^\nu, \sigma)$$

(see Theorem 4.1 below).

In the proof of limit theorems mentioned in the present article, some kind of "independence" or "orthogonality" properties are necessary. For example, in the proof of Theorem 1.1 and Theorem 2.1, the Kronecker-Weyl theorem on the uniform distribution of sequences is used. Ihara's argument [10] for L-functions is based on the orthogonality of Dirichlet characters. In the present situation, the necessary tool is supplied by Petersson's formula, in the form shown in the second author's article [9]. In view of the formula in [9], we define the following weighted sum for any sequence $\{A_f\}$ over primitive forms $f \in S_k(q^m)$:

$$\sum_f{}' A_f = \frac{1}{C_k(1 - C_q(m))} \sum_f \frac{A_f}{\langle f, f \rangle_P}, \tag{4.3}$$

where

$$C_k = \frac{(4\pi)^{k-1}}{\Gamma(k-1)}, \quad C_q(m) = \begin{cases} 0, & m = 1, \\ q(q^2-1)^{-1}, & m = 2, \\ q^{-1}, & m \geq 3, \end{cases}$$

the symbol $\langle , \rangle_P$ is the Petersson inner product, and the sum on the right-hand side of (4.3) runs over all primitive forms belonging to $S_k(q^m)$.

We define two types of averages in the level aspect. The first one is

$$\begin{aligned} &\mathrm{Avg}_{\mathrm{prime}} \Psi(\log L_q(\mathrm{Sym}_f^\mu, \sigma) - \log L_q(\mathrm{Sym}_f^\nu, \sigma)) \\ &= \lim_{q \to \infty} \sum_f{}' \Psi(\log L_q(\mathrm{Sym}_f^\mu, \sigma) - \log L_q(\mathrm{Sym}_f^\nu, \sigma)) \end{aligned} \tag{4.4}$$

for fixed m, where $\Psi : \mathbb{R} \to \mathbb{C}$ is a test function. The second one is

$$\begin{aligned} &\mathrm{Avg}_{\mathrm{power}} \Psi(\log L_q(\mathrm{Sym}_f^\mu, \sigma) - \log L_q(\mathrm{Sym}_f^\nu, \sigma)) \\ &= \lim_{m \to \infty} \sum_f{}' \Psi(\log L_q(\mathrm{Sym}_f^\mu, \sigma) - \log L_q(\mathrm{Sym}_f^\nu, \sigma)) \end{aligned} \tag{4.5}$$

for fixed q, where q is a prime and $q \geq Q(\mu)$ if $1 \geq \sigma > 1/2$.

Theorem 4.1 ([27]). *Let $f \in S_k(N)$ be a primitive form, $2 \le k < 12$ or $k = 14$, and $N = q^m$ with a certain prime q. Let $\mu, \nu \in \mathbb{N}$, $\mu - \nu = 2$. We assume that the symmetric power L-functions $L_q(\mathrm{Sym}_f^{\mu}, s)$, $L_q(\mathrm{Sym}_f^{\nu}, s)$ can be continued holomorphically to $\sigma > 1/2$, satisfy the estimate $\ll q^m(|t| + 2)$ in the strip $2 \ge \sigma > 1/2$, and have no zero in $1 \ge \sigma > 1/2$. Then, for any $\sigma > 1/2$, there exists a density function $\mathcal{M}_\sigma : \mathbb{R} \to \mathbb{R}_{\ge 0}$ which can be explicitly constructed, and for which the formula*

$$\begin{aligned}
&\mathrm{Avg}_{\mathrm{prime}} \Psi(\log L_q(\mathrm{Sym}_f^{\mu}, \sigma) - \log L_q(\mathrm{Sym}_f^{\nu}, \sigma)) \\
&\quad = \mathrm{Avg}_{\mathrm{power}} \Psi(\log L_q(\mathrm{Sym}_f^{\mu}, \sigma) - \log L_q(\mathrm{Sym}_f^{\nu}, \sigma)) \\
&\quad = \int_{\mathbb{R}} \mathcal{M}_\sigma(u) \Psi(u) \frac{du}{\sqrt{2\pi}} \qquad (4.6)
\end{aligned}$$

holds for any test function Ψ which is bounded continuous, or a compactly supported characteristic function.

In this theorem we require several assumptions, which are plausible but seem very difficult to prove. The main reason of using those assumptions is that we have no idea of showing suitable mean value estimates for symmetric power L-functions.

For any $\sigma > 1$, since $\mu - \nu = 2$, we have

$$\begin{aligned}
&\log L_q(\mathrm{Sym}_f^{\mu}, s) - \log L_q(\mathrm{Sym}_f^{\nu}, s) \\
&\quad = \sum_{p \ne q} (-\log(1 - \alpha_f^{\mu}(p) p^{-s}) - \log(1 - \beta_f^{\mu}(p) p^{-s})).
\end{aligned}$$

If we could find a method for the study of $\mathrm{Avg}_{\mathrm{prime}}$ and $\mathrm{Avg}_{\mathrm{power}}$ of the right-hand side of the above equation in the case $\mu = 1$, it would imply the limit theorem for $\log L(f, s)$ similar to (3.4), but at present we cannot extend the theorem to $\log L(f, s)$. (The theorem is shown only for $\mu \ge 3$.)

Lebacque and Zykin [22] studied $\log L(f, s)$ and $(L'/L)(f, s)$ along the line of [13], and obtained a result analogous to [13, Theorem 1]. However their argument also does not arrive at the limit theorem for $\log L(f, s)$ or $(L'/L)(f, s)$ of the form (3.1) or (3.4).

5. The value-distribution of automorphic L-functions (the t-aspect)

Now we return to the matter of t-aspect. As we mentioned in Section 2, the part (ii) of Theorem 1.1 has been generalized only for some special cases when convex properties can be used.

Automorphic L-functions are typical examples for which the corresponding curves are not always convex, so it is important how to generalize the part (ii) of Theorem 1.1 to the case of automorphic L-functions $L(f, s)$. This has been done in [28].

Since $L(f, s) \in \mathscr{M}_{00}$, the existence of the limit $W_\sigma(R; L(f, \cdot))$ (for $\sigma > 1/2$) is already known by Theorem 2.1.

Theorem 5.1 ([28]). *For any $\sigma > 1/2$, there exists a continuous non-negative function $\mathcal{M}_\sigma(z, L(f,\cdot))$, explicitly defined on $\mathbb{C}$, for which*

$$W_\sigma(R; L(f,\cdot)) = \int_R \mathcal{M}_\sigma(z, L(f,\cdot))|dz| \tag{5.1}$$

holds.

Remark 5.2. Once (5.1) is proved, then we can deduce

$$\lim_{T\to\infty} \frac{1}{2T}\int_{-T}^{T} \Phi(\log L(f, s+i\tau))d\tau = \int_{\mathbb{C}} \mathcal{M}_\sigma(z, L(f,\cdot))\Phi(z)|dz| \tag{5.2}$$

for any test function Φ as in the statement of Theorem 3.1, by the argument given in [12, Remark 9.1]. Note that the left-hand side of (5.2) is the function of variable s, but the M-function on the right-hand side depends only on $\sigma = \Re s$.

The basic structure of the proof of Theorem 5.1 in [28], which we briefly outline here, is along the line similar to [24]. Actually in [28], we are working in more general situation, that is in the class $\mathscr{M}$. Let $\varphi \in \mathscr{M}$. Define the integral

$$K_n(w;\varphi) = \int_0^1 \exp\left(i\langle z_n(\theta_n;\varphi), w\rangle\right) d\theta_n \qquad (n \in \mathbb{N}), \tag{5.3}$$

where $z_n(\theta_n;\varphi)$ is defined by (2.6) and $\langle z, w\rangle = \Re z \Re w + \Im z \Im w$. In [28], we prove the following

Lemma 5.3 ([28]). *If there are at least five n's for which*

$$K_n(w;\varphi) = O_n(|w|^{-1/2}) \qquad (|w| \to \infty) \tag{5.4}$$

holds, then we can find a continuous non-negative function $\mathcal{M}_\sigma(z,\varphi)$ for $\sigma > \sigma_0$ by which we can write

$$W_\sigma(R;\varphi) = \int_R \mathcal{M}_\sigma(z,\varphi)|dz|. \tag{5.5}$$

Moreover $\mathcal{M}_\sigma(z,\varphi)$ is explicitly given by

$$\mathcal{M}_\sigma(z,\varphi) = \int_{\mathbb{C}} e^{-i\langle z,w\rangle}\Lambda(w;\varphi)|dw|, \tag{5.6}$$

where

$$\Lambda(w;\varphi) = \int_{\mathbb{C}} e^{i\langle z,w\rangle} dW_\sigma(z;\varphi). \tag{5.7}$$

Therefore the main problem is reduced to the proof of (5.4). Jessen and Wintner [16] proved that $K_n(w,\varphi) = O(|w|^{-1/2})$ for any n, when the corresponding curves are convex. This is the original Jessen-Wintner inequality.

Now consider the case of automorphic L-functions. Let $\mathbb{P}_f(\varepsilon)$ be the set of primes p satisfying $|\lambda_f(p)| > \sqrt{2} - \varepsilon$. Then $\mathbb{P}_f(\varepsilon)$ is of positive density (M. R. Murty [34] for the full modular case, and M. R. Murty and V. K. Murty [35] for any level N). In [28], we observed geometric behavior of the corresponding curves and proved

Lemma 5.4 ([28]). *If $p_n \in \mathbb{P}_f(\varepsilon)$ and n is sufficiently large, then*

$$K_n(w; L(f,\cdot)) = O_\varepsilon\left(p_n^{\sigma/2}|w|^{-1/2} + p_n^{\sigma}|w|^{-1}\right) \tag{5.8}$$

holds.

Since $\mathbb{P}_f(\varepsilon)$ is of positive density, obviously we can find more than five (actually infinitely many) n's for which (5.8) is valid. Therefore using Lemma 5.3 we can deduce the conclusion of Theorem 5.1.

6. The value-distribution of symmetric power L-functions (the t-aspect)

Now we proceed to state our new results in the present paper, on the value-distribution of symmetric power L-functions. The proof of the results stated in this section will be given in Sections 7 and 8.

Assume N is square-free and let $f \in S_k(N)$ be a primitive form. First consider the case $\gamma = 2$, that is the symmetric square L-functions

$$L(\mathrm{Sym}_f^2, s) = L_N(\mathrm{Sym}_f^2, s)\prod_{p|N}(1-\lambda_f(p^2)p^{-s})^{-1},$$

where $L_N(\mathrm{Sym}_f^2, s)$ is defined by (4.1).

Let

$$\Lambda(\mathrm{Sym}_f^2, s) = N^s\pi^{-3s/2}\Gamma\left(\frac{s+1}{2}\right)\Gamma\left(\frac{s+k-1}{2}\right)\Gamma\left(\frac{s+k}{2}\right)L(\mathrm{Sym}_f^2, s).$$

Then it is known (Shimura [38], Gelbart and Jacquet [6]; see also [15]) that $\Lambda(\mathrm{Sym}_f^2, s)$ can be continued to an entire function, and satisfies the functional equation

$$\Lambda(\mathrm{Sym}_f^2, s) = \Lambda(\mathrm{Sym}_f^2, 1-s). \tag{6.1}$$

Because of (6.1), we can apply the general theorem of Kanemitsu, Sankaranarayanan and Tanigawa [19]. The part (iii) of their Theorem 1 implies that, in the strip $2/3 < \sigma < 1$, it holds that

$$\int_1^T |L(\mathrm{Sym}_f^2, \sigma+it)|^2 dt = C_2(\sigma, f)T + O\left(T^{2-(3/2)\sigma+\varepsilon}\right) \tag{6.2}$$

for any $\varepsilon > 0$, where $C_2(\sigma, f)$ is a constant depending on σ and f. (Note that the first author [26] developed a more refined general theory, which improves the error estimate in (6.2) to $O(T^{3-3\sigma+\varepsilon})$; see [26, (3.10)].) From (6.2) we find that

$$\int_1^T |L(\mathrm{Sym}_f^2, \sigma+it)|^2 dt = O(T) \tag{6.3}$$

for $\sigma > 2/3$. This is condition (iii) of the class $\mathscr{M}_{00}$. Condition (ii) also follows from (6.1) by invoking the Phragmén-Lindelöf principle. Therefore $L(\mathrm{Sym}_f^2, \cdot) \in \mathscr{M}_{00}$, so the method in [28] can be applied to $L(\mathrm{Sym}_f^2, \cdot)$. The result is

Theorem 6.1. *Let N be a square-free integer, and $f \in S_k(N)$ a primitive form. For any $\sigma > 2/3$, there exists a continuous non-negative function $\mathcal{M}_\sigma(z, L(\mathrm{Sym}_f^2, \cdot))$, explicitly defined on $\mathbb{C}$, for which*

$$\lim_{T\to\infty} \frac{1}{2T} \int_{-T}^{T} \Phi(\log L(\mathrm{Sym}_f^2, s+i\tau))d\tau = \int_{\mathbb{C}} \mathcal{M}_\sigma(z, L(\mathrm{Sym}_f^2, \cdot))\Phi(z)|dz| \quad (6.4)$$

holds for any test function Φ as in the statement of Theorem 3.1.

Next consider more general symmetric power L-functions. Recall the partial L-function $L_N(\mathrm{Sym}_f^\gamma, s)$ (see (4.1)) associated with a primitive form $f \in S_k(N)$, where N is a positive integer. It is known that $L_N(\mathrm{Sym}_f^\gamma, s)$ has meromorphic continuation to the whole complex plane (see [2]). We assume the following

Assumption 6.2. There are predicted local factors $L_p(\mathrm{Sym}_f^\gamma, s)$ for $p \mid N$ and $L_N(\mathrm{Sym}_f^\gamma, s)$ satisfies the functional equation

$$\Lambda(\mathrm{Sym}_f^\gamma, s) = \varepsilon_{\gamma,f}\Lambda(\mathrm{Sym}_f^\gamma, 1-s), \quad (6.5)$$

where $|\varepsilon_{\gamma,f}| = 1$ and

$$\Lambda(\mathrm{Sym}_f^\gamma, s) = q_{\gamma,f}^{s/2}\widetilde{\Gamma}_\gamma(s)L_N(\mathrm{Sym}_f^\gamma, s)\prod_{p|N} L_p(\mathrm{Sym}_f^\gamma, s)$$

with the conductor $q_{\gamma,f}$ and the "gamma factor" $\widetilde{\Gamma}_\gamma(s)$. Here, the gamma factor is written by

$$\widetilde{\Gamma}_\gamma(s) = \pi^{-(\gamma+1)s/2}\prod_{j=1}^{\gamma+1}\Gamma\left(\frac{s+\kappa_{j,\gamma}}{2}\right), \quad (6.6)$$

where $\kappa_{j,\gamma} \in \mathbb{R}$, and each local factor for $p|N$ is written as

$$L_p(\mathrm{Sym}_f^\gamma, s) = (1-\lambda_{p,\gamma,f}p^{-s})^{-1}, \quad |\lambda_{p,\gamma,f}| \le p^{-\gamma/2} \quad (6.7)$$

(see Cogdell and Michel [5], Moreno and Shahidi [32], Rouse [36], and Rouse and Thorner [37]).

The above assumptions are reasonable in view of the Langlands functoriality conjecture. Now define the γ th symmetric power L-function

$$L(\mathrm{Sym}_f^\gamma, s) = L_N(\mathrm{Sym}_f^\gamma, s)\prod_{p|N} L_p(\mathrm{Sym}_f^\gamma, s).$$

From (4.1) and (6.7) we see that the Dirichlet series expansion of $L(\mathrm{Sym}_f^\gamma, s)$ is of the form $\sum_{n=1}^\infty c_n n^{-s}$, $|c_n| \ll n^\varepsilon$. Since the gamma factor is given by (6.6), again using the general result of [19], we obtain

$$\int_1^T |L(\mathrm{Sym}_f^\gamma, \sigma+it)|^2 dt = C_\gamma(\sigma, f)T + O\left(T^{1+(\gamma/2)-((\gamma+1)/2)\sigma+\varepsilon}\right) \quad (6.8)$$

in the strip $1 - 1/(\gamma + 1) < \sigma < 1$, with a certain constant $C_\gamma(\sigma, f)$. Therefore $L(\mathrm{Sym}_f^\gamma, \cdot) \in \mathscr{M}_{00}$.

Another tool we use is the following quantitative version of the Sato-Tate conjecture due to Thorner [40]. We write $\alpha_f(p) = e^{i\theta_f(p)}$; we may assume $0 \le \theta_f(p) \le \pi$. Let I be any subset of $[0, \pi]$, and let

$$\pi_I(x) = \#\{p : \text{prime} \mid p \le x,\ \theta_f(p) \in I\}.$$

Then Thorner's result is, under Assumption 6.2,

$$\frac{\pi_I(x)}{\pi(x)} = \frac{2}{\pi}\int_a^b \sin^2\theta d\theta + O\left(\frac{x}{\pi(x)(\log x)^{9/8-\varepsilon}}\right) \tag{6.9}$$

for any $\varepsilon > 0$, where $I = [a, b]$. (Under the assumption of the GRH for $L(\mathrm{Sym}_f^\gamma, s)$, sharper estimates for the error term are known.)

Theorem 6.3. *Let N be a positive integer. Let $f \in S_k(N)$ be a primitive form which is not of CM-type. Let $\gamma \ge 2$, and assume Assumption 6.2. Then, for any $\sigma > 1 - 1/(\gamma + 1)$, there exists a continuous non-negative function $\mathcal{M}_\sigma(z, L(\mathrm{Sym}_f^\gamma, \cdot))$, explicitly defined on $\mathbb{C}$, for which*

$$\lim_{T\to\infty}\frac{1}{2T}\int_{-T}^{T}\Phi(\log L(\mathrm{Sym}_f^\gamma, s + i\tau))d\tau$$

$$= \int_{\mathbb{C}}\mathcal{M}_\sigma(z, L(\mathrm{Sym}_f^\gamma, \cdot))\Phi(z)|dz| \tag{6.10}$$

holds for any test function Φ as in the statement of Theorem 3.1.

Remark 6.4. In Theorem 6.3 we assume Assumtion 6.2, because it is not yet fully proved. However, Barnet-Lamb et al. [2] proved the "potential automorphy" of $L(\mathrm{Sym}_f^\gamma, s)$, which gives a certain functional equation (see [2, Theorem B, Assertion 2]). If the factors appearing in the functional equation are shown to be sufficiently well-behaved, we can apply the result in [19] to obtain some suitable mean value result unconditionally, so we can remove Assumtion 6.2 from the statement of Theorem 6.3.

Remark 6.5. In [27], we adopt a more restricted form of local factors for $p|N$ in the definition of symmetric power L-functions. However, the argument in [27] is valid without change even if we use the above definition of symmetric power L-functions in the present paper. Therefore the main result in [27], which is Theorem 4.1 in the present paper, is also valid as it is.

7. Some general lemmas

We start the proof of theorems stated in the preceding section. In this section we consider the general situation that $\varphi \in \mathscr{M}_{00}$ with $f(k, n) = 1$ for all k and n. Then

$$z_n(\theta_n; \varphi) = -\sum_{k=1}^{g(n)}\log(1 - a_n^{(k)} p_n^{-\sigma} e^{2\pi i\theta_n}). \tag{7.1}$$

Put

$$R_n(X;\varphi) = -\sum_{k=1}^{g(n)} \log(1 - a_n^{(k)} X),$$

and write its Taylor expansion as $R_n(X;\varphi) = \sum_{j=1}^{\infty} r_{j,n} X^j$. Then we have

$$z_n(\theta_n;\varphi) = R_n(p_n^{-\sigma} e^{2\pi i\theta_n};\varphi) = \sum_{j=1}^{\infty} r_{j,n} p_n^{-j\sigma} e^{2\pi i j\theta_n}. \tag{7.2}$$

Let $x_n(\theta_n;\varphi) = \Re z_n(\theta_n;\varphi)$ and $y_n(\theta_n;\varphi) = \Im z_n(\theta_n;\varphi)$. Write $w = |w|e^{i\tau} = |w|\cos\tau + i|w|\sin\tau$. Then

$$\langle z_n(\theta_n;\varphi), w\rangle = |w| g_{\tau,n}(\theta_n;\varphi), \tag{7.3}$$

where

$$g_{\tau,n}(\theta_n;\varphi) = x_n(\theta_n;\varphi)\cos\tau + y_n(\theta_n;\varphi)\sin\tau.$$

Substituting this into (5.3), we have

$$K_n(w,\varphi) = \int_0^1 \exp\left(i|w| g_{\tau,n}(\theta_n;\varphi)\right) d\theta_n. \tag{7.4}$$

Therefore, to evaluate $K_n(w,\varphi)$, the essential point is to analyze the behavior of $g_{\tau,n}(\theta_n;\varphi)$. We prove

Lemma 7.1. *Let $\varphi \in \mathscr{M}_{00}$. The function $g_{\tau,n}(\theta_n;\varphi)$ is a C^∞-class function as a function in θ_n. Moreover, if n is sufficiently large, and*

$$|r_{1,n}| \geq C \tag{7.5}$$

holds with a positive constant C, then for those n, $g''_{\tau,n}(\theta_n;\varphi)$ has exactly two zeros on the interval $[0,1)$. *The same assertion also holds for $g'_{\tau,n}(\theta_n;\varphi)$.*

Proof. This lemma is an analogue of [28, Lemma 7.1]. From the definition, we have

$$r_{j,n} = \frac{1}{j}\sum_{k=1}^{g(n)} (a_n^{(k)})^j. \tag{7.6}$$

Since $\varphi \in \mathscr{M}_{00}$, we find that $|r_{j,n}| \leq g(n)/j \leq C_0/j$. Noting this point, we can see that exactly the same argument as in the proof of [28, Lemma 7.1] can be applied to our present situation. (The part on $g'_{\tau,n}(\theta_n;\varphi)$ is the same as in [28, Remark 7.1].) □

Now we can show the following lemma, which is the analogue of Lemma 5.4 for $\varphi \in \mathscr{M}_{00}$.

Lemma 7.2 (The Jessen-Wintner inequality for φ). *Let $\varphi \in \mathscr{M}_{00}$, and assume that n is sufficiently large and* (7.5) *holds. Then we have*

$$K_n(w,\varphi) = O\left(p_n^{\sigma/2}|w|^{-1/2} + p_n^{\sigma}|w|^{-1}\right). \tag{7.7}$$

Proof. The method of the proof is the same as in [28, Proposition 7.1] (whose idea goes back to Jessen and Wintner [16]), so we just sketch the idea briefly.

Using (7.2) we have

$$g_{\tau,n}(\theta_n;\varphi)=\sum_{j=1}^{\infty}|r_{j,n}|p_n^{-j\sigma}\cos(\gamma_{j,n}+2\pi j\theta_n-\tau),$$

where $\gamma_{j,n}=\arg r_{j,n}$, and hence

$$g'_{\tau,n}(\theta_n;\varphi)=-2\pi|r_{1,n}|p_n^{-\sigma}\sin(\gamma_{1,n}+2\pi\theta_n-\tau)+O(p_n^{-2\sigma}),$$
$$g''_{\tau,n}(\theta_n;\varphi)=-(2\pi)^2|r_{1,n}|p_n^{-\sigma}\cos(\gamma_{1,n}+2\pi\theta_n-\tau)+O(p_n^{-2\sigma}).$$

Let $\theta_n=\theta_1^{\mathrm{c}},\theta_2^{\mathrm{c}}$ be two solutions of $\cos(\gamma_{1,n}+2\pi\theta_n-\tau)=0$ $(0\le\theta_n<1)$. Then, when n is sufficiently large and (7.5) holds, the two solutions of $g''_{\tau,n}(\theta_n;\varphi)=0$ stated in Lemma 7.1 are close to $\theta_1^{\mathrm{c}},\theta_2^{\mathrm{c}}$. Similarly, the two solutions of $g'_{\tau,n}(\theta_n;\varphi)=0$ are close to the two solutions $\theta_n=\theta_1^{\mathrm{s}},\theta_2^{\mathrm{s}}$ of $\sin(\gamma_{1,n}+2\pi\theta_n-\tau)=0$. Then, for each i,j $(1\le i,j\le 2)$, there exists a unique θ_{ij} between θ_i^{c} and θ_j^{s} for which

$$|\sin(\gamma_{1,n}+2\pi\theta_n-\tau)|=|\cos(\gamma_{1,n}+2\pi\theta_n-\tau)|=1/\sqrt{2}$$

holds.

We divide the interval $0\le\theta_n<1$ (mod 1) into four subintervals at the values θ_{ij}, and divide also the integral (7.4) accordingly.

On two of those subintervals $|\sin(\gamma_{1,n}+2\pi\theta_n-\tau)|\ge 1/\sqrt{2}$, which implies that $|g'_{\tau,n}(\theta_n;\varphi)|$ is not close to 0. Therefore the integrals on those subintervals can be evaluated by the first derivative test. On the other two subintervals $|g''_{\tau,n}(\theta_n;\varphi)|$ is not close to 0, so the second derivative test works. These evaluations give the conclusion (7.7). □

If there exist at least five large values of n for which (7.5) holds, then we can apply Lemma 7.2 to Lemma 5.3 to obtain

$$W_\sigma(R;\varphi)=\int_R\mathcal{M}_\sigma(z,\varphi)|dz| \tag{7.8}$$

for any $\sigma>\sigma_0$, with an explicitly constructed continuous non-negative function $\mathcal{M}_\sigma(z,\varphi)$ (the associated M-function). Then, as indicated in Remark 5.2, we can deduce the formula of the form

$$\lim_{T\to\infty}\frac{1}{2T}\int_{-T}^{T}\Phi(\log\varphi(s+i\tau))d\tau=\int_{\mathbb{C}}\mathcal{M}_\sigma(z,\varphi)\Phi(z)|dz| \tag{7.9}$$

in the region $\sigma>\sigma_0$, for any test function Φ as in the statement of Theorem 3.1. Therefore, to complete the proof of our theorems, the only remaining task is to show (7.5) for sufficiently many large values of n.

8. Proof of Theorems 6.1 and 6.3

Now we return to the specific situation of symmetric power L-functions.

Proof of Theorem 6.1. In this case, for any n such that $p_n \nmid N$, we see that $g(n) = 3$, and from (7.6) we have

$$\begin{aligned} r_{1,n} &= \alpha_f^2(p_n) + \alpha_f(p_n)\beta_f(p_n) + \beta_f^2(p_n) \\ &= (\alpha_f(p_n) + \beta_f(p_n))^2 - \alpha_f(p_n)\beta_f(p_n) \\ &= (\lambda_f(p_n))^2 - 1. \end{aligned} \tag{8.1}$$

If $p_n \in \mathbb{P}_f(\varepsilon)$, then $|\lambda_f(\varepsilon)| > \sqrt{2} - \varepsilon$, so

$$r_{1,n} > (\sqrt{2} - \varepsilon)^2 - 1 = 1 - (2\sqrt{2}\varepsilon - \varepsilon^2),$$

which is positive if ε is small. Since $\mathbb{P}_f(\varepsilon)$ is a set of positive density, we now obtain the inequality (7.5) for infinitely many values of n. This completes the proof. □

Proof of Theorem 6.3. In this case, for any n such that $p_n \nmid N$,

$$r_{1,n} = \sum_{h=0}^{\gamma} \alpha_f^{\gamma-h}(p_n)\beta_f^h(p_n).$$

In particular $r_{1,n}$ is real, and so

$$r_{1,n} = \Re r_{1,n} = \sum_{h=0}^{\gamma} \cos((\gamma - 2h)\theta_f(p_n)).$$

Then it is easy to see that

$$r_{1,n} = \begin{cases} \sin((\gamma+1)\theta_f(p_n))/\sin\theta_f(p_n) & \theta_f(p_n) \neq 0, \pi \\ \gamma + 1 & \theta_f(p_n) = 0 \\ \gamma + 1 & \theta_f(p_n) = \pi,\ \gamma \text{ is even} \\ -\gamma - 1 & \theta_f(p_n) = \pi,\ \gamma \text{ is odd} \end{cases}$$

(cf. [35, p.86]), hence

$$|r_{1,n}| \geq |\sin((\gamma + 1)\theta_f(p_n))|. \tag{8.2}$$

Fix a number $\xi \in (0, \pi/2)$, and let $\eta = \sin\xi$. Then $0 < \eta < 1$. Define the intervals

$$A(j) = \left[\frac{2\pi j + \xi}{\gamma + 1}, \frac{2\pi j + \pi - \xi}{\gamma + 1}\right], \quad B(j) = \left[\frac{2\pi j + \pi + \xi}{\gamma + 1}, \frac{2\pi j + 2\pi - \xi}{\gamma + 1}\right]$$

where j is a non-negative integer. If γ is odd, then

$$|\sin((\gamma + 1)\theta_f(p_n))| \geq \eta \tag{8.3}$$

if and only if

$$\theta_f(p_n) \in I_1 := \bigcup_{j=0}^{(\gamma-1)/2} (A(j) \cup B(j)). \tag{8.4}$$

If γ is even, then (8.3) holds if and only if

$$\theta_f(p_n) \in I_2 := \bigcup_{j=0}^{(\gamma-2)/2} (A(j) \cup B(j)) \cup A(\gamma/2). \tag{8.5}$$

These observations, (8.2) and (8.3) imply that $|r_{1,n}| \geq \eta$ if $\theta_f(p_n) \in I_1$ (if γ is odd) or $\in I_2$ (if γ is even). Therefore, to prove Theorem 6.3, it is enough to show that the set

$$\{p : \text{prime} \mid \theta_f(p_n) \in I_\ell\} \quad (\ell = 1, 2) \tag{8.6}$$

is of positive density.

Since

$$\int_a^b \sin^2 \theta d\theta = \frac{1}{2}\left(b - a - \frac{1}{2}(\sin 2b - \sin 2a)\right),$$

from (6.9) we have

$$\frac{\pi_I(x)}{\pi(x)} = \frac{1}{\pi}\left(b - a - \frac{1}{2}(\sin 2b - \sin 2a)\right) + O\left((\log x)^{-1/8+\varepsilon}\right) \tag{8.7}$$

for $I = [a, b]$. Denote

$$a_{A(j)} = \frac{2\pi j + \xi}{\gamma + 1}, \quad b_{A(j)} = \frac{2\pi j + \pi - \xi}{\gamma + 1},$$
$$a_{B(j)} = \frac{2\pi j + \pi + \xi}{\gamma + 1}, \quad b_{B(j)} = \frac{2\pi j + 2\pi - \xi}{\gamma + 1}.$$

Then from (8.7) we can write

$$\frac{\pi_{I_\ell}(x)}{\pi(x)} = \frac{1}{\pi}S_\ell + \frac{1}{2\pi}T_\ell + O\left((\log x)^{-1/8+\varepsilon}\right) \qquad (\ell = 1, 2), \tag{8.8}$$

where

$$S_1 = \sum_{j=0}^{(\gamma-1)/2} \left((b_{A(j)} - a_{A(j)}) + (b_{B(j)} - a_{B(j)})\right),$$

$$S_2 = \sum_{j=0}^{(\gamma-2)/2} \left((b_{A(j)} - a_{A(j)}) + (b_{B(j)} - a_{B(j)})\right) + \left(b_{A(\gamma/2)} - a_{A(\gamma/2)}\right),$$

$$T_1 = \sum_{j=0}^{(\gamma-1)/2} \left((\sin(2b_{A(j)}) - \sin(2a_{A(j)})) + (\sin(2b_{B(j)}) - \sin(2a_{B(j)}))\right),$$

$$T_2 = \sum_{j=0}^{(\gamma-2)/2} \left((\sin(2b_{A(j)}) - \sin(2a_{A(j)})) + (\sin(2b_{B(j)}) - \sin(2a_{B(j)}))\right) + \left(\sin(2b_{A(\gamma/2)}) - \sin(2a_{A(\gamma/2)})\right).$$

It is easy to see that

$$S_\ell = \pi - 2\xi \qquad (\ell = 1, 2). \tag{8.9}$$

Next we show that

$$T_\ell = 0 \qquad (\ell = 1, 2). \tag{8.10}$$

In fact, we know

$$(\sin(2b_{\square(j)}) - \sin(2a_{\square(j)})) = 2\sin\frac{\pi - 2\xi}{\gamma + 1}\cos\frac{4\pi j + c\pi}{\gamma + 1},$$

where $c = 1$ if $\square = A$ and $c = 3$ if $\square = B$. Then

$$T_1 = 2\sin\frac{\pi - 2\xi}{\gamma + 1}\sum_{j=0}^{(\gamma-1)/2}\left(\cos\frac{4\pi j + \pi}{\gamma + 1} + \cos\frac{4\pi j + 3\pi}{\gamma + 1}\right)$$

$$= 4\sin\frac{\pi - 2\xi}{\gamma + 1}\cos\frac{\pi}{\gamma + 1}\sum_{j=0}^{(\gamma-1)/2}\cos\frac{4\pi j + 2\pi}{\gamma + 1},$$

and

$$\sin\frac{2\pi}{\gamma + 1}\sum_{j=0}^{(\gamma-1)/2}\cos\frac{4\pi j + 2\pi}{\gamma + 1} = \frac{1}{2}\sum_{j=0}^{(\gamma-1)/2}\left(\sin\frac{4\pi(j + 1)}{\gamma + 1} - \sin\frac{4\pi j}{\gamma + 1}\right)$$

$$= \frac{1}{2}(\sin(2\pi) - \sin 0) = 0,$$

therefore $T_1 = 0$ (note that $\sin(2\pi/(\gamma + 1)) \neq 0$ because $\gamma \geq 2$). Similarly we find that

$$T_2 = 4\sin\frac{\pi - 2\xi}{\gamma + 1}\cos\frac{\pi}{\gamma + 1}\sum_{j=0}^{(\gamma-2)/2}\cos\frac{4\pi j + 2\pi}{\gamma + 1} + 2\sin\frac{\pi - 2\xi}{\gamma + 1}\cos\frac{\pi}{\gamma + 1},$$

and the sum on the right-hand side is equal to $-1/2$, and hence $T_2 = 0$.

From (8.8), (8.9) and (8.10) we obtain

$$\frac{\pi_{I_\ell}(x)}{\pi(x)} = 1 - \frac{2\xi}{\pi} + O\left((\log x)^{-1/8+\varepsilon}\right) \qquad (\ell = 1, 2). \tag{8.11}$$

Since $\xi < \pi/2$, this implies that the set (8.6) is of positive density in the set of all primes. This completes the proof. □

Remark 8.1. Actually, to prove Theorem 6.3, it is not necessary to invoke the quantitative result of Thorner [40]. The above argument, combined with the famous solution of the Sato-Tate conjecture [2], implies

$$\frac{\pi_{I_\ell}(x)}{\pi(x)} \sim 1 - \frac{2\xi}{\pi} > 0, \tag{8.12}$$

which is sufficient for our purpose. However we may expect that a quantitative formula like (8.11) will be useful when we try to develop more detailed study on M-functions.

Acknowledgement

A part of the contents of this paper was presented at the International Conference on Number Theory, celebrating the 130th birth anniversary of Srinivasa Ramanujan, held in IIT Ropar, Dec 2017. The first author expresses his gratitude to Professor Sanoli Gun and Professor Tapas Chatterjee for their kind invitation and hospitality. Research of the first author is supported by Grant-in-Aid for Science Research (B) 18H01111, and that of the second author is by Grant-in-Aid for Young Scientists (B) 23740020, JSPS.

References

[1] A. Akbary and A. Hamieh, Value-distribution of cubic Hecke L-functions, *J. Number Theory*, **206** (2020) 81–122.

[2] T. Barnet-Lamb, D. Geraghty, M. Harris and R. Taylor, A family of Calabi-Yau varieties and potential automorphy II, *Publ. RIMS Kyoto Univ.*, **47** (2011) 29–98.

[3] H. Bohr and B. Jessen, Über die Werteverteilung der Riemannschen Zetafunktion, Erste Mitteilung, *Acta Math.*, **54** (1930) 1–35; Zweite Mitteilung, *ibid.* **58** (1932) 1–55.

[4] H. Bohr and B. Jessen, Om Sandsynlighedsfordelinger ved Addition af konvekse Kurver, *Dan. Vid. Selsk. Skr. Nat. Math. Afd. (8)*, **12** (1929) 1–82.

[5] J. Cogdell and P. Michel, On the complex moments of symmetric power L functions at $s = 1$, *Intern. Math. Res. Notices*, (2004) no. 31, 1561–1617.

[6] S. Gelbart and H. Jacquet, A relation between automorphic representations of GL(2) and GL(3), *Ann. Sci. Éc. Norm. Sup. (4)*, **11** (1978) 471–542.

[7] C. R. Guo, The distribution of the logarithmic derivative of the Riemann zeta function, *Proc. London Math. Soc. (3)*, **72** (1996) 1–27.

[8] C. R. Guo, On the zeros of the derivative of the Riemann zeta function, *ibid.*, 28–62.

[9] Y. Ichihara (= Y. Umegaki), The first moment of L-functions of primitive forms on $\Gamma_0(p^\alpha)$ and a basis of old forms, *J. Number Theory*, **131** (2011) 343–362.

[10] Y. Ihara, On "M-functions" closely related to the distribution of L'/L-values, *Publ. RIMS Kyoto Univ.*, **44** (2008) 893–954.

[11] Y. Ihara and K. Matsumoto, On L-functions over function fields: Power-means of error terms and distribution of L'/L-values, in *Algebraic Number Theory and Related Topics 2008*, H. Nakamura et al. (eds.), *RIMS Kôkyûroku Bessatsu*, **B19** (2010) 221–247.

[12] Y. Ihara and K. Matsumoto, On certain mean values and the value-distribution of logarithms of Dirichlet L-functions, *Quart. J. Math. (Oxford)*, **62** (2011) 637–677.

[13] Y. Ihara and K. Matsumoto, On $\log L$ and L'/L for L-functions and the associated "M-functions": Connections in optimal cases, *Moscow Math. J.*, **11** (2011) 73–111.

[14] Y. Ihara and K. Matsumoto, On the value-distribution of logarithmic derivatives of Dirichlet L-functions, in *Analytic Number Theory, Approximation Theory, and Special Functions*, G. V. Milovanović et al. (eds.), Springer-Verlag, (2014) 79–91.

[15] H. Iwaniec and P. Michel, The second moment of the symmetric square L-functions, *Ann. Acad. Sci. Fenn. Math.* **26** (2001) no. 2, 465–482.

[16] B. Jessen and A. Wintner, Distribution functions and the Riemann zeta function, *Trans. Amer. Math. Soc.* **38** (1935) 48–88.

[17] D. Joyner, Distribution Theorems of L-functions, Longman Sci. & Tech., (1986).

[18] E. R. van Kampen and A. Wintner, Convolutions of distributions on convex curves and the Riemann zeta function, *Amer. J. Math.*, **59** (1937) 175–204.

[19] S. Kanemitsu, A. Sankaranarayanan and Y. Tanigawa, A mean value theorem for Dirichlet series and a general divisor problem, *Monatsh. Math.*, **136** (2002) 17–34.

[20] R. Kershner and A. Wintner, On the asymptotic distribution of $\zeta'/\zeta(s)$ in the critical strip, *Amer. J. Math.*, **59** (1937) 673–678.

[21] A. Laurinčikas, *Limit Theorems for the Riemann Zeta-Function*, Kluwer (1996).

[22] P. Lebacque and A. Zykin, On M-functions associated with modular forms, *Moscow Math. J.*, **18** (2018) 437–472.

[23] K. Matsumoto, Value-distribution of zeta-functions, in *Analytic Number Theory, Proc. Japanese-French Sympos. held in Tokyo*, K. Nagasaka and E. Fouvry (eds.), *Lect. Notes in Math.*, Springer-Verlag, **1434** (1990) 178–187.

[24] K. Matsumoto, Asymptotic probability measures of zeta-functions of algebraic number fields, *J. Number Theory*, **40** (1992) 187–210.

[25] K. Matsumoto, Asymptotic probability measures of Euler products, in *Proc. Amalfi Conf. on Analytic Number Theory*, E. Bombieri et al. (eds.), Univ. Salerno, (1992) 295–313.

[26] K. Matsumoto, Liftings and mean value theorems for automorphic L-functions, *Proc. London Math. Soc. (3)*, **90** (2005) 297–320.

[27] K. Matsumoto and Y. Umegaki, On the value-distribution of the difference between logarithms of two symmetric power L-functions, *Intern. J. Number theory*, **14** (2018) 2045–2081.

[28] K. Matsumoto and Y. Umegaki, On the density function for the value-distribution of automorphic L-functions, *J. Number Theory*, **198** (2019) 176–199.

[29] M. Mine, On the value-distributions of logarithmic derivatives of Dedekind zeta functions, preprint, arXiv:1705.07865.

[30] M. Mine, The density function for the value-distribution of Lerch zeta functions and its applications, *Michigan Math. J.*, to appear, arXiv:1805.11066.

[31] M. Mine, On certain mean values of logarithmic derivatives of L-functions and the related density functions, *Funct. Approx. Comment. Math.*, **61** (2019) 179–199.

[32] C. J. Moreno and F. Shahidi, The L-functions $L(s, \mathrm{Sym}^m(r), \pi)$, *Canad. Math. Bull.*, **28** (1985) 405–410.

[33] M. Mourtada and V. K. Murty, Distribution of values of $L'/L(\sigma, \chi_D)$, *Moscow Math. J.*, **15** (2015) 497–509.

[34] M. R. Murty, Oscillations of Fourier coefficients of modular forms, *Math. Ann.*, **262** (1983) 431–446.

[35] M. R. Murty and V. K. Murty, Non-Vanishing of L-Functions and Applications, *Progr. in Math.*, **157**, Birkhäuser (1997).

[36] J. Rouse, Atkin-Serre type conjectures for automorphic representations on $GL(2)$, *Math. Res. Lett.*, **14** (2007) no. 2, 189–204.

[37] J. Rouse and J. Thorner, The explicit Sato-Tate conjecture and densities pertaining to Lehmer-type questions, *Trans. Amer. Math. Soc.*, **369** (2017) 3575–3604.

[38] G. Shimura, On the holomorphy of certain Dirichlet series, *Proc. London Math. Soc. (3)*, **31** (1975) 79–98.

[39] M. Suzuki, Nearest neighbor spacing distributions for the zeros of the real or imaginary part of the Riemann xi-function on vertical lines, *Acta Arith.*, **170** (2015) 47–65.

[40] J. Thorner, The error term in the Sato-Tate conjecture, *Arch. Math.*, **103** (2014) 147–156.

Topics in Number Theory, RMS-Lecture Notes Series No. 26, 2020, pp. 169–173.

The Gel'fond-Schneider Theorem Revisited

V. Kumar Murty

Department of Mathematics, University of Toronto, 40 St. George Street, Toronto, Canada M5S 2E4.
Fields Institute for Research in Mathematical Sciences, 222 College Street, Toronto, Canada M5T 3J1.
e-mail: murty@math.toronto.edu

Abstract. We give a proof of the Gel'fond-Schneider theorem by estimating the growth of the degree of certain number fields. The method is inspired by a paper of Lang in which he studies lower bounds for the degrees of fields generated by division points on an elliptic curve.

Keywords. Transcendence, Siegel's Lemma, Gel'fond-Schneider theorem.

2010 Subject Classification: Primary 11J81, 11J91

1. Introduction

The Gel'fond-Schneider theorem asserts that if β is an algebraic irrational, and $\alpha \neq 0, 1$ is algebraic, then α^{β} is transcendental. A good exposition of it can be found in the monograph of R. Murty and P. Rath ([3], Chapter 9) where it is derived from the Lang-Schneider theorem using the differential equation satisfied by the exponential function. The original proof of Schneider gave another approach by using the functional equation of the exponential function. We give a proof which is similar to Schneider's approach but which seems to be a little different from the usual approach.

I wrote this argument out in 1987 and circulated it to a few people. As pointed out to me at the time by M. Waldschmidt, the argument can actually be seen as a special case of Theorem 2.1 of his paper with Gramain and Mignotte [1]. However, for some technical reasons (such as the location of the zeros of the auxiliary function in a disc that is growing slowly with respect to other parameters), our approach still seems to be of interest. At the urging of the editors of this volume, I am presenting the notes here.

Our argument is inspired by an earlier paper by Lang [2]. In that article, Lang was trying to get information about the degree of the field generated by division points on an elliptic curve. Combining results of Deuring with those of Serre, we know that the Galois groups of such fields are as large as they can be (taking into account endomorphisms) but the proofs involve deep properties of elliptic curves. Lang was exploring what one could say about these fields of division points using the methods of transcendence. In particular, he proved that the degree of the field generated by the division points of order $N > 1$ grows at least as fast as a constant times N. This of course falls short of the theorems quoted above which tell us that, up to constants, the degree should grow like N^2 in the complex multiplication case, and like N^4 in the non-complex multiplication case.

The point of this note is to show that if we apply Lang's approach to the exponential function, we get the Gel'fond-Schneider theorem as a consequence. We shall prove the following.

Theorem 1. *Let α_0, α_1 be algebraic numbers that are $\mathbb{Q}$-linearly independent (that is, $\alpha_1/\alpha_0 \notin \mathbb{Q}$). Let $t \in \mathbb{C}\backslash\{0\}$. Then, at least one of $e^{t\alpha_0}$ and $e^{t\alpha_1}$ is transcendental.*

The Gel'fond-Schneider theorem follows by taking $t = \log \alpha$, $\alpha_0 = 1$ and $\alpha_1 = \beta$. Conversely, the Theorem follows from Gel'fond-Schneider by noting that if $e^{t\alpha_0}$ is algebraic, then as it is not equal to 0 or 1 (as $t \neq 0$), we have $(e^{t\alpha_0})^{\alpha_1/\alpha_0}$ is transcendental.

The strategy of proof is to consider the field

$$K = \mathbb{Q}(\alpha_0, \alpha_1, e^{t\alpha_0}, e^{t\alpha_1}).$$

If the theorem is false, this is a number field and we can set $A = [K : \mathbb{Q}]$. For each integer $N \geq 1$ and each pair of integers r_0, r_1, consider also the field

$$K_{N,r_0,r_1} = \mathbb{Q}\left(e^{t\left(\frac{r_0\alpha_0 + r_1\alpha_1}{N}\right)}\right).$$

Denote by d_{N,r_0,r_1} its degree over $\mathbb{Q}$ and set

$$d_N = \max_{r_0,r_1 \in \mathbb{Z}} d_{N.r_0,r_1}.$$

Then, we see that

$$d_N \leq AN.$$

We shall show that in fact

$$d_N \gg N \log N$$

thereby getting a contradiction.

2. Notation

We introduce some notation that will be used throughout and which can be referred to as one goes through the argument.

- $$R_1 = \max_{\sigma}\left(\sqrt{2}(|\alpha_0^\sigma|^2 + |\alpha_1^\sigma|^2)^{1/2}, 1\right)$$

  as σ runs over $\mathrm{Aut}(\mathbb{C}/\mathbb{Q})$.
- μ a large constant satisfying

  $$\mu > \max\left(3, \frac{2}{|t|}, eR_1\right)$$

  and $(\log x)/x \leq |t|$ for $x \geq \mu$.

- L a free parameter satisfying
$$L > \max\left((576\mu|t|)^2, \frac{1}{|t|}\right)$$
and $L/\log L > \mu^2$.
- $r = R_1 \log L$
- $R = \mu(L \log L)^{1/2}$
- $U = 3|t|LR$
- $S = 1728\mu^2|t|^2L$
- C a large integer that is a multiple of the denominators of $\alpha_0, \alpha_1, e^{t\alpha_0}, e^{t\alpha_1}$ and an upper bound for all their conjugates
- A constant
$$c_1 = \frac{3\log C}{|t|} + \frac{2}{3|t|} + \frac{2}{3}C + 192\mu^2|t|$$
- c_2 a constant larger than $2c_1$.

3. Lemmas

Lemma 1. *There are rational integers p_{λ_0,λ_1}, where $0 \le \lambda_0, \lambda_1 < L$, not all zero, with*
$$|p_{\lambda_0,\lambda_1}| < e^S$$
and such that
$$F(z) = \sum_{0\le\lambda_0,\lambda_1<L} p_{\lambda_0,\lambda_1} z^{\lambda_0} e^{tz\lambda_1}$$
satisfies
$$|F|_r \le e^{-U}.$$

This is a version of Siegel's lemma due to Waldschmidt [4].

Lemma 2. *The denominator of*
$$e^{t\left(\frac{\mathbf{r}\cdot\mathbf{a}}{N}\right)},$$
where $\mathbf{r} = (r_0, r_1)$ and $\mathbf{a} = (\alpha_0, \alpha_1)$, is
$$\le C^{2+2\max(r_0,r_1)/N}.$$

Proof. Indeed, write $r_i = \rho_i N + \lambda_i$ for $i = 0, 1$, $0 \le \lambda_i < N$, $|\rho_i| \le r_i/N$. Set
$$\gamma = C^2 e^{t\frac{\lambda_0\alpha_0+\lambda_1\alpha_1}{N}}.$$

Then,
$$\gamma^N = (Ce^{t\alpha_0})^{\lambda_0}(Ce^{t\alpha_1})^{\lambda_1}C^{2N-(\lambda_0+\lambda_1)}$$
is an algebraic integer of K. Also, the denominator of
$$e^{t(\rho_0\alpha_0+\rho_1\alpha_1)}$$
is
$$\le C^{\rho_0+\rho_1} \le C^{2\max(r_0,r_1)/N}. \qquad \square$$

Lemma 3. *For every integer*

$$N \in \left(\frac{R}{2c_2 A \log R}, \frac{R}{c_2 A \log R} \right)$$

and $\mathbf{r} = (r_0, r_1) \in \mathbb{Z}^2$ *with* $0 \le r_0, r_1 < N \log N$, $(r_0, N) = (r_1, N) = 1$, *we have*

$$F\left(\frac{\mathbf{r}\cdot\mathbf{a}}{N}\right) = 0.$$

Proof. We have

$$\left|\frac{\mathbf{r}\cdot\mathbf{a}}{N}\right| \le (\log N) R_1 \le R_1 \log L = r.$$

Hence, if $F(\mathbf{r}\cdot\mathbf{a}/N) \neq 0$ we have by Liouville

$$\left(L^2 e^S (CN)^L (CN \log N)^L C^{3L \log N} e^{2|t| CL \log N}\right)^{-d_N} \le \left|F\left(\frac{\mathbf{r}\cdot\mathbf{a}}{N}\right)\right| \le e^{-U}.$$

Thus,

$$d_N \ge \frac{R}{c_1 \log N} \ge \frac{c_2 AN \log R}{c_1 \log N} \ge 2AN$$

which is a contradiction. □

4. Proof of the Theorem

Let M be the least integer larger than $R/c_2 A \log R$ for which there exists $\mathbf{s} = (s_0, s_1) \in \mathbb{Z}^2$ with $0 \le s_0, s_1 < M \log M$, $(s_0, M) = (s_1, M) = 1$ with $F(\mathbf{s}\cdot\mathbf{a}/M) \neq 0$. Set

$$(\rho, \theta) = \begin{cases} (r, R) & \text{if } M < R \\ (R_1 \log M, 2R_1 \log M) & \text{if } M > R. \end{cases}$$

In Lemma 3, we showed that F vanishes at the points $\mathbf{r}\cdot\mathbf{a}$ (where $0 \le r_0$, $r_1 < N \log N$ and $(r_0, N) = (r_1, N) = 1$) and these are all distinct because of the $\mathbb{Q}$-linear independence of α_0 and α_1. Thus, from Lemma 3, we have constructed

$$\ge \sum \left(\frac{\phi(N)}{N} N \log N\right)^2 \ge c_3 M^3 (\log M)^2$$

zeros of F in $|z| = \rho$. In the above, the sum ranges over

$$\frac{R}{2c_2 A \log R} < N < M.$$

Then,

$$(c_1 L \log M)^{-d_M} \le \left|F\left(\frac{\mathbf{s}\cdot\mathbf{a}}{M}\right)\right| \le \frac{e^S L^2 \theta^L e^{|t|\theta L}}{(\theta/\rho)^{c_3 M^3 (\log M)^2}}$$

and so

$$d_M \geq 2AM \frac{c_3}{2Ac_1} \frac{M^2(\log M)\log(\theta/\rho)}{L} - \frac{1728\mu^2|t|^2 + 2(\log L)/L + \log\theta + |t|\theta}{c_1 \log M}.$$

Suppose first that $M < R$. Then, we have

$$\frac{M^2(\log M)(\log\theta/\rho)}{L} \gg \left(\frac{R}{c_2 A \log R}\right)^2 \frac{(\log R)^2}{L} \gg \frac{R^2}{L} \gg \log L \gg \log M.$$

On the other hand, if $M > R$, we have

$$\frac{M^2(\log M)(\log\theta/\rho)}{L} \gg \frac{R^2 \log M}{L} \gg \log M.$$

Thus, in all cases, we have

$$\frac{M^2(\log M)(\log\theta/\rho)}{L} \gg \log M.$$

Moreover,

$$\frac{1728\mu^2|t|^2 + 2(\log L)/L + \log\theta + |t|\theta}{c_1 \log M} \ll M$$

in all cases. Hence,

$$d_M \gg M \log M$$

and this is a contradiction as by letting $L \to \infty$, we can make $M \to \infty$: the implied constant depends only on μ, t and R_1.

References

[1] F. Gramain, M. Mignotte and M. Waldschmidt, Valeurs algébriques de fonctions analytiques, *Acta Arith.*, **67** (1986) 97–121.

[2] S. Lang, Division points of elliptic curves and Abelian functions over number fields, *Amer. J. Math.*, **97** (1975) 124–132.

[3] M. Ram Murty and P. Rath, Transcendental Numbers, Springer, New York (2014).

[4] M. Waldschmidt, Transcendence et exponentielles en plusieurs variables, *Inventiones Math.*, **63** (1981) 97–127.

Topics in Number Theory, RMS-Lecture Notes Series No. 26, 2020, pp. 175–188.

On Non-Vanishing and Sign Changes of the Fourier Coefficients of Hilbert Cusp Forms

Tarun Dalal and Narasimha Kumar

Department of Mathematics, Indian Institute of Technology Hyderabad, Kandi, Sangareddy 502 285, India.
e-mail: ma17resch11005@iith.ac.in; narasimha.kumar@iith.ac.in

Abstract. In this article, we study (simultaneous) non-vanishing, (simultaneous) sign changes of Fourier coefficients of (two) Hilbert cusp forms, respectively.

Keywords. Hilbert modular forms, Fourier coefficients, sign changes, non-vanishing.

2010 Subject Classification: Primary 11F03, 11F11, 11F30; Secondary 11F41

1. Introduction

The problem of non-vanishing and sign changes of the Fourier coefficients of modular forms over a number field is an active area of research in number theory. For modular forms over $\mathbb{Q}$, there had been extensive study of these problems by several mathematicians (cf. [Mur83, KM14, GKR15]). For modular forms over totally real number fields, a similar study has been initiated recently in [MT14, KK18].

In §2, we shall recall the definition of Hilbert modular forms, their Fourier coefficients, and we will introduce some notations.

In §3, we shall study the simultaneous non-vanishing of Fourier coefficients of distinct primitive forms at powers of prime ideals (cf. Theorem 3.3 in the text). In [GKP], the authors proved that if f and g are two Hecke eigenforms of integral weights with $a_f(n), a_g(n) \in \mathbb{R}$, respectively, then for all but finitely many primes p, the set $\{m \in \mathbb{N} \mid a_f(p^m)a_g(p^m) \neq 0\}$ has positive density. In [KK18, Theorem 3.1], the authors extended this result to Hilbert primitive forms over K, by showing that the set in (3.4) has positive density. In this article, we improve this result by showing that this density is at least $\frac{1}{2}$, when $[K:\mathbb{Q}]$ is odd. In fact, we will show that the density can either be only $\frac{1}{2}$ or 1. The proof of this theorem is completely different from that of Theorem in *loc. cit.*. Our proof depends on a generalization of the lemma [KRW07, Lemma 2.2] or [MM07, Lemma 2.5] to Hilbert modular forms (cf. Proposition 3.1 in the text).

In §4, we shall study the sign change results for Fourier coefficients of primitive forms over K at powers of prime ideals, where $[K:\mathbb{Q}]$ is odd. In Proposition 4.1, for almost all prime ideals $\mathfrak{p}$, we show that the Fourier coefficients at $\mathfrak{p}^r (r \in \mathbb{N})$ change signs infinitely often. In Theorem 4.4, we show that a similar result hold by fixing an exponent and varying over prime ideals.

Let $a_f(n), a_g(n) \in \mathbb{R}$ be the Fourier coefficients of two non-zero cusp forms f, g, respectively, of same level but different non-parallel even weights. In [GKR15, Theorem 1], the authors showed that if $a_f(1)a_g(1) \neq 0$, then $a_f(n)a_g(n)(n \in \mathbb{N})$ change signs infinitely many often. In [KK18, Theorem 3.1], the authors extend this result to Hilbert modular forms. In this article, we have improved the conditions of theorem in *loc. cit.*, so that it can be applied to a broader class of modular forms.

2. Preliminaries

Let F be a totally real number field of degree $n > 1$ and let $\mathcal{O}_F$ denote the integral closure of $\mathbb{Z}$ inside F. In this section, we shall recall the basic definition of Hilbert modular forms over F and it's Fourier coefficients for all integral ideals $\mathfrak{m} \subseteq \mathcal{O}_F$ (for more details, see [Gar90, Fre90]).

Let $k = (k_1, \ldots, k_n) \in \mathbb{N}^n$. For a non-archimedean place $\mathfrak{p}$ of F, let $F_\mathfrak{p}$ denote the completion of F at $\mathfrak{p}$. Let $\mathfrak{D}_F$ denote the absolute different of F. Let $\mathfrak{a}$ and $\mathfrak{b}$ be integral ideals of F, and define a subgroup $K_\mathfrak{p}(\mathfrak{a}, \mathfrak{b})$ of $\mathrm{GL}_2(F_\mathfrak{p})$ as

$$K_\mathfrak{p}(\mathfrak{a}, \mathfrak{b}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(F_\mathfrak{p}) \ : \ \begin{matrix} a \in \mathcal{O}_\mathfrak{p}, & b \in \mathfrak{a}_\mathfrak{p}^{-1}\mathfrak{D}_\mathfrak{p}^{-1}, & \\ c \in \mathfrak{b}_\mathfrak{p}\mathfrak{D}_\mathfrak{p}, & d \in \mathcal{O}_\mathfrak{p}, & |ad - bc|_\mathfrak{p} = 1 \end{matrix} \right\},$$

where the subscript $\mathfrak{p}$ means the $\mathfrak{p}$-parts of given ideals. Furthermore, we put

$$K_0(\mathfrak{a}, \mathfrak{b}) = \mathrm{SO}(2)^n \cdot \prod_{\mathfrak{p}<\infty} K_\mathfrak{p}(\mathfrak{a}, \mathfrak{b}) \quad \text{and} \quad W(\mathfrak{a}, \mathfrak{b}) = \mathrm{GL}_2^+(\mathbb{R})^n K_0(\mathfrak{a}, \mathfrak{b}).$$

In particular, if $\mathfrak{a} = \mathcal{O}_F$, then we simply write $K_\mathfrak{p}(\mathfrak{b}) := K_\mathfrak{p}(\mathcal{O}_F, \mathfrak{b})$, $W(\mathfrak{b}) := W(\mathcal{O}_F, \mathfrak{b})$. Then, we have the following disjoint decomposition of $\mathrm{GL}_2(\mathbb{A}_F)$:

$$\mathrm{GL}_2(\mathbb{A}_F) = \bigcup_{\nu=1}^{h} \mathrm{GL}_2(F) x_\nu^{-\iota} W(\mathfrak{b}), \tag{2.1}$$

where $x_\nu^{-\iota} = \begin{pmatrix} t_\nu^{-1} & \\ & 1 \end{pmatrix}$ with $\{t_\nu\}_{\nu=1}^h$ taken to be a complete set of representatives of the narrow class group of F. We note that such t_ν can be chosen so that the infinity part $t_{\nu,\infty}$ is 1 for all ν. For each ν, we also put

$$\begin{aligned} \Gamma_\nu(\mathfrak{b}) &= \mathrm{GL}_2(F) \cap x_\nu W(\mathfrak{b}) x_\nu^{-1} \\ &= \left\{ \begin{pmatrix} a & t_\nu^{-1} b \\ t_\nu c & d \end{pmatrix} \in \mathrm{GL}_2(F) : \begin{matrix} a \in \mathcal{O}_\mathfrak{p}, & b \in \mathfrak{a}_\mathfrak{p}^{-1}\mathfrak{D}_\mathfrak{p}^{-1}, & \\ c \in \mathfrak{b}_\mathfrak{p}\mathfrak{D}_\mathfrak{p}, & d \in \mathcal{O}_\mathfrak{p}, & |ad - bc|_\mathfrak{p} = 1 \end{matrix} \right\}. \end{aligned}$$

Let ψ be a Hecke character of $\mathbb{A}_F^\times$ whose conductor divides $\mathfrak{b}$ and ψ_∞ is of the form

$$\psi_\infty(x) = \mathrm{sgn}(x_\infty)^k |x_\infty|^{i\mu},$$

with $\mu \in \mathbb{R}^n$ and $\sum_{j=1}^n \mu_j = 0$. We let $M_k(\Gamma_\nu(\mathfrak{b}), \psi_\mathfrak{b}, \mu)$ denote the space of all functions f_ν that are holomorphic on $\mathfrak{h}^n$ and at cusps, satisfying

$$f_\nu ||_k \gamma = \psi_\mathfrak{b}(\gamma) \det \gamma^{i\mu/2} f_\nu$$

for all γ in $\Gamma_\nu(\mathfrak{b})$. We note that such a function f_ν has a Fourier expansion

$$f_\nu(z) = \sum_{\xi \in F} a_\nu(\xi) \exp(2\pi i \xi z)$$

where ξ runs over all the totally positive elements in $t_\nu^{-1}\mathcal{O}_F$ and $\xi = 0$. A Hilbert modular form is a cusp form, if for all $\gamma \in \mathrm{GL}_2^+(F)$, the constant term of $f_\nu||_k\gamma$ in its Fourier expansion is 0, and the space of cusp forms with respect to $\Gamma_\nu(\mathfrak{b})$ is denoted by $S_k(\Gamma_\nu(\mathfrak{b}), \psi_\mathfrak{b}, \mu)$.

Now, put $\mathbf{f} := (f_1, \ldots, f_h)$ where f_ν belongs $M_k(\Gamma_\nu(\mathfrak{b}), \psi_\mathfrak{b}, \mu)$ for each ν, and define $\mathbf{f}$ to be a function on $\mathrm{GL}_2(\mathbb{A}_F)$ as

$$\mathbf{f}(g) = \mathbf{f}(\gamma x_\nu^{-\iota} w) := \psi_\mathfrak{b}(w^\iota) \det w_\infty^{i\mu/2} (f_\nu||_k w_\infty)(\boldsymbol{i})$$

where $\gamma x_\nu^{-\iota} w \in \mathrm{GL}_2(F) x_\nu^{-\iota} W(\mathfrak{b})$ as in (2.1), and $w^\iota := \omega_0({}^t w)\omega_0^{-1}$ with $\omega_0 = \begin{pmatrix} & 1 \\ -1 & \end{pmatrix}$. The $\mathbb{C}$-vector space generated by such $\mathbf{f}$ is denoted as $M_k(\psi_\mathfrak{b}, \mu) = \prod_\nu M_k(\Gamma_\nu(\mathfrak{b}), \psi_\mathfrak{b}, \mu)$. Furthermore, the space consisting of all $\mathbf{f} = (f_1, \ldots, f_h) \in M_k(\psi_\mathfrak{b}, \mu)$ satisfying

$$\mathbf{f}(sg) = \psi(s)\mathbf{f}(g) \quad \text{for any} \quad s \in \mathbb{A}_F^\times \quad \text{and} \quad x \in \mathrm{GL}_2(\mathbb{A}_F)$$

is denoted as $M_k(\mathfrak{b}, \psi)$. If $f_\nu \in S_k(\Gamma_\nu(\mathfrak{b}), \psi_\mathfrak{b}, \mu)$ for each ν, then the $\mathbb{C}$-vector space of such $\mathbf{f}$ is denoted by $S_k(\mathfrak{b}, \psi)$.

Let $\mathfrak{m}$ be an integral ideal of F and write $\mathfrak{m} = \xi t_\nu^{-1}\mathcal{O}_F$ with a totally positive element ξ in F. Then, we define the Fourier coefficients of $\mathbf{f}$ as

$$C(\mathfrak{m}, \mathbf{f}) := \begin{cases} N(\mathfrak{m})^{\frac{k_0}{2}} a_\nu(\xi)\xi^{-(k+i\mu)/2} & \text{if} \quad \mathfrak{m} = \xi t_\nu^{-1}\mathcal{O}_F \subset \mathcal{O}_F \\ 0 & \text{if} \quad \mathfrak{m} \text{ is not integral} \end{cases} \tag{2.2}$$

where $k_0 = \max\{k_1, \ldots, k_n\}$.

We let F (resp., K) to denote a totally real number field (resp., of odd degree). Let $\mathbf{P}$ (resp., $\mathbb{P}$) denote the set of all prime ideals of $\mathcal{O}_F$ (resp., odd inertia degree). We shall use the same notations $\mathbf{P}$ (resp., $\mathbb{P}$) for prime ideals (resp., odd inertia degree) of $\mathcal{O}_K$ as well and it shall be clear from the context. Throughout this article, by a primitive form $\mathbf{f}$ over F of level $\mathfrak{b}$, with character χ and weight k, we mean $\mathbf{f}$ is a normalized Hilbert Hecke eigenform in $S_k^{\mathrm{new}}(\mathfrak{b}, \chi)$ (cf. for the theory of new forms, please refer to [Shi78]).

Observe that, by ramification theory, for any prime $p \in \mathbb{Z}$, there exists a prime ideal $\mathfrak{p} \subseteq \mathcal{O}_K$ over p with odd inertia degree. Furthermore, if K is Galois, then every prime ideal of $\mathcal{O}_K$ has odd inertia degree.

2.1 *Sato-Tate equi-distribution theorem*

In this section, we shall state the Sato-Tate equi-distribution theorem for non-CM primitive forms $\mathbf{f}$ (cf. [KKT18, Theorem 3.3] which is a re-formulation of [BGG11, Corollary 7.17] for $\mathbf{f}$) in a way that shall be useful in our context.

Let $\mathbf{f}$ be a primitive form over F of level $\mathfrak{c}$, with trivial character and weight $2k$. For any ideal $\mathfrak{a} \subseteq \mathcal{O}_F$, define $\beta(\mathfrak{a}, \mathbf{f}) := \frac{C(\mathfrak{a},\mathbf{f})}{N(\mathfrak{a})^{\frac{2k_0-1}{2}}}$. By Deligne's bound for $\mathbf{f}$, for any prime ideal $\mathfrak{p} \nmid \mathfrak{c}\mathfrak{D}_F$, we have $\beta(\mathfrak{p}, \mathbf{f}) \in [-2, 2]$. Hence, we can write

$$\beta(\mathfrak{p}, \mathbf{f}) = 2\cos\theta_{\mathfrak{p}}(\mathbf{f}), \tag{2.3}$$

for some $\theta_{\mathfrak{p}}(\mathbf{f}) \in [0, \pi]$. Now, we shall recall the Sato-Tate equi-distribution theorem of Barnet-Lamb, Gee, and Geraghty ([BGG11, Corollary 7.17]).

Theorem 2.1. *Let* $\mathbf{f}$ *be a non-CM primitive form over* F *of level* $\mathfrak{c}$*, with trivial character and weight* $2k$*. Then* $\{\theta_{\mathfrak{p}}(\mathbf{f})\}_{\mathfrak{p}\in\mathbf{P},\mathfrak{p}\nmid\mathfrak{c}\mathfrak{D}_F}$ *is equi-distributed in* $[0, \pi]$ *with respect to* $\mu_{\mathrm{ST}} = \frac{2}{\pi}\sin^2\theta d\theta$*. In other words, for any sub-interval* $I \subseteq [0, \pi]$*, we have*

$$\lim_{x\to\infty} \frac{\#\{\mathfrak{p} \in \mathbf{P} \mid \mathfrak{p} \nmid \mathfrak{c}\mathfrak{D}_F, N(\mathfrak{p}) \leq x, \theta_{\mathfrak{p}}(\mathbf{f}) \in I\}}{\#\{\mathfrak{p} \in \mathbf{P} \mid N(\mathfrak{p}) \leq x\}} = \mu_{\mathrm{ST}}(I) = \frac{2}{\pi}\int_I \sin^2\theta d\theta \tag{2.4}$$

i.e., the natural density of $S = \{\mathfrak{p} \in \mathbf{P} \mid \mathfrak{p} \nmid \mathfrak{c}\mathfrak{D}_F, \theta_{\mathfrak{p}}(\mathbf{f}) \in I\}$ *is* $\mu_{\mathrm{ST}}(I)$*.*

3. Non-vanishing of Fourier coefficients at prime powers

In this section, we shall prove a result concerning the simultaneous non-vanishing of Fourier coefficients of primitive forms at prime powers. Before proving this result, we prove an important proposition, which is a generalization of [KRW07, Lemma 2.2] or [MM07, Lemma 2.5] to K.

Recall that K is totally real number field of odd degree and $\mathbb{P}$ denote the set of all prime ideals of $\mathcal{O}_K$ with odd inertia degree. The following proposition holds only for primes of $\mathbb{P}$. This is because for primes of $\mathbf{P}\backslash\mathbb{P}$, in the below proof, (3.2) does not imply (3.3). In that case, we may not be able to say that the number of such primes are finite. This is main reason for working over K instead over F.

Proposition 3.1. *Let* $\mathbf{f}$ *be a primitive form over* K *of level* $\mathfrak{c}$*, with character* χ *and weight* $2k$*. Then there exists an integer* $M_{\mathbf{f}} \geq 1$ *with* $N(\mathfrak{c}) \mid M_{\mathbf{f}}$ *such that for any prime* $p \nmid M_{\mathbf{f}}$ *and for any prime ideal* $\mathfrak{p} \in \mathbb{P}$ *over* p*, we have either* $C(\mathfrak{p}, \mathbf{f}) = 0$ *or* $C(\mathfrak{p}^r, \mathbf{f}) \neq 0$ *for all* $r \geq 1$*.*

Proof. Let p be a prime number such that $p \nmid N(\mathfrak{c})$. Let $\mathfrak{p} \in \mathbb{P}$ be a prime ideal of $\mathcal{O}_K$ over p and $\mathfrak{p} \nmid \mathfrak{c}$. If $C(\mathfrak{p}, \mathbf{f}) = 0$, then there is nothing prove. If $C(\mathfrak{p}, \mathbf{f}) \neq 0$, then we need to show that $C(\mathfrak{p}^r, \mathbf{f}) \neq 0$ for all $r \geq 2$, except for finitely many prime ideals $\mathfrak{p} \in \mathbb{P}$.

Suppose that $C(\mathfrak{p}, \mathbf{f}) \neq 0$ but $C(\mathfrak{p}^r, \mathbf{f}) = 0$ for some $r \geq 2$. Since $\mathbf{f}$ is a primitive form, then by Hecke relations, we have

$$C(\mathfrak{p}^{m+1}, \mathbf{f}) = C(\mathfrak{p}, \mathbf{f})C(\mathfrak{p}^m, \mathbf{f}) - \chi(\mathfrak{p})N(\mathfrak{p})^{2k_0-1}C(\mathfrak{p}^{m-1}, \mathbf{f}).$$

These relations can be re-interpreted as

$$\sum_{r=0}^{\infty} C(\mathfrak{p}^r, \mathbf{f})X^r = \frac{1}{1 - C(\mathfrak{p}, \mathbf{f})X + \chi(\mathfrak{p})N(\mathfrak{p})^{2k_0-1}X^2}. \tag{3.1}$$

Suppose that

$$1 - C(\mathfrak{p}, \mathbf{f})X + \chi(\mathfrak{p})N(\mathfrak{p})^{2k_0-1}X^2 = (1 - \alpha(\mathfrak{p})X)(1 - \beta(\mathfrak{p})X).$$

By comparing the coefficients, we get that

$$\alpha(\mathfrak{p}) + \beta(\mathfrak{p}) = C(\mathfrak{p}, \mathbf{f}) \quad \text{and} \quad \alpha(\mathfrak{p})\beta(\mathfrak{p}) = \chi(\mathfrak{p})N(\mathfrak{p})^{2k_0-1} \neq 0,$$

since $\mathfrak{p} \nmid \mathfrak{c}$ and hence $\chi(\mathfrak{p}) \neq 0$. If $\alpha(\mathfrak{p}) = \beta(\mathfrak{p})$, then

$$C(\mathfrak{p}^r, \mathbf{f}) = (r+1)\alpha(\mathfrak{p})^r \neq 0,$$

which cannot happen for any $r \geq 2$. So, $\alpha(\mathfrak{p})$ cannot be equal to $\beta(\mathfrak{p})$. Then by induction, for any $r \geq 2$, we have the following

$$C(\mathfrak{p}^r, \mathbf{f}) = \frac{\alpha(\mathfrak{p})^{r+1} - \beta(\mathfrak{p})^{r+1}}{\alpha(\mathfrak{p}) - \beta(\mathfrak{p})}.$$

In this case, we have

$$C(\mathfrak{p}^r, \mathbf{f}) = 0 \text{ if and only if } \left(\frac{\alpha(\mathfrak{p})}{\beta(\mathfrak{p})}\right)^{r+1} = 1,$$

which implies that the ratio $\frac{\alpha(\mathfrak{p})}{\beta(\mathfrak{p})}$ is a root of unity. Since $C(\mathfrak{p}, \mathbf{f}) \neq 0$, we get that $\alpha(\mathfrak{p}) = \zeta\beta(\mathfrak{p})$ where ζ is a root of unity and $\zeta \neq -1$. By the product relation, we get that $\alpha(\mathfrak{p})^2 = \zeta\chi(\mathfrak{p})N(\mathfrak{p})^{2k_0-1}$, hence $\alpha(\mathfrak{p}) = \pm\gamma N(\mathfrak{p})^{(2k_0-1)/2}$, where $\gamma^2 = \zeta\chi(\mathfrak{p})$. Therefore,

$$C(\mathfrak{p}, \mathbf{f}) = (1 + \zeta^{-1})\alpha(\mathfrak{p}) = \pm\gamma(1 + \zeta^{-1})N(\mathfrak{p})^{(2k_0-1)/2} \neq 0.$$

In particular, $\mathbb{Q}(\gamma(1+\zeta^{-1})N(\mathfrak{p})^{\frac{2k_0-1}{2}}) \subseteq \mathbb{Q}(\mathbf{f})$, where $\mathbb{Q}(\mathbf{f})$ is the field generated by $\{C(\mathfrak{m}, \mathbf{f})\}_{\mathfrak{m} \subseteq \mathcal{O}_K}$ and by the values of the character χ. Since $\mathfrak{p} \in \mathbb{P}$, $N(\mathfrak{p}) = p^f$, where $f \in \mathbb{N}$ odd. Hence, we have

$$\mathbb{Q}(\gamma(1+\zeta^{-1})p^{\frac{f(2k_0-1)}{2}}) \subseteq \mathbb{Q}(\mathbf{f}). \tag{3.2}$$

Since $2k_0 - 1$, f are odd, we have that

$$\mathbb{Q}(\gamma(1+\zeta^{-1})\sqrt{p}) \subseteq \mathbb{Q}(\mathbf{f}). \tag{3.3}$$

By [Shi78, Proposition 2.8], the field $\mathbb{Q}(\mathbf{f})$ is a number field. Hence, the number of such primes p are finite. Take $M_{\mathbf{f}}$ to be the product of all such primes p and $N(\mathfrak{c})$. Thus, for any prime $p \nmid M_{\mathbf{f}}$ and for any prime ideal $\mathfrak{p} \in \mathbb{P}$ over p, we have either $C(\mathfrak{p}, \mathbf{f}) = 0$ or $C(\mathfrak{p}^r, \mathbf{f}) \neq 0$ for all $r \geq 1$. □

If K is Galois over $\mathbb{Q}$, then the above proposition can be re-stated as:

Lemma 3.2. *Let* $\mathbf{f}$ *be as in Proposition 3.1. If* K *is Galois over* $\mathbb{Q}$*, then there exists an integer* $M_{\mathbf{f}} \geq 1$ *with* $N(\mathfrak{c}) \mid M_{\mathbf{f}}$ *such that for any prime* $p \nmid M_{\mathbf{f}}$ *and for any prime ideal* $\mathfrak{p} \in \mathbf{P}$ *over* p*, we have either* $C(\mathfrak{p}, \mathbf{f}) = 0$ *or* $C(\mathfrak{p}^r, \mathbf{f}) \neq 0$ *for all* $r \geq 1$.

Now, we are in a position to state our main result of this section, which improves the result [KK18, Theorem 3.2]. Let $k = (k_1, \ldots, k_n) \in \mathbb{N}^n$ and $l = (l_1, \ldots, l_n) \in \mathbb{N}^n$.

Theorem 3.3. *Let* $\mathbf{f}$ *and* $\mathbf{g}$ *be two primitive forms over* K *and of levels* $\mathfrak{c}_1, \mathfrak{c}_2$*, with characters* χ_1 and χ_2 *and weights* $2k, 2l$*, respectively. For any prime* $p \nmid M_{\mathbf{f}} M_{\mathbf{g}}$*, for any prime ideal* $\mathfrak{p} \in \mathbb{P}$ *over* p*, the set*

$$A_{\mathfrak{p}} := \{m \in \mathbb{N} | C(\mathfrak{p}^m, \mathbf{f}) C(\mathfrak{p}^m, \mathbf{g}) \neq 0\} \tag{3.4}$$

contains $2\mathbb{N}$*, where* $M_{\mathbf{f}}$ *and* $M_{\mathbf{g}}$ *are as in Proposition 3.1 for* $\mathbf{f}, \mathbf{g}$*, respectively. Moreover, the natural density of the set* $A_{\mathfrak{p}}$ *is either* $\frac{1}{2}$ *or* 1.

Proof. For any prime $p \nmid M_{\mathbf{f}} M_{\mathbf{g}}$, let $\mathfrak{p} \in \mathbb{P}$ be a prime ideal over p. If $C(\mathfrak{p}, \mathbf{f}) C(\mathfrak{p}, \mathbf{g}) \neq 0$, then by Proposition 3.1, we have that

$$\{m \in \mathbb{N} | C(\mathfrak{p}^m, \mathbf{f}) C(\mathfrak{p}^m, \mathbf{g}) \neq 0\} = \mathbb{N}.$$

In this case, the natural density of $A_{\mathfrak{p}}$ is 1.

Suppose at least one of $C(\mathfrak{p}, \mathbf{f})$ or $C(\mathfrak{p}, \mathbf{g})$ is zero, say $C(\mathfrak{p}, \mathbf{f}) = 0$. By the Hecke relations for the primitive form $\mathbf{f}$

$$C(\mathfrak{p}^m, \mathbf{f}) = -\chi_1(\mathfrak{p}) N(\mathfrak{p})^{2k_0 - 1} C(\mathfrak{p}^{m-2}, \mathbf{f}), \tag{3.5}$$

where $\chi_1(\mathfrak{p}) \neq 0$, since $\mathfrak{p} \nmid \mathfrak{c}_1$. Hence, we see that the vanishing or non-vanishing of $C(\mathfrak{p}^m, \mathbf{f})$ depends only on $m \pmod 2$. Therefore, $C(\mathfrak{p}^{2m+1}, \mathbf{f}) = 0$ (resp., $C(\mathfrak{p}^{2m}, \mathbf{f}) \neq 0$) as $C(\mathfrak{p}, \mathbf{f}) = 0$ (resp., $C(\mathfrak{p}^2, \mathbf{f}) \neq 0$) for all $m \geq 1$. Hence, we have that

$$\{m \in \mathbb{N} \mid C(\mathfrak{p}^m, \mathbf{f}) \neq 0\} = 2\mathbb{N}.$$

Arguing similarly for the primitive form $\mathbf{g}$, we see that the set $\{m \in \mathbb{N} | C(\mathfrak{p}^m, \mathbf{g}) \neq 0\}$ is either $\mathbb{N}$ or $2\mathbb{N}$ depends on whether $C(\mathfrak{p}, \mathbf{g}) \neq 0$ or $C(\mathfrak{p}, \mathbf{g}) = 0$, respectively. So any of these cases, we get that

$$\{m \in \mathbb{N} | C(\mathfrak{p}^m, \mathbf{f}) C(\mathfrak{p}^m, \mathbf{g}) \neq 0\} = 2\mathbb{N}.$$

In this case, the natural density of $A_{\mathfrak{p}}$ is $\frac{1}{2}$. This proves the Theorem. □

In the following proposition, we answer how often the set $A_{\mathfrak{p}}$ is $\mathbb{N}$, when $\mathfrak{p}$ varies over $\mathbb{P}$.

Proposition 3.4. *Let* $\mathbf{f}$ *and* $\mathbf{g}$ *be same as in Theorem 3.3. If* $\mathbf{f}, \mathbf{g}$ *are non-CM eigenforms, then there exists a set* $S \subseteq \mathbb{P}$ *with natural density is* 0 *such that*

$$A_{\mathfrak{p}} = \{m \in \mathbb{N} \mid C(\mathfrak{p}^m, \mathbf{f}) C(\mathfrak{p}^m, \mathbf{g}) \neq 0\} = \mathbb{N} \tag{3.6}$$

for all prime ideals $\mathfrak{p} \in \mathbb{P}$ *outside of* S.

Proof. Define the set $S' = \{\mathfrak{p} \in \mathbb{P} \mid C(\mathfrak{p}, \mathbf{f}) C(\mathfrak{p}, \mathbf{g}) = 0\}$. Clearly, we have

$$\{\mathfrak{p} \in \mathbb{P} \mid C(\mathfrak{p}, \mathbf{f}) = 0\} \subseteq S' \subseteq \{\mathfrak{p} \in \mathbb{P} \mid C(\mathfrak{p}, \mathbf{f}) = 0\} \cup \{\mathfrak{p} \in \mathbb{P} \mid C(\mathfrak{p}, \mathbf{g}) = 0\}.$$

By Theorem 2.1, the natural density of $\{\mathfrak{p} \in \mathbf{P} \mid C(\mathfrak{p}, \mathbf{f}) = 0\}$ is 0 and hence the natural density of $\{\mathfrak{p} \in \mathbb{P} \mid C(\mathfrak{p}, \mathbf{f}) = 0\}$ is 0. Similarly, for the eigenform $\mathbf{g}$ as well. Hence, the natural density of S' is 0. Therefore, the natural density of the set $S = S' \cup \{\mathfrak{p} \in \mathbb{P} \mid \mathfrak{p} \mid p \text{ and } p \mid M_{\mathbf{f}} M_{\mathbf{g}}\}$ is 0. For any $\mathfrak{p} \notin S$, by Lemma 3.1, we have $C(\mathfrak{p}^m, \mathbf{f})C(\mathfrak{p}^m, \mathbf{g}) \neq 0$ for all $m \geq 1$. □

We remark that if we assume K is Galois in the above result, then (3.6) holds for density 1 set of primes in $\mathbf{P}$ (because, in this case $\mathbb{P} = \mathbf{P}$).

4. Sign changes of Hilbert modular forms

In this section, we shall study the sign change results for the Fourier coefficients of primitive forms, and later we study the simultaneous sign changes for the Fourier coefficients of two non-zero Hilbert modular forms of different integral weights.

4.1 *Sign changes*

In [MT14, Theorem 1.1], the authors show that a non-zero Hilbert cusp form with real Fourier coefficients change signs infinitely often. In the next proposition, for primitive forms, we show that for almost all the primes $\mathfrak{p} \in \mathbb{P}$, the Fourier coefficients $\{C(\mathfrak{p}^r, \mathbf{f})\}_{r \in \mathbb{N}}$ change signs infinitely often.

Proposition 4.1. *Let* $\mathbf{f}$ *be a primitive form over* K *of level* $\mathfrak{c}$*, trivial character and weight* $2k$*. Then, for all but finitely many* $\mathfrak{p} \in \mathbb{P}$*, the Fourier coefficients* $\{C(\mathfrak{p}^r, \mathbf{f})\}_{r \in \mathbb{N}}$ *change signs infinitely often.*

Proof. Let $\mathfrak{p} \in \mathbb{P}$ be a prime ideal such that $C(\mathfrak{p}^r, \mathbf{f}) \geq 0$ for all $r \gg 0$ (a similar argument holds in the other case as well). Since $\mathbf{f}$ is primitive, by Hecke relations, we have

$$\sum_{r=0}^{\infty} C(\mathfrak{p}^r, \mathbf{f}) X^r = (1 - \alpha(\mathfrak{p})X)^{-1}(1 - \beta(\mathfrak{p})X)^{-1}, \tag{4.1}$$

where

$$1 - C(\mathfrak{p}, \mathbf{f})X + N(\mathfrak{p})^{2k_0 - 1}X^2 = (1 - \alpha(\mathfrak{p})X)(1 - \beta(\mathfrak{p})X).$$

Comparing the coefficients we have

$$\alpha(\mathfrak{p}) + \beta(\mathfrak{p}) = C(\mathfrak{p}, \mathbf{f}) \text{ and } \alpha(\mathfrak{p})\beta(\mathfrak{p}) = N(\mathfrak{p})^{2k_0 - 1},$$

where

$$\alpha(\mathfrak{p}), \beta(\mathfrak{p}) = \frac{C(\mathfrak{p}, \mathbf{f}) \pm \sqrt{C(\mathfrak{p}, \mathbf{f})^2 - 4N(\mathfrak{p})^{2k_0 - 1}}}{2}. \tag{4.2}$$

For $s \in \mathbb{C}$, replacing X by $N(\mathfrak{p})^{-s}$ in (4.1), we get that

$$\sum_{r=0}^{\infty} C(\mathfrak{p}^r, \mathbf{f}) N(\mathfrak{p})^{-sr} = (1 - \alpha(\mathfrak{p})N(\mathfrak{p})^{-s})^{-1}(1 - \beta(\mathfrak{p})N(\mathfrak{p})^{-s})^{-1}. \tag{4.3}$$

The above Dirichlet series converges for $\mathrm{Re}(s) \gg 0$ and the coefficients are non-negative except for finitely many terms. By Landau's theorem for Dirichlet series with non-negative terms, we get the series (4.3) is either converges everywhere or it has a singularity at the real point of its abscissa of convergence. The series has a pole at $s \in \mathbb{C}$ for which $N(\mathfrak{p})^s = \alpha(\mathfrak{p})$ or $N(\mathfrak{p})^s = \beta(\mathfrak{p})$ holds, hence the first case is not possible. Then the only possibility is that the series has a singularity at the real point of its abscissa of convergence. In particular, one of (and hence both of) $\alpha(\mathfrak{p})$ or $\beta(\mathfrak{p})$ must be real. Hence, we get that $C(\mathfrak{p}, \mathbf{f})^2 \geq 4N(\mathfrak{p})^{2k_0-1}$. However, by Deligne's bound for $\mathbf{f}$, we have

$$C(\mathfrak{p}, \mathbf{f})^2 \leq 4N(\mathfrak{p})^{2k_0-1}. \tag{4.4}$$

Therefore,

$$C(\mathfrak{p}, \mathbf{f}) = \pm 2N(\mathfrak{p})^{\frac{2k_0-1}{2}} \in \mathbb{Q}(\mathbf{f}). \tag{4.5}$$

Since $\mathfrak{p} \in \mathbb{P}$, by (4.5), we get $\sqrt{p} \in \mathbb{Q}(\mathbf{f})$, which can only happen for finitely many primes p. This proves the proposition. □

In [KM14], Kohnen and Martin remarked that the sign change results for the Fourier coefficients can also be proved by using sign changes of $\sin(\theta)$. We elaborate this remark and reprove the above result. For this, we need to recall the following lemma (cf. by [KK18, Proposition 5.1] for a proof).

Lemma 4.2. *Let* $\mathbf{f}$ *be a primitive form over* F *of level* $\mathfrak{c}$, *with trivial character and weight* $2k$. *For any prime ideal* $\mathfrak{p} \nmid \mathfrak{c}\mathfrak{D}_F$, *let* $\theta_{\mathfrak{p}}(\mathbf{f}) \in [0, \pi]$ *be defined as in* (2.3). *Then, for any* $m \geq 1$, *we have*

$$\beta(\mathfrak{p}^m, \mathbf{f}) = \begin{cases} (-1)^m(m+1) & \text{if } \theta_{\mathfrak{p}}(\mathbf{f}) = \pi, \\ m+1 & \text{if } \theta_{\mathfrak{p}}(\mathbf{f}) = 0, \\ \frac{\sin((m+1)\theta_{\mathfrak{p}}(\mathbf{f}))}{\sin\theta_{\mathfrak{p}}(\mathbf{f})} & \text{if } 0 < \theta_{\mathfrak{p}}(\mathbf{f}) < \pi. \end{cases} \tag{4.6}$$

Now, we shall give another proof of Proposition 4.1.

Proof. For any $\mathfrak{p} \in \mathbb{P}$, if $\theta_{\mathfrak{p}}(\mathbf{f}) = 0$ or π, then $C(\mathfrak{p}, \mathbf{f}) = \pm 2N(\mathfrak{p})^{\frac{2k_0-1}{2}} \in \mathbb{Q}(\mathbf{f})$, which can happen only for finitely many $\mathfrak{p} \in \mathbb{P}$. So, without loss of generality, we can assume that $0 < \theta_{\mathfrak{p}}(\mathbf{f}) < \pi$, hence $\sin(\theta_{\mathfrak{p}}(\mathbf{f})) > 0$. By (4.6), we have

$$C(\mathfrak{p}^m, \mathbf{f}) \gtrless 0 \iff \sin 2\pi(m+1)\frac{\theta_{\mathfrak{p}}(\mathbf{f})}{2\pi} \gtrless 0.$$

Let $x = \frac{\theta_{\mathfrak{p}}(\mathbf{f})}{2\pi}$. For any $j \in \mathbb{N}$, the lengths of the intervals $\left(\frac{2j}{2x}, \frac{(2j+1)}{2x}\right)$ and $\left(\frac{(2j-1)}{2x}, \frac{2j}{2x}\right)$ are bigger than 1, as $\frac{1}{2x} > 1$. Hence, there exists $n_j, m_j \in \mathbb{Z}$ such that $n_j + 1 \in \left(\frac{2j}{2x}, \frac{2j+1}{2x}\right)$ and $m_j + 1 \in \left(\frac{2j-1}{2x}, \frac{2j}{2x}\right)$. Therefore, we have $\sin\left((n_j+1)\theta_{\mathfrak{p}}(\mathbf{f})\right) > 0$ and $\sin((m_j+1)\theta_{\mathfrak{p}}(\mathbf{f})) < 0$. This completes the proof. □

In the above proposition, for a prime $\mathfrak{p} \in \mathbb{P}$, we have studied the sign changes for $\{C(\mathfrak{p}^r, \mathbf{f})\}_{r \in \mathbb{N}}$. Now, for a fixed $r \in \mathbb{N}$, we are interested in studying the sign changes for $\{C(\mathfrak{p}^r, \mathbf{f})\}_{\mathfrak{p} \in \mathbf{P}}$.

For primitive forms over $\mathbb{Q}$, this question has been studied in [MKV18, Theorem 1.1]. In fact, they have computed the natural densities of these sets depending on r is even or odd. In this next theorem, we shall show that a similar result holds for primitive forms over F, essentially by following the same approach. So, we shall state the theorem and sketch a proof of it. To state it, we shall need the notion of natural density for a subset of prime ideals.

Definition 4.3. *Let F be a number field and $S \subseteq \mathbf{P}$ be a subset of prime ideals of $\mathcal{O}_F$. The natural density of S defined as*

$$d(S) = \lim_{x\to\infty} \frac{\#\{\mathfrak{p} \in S \mid (\mathfrak{p}) \leq x\}}{\#\{\mathfrak{p} \in \mathbf{P} \mid (\mathfrak{p}) \leq x\}},$$

if the limit exists.

Theorem 4.4. *Let $\mathbf{f}$ be a non-CM primitive form over F of level $\mathfrak{c}$, with trivial character and weight $2k$. For any $m \geq 1$, we define*

$$\mathbf{P}(m)_{\gtrless 0} = \{\mathfrak{p} \in \mathbf{P} \mid \mathfrak{p} \nmid \mathfrak{c}\mathfrak{D}_F, C(\mathfrak{p}^m, \mathbf{f}) \gtrless 0\}.$$

(1) If $m \equiv 1 \pmod 2$, then

$$d(\mathbf{P}(m)_{>0}) = d(\mathbf{P}(m)_{<0}) = \frac{1}{2}.$$

(2) If $m \equiv 0 \pmod 2$, then

$$d(\mathbf{P}(m)_{>0}) = \frac{m+2}{2(m+1)} - \frac{1}{2\pi}\tan\left(\frac{\pi}{m+1}\right), \text{ and}$$

$$d(\mathbf{P}(m)_{<0}) = \frac{m}{2(m+1)} + \frac{1}{2\pi}\tan\left(\frac{\pi}{m+1}\right).$$

In particular, then for any $m \in \mathbb{N}$, the sequence $\{C(\mathfrak{p}^m, \mathbf{f})\}_{\mathfrak{p}\in\mathbf{P}}$ changes sign infinitely often.

Proof. By Theorem 2.1, the natural density of $T = \{\mathfrak{p} \in \mathbf{P} \mid \theta_{\mathfrak{p}}(\mathbf{f}) = 0, \pi\} \cup \{\mathfrak{p} \in \mathbf{P} \mid \mathfrak{p} \mid \mathfrak{c}\mathfrak{D}_F\}$ is zero. By (4.6), we have the following equality

$$\mathbf{P}(m)_{\gtrless 0} = \{\mathfrak{p} \in \mathbf{P} \mid \mathfrak{p} \notin T, \sin((m+1)\theta_{\mathfrak{p}}(\mathbf{f})) \gtrless 0\}.$$

If $m \equiv 0 \pmod 2$, then

$$\sin((m+1)\theta_{\mathfrak{p}}(\mathbf{f})) > 0 \Leftrightarrow \theta_{\mathfrak{p}}(\mathbf{f}) \in S := \bigcup_{j=0}^{\frac{m}{2}} \left(\frac{2j\pi}{m+1}, \frac{(2j+1)\pi}{m+1}\right),$$

and

$$\sin((m+1)\theta_{\mathfrak{p}}(\mathbf{f})) < 0 \Leftrightarrow \theta_{\mathfrak{p}}(\mathbf{f}) \in \bigcup_{j=1}^{\frac{m}{2}} \left(\frac{(2j-1)\pi}{m+1}, \frac{2j\pi}{m+1}\right).$$

By Theorem 2.1, the density of $\mathbf{P}(m)_{>0}$ exists and $d(\mathbf{P}(m)_{>0}) = \mu_{\mathrm{ST}}(S)$, where $\mu_{\mathrm{ST}}(S) = \frac{2}{\pi}\int_S \sin^2 t dt$. The explicit calculation of $\mu_{\mathrm{ST}}(S)$ is exactly the same as that of [MKV18, Theorem 1.1]. Again by Theorem 2.1, we see that the natural density of $\{\mathfrak{p} \in \mathbf{P} \mid \mathfrak{p} \nmid \mathfrak{c}\mathfrak{D}_F, C(\mathfrak{p}^m, \mathbf{f}) = 0\}$ is 0, hence we have

$$d(\mathbf{P}(m)_{<0}) = 1 - d(\mathbf{P}(m)_{>0}).$$

In the case of $m \equiv 1 \pmod 2$, a similar calculation in *loc.cit.* works as well. □

4.2 *Simultaneous sign changes*

In [KK18, Theorem 3.1], the authors proved that, if $C(\mathcal{O}_F, \mathbf{f})C(\mathcal{O}_F, \mathbf{g}) \neq 0$, then there exists infinitely many integral ideals such that the product of the Fourier coefficients of $\mathbf{f}$ and $\mathbf{g}$ is positive (resp., negative). Now, we shall state the main theorem of this section.

Theorem 4.5. *Let* $\mathbf{f}$ *and* $\mathbf{g}$ *be non-zero Hilbert cusp forms over* F *of level* $\mathfrak{c}$*, trivial character and different non-parallel even weights k, l, respectively. For each ideal* $\mathfrak{m} \subseteq \mathcal{O}_F$*, we assume that* $C(\mathfrak{m}, \mathbf{f})$ *and* $C(\mathfrak{m}, \mathbf{g})$ *are real numbers. Suppose that for every ideal* $\mathfrak{n} \subseteq \mathcal{O}_F$*, there exists an ideal* $\mathfrak{r} \subseteq \mathcal{O}_F$ *such that* $(\mathfrak{n}, \mathfrak{r}) = 1$ *such that* $C(\mathfrak{r}, \mathbf{f})C(\mathfrak{r}, \mathbf{g}) \neq 0$*. Then there exist infinitely many ideals* $\mathfrak{m} \subseteq \mathcal{O}_F$ *such that* $C(\mathfrak{m}, \mathbf{f})C(\mathfrak{m}, \mathbf{g}) > 0$ *and infinitely many ideals* $\mathfrak{m} \subseteq \mathcal{O}_F$ *such that* $C(\mathfrak{m}, \mathbf{f})$ $C(\mathfrak{m}, \mathbf{g}) < 0$*.*

Remark 4.6. In the above theorem, the condition of simultaneous non-vanishing of Fourier coefficients is required only to ensure that the L-function in (4.9) is non-zero, otherwise there is no other reason for this assumption.

The main idea in the proof of Theorem 4.5 comes from [KM18, Theorem 1.5], which mainly uses the following theorem of Pribitkin [Pri08].

Theorem 4.7. *Let* $F(s) = \sum_{n=1}^{\infty} a_n e^{-s\lambda_n}$ *be a non-trivial general Dirichlet series which converges somewhere, where the sequence* $\{a_n\}_{n=1}^{\infty}$ *is complex and the exponent sequence* $\{\lambda_n\}_{n=1}^{\infty}$ *is real and strictly increasing to* ∞*. If the function F is holomorphic on the whole real line and has infinitely many real zeros, then there exist infinitely many* $n \in \mathbb{N}$ *such that* $a_n > 0$ *(resp.,* $a_n < 0$*).*

Before we proceed to prove Theorem 4.5, we need the following propositions to construct new Hilbert modular forms out of the existing modular form with some prescribed vanishing of Fourier coefficients at certain ideals. We recall the following proposition, which is a melange of [Shi78, Proposition 2.3] and [Pan91, Page 124].

Proposition 4.8. *For any integral ideal* $\mathfrak{q} \subseteq \mathcal{O}_F$ *and every* $\mathbf{f} \in M_k(\mathfrak{c}, \psi)$*, there exists a unique element* $\mathbf{f}|\mathfrak{q}$ *of* $M_k(\mathfrak{q}\mathfrak{c}, \psi)$ *such that*

$$C(\mathfrak{m}, \mathbf{f}|\mathfrak{q}) = C(\mathfrak{q}^{-1}\mathfrak{m}, \mathbf{f}),$$

and there exists an unique element $\mathbf{f}|U(\mathfrak{q})$ *of* $M_k(\mathfrak{q}\mathfrak{c}, \psi)$ *such that*

$$C(\mathfrak{m}, \mathbf{f}|U(\mathfrak{q})) = C(\mathfrak{q}\mathfrak{m}, \mathbf{f}).$$

We now recall the prove the following important proposition (cf. [KK18, Proposition 4.5] for a proof).

Proposition 4.9. *Let* $\mathbf{f} \in S_k(\mathfrak{c}, \psi)$ *and* $\mathfrak{q}$ *be an integral ideal of* $\mathcal{O}_F$. *Then* $\mathbf{g} = \mathbf{f} - (\mathbf{f}|U(\mathfrak{q}))|\mathfrak{q}$ *is a Hilbert cusp form of weight* k. *Further, it has the property that* $C(\mathfrak{m}\mathfrak{q}, \mathbf{g}) = 0$ *and* $C(\mathfrak{m}, \mathbf{g}) = C(\mathfrak{m}, \mathbf{f})$, *if* $(\mathfrak{m}, \mathfrak{q}) = 1$.

Now, we are ready to prove Theorem 4.5.

Proof. First, we shall show that there exist infinitely many $\mathfrak{m} \subseteq \mathcal{O}_F$ such that

$$C(\mathfrak{m}, \mathbf{f})C(\mathfrak{m}, \mathbf{g}) < 0. \tag{4.7}$$

A similar proof works for the other case as well, by replacing $\mathbf{f}$ by $-\mathbf{f}$. If (4.7) is not true, then there exist an ideal $\mathfrak{m}' \subseteq \mathcal{O}_F$ such that

$$C(\mathfrak{m}, \mathbf{f})C(\mathfrak{m}, \mathbf{g}) \geq 0 \tag{4.8}$$

for all $\mathfrak{m} \subseteq \mathcal{O}_F$ with $N(\mathfrak{m}) \geq N(\mathfrak{m}')$. Set $\mathfrak{n} := \prod_{N(\mathfrak{p}) \leq N(\mathfrak{m}')} \mathfrak{p}$, where $\mathfrak{p}$ are prime ideals of $\mathcal{O}_F$.

Let $\mathbf{f}_1 := \mathbf{f} - (\mathbf{f}|U(\mathfrak{n}))|\mathfrak{n}$ and $\mathbf{g}_1 = \mathbf{g} - (\mathbf{g}|U(\mathfrak{n}))|\mathfrak{n}$ be two Hilbert modular cusp forms obtained from $\mathbf{f}$ and $\mathbf{g}$ respectively (cf. Proposition 4.9). Clearly, $\mathbf{f}_1$ and $\mathbf{g}_1$ are also Hilbert cusp forms of even weights k and l respectively, and of level $\mathfrak{c}_1$. We just say that the level is $\mathfrak{c}_1$, because as such we do not need the explicit level in the further calculations.

For $s \in \mathbb{C}$ with $\mathrm{Re}(s) \gg 1$, the Rankin-Selberg L-function of $\mathbf{f}_1$ and $\mathbf{g}_1$ is defined by

$$R_{\mathbf{f}_1,\mathbf{g}_1}(s) := \sum_{\mathfrak{m} \subseteq \mathcal{O}_F, (\mathfrak{m},\mathfrak{n})=1} \frac{C(\mathfrak{m}, \mathbf{f})C(\mathfrak{m}, \mathbf{g})}{N(\mathfrak{m})^s}. \tag{4.9}$$

In above summation $C(\mathfrak{m}, \mathbf{f})C(\mathfrak{m}, \mathbf{g}) \geq 0$, since, if $N(\mathfrak{m}) \leq N(\mathfrak{m}')$ then $\mathfrak{m} = \prod_{\mathfrak{p}_i|\mathfrak{n}} \mathfrak{p}_i^{e_i}$ implies $(\mathfrak{m}, \mathfrak{n}) \neq 1$. The Rankin-Selberg L-function $R_{f_1,g_1}(s)$ is a non-zero function since there exists $\mathfrak{m}$ with $(\mathfrak{m}, \mathfrak{n}) = 1$ such that $C(\mathfrak{m}, \mathbf{f})C(\mathfrak{m}, \mathbf{g}) \neq 0$, by hypothesis.

For $\mathrm{Re}(s) \gg 1$, we set

$$L_{\mathbf{f}_1,\mathbf{g}_1}(s) := \zeta_F^{\mathfrak{c}_1}(2s - (k_0 + l_0) + 2)R_{\mathbf{f}_1,\mathbf{g}_1}(s),$$

where $\zeta_F^{\mathfrak{c}_1}(s) = \prod_{\mathfrak{p}|\mathfrak{c}_1, \mathfrak{p}:\text{prime}}(1 - N(\mathfrak{p})^{-s})\zeta_F(s)$, where $\zeta_F(s) = \sum_{\mathfrak{m} \subseteq \mathcal{O}_F} N(\mathfrak{m})^{-s}$ is Dedekind zeta function of F. By the Euler expansion of Dedekind zeta function of F, we get that

$$\begin{aligned}\zeta_F^{\mathfrak{c}_1}(s) &= \prod_{\mathfrak{p}|\mathfrak{c}_1, \mathfrak{p}:\text{prime}} (1 - N(\mathfrak{p})^{-s}) \prod_{\mathfrak{p}:\text{prime}} (1 - N(\mathfrak{p})^{-s})^{-1} \\ &= \sum_{\mathfrak{m} \subseteq \mathcal{O}_F, (\mathfrak{m},\mathfrak{c}_1)=1} \frac{1}{N(\mathfrak{m})^s} = \sum_{n=1}^{\infty} \frac{a_n(\mathfrak{c}_1)}{n^s},\end{aligned}$$

where $a_n(\mathfrak{c}_1)$ is the number of integral ideals of norm n that are co-prime to $\mathfrak{c}_1$. Hence, we can write

$$L_{\mathbf{f}_1,\mathbf{g}_1}(s) = \sum_{n=1}^{\infty} \frac{a_n(\mathfrak{c}_1)n^{k_0+l_0-2}}{n^{2s}} \sum_{\mathfrak{m}\subseteq\mathcal{O}_F,(\mathfrak{m},\mathfrak{n})=1} \frac{C(\mathfrak{m},\mathbf{f})C(\mathfrak{m},\mathbf{g})}{N(\mathfrak{m})^s}.$$

Now, we can re-write

$$L_{\mathbf{f}_1,\mathbf{g}_1}(s) = \sum_{m=1}^{\infty} \frac{\mathfrak{b}_m^{\mathfrak{c}_1}(\mathbf{f}_1,\mathbf{g}_1)}{m^s} = \sum_{m=1}^{\infty} \mathfrak{b}_m^{\mathfrak{c}_1}(\mathbf{f}_1,\mathbf{g}_1)e^{-s\log m},$$

where

$$\mathfrak{b}_m^{\mathfrak{c}_1}(\mathbf{f}_1,\mathbf{g}_1) = \sum_{n^2|m} \left(a_n(\mathfrak{c}_1)n^{k_0+l_0-2} \sum_{(\mathfrak{m},\mathfrak{n})=1,N(\mathfrak{m})=m/n^2} C(\mathfrak{m},\mathbf{f})C(\mathfrak{m},\mathbf{g}) \right).$$

Define, for any j, $k'_j := k_0 - k_j$, and similarly, define l'_j. Now, look at the complete L-function, defined by the product

$$\Lambda_{\mathbf{f}_1,\mathbf{g}_1}(s) = \prod_{j=1}^{n} \Gamma\left(s+1+\frac{k_j-l_j-k_0-l_0}{2}\right)\Gamma\left(s-\frac{k'_j+l'_j}{2}\right)L_{\mathbf{f}_1,\mathbf{g}_1}(s)$$

can be continued to a holomorphic function on the whole plane, since the weights are different (cf. [Shi78, Proposition 4.13]). As the Γ-function is extended by analytic continuation to all complex numbers except the non-positive integers, where the function has simple poles, we get that that function $L_{\mathbf{f}_1,\mathbf{g}_1}(s)$ is also entire and has infinitely many real zeros because the Γ-factors have poles at non-positive integers.

By Landau's Theorem for Dirichlet series with non-negative coefficients, it follows that the Dirichlet series $L_{\mathbf{f}_1,\mathbf{g}_1}(s)$ converges everywhere. By Theorem 4.7, there exist infinitely many $m \in \mathbb{N}$ such that $\mathfrak{b}_m^{\mathfrak{c}_1}(\mathbf{f}_1,\mathbf{g}_1) > 0$ and there exist infinitely many $m \in \mathbb{N}$ such that $\mathfrak{b}_m^{\mathfrak{c}_1}(\mathbf{f}_1,\mathbf{g}_1) < 0$. This is a contradiction to the fact $\mathfrak{b}_m^{\mathfrak{c}_1}(\mathbf{f}_1,\mathbf{g}_1) \geq 0$ for all m (this is because, by (4.8), $C(\mathfrak{m},\mathbf{f})C(\mathfrak{m},\mathbf{g}) \geq 0$ for all $(\mathfrak{m},\mathfrak{n}) = 1$). This completes the proof of Theorem 4.5. □

In the following proposition, we compute the natural density of $n \in \mathbb{N}$ such that the product $C(\mathfrak{p}^n,\mathbf{f})C(\mathfrak{p}^n,\mathbf{g})$ have the same sign (resp., opposite sign). For primitive forms over $\mathbb{Q}$, this a result due to Amri (cf. [Amr18, Theorem 1.1]).

Proposition 4.10. *Let* $\mathbf{f},\mathbf{g}$ *be two distinct non-CM primitive forms over* F *of levels* $\mathfrak{c}_1,\mathfrak{c}_2$*, with trivial characters, and weights* $2k, 2l$*, respectively. For any prime ideal* $\mathfrak{p} \in \mathbf{P}$ *with* $\mathfrak{p} \nmid \mathfrak{c}_1\mathfrak{c}_2\mathfrak{D}_F$*, let* $\theta_{\mathfrak{p}}(\mathbf{f}),\theta_{\mathfrak{p}}(\mathbf{g}) \in [0,\pi]$ *be defined as in* (2.3)*. Then, for a natural density* 1 *set of primes* $\mathfrak{p} \in \mathbf{P}$*, the linear independence of* $1, \frac{\theta_{\mathfrak{p}}(\mathbf{f})}{2\pi}, \frac{\theta_{\mathfrak{p}}(\mathbf{g})}{2\pi}$ *over* $\mathbb{Q}$ *implies*

$$\lim_{x\to\infty} \frac{\#\{n \leq x : C(\mathfrak{p}^n,\mathbf{f})C(\mathfrak{p}^n,\mathbf{g}) \gtrless 0\}}{x} = \frac{1}{2}.$$

Proof. By Theorem 2.1, the natural density $\mathfrak{p} \in \mathbf{P}$ such that $\theta_{\mathfrak{p}}(\mathbf{f}), \theta_{\mathfrak{p}}(\mathbf{g}) \in \{0, \pi\}$ is zero. Let $\mathfrak{p} \in \mathbf{P}$ be a prime ideal such that $\theta_{\mathfrak{p}}(\mathbf{f}), \theta_{\mathfrak{p}}(\mathbf{g}) \in (0, \pi)$. If $1, \frac{\theta_{\mathfrak{p}}(\mathbf{f})}{2\pi}, \frac{\theta_{\mathfrak{p}}(\mathbf{g})}{2\pi}$ are linearly independent over $\mathbb{Q}$, the sequence $\{(n\frac{\theta_{\mathfrak{p}}(\mathbf{f})}{2\pi}, n\frac{\theta_{\mathfrak{p}}(\mathbf{g})}{2\pi})\}_{n\in\mathbb{N}}$ is uniformly distributed $\pmod 1$ in $\mathbb{R}^2$ (cf. [KN74, Theorem 6.3]). Now, the rest of the proof is similar to that of [Amr18, Theorem 1.1]. □

In the above result, instead of F, if we work over K, then one can show the same result holds for all but finitely many primes $\mathfrak{p} \in \mathbb{P}$, instead of density 1 set of primes $\mathfrak{p} \in \mathbf{P}$. In this case, we can even drop the assumption on **f**, **g** being non-CM.

Acknowledgements

The authors are thankful to the anonymous referee for the valuable suggestions towards the improvement of this paper. The first author thanks the University Grants Commission (UGC), India for the financial support provided in the form of Research Fellowship to carry out this research work at IIT Hyderabad. The second author's research was partially supported by the SERB grant MTR/2019/000137.

References

[Amr18] Amri, Mohammed Amin. Simultaneous sign change and equidistribution of signs of Fourier coefficients of two cusp forms. *Arch. Math. (Basel)*, **111** (2018) no. 3, 257–266.

[BGG11] Barnet-Lamb, Thomas; Gee, Toby; Geraghty, David. The Sato-Tate conjecture for Hilbert modular forms. *J. Amer. Math. Soc.*, **24** (2011) no. 2, 411–469.

[Fre90] Freitag, Eberhard. Hilbert modular forms. Springer-Verlag, Berlin (1990).

[Gar90] Garrett, Paul B. Holomorphic Hilbert modular forms. The Wadsworth & Brooks/Cole Mathematics Series, CA (1990).

[GKP] Gun, Sanoli; Kumar, Balesh; Paul, Biplab. The first simultaneous sign change and non-vanishing of Hecke eigenvalues of newforms. https://arxiv.org/pdf/1801.10590

[GKR15] Gun, Sanoli; Kohnen, Winfried; Rath, Purusottam. Simultaneous sign change of Fourier-coefficients of two cusp forms. *Arch. Math. (Basel)*, **105** (2015) no. 5, 413–424.

[KK18] Kaushik, Surjeet; Kumar, Narasimha. Simultaneous behaviour of the Fourier coefficients of two Hilbert modular cusp forms. *Arch. Math.*, (2018). https://doi.org/10.1007/s00013-018-1275-9

[KKT18] Kaushik, Surjeet; Kumar, Narasimha; Tanabe, Naomi. Equidistribution of signs for Hilbert modular forms of half-integral weight. *Res. Number Theory*, **4** (2018) no. 2, Art. 13, 10.

[KM14] Kohnen, Winfried; Martin, Yves. Sign changes of Fourier coefficients of cusp forms supported on prime power indices. *Int. J. Number Theory*, **10** (2014) no. 8, 1921–1927.

[KM18] Kumari, Moni; Murty, M. Ram. Simultaneous non-vanishing and sign changes of Fourier coefficients of modular forms. *Int. J. Number Theory*, **14** (2018) no. 8, 2291–2301.

[KN74] Kuipers, L.; Niederreiter, H. Uniform distribution of sequences. Pure and Applied Mathematics. Wiley-Interscience, New York-London-Sydney (1974).

[KRW07] Kowalski, Emmanuel; Robert, Olivier; Wu, Jie. Small gaps in coefficients of L-functions and B-free numbers in short intervals. *Rev. Mat. Iberoam.*, **23** (2007) no. 1, 281–326.

[MKV18] Meher, Jaban; Shankhadhar, Karam Deo; Viswanadham, G. K. On the coefficients of symmetric power L-functions. *Int. J. Number Theory*, **14** (2018) no. 3, 813–824.

[MM07] Ram Murty, M.; Kumar Murty, V. Odd values of Fourier coefficients of certain modular forms. *Int. J. Number Theory*, **3** (2007) no. 3, 455–470.

[MT14] Meher, Jaban; Tanabe, Naomi. Sign changes of Fourier coefficients of Hilbert modular forms. *J. Number Theory*, **145** (2014) 230–244.

[Mur83] Murty, M. Ram. Oscillations of Fourier coefficients of modular forms. *Math. Ann.*, **262** (1983) no. 4, 431–446.

[Pan91] Panchishkin, Alexey A. Non-Archimedean L-functions of Siegel and Hilbert modular forms. *Lecture Notes in Mathematics*, 1471. Springer-Verlag, Berlin (1991).

[Pri08] Pribitkin, Wladimir de Azevedo. On the sign changes of coefficients of general Dirichlet series. *Proc. Amer. Math. Soc.*, **136** (2008) no. 9, 3089–3094.

[Shi78] Shimura, Goro. The special values of the zeta functions associated with Hilbert modular forms. *Duke Math. J.*, **45** (1978) no. 3, 637–679.

Topics in Number Theory, RMS-Lecture Notes Series No. 26, 2020, pp. 189–201.

Some Remarks on Classical Algebraic Independence Theory

Philippon Patrice*

Équipe de Théorie des Nombres, Institut de Mathématiques de Jussieu-Paris Rive Gauche, UMR CNRS 7586, Case courrier 247, 4 place Jussieu, 75252 Paris Cedex 05, France.
e-mail: patrice.philippon@imj-prg.fr

Abstract. This note has two parts. It first presents results on large transcendence degrees of values of analytic functions (what we call classical algebraic independence), as they stand. Then it dives into the heart of the so-called Gel'fond-Schneider method used to prove some of these results, unfortunately not completely. And step by step it switches the point of view to a more geometrical one, eventually pointing towards conjectures that, hopefully, open the way to new breakthroughs.

Keywords. Algebraic independence, E-function, Mahler function, Gelfond-Schneider method, algebraic approximation

2000 Subject Classification: 11G50, 11J85, 11J95, 14G40

1. Early steps and developments

The first example of transcendental numbers was given by Joseph Liouville in 1844, then developed in 1851 [13]. The transcendency is proved with the help of very good approximations by rational numbers.

An algebraic number cannot have too good rational approximations. Let $\alpha \in \overline{\boldsymbol{Q}} \cap \boldsymbol{R}$ and P its minimal polynomial in $\boldsymbol{Z}[X]$, then Liouville showed

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{1}{|P'(\alpha)|(2q)^{\mathrm{d}^\circ P}} \text{ for } q \geq \max_{\substack{P(\alpha')=0 \\ \alpha\neq\alpha'}} |\alpha-\alpha'|^{-1} \text{ and } \frac{p}{q} \neq \alpha. \tag{1}$$

The rational approximations of a real number are encoded in its continued fraction expansion. For example, it is an exercise, with the so-called folding lemma [15], to show that the continued fraction of the number $\xi = \sum_{\ell=1}^{\infty} 10^{-\ell!}$ is given as follow. For $a_1, \ldots, a_k$ and c integers, define the transformation

$$\rho_c(a_1, \ldots, a_k) = a_1, \ldots, a_k, c-1, 1, a_k - 1, a_{k-1}, \ldots, a_1.$$

Then

$$\begin{aligned}\xi &= \left[0, \lim_{\ell\to\infty} \rho_{10^{(\ell-1)\ell!}} \circ \cdots \circ \rho_{10^{72}} \circ \rho_{10^{12}} \circ \rho_{10^2}(9, 11)\right] \\ &= [0, 9, 11, 99, 1, 10, 9, 999999999999, 1, 8, 10, 1, 99, 11, 9, \underbrace{9\ldots\ldots\ldots9}_{72\ 9's}, 1, \ldots].\end{aligned}$$

*The author thanks heartily the referee, who suggested many additions and corrections which improved the text much.

The big partial quotients spot the very good approximations, some of them coming just from truncating the series. If ξ were algebraic, these very good approximations would contradict (1).

1.1 *a) Roth and the subspace theorem*

Liouville inequality has been improved by several authors (notably Axel Thue, Carl Ludwig Siegel) till Klaus Friedrich Roth established in 1955 that for any positive real number $\varepsilon > 0$ there exists a positive real number $c(\alpha, \varepsilon) > 0$ satisfying:

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{c(\alpha, \varepsilon)}{q^{2+\varepsilon}}.$$

This was generalised in 1972 by Wolfgang Schmidt, *see* [23], to higher dimension with the so called subspace theorem, which turned to be incredibly useful in all kind of applications, *see* for example [30] for some of these to Diophantine equations.

However, a caveat in Roth theorem is that the real $c(\alpha, \varepsilon)$ cannot be in general effectively computed or uniformly bounded in terms of α (running, for example, over all the algebraic numbers of bounded degrees).

1.2 *b) A method for transcendence*

Many numbers (in particular the ones we are interested in, like e or π) cannot be distinguished from algebraic numbers by their rational approximation. This may happen because we don't know enough specific properties of the continued fraction expansion of algebraic numbers, but this may be as well due to the fact that there are not much of them.

Charles Hermite [7] devised in 1873 a method for proving the transcendency of e, based on approximations by algebraic numbers, rather than rational ones. This method was taken up by Ferdinand von Lindemann [12] in 1882 who proved the transcendency of π (settling for good that squaring the circle is impossible). Combining authors and results we now speak of the Hermite-Lindemann theorem which states that: *for any nonzero algebraic number α its exponential* e^{α} *is a transcendental number*, *i.e.* $\mathrm{e}^{\alpha} \notin \overline{\boldsymbol{Q}}$. The transcendency of e follows with $\alpha = 1$ and that of π with $\alpha = \mathrm{i}\pi$.

Since then, classical transcendence theory aims at showing that complex numbers that have no "good" reason to be algebraic are indeed transcendental or, more generally, to determine the algebraic relations among several given numbers. In this context, "good" reasons are mainly given by geometry, often through the action of an algebraic group.

2. Algebraic independence

Lindemann asserted more than a transcendence result, but proofs had to be completed by Karl Weierstrass [29] in 1885 in order to state: *for $\alpha_1, \ldots, \alpha_n$ algebraic numbers,* *linearly independent over* $\boldsymbol{Q}$*, the numbers* $e^{\alpha_1}, \ldots, e^{\alpha_n}$ *are algebraically independent over* $\boldsymbol{Q}$ (*i.e.* do not satisfy a polynomial equation with coefficients in $\boldsymbol{Q}$ or $\overline{\boldsymbol{Q}}$).

In 1960 Stephen Schanuel proposed a beautiful conjecture, which is supposed to contain all the "reasonable" statements that can be made on the value of the exponential function: *let* $x_1, \ldots, x_n$ *be complex numbers, linearly independent over* $\boldsymbol{Q}$*, then at least* n *of the numbers* $x_1, \ldots, x_n, e^{x_1}, \ldots, e^{x_n}$ *are algebraically independent over* $\boldsymbol{Q}$. This conjecture is wide open, except for the case of algebraic numbers, which is Lindemann-Weierstrass theorem, and the case $n = 1$ which follows from Hermite-Lindemann theorem.

2.1 *a) The four exponentials conjecture*

However, it is less straightforward to deduce from Schanuel conjecture the following: *given four nonzero complex numbers* x_1, x_2, y_1, y_2 *such that* x_2/x_1 *and* y_2/y_1 *are irrational numbers, then at least one of the four numbers* $e^{x_i y_j}$*,* $1 \le i, j \le 2$ *is transcendental.* This question goes back to one by Leonidas Alaoglu and Paul Erdös in 1944: *is the quotient of two consecutive colossally abundant numbers*[1] *a prime or not*, which can be reduced to a special case of the four exponentials problem.

Serge Lang in 1966 and Kanakanahalli Ramachandra in 1968 proved independently the six exponentials theorem (where one takes two x's and three y's $\boldsymbol{Q}$-linearly independent, for the same conclusion), *see* [27, Chapter 1, §3]. But this latter result, the relevant special case of which was already certified by Siegel, only implies that the quotient of two consecutive colossally abundant numbers is a prime *or* the product of two distinct primes.

2.2 *b) Baker theorem*

In 1966 Alan Baker, *see* [2, Chapter 2], proved the following first small step dealing with the case of logarithm of algebraic numbers: *if* $e^{x_1}, \ldots, e^{x_n}$ *are algebraic numbers then* $x_1, \ldots, x_n$ *are linearly independent over* $\overline{\boldsymbol{Q}}$ *if and only if they are linearly independent over* $\boldsymbol{Q}$.

But the real strength of this result is in the fact that it allows to give explicit lower bounds for linear forms in logarithms of algebraic numbers, precise enough, whereas one reminds that Roth and the subspace theorem are ineffective. This was already pointed by Alexander Osipovich Gel'fond with two logarithms and then developed by Alan Baker and many authors, *see* [2, Chapter 3] or/and [27, Chapter 10, §4].

2.3 *c) Commutative algebraic groups and motives*

Following a remark of Pierre Cartier, Lang [11] was the first to develop systematically transcendence theory in the frame of commutative algebraic groups. For example,

[1] *colossally abundant numbers*, first studied by Srinivasa Ramanujan, are the positive numbers $n \in \boldsymbol{N}^{\times}$ such that, for some $\varepsilon > 0$, one has $\frac{\sigma(n)}{n^{1+\varepsilon}} \ge \frac{\sigma(m)}{m^{1+\varepsilon}}$ if $m \le n$ and $\frac{\sigma(n)}{n^{1+\varepsilon}} > \frac{\sigma(m)}{m^{1+\varepsilon}}$ if $m > n$, where $\sigma(n) := \sum_{\ell | n} \ell$ and $m \in \boldsymbol{N}^{\times}$.

this leads to the following abelian generalisation of Schanuel conjecture: *let A be an abelian variety defined over $\overline{\boldsymbol{Q}}$ and u a point in the tangent space of $A(\boldsymbol{C})$, then the transcendence degree of the field generated by the coordinates of u and* $\exp_A(u)$ *is at least the dimension of the smallest algebraic subgroup of A containing* $\exp_A(u)$. One may even consider abelian varieties defined over any subfield K of $\boldsymbol{C}$, but then this is the field generated over K by the coordinates of u and $\exp_A(u)$ that should have transcendence degree (over $\boldsymbol{Q}$) at least the dimension of the smallest algebraic subgroup of A containing $\exp_A(u)$.

More generally, a conjecture of Alexandre Grothendieck [10] (*see* [11, Chapter IV] for the precise statement) asserts that *the transcendence degree of the field generated by the periods of a smooth projective variety defined over $\overline{\boldsymbol{Q}}$ is equal to the dimension of its motivic Galois group*. Extending this, Yves André has casted a beautiful conjecture: *let K be a subfield of $\boldsymbol{C}$. If M is a* 1*-motive defined over K, then the transcendence degree over $\boldsymbol{Q}$ of the field generated over K by the periods of M is at least the dimension of the Mumford-Tate group of M*. It encompasses a lot of informations on the algebraic relations between periods, see for example [3] and [1]. As shown recently by Grégory Vallée [26, Théorème 2], Yves André's conjecture implies the above abelian Schanuel conjecture.

3. Three methods

3.1 *a) E-functions*

In 1929 Siegel introduced the notion of E-function (modeled on the exponential function): $f(z) = \sum_{k=0}^{\infty} \frac{a_k}{k!} z^k$, $a_k \in \overline{\boldsymbol{Q}}$, $h(a_0, \dots, a_k) = O(k)$ for all k (actually, Siegel required a slightly weaker condition) and f satisfies $f^{(m)}(z) + r_{m-1}(z) f^{(m-1)}(z) + \cdots + r_0(z) f(z) = 0$ with $r_i(z) \in \overline{\boldsymbol{Q}}(z)$. Beyond the exponential function, Bessel functions are examples of E-functions.

Siegel generalised the Lindemann-Weierstrass theorem to this class of functions, however under some kind of irreducibility condition on the differential operator of minimal order killing the function. Andrei Borisovich Shidlovsky [22] was able to remove this extra condition in 1956, thus proving: *let $f_1, \dots, f_m$ be E-functions satisfying*

$$\begin{pmatrix} f_1'(z) \\ \vdots \\ f_m'(z) \end{pmatrix} = A(z) \begin{pmatrix} f_1(z) \\ \vdots \\ f_m(z) \end{pmatrix}$$

with $A(z)$ an $m \times m$ matrix with entries in $\overline{\boldsymbol{Q}}(z)$. If $\alpha \in \overline{\boldsymbol{Q}}^{\times}$ is not a singularity of $A(z)$, then the transcendence degree of the field generated by the values $f_1(\alpha), \dots, f_m(\alpha)$ over $\overline{\boldsymbol{Q}}$ is equal to the transcendence degree of the field generated by the functions themselves over $\overline{\boldsymbol{Q}}[z]$. It is a feature of this method to consider only values at algebraic points.

Yuri Valentinovich Nesterenko and Shidlovsky proved further in 1996 that for all $\alpha \in \overline{\boldsymbol{Q}}^{\times}$ except finitely many, the algebraic relations over $\overline{\boldsymbol{Q}}$ between

$f_1(\alpha), \dots, f_m(\alpha)$ comes from specialisation of an algebraic relation over $\overline{\boldsymbol{Q}}(z)$ between the functions $f_1(z), \dots, f_m(z)$. However, they had no control on the exceptional set itself. They could effectively construct a larger set containing it, but not determine it exactly. Ten years later, in 2006, Frits Beukers [4] showed that the exceptional set is actually reduced to the singularity of $A(z)$.

The final task is to determine a basis of algebraic relations between the functions, to this end differential Galois theory is very useful.

3.2 *b) Mahler functions*

Here we consider the field $\overline{\boldsymbol{Q}}(z)$ endowed with the endomorphism $\sigma : z \mapsto z^q$, where $q \geq 2$ is an integer, or more generally $z \mapsto r(z) \in \overline{\boldsymbol{Q}}(z)$. A Mahler function is a series $f(z) \in \overline{\boldsymbol{Q}}[[z]]$ satisfying a functional equation $\sigma^m(f) + p_{m-1}\sigma^{m-1}(f) + \cdots + p_0 f = 0$, $p_i \in \overline{\boldsymbol{Q}}(z)$. The first and typical example of Mahler function is the Fredholm series $f(z) = \sum_{\ell=0}^{\infty} z^{2^\ell}$, which satisfies $f(z^2) = f(z) - z$ hence $f(z^4) - (z+1)f(z^2) + zf(z) = 0$. Other examples are given by generating functions of automatic sequences, Böttcher functions, ...

In 1930 Kurt Mahler proved that for functions $f_1(z), \dots, f_m(z)$ satisfying a system of functional equations

$$\begin{pmatrix} f_1(z^q) \\ \vdots \\ f_m(z^q) \end{pmatrix} = A \begin{pmatrix} f_1(z) \\ \vdots \\ f_m(z) \end{pmatrix} + B(z)$$

with A an $m \times m$ matrix, non-degenerate, with entries in $\overline{\boldsymbol{Q}}$ and $B(z)$ a column vector with components in $\overline{\boldsymbol{Q}}(z)$, the transcendence degree of the field generated over $\overline{\boldsymbol{Q}}$ by their values at a point $\alpha \in \overline{\boldsymbol{Q}}^\times$ which is not a pole of $B(z^{q^k})$ for all $k \in \boldsymbol{N}$, is equal to the transcendence degree of the field generated by the functions over $\overline{\boldsymbol{Q}}(z)$. In fact, Mahler dealt more generally with functions of several analytic variables, *see* [14].

It was much later, in 1996, that Kumiko Nishioka [17, Theorem 4.2.1] extended this result to systems with entries of the matrix A in $\overline{\boldsymbol{Q}}(z)$. The condition on the algebraic point α is now: no power α^{q^k}, $k \in \boldsymbol{N}$, can be a pole of $A(z)$ or $B(z)$. But the method also allows to consider values at non algebraic points.

Furthermore, assume that the functions are analytic in a disc of some radius ρ centred at the origin, then for any $\alpha \in \overline{\boldsymbol{Q}}^\times$ in this disc of convergence which is neither a singularity of $A(z)$ nor of $B(z)$, the algebraic relations over $\overline{\boldsymbol{Q}}$ between the values $f_1(\alpha), \dots, f_m(\alpha)$ come from specialisation of algebraic relations over $\overline{\boldsymbol{Q}}[z]$ between the functions $f_1(z), \dots, f_m(z)$. Similarly to the case of E-functions, Galois theory of systems of functional equations is very useful in order to determine the algebraic relations between the functions, *see* for example [6].

Paul-Georg Becker extended Mahler method for transcendence to algebraic functional equations, rather than linear or rational ones, while Becker, Thomas Töpfer and Evgeniy Zorin extended algebraic independence results to rational transformation of the variable.

Mahler himself observed that his method could not be applied to the modular function $J(z) = \frac{1}{z} + 744 + \dots$. However, in 1996 Katia Barré-Siriex, Guy Diaz, François Gramain and Georges Philibert were able to overcome the difficulty pointed out by Mahler (and several authors after him). They proved the so-called Mahler-Manin conjecture: *for ξ a nonzero complex or p-adic number of absolute value < 1 one of the two numbers ξ and $J(\xi)$ is transcendental.*

Stepping on this breakthrough, Nesterenko addressed a question of Daniel Bertrand and obtained a multiplicity estimate for polynomials in z and the Eisenstein series $E_2(z)$, $E_4(z)$ and $E_6(z)$, where $E_{2k}(z) = 1 + \gamma_k \sum_{n=1}^{\infty} \left(\sum_{\ell | n} \ell^{2k-1}\right) z^n$, $\gamma_1 = -24$, $\gamma_2 = 240$ and $\gamma_3 = -504$, *see* [16, Chapter 3]. Recall that with these notations $J(z) = \frac{1728 E_4(z)^3}{E_4(z)^3 - E_6(z)^2}$. Combined with a criterion for algebraic independence this established: *for ξ as above at least three of the four numbers ξ, $E_2(\xi)$, $E_4(\xi)$ and $E_6(\xi)$ are algebraically independent over $\boldsymbol{Q}$.*

3.3 *c) Gel'fond-Schneider*

Gel'fond [8] and Theodor Schneider [24] devised independently in 1934 transcendental methods in order to solve David Hilbert's seven problem: *let $\alpha, \beta \in \overline{\boldsymbol{Q}}$, $\alpha \neq 0, 1$ and $\beta \notin \boldsymbol{Q}$, then $\alpha^\beta \notin \overline{\boldsymbol{Q}}$.*

Their approaches could be united in a stronger method and were subject to generalisations to exponential maps of commutative algebraic groups, for example elliptic Weierstrass functions which parameterise elliptic curves.

Gel'fond went a step out of firm ground [9], asserting that he could prove that, denoting $d = [\boldsymbol{Q}(\beta) : \boldsymbol{Q}]$, the numbers $\alpha^\beta, \dots, \alpha^{\beta^{d-1}}$ were algebraically independent over $\boldsymbol{Q}$[2]. This statement is since then called Gel'fond's conjecture, it was reproduced in Schneider's book [25] on transcendental numbers (1957). The best known result in this direction is still Guy Diaz [5]: *there are at least $\left[\frac{d+1}{2}\right]$ algebraically independent numbers among $\alpha^\beta, \dots, \alpha^{\beta^{d-1}}$*. For $d = 3$ it was already proved by Gel'fond and gives the algebraic independence of the two numbers α^β and α^{β^2}.

On an other hand we have the analog of Lindemann-Weierstrass theorem for elliptic functions (and even abelian functions, 1983) parameterising an elliptic curve with complex multiplication:

$$\boldsymbol{C}/\Lambda \to \boldsymbol{P}_2(\boldsymbol{C}) \quad z \mapsto (1 : \wp(z) : \wp'(z)),$$

then for $\alpha_1, \dots, \alpha_m$ linearly independent over the field of multiplications, the numbers $\wp(\alpha_1), \dots, \wp(\alpha_m)$ are algebraically independent over $\boldsymbol{Q}$. *See* [28, Theorem 39].

As it stands, Gel'fond method for algebraic independence is far from giving as strong results as Siegel and Mahler's methods. In the sequel we want to discuss a key point of this method, its strength and weakness. This will lead us to recast the whole approach in a more geometric mould, calling for a closer study of singularities.

[2]In the same note, Gel'fond asserts the algebraic independence of logarithms of multiplicatively independent algebraic numbers as well.

4. From Gel'fond to CIA

In transcendence and algebraic independence theory proofs usually proceed by contradiction. One assume that the transcendence degree is smaller than expected and one constructs (*via* extrapolation of an auxiliary function) polynomials taking small values at the point under consideration. If the transcendence degree is assumed to be zero one concludes with the size inequality (a guise of the product formula). If the transcendence degree is assumed to be 1 then we may appeal to the following criterium due to Gel'fond.

We denote $t(P) = \log M(P) + \mathrm{d}^\circ P$ the *size*[3] of the polynomial P with coefficients in $\boldsymbol{Z}$.

Theorem 1 (Gel'fond criterium). *Let $\theta \in \boldsymbol{C}$ and $\tau, \delta : \boldsymbol{N} \to \boldsymbol{N}^\times$ be two increasing functions. Assume there exists a sequence of nonzero polynomials $(P_N)_{N\in\boldsymbol{N}} \subset \boldsymbol{Z}[X]$ satisfying $t(P_N) \leq \tau(N)$, $\mathrm{d}^\circ P_N \leq \delta(N)$ and*

$$\frac{-\log|P_N(\theta)|}{\tau(N+1)\delta(N+1)} \underset{N\to\infty}{\longrightarrow} \infty.$$

Then θ is an algebraic number (over $\boldsymbol{Q}$), zero of P_N for all N large enough.

In higher dimension this criterium generalises as follows, *see* [18].

Theorem 2 (CIA). *Let $\theta \in \boldsymbol{C}^n$ and $\tau, \delta : \boldsymbol{N} \to \boldsymbol{N}^\times$ be two increasing functions. Assume there exists a sequence of ideals $(P_{N,1}, \dots, P_{N,m(N)})_{N\in\boldsymbol{N}} \subset \boldsymbol{Z}[X_1, \dots, X_n]$ satisfying $t(P_{N,i}) \leq \tau(N)$, $\mathrm{d}^\circ P_{N,i} \leq \delta(N)$ for $i = 1, \dots, m(N)$,*

$$\sigma(N+1)^{n+1} := \frac{-\log\max_{1\leq i\leq m(N)}|P_{N,i}(\theta)|}{\tau(N+1)\delta(N+1)^n} \underset{N\to\infty}{\longrightarrow} \infty$$

and furthermore that the polynomials $P_{N,1}, \dots, P_{N,m(N)}$ only have a finite number of common zeros in the ball of radius $\exp(-\sigma(N)^{n+2}\tau(N)\delta(N)^n)$ centred at θ. Then $\theta \in \overline{\boldsymbol{Q}}^n$ is a common zero of the $P_{N,i}$ for all N large enough.

In the other direction we have:

Proposition 3. *Let $n \geq 2$ and $\psi : \boldsymbol{N} \to \boldsymbol{R}_{>0}$. There exists $\theta_1, \dots, \theta_n \in \boldsymbol{C}$ algebraically independent over $\boldsymbol{Q}$ and for all $N \in \boldsymbol{N}$ integers $(a_{i,j}^{(N)})_{\substack{i=1,\dots,n-1\\ j=0,1,2}}$ of absolute value $\leq N$ satisfying $|a_{i,2}^{(N)}\theta_{i+1} + a_{i,1}^{(N)}\theta_1 + a_{i,0}^{(N)}| < \psi(N)$ and $a_{i,2}^{(N)} \neq 0$.*

Proof. *See* [18, Appendix]. □

The common zeros of the linear forms $a_{i,2}^{(N)}X_{i+1} + a_{i,1}^{(N)}X_1 + a_{i,0}^{(N)}$, $i = 1, \dots, n-1$, form a line (dimension 1). In particular, for $n \geq 2$ the statement of CIA is false without the hypothesis of dimension 0 in a neighbourhood of θ. Of course, this condition is implicit in Theorem 1.

[3] Here $M(P)$ stands for some norm or measure (preferably multiplicative) of the polynomial P, for example the Mahler measure.

5. Measures of algebraic independence

Assuming that the locus of zeros of the ideals appearing in Theorem 2 does not intersect the prescribed ball (at all), we can go further in the conclusion and give a lower bound for the distance between the point θ and a given variety.

Let $\theta \in \boldsymbol{P}_n(\boldsymbol{C})$ and $V \subset \boldsymbol{P}_n$ defined over $\overline{\boldsymbol{Q}}$, of dimension d, it is a question of bounding from below quantitatively the distance $\mathrm{Dist}(\theta, V)$ from θ to V where $\log(\mathrm{Dist}(\theta, V))$ is an average over $x \in V(\boldsymbol{C})$ of $\log(\mathrm{Dist}(\theta, x)) := \log\left(\frac{\|\theta\wedge x\|}{\|\theta\|\cdot\|x\|}\right)$, in terms of the height $h(V)$ and the degree $d(V)$ of V. In case V is defined by a single equation $P(X_0, \dots, X_n) = \sum_\alpha P_\alpha X_0^{\alpha_0} \dots X_n^{\alpha_n}$, we have $\mathrm{Dist}(\theta, V) = \frac{|P(\theta)|}{\|P\|\cdot\|\theta\|^{\mathrm{d}^\circ P}}$ with $\|P\| := \sqrt{\sum_\alpha |P_\alpha|^2/\binom{\mathrm{d}^\circ P}{\alpha}}$.

Set $d = \dim(V)$ and let δ, τ, σ and U be real numbers ≥ 1 satisfying $\sigma^{d+1} < \tau$ and

$$\sigma^{d+1}\delta^d(\delta h(V) + (d+1)\tau d(V) + 3(d+1)^2\log(n+1)\delta d(V)) < U. \tag{2}$$

The starting point of the criterium is the following hypothesis:

Hypothesis 4. *For each* $\tau/\sigma^{d+1} < S < U/\sigma^{d+1}$ *there exists forms* $Q_1, \dots, Q_m$ *in* $\boldsymbol{Z}[X_0, \dots, X_n]$ *satisfying:*

1) $\mathrm{d}^\circ Q_i \leq \delta$, $\log\|Q_i\| \leq \tau$*;*

2) $\frac{|Q_i(\theta)|}{\|Q_i\|\cdot\|\theta\|^{\mathrm{d}^\circ Q_i}} < \mathrm{e}^{-S\sigma^{d+1}}$*;*

3) the forms $Q_1, \dots, Q_m$ *have no common zero in the ball*

$$\{x \in \boldsymbol{P}_n(\boldsymbol{C}); \mathrm{Dist}(\theta, x) \leq \mathrm{e}^{-S\sigma^{d+2}}\}.$$

Then Christian Jadot proved:

Theorem 5. *Under Hypothesis 4 one has:* $\log(\mathrm{Dist}(\theta, V)) \geq -U$.

Proof. *See* [16, Chapter 8]. □

In particular, making U tends to the left hand side of (2) one gets:

$$\log(\mathrm{Dist}(\theta, V)) \geq -\sigma^{d+1}\delta^d(\delta h(V) + (d+1)\tau d(V) + 3(d+1)^2\log(n+1)\delta d(V)). \tag{3}$$

For $\delta = 1$ and $d(V) = 1$, this statement improves a criterium for *linear* independence of Nesterenko.

6. Descent and Gel'fond step

The proof of these criteria is by contradiction and rests on a descent of the dimension, summarised in the following lemma:

Lemma 6. *With all the hypothesis of Section 5, assume further that* $\log(\mathrm{Dist}(\theta, V)) < -U$*. Then, for all* $\ell = d+1, \dots, 0$ *there exists a projective variety* Z_ℓ *defined over* $\boldsymbol{Q}$ *of dimension* $\ell - 1$ *satisfying:*

1_ℓ) $d(Z_\ell) \le \delta^{d-\ell+1} d(V)$ *and* $h(Z_\ell) \le (\delta h(V) + (d-\ell+1)\tau d(V))\delta^{d-\ell}$;

2_ℓ) $\log(\mathrm{Dist}(\theta, Z_\ell)) < -\sigma^\ell \delta^{\ell-1}(\delta h(Z_\ell) + \ell(\tau + 3(d+1)\log(n+1)\delta)d(Z_\ell))$.

Proof. See ibidem [16, Chapter 8]. □

One takes $Z_{d+1} = V$. Since $Z_0 = \emptyset$ one has $\log(\mathrm{Dist}(\theta, Z_0)) = 0$ leading to a contradiction with 2_0). It follows that the hypothesis $\log(\mathrm{Dist}(\theta, V) < -U$ is unsustainable, proving Theorem 5.

In the proof of Theorem 2 (CIA) in Section 4, the existence of common zeros of the forms Q_i close to θ prevent descending to $\ell = 0$ in Lemma 6. The last step is replaced by the fact that $U = \infty$. One constructs a sequence of varieties $(Z_1^{(i)})_{i \in \boldsymbol{N}}$, of dimension zero, such that $\mathrm{Dist}(\theta, Z_1^{(i)}) \underset{i\to\infty}{\longrightarrow} 0$, and we show (Gel'fond step) that they coincide…and thus must ultimately contain θ.

Weakening the hypothesis $\log(\mathrm{Dist}(\theta, V)) < -U$ to $\log(\mathrm{Dist}(\theta, V)) < -\varepsilon U$ for some $0 < \varepsilon \le 1$ such that $\varepsilon\delta \ge 1$, then this relaxed hypothesis is realisable and Lemma 6 leads to a statement of type approximation.

For example taking $V = \boldsymbol{P}_n$, $\sigma = 1$, one has a more accurate result. More precisely, let δ, τ be real numbers ≥ 1 and $0 < \varepsilon \le 1$ satisfying $\varepsilon\delta \ge 1$, set

$$U := \varepsilon(n+1)(\tau + 3\delta\log(n+1))\delta^n. \tag{4}$$

Denote $H(\delta, \tau)$ (*resp.* $H(\varepsilon^2\delta, \varepsilon^2\tau)$) the Hypothesis 4 with $\sigma = 1$ and the parameters δ, τ and U as in (4) (*resp.* $\varepsilon^2\delta$, $\varepsilon^2\tau$ and $\varepsilon^{2n+2}U$).

Corollary 7. *Assume hypotheses $H(\delta, \tau)$ and $H(\varepsilon^2\delta, \varepsilon^2\tau)$ are verified. Then, there exists $\alpha \in \boldsymbol{P}(\overline{\boldsymbol{Q}})$ satisfying:*

1) $d(\alpha) := [\boldsymbol{Q}(\alpha) : \boldsymbol{Q}] \le \delta^n$ *and* $d(\alpha)h(\alpha) \le n(\tau + 2\delta\log(n+1))\delta^{n-1}$;

2) $\log(\mathrm{Dist}(\theta, \alpha)) < -\varepsilon^{2n+3}(1-\varepsilon)(\delta h(\alpha) + \tau + 3\delta\log(n+1))d(\alpha)$.

7. Approximations

A natural question is whether the approximation property in Corollary 7 is true independently of the Hypothesis 4 of the criterium.

Conjecture 8 (First approximation conjecture). *Let $n \in \boldsymbol{N}^*$ there exists a real $c(n)$ such that for all $\theta \in \boldsymbol{P}_n(\boldsymbol{C})$, $d \in \{0, \dots, n\}$, and reals $\delta \ge c(n)$, $\tau \ge 1$, there exists an algebraic subvariety Z of $\boldsymbol{P}_n$ of dimension d, defined over $\boldsymbol{Q}$, satisfying:*

1) $d(Z) \le (c(n)\delta)^{n-d}$ *and* $h(Z) \le c(n)^{n-d}\tau\delta^{n-d-1}$;

2) $\log(\mathrm{Dist}(\theta, Z)) < -c(n)^{d-n}\delta^d(\delta h(Z) + (\tau + \log(\delta))d(Z))$.

This conjecture is still open. It is proved for $d \in \{n-3, n-2, n-1, n\}$ but the interesting case is $d = 0$ which is reached only for $n \le 3$, [19]. Applications of the case $n = 1$ are detailed in [21]. It is also proved in the functional case (replacing the base ring $\boldsymbol{Z}$ by a ring of formal series in one variable and the distance by the order of vanishing along an analytic curve), [20].

In the case $d = 0$, one may hope to be a little more precise:

Conjecture 9 (Second approximation conjecture). *Let* $n \in \boldsymbol{N}^*$ *there exists a real* $c'(n)$ *such that for all* $\theta \in \boldsymbol{P}_n(\boldsymbol{C})$, $d \in \{0, \ldots, n\}$, *and reals* $\delta \geq c'(n)$, $\tau \geq c'(n)\log(\delta+1)$, *there exists* $\alpha \in \boldsymbol{P}_n(\overline{\boldsymbol{Q}})$, *satisfying:*

1) $d(\alpha) := [\boldsymbol{Q}(\alpha) : \boldsymbol{Q}] \leq (c'(n)\delta)^n$ *and* $h(\alpha)d(\alpha) \leq c'(n)^n \tau \delta^{n-1}$*;*

2) $\log(\mathrm{Dist}(\theta, \alpha)) < -c'(n)^{-n}(\delta h(\alpha) + \tau)d(\alpha)$.

This is shown for $n = 1, 2$ as an extension of Conjecture 8, [19].

8. Approximations of analytic subgroups

Many questions of algebraic independence deal with values of analytic or meromorphic functions satisfying differential and/or functional equations.

The most classical case is with the exponential function which is the exponential map of the multiplicative group $\boldsymbol{G}_m$. For example, Gel'fond-Schneider's conjecture is written naturally with the one-parameter analytic subgroup $\varphi : \boldsymbol{C} \to \boldsymbol{C} \times (\boldsymbol{C}^\times)^d$, $z \mapsto (z, \mathrm{e}^z, \mathrm{e}^{\beta z}, \ldots, \mathrm{e}^{\beta^{d-1}z})$, where β is an algebraic number of degree $d \geq 2$ over $\boldsymbol{Q}$.

It amounts to prove that the origin is the only point for which $\varphi(z)$ is defined over a field of transcendence degree $< d$. We know [5] that it is the only point where $\varphi(z)$ is defined over a field of transcendence degree $< [(d+1)/2]$.

Question 10. *Let* $G \subset \boldsymbol{P}_n$ *be a commutative algebraic group of dimension* g *and* φ *a one-parameter subgroup, Zariski dense in* G*, defined over a number field* K*. If* $\theta \in \mathrm{im}(\varphi)$ *belongs to an algebraic subvariety of* G *of dimension* $k \geq 1$*, defined over* K*, does there exist a real number* $c > 0$ *and infinitely many cycles* Z *of dimension* 0*, defined over* K*, satisfying:*

$$\log(\mathrm{Dist}(\theta, Z)) < -c \cdot (h(Z) + d(Z))^{g/k}?$$

It is interesting to state an analogous conjecture for the analytic subgroups of several parameters: *if* φ *is a* t*-parameter analytic subgroup of* $G \subset \boldsymbol{P}_n$*, Zariski dense in* G*, defined over a number field and* $\theta \in \mathrm{im}(\varphi)$ *belongs to an algebraic subvariety of* G *of dimension* k*, does there exists* $c > 0$ *and infinitely many cycles* Z *of dimension* 0*, defined over* K *and satisfying* $\log(\mathrm{Dist}(\theta, Z) < -c(h(Z) + d(Z))^{1/\sigma k}$*, where we assume*

$$\sigma := \min_H(\dim(\mathrm{im}(\varphi)/\mathrm{im}(\varphi) \cap H) / \dim(G/H)) < 1$$

the minimum being taken over all the proper algebraic subgroups H *of* G*?*

Using a zero estimate, one can give a positive answer to a weaker version of the above Question 10, omitting the term $h(Z)$. Here is the sketch of proof of this claim.

Claim 11. In the context of Question 10 there exists infinitely many cycles Z, defined over K, of dimension 0, satisfying

$$\log(\mathrm{Dist}(\theta, Z)) < -c \cdot d(Z)^{g/k}.$$

Proof. For a given integer D, one constructs a sequence $q_1, \ldots, q_g$ of forms in $A/\mathfrak{g}$ (viewed as sections on G) of degrees $\leq D$, regular on G and such that $\mathrm{ord}_\varphi(q_i) \gg D^g$. The construction of q_1 rests on linear algebra. The forms $q_1, \ldots, q_{i-1}$ being constructed for some $i \leq g$, let $\mathfrak{p}$ be a prime ideal associated to $(q_1, \ldots, q_{i-1})$ (therefore of rank $i-1$). In order to construct q_i we differentiate q_{i-1} along φ sufficiently to get a form of degree $\ll D$ not in $\mathfrak{p}$. According to the zero estimate, this can be achieved with a derivation of order T bounded above by $T \ll D^{i-1}$. The form q_i is obtained as a general linear combination of the various forms constructed when $\mathfrak{p}$ varies. It is therefore of degree $\ll D$ and satisfies $\mathrm{ord}_\varphi(q_i) \gg D^g$, because $i-1 < g$. One then deduces with a Schwarz lemma that $-\log \|q_i(\theta)\| \gg D^g$.

Then, in a second run, we intersect the variety V containing θ with k general linear combinations of the q_i so that the dimension steps down to 0. We observe that V is smooth (thus, Cohen-Macaulay) in a neighbourhood of θ and that the forms q_i do not vanish simultaneously in this neighbourhood. In this way we get, step by step, algebraic sets $V = V_k, \ldots, V_0$ with V_i pure of dimension i, satisfying $d(V_i) \ll d(V)D^{k-i}$ and $-\log \mathrm{Dist}(\theta, V_i) \gg D^g$, by Bézout theorems (geometric and metric, *see* [16, Chapter 6]). It suffices to set Z a relevant component of V_0 defined over K. □

The above proof rests on the fact that derivations of a section along an analytic subgroup in a commutative algebraic group does not increase the degree of the section. But the height of the section is increased roughly by $O(T\log(T))$ where T is the order of the derivation. In the above proof, it is not clear that one actually needs to differentiate q_{i-1} as much as D^{i-1} times in order to escape from $\mathfrak{p}$. In fact, Bertini's lemma shows that, if at each step we have enough freedom in the choice of q_{i-1}, we can assert that $\mathfrak{p}$ has multiplicity 1 as a component of $(q_1, \ldots, q_{i-1})$. And then a derivation of bounded order would suffice in order to construct q_i. Some intermediate statement may be more at hand (for example not requiring so much freedom but allowing an order of derivation up to D).

A positive answer to the above Question 10, combined with the classical construction-extrapolation in the proofs of transcendency, imply for example a positive answer to Gel'fond-Schneider conjecture. More precisely, one proceeds as follows: construct a polynomial $P \in \mathbf{Z}[Y, X_1, \ldots, X_d]$ of degree D, height $c_1 D^2$, satisfying:

$$\log|P(\theta)| < -c_2 D^{d+1}\log(D).$$

We then consider the cycle Z given by the above Question 10 and one evaluates (noting $t(Z) := h(Z) + d(Z)$)

$$\log|P(Z)| := \sum_{x\in Z}\log|P(x)| \leq -\sum_{x\in Z}(\min(c_2 D^{d+1}\log(D); \log\|\theta - x\|) + c_1 D^2)$$

$$\leq -c_2\min(D^{d+1}\log(D); t(Z)^{(d+1)/k}) + c_3 D^2 t(Z),$$

then, by the size inequality for $P(Z) \in \overline{\boldsymbol{Q}}$,

$$\log|P(Z)| \geq -c_4 D^2 t(Z).$$

Taking $D = \left[\frac{t(Z)^{1/k}}{(\log(t(Z)))^{1/(d+1)}}\right]$ and assuming $t(Z)$ large enough, we get

$$t(Z)^{(d+1)/k}(\log(t(Z)))^{2/(d+1)} \ll t(Z)^{1+2/k},$$

from which follows $k > d - 1$. This allows to conclude that the dimension of an algebraic subvariety of $\boldsymbol{C} \times (\boldsymbol{C}^{\times})^d$ containing $(z, e^z, e^{\beta z} \dots, e^{\beta^{d-1} z})$ is at least $d \dots$ if we have a positive answer to Question 10.

We conclude this note by giving a multiplicity estimate which is useful in the above context:

Lemma 12. *Let* $\omega(W)$ *be the smallest degree of a form vanishing identically on* W*, one has* $\mathrm{ord}_\varphi(W) \ll d(W)\omega(W)^{\dim(W)}$.

Proof. We proceed by recursion on the dimension d of W. The case of dimension 0 is verified because $\mathrm{ord}_\varphi(W)$ is just the multiplicity of the point $\varphi(0)$ as component of W. Let P be a form of degree $\omega(W)$ vanishing on W. A derivative P' of P along φ of bounded order, intersect properly W. Bézout's theorems imply $\mathrm{ord}_\varphi(W \cap \mathcal{Z}(P')) \gg \mathrm{ord}_\varphi(W)$ and $d(W \cap \mathcal{Z}(P')) \ll d(W)\omega(W)$. Assume the case of dimension $d - 1$ is established, for all component Y of $W \cap \mathcal{Z}(P')$ of dimension $d - 1$ ($d = \dim(W)$), one has $\mathrm{ord}_\varphi(Y) \ll d(Y)\omega(Y)^{d-1}$ and $\omega(Y) \le \omega(W)$ (because $Y \subset W$), from which follows

$$\mathrm{ord}_\varphi(W) \ll \mathrm{ord}_\varphi(W \cap \mathcal{Z}(P')) = \sum_Y m_Y \mathrm{ord}_\varphi(Y)$$

$$\ll \sum_Y m_Y d(Y)\omega(Y)^{d-1} \le d(W \cap \mathcal{Z}(P'))\omega(W)^{d-1} \ll d(W)\omega(W)^d. \quad \square$$

References

[1] Y. André, Groupes de Galois motiviques et périodes, Sém. Bourbaki (2016).

[2] A. Baker, *Transcendental Number Theory*, Cambridge Univ. Press, Cambridge (1975); second edition (1990).

[3] C. Bertolin, Periodes de 1-motifs et transcendance, *J. Number Theory*, **97** (2002) 204–221.

[4] F. Beukers, A refined version of the Siegel-Shidlovskii theorem, *Ann. of Math.*, **163** (2006) 369–379.

[5] G. Diaz, Grands degrs de transcendance pour des familles d'exponentielles, *J. Number Theory*, **31**, no. 1, (1989) 1–23.

[6] T. Dreyfus, C. Hardouin and J. Roques, Hypertranscendence of solutions of Mahler equations, *J. Eur. Math. Soc.*, **20** (2018) 2209–2238.

[7] Ch. Hermite, Sur la fonction exponentielle, *C. R. Acad. Sci. Paris*, **77** (1873) 18–24, 74–79, 226–233 & 285–293 = Œuvres III, 150–181.

[8] A. Gel'fond, Sur le septième problème de D. Hilbert, *Bull. Acad. Sci. Math. URSS*, **4(7)** (1934) p. 623.

[9] A. Gel'fond, Sur quelques résultats nouveaux dans la théorie des nombres transcendants, *C.R. Acad. Sci. Paris*, (Juillet 1934), **199**, p. 259.

[10] A. Grothendieck, On the de Rham cohomology of algebraic varieties, *Publ. Math. Inst. Hautes Études Sci.*, **29** (1966) 351–359.

[11] S. Lang, Transcendental Numbers, Addison Wesley, Reading, MA, **4176** (1966).

[12] F. Lindemann, Über die Zahl π, *Math. Ann.*, **20** (1882) 213–225.

[13] J. Liouville, Sur des classes très étendues de quantités dont la valeur n'est ni algébrique, ni même réductible à des irrationnelles algébriques, *J. Math. Pures Appl.*, **1** (1851) 133–142.

[14] K. Mahler, Arithmetisches Eigenschaften einer Klasse Tranzendental-Tranzendenter Funktionen, *Math. Z.*, **32** (1930) 545–585.

[15] M. Mendès-France, Sur les fractions continues limitées, *Acta Arith.*, **23** (1973) 207–215.

[16] Y. V. Nesterenko and P. Philippon (eds), Introduction to algebraic independence theory, *Lecture Notes in Math.*, Spinger, **1752** (2001).

[17] K. Nishioka, Mahler functions and transcendence, *Lecture Notes in Math.*, Springer, **1631** (1996).

[18] P. Philippon, Critères pour l'indépendance algébrique, *Publ. Math. Inst. Hautes Études Sci.*, **64** (1986) 5–52.

[19] P. Philippon, Approximations algébriques des points dans les espaces projectifs, *J. Number. Theory*, **81** (2000) 234–253.

[20] P. Philippon, Approximations fonctionnelles des courbes des espaces projectifs, *Internat. J. Number. Theory*, **7** (2011) 1195–1215.

[21] D. Roy and M. Waldschmidt, Simultaneous approximation and algebraic independence, *The Ramanujan Journal*, **1** (1997) 379–430.

[22] A. B. Shidlovsky, Transcendental Numbers, *Studies in Mathematics*, Walter de Gruyter, **12** (1989).

[23] W. M. Schmidt, Diophantine approximations and diophantine equations, *Lecture Notes in Math.*, Springer Verlag, **1467** (1991).

[24] Th. Schneider, Transzendenzuntersuchungen periodischer Funktionen I & II, *J. Reine Angew. Math.*, **172** (1934) 65–69 & 70–74.

[25] Th. Schneider, Introduction aux nombres transcendants, Gauthier-Villars, Paris (1959).

[26] G. Vallée, Sur la conjecture de Schanuel abélienne, preprint (August 2018), 12p.

[27] M. Waldschmidt, Diophantine approximation on linear algebraic groups, *Grund. Math. Wissen.*, Springer, **326** (2000).

[28] M. Waldschmidt, Elliptic Functions and Transcendence, in Surveys in Number Theory, *Developments in Math.*, Springer Verlag, **17** (2008) 143–188.

[29] K. Weierstrass, Zur Lindemann's Abhandlung: "Über die Ludolph'sche Zahl", *S.B. Preuss. Akad. Wiss.*, (1885), 1067–1085; *Math. Werke* II, 341–362.

[30] U. Zannier, Some applications of Diophantine approximation equations, with special emphasis on the Schmidt subspace theorem, Forum, Università Udine (2003).

Topics in Number Theory, RMS-Lecture Notes Series No. 26, 2020, pp. 203–222.

Relations between Certain Power Series and Functions Involving Zeros of Zeta Functions

M. Ram Murty[1*] and Siddhi Pathak[2†]

[1]Department of Mathematics and Statistics, Queen's University, Kingston, ON Canada K7L 3N6.
e-mail: murty@mast.queensu.ca

[2]Department of Mathematics, Pennsylvania State University, McAllister Building, State College PA 16802, United States of America.
e-mail: siddhi.pathak@psu.edu

Abstract. We study infinite series of the form

$$\sum_{n=1}^{\infty} \frac{A(n)}{B(n)} x^n$$

where $A(t), B(t) \in \mathbb{C}[t]$ are polynomials and $0 < x \leq 1$. We relate these series to other series involving zeros of the Riemann zeta-function. We also discuss functional relations between such power series and the zeros of other zeta-functions.

Keywords. Infinite series, series over zeros of zeta functions, η-coefficients.

2010 Subject Classification: 11M06, 11M26

1. Introduction

In 1735, Euler proved that for $k \in \mathbb{N}$,

$$\zeta(2k) = \sum_{n=1}^{\infty} \frac{1}{n^{2k}} = \frac{(2\pi i)^{2k} B_{2k}}{2(2k)!},$$

where B_k is the k-th Bernoulli number given by the generating function

$$\frac{t}{e^t - 1} = \sum_{k=0}^{\infty} \frac{B_k t^k}{k!}.$$

Thus, the Bernoulli numbers are rational numbers and we conclude that $\zeta(2k) \in \pi^{2k}\mathbb{Q}$. The nature of $\zeta(2k+1)$ however is still shrouded in mystery even though spectacular breakthroughs have been made by Apéry [A] in 1978 who showed

*Research of the first author was supported by an NSERC Discovery grant.
†Research of the second author was supported by an Ontario Graduate Scholarship.

that $\zeta(3) \notin \mathbb{Q}$ and by Rivoal [R] in 2000 who showed that for infinitely many k, $\zeta(2k+1) \notin \mathbb{Q}$.

It is thus natural to inquire whether we can evaluate explicitly a series of the form

$$\sum_{n=1}^{\infty} \frac{A(n)}{B(n)} \tag{1}$$

where $A(t), B(t) \in \mathbb{C}[t]$ are polynomials with $\deg A < \deg B$ and natural conditions are imposed to ensure that the series converges. We may consider more generally power series of the form

$$\sum_{n=1}^{\infty} \frac{A(n)}{B(n)} x^n \tag{2}$$

with $|x| \leq 1$. The goal of this paper is to investigate these series and relate them to series of the form

$$\sum_{\rho} \frac{A(\rho)}{B(\rho)} y^{\rho} \tag{3}$$

where the sum is over non-trivial zeros of the Riemann zeta-function. There is nothing special about the Riemann zeta-function. One could replace it with any other L-function or more generally, a suitable element of the Selberg class. Such a connection was first discovered in a recent paper by S. Gun, M. R. Murty and P. Rath [GMR1] but their focus was on the transcendental nature of such sums. Here, our focus will be more on establishing a curious functional relation between sums of the form (2) and (3).

Returning momentarily to series of the form (1) and (2), we can identify certain cases when these can be evaluated explicitly. For example, if $A(t) \in \overline{\mathbb{Q}}[t]$, $B(t) \in \mathbb{Q}[t]$ where $B(t)$ has simple rational roots, S. D. Adhikari, N. Saradha, T. N. Shorey and R. Tijdeman [ASST] showed that (1) can be written as a linear form in logarithms of algebraic numbers with algebraic coefficients, and so by Baker's theory [B], the sum is transcendental provided it is not zero. They also discussed the transcendence of linear combinations of sums of the form (2) when $x \in \overline{\mathbb{Q}}$ (see Corollary 4.1 of [ASST] as well as Corollary 3.1).

If $B(t)$ does not have simple rational roots, the situation becomes more complicated, as can be inferred by the fact that $\zeta(3)$ or generally $\zeta(2k+1)$ fall into this category. The first serious investigation of such series was initiated by M. R. Murty and C. Weatherby [MW1] as well as S. Gun, M. R. Murty and P. Rath [GMR2]. In [MW1], the authors study (among other things)

$$\sum_{n \in \mathbb{Z}} \frac{A(n)}{B(n)} \tag{4}$$

and derive general results and explicit evaluations. In particular, Euler's evaluation of $\zeta(2k)$ is a special case of their work. A stunning example is given by the following:

$$\sum_{n \in \mathbb{Z}} \frac{1}{An^2 + Bn + C} = \frac{2\pi}{\sqrt{D}} \left(\frac{e^{2\pi\sqrt{D}/A - 1}}{e^{2\pi\sqrt{D}/A} - 2\cos(\pi B/A) e^{\pi\sqrt{D}/A} + 1} \right) \tag{5}$$

is transcendental if $A, B, C \in \mathbb{Z}$ and $-D = B^2 - 4AC < 0$.

More generally, one can evaluate explicitly

$$\sum_{n\in\mathbb{Z}} \frac{1}{(An^2+Bn+C)^k}$$

and deduce transcendence results [MW2]. A critical role is played by a theorem of Nesterenko [N] that states that π and $e^{\pi\sqrt{D}}$ are algebraically independent. Thus, (5) is a transcendental number.

The essential idea animating much of the work in [MW1] and [MW2] is the following. Writing $A(X)/B(X)$ as a partial fraction, (and assuming for now that $B(X)$ has only simple zeros) we are led to sums of the form

$$\sum_{n\in\mathbb{Z}} \frac{1}{n+\alpha_i} \tag{6}$$

where the α_i are roots of $B(X)$. This is $\pi \cot \pi\alpha_i$ deduced from the classical cotangent expression

$$\pi \cot \pi z = \sum_{n\in\mathbb{Z}} \frac{1}{n+z}, \quad z \notin \mathbb{Z}. \tag{7}$$

Of course, we must make some assumptions about the α_i and also understand the convergence in (6) and (7) as a limit:

$$\sum_{n\in\mathbb{Z}} f(n) = \lim_{N\to\infty} \sum_{|n|\le N} f(n).$$

By successive differentiation of (7) one can handle the case when $B(X)$ has multiple roots as well. These considerations lead one to explicit evaluations of series of the form (4). To go further into the study, one needs to invoke some algebraic number theory as well as a celebrated conjecture of Gelfond and Schneider, namely that if α is an algebraic number with $\alpha \neq 0, 1$ and β is an algebraic irrational number of degree d, then the $d-1$ numbers

$$\alpha^{\beta}, \alpha^{\beta^2}, \cdots, \alpha^{\beta^{d-1}} \tag{8}$$

are algebraically independent. A result of Diaz [D] states that the transcendence degree of the field generated by the numbers in (8) over $\overline{\mathbb{Q}}$ is at least $[(d+1)/2]$. When $d = 2$, this is the famous Gelfond-Schneider theorem resolving a problem of Hilbert's list of 23 problems presented at the 1900 congress of mathematics in Paris. The case $d = 3$ was also known earlier and is due to Gelfond. Invoking these results, we can deduce various transcendence theorems. We refer the reader to [MW1] for precise details.

In [PP], the authors consider (1), where the sum is over $n \geq 1$:

$$\sum_{n=1}^{\infty} \frac{A(n)}{B(n)}$$

and (via partial fractions) are led to the study of the series of the form

$$\sum_{n=1}^{\infty} \frac{1}{n+\alpha_i} \tag{9}$$

and more generally

$$\sum_{n=1}^{\infty} \frac{1}{(n+\alpha_i)^k}. \tag{10}$$

The fundamental idea in their work is the recognition that (9) is essentially the digamma function $\Psi(\alpha_i)$ and (10) is related to the k-th derivative $\Psi^{(k)}(\alpha_i)$. More precisely, we have

$$\Psi(z) := \frac{\Gamma'(z)}{\Gamma(z)}$$

and

$$-\Psi(z) = \gamma + \frac{1}{z} + \sum_{n=1}^{\infty} \left(\frac{1}{n+z} - \frac{1}{n} \right)$$

where γ is Euler's constant. The digamma function $\Psi(x)$ appears in the constant term of the Laurent series expansion of the Hurwitz zeta-function at $s = 1$. Recall that for $0 < x \le 1$, the Hurwitz zeta-function

$$\zeta(s, x) = \sum_{n=0}^{\infty} \frac{1}{(n+x)^s}$$

has the expansion:

$$\zeta(s, x) = \frac{1}{s-1} - \Psi(x) + O(s-1).$$

Thus, one can prove without difficulty that

$$\sum_{n=1}^{\infty} \frac{A(n)}{B(n)},$$

where $B(t)$ has simple zeros $\alpha_1, \alpha_2, \ldots, \alpha_r$ (say), is essentially a linear combination of $\Psi(\alpha_i)$ (see Theorem 10 of [MS]). If the α_i are rational numbers, a classical theorem of Gauss discovered in 1813 shows that for $(a, q) = 1$,

$$\Psi\left(\frac{a}{q}\right) = -\gamma - \log 2q - \frac{\pi}{2} \cot \frac{\pi a}{q} + 2 \sum_{0<j\le q/2} \cos \frac{2\pi a j}{q} \left(\log \sin \frac{\pi j}{q} \right), \tag{11}$$

see for example [MS, pg. 300]. If however the zeros are neither simple, nor rational then there are considerable difficulties in evaluating in “closed form” the value of the sum and in ascertaining its algebraic or transcendental nature. For instance, if the roots of $B(t)$ are rational, but not simple, the value of the sum can be given as a linear combination of special values of the Hurwitz zeta-function at rational arguments.

In [GMR2], the authors used the Chowla-Milnor conjecture regarding the $\mathbb{Q}$-linear independence of

$$\zeta\left(k, \frac{a}{q}\right) \; 1 \le a < q, \;\; (a, q) = 1.$$

The nature of the Hurwitz zeta-function at irrational arguments is unknown and (to our knowledge) there has been scant attention given to such questions.

In this paper, we offer a new perspective on sums of the form (1) and (2) and relate such a study to cognate sums involving the zeros of the Riemann zeta-function. As will be explained below, one could replace the Riemann zeta-function by any L-function or more generally by an element of the Selberg class. To keep the prerequisites of this paper to a minimum, we do not do this here but indicate in our concluding remarks what needs to be modified and what can be expected.

Such sums involving zeros of the Riemann zeta-function are intricately connected to the Laurent series expansion of its logarithmic derivative. A case in point is Li's criterion for the Riemann hypothesis obtained by X.-J. Li [Li] in 1997. More specifically, let

$$\lambda_n := \sum_{\rho} \left(1 - \left(1 - \frac{1}{\rho}\right)^n\right),$$

where the sum is over non-trivial zeros of the Riemann zeta-function. Then the Riemann hypothesis is equivalent to the positivity of λ_n for all $n \in \mathbb{N}$. Furthermore, if

$$-\frac{\zeta'}{\zeta}(s) = \frac{1}{s-1} + \sum_{j=0}^{\infty} \eta_j (s-1)^j, \tag{12}$$

then it was shown in [BL] that

$$\lambda_n = -\sum_{j=1}^{n} \left[\binom{n}{j} \eta_{j-1}\right] + 1 - (\log 4\pi + \gamma)\frac{n}{2} + \sum_{j=2}^{n} (-1)^j \binom{n}{j} (1 - 2^{-j}) \zeta(j). \tag{13}$$

The study of η_j's is highly important for a variety of reasons. They enter into our understanding of Li's criterion for the Riemann hypothesis to hold as expressed by the formula (13) above. In this context, Coffey [Co] writes

$$\lambda_n = 1 - \frac{n}{2}(\gamma + \log 4\pi) + S_1(n) + S_2(n),$$

where

$$S_1(n) = \sum_{j=2}^{n} (-1)^j \binom{n}{j} \left(1 - \frac{1}{2^j}\right) \zeta(j)$$

and

$$S_2(n) = -\sum_{j=1}^{n} \binom{n}{j} \eta_{j-1},$$

where η_j's are as defined in (12). He shows that for $n \geq 2$,

$$\frac{1}{2}(n(\log n + \gamma - 1) + 1) \leq S_1(n) \leq \frac{1}{2}(n(\log n + \gamma + 1) - 1),$$

so that

$$\lambda_n = \frac{1}{2}\, n \log n + S_2(n) + O(n).$$

Now, Bombieri and Lagarias [BL] have shown that to deduce the Riemann hypothesis, it suffices to show that for any $\epsilon > 0$, there is a constant $c(\epsilon) > 0$ such that

$$\lambda_n \geq -c(\epsilon) e^{\epsilon n},$$

for every $n \geq 1$. In other words, the Riemann hypothesis can be deduced from a good estimate for $S_2(n)$ involving the η_j's.

A generalized version of the η_j-coefficients appear in our analysis of sums of the form (3). In particular, let s_0 be a pole of logarithmic derivative of the Riemann zeta-function, i.e, $s_0 = 1, -2n$ for some $n \in \mathbb{N}$ or ρ for a non-trivial zero ρ of $\zeta(s)$. We define the *generalized η_j-coefficients* by

$$-\frac{\zeta'}{\zeta}(s) = \frac{R(s_0)}{s - s_0} + \sum_{j=0}^{\infty} \eta_j(s_0)\,(s - s_0)^j, \tag{14}$$

where $R(s_0)$ is the residue at $s = s_0$ of $-\zeta'/\zeta$. It is easy to see that $R(s_0) = 1$ if $s_0 = 1$ and $R(s_0) = -1$ if $s_0 = -2n$ for some $n \in \mathbb{N}$. If $s_0 = \rho$ for some non-trivial zero ρ of the Riemann zeta-function, $-R(\rho)$ is simply the order of the zero ρ and there is a folklore conjecture that the non-trivial zeros of $\zeta(s)$ are simple and thus, $R(\rho) = -1$. When $s_0 = 1$, these are the classical η-coefficients defined by Laurent series expansion of $-\,\zeta'/\zeta$ around $s = 1$ as given in (12). These generalized η-coefficients enter into formulas stated in Theorem 1.3 below in a fundamental way if $B(t)$ has a simple zero at s_0 which also happens to be either 1 or a zero of $\zeta(s)$. In order to understand these coefficients concretely, we derive an integral representation and a limit formula for these constants in a more general setting.

Proposition 1.1. *Let*

$$f(s) := \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

be a Dirichlet series, absolutely convergent on $\Re(s) > 1$. Suppose that for any $A > 0$,

$$S(x) := \sum_{n \leq x} a_n = \delta x + E(x), \tag{15}$$

for some $\delta \in \mathbb{R}$ and

$$E(x) = O\left(\frac{x}{(\log x)^A}\right). \tag{16}$$

Then, by partial summation, $f(s)$ can be analytically continued to $\Re(s) \geq 1$, with a possible simple pole at $s = 1$ and one can write its Laurent series expansion around $s = 1$ as

$$f(s) = \frac{\delta}{s-1} + \sum_{j=0}^{\infty} \eta_j(1, f)(s-1)^j.$$

Then,

$$\eta_0(1, f) = \delta + \int_1^{\infty} \frac{E(t)}{t^2}\, dt,$$

and for $j \geq 1$,

$$\eta_j(1, f) = \frac{(-1)^j}{j!} \int_1^{\infty} \frac{E(t)}{t^2} \left((\log t)^j - j(\log t)^{j-1} \right) dt. \tag{17}$$

Further, for $j \geq 1$,

$$\eta_j(1, f) = \frac{(-1)^j}{j!} \left\{ \lim_{x\to\infty} \left[\sum_{n\leq x} \frac{a_n (\log n)^j}{n} \right] - \delta\, \frac{(\log x)^{j+1}}{j+1} \right\}.$$

Thus, the generalized η_j-coefficients defined in the context of $-\zeta'/\zeta$ by (14) are nothing but $\eta_j(s_0) := \eta_j(s_0, -\zeta'/\zeta)$ in the above notation.

On the other hand, the constants $\eta_j(1, \zeta)$ (known as Stieltjes constants) were first introduced by Stieltjes (see [Na, pg. 161]), who proved that

$$\eta_j(1, \zeta) = \frac{(-1)^j}{j!} \left\{ \lim_{x\to\infty} \left[\sum_{n\leq x} \frac{(\log n)^j}{n} \right] - \frac{(\log x)^{j+1}}{j+1} \right\},$$

in a letter to Hermite in 1885. This formula seems to have been rediscovered by Briggs and Chowla in 1955 (see [Na, pg. 163]). Clearly, this result can be stated in a more general setting, as is seen in Proposition 1.1.

Since this paper focuses on the logarithmic derivative of the Riemann zeta-function, we will use $\eta_j(s_0)$ for $\eta_j(s_0, -\zeta'/\zeta)$ and η_j for $\eta_j(1, -\zeta'/\zeta)$ to simplify notation. For the sake of clarity, we state the special case for $f(s) = -\zeta'/\zeta(s)$ separately below.

Proposition 1.2. *Let η_j be as defined in* (12). *Let $\Lambda(n)$ denote the von-Mangoldt function defined by*

$$\Lambda(n) = \begin{cases} \log p & \text{if } n = p^{\alpha},\ \alpha \geq 1, \\ 0 & \text{otherwise.} \end{cases} \tag{18}$$

Then, for $j \geq 1$,

$$\eta_j = \frac{(-1)^j}{j!} \left\{ \lim_{x\to\infty} \left[\sum_{n\leq x} \frac{\Lambda(n)(\log n)^j}{n} \right] - \frac{(\log x)^{j+1}}{j+1} \right\}.$$

The main theorem of this paper is the following.

Theorem 1.3. *Let $x > 1$ and $A(t)$, $B(t) \in \mathbb{C}[t]$ with $B(t)$ having simple zeros, α_1, $\alpha_2, \ldots \alpha_r$. First suppose that none of the α_i equal 1, a non-trivial zero of $\zeta(s)$ or $-2n$ ($n \in \mathbb{N}$).*

Then, if x is not a prime power,

$$\sum_{\rho} \frac{A(\rho)}{B(\rho)} x^{\rho} + \sum_{n=1}^{\infty} \frac{A(-2n)}{B(-2n)} \left(\frac{1}{x}\right)^{2n} - \frac{xA(1)}{B(1)}$$

$$= -\sum_{i} \lambda_i x^{\alpha_i} \left(\sum_{n \le x} \frac{\Lambda(n)}{n^{\alpha_i}} \right) - \sum_{i} \lambda_i x^{\alpha_i} \frac{\zeta'}{\zeta}(\alpha_i), \tag{19}$$

where

$$\frac{A(t)}{B(t)} = \sum_{i} \frac{\lambda_i}{t - \alpha_i}.$$

Now, suppose $\alpha_1 = \rho_0$, a non-trivial zero of $\zeta(s)$ and none of the α_j, $2 \le j \le r$ are equal to 1, ρ or $-2n$. Then,

$$\sum_{\rho \neq \rho_0} \frac{A(\rho)}{B(\rho)} x^{\rho} + \sum_{n=1}^{\infty} \frac{A(-2n)}{B(-2n)} \left(\frac{1}{x}\right)^{2n} - \frac{xA(1)}{B(1)}$$

$$= -\sum_{i} \lambda_i x^{\alpha_i} \left(\sum_{n \le x} \frac{\Lambda(n)}{n^{\alpha_i}} \right) - \sum_{i \neq 1} \lambda_i x^{\alpha_i} \frac{\zeta'}{\zeta}(\alpha_i)$$

$$- x^{\rho_0} \left(\sum_{i \neq 1} \frac{\lambda_i \, x^{\alpha_i}}{\rho_0 - \alpha_i} \right) + \lambda_1 \, x^{\rho_0} \;\; \eta_0(\rho_0) + \lambda_1 x^{\rho_0} \log x. \tag{20}$$

Similarly, if $\alpha_1 = -2m$ for some $m \in \mathbb{N}$ and none of the α_j, $2 \le j \le r$ are equal to 1, ρ or $-2n$, then,

$$\sum_{\rho} \frac{A(\rho)}{B(\rho)} x^{\rho} + \sum_{\substack{n=1, \\ n \neq m}}^{\infty} \frac{A(-2n)}{B(-2n)} \left(\frac{1}{x}\right)^{2n} - \frac{xA(1)}{B(1)}$$

$$= -\sum_{i} \lambda_i x^{\alpha_i} \left(\sum_{n \le x} \frac{\Lambda(n)}{n^{\alpha_i}} \right) - \sum_{i \neq 1} \lambda_i x^{\alpha_i} \frac{\zeta'}{\zeta}(\alpha_i)$$

$$+ x^{-2m} \left(\sum_{i \neq 1} \frac{\lambda_i x^{\alpha_i}}{2m + \alpha_i} \right) + \lambda_1 \, x^{-2m} \;\; \eta_0(-2m) + \lambda_1 x^{-2m} \log x, \tag{21}$$

and when $\alpha_1 = 1$ *and none of the* α_j, $2 \le j \le r$ *are equal to* 1, ρ *or* $-2n$, *then,*

$$\sum_{\rho} \frac{A(\rho)}{B(\rho)} x^{\rho} + \sum_{n=1}^{\infty} \frac{A(-2n)}{B(-2n)} \left(\frac{1}{x}\right)^{2n} - x \sum_{i \neq 1} \frac{\lambda_i}{1-\alpha_i}$$

$$= -\sum_{i} \lambda_i x^{\alpha_i} \left(\sum_{n \le x} \frac{\Lambda(n)}{n^{\alpha_i}} \right) - \sum_{i \neq 1} \lambda_i x^{\alpha_i} \frac{\zeta'}{\zeta}(\alpha_i) + \lambda_1 \, x \, \eta_0(1) + \lambda_1 \, x \log x. \quad (22)$$

Generally, if $B(t)$ *has a subset of zeros which are equal to* 1 *or a zero of* $\zeta(s)$, *one modifies* (19) *in the appropriate way.*

If x *is a prime power, then the sum*

$$\sum_{n \le x} \frac{\Lambda(n)}{n^{\alpha_i}}$$

on the right hand side of (19), (20), (21) *and* (22) *is replaced by*

$$\sum_{n < x} \frac{\Lambda(n)}{n^{\alpha_i}} + \frac{1}{2} \frac{\Lambda(x)}{x^{\alpha_i}}.$$

2. Preliminaries

In our discussion, a fundamental role is played by:

Lemma 2.1. *If* $x > 1$, $x \neq p^m$ *(*p *prime) then*

$$\sum_{n \le x} \frac{\Lambda(n)}{n^s} = -\frac{\zeta'}{\zeta}(s) + \frac{x^{1-s}}{1-s} - \sum_{\rho} \frac{x^{\rho-s}}{\rho-s} + \sum_{n=1}^{\infty} \frac{x^{-2n-s}}{2n+s}, \quad (23)$$

provided $s \neq 1$, $s \neq \rho$, $s \neq -2n$ *for any* $n \in \mathbb{N}$.

If $s = 1$, *a non-trivial zero* ρ_0 *of* $\zeta(s)$ *or* $-2m$ *for some* $m \in \mathbb{N}$, *then the right hand side of* (23) *should be replaced by*

$$\eta_0(1) + \log x - \sum_{\rho} \frac{x^{\rho-1}}{\rho-1} + \sum_{n=1}^{\infty} \frac{x^{-2n-1}}{2n+1},$$

or

$$\eta_0(\rho_0) + \log x + \frac{x^{1-\rho_0}}{1-\rho_0} - \sum_{\rho \neq \rho_0} \frac{x^{\rho-\rho_0}}{\rho-\rho_0} + \sum_{n=1}^{\infty} \frac{x^{-2n-\rho_0}}{2n+\rho_0},$$

or

$$\eta_0(-2m) + \log x + \frac{x^{1+2m}}{1+2m} - \sum_{\rho} \frac{x^{\rho+2m}}{\rho+2m} + \sum_{\substack{n=1,\\ n \neq m}}^{\infty} \frac{x^{-2n+2m}}{2n-2m},$$

respectively.

If $x = p^m$, *the left hand side must be corrected by the term* $\Lambda(x)/2$.

Proof. This follows by the standard method of contour integration. The statement of the first part is found in several places (e.g. [IK, pg. 566] where we caution the reader that there is a typo in (25.21) in which the second "=" symbol on the right hand side should be a minus sign). Since no proof is available in the English language, we now give it.

We use Perron's formula in the following form [T, pg. 60]. Let

$$f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}, \quad \sigma = \Re(s) > 1,$$

where $a_n = O(\Phi(n))$, $\Phi(n)$ is increasing and assume

$$\sum_{n=1}^{\infty} \frac{|a_n|}{n^\sigma} = O\left(\frac{1}{(1-\sigma)^\alpha}\right)$$

for some $\alpha \geq 0$, as $\sigma \to 1^+$. If $c > 0$ and $\sigma + c > 1$, x is not an integer and N is the nearest integer to x, we have

$$\sum_{n \leq x} \frac{a_n}{n^s} = \frac{1}{2\pi i} \int_{c-iT}^{c+iT} f(s+w) \frac{x^w}{w}\, dw + O\left(\frac{x^c}{T(\sigma+c-1)^\alpha}\right) + O\left(\frac{\Phi(2x) x^{1-\sigma} \log x}{T}\right) + O\left(\frac{\Phi(N) x^{1-\sigma}}{T|x-N|}\right).$$

If x is an integer, then

$$\sum_{n=1}^{x-1} \frac{a_n}{n^s} + \frac{a_x}{2x^s} = \frac{1}{2\pi i} \int_{c-iT}^{c+iT} f(s+w) \frac{x^w}{w}\, dw + O\left(\frac{x^c}{T(\sigma+c-1)^\alpha}\right) + O\left(\frac{\Phi(2x) x^{1-\sigma} \log x}{T}\right) + O\left(\frac{\Phi(x) x^{-\sigma}}{T}\right),$$

for any $T > 0$. We apply this to

$$-\frac{\zeta'}{\zeta}(s) = \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s}.$$

Since $\Lambda(n)$ is supported on prime powers, we deduce

$$\sum_{n \leq x} \frac{\Lambda(n)}{n^s} = \frac{1}{2\pi i} \int_{c-iT}^{c+iT} \left(-\frac{\zeta'}{\zeta}(s+w)\right) \frac{x^w}{w}\, dw + O\left(\frac{x^c}{T(\sigma+c-1)^\alpha}\right) + O\left(\frac{x^{1-\sigma} \log^2 x}{T}\right) + O\left(\frac{\log(N)\, x^{1-\sigma}}{T|x-N|}\right)$$

if x is not a prime power, whereas if x is a prime power, the last term is replaced by

$$O\left(\frac{x^{-\sigma}\log x}{T}\right).$$

Here c is chosen so that $c+\sigma>1$.

The integral is evaluated using Cauchy's residue theorem as follows. If R denotes the oriented rectangle with vertices $c-iT$, $c+iT$, $-U+iT$ and $-U-iT$, with U large and unequal to an integer, then by the residue theorem,

$$\frac{1}{2\pi i}\int_R\left(-\frac{\zeta'}{\zeta}(s+w)\right)\frac{x^w}{w}\,dw=-\frac{\zeta'}{\zeta}(s)+\frac{x^{1-s}}{1-s}-\sum_\rho\frac{x^{\rho-s}}{\rho-s}+\sum_{n=1}^{U}\frac{x^{-2n-s}}{2n+s}$$

because

$$-\frac{\zeta'}{\zeta}(s+w)\,\frac{x^w}{w}$$

has poles at $w=0,\ 1-s,\ \rho-s$ and $-2n-s$ with $|\Im(\rho)|\le T$ and $n\le U$ in the rectangle R. We want to let $T, U\to\infty$ but before we do that, we need to estimate the line integrals along the other three edges of the rectangle. Of course, we must choose T so that it is not the ordinate of a zero of $\zeta(s)$. But these estimates are quite standard (see [Mu, Exercise 7.2.4]).

The key point is to know for this suitable choice of T, we have

$$\left|-\frac{\zeta'}{\zeta}(s+w)\right|=O(\log^2 T)$$

which leads to the final estimate of

$$O\left(\frac{x^c\log^2 T}{T\log x}\right)$$

for the horizontal line integrals. For the vertical line integral, we have an estimate of

$$O\left(\frac{\log U}{U}\cdot\frac{T}{x^T}\right)$$

as seen in [Mu, pg. 392]. We let $U\to\infty$ first and then let $T\to\infty$ to deduce the final result. This completes the proof of Lemma 2.1 if $s\ne 1$, ρ or $-2n$ for $n\in\mathbb{N}$.

If $s=1$, ρ_0 or $-2m$ for some $m\in\mathbb{N}$, we take limits of both sides as $s\to 1$, ρ_0 or $-2m$. We illustrate this using the case of $s=1$ since the analysis for $s=\rho_0$ or $-2m$ is similar. Taking the limit of right-hand side of (23) as $s\to 1$, we obtain

$$-\sum_\rho\frac{x^{\rho-1}}{\rho-1}+\sum_{n=1}^{\infty}\frac{x^{-2n-1}}{2n+1}+\lim_{s\to 1}\left(\frac{x^{1-s}}{1-s}-\frac{\zeta'}{\zeta}(s)\right).$$

Now, using (14) at $s_0 = 1$, $R(s_0) = 1$ and

$$\frac{x^{1-s}}{1-s} = \frac{-1}{s-1} + \log x + O(1-s),$$

we see that the limit evaluates to $\eta_0(1) + \log x$ and thus, Lemma 2.1 is proved. □

Incidentally, $\eta_0(1) = -\gamma$ and this is not difficult to see because

$$\zeta(s) = \frac{1}{s-1} + \gamma + O(s-1).$$

3. Proofs of the Propositions

In this section, we give proofs of the Propositions in Section 1.

3.1 *Proof of Proposition 1.1*

Let

$$f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}.$$

Then the usual partial summation method gives,

$$\begin{aligned} f(s) &= s\int_1^\infty \frac{S(x)}{x^{s+1}}\,dx \\ &= \frac{\delta s}{s-1} + s\int_1^\infty \frac{S(x)-\delta x}{x^{s+1}}\,dx. \end{aligned}$$

By our hypothesis, the integral on the right hand side converges absolutely for $\Re(s) \geq 1$. Thus, we can derive the Laurent expansion at $s = 1$ using this integral. Writing $E(x) = S(x) - \delta x$, we find

$$\begin{aligned} s\int_1^\infty \frac{E(x)}{x^{s+1}}\,dx &= ((s-1)+1)\int_1^\infty \frac{E(x)}{x^2}\sum_{j=0}^{\infty}\frac{(-1)^j\,(\log x)^j}{j!}\,(s-1)^j\,dx \\ &= \int_1^\infty \frac{E(x)}{x^2}\sum_{j=0}^{\infty}\frac{(-1)^j\,(\log x)^j}{j!}(s-1)^{j+1}\,dx \\ &\quad + \int_1^\infty \frac{E(x)}{x^2}\sum_{j=0}^{\infty}\frac{(-1)^j\,(\log x)^j}{j!}\,(s-1)^j\,dx \\ &= \int_1^\infty \frac{E(x)}{x^2}\,dx \\ &\quad + \sum_{j=1}^{\infty}\frac{(-1)^j}{j!}\,(s-1)^j\int_1^\infty \frac{E(x)}{x^2}\left((\log x)^j - j(\log x)^{j-1}\right)dx, \end{aligned}$$

the interchange of summation and integral being justified by the absolute convergence of the integral at $s = 1$. Thus, we see that an integral representation for the Laurent series coefficients at $s = 1$ of a general Dirichlet series can be obtained.

On the other hand, analysis with the help of partial summation gives

$$\sum_{n\le x} \frac{a_n (\log n)^j}{n} = \frac{S(x)\,(\log x)^j}{x} + \int_1^x \frac{S(t)}{t^2}\left((\log t)^j - j(\log t)^{j-1}\right)\,dt$$

$$= \frac{S(x)\,(\log x)^j}{x} + \delta\int_1^x \frac{(\log t)^j}{t}\,dt - j\,\delta\int_1^x \frac{(\log t)^{j-1}}{t}\,dt$$

$$+ \int_1^x \frac{E(t)}{t^2}\left((\log t)^j - j(\log t)^{j-1}\right)\,dt,$$

by (15). Hence, we deduce that

$$\sum_{n\le x} \frac{a_n (\log n)^j}{n} = \delta\,\frac{(\log x)^{j+1}}{j+1} + \int_1^\infty \frac{E(t)}{t^2}\left((\log t)^j - j(\log t)^{j-1}\right)\,dt$$

$$+ \left(\frac{S(x)\,(\log x)^j}{x} - \delta\,(\log x)^j\right) + \mathcal{E}(x),$$

where

$$\mathcal{E}(x) = \int_x^\infty \frac{E(t)}{t^2}\left((\log t)^j - j(\log t)^{j-1}\right)\,dt.$$

Note that $\mathcal{E}(x)$ is the tail of a convergent integral by (16) and since $j \ge 1$ and therefore, tends to zero as $x \to \infty$. Moreover, the third term on the right hand side also goes to zero as $x \to \infty$ by (15). On comparison with (17), the proposition is proved.

3.2 *Proof of Proposition 1.2*

Let $\Lambda(n)$ denote the von-Mangoldt function given by (18). Recall that

$$-\frac{\zeta'}{\zeta}(s) = \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s},$$

for $\Re(s) > 1$ and that

$$-\frac{\zeta'}{\zeta}(s) = \frac{1}{s-1} + \sum_{j=0}^{\infty} \eta_j (s-1)^j.$$

Let

$$\psi(x) := \sum_{n\le x} \Lambda(n).$$

Then the prime number theorem (see [Mu, Theorem 4.2.9]) gives

$$\psi(x) = x + E(x),$$

with

$$E(x) = O\left(x \exp\left(-c\ (\log x)^{1/10}\right)\right),$$

for some positive constant c. Thus, we can apply Proposition 1.1 to obtain the result.

4. Proof of the Main Theorem

First suppose that x is not a prime power. Without loss of generality, we may assume that $B(t)$ is monic. For the moment, we suppose that $B(t)$ has only simple zeros and none of which are equal to a non-trivial zero or a pole of the Riemann zeta-function, or $-2n$ for some natural number n. We write using partial fractions

$$\frac{A(t)}{B(t)} = \sum_i \frac{\lambda_i}{t - \alpha_i} \tag{24}$$

where $\lambda_i = A(\alpha_i)/B'(\alpha_i)$. Then

$$\sum_\rho \frac{A(\rho)}{B(\rho)} x^\rho = \sum_i \lambda_i \left(\sum_\rho \frac{x^\rho}{\rho - \alpha_i}\right).$$

We analyze the inner sum using the lemma: by (23),

$$\sum_\rho \frac{x^{\rho-\alpha}}{\rho - \alpha} = -\frac{\zeta'}{\zeta}(\alpha) + \frac{x^{1-\alpha}}{1-\alpha} + \sum_{n=1}^\infty \frac{x^{-2n-\alpha}}{2n+\alpha} - \sum_{n \le x} \frac{\Lambda(n)}{n^\alpha}.$$

We put $\alpha = \alpha_i$, multiply by $\lambda_i x^{\alpha_i}$ and sum over the i to get

$$\sum_\rho \frac{A(\rho)}{B(\rho)} x^\rho = -\sum_i \lambda_i x^{\alpha_i} \frac{\zeta'}{\zeta}(\alpha_i) + \frac{xA(1)}{B(1)} - \sum_i \lambda_i x^{\alpha_i} \left(\sum_{n \le x} \frac{\Lambda(n)}{n^{\alpha_i}}\right)$$
$$+ \sum_{n=1}^\infty x^{-2n} \left(\sum_i \frac{\lambda_i}{2n + \alpha_i}\right).$$

Note that using (24),

$$\sum_i \frac{\lambda_i}{2n + \alpha_i} = -\frac{A(-2n)}{B(-2n)}.$$

This proves that

$$\sum_\rho \frac{A(\rho)}{B(\rho)} x^\rho + \sum_{n=1}^\infty \frac{A(-2n)}{B(-2n)} \left(\frac{1}{x}\right)^{2n}$$
$$= \frac{xA(1)}{B(1)} - \sum_i \lambda_i x^{\alpha_i} \left(\sum_{n \le x} \frac{\Lambda(n)}{n^{\alpha_i}}\right) - \sum_i \lambda_i x^{\alpha_i} \frac{\zeta'}{\zeta}(\alpha_i).$$

An appropriate modification gives the case when x is a prime power where we need to add

$$\frac{1}{2}\,\Lambda(x)\left(\sum_i \lambda_i\right).$$

If we assume that deg $A \leq$ deg $B - 2$, then one can deduce from the partial fraction decomposition of $A(X)/B(X)$ that $\sum_i \lambda_i = 0$.

Finally, when $B(t)$ has a zero at 1, ρ_0 or $-2m$, the terms in the summation have to be adjusted appropriately. Since the analysis of the three cases is identical, we demonstrate this in the case $\alpha_1 = 1$, α_j is not 1, ρ or $-2n$ for $j = 2, \ldots, r$. For x not a prime power, Lemma 2.1 gives

$$\sum_\rho \frac{x^{\rho-1}}{\rho - 1} = \eta_0(1) + \log x + \sum_{n=1}^{\infty} \frac{x^{-2n-1}}{2n+1} - \sum_{n \leq x} \frac{\Lambda(n)}{n}.$$

Thus, modifying the previous argument for α_1 as above, we get

$$\sum_\rho \frac{A(\rho)}{B(\rho)}\,x^\rho + \sum_{n=1}^{\infty} \frac{A(-2n)}{B(-2n)}\left(\frac{1}{x}\right)^{2n} - x \sum_{i \neq 1} \frac{\lambda_i}{1 - \alpha_i}$$
$$= -\sum_i \lambda_i x^{\alpha_i}\left(\sum_{n \leq x} \frac{\Lambda(n)}{n^{\alpha_i}}\right) - \sum_{i \neq 1} \lambda_i x^{\alpha_i}\,\frac{\zeta'}{\zeta}(\alpha_i) + \lambda_1 x \eta_0(1) + \lambda_1\, x \log x.$$

This completes proof of the main theorem.

5. Connections with other L-series

As noted in [GMR1], our study of series of the form (3) can be expanded to the realm of the Selberg class. Before amplifying the general setting, let us focus on two specific cases.

If χ is a non-principal Dirichlet character mod q which is even (that is $\chi(-1) = 1$), then our earlier discussion extends mutatis mutandis to this case also with only one minor modification. Since $L(s,\chi)$ does not have a pole at $s = 1$, the analog of Lemma 2.1 becomes

$$\sum_{n \leq x} \frac{\Lambda(n)\chi(n)}{n^s} = -\frac{L'}{L}(s,\chi) - \sum_\rho \frac{x^{\rho - s}}{\rho - s} + \sum_{n=1}^{\infty} \frac{x^{-2n-s}}{2n+s} \tag{25}$$

where the second sum on the right hand side is over the non-trivial zeros of $L(s,\chi)$. Our main theorem modified to deal with this case becomes

$$\sum_\rho \frac{A(\rho)}{B(\rho)}\,x^\rho + \sum_{n=1}^{\infty} \frac{A(-2n)}{B(-2n)}\left(\frac{1}{x}\right)^{2n}$$
$$= -\sum_i \lambda_i x^{\alpha_i}\left(\sum_{n \leq x} \frac{\Lambda(n)\chi(n)}{n^{\alpha_i}}\right) - \sum_i \lambda_i x^{\alpha_i}\,\frac{L'}{L}(\alpha_i,\chi),$$

if x is not a prime power. As noted earlier, if x is a prime power, the sum

$$\sum_{n\le x}\frac{\Lambda(n)\chi(n)}{n^s}$$

must be replaced by

$$\sum_{n<x}\frac{\Lambda(n)\chi(n)}{n^{\alpha_i}}+\frac{1}{2}\frac{\Lambda(x)}{x^{\alpha_i}}\chi(x).$$

Since the method of contour integration employed in the proof of Lemma 2.1 goes through with little change, we leave the details to the reader.

If χ is an odd character, the analogous derivation needs some modification but only in one step. The trivial zeros of $L(s,\chi)$ are now at the negative odd integers $-1,-3,-5,\ldots$ so that the last term on the right hand side of (25) changes to

$$\sum_{n=0}^{\infty}\frac{x^{-2n-1-s}}{2n+1+s}$$

and the analog of Theorem 1.3 becomes

$$\sum_{\rho}\frac{A(\rho)}{B(\rho)}x^{\rho}+\sum_{n=1}^{\infty}\frac{A(-2n-1)}{B(-2n-1)}\left(\frac{1}{x}\right)^{2n+1}$$
$$=-\sum_{i}\lambda_i x^{\alpha_i}\left(\sum_{n\le x}\frac{\Lambda(n)\chi(n)}{n^{\alpha_i}}\right)-\sum_{i}\lambda_i x^{\alpha_i}\frac{L'}{L}(\alpha_i,\chi),$$

for $x>1$, x not a prime power. If x is a prime power, we need to make the same modification as we made earlier.

These theorems extend smoothly to elements of the Selberg class. We will not adumbrate the properties of this class here, but refer the reader to the exposition in [GMR1] where the authors study sums of the form

$$\sum_{\rho}\frac{A(\rho)}{B(\rho)}x^{\rho}$$

when ρ runs over the non-trivial zeros of a fixed element F of the Selberg class. The essential point to note is that the nature of the second term in the appropriate analogue of (25) is determined by the trivial zeros of $F(s)$. These sums will often not be of the form

$$\sum_{n=1}^{\infty}\frac{A(-2n)}{B(-2n)}\left(\frac{1}{x}\right)^{2n},\ \sum_{n=1}^{\infty}\frac{A(-2n-1)}{B(-2n-1)}\left(\frac{1}{x}\right)^{2n+1}\ \text{or}\ \sum_{n=1}^{\infty}\frac{A(-n)}{B(-n)}\left(\frac{1}{x}\right)^{n}\qquad(26)$$

because these terms are determined by the nature of Γ-factors in the functional equation of $F(s)$. Only in special cases does the second term on the left-hand side of the analogue of (25) take such a simple form. For instance, if the Γ-factor in the functional equation is

$$\Gamma\left(\frac{s}{2}\right),\ \Gamma\left(\frac{s+1}{2}\right) \text{ or } \Gamma(s),$$

then the second term on the left-hand side is one of the expressions in (26) respectively.

We have already seen the first two cases of these Γ-factors arising in the case of $L(s,\chi)$ with χ even or odd. The case of $\Gamma(s)$ emerges if $F(s)$ is the L-function attached to a Hecke eigenform. This case leads to an expression of the form

$$\sum_{n=1}^{\infty} \frac{A(-n)}{B(-n)} \left(\frac{1}{x}\right)^n .$$

In these formulas, we have assumed that $x > 1$. One could analyze the case $x \to 1^+$ and derive corresponding results.

As noticed in [GMR1], one can investigate the case $0 < x < 1$ of the series

$$\sum_{\rho} \frac{A(\rho)}{B(\rho)} x^{\rho}$$

in a similar manner. By the method used in the proof of Lemma 2.1, one can show that if $s \neq 0, 1, 3, 5, \ldots$ and $1/x$ is not a prime power, then

$$\sum_{n \le 1/x} \frac{\Lambda(n)}{n^{1-s}} = -\frac{\zeta'}{\zeta}(1-s) + \frac{x^{-s}}{s} + \sum_{\rho} \frac{x^{\rho-s}}{\rho-s} + \sum_{n=1}^{\infty} \frac{x^{2n+1-s}}{2n+1-s}.$$

An appropriate adjustment of the left hand side is needed if $1/x$ is a prime power. Clearly, similar results can be derived for elements of the Selberg class.

What these results suggest is a method (perhaps) to analyze relations that may exist among special values of logarithmic derivative of the Riemann zeta function. If we consider (say) $L(s,\chi)$ with χ even, then one could explore any rational linear combination of special values of the logarithmic derivatives of $L(s,\chi)$ as χ varies. These investigations we relegate to a future occasion.

6. Concluding Remarks

Our study here opens a new line of investigation regarding on the one hand sums of the form (1) and generally (2) relating them to sums of the form (3) expressing a functional relation. On the other hand, this relation involves linear forms in logarithms as well as the η_j-coefficients of a general kind.

Scattered throughout the literature are various (seemingly unrelated) investigations and it is hoped that these disparate researches can be brought into a cohesive unity that will illuminate our understanding about these sums and perhaps shed some light on the Riemann hypothesis.

To give one example of related results in the literature, we state here a fascinating formula found by Ihara, Murty and Shimura [IMS].

Let K be an algebraic number field and write

$$\zeta_K(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

for its Dedekind zeta function. Let χ be a primitive Dirichlet character. Modifying the (confusing) notation of [IMS], we define

$$L_K(s,\chi) = \sum_{n=1}^{\infty} \frac{a_n \chi(n)}{n^s}.$$

It is well-known that $L_K(s,\chi)$ extends to an entire function if $\chi \neq \chi_0$, the principal character. Define γ_K to be the constant term divided by the residue of the Laurent expansion of $\zeta_K(s)$ at $s = 1$. Set

$$\gamma^*_{K,\chi} = \begin{cases} \gamma_K + 1, & \text{if } \chi = \chi_0, \\ \frac{L'_K(1,\chi)}{L_K(1,\chi)} & \text{if } \chi \neq \chi_0, \end{cases}$$

and define for $x > 1$,

$$\Phi_{K,\chi}(x) := \frac{1}{x-1} \sum_{N(\mathfrak{p})^k \leq x} \left(\frac{x}{N\mathfrak{p}^k} - 1 \right) \chi(N\mathfrak{p}) \log(N\mathfrak{p}).$$

Then, for $x > 1$,

$$\gamma^*_{K,\chi} = \delta_\chi \log x - \Phi_{K,\chi}(x) + \frac{1}{x-1} \sum_\rho \frac{x^\rho - 1}{\rho(1-\rho)}$$
$$+ \frac{a}{2} F_1(x) + \frac{a'}{2} F_3(x) + r_2 F_2(x),$$

where $\delta_\chi = 1$ or 0 depending on whether $\chi = \chi_0$ or not, ρ runs over non-trivial zeros of $L_K(s,\chi)$, a is the number of real places of K where χ is unramified, a' is the number of real places of K where χ is ramified, $r_1 = a + a'$ (resp. r_2) is the total number of real (resp. complex) places of K and

$$F_1(x) = \log \frac{x+1}{x-1} + \frac{2}{x-1} \log \frac{x+1}{2},$$

$$F_3(x) = \log \frac{x^2}{x^2-1} + \frac{2}{x-1} \log \frac{2x}{x+1},$$

and

$$F_2(x) = \log \frac{x}{x-1} + \frac{\log x}{x-1},$$

see [IMS, Theorem 1]. This formula can be deduced by our general methodology discussed in earlier sections of this paper. The novelty here is the meaning of the expression on the right hand side.

Related to this, the authors in [IMS] also derive the following. Let d_K be the discriminant of K, F_χ be the conductor of χ and put $d_\chi = |d_K| N(F_\chi)$. Let

$$\alpha_{K,\chi} = \frac{1}{2}\log d_\chi$$

and

$$\beta_{K,\chi} - \left(\frac{a+r_2}{2}\right)(\gamma + \log 4\pi) - \left(\frac{a'+r_2}{2}\right)(\gamma + \log \pi).$$

Then,

$$\gamma^*_{K,\chi} = \sum_\rho \frac{1}{1-\rho} - \alpha_{K,\chi} - \beta_{K,\chi}.$$

In particular, one deduces that for $x > 1$, x algebraic,

$$\gamma^*_{K,\chi} - \frac{1}{x-1}\sum_\rho \frac{x^\rho - 1}{\rho(1-\rho)}$$

is a linear form in logarithms of algebraic numbers. Baker's theory implies that this is a transcendental number if it is non-zero, related to the theme of [GMR1].

This raises a series of cognate questions, the foremost being the non-vanishing of $L'_K(1,\chi)$. Indeed, in [MM], it was shown that if $K = \mathbb{Q}$ and χ is the quadratic character associated to the imaginary quadratic field $\mathbb{Q}(\sqrt{-d})$ ($d > 0$), such that $L'(1,\chi) = 0$, then e^γ is transcendental. The vanishing or non-vanishing of $L'(1,\chi)$ has received very little attention in the literature and these remarks indicate that the problem is worthy of serious study.

We also signal the importance of related themes discovered by A. P. Guinand [G] and his doctoral student I. C. Chakravarty [C]. Special cases of the functional relation we derived in this paper can be found in [G], where curiously the author assumes the Riemann hypothesis. They also study the "secondary zeta-functions" defined as

$$\sum_{\gamma > 0} \gamma^{-s},$$

where γ runs through the imaginary parts of the non-trivial zeros of $\zeta(s)$. They derive analytic continuation and functional equation of such series.

These researches reveal that there are further patterns to explore and embrace into a larger theory. We relegate this to the future.

7. Acknowledgements

We thank Professors Sanoli Gun and Tapas Chatterjee for their comments on an earlier version of this paper. We are grateful to them for their invitation and hospitality at IIT Ropar in December 2017. We also thank the referee for useful suggestions.

References

[ASST] S. Adhikari, N. Saradha, T. N. Shorey and R. Tijdeman, Transcendental infinite sums, *Indag. Math. (N.S.)*, **12(1)** (2001) 1–14.

[A] R. Apéry, Irrationalité de $\zeta(2)$ et $\zeta(3)$, *Astérisque*, **61** (1979) 11–13.

[B] A. Baker, Transcendental Number Theory, Cambridge University Press (1975).

[BL] E. Bombieri and J. Lagarias, Complements to Li's criterion for the Riemann hypothesis, *Journal of Number Theory*, **77** (1999) 274–287.

[C] I. C. Chakravarty, The secondary zeta functions, *Journal of Mathematical Analysis and Applications*, **30** (1970) 280–294.

[Co] M. W. Coffey, Toward verification of the Riemann hypothesis: application of the Li criterion, *Math. Phys. Analysis Geometry*, **8** (2005) 211–255.

[D] G. Diaz, Grands degrés de transcendance pour des familles d'exponentielles, *C. R. Acad. Sci. Paris Sér. I. Math.*, **305(5)** (1987) 159–162.

[G] A. P. Guinand, Summation formulae and self-reciprocal functions (III), *The Quarterly Journal of Mathematics*, **13(1)** (1942) 30–39.

[GMR1] S. Gun, M. R. Murty and P. Rath, Transcendental sums related to zeros of zeta functions, *Mathematika*, **64** (2018) 875–897.

[GMR2] S. Gun, M. R. Murty and P. Rath, On a conjecture of Chowla and Milnor, *Canadian Journal of Mathematics*, **63** (2011) 1328–1344.

[IMS] Y. Ihara, V. K. Murty and M. Shimura, On the logarithmic derivatives of Dirichlet L-functions, *Acta Arithmetica*, **137** (2009) 253–276.

[IK] H. Iwaniec and E. Kowalski, Analytic Number Theory, *Colloquium Publications*, **53** (2004).

[Li] X.-J. Li, The positivity of a sequence of numbers and the Riemann hypothesis, *Journal of Number Theory*, **65** (1997) 325–333.

[Mu] M. Ram Murty, Problems in Analytic Number Theory, 2nd edition Springer, New York, (2008).

[MM] M. R. Murty and V. K. Murty, Transcendental values of class group L-functions, *Math. Annalen*, **351(4)** (2011) 835–855.

[MS] M. R. Murty and N. Saradha, Transcendental values of the digamma function, *Journal of Number Theory*, **125** (2007) no. 2, 298–318.

[MW1] M. R. Murty and C. Weatherby, On the transcendence of certain infinite series, *International Journal of Number Theory*, **7(2)** (2011) 323–339.

[MW2] M. R. Murty and C. Weatherby, On a generalization of Euler's theorem for $\zeta(2k)$, *American Mathematical Monthly*, **123** (2016) 53–65.

[Na] W. Narkiewicz, The Development of Prime Number Theory, Springer Berlin, Hiedelberg (2000).

[N] Y. V. Nesterenko, Algebraic independence for values of Ramanujan functions, in Introduction to Algebraic Independence Theory, eds. Y. V. Nesterenko and P. Philippon, *Lecture Notes in Mathematics*, **1752** (Springer, 2001) 27–46.

[PP] Kh. Hessami Pilehrood and T. Hessami Pilehrood, Infinite sums as linear combinations of polygamma functions, *Acta Arithmetica*, **130(3)** (2007) 231–254.

[R] T. Rivoal, La fonction zêta de Riemann prend une infinité de valeurs irrationnelles aux entiers impairs, **331(4)** (15 August 2000) 267–270.

[T] E. C. Titchmarsh, The theory of the Riemann zeta-function, revised by D. R. Heath-Brown, second edition Oxford University Press, Oxford, (2007).

Topics in Number Theory, RMS-Lecture Notes Series No. 26, 2020, pp. 223–233.

On the Supnorm of Maass Lifts

Soumya Das[1] and Jyoti Sengupta[2]

[1]Department of Mathematics, Indian Institute of Science, Bangalore 560 012, India.
e-mail: soumya@iisc.ac.in

[2]School of Mathematics, Tata Institute of Fundamental Research, Mumbai 400 005, India.
e-mail: sengupta@math.tifr.res.in

Abstract. We prove that the supnorm of an L^2-normalised Siegel cusp form of weight k, which is a Maass lift of a Hecke eigenform on $\mathrm{SL}(2, \mathbf{Z})$, is bounded by $k^{17/12+\varepsilon}$ upto a constant depending only on ε. This provides an alternative approach to the same problem treated by V. Blomer.

Keywords. Sup-norm, Saito-Kurokawa lift.

2010 Subject Classification: 11F46, 11F50

1. Introduction

Sup-norm bounds for automorpic forms on various arithmetic subgroups of $\mathrm{GL}(n, \mathbf{R})$ has been a quite active area of research. It is a classical problem to estimate the sup-norm of a holomorphic cusp form or a Maass form on a congruence subgroup of $\mathrm{SL}(2, \mathbf{Z})$ with respect to their respective spectral paramaters, and several results are available in the literature, see e.g. the introduction in [1]. In this paper, motivated by V. Blomer's work [1], we consider this question in the case of a Siegel cusp form F of degree 2 and weight k. More precisely, we are interested in estimating the quantity

$$\|F\|_\infty := \sup_{Z=X+iY\in \mathrm{Sp}(2,\mathbf{Z})\backslash \mathbf{H}_2} (\det Y)^{k/2}|F(Z)|,$$

when F is the Saito-Kurokawa lift (see e.g., [2]) of an elliptic Hecke eigenform on $\mathrm{SL}(2, \mathbf{Z})$ of weight $2k-2$. The reason for such a restriction is due to the fact that Fourier coefficients of "non-lifts" are harder to work with; this is discussed in particular in [1]. In this paper we establish a bound for $\|F\|_\infty$ when F is a Saito-Kurokawa lift.

V. Blomer's approach to this problem [1] was direct, and he estimated the size of $\|F\|_\infty$ by bounding absolutely the Fourier expansion of F. In this way, the argument was similar to Xia [6]. Crucial was the fact that the Fourier coefficients of F can be conveniently written in terms of that of the lifted form; along with the fact that there is also a relation among the corresponding L^2-norms. This, along with some careful estimates of certain sums over symmetric matrices yielded the bound

$$\|F\|_\infty \ll_\varepsilon k^{3/4+\varepsilon}, \tag{1.1}$$

conditional on the Generalised Lindelöf Hypothesis for $L(1/2, f \times \chi_D)$ for all negative fundamental discriminants D. Also there exist Maass lifts where (1.1) is the correct order of magnitude (cf. [1, Thm. 1]). Let us point out here (see Remark 1.2 for more details) that if instead of the Lindelöf Hypothesis, one uses the current best (hybrid) sub-convex bound for these L-values (see (2.29)), then one obtains the bound

$$\|F\|_\infty \ll_\varepsilon k^{5/4+\varepsilon}. \tag{1.2}$$

This wasn't worked out in [1], so we do it in Remark 2.5.

In this article, we take a somewhat different approach, which is also direct, but we work with the Fourier-Jacobi expansion of F. Since F is determined by its first Fourier-Jacobi coefficient ϕ_1, we can reduce the problem to ϕ_1. We then prove a suitable upper bound for the supnorm of (the Γ^J-invariant function associated to) ϕ_1 via its theta-decomposition and using its relation to the lifted form on $\mathrm{SL}(2, \mathbf{Z})$. This makes our calculations much simpler than that in [1]. Our result is the following.

Theorem 1.1. *Let $F \in S_k^2$ be a (L^2-normalised) Saito-Kurokawa lift of an eigenform on* $\mathrm{SL}(2, \mathbf{Z})$. *Then its L^∞-norm satisfies*

$$\|F\|_\infty \ll_\varepsilon k^{17/12+\varepsilon}.$$

Of course this bound is weaker than what one obtains from (1.2); but the main point of this article is to note that our method seems to have the potential to generalise and give at least a polynomial bound for the L^∞-norm of a Siegel cusp form of any degree. This is under preparation (possibly in conjunction with other methods) and the details would appear elsewhere. We make some remarks on this later, see Remark 2.4.

Remark 1.2. (1) As mentioned in [1], using a Bergman kernel for $\mathrm{Sp}(2, \mathbf{Z})$ it follows that over fixed compacts sets Ω, one gets the "convexity" or trivial bound

$$\|F|_\Omega\|_\infty \ll k^{3/2}.$$

So even our method, which does not restrict to compact sets, beats this bound.

(2) Perhaps an explanation of a better bound this way is linked to the possible cancellation inside each Fourier-Jacobi coefficient of F.

Acknowledgements

S.D. would like to express his thanks to the organisers of the conference"Number Theory: Arithmetic, Diophantine and Transcendence" during December 22–25, 2017 on the occasion of Srinivasa Ramanujan's 130th birthday at IIT Ropar in Punjab jointly organized with IMSC, Chennai, India. He also wishes to thank IISc., Bangalore, UGC centre for Advanced Studies for financial support; and the T.I.F.R. Mumbai and Alfréd Rényi Institute for Mathematics, Budapest where this work was done, for excellent working atmosphere. During the preparation of this work S.D. was supported by a MATRICS grant MTR/2017/000496 from DST-SERB, India. The authors also thank the referee for a thorough checking of the paper.

2. Proof of Theorem 1.1

Let $J^o_{k,m}$ denote the space of cusp forms of weight k and index m (see [2] for details). We start from the expression

$$F(Z) = \sum_{m\geq 1} (V_m\,\phi)(\tau, z) e(m\tau'), \qquad (e(z) := e^{2\pi i z}) \tag{2.1}$$

where $\phi \in J^o_{k,1}$ is a Hecke eigenform and for $m \geq 1$ the Hecke operators V_m are defined as maps from $J^o_{k,1}$ to $J^o_{k,m}$ by

$$V_m\phi(\tau, z) = m^{k-1} \sum_{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_1\backslash A_m(\mathbf{Z})} (c\tau + d)^{-k} e^m \left(\frac{-cz^2}{c\tau + d}\right) \phi\left(\frac{a\tau + b}{c\tau + d}, \frac{mz}{c\tau + d}\right), \tag{2.2}$$

where we have put

$$A_m(\mathbf{Z}) = \{\gamma \in M_2(\mathbf{Z}) \mid \det(\gamma) = m\}.$$

Choosing convenient upper triangular coset representatives, one can write

$$V_\ell\phi(\tau, z) = \ell^{-1} \sum_{a|\ell,\, ad=\ell} \sum_{b \bmod d} a^k \phi\left(\frac{a\tau + b}{d}, az\right) \tag{2.3}$$

Let us write $Z = X + iY \in \mathfrak{F} := \mathrm{Sp}(2, \mathbf{Z})\backslash \mathbf{H}_2$, so in particular Y is Minkowski-reduced. Throughout the paper, we would use the decomposition

$$Z = \begin{pmatrix} \tau & z \\ z & \tau' \end{pmatrix},$$

with $u + iv = \tau, \tau' = u' + iv' \in \mathbf{H}$ and $z = x + iy \in \mathbf{C}$. Further, let us set $|Y| = \det(Y)$. It is also convenient to introduce the parameter t by defining

$$\mathrm{t} := |Y|/v = v' - y^2/v. \tag{2.4}$$

Then it follows from reduction theory that $v, v' \geq \sqrt{3}/2$ (cf. [3]). Moreover, for the same reason,

$$\mathrm{t} = |Y|/v \gg v' \gg 1.$$

For $Z \in \mathfrak{F}$ we use (2.1) to estimate:

$$\begin{aligned}
|Y|^{k/2}|F(Z)| &\leq |Y|^{k/2} \sum_{m=1}^{\infty} |V_m\,\phi| e^{-2\pi m v'} \\
&= \mathrm{t}^{k/2} \sum_{m=1}^{\infty} (v^{k/2} e^{-2\pi m y^2/v} |V_m\,\phi|) e^{-2\pi m (v' - y^2/v)} \\
&= \mathrm{t}^{k/2} \sum_{m=1}^{\infty} \widetilde{V_m\,\phi}\, e^{-2\pi m \mathrm{t}},
\end{aligned}$$

where for any $\psi \in \mathrm{Hol}(\mathbf{H} \times \mathbf{C})$, we put

$$\widetilde{\psi} := v^{k/2} e^{-2\pi m y^2/v} |\psi(\tau, z)|. \tag{2.5}$$

If $\psi \in J^o_{k,m}$, then $\widetilde{\psi}$ is a bounded Γ^J invariant function. Moreover for $\psi \in J^o_{k,m}$ as above, we put

$$\|\psi\|_\infty := \sup_{(\tau,z)\in\Gamma^J\backslash\mathbf{H}\times\mathbf{C}} \widetilde{\psi}. \tag{2.6}$$

Therefore we can say that

$$|Y|^{k/2}|F(Z)| \ll \mathrm{t}^{k/2} \sum_{m=1}^{\infty} \|V_m\,\phi\|_\infty\, e^{-2\pi m \mathrm{t}}. \tag{2.7}$$

Our next task is to estimate the quantity $\|V_m\,\phi\|_\infty$ in terms of m and $\|\phi\|_\infty$. With the setting of (2.3) in mind, we compute for $\phi \in J^o_{k,1}$, the following.

$$\begin{aligned}\widetilde{\phi}\left(\frac{a\tau+b}{d}, az\right) &= \left(\frac{a}{d}\right)^{k/2} v^{k/2} e^{-2\pi d a^2 y^2/av} \left|\phi\left(\frac{a\tau+b}{d}, az\right)\right| \\ &= \left(\frac{a}{d}\right)^{k/2} v^{k/2} e^{-2\pi m y^2/v} \left|\phi\left(\frac{a\tau+b}{d}, az\right)\right|. \end{aligned} \tag{2.8}$$

Remark 2.1. If one could establish an explicit bound of the form

$$\|V_m\,\phi\|_\infty \ll_\varepsilon k^{a+\varepsilon} m^{k/2-b+\varepsilon} \|V_m\,\phi\|_2,$$

for some a, b with the implied constant depending only on ε, then using the formula (cf. [4])

$$\|V_m\,\phi\|_2^2 = m^{k-3/2} \sum_{t|m} K(t) t^{-1/2} \|\phi\|_2^2, \qquad (K(t) = t\prod_{p|t}(1+1/p))$$

we could perhaps bound $\|V_m\,\phi\|_\infty$ better.

Then we can estimate, upon using (2.5) and (2.8) that

$$\begin{aligned}\widetilde{V_m\,\phi}(\tau, z) &\le m^{-1} v^{k/2} e^{-2\pi m y^2/v} \sum_{a|m, ad=m} \sum_{b \bmod d} a^k \left|\phi\left(\frac{a\tau+b}{d}, az\right)\right| \\ &\le m^{-1} \sum_{a|m} \sum_{b \bmod d} a^k \left(\frac{d}{a}\right)^{k/2} \left|\widetilde{\phi}\left(\frac{a\tau+b}{d}, az\right)\right| \\ &\le m^{k/2-1} \sum_{a|m} m/a \cdot \sup_{(\tau,z)\in\Gamma^J\backslash\mathbf{H}\times\mathbf{C}} \widetilde{\phi} \\ &\ll m^{k/2} \log(m) \cdot \|\phi\|_\infty, \end{aligned} \tag{2.9}$$

where the implied constant is absolute. This gives our desired relations between the sup-norms for every $m \geq 1$:

$$\|V_m \phi\|_\infty \ll m^{k/2} \log(m) \cdot \|\phi\|_\infty.$$

We now turn back to our original goal. Let us note that the function $f(x) := x^{k/2+\varepsilon} e^{-2\pi x \mathrm{t}}$ increases upto $x = \Upsilon := \frac{k/2+\varepsilon}{2\pi \mathrm{t}}$ and decreases thereafter. From (2.7) and (2.9) we therefore get, using the fact that $\sum_{m=1}^{\infty} f(m) \leq \int_0^\infty f(t)dt + 2f(\Upsilon)$ when $\Upsilon \geq 1$ (see [6]), that

$$\begin{aligned}
&|Y|^{k/2}|F(Z)| \\
&\ll_\varepsilon \mathrm{t}^{k/2} \left(\sum_{m=1}^{\infty} m^{k/2+\varepsilon}\, e^{-2\pi m \mathrm{t}} \right) \cdot \|\phi\|_\infty \\
&\ll_\varepsilon \mathrm{t}^{k/2} \left(\int_0^\infty x^{k/2+\varepsilon} e^{-2\pi \mathrm{t} x} dx + 2 \left(\frac{k/2+\varepsilon}{2\pi \mathrm{t}} \right)^{k/2+\varepsilon} e^{-k/2-\varepsilon} \right) \cdot \|\phi\|_\infty \\
&\ll_\varepsilon \mathrm{t}^{k/2} \left((2\pi \mathrm{t})^{-k/2-1-\varepsilon} \Gamma(k/2+1+\varepsilon) + 2 \left(\frac{k/2+\varepsilon}{2\pi \mathrm{t}} \right)^{k/2+\varepsilon} e^{-k/2-\varepsilon} \right) \cdot \|\phi\|_\infty \\
&\ll_\varepsilon \left(\frac{\Gamma(k/2+1+\varepsilon)}{\mathrm{t}} + (k/2+\varepsilon)^{k/2+\varepsilon} e^{-k/2-\varepsilon} \right) \cdot \frac{\|\phi\|_\infty}{(2\pi)^{k/2}} \\
&\ll_\varepsilon \frac{\Gamma(k/2+1+\varepsilon)}{(2\pi)^{k/2}} \cdot \|\phi\|_\infty \qquad \text{(since } \mathrm{t} \gg 1). \qquad (2.10)
\end{aligned}$$

The case $\Upsilon < 1$ is similar, and we get the same bound as (2.10) using the inequality $\sum_{m=1}^{\infty} f(m) \leq \int_0^\infty f(t)dt + f(1)$ and $f(1) \leq f(\Upsilon)$.

We now turn to bounding $\|\phi\|_\infty$ in terms of k and $\|\phi\|_2$. For this, we would appeal to the theta decomposition of ϕ and with some modifications, reduce the question to its theta-components, and then use a recent result of R. Steiner [5] on bounds for the sup-norm of half-integral weight Hecke eigenform.

Let us recall the theta-decomposition of ϕ.

$$\phi(\tau, z) = h_0(\tau)\theta_0(\tau, z) + h_1(\tau)\theta_1(\tau, z),$$

where $h_j \in S_{k-1/2}(\Gamma(4))$ and θ_0, θ_1 are certain Jacobi-theta series defined by (with $\mu \in \{0, 1\}$)

$$\theta_\mu(\tau, z) = \sum_{\substack{r \in \mathbf{Z} \\ r \equiv \mu \bmod 2}} q^{\frac{r^2}{4}} \zeta^r. \qquad (q = e(\tau), \zeta = e(z))$$

The Eichler-Zagier map acting on $\phi \in J_{k,1}^{o}$ (which is Hecke equivariant) gives rise to a form $h \in S_{k-1/2}^{+}(\Gamma_0(4))$. Explicitly,

$$h(\tau) = h_0(4\tau) + h_1(4\tau).$$

Now from the transformation properties of ϕ, (h_0, h_1) satisfy the following functional equation:

$$h_0(-\tau^{-1}) = (-2i)^{-k}(-2i\tau)^{k-1/2}(h_0(\tau) + h_1(\tau)),$$
$$h_1(-\tau^{-1}) = (-2i)^{-k}(-2i\tau)^{k-1/2}(h_0(\tau) - h_1(\tau)).$$

Our aim is to express both h_0 and h_1 in terms of h. Therefore by changing $\tau \mapsto 4\tau$, we can write

$$h_0|W_4(\tau) = i^k 2^{k-1} h(\tau), \quad h_1|W_4(\tau) = i^k 2^{k-1}(2h_0(4\tau) - h(\tau)).$$

Here we use the same normalisation for W_4 as in [5]:

$$W_4 = \left(\begin{pmatrix} 0 & -1/2 \\ 2 & 0 \end{pmatrix}, (-2i\tau)^{k-1/2} \right)$$

Using the fact that W_4 is an involution, we immediately get

$$h_0(\tau) = i^k 2^{k-1} h|W_4(\tau),$$
$$h_1(\tau) = h(\tau/4) - i^k 2^{k-1} h|W_4(\tau). \tag{2.11}$$

Let us put, for $g \in S_{k-1/2}(\Gamma_0(4))$, the quantity

$$\widetilde{g}(\tau) := v^{k/2-1/4}|g(\tau)|.$$

We can then estimate

$$v^{k/2} e^{-2\pi y^2/v} |\phi(\tau, z)|$$
$$\leq v^{k/2-1/4}|h_0(\tau)| v^{1/4} e^{-2\pi y^2/v} |\theta_0(\tau, z)| + v^{k/2-1/4}|h_1(\tau)| v^{1/4} e^{-2\pi y^2/v} |\theta_1(\tau, z)| \tag{2.12}$$
$$\ll \max\{2^k v^{1/4} \cdot \widetilde{h|W_4}(\tau), v^{1/4}\widetilde{h_1}(\tau)\} \left(e^{-2\pi y^2/v} (|\theta_0(\tau, z)| + |\theta_1(\tau, z)|) \right)$$
$$\ll 2^k v^{1/4} \max\{\widetilde{h|W_4}(\tau), \widetilde{h}(\tau/4)\} G(\tau, z); \tag{2.13}$$

where we have put

$$G(\tau, z) = e^{-2\pi y^2/v} (|\theta_0(\tau, z)| + |\theta_1(\tau, z)|). \tag{2.14}$$

Let us now show that G above is a bounded function for all $(\tau, z) \in \mathfrak{F}^J$, where $\mathfrak{F}^J$ denotes the standard fundamental domain for the action of the Jacobi group on $\mathbf{H} \times \mathbf{C}$. We note that for $(\tau, z) \in \mathfrak{F}^J$ we may assume that $v \geq \sqrt{3}/2$ and $0 \leq y \leq v$. Thus,

$$G(\tau, z) \leq \sum_{r \in \mathbf{Z}} e^{-2\pi v (r^2 v/4 - |r| y + y^2/v^2)}$$
$$\leq 1 + 2 \sum_{r \geq 1} e^{-2\pi v (|r|/2 - y/v)^2}.$$

We split the r-sum into two parts:

$$(\mathrm{A})\, r \geq 1, r > 4|y|/v, \qquad (\mathrm{B})\, r \geq 1, r \leq 4|y|/v.$$

In case (A), we have $|r - 2y/v| \geq r/2$ whence

$$\sum_{r>4|y|/v} e^{\frac{-\pi v r^2}{8}} \ll \sum_{r\geq 1} e^{-\pi \frac{\sqrt{3} r^2}{16}} \ll 1.$$

In case (B), the number of summands is absolutely bounded since $2|y|/v \leq 2$, and the sum is $\ll 1$.

Let $\mathcal{F}_4$ denote the standard fundamental domain of $\Gamma_0(4)$ on $\mathbf{H}$. We note in the passing that we actually would work in the context of elliptic cusp forms (as in other works on this topic, e.g. [5]) on a supersets of $\mathcal{F}_4$ of the form (of translates of suitable Siegel sets)

$$\mathcal{S}(c) := S(c) \cup W_4(S(c)) \cup B_4(S(c)) \quad (c = \sqrt{3}/8, \sqrt{3}/32);$$

where for $c > 0$, $S(c) := \{z \in \mathbf{H} | \Im(\tau) > c\}$ and $B_4 = \left(\left(\begin{smallmatrix} 1 & 0 \\ 2 & 1 \end{smallmatrix}\right), (-i(2\tau+1))^{k-1/2}\right)$. Thus in the following, we work with $\mathcal{S}(c)$ with $c = \sqrt{3}/8, \sqrt{3}/32$, the ensuing bounds are exactly the same in the k-aspect, only the implied absolute constants involved may change for these different values of c. This is done to accommodate the function $\widetilde{h}(\tau/4)$ from (2.13).

Following Steiner [5] we would now divide our argument in two regions (we would choose $\eta > 0$ appearing below, later):

(I) $\mathcal{F}^+ = \{\tau \in \mathcal{F}_4 | v \gg k^\eta\}$, and
(II) $\mathcal{F}_4^- = \{\tau \in \mathcal{F}_4 | v \ll k^\eta\}$.

In the region (I), we argue using the Fourier expansion. Note however that the quantity $\widetilde{\theta}_0$ (cf. (2.5)) blows up, so we try to compensate this by leveraging with the bounds obtained in [5]. To this end, let us quote from [5, Prop. 6 and 7] the following statements, stated in a way that is convenient for us.

Proposition 2.2 ([5]). *Let $k \in 1/2 + \mathbf{Z}$ and $k \geq 5/2$. For an L^2-normalised Hecke eigenform $f \in S_k^+(\Gamma_0(4))$ we have the following. Assume the bound $L(F, \chi, 1/2) \ll k^{\alpha+\epsilon} q^{\beta+\epsilon}$, where $F \in S_{2k-1}$ denotes the (Hecke normalised) Shimura lift of f and χ is a real primitive quadratic character* mod$q$. *If $\beta > 0$, then for all $v \geq \frac{\sqrt{3}}{8}$ (actually in $\mathcal{S}(\sqrt{3}/8)$ and hence also in any $\mathcal{S}(c)$ with $c \geq \sqrt{3}/8$ being absolute) one has the following bounds:*

$$\max\{\widetilde{f}, \widetilde{f|W_4}\} \ll_\epsilon \frac{k^{1/4+\alpha/2+\beta/2+\varepsilon}}{v^{1/2+\beta/2}}(1 + v k^{-1/2}). \tag{2.15}$$

Proposition 2.3 ([5]). *Let all the hypotheses of Proposition 2.2 hold. Then for $k \geq \beta > 0$ and all $v > \frac{12k}{\pi}$ one has the bound:*

$$\max\{\widetilde{f}, \widetilde{f|W_4}\} \ll_\epsilon \frac{k^{1/4+\alpha/2+\beta/2+\varepsilon}}{v^{1/2+\beta/2}}(1 + k^{1/2}\exp(-\pi v)). \tag{2.16}$$

We are going to use Proposition 2.2 and Proposition 2.3 in the following way. Let $\mathfrak{g}$ denote any of the quantities $\widetilde{h}, \widetilde{h|W_4}$. Then under the assumption that $\eta > 0$, we infer (respectively) from (2.15) and (2.16) the following bounds (noting that $\|h\|_2 \asymp \|h|W_4\|_2$, in fact they are same upto some absolute constant).

$$v^{1/4}\widetilde{\mathfrak{g}} \ll_\varepsilon \begin{cases} \frac{k^{1/4+\alpha/2+\beta/2+\varepsilon}}{v^{1/4+\beta/2}}(1+vk^{-1/2})\|h\|_2 & (k^\eta \ll v \ll k) \\ \frac{k^{1/4+\alpha/2+\beta/2+\varepsilon}}{v^{1/4+\beta/2}}(1+k^{1/2}\exp(-\pi v))\|h\|_2 & (k \ll v) \end{cases}. \tag{2.17}$$

For simplicity, from now on let us use the current best possible values of (α, β) from the subconvexity results of [7] and put $(\alpha, \beta) = (1/3, 1/3)$. From (2.17), it then follows that

$$v^{1/4}\widetilde{\mathfrak{g}} \ll_\varepsilon \begin{cases} k^{2/3+\varepsilon} \cdot \|h\|_2 & (k^\eta \ll v \ll k) \\ k^{1/6+\varepsilon} \cdot \|h\|_2 & (k \ll v) \end{cases}. \tag{2.18}$$

Then we record:

$$v^{1/4}\widetilde{\mathfrak{g}} \ll_\varepsilon k^{2/3+\varepsilon} \cdot \|h\|_2 \qquad (k^\eta \ll v). \tag{2.19}$$

For the region (II), we use another bound from [5, (3.24)] which says that for a certain parameter $\Lambda = k^\gamma$ one has

$$\begin{aligned} v^{1/2}\widetilde{\mathfrak{g}}^2 &\ll k^{1+\varepsilon}\Lambda^\varepsilon\left(\Lambda^{-1} + vk^{-1/2} + \Lambda^2 k^{-1/2} + \Lambda^6 k^{-1}\right) v^{1/2}\|h\|_2 \\ &\ll k^{1+\eta/2+\varepsilon}(k^{-\gamma} + k^{\eta-1/2} + k^{2\gamma-1/2} + k^{6\gamma-1})\|h\|_2 \\ &\ll k^{5/4+\varepsilon}\|h\|_2; \end{aligned} \tag{2.20}$$

upon choosing $\eta = 1/2$ and $\gamma = 1/6$.

In all (using (2.19), (2.20)), we have proved so far that

$$v^{1/4}\widetilde{\mathfrak{g}} \ll k^{2/3+\varepsilon}\|h\|_2. \tag{2.21}$$

Thus from (2.12), (2.13), (2.21) and the fact that $G(\tau, z)$ (cf. (2.14)) is bounded in $\mathfrak{F}^J$ we arrive at the bound:

$$\|\phi\|_\infty \ll k^{2/3+\varepsilon}2^k\|h\|_2. \tag{2.22}$$

Let us also note that to arrive at (2.13), we have tacitly used the fact that $v^{1/4}\widetilde{h}(\tau/4)$ satisfies the same bound as in (2.21); since (2.21) in fact holds for all $\tau \in \mathcal{S}(\sqrt{3}/8)$ and also for all $\tau \in \mathcal{S}(\sqrt{3}/32)$.

Furthermore, we have the following relation between the Petersson norms of ϕ and h (see [2]):

$$\|\phi\|_2 = 2^{k-3/2}\|h\|_2. \tag{2.23}$$

Therefore comparing (2.22) and (2.23) we get

$$\|\phi\|_\infty \ll k^{2/3+\varepsilon}\|\phi\|_2. \tag{2.24}$$

We now recall the last piece of information about the relation between the Petersson norms of ϕ and F (cf. [4, corollary to Thm. 2]):

$$\|\phi\|_2 = \frac{\pi^{k/2} 3^{1/2} 2^{k+1/2}}{|L(k,f)|^{1/2}\,\Gamma(k)^{1/2}} \cdot \|F\|_2, \tag{2.25}$$

where $f \in S_{2k-2}$ is the Shimura lift of h. Note that one has $L(k, f) \gg 1$ since $s = k$ falls within the region of absolute convergence of $L(s, f)$.

Substituting the formula (2.25) in the inequality (2.24) we get

$$\|\phi\|_\infty \ll \frac{k^{2/3+\varepsilon} \pi^{k/2} 2^k}{\Gamma(k)^{1/2}} \cdot \|F\|_2. \tag{2.26}$$

If we now go back to (2.10), and use the bound (2.26) for $\|\phi\|_\infty$ there, we finally obtain (since $\|F\|_2 = 1$)

$$\begin{aligned}\|F\|_\infty &\ll \frac{k^{2/3+\varepsilon}\pi^{k/2}2^k\Gamma(k/2+1+\epsilon)}{2^{k/2}\pi^{k/2}\Gamma(k)^{1/2}} \\ &\ll \frac{k^{2/3+3/4+\epsilon}2^k}{2^{k/2}\cdot 2^{k/2}} \\ &\ll k^{17/12+\varepsilon}.\end{aligned} \tag{2.27}$$

This finishes the proof of Theorem 1.1. □

Remark 2.4. We believe that in the same vein, one could prove a polynomial bound for the sup-norm of any Siegel cusp form of degree n. One would appeal to the Fourier-Jacobi coefficients and bound them via their theta-components. Of course, here the situation would be much more complicated as there is no 'parametrisation' by a single half-integral weight newform like h in this paper; nevertheless with enough work a polynomial bound is expected to be obtained in this fashion. Its another matter to improve this bound further.

Remark 2.5. We wish to briefly indicate how to obtain the bound $\|F\|_\infty \ll k^{5/4+\varepsilon}$ (cf. (1.2)) for F being L^2-normalised, which was mentioned in the introduction. We start from section 4 of [1] and note that with our (which is the same as in [5]) normalisation,

$$a(T) = \sum_{d|\mathfrak{c}(T)} d^{k-1} c_h(\det 2T/d^2),$$

where we denote by $h \in S^+_{k-1/2}(4)$, the half-integral newform in Kohnen's plus space of level 4 and $\mathfrak{c}(T)$ denotes the content of T. It is well-known (see e.g., [2]) that $c_\phi(|D|) = c_h(|D|)$ for all discriminants $D < 0$ and that $\phi \mapsto h$ is an isomorphism (an isometry with proper normalisation). Moreover, from [7], we state the following bound for the Fourier coefficients $c_h(m)$:

$$c_h(m) \ll_\varepsilon \frac{(4\pi)^{k/2}}{\Gamma(k-1/2)^{1/2}} \cdot k^{\alpha/2+\varepsilon} \cdot m^{\frac{k-3/2+\beta}{2}} \|h\|_2 \tag{2.28}$$

where (α, β) are the exponents of a subconvex bound in the k and D aspect of the central value of the L-function $L(1/2, f \times \chi_D)$ with D fundamental, i.e.,

$$L(1/2, f \times \chi_D) \ll_\varepsilon k^{\alpha+\varepsilon}|D|^{\beta+\varepsilon}. \tag{2.29}$$

Note that the inequality (4.1) in [1] now becomes (using (2.28), (2.29), (2.23) and (2.25))

$$a(T) \ll (\det 2T)^{\frac{k-3/2+\beta+\varepsilon}{2}} \mathfrak{c}(T)^{1/2-\beta+\varepsilon} \cdot \frac{(2\pi)^k}{\Gamma(k)} \cdot k^{\alpha/2+1/4+\varepsilon} \cdot \|F\|_2.$$

Let us note here that the exponents $\alpha/2$ and $1/4$ in k both come from the bound (2.28). In particular the exponent $1/4$ comes from the ratio $\frac{\Gamma(k)^{1/2}}{\Gamma(k-1/2)^{1/2}}$. Further another factor of $\Gamma(k)^{1/2}$ comes from (2.25).

Putting this bound into the Fourier expansion of F with the choice $(\alpha, \beta) = (1/3, 1/3)$ from [7], and proceeding as in [1] leads us to the bound

$$\begin{aligned}
\frac{\|F\|_\infty}{\|F\|_2} &\ll \frac{(4\pi)^k}{\Gamma(k)} \cdot k^{5/12+\varepsilon} \sum_T \frac{\mathfrak{c}(T)^{1/6+\varepsilon}}{(\det T)^{7/12-\varepsilon}} (\det TY)^{k/2} e^{-2\pi \operatorname{tr}(TY)} \\
&\ll \frac{(4\pi)^k}{\Gamma(k)} \cdot k^{5/12+\varepsilon} \sum_d \frac{1}{d^{1-\varepsilon}} \sum_T \frac{(\det TY_d)^{k/2} e^{-2\pi \operatorname{tr}(TY_d)}}{(\det T)^{7/12-\varepsilon}} \\
&\ll k^{5/12+1/2+\varepsilon} \sum_d \frac{1}{d^{1-\varepsilon}} \sum_{TY_d \in \mathcal{X}} \frac{(\det Y_d)^{7/12-\varepsilon}}{(\det TY_d)^{7/12-\varepsilon}} \\
&\ll k^{11/12-7/6+\varepsilon} \left\{ \sup_{Y \in \mathcal{Y}} (\det Y)^{7/12-\varepsilon} \sum_{TY \in \mathcal{X}} 1 \right\}.
\end{aligned} \tag{2.30}$$

From the definition of $\mathcal{Y}$ and $\mathcal{X}$ (loc. cit.) it follows easily that the quantity in $\{\cdots\}$ is bounded by $k^{3/2+\varepsilon}$ (see the last display in the proof of [1, Lemma 4], one has to multiply it with the factor $\det Y^{7/12-\epsilon}$ instead of $\det Y^{3/4}$), so our claim follows since $11/12 - 7/6 + 3/2 = 15/12 = 5/4$.

Remark 2.6. Just putting in a bound for $c_h(m)$ into the Fourier expansion of ϕ brings to us the factor of $v^{3/4-\beta/2}$. To avoid this, we are forced to choose $\beta = 3/2$, and the ensuing bounds are, not surprisingly, very bad.

Remark 2.7. It may be possible to use a Bergman kernel function on $J^o_{k,m}$ and carry out Steiner's arguments in this setting. Work is in progress on this and the related problem in the context of Siegel cusp forms, as mentioned in the introduction.

References

[1] V. Blomer, On the size of Ikeda lifts. *Manuscripta Math.*, **148** (2015) 341–349.

[2] M. Eichler and D. Zagier, The Theory of Jacobi Forms. *Progress in Mathematics*, Boston-Basel-Stuttgart: Birkhäuser, **55** (1985).

[3] E. Freitag, Siegelsche Modulfunktionen. *Grundl. Math. Wiss.*, Springer–Verlag, **254** (1983).
[4] W. Kohnen and N.-P. Skoruppa, A certain Dirichlet series attached to a Siegel modular form of degree two. *Invent. Math.*, **95** (1989) 541–558.
[5] R. S. Steiner, Supnorm of modular forms of half-integral weight in the weight aspect. *Acta Arith.*, **177** (2017) no. 3, 201–218.
[6] H. Xia, On L^{∞}-norms of holomorphic cusp forms. *J. Number Theory*, **124** (2007) 325–327.
[7] M. P. Young, Weyl-type hybrid subconvexity bounds for twisted L-functions and Heegner points on shrinking sets. *J. Eur. Math. Soc.*, (2017) **17** no. 5, 1545–1576.

Topics in Number Theory, RMS-Lecture Notes Series No. 26, 2020, pp. 235–256.

On the Structure of Fine Selmer Groups and Selmer Groups of CM Elliptic Curves

Meng Fai Lim[1] and Ramdorai Sujatha[2]

[1]School of Mathematics and Statistics & Hubei Key Laboratory of Mathematical Sciences, Central China Normal University, Wuhan, 430079, P. R. China.
e-mail: limmf@mail.ccnu.edu.cn

[2]Department of Mathematics, University of British Columbia, Vancouver BC, V6T 1Z2, Canada.
e-mail: sujatha@math.ubc.ca

Abstract. In this paper, we examine the structure of the fine Selmer group and Selmer group of an elliptic curve with complex multiplication and good ordinary reduction at p over their fields of π-power division points and p-power division points.

Keywords. CM elliptic curves, strict Selmer groups, fine Selmer groups, Conjecture A, Conjecture B.

2010 Subject Classification: 11R23, 11R34, 11F80, 16S34

1. Introduction

Let p be an odd prime and E an elliptic curve defined over a number field F. The fine Selmer group of the elliptic curve is a much studied object in Iwasawa theory and occurs in the formulation (and proof) of the Iwasawa main conjecture (see [23, 24, 40]). Coates and the second author undertook a systematic study of the fine Selmer group in [6], where several important conjectures on the structure of these groups are postulated, and we briefly recall them. Let F^{cyc} denote the cyclotomic $\mathbb{Z}_p$-extension of F and $R(E/F^{\mathrm{cyc}})$ be the fine Selmer group of E over F^{cyc}. Coates and the second author conjectured that $R(E/F^{\mathrm{cyc}})$ is cofinitely generated over $\mathbb{Z}_p$ ([6, Conjecture A]). This conjecture is a natural analogue of a classical conjecture of Iwasawa which asserts that the p-exponent of the class groups in a cyclotomic $\mathbb{Z}_p$-extension grows linearly (see [20, 21]). In fact, there is a very precise relation between the two conjectures and we refer readers to [6, Theorem 3.4], [29, Theorem 3.5], [31, Theorem 5.5], [44, Theorem 4.5] and [48, Section 8] for further discussion on this. In their paper [6], Coates and the second author also studied the structure of the fine Selmer group over extensions of F whose Galois group $G = \mathrm{Gal}(F_\infty/F)$ is a p-adic Lie group of dimension larger than 1. Their conjecture on the structure of the Pontryagin dual of the fine Selmer group of an elliptic curve over such an extension predicts that the said module is pseudo-null over the corresponding Iwasawa algebra $\mathbb{Z}_p[\![G]\!]$ (see [6, Conjecture B]).

In this paper, we investigate the structure of the fine Selmer group of an elliptic curve with complex multiplication. Our approach towards this study is via the Selmer group which we now describe briefly. For simplicity, we assume in this introduction that E is an elliptic curve defined over an imaginary quadratic field K which has complex multiplication given by the ring of integers of K and which has good ordinary reduction at every prime above p. It follows that the prime necessarily splits in K, say $p = \mathfrak{p}\overline{\mathfrak{p}}$. Denote by $K_{\mathfrak{p}^\infty}$ the $\mathbb{Z}_p$-extension of K unramified outside $\mathfrak{p}$. A well-known result of Gillard and Schneps [11, 12, 42] tells us that the $\mathfrak{p}^\infty$-Selmer group over $K_{\mathfrak{p}^\infty}$ is cofinitely generated over $\mathbb{Z}_p$. The aim of this paper is to analyse the consequence of this result on the structure of the full p^∞-Selmer group of the elliptic curve which is then applied to study the structure of the fine Selmer group of the elliptic curve. Our main result for the full p^∞-Selmer group is as follows (see Theorem 3.6 for a more refined statement).

Theorem 1.1 (Theorem 3.6). *The dual strict Selmer group $X(E/K_\infty)$ is finitely generated over $\mathbb{Z}_p[\![H_\mathfrak{p}]\!]$, where $H_\mathfrak{p} = \mathrm{Gal}(K_\infty/K_{\mathfrak{p}^\infty})$.*

The above result will be applied to study the fine Selmer group which allows us to obtain the following.

Proposition 1.2 (Proposition 4.1). *The dual fine Selmer group $R(E/K_\infty)^\vee$ has trivial μ_G-invariant, where $G = \mathrm{Gal}(K_\infty/K)$.*

Recall from [3, 9] that $X(E/K_\infty)$ is said to satisfy the $\mathfrak{M}_H(G)$-conjecture if $X(E/K_\infty)/X(E/K_\infty)[p^\infty]$ is finitely generated over $\mathbb{Z}_p[\![H]\!]$, where $H = \mathrm{Gal}(K_\infty/K^{\mathrm{cyc}})$. Our discussion in this paper provides a first instance where the $\mathfrak{M}_H(G)$-conjecture and Conjecture A are related.

Proposition 1.3 (Proposition 4.3). *Suppose that the $\mathfrak{M}_H(G)$-conjecture is valid for $X(E/K_\infty)$. Then $R(E/K^{\mathrm{cyc}})^\vee$ is finitely generated over $\mathbb{Z}_p$.*

We now describe the plan of the paper. In Section 2, we introduce the strict Selmer group in the sense of Greenberg [14] and collect certain results on the structure of these Selmer groups. In Section 3, we turn to the case which interests us in this paper, namely the complex multiplication situation. Here we combine the results in Section 2 with the result of Gillard and Schneps to prove some results on the structure of the Selmer group of the elliptic curve. These results are then applied to study the structure of the fine Selmer group in Section 4. Here we also mention how our result can be viewed as a weak partial support to Conjecture A of [6]. In Section 5, we discuss some relation between our result with Conjecture B of [6]. Finally in Section 6, we record an interesting consequence of Conjecture B which gives a precise relation between the elliptic units and global units. It appears that this latter observation has not been explicitly recorded in literature despite being well-known to the experts, and we therefore felt it worthwhile to do so here.

Acknowledgements

The authors would like to thank Thong Nguyen Quang Do and Romyar Sharifi for their interest and valuable comments pertaining to Section 6 of this paper. The authors would also like the anonymous referee for providing helpful comments and suggestions which helped improve the exposition of the paper. Some part of the research of this article took place when the first author was visiting the National Center for Theoretical Sciences of Taiwan and he would like to acknowledge the hospitality and conducive working conditions provided by the said institute. Finally, the first author's research is supported by the National Natural Science Foundation of China under Grant No. 11550110172 and Grant No. 11771164. The second author gratefully acknowledges support from NSERC (Discovery Grant No: 402071).

2. Selmer groups

Throughout this section, we let p be a prime and F a number field which is further assumed to have no real primes if $p = 2$. In this section, we introduce the strict Selmer groups associated to certain datum in the sense of Greenberg [14]. As a start, we introduce the axiomatic conditions on our datum which is denoted by $\big(A, \{A_v\}_{v|p}\big)$ and satisfies all of the following four conditions **(C1)–(C4)**.

(C1) A is a cofinitely generated cofree $\mathbb{Z}_p$-module of $\mathbb{Z}_p$-corank d with a continuous, $\mathbb{Z}_p$-linear $\mathrm{Gal}(\bar{F}/F)$-action which is unramified outside a finite set of primes of F.

(C2) For each prime v of F above p, there is a distinguished $\mathrm{Gal}(\bar{F}_v/F_v)$-submodule A_v of A which is cofree of $\mathbb{Z}_p$-corank d_v.

(C3) For each real prime v of F, $A_v^+ := A^{\mathrm{Gal}(\bar{F}_v/F_v)}$ is cofree of $\mathbb{Z}_p$-corank d_v^+.

(C4) The following equality

$$\sum_{v|p}(d - d_v)[F_v : \mathbb{Q}_p] = dr_2(F) + \sum_{v \text{ real}}(d - d_v^+)$$

holds. Here $r_2(F)$ denotes the number of complex primes of F.

As is usual in Iwasawa theory, we will need to work with Selmer groups defined over a tower of number fields. Thus, we need to consider the base change of our datum which we now do. Let L be a finite extension of F. The base change of our datum $\big(A, \{A_w\}_{w|p}, \{A_w^+\}_{w|\mathbb{R}}\big)$ over L is given as follows:

(1) A can be viewed as a $\mathrm{Gal}(\bar{F}/L)$-module via restriction of the Galois action.

(2) For each prime w of L above p, we set $A_w = A_v$, where v is a prime of F below w, and view it as a $\mathrm{Gal}(\bar{F}_v/L_w)$-module via the appropriate restriction. Note that we then have $d_w = d_v$.

(3) For each real prime w of L which lies above a real prime v of F, we set $A_w^+ = A^{\mathrm{Gal}(\bar{F}_v/F_v)}$ and write $d_w^+ = d_v^+$.

We now record the following lemma which gives some sufficient conditions for equality in **(C4)** to hold for the datum $\big(A, \{A_w\}_{w|p}, \{A_w^+\}_{w|\mathbb{R}}\big)$ over L.

Lemma 2.1. *Suppose that* $\big(A, \{A_v\}_{v|p}, \{A_v^+\}_{v|\mathbb{R}}\big)$ *is a datum defined over* F*. Suppose further that at least one of the following statements holds.*

(i) All the archimedean primes of F *are unramified in* L*.*
(ii) $[L : F]$ *is odd*
(iii) F *has no real primes.*

Then the datum $\big(A, \{A_w\}_{w|p}, \{A_w^+\}_{w|\mathbb{R}}\big)$ *obtained by base change satisfies **(C1)-(C4)**. In particular, we have the equality*

$$\sum_{w|p}(d - d_w)[L_w : \mathbb{Q}_p] = dr_2(L) + \sum_{w \text{ real}} (d - d_w^+).$$

Proof. It remains to verify that **(C4)** holds for $\big(A, \{A_w\}_{w|p}, \{A_w^+\}_{w|\mathbb{R}}\big)$. Note that if either of the assertions in (ii) or (iii) holds, then the assertion in (i) holds. Therefore, to prove the lemma in these cases, it suffices to prove it under the assumption of (i). We first perform the following calculation

$$\begin{aligned}
\sum_{w|p}(d - d_w)[L_w : \mathbb{Q}_p] &= \sum_{v|p}\sum_{w|v}(d - d_v)[L_w : F_v][F_v : \mathbb{Q}_p] \\
&= \sum_{v|p}(d - d_v)[F_v : \mathbb{Q}_p]\sum_{w|v}[L_w : F_v] \\
&= [L : F]\sum_{v|p}(d - d_v)[F_v : \mathbb{Q}_p] \\
&= d[L : F]r_2(F) + [L : F]\sum_{v \text{ real}}(d - d_v^+),
\end{aligned}$$

where the last equality follows from the fact that $\big(A, \{A_v\}_{v|p}, \{A_v^+\}_{v|\mathbb{R}}\big)$ satisfies **(C4)**. Now if (i) holds, then every prime of L above a real prime (resp., complex prime) of F is a real prime (resp., complex prime). Therefore, one has $[L : F]r_2(F) = r_2(L)$ and

$$[L : F]\sum_{v \text{ real}}(d - d_v^+) = \sum_{w \text{ real}}(d - d_w^+).$$

The required conclusion then follows. □

We now define the strict Selmer group associated to our datum following Greenberg [14]. Let S be a finite set of primes of F which contains all the primes above p, the ramified primes of A and all the infinite primes of F. Denote by F_S the maximal algebraic extension of F unramified outside S and write $G_S(\mathcal{L}) = \mathrm{Gal}(F_S/\mathcal{L})$ for every algebraic extension $\mathcal{L}$ of F which is contained in F_S. Let L be a finite extension of F contained in F_S. For a prime w of L lying over S, set

$$H^1_{str}(L_w, A) = \begin{cases} \ker\big(H^1(L_w, A) \longrightarrow H^1(L_w, A/A_w)\big) & \text{if } w \text{ divides } p, \\ \ker\big(H^1(L_w, A) \longrightarrow H^1(L_w^{ur}, A)\big) & \text{if } w \text{ does not divide } p, \end{cases}$$

where L_w^{ur} is the maximal unramified extension of L_w. The (strict) Selmer group attached to the data is then defined by

$$S^{str}(A/L) := \mathrm{Sel}^{str}(A/L) := \ker\Big(H^1(G_S(L), A) \longrightarrow \bigoplus_{w\in S(L)} H^1_s(L_w, A)\Big),$$

where we write $H^1_s(L_w, A) = H^1(L_w, A)/H^1_{str}(L_w, A)$ and $S(L)$ denotes the set of primes of L above S. For an infinite algebraic extension $\mathcal{L}$ of F contained in F_S, we define $S^{str}(A/\mathcal{L}) = \varinjlim_L S^{str}(A/L)$, where the direct limit is taken with respect to the natural maps, as L varies over finite subextensions of the base field F in the larger extension $\mathcal{L}$. We write $X(A/\mathcal{L})$ for its Pontryagin dual.

The following important example of a datum satisfying the conditions above will be used in subsequent discussion in the paper. Assume now for simplicity that F is totally imaginary. Let E be an elliptic curve defined over F with good ordinary reduction at all primes of F above p. Then for each prime v of F above p, we have the following short exact sequence

$$0 \longrightarrow \hat{E}(\bar{F}_v)[p^\infty] \longrightarrow E(\bar{F}_v)[p^\infty] \longrightarrow \tilde{E}(\bar{F}_v)[p^\infty] \longrightarrow 0,$$

where $\hat{E}(\bar{F}_v)$ (resp., $\tilde{E}(\bar{F}_v)$) denotes the associated formal group (resp. the reduced elliptic curve). In this case, our datum will consist of $(E[p^\infty], \{\hat{E}(\bar{F}_v)[p^\infty]\}_{v|p})$. It is easy to check that the equality in condition **(C4)** is satisfied. In this example, the strict Selmer group of E over $\mathcal{L}$ will always be denoted by $S^{str}(E/\mathcal{L})$.

We return to the general setting. For a given set of data $\big(A, \{A_v\}_{v|p}, \{A_v^+\}_{v|\mathbb{R}}\big)$, we define its (Tate) dual data as follows. For an $\mathcal{O}$-module N, let $T_p(N)$ denote its p-adic Tate module, i.e., $T_p(N) = \varprojlim_i N[p^i]$. We then set $A^* = \mathrm{Hom}_{\mathrm{cts}}(T_p(A), \mu_{p^\infty})$. Similarly, for each $v|p$ (resp., v real), we set $A_v^* = \mathrm{Hom}_{\mathrm{cts}}(T_p(A/A_v), \mu_{p^\infty})$ (resp., $(A^*)_v^+ = \mathrm{Hom}_{\mathrm{cts}}(T_p(A/A_v^+), \mu_{p^\infty})$). It is an easy exercise to verify that $\big(A^*, \{A_v^*\}_{v|p}, \{(A^*)_v^+\}_{v|\mathbb{R}}\big)$ satisfies the conditions **(C1)–(C4)** as defined in the beginning of the section. Therefore, we can attach strict Selmer groups to this dual data which will be denoted by $S^{str}(A^*/\mathcal{L})$. The Pontryagin dual of $S^{str}(A^*/\mathcal{L})$ is then denoted by $X(A^*/\mathcal{L})$.

Returning to the elliptic curve example given above, it follows from the Weil pairing that the datum $(E[p^\infty], \{\hat{E}(\bar{F}_v)[p^\infty]\}_{v|p})$ is self-dual in the sense that its dual datum (as defined in the preceding paragraph) coincides with itself. In Section 3, when the elliptic curve E has complex multiplication, we will attach another datum to E which is not self dual.

For now, we continue with our discussion in the general context. As a start, we recall the notion of the μ_G-invariant. Let G be a pro-p group with no p-torsion and M a finitely generated $\mathbb{Z}_p[\![G]\!]$-module. It then follows from [19, Proposition 1.11] (see also [46, Theorem 3.40]) that there is a $\mathbb{Z}_p[\![G]\!]$-homomorphism

$$\varphi : M[p^\infty] \longrightarrow \bigoplus_{i=1}^{s} \mathbb{Z}_p[\![G]\!]/p^{\alpha_i},$$

whose kernel and cokernel are pseudo-null $\mathbb{Z}_p[\![G]\!]$-modules, and where the integers s and α_i are uniquely determined. The μ_G-invariant of M is then defined to be $\mu_G(M) = \sum_{i=1}^{s} \alpha_i$. We are now in a position to state the following.

Proposition 2.2. *Let F_∞ be a pro-p-extension of F which is contained in F_S with Galois group $G = \mathrm{Gal}(F_\infty/F)$ being a compact p-adic Lie group with no p-torsion. Let n be a fixed arbitrary integer. Also, suppose that for every prime υ of F in S, the decomposition group of G at υ has dimension ≥ 1. Then we have*

$$\mu_G\big(X(A/F_\infty)/p^n\big) = \mu_G\big(X(A^*/F_\infty)/p^n\big).$$

Proof. The proof is similar to that in [30, Proposition 4.1.3] (also see the proof of [14, Theorem 2]). Although in these citations, the extensions considered are those containing the cyclotomic $\mathbb{Z}_p$-extension, it has been noted in [30, Remark 4.1.5] that the same proof carries over as long as for each prime $\upsilon \in S$, the decomposition group of $\mathrm{Gal}(F_\infty/F)$ at υ is of dimension 1 which follows from the hypothesis of the proposition. □

Corollary 2.3. *Retain the setting of the preceding proposition. Then $X(A/F_\infty)$ is a finitely generated torsion $\mathbb{Z}_p[\![G]\!]$-module with trivial μ_G-invariant if and only if $X(A^*/F_\infty)$ is a finitely generated torsion $\mathbb{Z}_p[\![G]\!]$-module with trivial μ_G-invariant.*

Furthermore, in the event that $G \cong \mathbb{Z}_p$, we then have that $X(A/F_\infty)$ is finitely generated over $\mathbb{Z}_p$ if and only if $X(A^*/F_\infty)$ is finitely generated over $\mathbb{Z}_p$.

Proof. By [30, Lemma 2.4.1], a $\mathbb{Z}_p[\![G]\!]$-module M is finitely generated torsion with trivial μ_G-invariant if and only if $\mu_G\big(M/p\big) = 0$. The first assertion of the corollary is now an immediate consequence of this and Proposition 2.2.

On the other hand, when $G \cong \mathbb{Z}_p$, it follows from the structure theorem of $\mathbb{Z}_p[\![G]\!]$-modules that a $\mathbb{Z}_p[\![G]\!]$-module M is finitely generated over $\mathbb{Z}_p$ if and only if $\mu_G\big(M/p\big) = 0$. The second assertion of the corollary is then an immediate consequence of this. □

To continue, we need to introduce the mod-p strict Selmer group. For each finite extension L of F contained in F_∞, the mod-p strict Selmer group is defined by

$$S^{str}(A[p]/L) = \ker\Big(H^1(G_S(L), A[p]) \longrightarrow \bigoplus_{w \in S(L)} H^1(L_w, D_w[p])\Big),$$

where $D_w = A/A_w$ or A according as w divides p or not. Write $S^{str}(A[p]/F_\infty) = \varinjlim_L S^{str}(A[p^n]/L)$. We can now record the following theorem which refines [33, Theorem 5.2].

Theorem 2.4. *Let F_∞ be a pro-p-extension of F which is contained in F_S with Galois group $G = \mathrm{Gal}(F_\infty/F)$ being a compact p-adic Lie group with no p-torsion. Also, suppose that for every prime υ of F in S, the decomposition group of G at υ has dimension ≥ 1.*

Then $X(A/F_\infty)$ is a finitely generated torsion $\mathbb{Z}_p[\![G]\!]$-module with trivial μ_G-invariant if and only if $H^2(G_S(F_\infty), A[p]) = 0$ and we have an exact sequence

$$0 \longrightarrow S^{str}(A[p]/F_\infty) \longrightarrow H^1(G_S(F_\infty), A[p]) \longrightarrow \bigoplus_{w\in S(F_\infty)} H^1(F_{\infty,w}, D_w[p]) \longrightarrow 0.$$

To prepare for the proof of the theorem, we need a few preparatory lemmas. As a start, we have the following control theorem.

Lemma 2.5. *Retain the assumptions of Theorem 2.4. The map*

$$S^{str}(A[p]/F_\infty) \longrightarrow S^{str}(A/F_\infty)[p]$$

has kernel and cokernel which are cotorsion $\mathbb{F}_p[\![G]\!]$-modules.

In particular, $S^{str}(A[p]/F_\infty)^\vee$ is torsion over $\mathbb{F}_p[\![G]\!]$ if and only if $X(A/F_\infty)$ is a finitely generated torsion $\mathbb{Z}_p[\![G]\!]$-module with trivial μ_G-invariant.

Proof. The cotorsionness of the kernel and cokernel follows from an argument similar to that in [9, Theorem 4.2], noting that we make use of the hypothesis that the decomposition group of G at v has dimension ≥ 1. It then follows from this that $S^{str}(A[p]/F_\infty)^\vee$ is torsion over $\mathbb{F}_p[\![G]\!]$ if and only if $X(A/F_\infty)/p$ is torsion over $\mathbb{F}_p[\![G]\!]$ (noting that $X(A/F_\infty)/p$ is the Pontryagin dual of $S^{str}(A/F_\infty)[p]$). The latter is equivalent to saying that $X(A/F_\infty)$ is a finitely generated torsion $\mathbb{Z}_p[\![G]\!]$-module with trivial μ_G-invariant by [46, Remark 3.33] (also see [30, Lemma 2.4.1]). □

We shall write $S^*(A^*[p]/F_\infty) = \varprojlim_L \big(S^{str}(A^*[p]/L)\big)$, where L runs though all the intermediate finite extensions of F in F_∞. We first record the following simple observation comparing this inverse limit of Selmer groups with different sets of primes.

Lemma 2.6. *Let S and T be two finite set of primes of F such that $S \subseteq T$. Then we have an injection*

$$S^*_S(A^*[p]/F_\infty) \hookrightarrow S^*_T(A^*[p]/F_\infty),$$

where $S^*_Z(A^*[p]/F_\infty)$ is the Selmer group defined with local conditions over Z, where $Z = S, T$.

Proof. For finite extensions $L \subseteq L'$ of F, it follows from [36, Proposition 1.5.5] that we have the following commutative diagram

$$\begin{array}{ccc} H^1(G_S(L'), A^*[p]) & \xrightarrow{\text{cor}} & H^1(G_S(L), A^*[p]) \\ {\scriptstyle\text{inf}}\big\downarrow & & \big\downarrow{\scriptstyle\text{inf}} \\ H^1(G_T(L'), A^*[p]) & \xrightarrow{\text{cor}} & H^1(G_T(L), A^*[p]) \end{array}$$

noting that $F(A^*[p]) \subseteq F_S \subseteq F_T$. This in turn induces an injection

$$\varprojlim_L H^1(G_S(L), A^*[p]) \hookrightarrow \varprojlim_L H^1(G_T(L), A^*[p]).$$

which fits into the following commutative diagram

$$\begin{array}{ccccccc}
0 \longrightarrow & S_S^*(A^*[p]/F_\infty) & \longrightarrow & \varprojlim_L H^1(G_S(L), A^*[p]) & \longrightarrow & \varprojlim_L \bigoplus_{w\in S(L)} H^1(L_w, D_w^*[p]) \\
 & \downarrow & & \downarrow & & \downarrow \\
0 \longrightarrow & S_T^*(A^*[p]/F_\infty) & \longrightarrow & \varprojlim_L H^1(G_T(L), A[p]) & \longrightarrow & \varprojlim_L \bigoplus_{w\in T(L)} H^1(L_w, D_w[p])
\end{array}$$

hence yielding the required inclusion of the lemma. □

Lemma 2.7. *Let F_∞ be a pro-p-extension of F which is contained in F_S with Galois group $G = \mathrm{Gal}(F_\infty/F)$ being a compact p-adic Lie group with no p-torsion. Also, suppose that for every prime v of F in S, the decomposition group of G at v has dimension ≥ 1. We then have that $S^*(A^*[p]/F_\infty)$ injects into a torsionfree $\mathbb{F}_p[\![G]\!]$-module.*

Proof. By the definition of $S^*(A^*[p]/F_\infty)$, we have an exact sequence

$$0 \longrightarrow S^*(A^*[p]/F_\infty) \longrightarrow H^1_{\mathrm{Iw}}(F_\infty/F, A^*[p]) \xrightarrow{\rho} \bigoplus_{v\in S} H^1_{\mathrm{Iw},v}(F_\infty/F, D_v^*[p]),$$

where $H^1_{\mathrm{Iw}}(F_\infty/F, A^*[p]) = \varprojlim_L H^1(G_S(F), A^*[p])$ and $H^i_{\mathrm{Iw},v}(F_\infty/F, D_v^*[p]) = \varprojlim_L \left(\bigoplus_{w|v} H^1(L_w, D_w^*[p])\right)$. If F_∞ is of dimension ≥ 2, then $H^1_{\mathrm{Iw}}(F_\infty/F, A^*[p])$ is a torsionfree $\mathbb{F}_p[\![G]\!]$-module (cf. [38, Remark before Proposition 3.4] or [45, Theorem 8.4]) and so the conclusion follows immediately in this case.

It remains to verify the lemma when F_∞/F is a 1-dimensional p-adic Lie extension. By Lemma 2.6, we may assume that S contains a prime of F outside p. Furthermore, by base-changing F, if necessary, we may assume that all the primes of S are inert in F_∞/F and hence, by abuse of notation, write v for the prime of F_∞ above v. Recall that Jannsen's spectral sequence (cf. [22, Theorem 1]; also see [32, Theorem 4.5.1] or [35, Theorem 5.4.5]) is given by

$$E^i\Big(H^j\big(G_S(F_\infty), A^*[p]\big)^\vee\Big) \Rightarrow H^{i+j}_{\mathrm{Iw}}(F_\infty/F, A^*[p]),$$

where $E^i(-) = \mathrm{Ext}^i_{\mathbb{F}_p[\![G]\!]}\Big(-, \mathbb{F}_p[\![G]\!]\Big)$. From this spectral sequence, we obtain the following exact sequence

$$0 \longrightarrow A^*(F_\infty)[p] \longrightarrow H^1_{\mathrm{Iw}}(F_\infty/F, A^*[p]) \longrightarrow E^0\Big(H^1\big(G_S(F_\infty), A^*[p]\big)^\vee\Big),$$

where we have made use of the fact that $E^1\Big(\big(A^*(F_\infty)[p]\big)^\vee\Big) \cong A^*(F_\infty)[p]$. The local version of Jannsen's spectral sequence (see [32, Theorem 4.2.2] or [35, Theorem 5.2.6])

$$E^i\Big((H^j(F_{\infty,v}, D_v^*[p]))^\vee\Big) \Rightarrow H^{i+j}_{\mathrm{Iw},v}(F_\infty/F, D_v^*[p]).$$

then yields an exact sequence

$$0 \longrightarrow D_v^*(F_{\infty,v})[p]) \longrightarrow H^1_{\mathrm{Iw},v}(F_\infty/F, A^*[p]) \longrightarrow E^0\Big(H^1(F_{\infty,v}, D_v^*[p])^\vee\Big).$$

By [32, Theorem 4.5.1], the two exact sequences fit into the following commutative diagram

$$\begin{array}{ccccccc}
0 \longrightarrow & A^*(F_\infty)[p] & \longrightarrow & H^1_{\mathrm{Iw}}(F_\infty/F, A^*[p]) & \longrightarrow & E^0\Big(H^1\big(G_S(F_\infty), A^*[p]\big)^\vee\Big) \\
& \Big\downarrow f & & \Big\downarrow \rho & & \Big\downarrow h \\
0 \longrightarrow & \bigoplus_{v\in S} D_v^*(F_{\infty,v})[p] & \longrightarrow & \bigoplus_{v\in S} H^1_{\mathrm{Iw},v}(F_\infty/F, D_v^*[p]) & \longrightarrow & \bigoplus_{v\in S} E^0\Big(H^1_v(F_\infty/F, D_v^*[p])^\vee\Big)
\end{array}$$

Since S contains a prime, say v_0, outside S, the map f at the v_0-component is given by the natural inclusion $A^*(F_\infty)[p] \hookrightarrow A^*(F_{\infty,v_0})[p]$ and hence f is injective. This implies that $S^*(A[p])/F_\infty)$ is contained in $\ker h$ which is in turn contained in $E^0\Big(H^1\big(G_S(F_\infty), A^*[p]\big)^\vee\Big)$. But the latter is a reflexive $\mathbb{F}_p[\![G]\!]$-module and hence torsionfree. This establishes the situation of a 1-dimensional p-adic Lie extension. The proof of the lemma is thus completed. □

We now prove Theorem 2.4.

Proof of Theorem 2.4. Suppose that $H^2(G_S(F_\infty), A[p]) = 0$ and that one has a short exact sequence

$$0 \longrightarrow S^{str}(A[p]/F_\infty) \longrightarrow H^1(G_S(F_\infty), A[p]) \longrightarrow \bigoplus_{w\in S(F_\infty)} H^1(F_{\infty,w}, D_w[p]) \longrightarrow 0.$$

Standard $\mathbb{F}_p[\![G]\!]$-rank calculations (cf. [38, Theorems 3.2 and 4.1]) tell us that

$$\mathrm{rank}_{\mathbb{F}_p[\![G]\!]}\left(H^1(G_S(F_\infty), A[p])^\vee\right) = dr_2(F) + \sum_{v \text{ real}} (d - d_v^+)$$

and

$$\mathrm{rank}_{\mathbb{F}_p[\![G]\!]}\Big(\bigoplus_{w\in S(F_\infty)} H^1(F_{\infty,w}, D_w[p])^\vee\Big) = \sum_{v|p} (d - d_v)[F_v : \mathbb{Q}_p].$$

Combining these calculations with **(C4)**, we have that $S^{str}(A[p]/F_\infty)^\vee$ has zero $\mathbb{F}_p[\![G]\!]$-rank. By Lemma 2.5, it then follows that $X(A/F_\infty)$ is a torsion $\mathbb{Z}_p[\![G]\!]$-module with trivial $\mu_{\mathbb{Z}_p[\![G]\!]}$-invariant.

To prove the converse, we first recall that $S^*(A^*[p]/F_\infty) = \varprojlim_L \big(S^{str}(A^*[p]/L)\big)$, where L runs though all the intermediate finite extensions of F in F_∞. The Poitou-Tate exact sequence gives us the following exact sequence

$$0 \longrightarrow S^{str}(A[p]/F_\infty) \longrightarrow H^1(G_S(F_\infty), A[p]) \longrightarrow \bigoplus_{w\in S(F_\infty)} H^1(F_{\infty,w}, D_w[p]) \longrightarrow$$

$$\longrightarrow S^*(A^*[p]/F_\infty)^\vee \longrightarrow H^2(G_S(F_\infty), A[p]) \longrightarrow 0,$$

where the rightmost zero follows from the fact that $\mathrm{Gal}(\bar{F}_{\infty,w}/F_{\infty,w})$ has p-cohomological dimension ≤ 1 (cf. [36, Theorem 7.1.8(i)]). Since $S^{str}(A[p]/F_\infty)$ is finitely generated over $\mathbb{Z}_p[\![G]\!]$ with trivial μ_G-invariant, it follows from Lemma 2.5 that $S^{str}(A[p]/F_\infty)^\vee$ is torsion over $\mathbb{F}_p[\![G]\!]$. Applying standard $\mathbb{F}_p[\![G]\!]$-rank calculations (cf. [38, Theorems 3.2 and 4.1]) in conjunction with the above exact sequence, we have that $S^*(A^*[p]/F_\infty)$ is torsion over $\mathbb{F}_p[\![G]\!]$. By Lemma 2.7, this forces $S^*(A^*[p]/F_\infty) = 0$. The conclusion now follows by applying this latter observation to the above exact sequence.

We now apply the preceding theorem to the $\mathbb{Z}_p$-extension situation.

Proposition 2.8. *Let F_∞ be a $\mathbb{Z}_p$-extension of F with the property that every prime of F in S decomposes finitely in F_∞/F. Suppose that $X(A/F_\infty)$ is finitely generated over $\mathbb{Z}_p$. Then the following statements hold.*

(a) We have $H^2(G_S(F_\infty), A[p]) = 0$ and there is a short exact sequence

$$0 \longrightarrow S^{str}(A[p]/F_\infty) \longrightarrow H^1(G_S(F_\infty), A[p]) \longrightarrow \bigoplus_{w \in S(F_\infty)} H^1(F_{\infty,w}, D_w[p]) \longrightarrow 0.$$

(b) We have $H^2(G_S(F_\infty), A) = 0$ and there is a short exact sequence

$$0 \longrightarrow S^{str}(A/F_\infty) \longrightarrow H^1(G_S(F_\infty), A) \longrightarrow \bigoplus_{w \in S(F_\infty)} H^1(F_{\infty,w}, D_w) \longrightarrow 0.$$

(c) $X(A/F_\infty)$ is a free $\mathbb{Z}_p$-module. In particular, it has no nontrivial finite $\mathbb{Z}_p[\![\Gamma]\!]$-submodules.

Proof. Since finitely generated $\mathbb{Z}_p$-modules are necessarily $\mathbb{Z}_p[\![\Gamma]\!]$-torsion with trivial $\mu_{\mathbb{Z}_p[\![\Gamma]\!]}$-invariant, statement (a) is an immediate consequence of Theorem 2.4. It then follows from this that we have the following diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & S^{str}(A[p]/F_\infty) & \longrightarrow & H^1(G_S(F_\infty), A[p]) & \longrightarrow & \bigoplus_{w \in S(F_\infty)} H^1(F_{\infty,w}, D_w[p]) & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle a} & & \downarrow{\scriptstyle b} & & \downarrow{\scriptstyle c=\oplus c_w} & & \\
0 & \longrightarrow & S^{str}(A/F_\infty)[p] & \longrightarrow & H^1(G_S(F_\infty), A)[p] & \longrightarrow & \bigoplus_{w \in S(F_\infty)} H^1(F_{\infty,w}, D_w)[p] & &
\end{array}$$

with exact rows. Since c is surjective, it follows that the bottom rightmost map is surjective which in turn yields an injection $\mathrm{Sel}^{str}(A/F_\infty)/p \hookrightarrow H^1(G_S(F_\infty), A)/p$. But $H^1(G_S(F_\infty), A)/p \cong H^2(G_S(F_\infty), A[p]) = 0$. Thus, we have $\mathrm{Sel}^{str}(A/F_\infty)/p = 0$, or equivalently, $X(A/F_\infty)[p] = 0$. This proves (c). Finally, statement (b) now follows from continuing with a similar argument to that in [5, Section 2]. □

Remark 2.9. The nonexistence of nontrivial finite $\mathbb{Z}_p[\![\Gamma]\!]$-submodules for the dual strict Selmer group was established for the cyclotomic $\mathbb{Z}_p$-extension of a non-totally real field F (see [1, Theorem 3.11], [28, Corollary 3.6] and [34, Proposition 7.5]). Proposition 2.8(c) thus generalizes these results by removing the "cyclotomic" and "non-totally real" assumptions.

3. Selmer groups of elliptic curves with CM

Let K be an imaginary quadratic field which the prime p splits completely, say $p = \mathfrak{p}\overline{\mathfrak{p}}$. Fix an integer h such that $\mathfrak{p}^h = (\pi)$ for some $\pi \in \mathcal{O}_K$, where $\mathcal{O}_K$ is the ring of integers of K. Write $\overline{\pi}$ for its corresponding conjugate which in turn is a generator for the ideal $\overline{\mathfrak{p}}^h$. Now if M is an $\mathcal{O}_K$-module, then the multiplication-by-π map defines an endomorphism on M, whose kernel is denoted to be $E[\pi]$. One can similarly define $M[\pi^n]$ for every integer $n \geq 1$. We then write $M[\mathfrak{p}^\infty] = \cup_{n\geq 1} M[\pi^n]$. It is a straightforward exercise to verify that this last definition is independent of the choices of h and π. We may therefore, once and for all, fix a choice of π. In this paper, M is usually taken to be the elliptic curve E or certain local cohomology groups $H^1(L_w, E)$ of E.

Let F_0 be a finite extension of K which is unramified at $\mathfrak{p}$. Let E be an elliptic curve defined over F_0 and assume throughout that our elliptic curve satisfies all of the following conditions.

(a) E has complex multiplication given by the ring of integers of K.
(b) E has good ordinary reduction at all primes of F_0 above p.
(c) $F_0(E_{tor})$ is an abelian extension of K.

Fix a finite extension F of F_0 which is contained in $F_0(E[p])$, and denote by $F_{\mathfrak{p}^\infty}$ the $\mathbb{Z}_p$-extension of F which is contained in $F(E[\mathfrak{p}^\infty])$. By [10, Chap. II, Proposition 1.9], the $\mathbb{Z}_p$-extension $F_{\mathfrak{p}^\infty}/F$ is totally ramified at primes above $\mathfrak{p}$ and finitely decomposed at other nonarchimedean primes.

For every extension L of F, the classical $\mathfrak{p}^\infty$-Selmer group of E over L is defined to be

$$\mathrm{Sel}(E[\mathfrak{p}^\infty]/L) = \ker\left(H^1(L, E[\mathfrak{p}^\infty]) \longrightarrow \prod_w H^1(L_w, E)[\mathfrak{p}^\infty]\right)$$

where w runs through all the primes of L.

Let S denote a finite set of primes of F containing the primes above p, the infinite primes, the primes at which E has bad reduction of E and the primes that are ramified in F/K. Denote by F_S the maximal algebraic extension of F unramified outside S. For every extension L of F contained in F_S, we write $G_S(L) = \mathrm{Gal}(F_S/L)$. Then a standard argument (cf. [8, 1.8]) shows that the $\mathfrak{p}^\infty$-Selmer group can be described as follow

$$\mathrm{Sel}(E[\mathfrak{p}^\infty]/L) = \ker\left(H^1(G_S(L), E[\mathfrak{p}^\infty]) \longrightarrow \bigoplus_{w\in S(L)} H^1(L_w, E)[\mathfrak{p}^\infty]\right),$$

where $S(L)$ denotes the set of primes of L above S. We may now record the following fundamental theorem of Gillard and Schneps.

Theorem 3.1 (Gillard, Schneps). $\mathrm{Sel}(E[\mathfrak{p}^\infty]/F_{\mathfrak{p}^\infty})^\vee$ *is finitely generated over* $\mathbb{Z}_p$.

Proof. Schneps established the result under the assumption that $F = K$ and K has class number one (see [42]). When F is general and K has class number one, the theorem was proved by Gillard in [12]. The class number one hypothesis on K was eventually removed in [11]; also see [10, Chap III, Theorem 2.12]). □

We now give an alternative description of the $\mathfrak{p}^{\infty}$-Selmer group in terms of the strict Selmer group as defined in the previous section. In order to do this, we first define a suitable datum. Set $A = E[\mathfrak{p}^{\infty}]$, and for every prime v above p, set A_v to be $E[\mathfrak{p}^{\infty}]$ or 0 according as v divides $\mathfrak{p}$ or $\overline{\mathfrak{p}}$. As a start, we verify that our datum satisfies the equality in condition **(C4)** (noting that F has no real primes).

Lemma 3.2.

$$\sum_{v|p}\big(\mathrm{corank}_{\mathbb{Z}_p}(A)-\mathrm{corank}_{\mathbb{Z}_p}(A_v)\big)[F_v:\mathbb{Q}_p]=\sum_{v|\overline{\mathfrak{p}}}[F_v:\mathbb{Q}_p]=r_2(F).$$

Proof. The first equality follows immediately from the definition of our datum. For the second, we simply note that

$$\sum_{v|\overline{\mathfrak{p}}}[F_v:\mathbb{Q}_p]=\sum_{v|\overline{\mathfrak{p}}}[F_v:K_{\overline{\mathfrak{p}}}]=[F:K]=\frac{1}{2}[F:\mathbb{Q}]=r_2(F).$$ □

We may now give the following identification of the classical $\mathfrak{p}^{\infty}$-Selmer groups and the strict Selmer group over $F_{\mathfrak{p}^{\infty}}$.

Proposition 3.3.

$$\begin{aligned}\mathrm{Sel}(E[\mathfrak{p}^{\infty}]/F_{\mathfrak{p}^{\infty}}) &= S^{str}(A/F_{\mathfrak{p}^{\infty}})\\ &= \ker\Bigg(H^1(G_S(F_{\mathfrak{p}^{\infty}}),E[\mathfrak{p}^{\infty}])\longrightarrow\bigoplus_{w\in S(F_{\mathfrak{p}^{\infty}}),w\nmid\mathfrak{p}}H^1(F_{\mathfrak{p}^{\infty},w},E[\mathfrak{p}^{\infty}])\Bigg).\end{aligned}$$

Proof. The second equality follows from a standard limit argument (for instance, see [14, §5]). It remains to show that $\mathrm{Sel}(E[\mathfrak{p}^{\infty}]/F_{\mathfrak{p}^{\infty}})$ can be described similarly. To see this, it suffices to show that $H^1(L_w,E)[\mathfrak{p}^{\infty}]=0$ or $H^1(L_w,E[\mathfrak{p}^{\infty}])$ according as w divides $\mathfrak{p}$ or w does not divide $\mathfrak{p}$. We first consider the case when w does not divide $\mathfrak{p}$. Kummer theory yields the following short exact sequence

$$0\longrightarrow E(L_w)\otimes K_{\mathfrak{p}}/\mathcal{O}_{\mathfrak{p}}\longrightarrow H^1(L_w,E[\mathfrak{p}^{\infty}])\longrightarrow H^1(L_w,E)[\mathfrak{p}^{\infty}]\longrightarrow 0.$$

By a theorem of Mattuck, we have $E(L_w)\cong(\mathcal{O}_{L_w})^n\times$(a finite group). Since w is coprime to $\mathfrak{p}$ and hence α, we have $E(L_w)\otimes K_{\mathfrak{p}}/\mathcal{O}_{\mathfrak{p}}=0$. The required equality now follows from this and the Kummer sequence.

For the case when v divides $\mathfrak{p}$, the vanishing of $H^1(L_w,E)[\mathfrak{p}^{\infty}]$ follows from a classical theorem of Coates (see [2, Theorem 12] or [10, Page 125, 1.7]). □

We now consider the (Tate) dual datum of $(A,\{A_v\}_{v|p})$ in the sense of Section 2. By the Weil pairing, this is given by $A^*=E[\overline{\mathfrak{p}}^{\infty}]$, and for every prime v above p, A_v^* is calculated to be 0 or $E[\overline{\mathfrak{p}}^{\infty}]$ according as v divides $\mathfrak{p}$ or $\overline{\mathfrak{p}}$. One easily checks that the strict Selmer group for the dual datum has the following description

$$S^{str}(A^*/F_{\mathfrak{p}^{\infty}})=\ker\Bigg(H^1(G_S(F_{\mathfrak{p}^{\infty}}),E[\overline{\mathfrak{p}}^{\infty}])\longrightarrow\bigoplus_{w\in S(F_{\mathfrak{p}^{\infty}}),w\nmid\overline{\mathfrak{p}}}H^1(F_{\mathfrak{p}^{\infty},w},E[\overline{\mathfrak{p}}^{\infty}])\Bigg).$$

Proposition 3.4.

$$S^{str}(E/F_{\mathfrak{p}^\infty}) = S^{str}(A/F_{\mathfrak{p}^\infty}) \oplus S^{str}(A^*/F_{\mathfrak{p}^\infty}).$$

Proof. It suffices to show the following assertion: for a finite extension L of F and a prime w of L above $\mathfrak{p}$ (resp., $\overline{\mathfrak{p}}$), one has $E(\bar{L}_w)[\mathfrak{p}^\infty] = \hat{E}(\bar{L}_w)[p^\infty]$ (resp. $E(\bar{L}_w)[\overline{\mathfrak{p}}^\infty] = \hat{E}(\bar{L}_w)[p^\infty]$). We will prove the case for $\mathfrak{p}$, the case of $\overline{\mathfrak{p}}$ can be dealt similarly. Since E has good ordinary reduction at w and $\overline{\pi}$ is coprime to $\mathfrak{p}$, multiplication by $\overline{\pi}$ is an automorphism of $\hat{E}(\bar{L}_w)$. This in turn induces an automorphism of $\hat{E}(\bar{L}_w)[p^h]$. Therefore, for every $x \in \hat{E}(\bar{L}_w)[p^h]$, there exists $y \in \hat{E}(\bar{L}_w)[p^h]$ such that $\overline{\pi}y = x$. It then follows that $\pi x = \pi\overline{\pi}y = p^h y = 0$ which implies that $\hat{E}(\bar{L}_w)[\pi] = \hat{E}(\bar{L}_w)[p^h]$. On the other hand, there is a natural injection $\hat{E}(\bar{L}_w)[\pi] \hookrightarrow E(\bar{L}_w)[\pi]$. But since both groups have the same order p^h, the injection must be an isomorphism. This proves $E(\bar{L}_w)[\pi] = \hat{E}(\bar{L}_w)[p^h]$. Similarly, one can prove that $E(\bar{L}_w)[\pi^n] = \hat{E}(\bar{L}_w)[p^{hn}]$ for every $n \geq 1$. The assertion is then a consequence of these observations. □

Theorem 3.5. *The dual strict Selmer group $X(E/F_{\mathfrak{p}^\infty})$ is a free $\mathbb{Z}_p$-module of finite rank.*

Proof. By the theorem of Gillard and Schneps, we have that $\mathrm{Sel}(E[\pi^\infty]/F_{\pi^\infty})^\vee$ is finitely generated over $\mathbb{Z}_p$. The conclusion of the theorem then follows from combining this observation with Corollary 2.3, Propositions 2.8, 3.3 and 3.4. □

We now consider the structure of the Selmer groups over F_∞, where F_∞ is the $\mathbb{Z}_p^2$-extension of F contained in $F_0(E[p^\infty])$. Write $G = \mathrm{Gal}(F_\infty/F)$ and $H_{\mathfrak{p}} = \mathrm{Gal}(F_\infty/F_{\mathfrak{p}^\infty})$. The following result describes the structure of the Selmer groups over F_∞.

Theorem 3.6. *The dual strict Selmer group $X(E/F_\infty)$ is finitely generated over $\mathbb{Z}_p[\![H_{\mathfrak{p}}]\!]$. Furthermore, if $F_0(E[p]) \subseteq F$, then $X(E/F_\infty)$ is a free $\mathbb{Z}_p[\![H_{\mathfrak{p}}]\!]$-module with*

$$\mathrm{rank}_{\mathbb{Z}_p[\![H_{\mathfrak{p}}]\!]}\big(X(E/F_\infty)\big) = \mathrm{rank}_{\mathbb{Z}_p}\big((X(E/F_{\mathfrak{p}^\infty})\big) + |S_{\overline{\mathfrak{p}}}(F_{\mathfrak{p}^\infty})| - 1,$$

where $S_{\overline{\mathfrak{p}}}(F_{\mathfrak{p}^\infty})$ is the set of all primes of $F_{\mathfrak{p}^\infty}$ above $\overline{\mathfrak{p}}$.

Remark 3.7. We note that the dual strict Selmer group $X(E/F_\infty)$ coincides with the classical dual p^∞-Selmer group (cf. [4]). We also note that an analogue of the second assertion of the theorem has been established for $X(E[\mathfrak{p}^\infty]/F_\infty)$ in [41, Theorems 1 and 2]. Our result may therefore be viewed as a refinement of those.

Proof. As noted in the beginning of this section, there are only finitely many primes of F_∞ above S (cf. [10, Chap. II, Proposition 1.9]). Therefore, the proof of [9, Lemma 2.4] carries over to show that the map

$$X(E/F_\infty)_{H_{\mathfrak{p}}} \longrightarrow X(E/F_{\mathfrak{p}^\infty})$$

has kernel and cokernel which are finitely generated over $\mathbb{Z}_p$. We then conclude from Theorem 3.5 that $X(E/F_\infty)_{H_{\mathfrak{p}}}$ is finitely generated over $\mathbb{Z}_p$. By Nakayama lemma, this implies that $X(E/F_\infty)$ is finitely generated over $\mathbb{Z}_p[[H_\mathfrak{p}]]$. To prove the second assertion, we proceed as in [41]. Since $F_0(E[p]) \subseteq F$, E has good ordinary reduction everywhere at F. Hence we may assume $S = S_p(F)$, where $S_p(F)$ is the set of primes of F above p. Consider the following diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & S(E/F_{\mathfrak{p}^\infty}) & \longrightarrow & H^1(G_S(F_{\mathfrak{p}^\infty}), E[p^\infty]) & \longrightarrow & \bigoplus_{w\in S_p(F_{\mathfrak{p}^\infty})} H^1(F_{\mathfrak{p}^\infty,w}, D_w[p]) & \longrightarrow & 0 \\ & & \downarrow s & & \downarrow h & & \downarrow g=\oplus g_w & & \\ 0 & \longrightarrow & S(E/F_\infty)^{H_\mathfrak{p}} & \longrightarrow & H^1(G_S(F_\infty), E[p^\infty])^{H_\mathfrak{p}} & \longrightarrow & \Big(\bigoplus_{u\in S_p(F_\infty)} H^1(F_{\infty,u}, D_u)\Big)^{H_\mathfrak{p}} & & \end{array}$$

with exact rows. By a similar argument to that in Proposition 2.8, we have that $H^1(H_\mathfrak{p}, S(E/F_\infty)) = 0$. Thus, by [29, Lemma 4.5], we have that

$$\mathrm{rank}_{\mathbb{Z}_p[[H_\mathfrak{p}]]}\big(X(E/F_\infty)\big) = \mathrm{rank}_{\mathbb{Z}_p}\big((X(E/F_{\mathfrak{p}^\infty})_{H_\mathfrak{p}}\big).$$

By a diagram chasing argument, the latter is equal to

$$\mathrm{rank}_{\mathbb{Z}_p}\big((X(E/F_{\mathfrak{p}^\infty})\big) + \mathrm{corank}_{\mathbb{Z}_p}\big(\ker g\big) - \mathrm{corank}_{\mathbb{Z}_p}\big(\ker h\big).$$

Since $F_0(E[p]) \subseteq F$, it follows that $F_{\mathfrak{p}^\infty} = F(E[\mathfrak{p}^\infty])$ and $F_\infty = F(E[p^\infty])$. Hence we have

$$\ker h = H^1(H_\mathfrak{p}, E[p^\infty]) = E[\mathfrak{p}^\infty]_{H_\mathfrak{p}} \oplus E[\overline{\mathfrak{p}}^\infty]_{H_\mathfrak{p}} = E[\mathfrak{p}^\infty]$$

which in turn implies that $\mathrm{corank}_{\mathbb{Z}_p}\big(\ker h\big) = 1$. For each $w \in S_p(F_\infty)$, we note that $D_w = E[\overline{\mathfrak{p}}^\infty]$ or $E[\mathfrak{p}^\infty]$ according as w divides $\mathfrak{p}$ or $\overline{\mathfrak{p}}$. A similar argument to that for $\ker h$ shows that $\ker g_w = 0$ or $E[\mathfrak{p}^\infty]$ according as w divides $\mathfrak{p}$ or $\overline{\mathfrak{p}}$. This in turns yields $\mathrm{corank}_{\mathbb{Z}_p}\big(\ker g_w\big) = 0$ or 1 according as w divides $\mathfrak{p}$ or $\overline{\mathfrak{p}}$. Combining these calculations, we obtain the required rank formula. Finally, we note that our calculation also shows that $\ker g$ is a cofree $\mathbb{Z}_p$-module. From the exact sequence

$$0 \longrightarrow (\ker g)^\vee \longrightarrow X(E/F_\infty)_{H_\mathfrak{p}} \longrightarrow X(E/F_{\mathfrak{p}^\infty})$$

and noting that $X(E/F_{\mathfrak{p}^\infty})$ has no p-torsion (cf. Proposition 3.5), we have that $X(E/F_\infty)_{H_\mathfrak{p}}$ has no p-torsion. Hence $X(E/F_\infty)_{H_\mathfrak{p}}$ is a free $\mathbb{Z}_p$-module.

Write $H_\mathfrak{p}^n = H_\mathfrak{p}^{p^n}$ for the unique subgroup of $H_\mathfrak{p}$ of index p^n. A similar diagram chasing argument as above shows that $X(E/F_\infty)_{H_\mathfrak{p}^n}$ is a free $\mathbb{Z}_p$-module for every n. By the structure theory of finitely generated $\mathbb{Z}_p[[H_\mathfrak{p}]]$-modules, this implies that $X(E/F_\infty)$ is a free $\mathbb{Z}_p[[H_\mathfrak{p}]]$-module. □

We have seen in the preceding theorem that when $F_0(E[p]) \subseteq F$, $X(E/F_\infty)$ is a free $\mathbb{Z}_p[[H_\mathfrak{p}]]$-module which, in particularly, implies that $X(E/F_\infty)[p^\infty] = 0$. It turns out that this latter assertion holds in general without the "$F_0(E[p]) \subseteq F$" assumption.

Corollary 3.8. *We always have $X(E/F_\infty)[p^\infty] = 0$.*

Proof. This can be proved by a similar argument following [28, Lemma 4.2] which we recall for convenience. Let L be an intermediate finite subextension of F_∞/F. By the descent argument as in the beginning of the proof of Theorem 3.6, we have that $X(E/L_{\mathfrak{p}^\infty})$ is finitely generated over $\mathbb{Z}_p$, where here we write $L_{\mathfrak{p}^\infty} = LF_{\mathfrak{p}^\infty}$. But since $X(E/F_\infty) = \varprojlim_L X(E/L_{\mathfrak{p}^\infty})$ and by Proposition 2.8(c), the multiplication by p map on $X(E/L_{\mathfrak{p}^\infty})$ is injective, it follows that the multiplication by p map on $X(E/F_\infty)$ is also injective. □

Now denote by F^{cyc} the cyclotomic $\mathbb{Z}_p$-extension of F, and write $H = \mathrm{Gal}(F_\infty/F^{\mathrm{cyc}})$. Recall from [3, 9] that $X(E/F_\infty)$ is said to satisfy the $\mathfrak{M}_H(G)$-conjecture if $X(E/F_\infty)/X(E/F_\infty)[p^\infty]$ is finitely generated over $\mathbb{Z}_p[\![H]\!]$. By Corollary 3.8, this in turn implies that in our complex multiplication situation, the $\mathfrak{M}_H(G)$-conjecture is equivalent to saying that $X(E/F_\infty)$ is finitely generated over $\mathbb{Z}_p[\![H]\!]$ which we formally state below.

Corollary 3.9. *Retain the settings of this section. Then $X(E/F_\infty)$ satisfies the $\mathfrak{M}_H(G)$-conjecture if and only if $X(E/F_\infty)$ is finitely generated over $\mathbb{Z}_p[\![H]\!]$.*

We should emphasis that when E does not have CM, the $\mathfrak{M}_H(G)$-conjecture is in general not equivalent to $\mathbb{Z}_p[\![H]\!]$-finite generation! Here is an example to illustrate this. Let E be the elliptic curve 11a2 of Cremona's table. Take $p = 5$, $F = \mathbb{Q}(\mu_5)$ and $F_\infty = \mathbb{Q}(E[5^\infty])$. It is well-known that F_∞ is a strongly admissible 5-adic extension of F. Furthermore, it follows from [8, Theorem 5.4] that $X(E/F^{\mathrm{cyc}})$ is finitely generated over $\mathbb{Z}_5$ which, by [9, Theorem 2.1], then implies that $X(E/F_\infty)$ is finitely generated over $\mathbb{Z}_5[\![H]\!]$. Now let E' be either 11a1 or 11a3. It follows from [3, Lemma 5.6] that $X(E'/F_\infty)$ satisfies the $\mathfrak{M}_H(G)$-conjecture. Therefore, we may apply [26, Theorem 3.1] to conclude that $\mu_G(X(E'/F_\infty)) = \mu_\Gamma(X(E'/F^{\mathrm{cyc}}))$. But this latter quantity is well-known to be nonzero (cf. [8, Theorem 5.28]) and hence $X(E'/F_\infty)$ is not finitely generated over $\mathbb{Z}_5[\![H]\!]$.

4. Some remarks on fine Selmer groups

The results in the previous section have some interesting consequences on the structure of the fine Selmer group which we now describe. As before, K is an imaginary quadratic field at which the prime p splits completely, and F_0 is a finite extension of K which is unramified at $\mathfrak{p}$. Let E be an elliptic curve defined over F_0 which is assumed to satisfy all of the following conditions.

(a) E has complex multiplication given by the ring of integers of K.
(b) E has good ordinary reduction at all primes of F_0 above p.
(c) $F_0(E_{tor})$ is an abelian extension of K.

Fix a finite extension F of F_0 which is contained in $F_0(E[p])$. For a finite extension L of F, the fine Selmer group of an elliptic curve E over L (cf. [6, 29]) is defined by

$$R(E/L) = \ker\Big(H^1(G_S(L), E[p^\infty]) \longrightarrow \bigoplus_{w\in S(L)} H^1(L_w, E[p^\infty])\Big).$$

For an algebraic (possibly infinite) extension $\mathcal{L}$ of F, we set $R(E/\mathcal{L}) = \varinjlim_{L} R(E/L)$, where L runs over all finite extension L of F contained in $\mathcal{L}$.

The following is the main result of this section.

Proposition 4.1. *The dual fine Selmer group $R(E/F_\infty)^\vee$ has trivial μ_G-invariant.*

Proof. It follows from Theorem 3.6 and [18, Lemma 2.7] that $X(E/F_\infty)$ is a finitely generated torsion $\mathbb{Z}_p[\![G]\!]$-module with trivial μ_G-invariant. Since $R(E/F_\infty)^\vee$ is a quotient of $X(E/F_\infty)$, the conclusion follows immediately. □

Remark 4.2. We emphasise that the above proposition is proven under the standing assumption that F_0/K is unramified at $\mathfrak{p}$. Had we worked with the stronger assumption that F_0/K is unramified at p, then we can give an alternative simpler proof which we now do. As noted above, it suffices to show that $X(E/F_\infty)$ is a torsion $\mathbb{Z}_p[\![G]\!]$-module with trivial μ_G-invariant. Since $X(E/F_\infty)$ is the direct sum of $S^{str}(E[\mathfrak{p}^\infty]/F_\infty)^\vee$ and $S^{str}(E[\overline{\mathfrak{p}}^\infty]/F_\infty)^\vee$, it suffices to do this for each of the summand. By Proposition 3.5, $S^{str}(E[\mathfrak{p}^\infty]/F_{\mathfrak{p}^\infty})^\vee$ is finitely generated over $\mathbb{Z}_p$ with no p-torsion. By a similar argument to that in Proposition 3.6, we can show that $S^{str}(E[(\mathfrak{p}^\infty]/F_\infty)^\vee$ is a torsion $\mathbb{Z}_p[\![G]\!]$-module with trivial μ_G-invariant. Since F_0/K is assumed to be unramified at p and hence at $\overline{\mathfrak{p}}$, we can apply a similar argument as above to show that $S^{str}(E[(\overline{\mathfrak{p}}^\infty]/F_\infty)^\vee$ is a torsion $\mathbb{Z}_p[\![G]\!]$-module with trivial μ_G-invariant via the $F_{\overline{\mathfrak{p}}^\infty}$-direction.

We now describe how Proposition 4.1 can be viewed as a weak partial support to the Conjecture A of Coates-Sujatha [6]. Denote by F^{cyc} the cyclotomic $\mathbb{Z}_p$-extension of F. Conjecture A then asserts that $R(E/F^{\mathrm{cyc}})^\vee$ is finitely generated over $\mathbb{Z}_p$. Under the assumption of the validity of Conjecture A, it follows from a standard descent argument (cf. [6, Lemma 3.1]) that $R(E/F_\infty)^\vee$ is finitely generated over $\mathbb{Z}_p[\![H]\!]$, where $H = \mathrm{Gal}(F_\infty/F^{\mathrm{cyc}})$. By a result of Howson [18, Lemma 2.7], this in turn implies that $R(E/F_\infty)^\vee$ has trivial μ_G-invariant. Our proposition thus verifies this latter prediction.

We end this section with the next result which gives a first instance where the $\mathfrak{M}_H(G)$-conjecture and Conjecture A are related.

Proposition 4.3. *Suppose further that the $\mathfrak{M}_H(G)$-conjecture is valid for $X(E/F_\infty)$. Then $R(E/F^{\mathrm{cyc}})^\vee$ is finitely generated over $\mathbb{Z}_p$.*

Proof. Since $R(E/F^{\mathrm{cyc}})^\vee$ is a quotient of $X(E/F^{\mathrm{cyc}})$, the conclusion follows immediately from Corollary 3.9. □

5. Analogue of Conjecture A over $F_{\mathfrak{p}^\infty}$ and relation with Conjecture B

In this section, we discuss an analogue of Conjecture A for the $\mathbb{Z}_p$-extension $F_{\mathfrak{p}^\infty}/F$ and its consequences. It seems that this has not been observed in the literature before, and hence we record this formally.

Proposition 5.1. *The dual fine Selmer group $R(E/F_{\mathfrak{p}^\infty})^\vee$ is a finitely generated $\mathbb{Z}_p$-module.*

Proof. This follows immediately from Theorem 3.5 and the fact that $R(E/F_{\mathfrak{p}^\infty})^\vee$ is a quotient of $X(E/F_{\mathfrak{p}^\infty})$. □

Of course, it is already well-known that the weak Leopoldt conjecture for $E[\mathfrak{p}^\infty]$ over $F_{\mathfrak{p}^\infty}$ is valid (cf. [39]). Here we can record the presumably stronger assertion, namely, the weak Leopoldt conjecture for $E[p^\infty]$ over $F_{\mathfrak{p}^\infty}$ is also valid.

Corollary 5.2. $H^2(G_S(F_{\mathfrak{p}^\infty}), E[p^\infty]) = 0.$

In view of Proposition 5.1, we can ask for a formula for the $\mathbb{Z}_p[\![H_\mathfrak{p}]\!]$-rank of $R(E/F_\infty)^\vee$ analogous to [6, Theorem 4.11]. This is precisely the next result. Here we write $H^2_{\mathrm{Iw}}(F_\infty/F, T_pE)\big) = \varprojlim H^2(G_S(L), T_pE)\big)$, where L runs through all the finite extensions L of F contained in F_∞ and the inverse limit is taken with respect to the corestriction maps.

Proposition 5.3. *Suppose that $F_0(E[p]) \subseteq F$. Then the dual fine Selmer group $R(E/F_\infty)^\vee$ is a finitely generated $\mathbb{Z}_p[\![H_\mathfrak{p}]\!]$-module with*

$$\mathrm{rank}_{\mathbb{Z}_p[\![H_\mathfrak{p}]\!]}\left(R(E/F_\infty)^\vee\right) = \mathrm{rank}_{\mathbb{Z}_p}\left(R(E/F_{\mathfrak{p}^\infty})^\vee\right) + |S_p(F_{\mathfrak{p}^\infty})| - 1$$
$$- \mathrm{rank}_{\mathbb{Z}_p}\left(H_1(H_\mathfrak{p}, H^2_{\mathrm{Iw}}(F_\infty/F, T_pE))\right),$$

where $S_p(F_{\mathfrak{p}^\infty})$ is the set of all primes of $F_{\mathfrak{p}^\infty}$ above p.

Proof. The proof is entirely similar to that in [6, Theorem 4.11]. □

In [6, Conjecture B], Coates and the second author conjectured that $R(E/F_\infty)^\vee$ is pseudo-null over $\mathbb{Z}_p[\![G]\!]$. The preceding proposition gives a criterion for this to hold (compare with [6, Theorem 4.11]).

Corollary 5.4. *Retain the settings of Proposition 5.3. Then $R(E/F_\infty)^\vee$ is pseudo-null over $\mathbb{Z}_p[\![G]\!]$ if and only if*

$$\mathrm{rank}_{\mathbb{Z}_p}\left(R(E/F_{\mathfrak{p}^\infty})^\vee\right) + |S_p(F_{\mathfrak{p}^\infty})| = 1 + \mathrm{rank}_{\mathbb{Z}_p}\left(H_1(H_\mathfrak{p}, H^2_{\mathrm{Iw}}(F_\infty/F, T_pE))\right).$$

Proof. Since $R(E/F_\infty)^\vee$ is finitely generated over $\mathbb{Z}_p[\![H_\mathfrak{p}]\!]$, it follows from a theorem of Venjakob [47] that $R(E/F_\infty)^\vee$ is pseudo-null over $\mathbb{Z}_p[\![G]\!]$ if and only if it is torsion over $\mathbb{Z}_p[\![H_\mathfrak{p}]\!]$. The corollary is now immediate from the preceding proposition. □

We end this section saying a bit more on the background of Conjecture B. To some extent, this conjecture can be thought as an analogue to a conjecture of Greenberg which we now describe. Recall that a Galois extension F_∞ of F is said to be a strongly admissible pro-p, p-adic Lie extension of F if (i) $G = \mathrm{Gal}(F_\infty/F)$ is a compact pro-p, p-adic Lie group without p-torsion, (ii) F_∞ contains the cyclotomic $\mathbb{Z}_p$ extension F^{cyc} of F and (iii) F_∞ is unramified outside a finite set of primes. Denote by $K(F_\infty)$ the maximal unramified abelian pro-p extension of F_∞ in which every prime above p splits completely. When F_∞ is the composite of all the $\mathbb{Z}_p$-extensions of F, Greenberg [15] conjectured that $\mathrm{Gal}(K(F_\infty)/F_\infty)$ is pseudo-null over $\mathbb{Z}_p[\![G]\!]$. (Actually, to be more precise, Greenberg's original conjecture is concerned with the pseudo-nullity of a slightly bigger Galois group. For a discussion of the relation between the original conjecture of Greenberg and the slightly weaker version adopted here, we refer readers to [25, Subsection 4.2].) For a general noncommutative F_∞, the module $\mathrm{Gal}(K(F_\infty)/F_\infty)$ is not necessarily pseudo-null, and this was first observed by Hachimori and Sharifi (see [16]). Despite the counterexamples constructed by Hachimori and Sharifi, Coates and the second named author have expressed optimism that the corresponding assertion for the dual fine Selmer group of an abelian variety should hold regardless of the strongly admissible extension F_∞ (see [6, Section 4]). Motivated by the close relationship between the Iwasawa μ-conjecture and Conjecture A, one might ask for an analogue relationship for the Greenberg conjecture and Conjecture B. Of course, the observations of Hachimori and Sharifi tell us that such a relation may not hold directly. Nevertheless, we may still ask whether there exists an implication of Conjecture B from Greenberg conjecture. Some (very) partial results in this direction have been obtained, and we refer the interested readers to [27, 33] for further discussion on these.

6. Further remark on Conjecture B

We now describe an interesting consequence of Conjecture B. Here we shall assume that our elliptic curve E is defined over an imaginary quadratic field K and has complex multiplication by $\mathcal{O}_K$. To facilitate further discussion, we need to introduce certain notations. Let $F_n = K(E[p^{n+1}])$. For each prime v_n of F_n above $\mathfrak{p}$, we let U_{n,v_n} denote the local units of F_{n,v_n} which are congruent to 1 modulo v_n. Write $U_n = \prod_{v_n} U_{n,v_n}$. Denote C_n for the group of elliptic units of F_n (see [10, Chap. II, §2] for definition). There is a natural map from C_n to U_n via the diagonal map and we denote the closure of this image by $\bar{C}_n$. The global units of F_n is then denoted by $\mathcal{E}_n$, and its closure in U_n by $\bar{\mathcal{E}}_n$. Write $\bar{\mathcal{E}}_\infty = \varprojlim_n \bar{\mathcal{E}}_n$. We have similar definitions for U_∞, $\bar{C}_\infty$. Denote by $M_\mathfrak{p}(F_\infty)$ (resp. $M(F_\infty)$) the maximal abelian pro-p extension of F_∞ unramified outside $\mathfrak{p}$ (resp. unramified everywhere). Class field theory then gives us an exact sequence

$$0 \longrightarrow \bar{\mathcal{E}}_\infty/\bar{C}_\infty \longrightarrow U_\infty/\bar{C}_\infty \longrightarrow \mathrm{Gal}(M_\mathfrak{p}(F_\infty)/F_\infty) \longrightarrow \mathrm{Gal}(M(F_\infty)/F_\infty) \longrightarrow 0.$$

Proposition 6.1. *The following statements are equivalent.*

(1) Conjecture B is valid for $R(E/F_\infty)^\vee$. In other words, $R(E/F_\infty)^\vee$ is pseudo-null over $\mathbb{Z}_p[\![G]\!]$.
(2) $\bar{\mathcal{E}}_\infty/\bar{C}_\infty = 0$.

Proof. By [6, Lemma 3.8], $R(E/F_\infty) = \mathrm{Hom}(\mathrm{Gal}(K(F_\infty)/F_\infty), E[p^\infty])$, where $K(F_\infty)$ is the maximal unramified abelian pro-p extension of F_∞ at which every prime of F_∞ splits completely. It follows that $R(E/F_\infty)^\vee$ is pseudo-null over $\mathbb{Z}_p[\![G]\!]$ if and only if $\mathrm{Gal}(K(F_\infty)/F_\infty)$ is pseudo-null over $\mathbb{Z}_p[\![G]\!]$. It then follows from [25, Théorème 4.4] that the latter assertion holds if and only if $\mathrm{Gal}(M(F_\infty)/F_\infty)$ is also pseudo-null over $\mathbb{Z}_p[\![G]\!]$ which, by [40, Theorem 4.1(i)], is equivalent to saying that $\mathcal{E}_\infty/\bar{C}_\infty$ is pseudo-null over $\mathbb{Z}_p[\![G]\!]$. Now by the work of Yager (cf. [49]; also see

[10, Chap III §1]), we know that $U_\infty/\bar{C}_\infty$ has no nonzero pseudo-null $\mathbb{Z}_p[\![G]\!]$-submodule. Hence the equivalence of statements (1) and (2) is now a consequence of this observation and the above discussion. □

We now mention a similar observation in the classical case. To do so, we now write F_n for the field $\mathbb{Q}(\mu_{p^{n+1}})^+$. Let C_n^1 be the group generated by the cyclotomic units modulo 1 in F_n (see [7, Definitions 4.3.2 and 4.3.3]) and U_n^1 the group associated to local units modulo 1 (see [7, Definition 4.3.3]). We also write $\mathcal{E}_n^1$ for the global units of F_n modulo 1 (cf. [7, Definition 4.5.1]). Denote by $\mathcal{E}_\infty^1$ the inverse limit of $\mathcal{E}_n^1$ taken with respect to the norm maps. We also have similar definitions for U_∞^1, C_∞^1. It follows from [7, Theorem 4.5.2] that we have an exact sequence

$$0 \longrightarrow \mathcal{E}_\infty^1/C_\infty^1 \longrightarrow U_\infty^1/C_\infty^1 \longrightarrow \mathrm{Gal}(M_p(F^{\mathrm{cyc}})/F^{\mathrm{cyc}}) \longrightarrow \mathrm{Gal}(M(F^{\mathrm{cyc}})/F^{\mathrm{cyc}}) \longrightarrow 0,$$

where $M_p(F^{\mathrm{cyc}})$ is the maximal abelian pro-p extension of F_∞ unramified outside p. Then we have the following proposition which is the classical analogue of Proposition 6.1.

Proposition 6.2. *The following statements are equivalent.*

(1) $\mathrm{Gal}(M(F^{\mathrm{cyc}})/F^{\mathrm{cyc}})$ *is finite.*
(2) $\mathcal{E}_\infty^1/C_\infty^1 = 0$.

Proof. The proof is similar to that in Proposition 6.1 noting that U_∞^1/C_∞^1 has no nontrivial finite $\mathbb{Z}_p[\![\Gamma]\!]$-submodules (see [7, Proof of Theorem 4.6.3]). □

The finiteness of $\mathrm{Gal}(M(F^{\mathrm{cyc}})/F^{\mathrm{cyc}})$ is a special case of a conjecture of Greenberg [13]. In the situation here, one in fact expects that $\mathrm{Gal}(M(F^{\mathrm{cyc}})/F^{\mathrm{cyc}}) = 0$ and this is the so-called Kummer-Vandiver Conjecture (or one of its equivalent form). When p is a regular prime, this conjecture vacuously holds. For irregular primes, this has been numerically verified up to primes less than 2^{31} (see [17] and the references therein for history and prior calculations before). We finally mention that it is already known that under the validity of the Kummer-Vandiver Conjecture, one has $\mathcal{E}_\infty^1/C_\infty^1 = 0$ (see [7, Proposition 4.5.3]). The point of Proposition 6.2 is that this vanishing is equivalent to the *a priori* weaker conjecture of Greenberg. We also mention that Proposition 6.2 is an old observation of Greenberg (we thank Thong Nguyen Quang Do and Romyar Sharifi for pointing this out to us).

In fact, Proposition 6.2 can be extended to a more general setting, and we are very grateful to Thong Nguyen Quang Do for explaining this to us. Let F denote an abelian totally real field, where the F_n's now stand for the intermediate subfields of F^{cyc}/F. We then write C_{F_n} for the circular units of F_n in the sense of Sinnott [43]. Write $\bar{C}_{F_n} = C_{F_n} \otimes \mathbb{Z}_p$. The global units of F_n is still denoted by $\mathcal{E}_{F_n}$. As before, we write $\mathcal{E}_\infty$ and $\bar{C}_\infty$ for the respective inverse limits.

Proposition 6.3. *Suppose that for every* $m \geq n \geq 0$, *we have* $\bar{C}_{F_m}^{\mathrm{Gal}(F_m/F_n)} = \bar{C}_{F_n}$. *Then the following statements are equivalent.*

(1) $\mathrm{Gal}(M(F^{\mathrm{cyc}})/F^{\mathrm{cyc}})$ *is finite.*
(2) $\mathcal{E}_\infty/C_\infty = 0$.

Proof. A similar argument as before shows that statement (1) is equivalent to saying that $\mathcal{E}_\infty/C_\infty$ is finite. On the other hand, it is known that under the hypothesis of the proposition that the projective dimension of $\mathcal{E}_\infty/C_\infty$ as a $\mathbb{Z}_p[\![\Gamma]\!]$-module is ≤ 1, or equivalently, $\mathcal{E}_\infty/C_\infty$ has no nontrivial finite $\mathbb{Z}_p[\![\Gamma]\!]$-submodule. The proposition is now an immediate consequence of these. □

We finally note that the criterion of Proposition 6.3 is satisfied in many cases (see [37, Proposition 2.4]).

References

[1] A. Chandrakant Sharma, Non existence of finite Λ-submodules of dual Selmer groups over a cyclotomic $\mathbb{Z}_p$-extension, *J. Ramanujan Math. Soc.*, **24(1)** (2009) 75–85.

[2] J. Coates, Infinite descent on elliptic curves with complex multiplication. Arithmetic and geometry, Vol. I, 107–137, *Progr. Math.* 35, Birkhäuser (1983).

[3] J. Coates, T. Fukaya, K. Kato, R. Sujatha and O. Venjakob, The GL_2 main conjecture for elliptic curves without complex multiplication, *Publ. Math. IHES*, **101** (2005) 163–208.

[4] J. Coates and R. Greenberg, Kummer theory for abelian varieties over local fields, *Invent. Math.*, **124** (1996) 129–174.

[5] J. Coates, P. Schneider and R. Sujatha, Links between cyclotomic and GL_2 Iwasawa theory, *Doc. Math.*, (2003) 187–215, Extra Volume: Kazuya Kato's fiftieth birthday.

[6] J. Coates and R. Sujatha, Fine Selmer groups of elliptic curves over p-adic Lie extensions, *Math. Ann.*, **331(4)** (2005) 809–839.

[7] J. Coates and R. Sujatha, Cyclotomic Fields and Zeta Values, Springer Monogr. Math. Springer-Verlag, Berlin (2006).

[8] J. Coates and R. Sujatha, Galois Cohomology of Elliptic Curves, 2nd Ed., Tata Institute of Fundamental Research Lectures on Mathematics, 88. Published by Narosa Publishing House, New Delhi; for the Tata Institute of Fundamental Research, Mumbai, 2010.

[9] J. Coates and R. Sujatha, On the $\mathfrak{M}_H(G)$-conjecture, in Non-abelian Fundamental Groups and Iwasawa Theory, eds J. Coates, M. Kim, F. Pop, M. Saidi and P. Schneider, *London Math. Soc. Lecture Note Ser.* 393, Cambridge Univ. Press (2012) 132–161.

[10] E. de Shalit, Iwasawa theory of elliptic curves with complex multiplication, *Perspectives in mathematics*, Academic Press, vol. 3 (1987).

[11] R. Gillard, Fonctions L p-adiques des corps quadratiques imaginaires et de leurs extensions abeliennes, *J. Reine Angew Math*, **358** (1985) 76–91.

[12] R. Gillard, Transformation de Mellin-Leopoldt des fonctions elliptiques, *J. Number Theory*, **25** (1987) 379–393.

[13] R. Greenberg, On the Iwasawa invariants of totally real number fields, *Amer. J. Math.*, **98** (1976) 263–284.

[14] R. Greenberg, Iwasawa theory for p-adic representations, in Algebraic Number Theory-in honor of K. Iwasawa, ed. J. Coates, R. Greenberg, B. Mazur and I. Satake, *Adv. Std. in Pure Math.*, **17** (1989) 97–137.

[15] R. Greenberg, Iwasawa theory-past and present, in: Class field Theory-its centenary and prospect, *Adv. Std. in Pure Math.*, **30** (2001) 335–385.

[16] Y. Hachimori and R. Sharifi, On the failure of pseudo-nullity of Iwasawa modules, *J. Alg. Geom.*, **14(3)** (2005) 567–591.

[17] W. Hart, D. Harvey and W. Ong, Irregular primes to two billion, *Math. Comp.*, **86** (2017) 3031–3049.

[18] S. Howson, Euler characteristics as invariants of Iwasawa modules, *Proc. London Math. Soc. (3)*, **85(3)** (2002) 634–658.

[19] S. Howson, Structure of central torsion Iwasawa modules, *Bull. Soc. Math. France*, **130(4)** (2002) 507–535.

[20] K. Iwasawa, On the μ-invariants of $\mathbb{Z}_l$-extensions, in: Number Theory, Algebraic Geometry and Commutative Algebra, in honour of Yasuo Akizuki, Kinokuniya, Tokyo, (1973) 1–11.

[21] K. Iwasawa, On $\mathbb{Z}_l$-extensions of algebraic number fields, *Ann. of Math.*, **98** (1973) 246–326.

[22] U. Jannsen, A spectral sequence for Iwasawa adjoints, *Münster J. Math.*, **7(1)** (2014) 135–148.

[23] K. Kato, p-adic Hodge theory and values of zeta functions of modular forms, in Cohomologies p-adiques et applications arithmétiques III, *Astérque*, **295** (2004) no. ix, 117–290.

[24] S. Kobayashi, Iwasawa theory for ellliptic curves at supersingular primes, *Invent. Math.*, **152** (2003) 1–36.

[25] A. Lannuzel and T. Nguyen Quang Do, Conjectures de Greenberg et extensions pro-p-libres d'un corps de nombres, *Manuscripta Math.*, **102** (2000) 187–209.

[26] M. F. Lim, A remark on the $\mathfrak{M}_H(G)$-conjecture and Akashi series, *Int. J. Number Theory*, **11(1)** (2015) 269–297.

[27] M. F. Lim, On the pseudo-nullity of the dual fine Selmer groups, *Int. J. Number Theory*, **11(7)** (2015) 2055–2063.

[28] M. F. Lim, Akashi series, characteristic elements and congruence of Galois representations, *Int. J. Number Theory*, **12(3)** (2016) 593–613.

[29] M. F. Lim, Notes on the fine Selmer groups, *Asian J. Math.*, **21** (2017) no. 2, 337–362.

[30] M. F. Lim, Comparing the π-primary submodules of the dual Selmer groups, *Asian J. Math*, **21** (2017) no. 6, 1153–1182.

[31] M. F. Lim and V. K. Murty, The growth of fine Selmer groups, *J. Ramanujan Math. Soc.*, **31(1)** (2016) 79–94.

[32] M. F. Lim and R. Sharifi, Nekovář duality over p-adic Lie extensions of global fields, *Doc. Math.*, **18** (2013) 621–678.

[33] M. F. Lim and R. Sujatha, Fine Selmer groups of congruent Galois representations, *J. Number Theory*, **187** (2018) 66–91.

[34] K. Matsuno, Finite Λ-submodules of Selmer groups of abelian varieties over cyclotomic $\mathbb{Z}_p$-extensions, *J. Number Theory*, **99(2)** (2003) 415–443.

[35] J. Nekovář, Selmer complexes, *Astrisque*, **310** (2006) viii+559 pp.

[36] J. Neukirch, A. Schmidt and K. Wingberg, Cohomology of Number Fields, 2nd Ed., *Grundlehren Math. Wiss.*, Springer, **323** (2008).

[37] T. Nguyen Quang Do and M. Lescop, Iwasawa Descent and Co-descent for Units Modulo Circular Units (with an appendix by J.-R. Belliard). *Pure Appl. Math. Q.*, **2** (2006) no. 2, Special Issue: In honor of John H. Coates. Part 2, 465–496.

[38] Y. Ochi and O. Venjakob, On ranks of Iwasawa modules over p-adic Lie extensions, *Math. Proc. Cambridge Philos. Soc.*, **135** (2003) 25–43.

[39] B. Perrin-Riou, Arithmetique des courbes elliptiques et theórie d'Iwasawa, *Mém. Soc. Math. Fr.*, **17** (1984).

[40] K. Rubin, The main conjectures of Iwasawa theory for imaginary quadratic fields, *Invent. Math*, **103** (1991) 25–68.

[41] A. Saikia, Selmer groups of elliptic curves with complex multiplication, *Canad. J. Math.*, **56(1)** (2004) 194–208.

[42] L. Schneps, On the μ-invariant of p-adic L-functions attached to elliptic curves with complex multiplication, *J. Number Theory*, **25** (1987) 20–33.

[43] W. Sinnott, On the Stickelberger ideal and the circular units of an abelian field, *Invent. Math*, **62** (1981) 181–234.

[44] R. Sujatha, Elliptic curves and Iwasawa's $\mu = 0$ conjecture, in: Quadratic forms, linear algebraic groups, and cohomology, *Dev. Math.*, Springer, New York, **18** (2010) 125–135.
[45] O. Thomas and O. Venjakob, On spectral sequences for Iwasawa adjoints à la Jannsen for families, arXiv:1710.1084[math.NT].
[46] O. Venjakob, On the structure theory of the Iwasawa algebra of a p-adic Lie group, *J. Eur. Math. Soc.*, **4(3)** (2002) 271–311.
[47] O. Venjakob, A non-commutative Weierstrass preparation theorem and applications to Iwasawa theory, *J. Reine Angew. Math.*, **559** (2003) 153–191.
[48] C. Wuthrich, Iwasawa theory of the fine Selmer group, *J. Alg. Geom.*, **16** (2007) 83–108.
[49] R. I. Yager, On two variable p-adic L-functions, *Ann. Math.*, **115(2)** (1982) 411–449.