UNIWERSYTET IM. ADAMA MICKIEWICZA W POZNANIU

WYDZIAŁ MATEMATYKI I INFORMATYKI

FUNCTIONES ET APPROXIMATIO
COMMENTARII MATHEMATICI

54.2 (2016)

WYDAWNICTWO NAUKOWE UAM

FUNCTIONES ET APPROXIMATIO
COMMENTARII MATHEMATICI

UNIWERSYTET IM. ADAMA MICKIEWICZA W POZNANIU
WYDZIAŁ MATEMATYKI I INFORMATYKI

FUNCTIONES ET APPROXIMATIO
COMMENTARII MATHEMATICI

54.2 (2016)

WYDAWNICTWO NAUKOWE

POZNAŃ 2016

Functiones et Approximatio
Commentarii Mathematici

Address: Faculty of Mathematics and Computer Science, Adam Mickiewicz University, ul. Umultowska 87, 61-614 Poznań, Poland.

CONTENTS

Part 1

Part 2

Functiones et Approximatio
54.2 (2016), 141–149
doi: 10.7169/facm/2016.54.2.1

CALCULATING POWER INTEGRAL BASES BY USING RELATIVE POWER INTEGRAL BASES

István Gaál, László Remete, Tímea Szabó

Abstract: Let $M \subset K$ be number fields. We consider the relation of relative power integral bases of K over M with absolute power integral bases of K over $\mathbb{Q}$. We show how generators of absolute power integral bases can be calculated from generators of relative ones. We apply our ideas in infinite families of octic fields with quadratic subfields.

Keywords: octic fields, relative quartic extension, power integral basis, relative power integral basis.

1. Introduction: monogenity in the absolute and relative case

Monogenity of number fields and the calculation of generators of power integral bases is a classical topic of algebraic number theory c.f. [17], [6]. We have general algorithms for calculating generators of power integral bases in lower degree number fields, [15], [13], [8], [1]. We only have partial results for higher degree fields [3], [10], [9], [11], [4].

Let K be an algebraic number field of degree n with ring of integers $\mathbb{Z}_K$. This field is *monogene* if $\mathbb{Z}_K$ is a simple ring extension of $\mathbb{Z}$, that is there exist $\vartheta \in \mathbb{Z}_K$ such that $\mathbb{Z}_K = \mathbb{Z}[\vartheta]$. In this case $\{1, \vartheta, \dots, \vartheta^{n-1}\}$ is an integral basis of K, called *power integral basis*. If $\alpha_1, \alpha_2 \in \mathbb{Z}_K$ are related by $\alpha_1 \pm \alpha_2 \in \mathbb{Z}$ then the elements α_1, α_2 are called *equivalent*. These elements have the same indices (see below) and α_1 generates a power integral basis of K if and only if α_2 does. Up to equivalence there are only finitely many generators of power integral bases of K.

We also considered monogenity and power integral bases in the *relative case* [5], [12], [16]. The element ϑ generates a *relative power integral basis* of K over the subfield M if $\mathbb{Z}_K = \mathbb{Z}_M[\vartheta]$ ($\mathbb{Z}_M$ denotes the ring of integers of M). In the relative case we call $\alpha_1, \alpha_2 \in \mathbb{Z}_K$ *equivalent* if $\alpha_1 + \varepsilon\alpha_2 \in \mathbb{Z}_M$ for some unit ε in M. These

The first author was supported in part by K115479 from the Hungarian National Foundation for Scientific Research.

2010 Mathematics Subject Classification: primary: 11R04; secondary: 11Y50

elements have the same relative indices (see below) and α_1 generates a relative power integral basis of K over M if and only if α_2 does. Up to equivalence there are only finitely many generators of relative power integral bases of K over M.

In the present paper we describe the relation of the generators of relative power integral bases with the generators of absolute ones. We show how the generators of relative power integral bases can be used to calculate generators of absolute power integral bases.

The algorithm is especially simple if M is a quadratic field. We apply our method to three infinite families of octic fields with imaginary quadratic subfields.

2. From relative power integral bases to absolute ones

Let M be an algebraic number field of degree m and K an extension of M with $[K : M] = k$. Then we have $[K : \mathbb{Q}] = k \cdot m$. Let $\mathcal{O}$ be either the ring of integers $\mathbb{Z}_K$ of K or an order in $\mathbb{Z}_K$. Denote by $\mathbb{Z}_M$ the ring of integers of M. We assume that there exist a relative integral basis of $\mathcal{O}$ over M. (As we shall see in the following the existence of a power integral basis of $\mathcal{O}$ implies the existence of a relative power integral basis.)

Denote by $D_{\mathcal{O}}$ and D_M the discriminants of $\mathcal{O}$ and the subfield M, respectively. (In case $\mathcal{O} = \mathbb{Z}_K$ we have $D_{\mathcal{O}} = D_K$ where D_K is the discriminant of the field K.) The *index* of a primitive element α of $\mathcal{O}$ with respect to the order $\mathcal{O}$ is

$$I_{\mathcal{O}}(\alpha) = \frac{\sqrt{|D(\alpha)|}}{\sqrt{|D_{\mathcal{O}}|}}. \tag{1}$$

We also have

$$I_{\mathcal{O}}(\alpha) = (\mathcal{O}^+ : \mathbb{Z}[\alpha]^+) = (\mathcal{O}^+ : \mathbb{Z}_M[\alpha]^+) \cdot (\mathbb{Z}_M[\alpha]^+ : \mathbb{Z}[\alpha]^+), \tag{2}$$

where the indices of the additive groups of the corresponding rings are calculated. The first factor is just the *relative index* of α:

$$I_{\mathcal{O}/M}(\alpha) = (\mathcal{O}^+ : \mathbb{Z}_M[\alpha]^+).$$

Denote by $D_{\mathcal{O}/M}$ the relative discriminant of $\mathcal{O}$ over M. As it is well known

$$D_{\mathcal{O}} = N_{M/\mathbb{Q}}(D_{\mathcal{O}/M}) \cdot D_M^{[K:M]}. \tag{3}$$

Denote by $\gamma^{(i)}$ the conjugates of any $\gamma \in M$ $(i = 1, \dots, m)$. Let $\delta^{(i,j)}$ be the images of $\delta \in K$ under the automorphisms of K leaving the conjugate field $M^{(i)}$ elementwise fixed $(j = 1, \dots, k)$. Then for any primitive element $\alpha \in \mathcal{O}$ we have

$$\begin{aligned} I_{\mathcal{O}/M}(\alpha) &= \frac{\sqrt{|N_{M/\mathbb{Q}}(D_{\mathcal{O}/M}(\alpha))|}}{\sqrt{|N_{M/\mathbb{Q}}(D_{\mathcal{O}/M})|}} \\ &= \frac{1}{\sqrt{|N_{M/\mathbb{Q}}(D_{\mathcal{O}/M})|}} \cdot \prod_{i=1}^{m} \prod_{1 \leqslant j_1 < j_2 \leqslant k} \left| \alpha^{(i,j_1)} - \alpha^{(i,j_2)} \right|. \end{aligned} \tag{4}$$

Further, by (1), (2), (3) and (4) we have

$$J(\alpha) = (\mathbb{Z}_M[\alpha]^+ : \mathbb{Z}[\alpha]^+)$$
$$= \frac{1}{\sqrt{|D_M|}^{[K:M]}} \cdot \prod_{1 \leqslant i_1 < i_2 \leqslant m} \prod_{j_1=1}^{k} \prod_{j_2=1}^{k} \left| \alpha^{(i_1,j_1)} - \alpha^{(i_2,j_2)} \right|. \tag{5}$$

The element α generates a power integral basis of $\mathcal{O}$ if and only if $I_{\mathcal{O}}(\alpha) = 1$. Here we formulate the straightforward consequences of it, which will be very useful in our calculations in the following sections.

By (2), $I_{\mathcal{O}}(\alpha) = 1$ can only be satisfied if both factors of (2) are equal to 1. Therefore,

Proposition 1. *A primitive element $\alpha \in \mathcal{O}$ generates a power integral basis of $\mathcal{O}$, if and only if*

$$I_{\mathcal{O}/M}(\alpha) = 1$$

and

$$J(\alpha) = (\mathbb{Z}_M[\alpha]^+ : \mathbb{Z}[\alpha]^+) = 1. \tag{6}$$

Hence we have

Corollary 2. *If α generates a power integral basis of $\mathcal{O}$, then it generates a relative power integral basis of $\mathcal{O}$ over M.*

It is well known that generators or relative power integral bases are determined up equivalence, that is up to multiplication by a unit in M and up to translation by element of $\mathbb{Z}_M$. Hence

Proposition 3. *If α generates a power integral basis of $\mathcal{O}$, then*

$$\alpha = A + \varepsilon \cdot \alpha_0, \tag{7}$$

where α_0 is a generator of a relative power integral basis of $\mathcal{O}$ over M, ε is a unit in M and $A \in \mathbb{Z}_M$.

Summarizing, in order to determine all generators of power integral bases of $\mathcal{O}$ we have to perform the following steps:

Step 1: Determine up to equivalence all generators $\alpha_0 \in \mathcal{O}$ of relative power integral bases of $\mathcal{O}$ over M.

In other words, determine all elements $\alpha_0 \in \mathcal{O}$ with relative index 1:

$$I_{\mathcal{O}/M}(\alpha_0) = 1.$$

Note that if α_0 has relative index 1, then by means of equivalence any α of the form (7) also has relative index 1.

Step 2: Given α_0 determine ε and A so that α of (7) has $J(\alpha) = 1$.

Let $\mu_1 = 1, \mu_2, \ldots, \mu_m$ be an integral basis of M. Then the above A can be represented in the form

$$A = a_1 + a_2\mu_2 + \ldots + a_k\mu_k. \tag{8}$$

Since the (absolute) index is invariant under translation by an element of $\mathbb{Z}$, we have to calculate $a_2, \ldots, a_m$ of (8) up to sign. Step 2 means to determine ε and $a_2, \ldots, a_k$ satisfying (6). In view of (5) this yields to solve an equation of degree $k^2m(m-1)/2$ depending on ε and $a_2, \ldots, a_k$.

This later task can became very complicated. However if M is an imaginary quadratic field, then there are only finitely many units ε in M and we get a polynomial equation in one variable a_2. We shall apply our method in this case in the following examples of infinite parametric families of octic number fields.

3. Simplest D_4 octics

Recently B.K.Spearman and K.S.Williams [18] studied the family of simplest D_4 octics. Let $t > 0$ be an integer parameter and ϑ a root of the polynomial $x^8 + (t^2+2)x^4 + 1$. They showed that these polynomials are irreducible, and the field $K = \mathbb{Q}(\vartheta)$ has Galois group D_4. Assuming that t^2+4 is square free they calculated the discriminant of K and gave an integral basis of K. By

$$x^8 + (t^2+2)x^4 + 1 = (x^4 + itx^2 + 1)(x^4 - itx^2 + 1)$$

$M = \mathbb{Q}(i)$ is a subfield of K.

Here we restrict ourselves to parameters of the form $t = 2T^2$. We explicitely describe all generators of relative power integral bases of the order $\mathcal{O} = \mathbb{Z}_M[\vartheta]$ over $\mathbb{Z}_M$. Moreover we show that the order $\mathcal{O}$ admits no power integral bases.

3.1. Relative power integral bases in the family of D_4 octics

Let T be a nonzero integer parameter and K the algebraic number field generated by a root ϑ of the polynomial $f(x) = x^8 + (4T^4+2)x^4 + 1$. Let $M = \mathbb{Q}(i)$. Denote by $\mathbb{Z}_K$ (resp. $\mathbb{Z}_M$) the ring of integers of K (resp. M). Consider the order $\mathcal{O} = \mathbb{Z}_M[\vartheta]$ of K.

Our purpose is to explicitely determine all generators of relative power integral bases of $\mathcal{O}$ over M. Obviously, any $\alpha \in \mathcal{O}$ can be written in the form

$$\alpha = A + X\vartheta + Y\vartheta^2 + Z\vartheta^3 \tag{9}$$

with $A, X, Y, Z \in \mathbb{Z}_M$.

Theorem 4. *Assume $T > 11$. Up to equivalence all generators of relative power integral bases of $\mathcal{O}$ over $\mathbb{Z}_M$ are given by*

$$\begin{aligned}
&\alpha = \vartheta,\\
&\alpha = -2iT^2\vartheta + \vartheta^3,\\
&\alpha = (1+4T^4)\vartheta \pm (1+i)T\vartheta^2 + 2iT^2\vartheta^3,\\
&\alpha = \pm(1+i)T\vartheta^2 + \vartheta^3.
\end{aligned}$$

Proof of Theorem 4. The octic polynomial $f(x)$ can be written as

$$f(x) = (x^4 + 2iT^2x^2 + 1)(x^4 - 2iT^2x^2 + 1)$$

hence the relative defining polynomial of ϑ over M is $x^4 - 2iT^2x^2 + 1$. In our proof we use the result of I.Gaál and M.Pohst [12] on power integral bases in relative quartic extensions (cf. also [6]).

According to [12] the coefficients $X, Y, Z \in \mathbb{Z}_M$ of α in (9) must satisfy

$$\begin{aligned} F(U,V) &= (U - 2iT^2V)(U - 2V)(U + 2V) = \varepsilon, \\ Q_1(X,Y,Z) &= X^2 - 2iT^2Y^2 + 4iT^2XZ + (1 - 4T^4)Z^2 = U, \\ Q_2(X,Y,Z) &= Y^2 - XZ - 2iT^2Z^2 = V, \end{aligned}$$

with a unit ε of M and with $U, V \in \mathbb{Z}_M$. We have to determine the solutions $U, V \in \mathbb{Z}_M$ of the first equation and for all pairs U, V to calculate the corresponding solutions X, Y, Z of the second and third equations. By the first equation we have $U - 2V = \varepsilon_1$ and $U + 2V = \varepsilon_2$ with units $\varepsilon_1, \varepsilon_2 \in M$. Therefore $4V = \varepsilon_2 - \varepsilon_1$. Since all units in M are $\pm 1, \pm i$, the only $V \in \mathbb{Z}_M$ satisfying this equation is $V = 0$. Hence U is again a unit in M. Following the method of [12] we set

$$Q_0(X,Y,Z) = UQ_2(X,Y,Z) - VQ_1(X,Y,Z) = 0.$$

Using standard arguments described in [12] we can parametrize X, Y, Z with parameters $P, Q \in \mathbb{Z}_M$ so that up to a unit factor we get

$$X = P^2 - 2iT^2Q^2, \qquad Y = PQ, \qquad Z = Q^2. \tag{10}$$

Substituting the formulas (10) into $Q_1(X,Y,Z) = U$ we obtain a quartic relative Thue equation over M:

$$P^4 - 2iT^2P^2Q^2 + Q^4 = \varepsilon, \tag{11}$$

with a unit ε in M. This equation can be written in the form

$$P^4 - ((1+i)T)^2P^2Q^2 + Q^4 = \varepsilon, \tag{12}$$

therefore we may apply the results of V.Zielger [19] on the solution of this equation by taking $t = (1+i)T$ as parameter. Theorem 2 of [19] implies that, assuming $|t^2| > 245$, that is $|T| > 11$, up to unit factors of M all solutions of (11) are

$$(P,Q) = (1,0),\ (0,1),\ (1, \pm(1+i)T),\ ((1+i)T, \pm 1). \tag{13}$$

Substituting these vales of (P,Q) into (10) we obtain the possible triplets:

	x	y	z
Case 1	1	0	0
Case 2	$-2iT^2$	0	1
Case 3	$1 + 4T^4$	$\pm(1+i)T$	$2iT^2$
Case 4	0	$\pm(1+i)T$	1

(14)

This proves Theorem 4. ■

3.2. Power integral bases in the family of D_4 octics

Despite of the promising result on relative power integral bases we have

Theorem 5. *For $|T| > 11$ the order $\mathcal{O}$ admits no power integral bases.*

Proof of Theorem 5. In view of (7) a generator α of a power integral basis of $\mathcal{O}$ must be of the form $\alpha = a_1 + a_2 i + \varepsilon\alpha_0$ where $a_1, a_2 \in \mathbb{Z}$, $\varepsilon = \pm 1, \pm i$ and the possibe values of α_0 are listed in Theorem 4. Any α of the above form has relative index $I_{\mathcal{O}/M}(\alpha) = 1$. The index of α is independent of a_1 and it is sufficient to determine α up to sign. Therefore we have to consider the possible values of α_0 and for $\varepsilon = 1$, $\varepsilon = i$ and we have to calculate $J(\alpha)$. We have $D_M = -4$ hence

$$J(\alpha) = \frac{1}{2^4} \prod_{j_1=1}^{4} \prod_{j_2=1}^{4} \left| \alpha^{(1,j_1)} - \alpha^{(2,j_2)} \right|.$$

In Case 1 we get

$$J(\alpha) = 2^4 \cdot |(4T^2a_2^2 - 1 + 4a_2^2)(4T^2a_2^2 + 1 - 4a_2^2)(T^8 + 8a_2^4T^4 + 16a_2^8 + 16a_2^4)|.$$

Hence $J(\alpha)$ is divisible by 2^4, yielding that α can not be a generator of a power integral basis.

In the other cases we got much more complicated formulas, but in each case $J(\alpha)$ is divisible by 2^4. ∎

3.3. Remarks on the numerical calculations

All calculations involved in the proof of Theorem 5 were performed in Maple [2] under Linux. $J(\alpha)$ is a polynomial with integer coefficients of degree 16 in a_2, depending also heavily on the parameter T. We used symmetric polynomials several times to simplify the formulas. Without being very careful the formulas became extremely complicated and Maple broke down in lack of memory space. Using careful approach all calculations took less than 2 minutes.

4. Composites of imaginary quadratic fields and pure quartic fields

In a recent paper [14] we considered number fields of type $K = \mathbb{Q}(\sqrt[4]{m}, i\sqrt{d})$ for $d = 3, 7, 11, 19, 43, 67, 163$ and for $1 < m \leqslant 5000$, $m \equiv 2, 3 \pmod 4$ with $(d, m) = 1$. Set $\xi = \sqrt[4]{m}, \omega = (1 + i\sqrt{d})/2$, then

$$\{1, \xi, \xi^2, \xi^3, \omega, \omega\xi, \omega\xi^2, \omega\xi^3\}$$

is an integral basis of K and $\{1, \xi, \xi^2, \xi^3\}$ is a relative integral basis of K over $M = \mathbb{Q}(i\sqrt{d})$. In [14] we described all generators

$$\alpha = A + X\xi + Y\xi^2 + Z\xi^3$$

of relative power integral bases of K over M with $A, X, Y, Z \in \mathbb{Z}_M$ and $\max(\overline{|X|}, \overline{|Y|}, \overline{|Z|}) < 10^{500}$ (here $\overline{|X|}$ denotes the size of X that is the maximum absolute value of its conjugates). The problem lead us to a quartic relative binomial Thue equation. Using the algorithm of [7] we calculated the "small" solutions of this equation which resulted Theorem 3 of [14]. Note that according to our experience these equations never have "large" solutions hence our list contains all solutions with high probability. Further, calculating the "small" solutions was the only way to deal with thousands of relative Thue equations.

Using the ideas of Section 2 we tested if there exist generators of power integral bases of K over $\mathbb{Q}$ corresponding to the relative power integral bases found in Theorem 3 of [14]. We have

Theorem 6. *Let $d = 3, 7, 11, 19, 43, 67, 163$ and $1 < m \leqslant 5000$ with $m \equiv 2, 3 \pmod 4$ and $(d, m) = 1$. Then the number field $K = \mathbb{Q}(\sqrt[4]{m}, i\sqrt{d})$ does not admit any generators of power integral bases of the form*

$$\alpha = A + \varepsilon(X\xi + Y\xi^2 + Z\xi^3)$$

where $A \in \mathbb{Z}_M$, ε a unit in M and $X, Y, Z \in \mathbb{Z}_M$ with

$$\max(\overline{|X|}, \overline{|Y|}, \overline{|Z|}) < 10^{500}.$$

Proof of Theorem 6. For all possible values of X, Y, Z listed in Theorem 3 of [14] and for all possible unit ε in M we set $A = a_1 + a_2\omega$. We calculated $J(\alpha)$ which is a polynomial in a_2 with integral coefficients of degree 16. In each case we found that $J(\alpha) = \pm 1$ is not solvable for a_2 in integers. Calculation with polynomials with integer coefficients was very fast, the whole calculation took a few seconds. ■

5. Parametric families of quartic extensions of imaginary quadratic fields

In [16] we calculated generators of relative power integral bases in infinite parametric families of orders of certain octic fields. Here in two of these families we check if there exist corresponding generators of (absolute) power integral bases. The challenge of these examples is that $J(\alpha)$ depends not only on a_2 but also on the quadratic field and the parameter of the family.

I. Let $d > 0$ be an integer, $-d \equiv 2, 3 \pmod 4$ and set $M = \mathbb{Q}(i\sqrt{d})$. Let $t \in \mathbb{Z}_M$ be a parameter and let ξ be a root of the polynomial

$$f(x) = x^4 - t^2x^2 + 1.$$

Consider $\mathcal{O} = \mathbb{Z}_M[\xi]$. In [16] we showed that for $|t| > 245$ up to equivalence there are five generators of relative power integral bases of $\mathcal{O}$ over $\mathbb{Z}_M$, namely

$$\alpha_0 = \xi, -t^2\xi + \xi^3, (1 - t^4)\xi + t\xi^2 + t^2\xi^3, (1 - t^4)\xi - t\xi^2 + t^2\xi^3, t\xi^2 + \xi^3, -t\xi^2 + \xi^3.$$

We have

Theorem 7. *Under the above conditions for $|t| > 245$ the order $\mathcal{O}$ admits no power integral bases.*

Proof of Theorem 7. Denote by α_0 a possible generator of a relative power integral basis of $\mathcal{O}$ over $\mathbb{Z}_M$, say

$$\alpha_0 = (1-t^4)\xi + t\xi^2 + t^2\xi^3$$

where $t = t_1 + t_2 i\sqrt{d}$ is the parameter ($t_1, t_2 \in \mathbb{Z}$). Note that since the minimal polynomial of ξ over $\mathbb{Z}_M$ depends on the parameter $t \in \mathbb{Z}_M$, hence ξ depends on t and also on d. We let $\varepsilon = \pm 1$ and represent α in the form

$$\alpha = a_1 + a_2 i\sqrt{d} + \varepsilon\alpha_0$$

with $a_1, a_2 \in \mathbb{Z}$. Then we calculate $J(\alpha)$. This is a very complicated polynomial of degree 16 depending not only on a_2 but also on t_1, t_2, d. Using symmetric polynomials and simplifying the formulas very carefully, we obtain that $J(\alpha)$ is disvisible by 16. Therefore there are no generators of power integral bases of $\mathcal{O}$ corresponding to α_0. The proof runs the same way for the other four candidates of α_0, as well. The Maple calculation took 10-60 seconds per case. ■

II. Let again $d > 0$ be an integer, $-d \equiv 2, 3 \pmod 4$, $M = \mathbb{Q}(i\sqrt{d})$. Let $t \in \mathbb{Z}_M$ be a parameter and let ξ be a root of the polynomial

$$f(x) = x^4 - 4tx^3 + (6t+2)x^2 + 4tx + 1.$$

Let $\mathcal{O} = \mathbb{Z}_M[\xi]$. According to [16] for $|t| > 1544803$ up to equivalence there are two generators of power integral bases of $\mathcal{O}$ over $\mathbb{Z}_M$, namely

$$\alpha_0 = \xi, (6t+2)\xi - 4t\xi^2 + \xi^3.$$

We have

Theorem 8. *Under the above conditions for $|t| > 1544803$ the order $\mathcal{O}$ admits no power integral bases.*

The proof of this statement is similar to the proof of Theorem 7.

References

[1] Y. Bilu, I. Gaál and K. Győry, *Index form equations in sextic fields: a hard computation*, Acta Arithm. **115.1** (2004), 85-96.

[2] B.W. Char, K.O. Geddes, G.H. Gonnet, M.B. Monagan, S.M. Watt (eds.) *MAPLE, Reference Manual*, Watcom Publications, Waterloo, Canada, 1988.

[3] I. Gaál, *Power integral bases in composits of number fields*, Canad. Math. Bull. **41** (1998), 158–161.

[4] I. Gaál, *Solving index form equations in fields of degree nine with cubic subfields*, J. Symbolic Comput. **30** (2000), 181-193.
[5] I. Gaál, *Power integral bases in cubic relative extensions*, Experimental Math., **10** (2001), 133–139.
[6] I. Gaál, *Diophantine equations and power integral bases*, Boston, Birkhäuser, 2002.
[7] I. Gaál, *Calculating "small" solutions of relative Thue equations*, Experimantal Math. **24** (2015), 1-8.
[8] I. Gaál and K. Győry, *Index form equations in quintic fields*, Acta Arith. **89** (1999), 379–396.
[9] I. Gaál, *Computing all power integral bases in orders of totally real cyclic sextic number fields*, Math. Comp. **65** (1996), 801–822.
[10] I. Gaál, P. Olajos and M. Pohst, *Power integral bases in orders of composits of number fields*, Experimental Math. **11** (2002), 87–90.
[11] I. Gaál and M. Pohst, *On the resolution of index form equations in sextic fields with an imaginary quadratic subfield*, J.Symbolic Comp. **22** (1996), 425–434.
[12] I. Gaál and M. Pohst, *On the resolution of index form equations in relative quartic extensions*, J.Number Theory **85** (2000), 201–219.
[13] I. Gaál, A. Pethő and M. Pohst, *Simultaneous representation of integers by a pair of ternary quadratic forms – with an application to index form equations in quartic number fields*, J.Number Theory **57** (1996), 90–104.
[14] I. Gaál, L. Remete and T. Szabó, *Calculating power integral bases by solving relative Thue equations*, Tatra Mt. Math. Publ. **59** (2014), 79–92.
[15] I. Gaál and N. Schulte, *Computing all power integral bases of cubic number fields*, Math. Comput. **53** (1989), 689–696.
[16] I. Gaál and T. Szabó, *Relative power integral bases in infinite families of quartic extensions of quadratic field*, JP Journal of Algebra, Number Theory and Applications **29** (2013), 31–43.
[17] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, Second Edition, Springer, 1974.
[18] B.K. Spearman and K.S. Williams, *The simplest D_4 octics*, Int. J. Algebra **2** (2008), 79–89.
[19] V. Ziegler, *On a family of relative quartic Thue inequalities*, J. Number Theory **120** (2006), 303–325.

Address: István Gaál, László Remete amd Tímea Szabó: University of Debrecen, Mathematical Institute, H–4010 Debrecen Pf.12., Hungary.

E-mail: igaal@science.unideb.hu, remetel42@gmail.com, szabo.timea@science.unideb.hu

Received: 12 June 2015; **revised:** 6 August 2015

Functiones et Approximatio
54.2 (2016), 151–161
doi: 10.7169/facm/2016.54.2.2

ON THE NUMBER OF REPRESENTATIONS OF CERTAIN QUADRATIC FORMS IN 20 AND 24 VARIABLES

B. Ramakrishnan, Brundaban Sahu

Abstract: In this paper, we find the number of representations of certain quadratic forms in 20 and 24 variables. We get this as an application of the evaluation of certain triple convolution sums of the divisor functions. Further, by comparing our formulas with that of Lomadze, we get expressions of certain cusp forms in terms of some finite sums involving the solution set of the quadratic form representation.

Keywords: convolution sums of the divisor functions, representation numbers of quadratic forms, modular forms of one variable.

1. Introduction

For positive integers a, b, s, t, define the convolution sum $W_{a,b}^{s,t}(n)$ by

$$W_{a,b}^{s,t}(n) := \sum_{\substack{l,m\in\mathbb{N}\\ al+bm=n}} \sigma_s(l)\sigma_t(m). \tag{1}$$

When $s = t = 1$, it is denoted by $W_{a,b}(n)$, and $W_{a,1}(n) = W_{1,a}(n)$ is denoted by $W_a(n)$. These type of sums were evaluated as early as the 19th century. For example, the sum $W_1(n)$ was evaluated by M. Besge, J. W. L. Glaisher and S. Ramanujan [2, 4, 14]. Some of the convlotution sums of the above type have been obtained by several authors (see for example [5, 15, 12, 17] and also the works of K. S. Williams and his co-authors ([16] and the references therein)).

We now define the triple convolution sums of the divisor functions by

$$W_{a,b,c}^{r,s,t}(n) := \sum_{\substack{l,m,p\in\mathbb{N}\\ al+bm+cp=n}} \sigma_r(l)\sigma_s(m)\sigma_t(p), \tag{2}$$

where $a, b, c, r, s, t \in \mathbb{N}$. We write $W_{a,b,c}^{1,1,1}(n) = W_{a,b,c}(n)$ for $a, b, c \in \mathbb{N}$. In [1], Alaca et al. evaluated the convolution sums $W_{1,2,2}(n), W_{1,1,2}(n)$ and $W_{1,2,4}(n)$

2010 Mathematics Subject Classification: primary: 11A25, 11E25; secondary: 11E20, 11F11

by expressing the product of Eisentein series in terms of their derivatives. In [7, p.11], Kim et al. have treated the convolution sum $W_{1,1,1}(n)$ and as an application, they prove that certain q-series satisfy a particular differential equation. Using the theory of modular forms and quasimodular forms, in this article, we evaluate the convolution sums $W^{1,3,3}_{a,b,c}(n)$, where $(a,b,c) \in \{(1,1,1),(1,1,3),(1,3,3),(3,1,1),(3,3,1)\}$ and $W^{3,3,3}_{a,b,c}(n)$, where $(a,b,c) \in \{(1,1,1),(1,1,3),(1,3,3)\}$. As an application, we find formulas for the number of representations of the quadratic forms

$$F_k : x_1^2 + x_1x_2 + x_2^2 + \ldots + x_{2k-1}^2 + x_{2k-1}x_{2k} + x_{2k}^2,$$

when $k = 10, 12$. Let

$$s_{2k}(n) = \text{card}\left\{(x_1, x_2, \cdots, x_{2k}) \in \mathbb{Z}^{2k} : F_k(x_1, x_2, \cdots, x_{2k}) = n\right\}$$

be the number of representations of a positive integer n by the quadratic form F_k. For $k = 2, 4, 6, 8$ formulas for s_{2k} are known due to the works of J. Liouville [9], J. G. Huard et al. [5], O. X. M. Yao and E. X. W. Xia [17] and the authors [13]. In [10], G. A. Lomadze gave formulas for $s_{2k}(n)$ for $2 \leqslant n \leqslant 17$, which involves the divisor functions and certain finite sums which involve the solution set of the representation of same quadratic forms of lower variables. However, the other formulas mentioned above are in terms of divisor functions and Fourier coefficients of certain cusp forms. Like in the works of [17] and [13], by comparing the formulas of Lomadze with our results, we also obtain identities connecting the Fourier coefficients of certain cusp forms in terms of finite sums (see Corollary 2.5).

2. Preliminaries and statement of the results

Let $M_k(N)$ be the space of modular forms of weight k for the congruence subgroup $\Gamma_0(N)$ and $S_k(N)$ be the subspace of cusp forms of weight k for the congruence subgroup $\Gamma_0(N)$. For $k \geqslant 4$, let E_k denote the normalized Eisenstein series of weight k in $M_k(1)$ given by

$$E_k(z) = 1 - \frac{2k}{B_k}\sum_{n\geqslant 1}\sigma_{k-1}(n)q^n,$$

where $q = e^{2i\pi z}$ and B_k is the k-th Bernoulli number defined by

$$\frac{x}{e^x - 1} = \sum_{m=0}^{\infty}\frac{B_m}{m!}x^m.$$

The first few Eisenstein series are given as follows:

$$\begin{aligned}
E_4(z) &= 1 + 240\sum_{n\geqslant 1}\sigma_3(n)q^n, \qquad & E_6(z) &= 1 - 504\sum_{n\geqslant 1}\sigma_5(n)q^n,\\
E_8(z) &= 1 + 480\sum_{n\geqslant 1}\sigma_7(n)q^n, \qquad & E_{10}(z) &= 1 - 264\sum_{n\geqslant 1}\sigma_9(n)q^n,\\
E_{12}(z) &= 1 + \frac{65520}{691}\sum_{n\geqslant 1}\sigma_{11}(n)q^n.
\end{aligned} \tag{3}$$

The following identity is well-known from the fact that $E_8 = E_4^2$:

$$W_{1,1}^{3,3}(n) = \frac{1}{120}\sigma_7(n) - \frac{1}{120}\sigma_3(n). \tag{4}$$

In order to evaluate the convolutions sums $W_{a,b,c}^{1,s,t}(n)$, we use the structure theorem on quasimodular forms of weight k and depth $\leqslant k/2$. For details on basics of modular forms and quasimodular forms, we refer the reader to [3, 6, 11]. The Eisenstein series E_2, which is a quasimodular form of weight 2, depth 1 on $SL_2(\mathbb{Z})$ is given by

$$E_2(z) = 1 - 24\sum_{n\geqslant 1}\sigma(n)e^{2\pi inz}$$

and this fundamental quasimodular form will be used in our results. The space of quasimodular forms of weight k, depth $\leqslant k/2$ on $\Gamma_0(N)$ is denoted by $\tilde{M}_k^{\leqslant k/2}(N)$. We need the following structure theorem (see [6, 11]). For an even integer k with $k \geqslant 2$, we have

$$\tilde{M}_k^{\leqslant k/2}(N) = \bigoplus_{j=0}^{k/2-1} D^j M_{k-2j}(N) \oplus \mathbb{C}D^{k/2-1}E_2, \tag{5}$$

where the differential operator D is defined by $D := \frac{1}{2\pi i}\frac{d}{dz}$. Using this one can express each quasimodular form of weight k and depth $\leqslant k/2$ as a linear combination of j-th derivatives of modular forms of weight $k-2j$ on $\Gamma_0(N)$, $0 \leqslant j \leqslant k/2-1$ and the $(k/2-1)$-th derivate of the quasimodular form E_2.

We need the following newforms for our results. Let $\Delta(z) = \sum_{n\geqslant 1}\tau(n)q^n = \eta^{24}(z)$ be the well-known unique normalized cusp form of weight 12, level 1, studied by Ramanujan. Here $\eta(z)$ is the Dedekind eta function given by

$$\eta(z) = q^{1/24}\prod_{n\geqslant 1}(1-q^n).$$

Let $\{\Delta_{k,N,j} : 1 \leqslant j \leqslant d\}$ be the basis (of dimension d) of normalized newforms of weight k, level N, having Fourier expansion

$$\Delta_{k,N,j}(z) = \sum_{n\geqslant 1}\tau_{k,N,j}(n)q^n.$$

If $d = 1$, then we write the function as $\Delta_{k,N}$ and its Fourier coefficients as $\tau_{k,N}(n)$.

The following are the main theorems of this section.

Theorem 2.1. *Let $n \in \mathbb{N}$, then*

$$\begin{aligned}
W_{1,1,1}^{1,3,3}(n) &= \frac{1}{240^2}\big[11\sigma_9(n) + 10(2-3n)\sigma_7(n) - 42\sigma_5(n) \\
&\quad + 20(3n-1)\sigma_3(n) + \sigma(n)\big], \\
W_{1,1,3}^{1,3,3}(n) &= \frac{1}{240^2}\Bigg[\frac{91}{671}\sigma_9(n) + \frac{7290}{7381}\sigma_9\left(\frac{n}{3}\right) - \frac{15}{41}n\sigma_7(n) - \frac{1215}{41}n\sigma_7\left(\frac{n}{3}\right) \\
&\quad + \frac{10}{41}\sigma_7(n) + \frac{810}{41}\sigma_7\left(\frac{n}{3}\right) - \frac{276}{13}\sigma_5(n) - \frac{270}{13}\sigma_5\left(\frac{n}{3}\right) + 30n\sigma_3(n) \\
&\quad + 30n\sigma_3\left(\frac{n}{3}\right) - 10\sigma_3(n) + 10\sigma_3\left(\frac{n}{3}\right) + \sigma(n) - \frac{280}{61}\tau_{10,3,1}(n) \\
&\quad + 115\tau_{10,3,2}(n) - \frac{600}{41}n\tau_{8,3}(n) + \frac{400}{41}\tau_{8,3}(n) - \frac{10}{13}\tau_{6,3}(n)\Bigg], \\
W_{1,3,3}^{1,3,3}(n) &= \frac{1}{240^2}\Bigg[\sigma(n) - 20(1-3n)\sigma_3\left(\frac{n}{3}\right) - \frac{6}{13}\sigma_5(n) - \frac{540}{13}\sigma_5\left(\frac{n}{3}\right) \\
&\quad - \frac{20}{13}\tau_{6,3}(n) + 10(2-3n)\sigma_7\left(\frac{n}{3}\right) + \frac{11}{7381}\sigma_9(n) + \frac{7380}{671}\sigma_9\left(\frac{n}{3}\right) \\
&\quad + \frac{160}{549}\tau_{10,3,1}(n) + \frac{70}{99}\tau_{10,3,2}(n)\Bigg], \\
W_{3,1,1}^{1,3,3}(n) &= \frac{1}{240^2}\Bigg[\sigma\left(\frac{n}{3}\right) + 20(n-1)\sigma_3(n) - \frac{60}{13}\sigma_5(n) - \frac{486}{13}\sigma_5\left(\frac{n}{3}\right) \\
&\quad + \frac{60}{13}\tau_{6,3}(n) + 10(2-n)\sigma_7(n) + \frac{890}{671}\sigma_9(n) + \frac{6561}{671}\sigma_9\left(\frac{n}{3}\right) \\
&\quad + \frac{480}{61}\tau_{10,3,1}(n) - \frac{210}{11}\tau_{10,3,2}(n)\Bigg], \\
W_{3,3,1}^{1,3,3}(n) &= \frac{1}{240^2}\Bigg[\sigma\left(\frac{n}{3}\right) + 10(n-1)\sigma_3\left(\frac{n}{3}\right) + 10(n-1)\sigma_3(n) - \frac{516}{13}\sigma_5\left(\frac{n}{3}\right) \\
&\quad - \frac{30}{13}\sigma_5(n) + \frac{30}{13}\tau_{6,3}(n) + \frac{10-5n}{41}\sigma_7(n) + \frac{810-405n}{41}\sigma_7\left(\frac{n}{3}\right) \\
&\quad + \frac{400}{41}\tau_{8,3}(n) + \frac{10}{671}\sigma_9(n) + \frac{7371}{671}\sigma_9\left(\frac{n}{3}\right) - \frac{280}{183}\tau_{10,3,1}(n) \\
&\quad - \frac{115}{33}\tau_{10,3,2}(n) - \frac{200}{41}n\tau_{8,3}(n)\Bigg].
\end{aligned}$$

Theorem 2.2. *Let $n \in \mathbb{N}$, then*

$$
\begin{aligned}
W_{1,1,1}^{3,3,3}(n) &= \frac{1}{19200}\sigma_3(n) - \frac{1}{9600}\sigma_7(n) + \frac{91}{13267200}\sigma_{11}(n) + \frac{1}{22112}\tau(n),\\
W_{1,1,3}^{3,3,3}(n) &= \frac{41}{484252800}\sigma_{11}(n) + \frac{6561}{968505600}\sigma_{11}\left(\frac{n}{3}\right) - \frac{7}{196800}\sigma_7(n)\\
&\quad - \frac{9}{131200}\sigma_7\left(\frac{n}{3}\right) + \frac{1}{28800}\sigma_3(n) + \frac{1}{57600}\sigma_3\left(\frac{n}{3}\right) - \frac{133}{720\times 11747}\tau(n)\\
&\quad + \frac{145071}{160\times 11747}\tau\left(\frac{n}{3}\right) - \frac{1}{29520}\tau_{8,3}(n) + \frac{1}{16\times 1241}\tau_{12,3}(n),\\
W_{1,3,3}^{3,3,3}(n) &= \frac{91}{19200\times 691\times 6643}\sigma_{11}(n) + \frac{91\times 6642}{19200\times 691\times 6643}\sigma_{11}\left(\frac{n}{3}\right)\\
&\quad - \frac{1}{1180800}\sigma_7(n) - \frac{61}{590400}\sigma_7\left(\frac{n}{3}\right) + \frac{1}{240^2}\sigma_3(n) + \frac{1}{28800}\sigma_3\left(\frac{n}{3}\right)\\
&\quad + \frac{199}{1440\times 11747}\tau(n) - \frac{1197}{80\times 11747}\tau\left(\frac{n}{3}\right) - \frac{1}{120\times 246}\tau_{8,3}(n)\\
&\quad + \frac{1}{144\times 1241}\tau_{12,3}(n).
\end{aligned}
$$

We apply the above convolution sums to derive the following theorems.

Theorem 2.3. *The number of representations of a positive integer n by the quadratic form F_{10} is given by*

$$s_{20}(n) = \frac{12}{11}\sigma_9^*(n) + \frac{648}{11}\tau_{10,3,2}(n),$$

where $\sigma_9^*(n) = \sigma_9(n) - 3^5\sigma_9\left(\frac{n}{3}\right)$.

Theorem 2.4. *The number of representations of a positive integer n by the quadratic form F_{12} is given by*

$$s_{24}(n) = \frac{6552}{50443}\sigma_{11}^*(n) + \frac{402624}{11747}\tau(n) + \frac{293512896}{11747}\tau\left(\frac{n}{3}\right) + \frac{46656}{1241}\tau_{12,3}(n),$$

where $\sigma_{11}^*(n) = \sigma_{11}(n) + 3^6\sigma_{11}\left(\frac{n}{3}\right)$.

Corollary 2.5. *Comparing our formulas in Theorem 2.3 and Theorem 2.4 with the formulas (IX) and (XI) in p. 12 of [10], we get the following identities:*

$$\tau_{10,3,2}(n) = \frac{1}{120}\sum_{F_6(x_1,\cdots,x_{12})=n}(42x_1^4 - 27nx_1^2 + n^2), \tag{6}$$

$$\begin{aligned}\frac{402624}{11747}\tau(n)+\frac{293512896}{11747}\tau\left(\frac{n}{3}\right)+\frac{46656}{1241}\tau_{12,3}(n)\\ =\frac{291096}{1765505}\sum_{F_8(x_1,\cdots,x_{16})=n}(135x_1^4-54nx_1^2+2n^2)\\ +\frac{864}{50443}\sum_{F_6(x_1,\cdots,x_{12})=n}(162x_1^6-162nx_1^4+36n^2x_1^2-n^3)\\ +\frac{30}{50443}\sum_{F_4(x_1,\cdots,x_8)=n}(1215x_1^8-2268nx_1^6+1260n^2x_1^4-210n^3x_1^2+5n^4).\end{aligned}\tag{7}$$

Remark 2.1. It would be interesting to get individual expressions for the cusp forms appearing in (7), which will give an explicit expression for the Ramanujan Tau function.

3. Proofs

For the proofs of our theorems, we need the newforms $\Delta_{k,N}(z)$, $(k,N)\in\{(6,3),(8,3),(12,3)\}$, $\Delta_{10,3,1}(z)$, $\Delta_{10,3,2}(z)$. Below we give their expressions in terms of Eisenstein series and eta products. We have used the L-functions and modular forms database [8] to get these expressions. (The expression for $\Delta_{8,3}(z)$ appeared in [13, Eq.(10)].)

$$\begin{aligned}\Delta_{6,3}(z)&=\eta^6(z)\eta^6(3z),\\ \Delta_{8,3}(z)&=\eta^{12}(z)\eta^4(3z)+81\eta^6(z)\eta^4(3z)\eta^6(9z)+18\eta^9(z)\eta^4(3z)\eta^3(9z),\\ \Delta_{10,3,1}(z)&=\frac{-1}{8}E_4(z)\Delta_{6,3}(z)+\frac{9}{8}E_4(3z)\Delta_{6,3}(z),\\ \Delta_{10,3,2}(z)&=\frac{1}{10}E_4(z)\Delta_{6,3}(z)+\frac{9}{10}E_4(3z)\Delta_{6,3}(z),\\ \Delta_{12,3}(z)&=\frac{98}{81}\Delta(z)-3402\Delta(3z)-\frac{17}{81}E_6(z)\Delta_{6,3}(z).\end{aligned}$$

3.1. Proof of Theorem 2.1

We need the following convolution sums (see [13, 17]).

Proposition 3.1. *Let $n\in\mathbb{N}$. Then*

$$\begin{aligned}W_{1,3}^{3,3}(n)&=-\frac{1}{240}\sigma_3(n)-\frac{1}{240}\sigma_3\left(\frac{n}{3}\right)+\frac{1}{9840}\sigma_7(n)+\frac{81}{9840}\sigma_7\left(\frac{n}{3}\right)+\frac{1}{246}\tau_{8,3}(n),\\ W_{1,3}^{1,1}(n)&=\frac{7}{80}\sigma_5(n)-\frac{1}{8}n\sigma_3(n)+\frac{1}{24}\sigma_3(n)-\frac{1}{240}\sigma\left(n\right),\\ W_{3,1}^{1,3}(n)&=\frac{1}{104}\sigma_5(n)-\frac{81}{1040}\sigma_5\left(\frac{n}{3}\right)+\frac{1-n}{24}\sigma_3(n)-\frac{1}{240}\sigma\left(\frac{n}{3}\right)-\frac{1}{104}\tau_{6,3}(n),\\ W_{1,3}^{1,3}(n)&=\frac{1}{1040}\sigma_5(n)+\frac{9}{104}\sigma_5\left(\frac{n}{3}\right)+\frac{1-3n}{24}\sigma_3\left(\frac{n}{3}\right)-\frac{1}{240}\sigma\left(n\right)+\frac{1}{312}\tau_{6,3}(n).\end{aligned}$$

The vector space $M_{10}(3)$ is of dimension 4 with a basis $\{E_{10}(z), E_{10}(3z), \Delta_{10,3,1}(z), \Delta_{10,3,2}(z)\}$, the vector space $M_8(3)$ is of dimension 3 with a basis $\{E_8(z), E_8(3z), \Delta_{8,3}(z)\}$, the vector space $M_6(3)$ is of dimension 3 with a basis $\{E_6(z), E_6(3z), \Delta_{6,3}(z)\}$, and the space $M_4(3)$ has dimension 2 with a basis $\{E_4(z), E_4(3z)\}$. Now using the structure theorem of quasimodular forms and using the above basis, we get the following.

$$\begin{aligned}
E_2(z)E_4^2(z) &= E_{10}(z) + \frac{3}{2}DE_8(z),\\
E_2(z)E_4(z)E_4(3z) &= \frac{91}{7381}E_{10}(z) + \frac{7290}{7381}E_{10}(3z) + \frac{6720}{61}\Delta_{10,3,1}(z)\\
&\quad - \frac{2760}{11}\Delta_{10,3,2}(z) + \frac{3}{164}DE_8(z) + \frac{243}{164}DE_8(3z)\\
&\quad + \frac{14400}{41}D\Delta_{8,3}(z),\\
E_2(z)E_4^2(3z) &= \frac{1}{7381}E_{10}(z) + \frac{7380}{7381}E_{10}(3z) - \frac{1280}{183}\Delta_{10,3,1}(z)\\
&\quad - \frac{560}{33}\Delta_{10,3,2}(z) + \frac{3}{2}DE_8(3z),\\
E_2(3z)E_4^2(z) &= \frac{820}{7381}E_{10}(z) + \frac{6561}{7381}E_{10}(3z) - \frac{11520}{61}\Delta_{10,3,1}(z)\\
&\quad + \frac{5040}{11}\Delta_{10,3,2}(z) + \frac{1}{2}DE_8(z),\\
E_2(3z)E_4(z)E_4(3z) &= \frac{10}{7381}E_{10}(z) + \frac{7371}{7381}E_{10}(3z) + \frac{2240}{61}\Delta_{10,3,1}(z)\\
&\quad + \frac{920}{11}\Delta_{10,3,2}(z) + \frac{1}{164}DE_8(z) + \frac{81}{164}DE_8(3z)\\
&\quad + \frac{4800}{41}D\Delta_{8,3}(z).
\end{aligned}$$

By comparing the n-th Fourier coefficients and using the convolution sums $W_{1,1}^{3,3}, W_{1,3}^{3,3}, W_{1,1}^{1,3}, W_{1,3}^{1,3}$ from Proposition 3.1 we get the required triple convolution sums.

3.2. Proof of Theorem 2.2

The vector space $M_{12}(1)$ has dimension 2 with a basis $\{E_{12}(z), \Delta(z)\}$, where $\Delta(z)$ is the unique normalized newform of weight 12 and level 1. Now $E_4^3(z) \in M_{12}(1)$ and writing as linear combination of basis, we have

$$E_4^3(z) = E_{12}(z) + \frac{432000}{691}\Delta(z).$$

The dimension of the space $M_{12}(3)$ is 5 having a basis $\{E_{12}(z), E_{12}(3z), \Delta(z), \Delta(3z), \Delta_{12,3}(z)\}$, where $\Delta_{12,3}(z)$ is the unique normalized newform of weight 12 and level 3.

Now $E_4^2(z)E_4(3z), E_4(z)E_4^2(3z) \in M_{12}(3)$. Writing as linear combination of the above basis, we get

$$E_4^2(z)E_4(3z) = \frac{82}{6643}E_{12}(z) + \frac{6561}{6643}E_{12}(3z) - \frac{2553600}{11747}\Delta(z) + \frac{12534134400}{11747}\Delta(3z) + \frac{86400}{1241}\Delta_{12,3}(z)$$

and

$$E_4(z)E_4^2(3z) = \frac{1}{6643}E_{12}(z) + \frac{6642}{6643}E_{12}(3z) + \frac{1910400}{11747}\Delta(z) - \frac{206841600}{11747}\Delta(3z) + \frac{96000}{1241}\Delta_{12,3}(z).$$

By comparing the n-th Fourier coefficients and using convolution sums $W_{1,1}^{3,3}$ from (4) and $W_{1,3}^{3,3}$ from Proposition 3.1 we get the required convolution sums.

3.3. Proof of Theorem 2.3

Let $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$. For $n \in N$ we know that (see [5], [10])

$$s_4(n) = 12\sigma(n) - 36\sigma\left(\frac{n}{3}\right), \tag{8}$$

and

$$s_8(n) = 24\sigma_3(n) + 216\sigma_3\left(\frac{n}{3}\right). \tag{9}$$

Then $s_{20}(n)$ is given by

$$\begin{aligned}
s_{20}(n) &= \sum_{\substack{a.b,c\in\mathbb{N}_0\\ a+b+c=n}} \left(\sum_{F_2(x_1,\cdots,x_4)=a} 1\right)\left(\sum_{F_4(x_5,\cdots,x_{12})=b} 1\right)\left(\sum_{F_4(x_{13},\cdots,x_{20})=c} 1\right)\\
&= s_4(n) + 2s_8(n) + \sum_{\substack{a,b\in\mathbb{N}\\ a+b=n}} s_8(a)s_8(b) + 2\sum_{\substack{a,b\in\mathbb{N}\\ a+b=n}} s_4(a)s_8(b)\\
&\quad + \sum_{\substack{a,b,c\in\mathbb{N}\\ a+b+c=n}} s_4(a)s_8(b)r_8(c)\\
&= 12\sigma(n) - 36\sigma\left(\frac{n}{3}\right) + 48\sigma_3(n) + 432\sigma_3\left(\frac{n}{3}\right) + 24^2W_{1,1}^{3,3} + 48\times 216W_{1,3}^{3,3}\\
&\quad + 216^2W_{1,1}^{3,3}\left(\frac{n}{3}\right) + 24^2W_{1,1}^{1,3} + 9\times 24^2W_{1,3}^{1,3} - 48\times 36W_{3,1}^{1,3}\\
&\quad - 36\times 216W_{1,1}^{1,3}\left(\frac{n}{3}\right) + 12\times 24^2W_{1,1,1}^{1,3,3} + 9\times 24^3W_{1,1,3}^{1,3,3}\\
&\quad + 12\times 216^2W_{1,3,3}^{1,3,3} - 36\times 24^2W_{3,1,1}^{1,3,3} - 72^3W_{3,1,3}^{1,3,3} - 1296^2W_{1,1,1}^{1,3,3}\left(\frac{n}{3}\right).
\end{aligned}$$

Now, we substitute the expressions for the covolution sums using (4) and Theorem 2.1, the required formula follows.

3.4. Proof of Theorem 2.4

We proceed as in the case of 20 variables. We have

$$\begin{aligned}
s_{24}(n) &= \sum_{\substack{a,b,c\in\mathbb{N}_0\\ a+b+c=n}} \left(\sum_{F_4(x_1,\cdots,x_8)=a} 1\right)\left(\sum_{F_4(x_9,\cdots,x_{16})=b} 1\right)\left(\sum_{F_4(x_{17},\cdots,x_{24})=c} 1\right)\\
&= 3s_8(n) + 3\sum_{\substack{a,b\in\mathbb{N}\\ a+b=n}} s_8(a)s_8(b) + \sum_{\substack{a,b,c\in\mathbb{N}\\ a+b+c=n}} s_8(a)s_8(b)s_8(c)\\
&= 72\sigma_3(n) + 648\sigma_3\left(\frac{n}{3}\right) + 3\sum_{\substack{a,b\in\mathbb{N}\\ a+b=n}} \left(24\sigma_3(a) + 216\sigma_3\left(\frac{a}{3}\right)\right)\\
&\quad\times\left(24\sigma_3(b) + 216\sigma_3\left(\frac{b}{3}\right)\right) + \sum_{\substack{a,b,c\in\mathbb{N}\\ a+b+c=n}} \left(24\sigma_3(a) + 216\sigma_3\left(\frac{a}{3}\right)\right)\\
&\quad\times\left(24\sigma_3(b) + 216\sigma_3\left(\frac{b}{3}\right)\right)\left(24\sigma_3(c) + 216\sigma_3\left(\frac{c}{3}\right)\right)\\
&= 72\sigma_3(n) + 648\sigma_3\left(\frac{n}{3}\right) + 3\times 24^2 W_{1,1}^{3,3}(n) + 54\times 24^2 W_{1,3}^{3,3}(n)\\
&\quad + 3^5\times 24^2 W_{1,1}^{3,3}\left(\frac{n}{3}\right) + 24^3\ W_{1,1,1}^{3,3,3}(n) + 3^3\times 24^3\ W_{1,1,3}^{3,3,3}(n)\\
&\quad + 3^5\times 24^3 W_{1,3,3}^{3,3,3}(n) + 216^3\ W_{1,1,1}^{3,3,3}\left(\frac{n}{3}\right).
\end{aligned}$$

Substituting the convolution sums using (4), Proposition 3.1 and Theorem 2.2, we get the required formula for $s_{24}(n)$.

We give below a table giving the first 15 values of $s_{10}(n)$ and $s_{24}(n)$.

n	$s_{20}(n)$	$s_{24}(n)$
1	60	72
2	1620	2376
3	25980	47592
4	275460	646344
5	2040552	6305904
6	10965780	45821160
7	44559840	255215808
8	145963620	1125009864
9	417830460	4097478600
10	1091417976	12975540336
11	2573551440	37101202848
12	5569628100	96867424872
13	11570383560	232791251760
14	22593025440	526183909056
15	41415305832	1128351033648

Acknowledgements. We have used the open-source mathematics software SAGE (www.sagemath.org) to do our calculations. The second author is partially funded by SERB grant SR/FTP/MS-053/2012. He would like to thank HRI, Allahabad for the warm hospitality where this work has been carried out. Finally, the authors thank the referee for his/her comments and also for pointing out the reference [7].

References

[1] S. Alaca, F. Uygul and K.S. Williams, *Some arithmetic identities involving divisor functions*, Funct. Approx. Comment. Math. **46** (2012), no. 2, 261–271.

[2] M. Besge, *Extrait d'une lettre de M. Besge á M. Liouville,* J. Math. Pures Appl. **7** (1862), 256.

[3] J.H. Bruinier, G. van der Geer, G. Harder and D. Zagier, *The 1-2-3 of modular forms*, Lectures from the Summer School on Modular Forms and their Applications held in Nordfjordeid, June 2004. Edited by Kristian Ranestad. Universitext. Springer-Verlag, Berlin, 2008. 266 pp.

[4] J.W.L. Glaisher, *On the squares of the series in which the coefficients are the sums of the divisor of the exponents*, Mess. Math. **15** (1885), 1–20.

[5] J.G. Huard, Z.M. Ou, B.K. Spearman and K.S. Williams, *Elementary evaluation of certain convolution sums involving divisor functions,* in Number Theory for the Millennium, II (Urbana, IL, 2000) (A. K. Peters, Natick, MA, 2002), 229–274.

[6] M. Kaneko and D. Zagier, *A generalized Jacobi theta function and quasimodular forms.* In "The moduli space of curves (Texel Island, 1994)", 165–172, Progr. Math. **129**, Birkhäuser Boston, Boston, MA, 1995.

[7] D. Kim, A. Kim and A. Sankaranarayanan, *Bernoulli numbers, convolution sums and congruences of coefficients for certain generating functions*, J. Inequal. Appl. **2013:225** (2013), 26 pp.

[8] LMFDB, The database of L-functions, modular forms, and related objects, http://www.lmfdb.org/

[9] J. Liouville, *Sur la formes* $x^2 + xy + y^2 + z^2 + zt + t^2$, J. Math. Pures. Appl. **8** (1863), 141–144.

[10] G.A. Lomadze, *Representation of numbers by sums of the quadratic forms* $x_1^2 + x_1x_2 + x_2^2$, Acta Arith. **54** (1989), 9–36. (in Russian)

[11] F. Martin and E. Royer, *Formes modulaires et périodes*, In 'Formes modulaires et transcendance', 1–117, Sémin. Congr., **12**, Soc. Math. France, Paris, 2005.

[12] B. Ramakrishnan and B. Sahu, *Evaluation of the convolution sums* $\sum_{l+15m=n} \sigma(l)\sigma(m)$ *and* $\sum_{3l+5m=n} \sigma(l)\sigma(m)$ *and an application*, Int. J. Number Theory **9** (2013), no. 3, 1–11.

[13] B. Ramakrishnan and B. Sahu, *On the number of representations of an integer by certain quadratic forms in sixteen variables*, Int. J. Number Theory **10** (2014), no. 8, 1929–1937.

[14] S. Ramanujan, *On certain arithmetical functions,* Trans. Cambridge Philos. Soc. 22 (1916) 159–184.

[15] E. Royer, *Evaluating convolution sums of the divisor function by quasimodular forms*, Int. J. Number Theory **3** (2007), no. 2, 231–261.

[16] K.S. Williams, *Number Theory in the spirit of Liouville*, London Mathematical Student Texts **76**, Cambridge Univ. Press, 2011.

[17] O.X.M. Yao and E.X.W. Xia, *Evaluation of the convolution sum* $\sum_{i+3j=n} \sigma(i)\sigma_3(j)$ *and* $\sum_{3i+j=n} \sigma(i)\sigma_3(j)$, Int. J. Number Theory **10** (2014), no. 1, 115–123.

Addresses: B. Ramakrishnan: Harish-Chandra Research Institute, Chhatnag Road, Jhunsi, Allahabad – 211 019, India.;
Brundaban Sahu: School of Mathematical Sciences, National Institute of Science Education and Research, PO: Sainik School, Bhubaneswar, Odisha – 751 005, India.

E-mail: ramki@hri.res.in, brundaban.sahu@niser.ac.in

Received: 9 July 2015; **revised:** 17 September 2015

Functiones et Approximatio
54.2 (2016), 163–171
doi: 10.7169/facm/2016.54.2.3

AN IRREDUCIBILITY CRITERION FOR THE SUM OF TWO RELATIVELY PRIME POLYNOMIALS

Nicolae Ciprian Bonciocat

Dedicated to the memory of Şerban Basarab

Abstract: We extend a result of Cavachi on sums of relatively prime polynomials by proving that a polynomial of the form $f(X)+p^k g(X)$, with f and g relatively prime polynomials with integer coefficients, $\deg f < \deg g$, and k a positive integer prime to $\deg g$ is irreducible over $\mathbb{Q}$ for all but finitely many prime numbers p.

Keywords: irreducible polynomials; prime numbers; resultant.

1. Introduction

If we add two algebraically relatively prime polynomials having coefficients in an arbitrary unique factorization domain, the resulting polynomial will not necessarily be irreducible, as one can easily check. However, if instead of the sum we consider linear combinations of the two polynomials, say $n_1 f(X) + n_2 g(X)$, then the resulting polynomials prove to be irreducible, provided some conditions on the factorization of n_1 and n_2 are satisfied. In this respect, several recent irreducibility criteria have been obtained for polynomials of the form $f(X)+pg(X)$, where f and g are relatively prime polynomials with rational coefficients, and p is a sufficiently large prime number. Inspired by some results of Fried [9] and Langmann [10], Cavachi [6] proved that for any relatively prime polynomials $f(X), g(X) \in \mathbb{Q}[X]$ with $\deg f < \deg g$, the polynomial $f(X) + pg(X)$ is irreducible over $\mathbb{Q}$ for all but finitely many prime numbers p. This result has been improved in [7] by providing an explicit lower bound b depending on f and g, such that for all primes $p > b$, the polynomial $f(X) + pg(X)$ is irreducible over $\mathbb{Q}$. The method in [7] was adapted in [4] in order to provide sharper bounds b as well as explicit upper bounds for the total number of factors over $\mathbb{Q}$ of linear combinations of the form $n_1 f(X) + n_2 g(X)$, where f and g are relatively prime polynomials with $\deg f \leqslant \deg g$, and n_1 and n_2 are non-zero integers with absolute value of n_2/n_1 exceeding an explicit lower

2010 Mathematics Subject Classification: primary: 11R09; secondary: 11C08

bound. Similar results have been also provided for compositions of polynomials with integer coefficients [3] and for multiplicative convolutions of polynomials with integer coefficients [1], [2]. We obviously cannot replace the prime p in Cavachi's result by a sufficiently large positive integer n, since for instance a polynomial of the form $f(X)^2 - ng(X)^2$ with f and g relatively prime is obviously reducible whenever n is a square. However, given a pair of relatively prime polynomials f and g with $\deg f < \deg g$, some families of composite numbers n exist such that $f + ng$ is irreducible. In this respect, in [5] several irreducibility results have been provided for polynomials of the form $f(X) + p^k g(X)$ with f and g relatively prime polynomials with integer coefficients, $\deg f < \deg g$, p a prime number, and k a positive integer prime to $\deg g - \deg f$. The main result in [5], that partially relies on a Newton polygon argument, is the following extension of Cavachi's result.

Theorem A ([5, Theorem 1.1.]). *Let $f, g \in \mathbb{Z}[X]$ be two relatively prime polynomials with $\deg g = n$ and $\deg f = n - d$, $d \geqslant 1$. Then for any prime number p that divides none of the leading coefficients of f and g, and any positive integer k prime to d such that*

$$p^k \geqslant \left(2 + \frac{1}{2^{n+1-d} H(g)^{n+1}}\right)^{n+1-d} H(f) H(g)^n - \frac{H(f)}{H(g)},$$

the polynomial $f(X) + p^k g(X)$ is irreducible over $\mathbb{Q}$.

Here and henceforth for a polynomial $f(X) = a_0 + a_1 X + \cdots + a_n X^n \in \mathbb{Z}[X]$ of degree n, $H(f)$ stands for the usual height of f, that is

$$H(f) = \max\{|a_0|, |a_1|, ..., |a_n|\}.$$

In this paper we will complement the results in [6], [4], [5] and [7] by proving that the result of Cavachi also holds if we replace the prime p by a prime power p^k with k prime to $\deg g$. We will actually prove the following effective result that provides an explicit lower bound for p depending on f and g, that once exceeded, will ensure the irreducibility of $f(X) + p^k g(X)$ over $\mathbb{Q}$.

Theorem 1.1. *Let $f, g \in \mathbb{Z}[X]$ be relatively prime polynomials with $\deg f = m$, $\deg g = n$, and $m < n$. Then for any prime number p and any positive integer k prime to n such that*

$$p > \left(2 + \frac{1}{2^{k(m+1)(n-1)}}\right)^{(m+1)(n-1)} H(f)^{n-1} H(g)^{m(n-1)+1},$$

the polynomial $f(X) + p^k g(X)$ is irreducible over $\mathbb{Q}$.

In particular, we have the following corollary.

Corollary 1.2. *Let $f, g \in \mathbb{Z}[X]$ be two relatively prime polynomials with $\deg f < \deg g$, and let k be a positive integer prime to $\deg g$. Then the polynomial $f(X) + p^k g(X)$ is irreducible over $\mathbb{Q}$ for all but finitely many prime numbers p.*

We note that Theorem 1.1 also holds in the particular case $\deg f = 0$, that is when f is a nonzero constant polynomial, say $f = a \in \mathbb{Z} \setminus \{0\}$. Actually, in this case one may prove a better result, namely that the irreducibility of $a + p^k g$ will hold provided a and the leading coefficient of g are not divisible by p, so here we do not need to ask p to exceed a certain lower bound, as in the statement of Theorem 1.1. More precisely, in this case we have the following result.

Theorem 1.3. *Let $g \in \mathbb{Z}[X]$ be a polynomial with $\deg g = n$ and leading coefficient b_n, and let a be a nonzero integer. Then for any prime number p that does not divide ab_n, and any positive integer k prime to n, the polynomial $a + p^k g(X)$ is irreducible over $\mathbb{Q}$.*

This result is also a special case of Theorem A (the case $d = n$ that was discussed in [5] in Remark 2.1), and its proof follows immediately by using the following celebrated irreducibility criterion of Dumas [8].

Irreducibility criterion of Dumas. *Let $f(X) = a_0 + a_1 X + \cdots + a_n X^n$ be a polynomial with integer coefficients, and let p be a prime number. If*

i) $\frac{\nu_p(a_i)}{i} > \frac{\nu_p(a_n)}{n}$ *for* $i = 1, \ldots, n-1$,
ii) $\nu_p(a_0) = 0$,
iii) $\gcd(\nu_p(a_n), n) = 1$,

then f is irreducible over $\mathbb{Q}$.

Here for an integer n and a prime number p, $\nu_p(n)$ stands for the largest integer i such that $p^i \mid n$ (by convention, $\nu_p(0) = \infty$).

One may easily obtain sharper results, if some additional information on the coefficients or on the roots of f and g is available. In this respect, we will also prove the following irreducibility criterion.

Theorem 1.4. *Let $f(X) = \sum_{i=0}^{m} a_i X^i, g(X) = \sum_{i=0}^{n} b_i X^i \in \mathbb{Z}[X]$ be two relatively prime polynomials with $a_m b_n \neq 0$, $m < n$, and assume that $|b_n| > |b_0| + \cdots + |b_{n-1}|$. Then for any prime number $p > |b_n|^n (|a_0| + \cdots + |a_m|)^{n-1}$ and any positive integer k prime to n, the polynomial $f(X) + p^k g(X)$ is irreducible over $\mathbb{Q}$.*

In particular, one obtains the following result.

Corollary 1.5. *Let $f(X) = \sum_{i=0}^{m} a_i X^i, g(X) = \sum_{i=0}^{n} b_i X^i \in \mathbb{Z}[X]$ with $a_m b_n \neq 0$, $m < n$, and assume that $|a_0| \geqslant |a_1| + \cdots + |a_m|$ and $|b_n| > |b_0| + \cdots + |b_{n-1}|$. Then for any prime number $p > |b_n|^n (|a_0| + \cdots + |a_m|)^{n-1}$ and any positive integer k prime to n, the polynomial $f(X) + p^k g(X)$ is irreducible over $\mathbb{Q}$.*

The proof of Theorem 1.1 will not rely on a Newton polygon argument, that was crucial in the proof of Theorem A. Here the proof will rely on a simultaneous analysis of some resultants associated to the alleged factors of $f(X) + p^k g(X)$. We end this section by noting that the lower bound on the prime p in the statement of Theorem 1.1 may be replaced by

$$\left(2 + \frac{1}{2^{(m+1)(n-1)}}\right)^{(m+1)(n-1)} H(f)^{n-1} H(g)^{m(n-1)+1},$$

which is independent on k.

2. Proof of the main results

Proof of Theorem 1.1. For the Proof of Theorem 1.1 we will adapt some of the ideas in [4], [5] and [7]. We will actually prove a sharper result, by showing that for $m \geqslant 1$ the same conclusion on the irreducibility of $f + p^k g$ holds if we replace the condition on p in the statement of Theorem 1.1 by

$$p \geqslant \left(2 + \frac{1}{2^{k(m+1)(n-1)} A}\right)^{(m+1)(n-1)} H(f)^{n-1} H(g)^{m(n-1)+1} \tag{1}$$

with $A = H(f)^{k(n-1)-1} H(g)^{k(m(n-1)+1)+1} \geqslant 1$.

So let $f(X) = a_0 + a_1 X + \cdots + a_m X^m$ and $g(X) = b_0 + b_1 X + \cdots + b_n X^n$ be two relatively prime polynomials with integer coefficients, $a_m b_n \neq 0$, $1 \leqslant m < n$, and let p be a prime number and k a positive integer prime to n satisfying (1). Now let us assume to the contrary that $f(X) + p^k g(X)$ is reducible, that is

$$f(X) + p^k g(X) = f_1(X) f_2(X), \tag{2}$$

with $f_1(X), f_2(X) \in \mathbb{Z}[X]$ and $\deg f_1 \geqslant 1$, $\deg f_2 \geqslant 1$, say

$$f_1(X) = c_0 + c_1 X + \cdots + c_s X^s,$$
$$f_2(X) = d_0 + d_1 X + \cdots + d_t X^t,$$

$c_0, \ldots c_s, d_0, \ldots d_t \in \mathbb{Z}$, $c_s d_t \neq 0$, and $s \geqslant 1$, $t \geqslant 1$, $s + t = n$. By equating the coefficients in (2) we see that $p^k b_n = c_s d_t$. Let us denote $c_s = p^\alpha c_s'$ and $d_t = p^\beta d_t'$, with $\alpha, \beta \in \mathbb{N}$, $c_s', d_t' \in \mathbb{Z}$ and $p \nmid c_s' d_t'$. In view of (1) we deduce that $p \nmid b_n$, so we have $\alpha + \beta = k$.

Now we are going to estimate the resultants $R(g, f_1)$ and $R(g, f_2)$. Since g and $f_1 f_2$ are relatively prime polynomials, both $R(g, f_1)$ and $R(g, f_2)$ must be non-zero integer numbers, so in particular we have

$$|R(g, f_1)| \geqslant 1 \qquad \text{and} \qquad |R(g, f_2)| \geqslant 1. \tag{3}$$

If we decompose f_1 and f_2, say

$$f_1(X) = c_s (X - \theta_1) \cdots (X - \theta_s),$$
$$f_2(X) = d_t (X - \xi_1) \cdots (X - \xi_t),$$

with $\theta_1, \ldots, \theta_s, \xi_1, \ldots, \xi_t \in \mathbb{C}$, then

$$|R(g, f_1)| = |c_s|^n \prod_{1 \leqslant j \leqslant s} |g(\theta_j)| \qquad \text{and} \qquad |R(g, f_2)| = |d_t|^n \prod_{1 \leqslant j \leqslant t} |g(\xi_j)|. \tag{4}$$

Since the roots θ_j of f_1 and the roots ξ_j of f_2 are also roots of $f(X) + p^k g(X)$, we have

$$g(\theta_j) = -\frac{f(\theta_j)}{p^k} \qquad \text{and} \qquad g(\xi_j) = -\frac{f(\xi_j)}{p^k} \tag{5}$$

and moreover, since f and g are relatively prime, $f(\theta_j) \neq 0$ and $g(\theta_j) \neq 0$ for any index $j \in \{1, \dots, s\}$, and also $f(\xi_j) \neq 0$ and $g(\xi_j) \neq 0$ for any index $j \in \{1, \dots, t\}$. Using now (4) and (5), we obtain

$$|R(g, f_1)| = \frac{p^{n\alpha}|c_s'|^n}{p^{ks}} \prod_{1 \leqslant j \leqslant s} |f(\theta_j)| \qquad \text{and} \qquad |R(g, f_2)| = \frac{p^{n\beta}|d_t'|^n}{p^{kt}} \prod_{1 \leqslant j \leqslant t} |f(\xi_j)|\,. \tag{6}$$

We will prove now that we either have $ks > n\alpha$, or $kt > n\beta$. To prove this we first note that $ks - n\alpha + kt - n\beta = k(s+t) - n(\alpha+\beta) = kn - nk = 0$. This shows that it is sufficient to prove that none of the integers $ks - n\alpha$ and $kt - n\beta$ can actually vanish. Indeed, if we assume that $ks = n\alpha$, say, then we must also have $kt = n\beta$, and since k is prime to n, we deduce that k must divide both α and β. On the other hand, since $\alpha + \beta = k$ and $\alpha \geqslant 0$, $\beta \geqslant 0$, we deduce that one of α and β must be equal to 0, while the other one must be equal to k, say $\alpha = 0$ and $\beta = k$. In particular, this yields $ks = 0$, which obviously cannot hold, so we must either have $ks > n\alpha$, or $kt > n\beta$. Without loss of generality, let us assume that $ks > n\alpha$ and hence $ks - n\alpha \geqslant 1$. Therefore, in view of (6) we deduce that

$$|R(g, f_1)| \leqslant \frac{|c_s'|^n}{p} \prod_{1 \leqslant j \leqslant s} |f(\theta_j)| \leqslant \frac{|b_n|^n}{p} \prod_{1 \leqslant j \leqslant s} |f(\theta_j)|\,. \tag{7}$$

We now proceed to find an upper bound for $|f(\theta_j)|$. The equality $f(\theta_j) + p^k g(\theta_j) = 0$ implies

$$(a_0 + p^k b_0) + \cdots + (a_m + p^k b_m)\theta_j^m + p^k b_{m+1}\theta_j^{m+1} + \cdots + p^k b_n \theta_j^n = 0,$$

from which we deduce that

$$\begin{aligned} p^k|b_n| \cdot |\theta_j|^n &\leqslant |a_0| + p^k|b_0| + (|a_1| + p^k|b_1|) \cdot |\theta_j| + \cdots + (|a_m| + p^k|b_m|) \cdot |\theta_j|^m \\ &\quad + p^k|b_{m+1}| \cdot |\theta_j|^{m+1} + \cdots + p^k|b_{n-1}| \cdot |\theta_j|^{n-1} \\ &\leqslant \big(H(f) + p^k H(g)\big)\left(1 + |\theta_j| + \cdots + |\theta_j|^{n-1}\right). \end{aligned}$$

Therefore, either $|\theta_j| \leqslant 1$, or if not, we find

$$p^k|b_n| \cdot |\theta_j|^n < \big(H(f) + p^k H(g)\big) \cdot \frac{|\theta_j|^n}{|\theta_j| - 1},$$

so in both cases we have

$$|\theta_j| < 1 + \frac{1}{|b_n|} \cdot \left(\frac{H(f)}{p^k} + H(g)\right). \tag{8}$$

Now, since obviously

$$|f(\theta_j)| \leqslant H(f) \cdot (1 + |\theta_j| + \cdots + |\theta_j|^m)\,,$$

inequality (8) yields

$$|f(\theta_j)| < H(f)\cdot\frac{\left[1+\frac{1}{|b_n|}\cdot\left(\frac{H(f)}{p^k}+H(g)\right)\right]^{m+1}}{\frac{1}{|b_n|}\cdot\left(\frac{H(f)}{p^k}+H(g)\right)}. \tag{9}$$

Using now (7) and (9), we obtain

$$|R(g,f_1)| < \frac{|b_n|^n}{p}\left[|b_n|H(f)\cdot\frac{\left[1+\frac{1}{|b_n|}\cdot\left(\frac{H(f)}{p^k}+H(g)\right)\right]^{m+1}}{\frac{H(f)}{p^k}+H(g)}\right]^s.$$

Since $s\leqslant n-1$, all we need to prove is that our assumption on p will force

$$\frac{|b_n|^{\frac{n}{n-1}}}{p^{\frac{1}{n-1}}}\left[|b_n|H(f)\cdot\frac{\left[1+\frac{1}{|b_n|}\cdot\left(\frac{H(f)}{p^k}+H(g)\right)\right]^{m+1}}{\frac{H(f)}{p^k}+H(g)}\right]\leqslant 1,$$

that is

$$|b_n|^{1+\frac{n}{n-1}}\left[1+\frac{1}{|b_n|}\cdot\left(\frac{H(f)}{p^k}+H(g)\right)\right]^{m+1}\leqslant\frac{p^{\frac{1}{n-1}}}{p^k}+\frac{p^{\frac{1}{n-1}}H(g)}{H(f)},$$

which is equivalent to

$$\frac{|b_n|^{1+\frac{n}{n-1}}}{|b_n|^{1+m}}\left[|b_n|+\frac{H(f)}{p^k}+H(g)\right]^{m+1}\leqslant\frac{p^{\frac{1}{n-1}}}{p^k}+\frac{p^{\frac{1}{n-1}}H(g)}{H(f)}.$$

Now, since for $n\geqslant 2$ and $m\geqslant 1$ we have

$$\frac{|b_n|^{1+\frac{n}{n-1}}}{|b_n|^{1+m}}\leqslant\frac{|b_n|^{1+\frac{n}{n-1}}}{|b_n|^2}=|b_n|^{\frac{1}{n-1}},$$

it will be sufficient to prove that

$$|b_n|^{\frac{1}{n-1}}\left[|b_n|+\frac{H(f)}{p^k}+H(g)\right]^{m+1}\leqslant\frac{p^{\frac{1}{n-1}}H(g)}{H(f)},$$

that is

$$p\geqslant\frac{H(f)^{n-1}}{H(g)^{n-1}}\cdot|b_n|\cdot\left[|b_n|+\frac{H(f)}{p^k}+H(g)\right]^{(m+1)(n-1)}.$$

Now, since $|b_n|\leqslant H(g)$, it suffices to prove that

$$p\geqslant\frac{H(f)^{n-1}}{H(g)^{n-1}}\cdot H(g)\cdot\left[2H(g)+\frac{H(f)}{p^k}\right]^{(m+1)(n-1)},$$

or equivalently, that

$$p \geqslant H(f)^{n-1}H(g)^{m(n-1)+1} \cdot \left[2 + \frac{H(f)}{p^k H(g)}\right]^{(m+1)(n-1)}. \tag{10}$$

Using the idea in [5], if we define now the function

$$\mathcal{F}(x) := H(f)^{n-1}H(g)^{m(n-1)+1} \cdot \left[2 + \frac{H(f)}{xH(g)}\right]^{(m+1)(n-1)} \qquad \text{for } \ x > 0,$$

then in view of (10) we have to search for a value of p as small as possible such that $p \geqslant \mathcal{F}(p^k)$. In this respect, since $\mathcal{F}$ is a decreasing function, it will be sufficient to search for a suitable $\delta > 0$, such that

$$p \geqslant B := \delta H(f)^{n-1}H(g)^{m(n-1)+1}$$

and

$$B \geqslant \mathcal{F}\left(B^k\right).$$

Therefore it will be sufficient to find a δ as small as possible satisfying

$$\delta \geqslant \left(2 + \frac{1}{\delta^k H(f)^{k(n-1)-1}H(g)^{k(m(n-1)+1)+1}}\right)^{(m+1)(n-1)},$$

that is

$$\delta \geqslant \left(2 + \frac{1}{\delta^k A}\right)^{(m+1)(n-1)}, \tag{11}$$

recalling our notation $A = H(f)^{k(n-1)-1}H(g)^{k(m(n-1)+1)+1}$. A suitable candidate for a δ satisfying (11) is easily seen to be

$$\delta_0 := \left(2 + \frac{1}{2^{k(m+1)(n-1)}A}\right)^{(m+1)(n-1)},$$

since obviously $\delta_0 > 2^{(m+1)(n-1)}$. This proves that for

$$p \geqslant \left(2 + \frac{1}{2^{k(m+1)(n-1)}A}\right)^{(m+1)(n-1)} H(f)^{n-1}H(g)^{m(n-1)+1}$$

we have $|R(g, f_1)| < 1$, which contradicts (3), and completes the proof. ■

Proof of Theorem 1.4. We will use the notation from the proof of Theorem 1.1. The case $m = 0$ follows directly from Theorem 1.3, so we may assume that $m \geqslant 1$ and hence $n \geqslant 2$. Therefore, our assumption that $p > |b_n|^n(|a_0| + \cdots + |a_m|)^{n-1}$ shows that $p > |a_0| + \cdots + |a_m|$ and therefore

$$p^k > |a_0| + \cdots + |a_m|. \tag{12}$$

On the other hand, the fact that $|b_n| > |b_0| + \cdots + |b_{n-1}|$ implies $|b_n| \geqslant 1 + |b_0| + \cdots + |b_{n-1}|$, so in view of (12) we deduce that

$$p^k|b_n| \geqslant p^k + \sum_{i=0}^{n-1} p^k|b_i| > \sum_{i=0}^{m} |a_i| + \sum_{i=0}^{n-1} p^k|b_i| \geqslant \sum_{i=0}^{m} |a_i + p^k b_i| + \sum_{i=m+1}^{n-1} p^k|b_i|, \quad (13)$$

with the rightmost sum in (13) appearing only if $n - m \geqslant 2$. In view of (13) we deduce that all the roots θ of $f(X) + p^k g(X)$ satisfy $|\theta| \leqslant 1$, so by (7) we obtain

$$|R(g, f_1)| \leqslant \frac{|b_n|^n(|a_0| + \cdots + |a_m|)^s}{p} \leqslant \frac{|b_n|^n(|a_0| + \cdots + |a_m|)^{n-1}}{p}.$$

Therefore, if $p > |b_n|^n(|a_0| + \cdots + |a_m|)^{n-1}$, then $f + p^k g$ must be irreducible over $\mathbb{Q}$. ■

Proof of Corollary 1.5. Here too we may assume $m \geqslant 1$. The fact that $|a_0| \geqslant |a_1| + \cdots + |a_m|$ forces the roots of f to satisfy $|z| \geqslant 1$, while condition $|b_n| > |b_0| + \cdots + |b_{n-1}|$ shows that the roots of g must satisfy $|z| < 1$. Therefore f and g must be algebraically relatively prime, and one applies Theorem 1.4. ■

Remark 2.1. We end by noting that slightly sharper conditions than those exhibited in Theorem 1.1 may be also obtained when $g(0) \neq 0$ and f is a monomial, say $f(X) = a_m X^m$ for some $m \in \{1, \ldots, n-1\}$, $a_m \neq 0$. In this case $H(f) = a_m$ and instead of (9) we obtain

$$|f(\theta_j)| < H(f)\left(1 + \frac{1}{|b_n|} \cdot \left(\frac{H(f)}{p^k} + H(g)\right)\right)^m,$$

and therefore

$$|R(g, f_1)| < \frac{|b_n|^n}{p} H(f)^{n-1}\left(1 + \frac{1}{|b_n|} \cdot \left(\frac{H(f)}{p^k} + H(g)\right)\right)^{m(n-1)}.$$

The reader may easily check that the same conclusion on the irreducibility of $f + p^k g$ holds in this case for primes p satisfying

$$p > \left(2 + \frac{1}{2^{km(n-1)}}\right)^{m(n-1)} H(f)^{n-1} H(g)^{m(n-1)+1}.$$

References

[1] A.I. Bonciocat, N.C. Bonciocat, A. Zaharescu, *On the number of factors of convolutions of polynomials with integer coefficients*, Rocky Mountain J. Math. **38**(2) (2008), 417–431.

[2] A.I. Bonciocat, N.C. Bonciocat, M. Cipu, *Irreducibility criteria for compositions and multiplicative convolutions of polynomials with integer coefficients*, An. Şt. Univ. Ovidius Constanţa, vol. **22**(1) (2014), 73–84.

[3] A.I. Bonciocat, A. Zaharescu, *Irreducibility results for compositions of polynomials with integer coefficients*, Monatsh. Math. **149**(1) (2006), 31–41.
[4] N.C. Bonciocat, *Upper bounds for the number of factors for a class of polynomials with rational coefficients*, Acta Arith. **113**(2) (2004), 175–187.
[5] N.C. Bonciocat, Y. Bugeaud, M. Cipu, M. Mignotte, *Irreducibility criteria for sums of two relatively prime polynomials*, Int. J. Number Theory **9**(6) (2013), 1529–1539
[6] M. Cavachi, *On a special case of Hilbert's irreducibility theorem*, J. Number Theory **82** (2000), no. 1, 96–99.
[7] M. Cavachi, M. Vâjâitu and A. Zaharescu, *A class of irreducible polynomials*, J. Ramanujan Math. Soc. **17** (2002), no. 3, 161–172.
[8] G. Dumas, *Sur quelques cas d'irreductibilité des polynômes á coefficients rationnels*, Journal de Math. Pure et Appl. **2** (1906), 191–258.
[9] M. Fried, *On Hilbert's irreducibility theorem*, J. Number Theory **6** (1974), 211–231.
[10] K. Langmann, *Der Hilbertsche Irreduzibilitätssatz und Primzahlfragen*, J. Reine Angew. Math. **413** (1991), 213–219.

Address: Nicolae Ciprian Bonciocat: Simion Stoilow Institute of Mathematics of the Romanian Academy, Research Unit 5, P.O. Box 1-764, Bucharest 014700, Romania.

E-mail: Nicolae.Bonciocat@imar.ro

Received: 23 March 2015; **revised:** 23 July 2015

Functiones et Approximatio
54.2 (2016), 173–193
doi: 10.7169/facm/2016.54.2.4

MEAN SQUARE OF THE ERROR TERM IN THE ASYMMETRIC MULTIDIMENSIONAL DIVISOR PROBLEM

Xiaodong Cao, Yoshio Tanigawa, Wenguang Zhai

Abstract: Let $\boldsymbol{a} = (a_1, \cdots, a_k)$ denote a k-tuple of positive integers such that $a_1 \leqslant a_2 \leqslant \cdots \leqslant a_k$. We put $d(\boldsymbol{a}; n) = \sum_{n_1^{a_1} \cdots n_k^{a_k} = n} 1$ and let $\Delta(\boldsymbol{a}; x)$ be the error term of the corresponding asymptotic formula for the summatory function of $d(\boldsymbol{a}; n)$. In this paper we show an asymptotic formula of the mean square of $\Delta(\boldsymbol{a}; x)$ under a certain condition. Moreover, when k equals 2 or 3, we give unconditional asymptotic formulas for these mean squares.

Keywords: asymmetric multidimensional divisor problem, mean square of the error term, Dirichlet series, functional equation, the Tong-type representation.

1. Introduction and the statement of results

Let k be a fixed positive integer and $x \geqslant 1$. We put $\boldsymbol{a} := (a_1, \ldots, a_k)$, where a_j $(j = 1, \ldots, k)$ are positive integers such that $a_1 \leqslant \cdots \leqslant a_k$. By $d(\boldsymbol{a}; n)$ we denote the number of representations of an integer n in the form $n = n_1^{a_1} \cdots n_k^{a_k}$, namely,

$$d(\boldsymbol{a}; n) = \sum_{n_1^{a_1} \cdots n_k^{a_k} = n} 1. \tag{1.1}$$

We define

$$\Delta(\boldsymbol{a}; x) := \sum_{n \leqslant x}{}' d(\boldsymbol{a}; n) - H(\boldsymbol{a}; x),$$

where $H(\boldsymbol{a}; x)$ is the main term of the summatory function of $d(\boldsymbol{a}; n)$ given by the sum of residues of $\prod_{j=1}^{k} \zeta(a_j s) \frac{x^s}{s}$, and $'$ in the summation symbol means that the last term $d(\boldsymbol{a}; x)$ should be counted with weight $1/2$ when x is an integer. The

The first and the third authors are supported by the National Key Basic Research Program of China (Grant No.2013CB834201), the National Natural Science Foundation of China (Grant No.11171344), the Natural Science Foundation of Beijing (Grant No.1112010) and the Fundamental Research Funds for the Central Universities in China (2012Ys01). The second author is supported by Grant-in-Aid for Scientific Research no.24540015.

2010 Mathematics Subject Classification: primary: 11N37

asymmetric multidimensional divisor problem (or the general divisor problem) is to study the behaviour of $\Delta(\boldsymbol{a}; x)$. See also Ivić [7] and Krätzel [10], or the survey paper [9].

When $a_1 = a_2 = 1$, $d(1,1;n) = \sum_{d|n} 1$, $\Delta(1,1;x) = \sum_{n\leqslant x} d(1,1,;n) - x(\log x + 2\gamma - 1)$, ($\gamma$ is the Euler constant), the above problem is the classical Dirichlet divisor problem. Dirichlet proved $\Delta(1,1;x) = O(x^{1/2})$ by his famous hyperbola method. The exponent $1/2$ was later improved by many researchers. The latest result is

$$\Delta(x) = O(x^{131/416}(\log x)^{26947/8320})$$

due to Huxley [6]. For the lower bounds, it is known that

$$\Delta(1,1;x) = \Omega_+\left(x^{\frac{1}{4}}(\log x)^{\frac{1}{4}}(\log\log x)^{\frac{3+\log 4}{4}}\exp(-c\sqrt{\log\log\log x})\right) \qquad (c>0)$$

and

$$\Delta(1,1;x) = \Omega_-\left(x^{\frac{1}{4}}\exp(c'(\log\log x)^{\frac{1}{4}}(\log\log\log x)^{-\frac{3}{4}})\right) \qquad (c'>0),$$

which are due to Hafner [5] and Corrádi and Kátai [3], respectively. Many corresponding upper bounds and Ω-results for the asymmetric multidimensional divisor problem can be found in [7] and [10].

The mean square estimate is one of the main topics in the theory of divisor problem. Let $R(T)$ be the error term defined by the following formula

$$R(T) = \int_1^T \Delta^2(1,1;x)dx - cT^{3/2},$$

where $c = \frac{1}{6\pi^2}\sum_{n=1}^{\infty}\frac{d(1,1;n)^2}{n^{3/2}}$ is a positive constant. Cramér [4] first proved that

$$R(T) = O(T^{5/4+\varepsilon}).$$

Cramér's estimate of $R(T)$ was improved to

$$R(T) = O(T\log^5 T) \tag{1.2}$$

by Tong [12] and recently to $R(T) = O(T\log^3 T\log\log T)$ by Lau and Tsang [11]. Tong's method of proving (1.2) is the initial motivation of our previous paper [2].

Ivić [8] studied the upper bound and Ω-result of the mean square of $\Delta(\boldsymbol{a}; x)$ for general k. As for the upper bound, he proved that if

$$\int_1^T \Delta^2(\boldsymbol{a}; x)dx \ll T^{1+2\beta_k} \qquad (\beta_k \geqslant 0)$$

then $\beta_k \geqslant g_k$, where

$$g_k = \frac{r-1}{2(a_1+\cdots+a_r)}$$

and r is the largest integer such that

$$(r-2)a_r \leqslant a_1 + \cdots + a_{r-1} \qquad (2 \leqslant r \leqslant k)$$

[8, (1.5)]. Moreover, he showed that if the estimate

$$\int_1^T |\zeta(1/2+it)|^{2k-2} dt \ll T^{1+\varepsilon}$$

holds, then $\beta_k = g_k$. In particular, $\beta_k = g_k$ holds for $k = 2$ and 3. For the lower bound, he showed that

$$\int_1^T \Delta^2(\boldsymbol{a}; x) dx = \Omega(T^{1+2g_k} \log^A T)$$

with some constant $A \geqslant 0$. Inspired by these facts, Ivić conjectured that the asymptotic formula

$$\int_1^T \Delta^2(\boldsymbol{a}; x) dx = (E_k + o(1)) T^{1+2g_k} \log^{A_k} T \tag{1.3}$$

holds for general $k \geqslant 2$ with some constants $E_k > 0$ and $A_k \geqslant 0$ [8, (5.7)].

When $k = 2$, Ivić's conjecture (1.3) was confirmed by Cao and Zhai [13]. More precisely they proved that

$$\int_1^T \Delta^2(\boldsymbol{a}; x) dx = c(\boldsymbol{a}) T^{\frac{1+a_1+a_2}{a_1+a_2}} + O\left(T^{\frac{1+a_1+a_2}{a_1+a_2} - \frac{a_1}{2a_2(a_1+a_2)(a_1+a_2-1)}} \log^{\frac{7}{2}} T\right), \tag{1.4}$$

where a_1 and a_2 are integers such that $1 \leqslant a_1 \leqslant a_2$, $\boldsymbol{a} = (a_1, a_2)$ and $c(\boldsymbol{a})$ is some constant. Their method is based on the transformation formula of the exponential sum and the Chowla and Walum type representation of $\Delta(\boldsymbol{a}; x)$ (see also [1]). When $a_1 = a_2 = 1$, the error term in (1.4) becomes $O(T^{\frac{5}{4}} \log^{\frac{7}{2}} T)$. Hence (1.4) is an analogue of Cramér's result for $\Delta(1, 1; x)$.

In this paper we shall study the mean square estimate of the error term $\Delta(\boldsymbol{a}; x)$ more closely by means of the Tong method [2, 12]. For this purpose, we need an auxiliary divisor function defined by

$$\hat{d}(\boldsymbol{a}; n) = \sum_{n_1^{a_1} \cdots n_k^{a_k} = n} n_1^{a_1 - 1} \cdots n_k^{a_k - 1}, \tag{1.5}$$

which is a dual function of $d(\boldsymbol{a}; n)$. For convenience, we write

$$b(n) = \pi^{2\alpha - k/2} \hat{d}(\boldsymbol{a}; n) \qquad \text{and} \qquad \mu_n = \pi^{2\alpha} n,$$

where

$$\alpha := (a_1 + \cdots + a_k)/2.$$

From (1.1) and (1.5), we have

$$\varphi(s) := \sum_{n=1}^{\infty} \frac{d(\boldsymbol{a}; n)}{n^s} = \prod_{j=1}^{k} \zeta(a_j s) \qquad (\operatorname{Re} s > 1/a_1)$$

and

$$\begin{aligned}\psi(s) &:= \sum_{n=1}^{\infty} \frac{b(n)}{\mu_n^s} = \pi^{2\alpha - k/2 - 2\alpha s} \sum_{n=1}^{\infty} \frac{\hat{d}(\boldsymbol{a}; n)}{n^s} \\ &= \pi^{2\alpha - k/2 - 2\alpha s} \prod_{j=1}^{k} \zeta(a_j s - a_j + 1) \qquad (\operatorname{Re} s > 1). \end{aligned} \tag{1.6}$$

Let $1/2 \leqslant \sigma^* < 1$ be a real number defined by

$$\sigma^* := \inf \left\{ \sigma \;\Big|\; \int_0^T |\psi(\sigma + it)|^2 dt \ll T^{1+\varepsilon} \right\}. \tag{1.7}$$

From (1.6) it is easy to check that

$$\sigma^* \geqslant 1 - \frac{1}{2a_k}. \tag{1.8}$$

In this paper we assume that σ^* satisfies the condition

$$\sigma^* < 1 - \frac{k-1}{4\alpha}. \tag{1.9}$$

This condition plays an important role in Tong's method. From (1.8), we note that (1.9) implies, as a necessary condition, that

$$(k-2)a_k < a_1 + \cdots + a_{k-1}. \tag{1.10}$$

We first prove a conditional asymptotic formula of the mean square of $\Delta(\boldsymbol{a}, x)$.

Theorem 1. *Suppose that* (1.9) *and* (1.10) *hold. Then we have*

$$\int_1^T \Delta^2(\boldsymbol{a}; x) dx = c(\boldsymbol{a}) T^{1 + \frac{k-1}{2\alpha}} + O\left(T^{1 + \frac{k-1}{2\alpha} - \eta(\boldsymbol{a}) + \varepsilon}\right), \tag{1.11}$$

where $c(\boldsymbol{a})$ is a certain positive constant and

$$\eta(\boldsymbol{a}) := \frac{2(1-\sigma^*) - \frac{k-1}{2\alpha}}{2\alpha(3 - 2\sigma^* - \frac{1}{a_k}) - 1} > 0. \tag{1.12}$$

It is an important problem to determine the exact value of σ^*. Generally it is a very difficult problem, but it is easy to see that if the Lindelöf hypothesis for $\zeta(s)$ is true, then $\sigma^* = 1 - 1/2a_k$. Hence from Theorem 1 we have

Corollary 1. *Suppose that* (1.10) *holds. If the Lindelöf hypothesis is true, then we have*

$$\int_1^T \Delta^2(\boldsymbol{a};x)dx = c(\boldsymbol{a})T^{1+\frac{k-1}{2\alpha}} + O\left(T^{1+\frac{k-1}{2\alpha}-\frac{2\alpha-(k-1)a_k}{2\alpha(2\alpha-1)a_k}+\varepsilon}\right),$$

where $c(\boldsymbol{a})$ is a certain positive constant.

When $k = 2$, we find that $\sigma^* = 1 - 1/2a_2$ holds unconditionally, which is a consequence of the fourth power moment of $\zeta(s)$ on the critical line. Hence (1.11) gives

Theorem 2. *Suppose $a_1 \leqslant a_2$. Then we have*

$$\int_1^T \Delta^2(a_1,a_2;x)dx = c_2T^{1+\frac{1}{a_1+a_2}} + O\left(T^{1+\frac{1}{a_1+a_2}-\frac{a_1}{a_2(a_1+a_2)(a_1+a_2-1)}+\varepsilon}\right), \quad (1.13)$$

where c_2 is a certain positive constant.

Theorem 2 improves the error term of (1.4). We note that if we take $a_1 = a_2 = 1$, the error term in (1.13) is $O(T^{1+\varepsilon})$. So (1.13) is an analogue of (1.2) modulo term T^{ε}.

Another interesting case is $k = 3$. In this case we can prove the following Theorem 3.

Theorem 3. *Let $k = 3$. If $a_1 \leqslant a_2 \leqslant a_3$ and $a_3 < a_1 + a_2$, then we have*

$$\int_1^T \Delta^2(a_1,a_2,a_3;x)dx = c_3T^{1+\frac{2}{a_1+a_2+a_3}} + O(T^{1+\frac{2}{a_1+a_2+a_3}-\eta_3+\varepsilon}),$$

where

$$\eta_3 = \begin{cases} \dfrac{1}{(a_1+a_2+a_3)(3+2(a_1+a_2+a_3)(1-1/a_3))} & \text{if } 3(a_2+a_3) \leqslant 7a_1, \\ \dfrac{4a_1a_3}{(a_1+a_2+a_3)\big((a_1+a_2+a_3)(a_1+3a_2+3a_3)(a_3-1)+a_3(5a_1+3a_2+3a_3)\big)} & \\ \qquad \text{if } 3(a_2+a_3) > 7a_1, 3a_3+a_1 \leqslant 5a_2 \text{ and } 3a_3 < a_1+3a_2, & \\ \dfrac{a_1+a_2-a_3}{a_3(a_1+a_2+a_3)(a_1+a_2+a_3-1)} & \text{otherwise,} \end{cases}$$

and c_3 is a certain positive constant.

We shall prove Theorem 3 in Section 4.

2. The truncated Tong-type formula of $\boldsymbol{\Delta(a;x)}$

In [12], Tong studied the mean square of $\Delta(\underbrace{1,\dots,1}_{k};x)$. By using the functional equation of $\zeta^k(s)$ he derived a very useful formula of $\Delta(1,\dots,1;x)$, which we call

the truncated Tong-type formula, where the first finite sum is the same as that of the truncated Voronoï formula, while its error term is represented by the integrals like (2.6) below.

In our case, using the functional equation of the Riemann zeta function

$$\pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\zeta(s) = \pi^{-(1-s)/2}\Gamma\left(\frac{1-s}{2}\right)\zeta(1-s),$$

we find easily that the functional equation of $\varphi(s)$ and $\psi(s)$ has a form

$$\Delta_1(s)\varphi(s) = \Delta_2(1-s)\psi(1-s), \tag{2.1}$$

where

$$\Delta_1(s) := \prod_{j=1}^{k}\Gamma\left(\frac{a_j s}{2}\right) \tag{2.2}$$

and

$$\Delta_2(s) := \prod_{j=1}^{k}\Gamma\left(\frac{a_j s - a_j + 1}{2}\right). \tag{2.3}$$

Note that $\hat{d}(\boldsymbol{a}; n)$ does not satisfy the Ramanujan conjecture and also the gamma factors on the left and right hand side of (2.1) are not the same for general $\boldsymbol{a}$, so the pair of Dirichlet series $\varphi(s)$ and $\psi(s)$ is not contained in the so-called Selberg class. In our previous paper [2], we developed the theory of the truncated Tong-type formula of the error term for such a pair of Dirichlet series. Obviously $\varphi(s)$ and $\psi(s)$ satisfy the conditions therein.

In order to write the truncated Tong-type formula for $\Delta(\boldsymbol{a}; x)$ in the present case, we use the same notations as in [2]. From (2.2) and (2.3), we have (we repeat the definion of α for its importance)

$$\alpha = \frac{a_1 + \cdots + a_k}{2}, \qquad r = 1,$$

$$\mu = \frac{1-k}{2}, \qquad \mu' = \sum_j\left(-\frac{a_j}{2}\right) + \frac{1}{2} = -\alpha + \frac{1}{2},$$

$$\nu = -\frac{1}{2}\sum_j \log a_j, \qquad \nu' = -\frac{1}{2}\sum_j a_j \log a_j,$$

$$\lambda = \sum_j a_j \log a_j = \lambda', \qquad h = 2\alpha e^{-\frac{\lambda+\lambda'}{2\alpha}} = 2\alpha\prod_{j=1}^{k} a_j^{-a_j/\alpha}$$

and

$$\theta_\varrho = \frac{r}{2} - \frac{1}{4\alpha} + \varrho\left(1 - \frac{1}{2\alpha}\right) + \frac{\mu' - \mu}{2\alpha}.$$

In this paper we only consider the case $\varrho = 0$, hence

$$\theta_0 = \frac{1}{2} - \frac{1}{4\alpha} + \frac{\mu' - \mu}{2\alpha} = \frac{k-1}{4\alpha}. \tag{2.4}$$

We also put

$$\lambda_0 = \theta_0 + \frac{1}{2\alpha} - r - 1 = \frac{k+1}{4\alpha} - 2. \tag{2.5}$$

In Tong's theory, it is important to approximate $\Delta(\boldsymbol{a}; x)$ by the K-th averaging integral

$$\int_{\mathbf{E}_K} \Delta(\boldsymbol{a}; \tilde{y}) d\mathrm{Y}_K,$$

where we use the notation

$$\int_{\mathbf{E}_K} g(\tilde{y}) d\mathrm{Y}_K = \int_0^1 \cdots \int_0^1 g(\tilde{y}) dy_1 \cdots dy_K,$$

with

$$\tilde{y} = y + \frac{1}{x}(y_1 + \cdots + y_K)$$

for an integrable function $g(y)$. Let $\hat{\Delta}(\boldsymbol{a}; x)$ be the error term of the asymptotic formula of summatory function of $\hat{d}(\boldsymbol{a}; n)$, which is defined mutatis mutandis as for $\Delta(\boldsymbol{a}; x)$. Then the averaging integral can be expressed by the function defined by

$$I(\lambda, M, N, y) = 2\pi i \int_M^N u^\lambda \hat{\Delta}(\boldsymbol{a}; u) \exp\left(-ih(uy)^{\frac{1}{2\alpha}}\right) du. \tag{2.6}$$

The next lemma gives the truncated Tong-type formula of $\Delta(\boldsymbol{a}; y)$. Applying Theorem 5 of [2] directly we get

Lemma 1. *Let $1 \leqslant x \leqslant y \leqslant (1+\delta)x$, $N = [x^{4\alpha-1-\varepsilon}]$ and $J = [(4\alpha^2 r + 4\alpha)\varepsilon^{-1}]$, where δ is a small positive constant. In every subinterval $[t, t + Bt^{1-1/2\alpha}] \subset [1, \sqrt{N}]$, there exists $M \neq \mu_n$ such that the following Tong-type formula holds:*

$$\Delta(\boldsymbol{a}; y) = \sum_{j=1}^{7} R_j(y),$$

where

$$\begin{aligned}
R_1(y) &= \kappa_0 y^{\theta_0} \sum_{\mu_n \leqslant M} \frac{b(n)}{\mu_n^{1-\theta_0}} \cos(h(y\mu_n)^{1/2\alpha} + c_0\pi) \\
&= \kappa_0 \pi^{2\alpha(\theta_0-1)} y^{\theta_0} \sum_{n \leqslant M'} \frac{b(n)}{n^{1-\theta_0}} \cos(h\pi(yn)^{1/2\alpha} + c_0\pi) \\
&= \kappa_0 \pi^{2\alpha\theta_0 - k/2} y^{\theta_0} \sum_{n \leqslant M'} \frac{\hat{d}(\boldsymbol{a}; n)}{n^{1-\theta_0}} \cos(h\pi(yn)^{1/2\alpha} + c_0\pi), \\
R_2(y) &= y^{\theta_0 + \frac{1}{2\alpha}} \operatorname{Re}\{c_{00} I(\lambda_0, M, N, y)\}, \\
R_3(y) &= \sum_{\substack{l=0 \\ l+m>0}}^{J} \sum_{m=0}^{J} \operatorname{Re}\left\{c_{lm} I\left(\lambda_0 + \frac{l-m}{2\alpha}, M, N, y\right)\right\} x^{-l} y^{-l+\theta_0+\frac{1}{2\alpha}+\frac{l-m}{2\alpha}},
\end{aligned}$$

$$R_4(y) = \sum_{j=0}^{K}\sum_{m=0}^{K} \mathrm{Re}\left\{c'_{jm} I\left(\lambda_0 - \frac{K+m}{2\alpha}, N, \infty, y + \frac{j}{x}\right)\right\}$$
$$\times x^K \left(y + \frac{j}{x}\right)^{K+\theta_0+\frac{1}{2\alpha}-\frac{K+m}{2\alpha}},$$
$$R_5(y) = x^{\frac{k-3}{4\alpha}} M^{\max(\frac{k-3}{4\alpha},0)+\varepsilon} + x^{\frac{k+1}{4\alpha-2}} M^{\frac{k+1}{4\alpha}+\varepsilon} + x^{\frac{k-1}{4\alpha}-\frac{1}{2}} M^{\omega_1-\frac{3}{2}+\frac{k-1}{4\alpha}}$$
$$+ x^{(4\alpha-1)(1+\omega_1)-2K+\frac{k}{2\alpha}+\frac{2K}{\alpha}-6\alpha},$$
$$R_6(y) = 0,$$
$$R_7(y) = \Delta(\boldsymbol{a}; y) - \int_{\mathbf{E}_K} \Delta(\boldsymbol{a}; \tilde{y}) d\mathrm{Y}_K,$$

where $M' = M/\pi^{2\alpha}$ and $\kappa_0 \neq 0, c_{00}, c_{lm}, c'_{jm}$ are certain constants, K is a suitably large integer and $\omega_1 < 1$ is a certain constant.

We need one remark on $R_6(y)$. In fact in [2] $R_6(y)$ is given by

$$R_6(y) \ll \begin{cases} 0 & \text{if } b(n) \geqslant 0, \\ x^{\theta_0} M^{\omega_0 - 1 + \frac{k-1}{4\alpha}}, & \text{if } b(n) \ll n^{\omega_0}. \end{cases}$$

In our case we can take $R_6(y) = 0$ since $b(n) = \pi^{2\alpha - k/2}\hat{d}(\boldsymbol{a}, n)$ is always non-negative.

We recall important estimates of the integral of $I(\lambda, M, N, y)$ which we will need in the next section.

Lemma 2. *Let $M < N < x^A$, where A is a fixed positive number, w be a real number and $0 < \mu < \frac{M}{2}$. Then we have*

$$\int_x^{(1+\delta)x} I(\lambda, M, N, y) y^w \cos(h(\mu y)^{1/2\alpha} + c_0\pi) dy$$
$$\ll x^{w+1-3/4\alpha+\varepsilon} \max_{M \leqslant P \leqslant N} P^{\lambda+\sigma^*+1-3/4\alpha}.$$

Lemma 3. *Let $2(\lambda+\sigma^*) \neq -1$, $M < N < x^A$, where A is a fixed positive number, and $\delta > 0$ with $(1+\delta)^{1/\alpha} - 1 < 1/4$. Then we have*

$$\int_x^{(1+\delta)x} |I(\lambda, M, N, y)|^2 dy \ll x^{1-1/\alpha+\varepsilon} \max_{M \leqslant P \leqslant N} P^{2(\lambda+\sigma^*+1)-1/\alpha}.$$

Lemma 4. *Let $2(\lambda + \sigma^*) \neq -1, 2(\lambda + \sigma^* + 1) < 1/\alpha, M \geqslant 1$ and $\delta > 0$ with $(1+\delta)^{1/\alpha} - 1 < 1/4$. Then we have*

$$\int_x^{(1+\delta)x} |I(\lambda, M, \infty, y)|^2 dy \ll x^{1-1/\alpha+\varepsilon} M^{2(\lambda+\sigma^*+1)-1/\alpha}.$$

These lemmas are Lemmas 8, 9 and 10 of [2], respectively. See [2] for details.

3. Mean square of $\Delta(\boldsymbol{a}, x)$

In the asymmetric multidimensional divisor problem, the number $(\mu' - \mu)/2 = -\alpha + k/2$ plays an important role. Although the proof of Theorem 1 is similar to that of Theorem 1 in [2], we shall give all details for the sake of completeness.

Let

$$K_1(y) = R_1(y) + R_2(y)$$

and

$$K_2(y) = \sum_{j=3}^{7} R_j(y).$$

It is sufficient to evaluate the integral $\int_x^{(1+\delta)x} (K_1(y) + K_2(y))^2 dy$ for $1 \leqslant x < T$, where δ is some fixed small positive number.

We need the upper bound of the summatory function of $\hat{d}^{\,2}(\boldsymbol{a}, n)$. Moreover, we have

Lemma 5. *Let $x > 1$. Then we have*

$$x^{2-1/a_k} \ll \sum_{n \leqslant x} \hat{d}^{\,2}(\boldsymbol{a}; n) \ll x^{2-1/a_k+\varepsilon}. \tag{3.1}$$

Proof. By Cauchy's inequality we get

$$\begin{aligned} \hat{d}^{\,2}(\boldsymbol{a}; n) &= \left(\sum_{n_1^{a_1} \cdots n_k^{a_k} = n} n_1^{a_1 - 1} \cdots n_k^{a_k - 1} \right)^2 \\ &\leqslant \sum_{n_1^{a_1} \cdots n_k^{a_k} = n} 1 \times \sum_{n_1^{a_1} \cdots n_k^{a_k} = n} n_1^{2(a_1-1)} \cdots n_k^{2(a_k-1)} \\ &\ll n^{\varepsilon} c(\boldsymbol{a}; n), \end{aligned}$$

where $c(\boldsymbol{a}; n) = \sum_{n_1^{a_1} \cdots n_k^{a_k} = n} n_1^{2(a_1-1)} \cdots n_k^{2(a_k-1)}$. We also note that $\hat{d}^{\,2}(\boldsymbol{a}; n) \geqslant c(\boldsymbol{a}; n)$. It is easy to see that the generating Dirichlet series of $c(\boldsymbol{a}; n)$ has the form

$$\sum_{n=1}^{\infty} \frac{c(\boldsymbol{a}; n)}{n^s} = \prod_{j=1}^{k} \zeta(a_j s - 2(a_j - 1)), \qquad \mathrm{Re}(s) > 2 - 1/a_k.$$

This Dirichlet series has poles at points $2 - 1/a_j \ \ (j = 1, \ldots, k)$, hence

$$\sum_{n \leqslant x} c(\boldsymbol{a}; n) = c x^{2-1/a_k} \log^{A-1} x \cdot (1 + o(1))$$

where c is some constant and A is the number of j such that $a_j = a_k$. Therefore Lemma 5 follows. ∎

Let σ^* be the number defined by (1.7) which satisfies (1.9). The inequality (1.9) is equivalent to

$$2(\lambda_0 + \sigma^* + 1) < \frac{1}{\alpha}, \tag{3.2}$$

where λ_0 was defined by (2.5).

3.1. Evaluation of $\int_x^{(1+\delta)x} K_1^2(y)dy$

Let $\kappa_0' = \kappa_0 \pi^{2\alpha(\theta_0-1)}$ for simplicity. By using the identity

$$\cos(x)\cos(y) = \frac{1}{2}(\cos(x-y) + \cos(x+y))$$

we get

$$\begin{aligned} R_1(y)^2 &= \frac{{\kappa_0'}^2}{2} y^{\frac{k-1}{2\alpha}} \sum_{n\leqslant M'} \sum_{m\leqslant M'} \frac{b(n)b(m)}{(nm)^{1-\frac{k-1}{4\alpha}}} \Big(\cos(h\pi y^{1/2\alpha}(n^{1/2\alpha} - m^{1/2\alpha})) \\ &\quad + \cos(h\pi y^{1/2\alpha}(n^{1/2\alpha} + m^{1/2\alpha}) + 2c_0\pi)\Big) \\ &= \frac{{\kappa_0'}^2}{2} \left(W_1(y) + W_2(y) + W_3(y)\right), \end{aligned}$$

where

$$\begin{aligned} W_1(y) &= y^{\frac{k-1}{2\alpha}} \sum_{n\leqslant M'} \frac{b(n)^2}{n^{2-\frac{k-1}{2\alpha}}}, \\ W_2(y) &= y^{\frac{k-1}{2\alpha}} \sum_{\substack{n,m\leqslant M' \\ n\neq m}} \sum \frac{b(n)b(m)}{(nm)^{1-\frac{k-1}{4\alpha}}} \cos(h\pi y^{1/2\alpha}(n^{1/2\alpha} - m^{1/2\alpha})), \\ W_3(y) &= y^{\frac{k-1}{2\alpha}} \sum_{n,m\leqslant M'} \sum \frac{b(n)b(m)}{(nm)^{1-\frac{k-1}{4\alpha}}} \cos(h\pi y^{1/2\alpha}(n^{1/2\alpha} + m^{1/2\alpha}) + 2c_0\pi). \end{aligned}$$

For the integral of $W_1(y)$, we have

$$\int_x^{(1+\delta)x} W_1(y)dy = \sum_{n\leqslant M'} \frac{b(n)^2}{n^{2-\frac{k-1}{2\alpha}}} \int_x^{(1+\delta)x} y^{\frac{k-1}{2\alpha}} dy.$$

Since (1.10) is equivalent to $\frac{k-1}{2\alpha} < \frac{1}{a_k}$, we find that the series $\sum_n^\infty \frac{b(n)^2}{n^{2-\frac{k-1}{2\alpha}}}$ is convergent. So from (3.1), we have

$$\sum_{n\leqslant M'} \frac{b(n)^2}{n^{2-\frac{k-1}{2\alpha}}} = \sum_{n=1}^{\infty} \frac{b(n)^2}{n^{2-\frac{k-1}{2\alpha}}} + O(M^{\frac{k-1}{2\alpha} - \frac{1}{a_k} + \varepsilon}).$$

Hence

$$\int_x^{(1+\delta)x} W_1(y)dy = \sum_{n=1}^{\infty} \frac{b(n)^2}{n^{2-\frac{k-1}{2\alpha}}} \int_x^{(1+\delta)x} y^{\frac{k-1}{2\alpha}} dy + O(x^{1+\frac{k-1}{2\alpha}} M^{\frac{k-1}{2\alpha}-\frac{1}{a_k}+\varepsilon}). \quad (3.3)$$

By the first derivative test, we have

$$\begin{aligned}\int_x^{(1+\delta)x} W_2(y)dy &\ll x^{\frac{k-1}{2\alpha}+1-\frac{1}{2\alpha}} \sum_{\substack{m,n\leqslant M' \\ m\neq n}}\sum \frac{b(n)b(m)}{(nm)^{1-\frac{k-1}{4\alpha}}} \frac{1}{|n^{1/2\alpha}-m^{1/2\alpha}|} \\ &= x^{\frac{k-2}{2\alpha}+1}\left\{\Sigma_1+\Sigma_2\right\},\end{aligned}$$

where the summation conditions of Σ_1 and Σ_2 are given by

$$SC(\Sigma_1) : |n^{1/2\alpha}-m^{1/2\alpha}| > \frac{1}{10}(nm)^{1/4\alpha}$$

and

$$SC(\Sigma_2) : |n^{1/2\alpha}-m^{1/2\alpha}| \leqslant \frac{1}{10}(nm)^{1/4\alpha},$$

respectively. It is not hard to see that

$$\begin{aligned}\Sigma_1 &\ll \sum_{\substack{n,m\leqslant M' \\ |n^{1/2\alpha}-m^{1/2\alpha}|>\frac{1}{10}(nm)^{1/4\alpha}}}\sum \frac{b(n)b(m)}{(nm)^{1-\frac{k-1}{4\alpha}}} \frac{1}{(nm)^{\frac{1}{4\alpha}}} \\ &\ll \left(\sum_{n\leqslant M'} \frac{b(n)}{n^{1-\frac{k-2}{4\alpha}}}\right)^2 \ll M^{\frac{k-2}{2\alpha}+\varepsilon},\end{aligned}$$

where we used the trivial estimate $\sum_{n\leqslant x} b(n) \ll x^{1+\varepsilon}$. Next we consider Σ_2. By Lagrange's mean value theorem we have

$$n^{1/2\alpha}-m^{1/2\alpha} = \frac{1}{2\alpha}u_0^{1/2\alpha-1}(n-m)$$

for some u_0 between n and m. Since $n \asymp m$ by $SC(\Sigma_2)$, we find

$$|n^{1/2\alpha}-m^{1/2\alpha}| \geqslant (nm)^{1/4\alpha-1/2}|n-m|,$$

thus we get

$$\begin{aligned}\Sigma_2 &\ll \sum_{\substack{n,m\leqslant M' \\ n\neq m}}\sum \frac{b(n)b(m)}{(nm)^{\frac{1}{2}-\frac{k-2}{4\alpha}}} \frac{1}{|n-m|} \\ &\ll \sum_{\substack{n,m\leqslant M' \\ n\neq m}}\sum \left\{\left(\frac{b(n)}{n^{\frac{1}{2}-\frac{k-2}{4\alpha}}}\right)^2 + \left(\frac{b(m)}{m^{\frac{1}{2}-\frac{k-2}{4\alpha}}}\right)^2\right\} \frac{1}{|n-m|}.\end{aligned}$$

By the symmetry of n and m and then using Lemma 5 we obtain

$$\Sigma_2 \ll \sum_{\substack{n,m\leqslant M'\\ n\neq m}}\sum \frac{b(n)^2}{n^{1-\frac{k-2}{2\alpha}}}\frac{1}{|n-m|} \ll M^{1-\frac{1}{a_k}+\frac{k-2}{2\alpha}+\varepsilon}.$$

Here we note that the exponent of M is $1-1/a_k+(k-2)/2\alpha \geqslant 0$ and Σ_2 is greater than Σ_1. Hence

$$\int_x^{(1+\delta)x} W_2(y)dy \ll x^{\frac{k-2}{2\alpha}+1}M^{1-\frac{1}{a_k}+\frac{k-2}{2\alpha}+\varepsilon}. \tag{3.4}$$

It is easy to see that $\int_x^{(1+\delta)x} W_3(y)dy$ is absorbed into the right hand side of (3.4).

From (3.3) and (3.4), we get

$$\begin{aligned}\int_x^{(1+\delta)x} R_1^2(y)dy = \frac{{\kappa_0'}^2}{2}\sum_{n=1}^{\infty}\frac{b(n)^2}{n^{2-\frac{k-1}{2\alpha}}}\int_x^{(1+\delta)x} y^{\frac{k-1}{2\alpha}}dy\\ + O\left(x^{\frac{k-1}{2\alpha}+1+\varepsilon}M^{\frac{k-1}{2\alpha}-\frac{1}{a_k}}\right) + O\left(x^{\frac{k-2}{2\alpha}+1+\varepsilon}M^{\frac{k-2}{2\alpha}+1-\frac{1}{a_k}}\right).\end{aligned} \tag{3.5}$$

Now we consider the mean square of $R_2(y)$. By Cauchy's inequality and Lemma 3, we have

$$\begin{aligned}\int_x^{(1+\delta)x} R_2^2(y)dy &\ll x^{\frac{k-1}{2\alpha}+\frac{1}{\alpha}}\int_x^{(1+\delta)x}|I(\lambda_0,M,N,y)|^2dy\\ &\ll x^{\frac{k-1}{2\alpha}+\frac{1}{\alpha}}x^{1-\frac{1}{\alpha}+\varepsilon}\max_{M\leqslant P\leqslant N}P^{2(\lambda_0+\sigma^*+1)-\frac{1}{\alpha}}.\end{aligned}$$

From (2.5) and assumption (1.9), we have

$$2(\lambda_0+\sigma^*+1)-1/\alpha < -1/a_k+(k-1)/2\alpha < 0.$$

Therefore

$$\int_x^{(1+\delta)x} R_2^2(y)dy \ll x^{\frac{k-1}{2\alpha}+1+\varepsilon}M^{2\sigma^*-2+\frac{k-1}{2\alpha}}. \tag{3.6}$$

Finally we consider $\int_x^{(1+\delta)x} R_1(y)R_2(y)dy$. From definitions of $R_1(y)$ and $R_2(y)$, we have

$$\begin{aligned}&\int_x^{(1+\delta)x} R_1(y)R_2(y)dy\\ &= \operatorname{Re}\kappa_0' c_{00}\int_x^{(1+\delta)x} y^{\frac{k}{2\alpha}}I(\lambda_0,M,N,y)\sum_{n\leqslant M'}\frac{b(n)}{n^{1-\frac{k-1}{4\alpha}}}\cos(h\pi(ny)^{1/2\alpha}+c_0\pi)dy\\ &= Re\kappa_0' c_{00}(I_1+I_2),\end{aligned}$$

where

$$I_1 = \int_x^{(1+\delta)x} y^{\frac{k}{2\alpha}} I(\lambda_0, M, N, y) \sum_{n \leqslant M'/2} \frac{b(n)}{n^{1-\frac{k-1}{4\alpha}}} \cos(h\pi(ny)^{1/2\alpha} + c_0\pi) dy$$

and

$$I_2 = \int_x^{(1+\delta)x} y^{\frac{k}{2\alpha}} I(\lambda_0, M, N, y) \sum_{M'/2 < n \leqslant M'} \frac{b(n)}{n^{1-\frac{k-1}{4\alpha}}} \cos(h\pi(ny)^{1/2\alpha} + c_0\pi) dy.$$

By Lemma 2 we have

$$I_1 \ll \sum_{n \leqslant M'} \frac{b(n)}{n^{1-\frac{k-1}{4\alpha}}} x^{\frac{k}{2\alpha}+1-\frac{3}{4\alpha}+\varepsilon} \max_{M \leqslant P \leqslant N} P^{\lambda_0+\sigma^*+1-\frac{3}{4\alpha}}.$$

By assumption (1.9), the exponent of P in the above estimate is negative. Hence by using $\sum_{n \leqslant x} b(n) \ll x^{1+\varepsilon}$ again, we get

$$\begin{aligned} I_1 &\ll x^{\frac{2k-3}{4\alpha}+1+\varepsilon} M^{\lambda_0+\sigma^*+1-3/4\alpha} \sum_{n \leqslant M'/2} \frac{b(n)}{n^{1-\frac{k-1}{4\alpha}}} \\ &\ll x^{\frac{2k-3}{4\alpha}+1+\varepsilon} M^{\sigma^*-1+\frac{2k-3}{4\alpha}}. \end{aligned} \tag{3.7}$$

By applying Cauchy's inequality to I_2, we have

$$I_2 \ll x^{\frac{k}{2\alpha}} (V_1 V_2)^{1/2}, \tag{3.8}$$

where

$$V_1 = \int_x^{(1+\delta)x} |I(\lambda_0, M.N, y)|^2 dy$$

and

$$V_2 = \int_x^{(1+\delta)x} \left| \sum_{M'/2 < n \leqslant M'} \frac{b(n)}{n^{1-\frac{k-1}{4\alpha}}} \cos(h\pi(ny)^{1/2\alpha} + c_0\pi) \right|^2 dy.$$

Applying Lemma 3 to V_1 we get

$$V_1 \ll x^{1-\frac{1}{\alpha}+\varepsilon} M^{2\sigma^*-2+\frac{k-1}{2\alpha}}. \tag{3.9}$$

The value of V_2 can be bounded by the same approach as the mean square of $R_1(y)$ and we get

$$V_2 \ll xM^{\frac{k-1}{2\alpha}-\frac{1}{a_k}+\varepsilon} + x^{1-\frac{1}{2\alpha}+\varepsilon} M^{1-\frac{1}{a_k}+\frac{k-2}{2\alpha}}. \tag{3.10}$$

By (3.8), (3.9) and (3.10) we get

$$I_2 \ll x^{1+\frac{k-1}{2\alpha}+\varepsilon} M^{\sigma^*-1+\frac{k-1}{2\alpha}-\frac{1}{2a_k}} + x^{1+\frac{2k-3}{4\alpha}+\varepsilon} M^{\sigma^*-\frac{1}{2}+\frac{2k-3}{4\alpha}-\frac{1}{2a_k}}. \tag{3.11}$$

From the estimates (3.5), (3.6), (3.7) and (3.11) we get

$$\int_x^{(1+\delta)x} K_1^2(y)dy = \frac{\kappa_0'^2}{2}\sum_{n=1}^{\infty}\frac{b(n)^2}{n^{2-\frac{k-1}{2\alpha}}}\int_x^{(1+\delta)x} y^{\frac{k-1}{2\alpha}}dy \tag{3.12}$$
$$+ O\left(x^{\frac{k-2}{2\alpha}+1+\varepsilon}M^{\frac{k-2}{2\alpha}+1-\frac{1}{a_k}}\right) + O\left(x^{\frac{k-1}{2\alpha}+1+\varepsilon}M^{2\sigma^*-2+\frac{k-1}{2\alpha}}\right),$$

where we used the facts $1 - 1/2a_k \leqslant \sigma^*$ and

$$x^{1+\frac{2k-3}{4\alpha}}M^{\sigma^*-\frac{1}{2}+\frac{2k-3}{4\alpha}-\frac{1}{2a_k}} = \left(x^{\frac{k-2}{2\alpha}+1}M^{\frac{k-2}{2\alpha}+1-\frac{1}{a_k}}\right)^{1/2}\left(x^{\frac{k-1}{2\alpha}+1}M^{2\sigma^*-2+\frac{k-1}{2\alpha}}\right)^{1/2}.$$

All error terms in (3.5), (3.7) and (3.11) are bounded by the two error terms in (3.12).

3.2. Evaluation of $\int_x^{(1+\delta)x} K_2^2(y)dy$

We first give the upper bounds of $\int_x^{(1+\delta)x} R_j^2(y)dy$ $(j = 3, \dots, 7)$. By Cauchy's inequality and Lemma 3, we have

$$\begin{aligned}\int_x^{(1+\delta)x} R_3^2(y)dy &\ll \sum_{\substack{0\leqslant l,m\leqslant J\\ l+m>0}}\sum x^{-4l+\frac{k+1}{2\alpha}+\frac{l-m}{\alpha}}\int_x^{(1+\delta)x}\left|I(\lambda_0+\frac{l-m}{2\alpha},M,N,y)\right|^2dy\\ &\ll \sum_{\substack{0\leqslant l,m\leqslant J\\ l+m>0}}\sum x^{-4l+\frac{k+1}{2\alpha}+\frac{l-m}{\alpha}}x^{1-\frac{1}{\alpha}+\varepsilon}\max_{M\leqslant P\leqslant N}P^{2(\lambda_0+\frac{l-m}{2\alpha}+\sigma^*+1)-\frac{1}{\alpha}}\\ &= \Sigma_3+\Sigma_4,\end{aligned}$$

where the summation conditions are

$$SC(\Sigma_3): 0\leqslant l\leqslant m\leqslant J,\ l+m>0 \qquad \text{and} \qquad SC(\Sigma_4): 0\leqslant m<l\leqslant J,$$

respectively. Since we have assumed $2(\lambda_0+\sigma^*+1) < 1/\alpha$, we have

$$\begin{aligned}\Sigma_3 &\ll \sum_{\substack{0\leqslant m\leqslant l\leqslant J\\ l+m>0}} x^{-4l+\frac{k-1}{2\alpha}+\frac{l-m}{\alpha}+1+\varepsilon}M^{2(\lambda_0+\sigma^*+1)-\frac{1}{\alpha}+\frac{l-m}{\alpha}}\\ &= x^{\frac{k-1}{2\alpha}+1+\varepsilon}M^{2(\sigma^*-1)+\frac{k-1}{2\alpha}}\sum_{\substack{0\leqslant m\leqslant l\leqslant J\\ l+m>0}} x^{-4l+\frac{l-m}{\alpha}}M^{\frac{l-m}{\alpha}}.\end{aligned}$$

The sum over l and m in the above formula is bounded by

$$\ll (xM)^{-1/\alpha} + x^{-4} \ll (xM)^{-1/\alpha}.$$

So we have

$$\Sigma_3 \ll x^{\frac{k-3}{2\alpha}+1+\varepsilon}M^{2(\sigma^*-1)+\frac{k-3}{2\alpha}}. \tag{3.13}$$

Next we treat Σ_4. Since

$$2(\lambda_0+\sigma^*+\frac{l-m}{2\alpha}+1)-\frac{1}{\alpha}\geqslant\frac{(a_k-a_1)+\cdots+(a_k-a_{k-1})+a_k}{(a_1+\cdots+a_k)a_k}>0,$$

we have

$$\begin{aligned}\Sigma_4&\ll\sum_{0\leqslant m<l\leqslant J}x^{-4l+\frac{k-1}{2\alpha}+1+\frac{l-m}{\alpha}+\varepsilon}N^{2(\lambda_0+\sigma^*+\frac{l-m}{2\alpha}+1)-\frac{1}{\alpha}}\\&=x^{\frac{k-1}{2\alpha}+1+\varepsilon}N^{2(\lambda_0+\sigma^*+1)-\frac{1}{\alpha}}\sum_{0\leqslant m<l\leqslant J}x^{-4l+\frac{l-m}{\alpha}}N^{\frac{l-m}{\alpha}}.\end{aligned}$$

Having in mind that $N=[x^{4\alpha-1-\varepsilon}]$, the sum over l and m is $O(1)$. So

$$\Sigma_4\ll x^{\frac{k-1}{2\alpha}+1+\varepsilon}N^{2(\lambda_0+\sigma^*+1)-\frac{1}{\alpha}}. \tag{3.14}$$

From (3.13), (3.14) and assumption $M\leqslant\sqrt{N}$ we get

$$\int_x^{(1+\delta)x}R_3^2(y)dy\ll x^{\frac{k-3}{2\alpha}+1+\varepsilon}M^{2(\sigma^*-1)+\frac{k-3}{2\alpha}}+x^{\frac{k-1}{2\alpha}+1+\varepsilon}M^{4(\sigma^*-1)+\frac{k-1}{\alpha}}. \tag{3.15}$$

By Lemma 4 we have

$$\begin{aligned}\int_x^{(1+\delta)x}R_4^2(y)dy&\ll\sum_{j,m=0}^{K}x^{4K+\frac{k-1}{2\alpha}+\frac{1}{\alpha}-\frac{K+m}{\alpha}}\\&\quad\times\int_x^{(1+\delta)x}\left|I\left(\lambda_0-\frac{K+m}{2\alpha},N,\infty,y+\frac{j}{x}\right)\right|^2dy\\&\ll\sum_{j,m=0}^{K}x^{4K+\frac{k-1}{2\alpha}+\frac{1}{\alpha}-\frac{K+m}{\alpha}}x^{1-\frac{1}{\alpha}+\varepsilon}N^{2(\lambda_0-\frac{K+m}{2\alpha}+\sigma^*+1)-\frac{1}{\alpha}}\\&=x^{4K+\frac{k-1}{2\alpha}+1-\frac{K}{\alpha}+\varepsilon}N^{2(\lambda_0+\sigma^*+1)-\frac{1}{\alpha}-\frac{K}{\alpha}}\sum_{j,m=0}^{K}(xN)^{-m/\alpha}.\end{aligned}$$

Since the sum over j and m is bounded, we get by the definition of N that

$$\begin{aligned}\int_x^{(1+\delta)x}R_4^2(y)dy&\ll x^{4K+\frac{k-1}{2\alpha}+1-\frac{K}{\alpha}+\varepsilon}N^{2(\lambda_0+\sigma^*+1)-\frac{1}{\alpha}}x^{-(4\alpha-1-\varepsilon)\frac{K}{\alpha}}\\&\ll x^{\frac{k-1}{2\alpha}+1-\frac{K}{\alpha}+\varepsilon}N^{2(\lambda_0+\sigma^*+1)-\frac{1}{\alpha}}.\end{aligned} \tag{3.16}$$

Now consider $R_5(y)$. By taking K large, we have

$$R_5(y)\ll x^{\frac{k-3}{2\alpha}}M^{\max(\frac{k-3}{4\alpha},0)+\varepsilon}+x^{\frac{k+1}{4\alpha}-2}M^{\frac{k+1}{4\alpha}+\varepsilon}+x^{\frac{k-1}{4\alpha}-\frac{1}{2}}M^{-\frac{1}{2}+\frac{k-1}{4\alpha}}.$$

It is easy to see that

$$R_5(y)\ll\begin{cases}x^{-1/4\alpha} & \text{if } k=2\\ x^{\frac{k-3}{4\alpha}}M^{\frac{k-3}{4\alpha}} & \text{if } k\geqslant 3 \text{ and } M\ll x^{2\alpha-1}.\end{cases}$$

Hence

$$\int_x^{(1+\delta)x} R_5^2(y)dy \ll \begin{cases} x^{1-1/2\alpha} & \text{if } k=2 \\ x^{1+\frac{k-3}{2\alpha}} M^{\frac{k-3}{2\alpha}} & \text{if } k \geqslant 3 \text{ and } M \ll x^{2\alpha-1}. \end{cases} \tag{3.17}$$

By the choice of M, $R_6(y)=0$, so its mean square is bounded trivially.

By the same method as in [2], we have

$$\int_x^{(1+\delta)x} R_7^2(y)dy \ll x^{\varepsilon}. \tag{3.18}$$

The first error term in the right hand side of (3.15) is clearly bounded by the term in the right hand side of (3.17). Hence from (3.15), (3.16), (3.17) and (3.18) we get

$$\begin{aligned} \int_x^{(1+\delta)x} K_2^2(y)dy &\ll x^{\frac{k-1}{2\alpha}+1+\varepsilon} M^{4(\sigma^*-1)+\frac{k-1}{\alpha}} \\ &\quad + \begin{cases} x^{1-1/2\alpha} & \text{if } k=2 \\ x^{1+\frac{k-3}{2\alpha}} M^{\frac{k-3}{2\alpha}} & \text{if } k \geqslant 3 \text{ and } M \ll x^{2\alpha-1}. \end{cases} \end{aligned} \tag{3.19}$$

3.3. Proof of Theorem 1

Choose M such that two error terms in (3.12) are of the same order, namely,

$$x^{\frac{k-2}{2\alpha}+1} M^{\frac{k-2}{2\alpha}+1-\frac{1}{a_k}} \asymp x^{\frac{k-1}{2\alpha}+1} M^{2(\sigma^*-1)+\frac{k-1}{2\alpha}}. \tag{3.20}$$

The above formula gives

$$M \asymp x^{\frac{1}{2\alpha(3-2\sigma^*-1/a_k)-1}}. \tag{3.21}$$

Clearly M satisfies $M \ll x^{2\alpha-1} \ll \sqrt{N}$. Therefore (3.12) becomes

$$\int_x^{(1+\delta)x} K_1^2(y)dy = \frac{{\kappa_0'}^2}{2} \sum_{n=1}^{\infty} \frac{b(n)^2}{n^{2-\frac{k-1}{2\alpha}}} \int_x^{(1+\delta)x} y^{\frac{k-1}{2\alpha}} dy + O\left(x^{1+\frac{k-1}{2\alpha}-\eta(\boldsymbol{a})+\varepsilon}\right), \tag{3.22}$$

where $\eta(\boldsymbol{a})$ is given by (1.12).

By Cauchy's inequality, formula (3.22) and bound (3.19) we have

$$\begin{aligned} \int_x^{(1+\delta)x} K_1(y)K_2(y)dy &\ll \left(\int_x^{(1+\delta)x} K_1^2(y)dy\right)^{1/2} \left(\int_x^{(1+\delta)x} K_2^2(y)dy\right)^{1/2} \\ &\ll x^{1+\frac{k-1}{2\alpha}+\varepsilon} M^{2(\sigma^*-1)+\frac{k-1}{2\alpha}} + \begin{cases} x & \text{if } k=2 \\ x^{1+\frac{k-2}{2\alpha}} M^{\frac{k-3}{4\alpha}} & \text{if } k \geqslant 3 \end{cases} \\ &\ll x^{1+\frac{k-1}{2\alpha}-\eta(\boldsymbol{a})+\varepsilon}, \end{aligned} \tag{3.23}$$

where in the last step we have used (3.20).

We also have

$$\int_x^{(1+\delta)x} K_2^2(y)dy \ll x^{1+\frac{k-1}{2\alpha}-\eta(\boldsymbol{a})+\varepsilon}. \tag{3.24}$$

Consider the first error term in (3.19) first. Since the exponent of M is negative, it is bounded by the term in the right hand side of (3.24). Next consider the second error term of (3.19). For $k = 2$ there is nothing to prove. For $k \geqslant 3$, it is enough to show that

$$\frac{1}{\alpha} - \frac{k-3}{2\alpha} \cdot \frac{1}{2\alpha(3 - 2\sigma^* - 1/a_k) - 1} > \eta(\boldsymbol{a}),$$

or equivalently $2 - 1/a_k > \sigma^*$. This is true under assumption (1.9).

From (3.22)-(3.24) we get immediately that

$$\int_x^{(1+\delta)x} \Delta^2(\mathbf{a}; y)dy = \frac{{\kappa_0'}^2}{2} \sum_{n=1}^{\infty} \frac{b(n)^2}{n^{2-\frac{k-1}{2\alpha}}} \int_x^{(1+\delta)x} y^{\frac{k-1}{2\alpha}} dy + O\left(x^{1+\frac{k-1}{2\alpha}-\eta(\boldsymbol{a})+\varepsilon}\right),$$

which implies Theorem 1 by a splitting argument. This completes the proof of Theorem 1.

4. Proof of Theorem 3

In order to prove Theorem 3 we need some preparations. Define $m(\sigma)$ (for $1/2 \leqslant \sigma < 1$) as the supremum of all numbers m such that

$$\int_1^T |\zeta(\sigma + it)|^m dt \ll T^{1+\varepsilon}.$$

It is known that $m(\sigma) \geqslant 4$ for $\sigma \geqslant 1/2$, $m(7/12) \geqslant 6$ and $m(5/8) \geqslant 8$. Ivić studied $m(\sigma)$ in great detail. Without loss of generality we can assume that $m(\sigma)$ is a continuous function of σ. One can find a lower bound of $m(\sigma)$ in [7, Theorem 8.4]. Especially we have the following simpler but a little weaker form:

$$m(\sigma) \geqslant \begin{cases} \frac{4}{3-4\sigma} & \text{if } \frac{1}{2} \leqslant \sigma \leqslant \frac{5}{8} \\ \\ \frac{3}{1-\sigma} & \text{if } \frac{5}{8} \leqslant \sigma < 1. \end{cases} \tag{4.1}$$

The following lemma is used essentially in Ivić's argument [8].

Lemma 6. *Let a_j $(1 \leqslant j \leqslant k)$ be positive integers such that $a_1 \leqslant \cdots \leqslant a_k$ and let $\psi(s)$ and σ^* be defined by* (1.6) *and* (1.7)*, respectively. Define the function $H(\sigma)$ by*

$$H(\sigma) = \sum_{j=1}^{k} \frac{1}{m(a_j\sigma - a_j + 1)}.$$

If

$$H(\sigma) \leqslant 1/2$$

for some σ, we have $\sigma^* \leqslant \sigma$.

Proof. We write $\sigma_j = a_j\sigma - a_j + 1$ for simplicity. Suppose that

$$\sum_{j=1}^{k} \frac{1}{m(\sigma_j)} \leqslant \frac{1}{2}.$$

Then by Hölder's inequality, we have

$$\begin{aligned}\int_1^T |\psi(s)|^2 dt &= \int_1^T \prod_{j=1}^{k} |\zeta(\sigma_j + ia_j t)|^2 dt \\ &\leqslant \prod_{j=1}^{k} \left(\int_1^T |\zeta(\sigma_j + ia_j t)|^{m(\sigma_j)} dt \right)^{\frac{2}{m(\sigma_j)}} \left(\int_1^T 1 dt \right)^{1-\sum_{j=1}^{k} \frac{2}{m(\sigma_j)}} \\ &\ll T^{1+\varepsilon}.\end{aligned}$$

Hence from the definition of σ^*, we have $\sigma^* \leqslant \sigma$. ∎

We remark that since $H(\sigma)$ is decreasing, if

$$H\left(1 - \frac{k-1}{4\alpha}\right) < \frac{1}{2},$$

then Theorem 1 holds.

Lemma 7. *Let $k = 3$, $a_1 \leqslant a_2 \leqslant a_3$ and $a_3 < a_1 + a_2$. Let σ^* be defined by* (1.7). *Then we have*

$$\sigma^* \begin{cases} \leqslant 1 - \frac{5}{4(a_1+a_2+a_3)} & \text{if } 3(a_2+a_3) \leqslant 7a_1, \\ \leqslant 1 - \frac{3}{a_1+3a_2+3a_3} & \text{if } 3(a_2+a_3) > 7a_1,\ 3a_3 + a_1 \leqslant 5a_2 \text{ and } 3a_3 < a_1 + 3a_2, \\ = 1 - \frac{1}{2a_3} & \text{otherwise.} \end{cases} \tag{4.2}$$

Proof. Let $a_1 \leqslant a_2 \leqslant a_3$ and $a_1 + a_2 > a_3$. By Lemma 6 we shall find σ such that

$$1 - \frac{1}{2a_3} \leqslant \sigma < 1 - \frac{1}{a_1 + a_2 + a_3}, \qquad H(\sigma) \leqslant 1/2.$$

For the sake of simplicity we put $\sigma_j = a_j\sigma - a_j + 1$ $(j = 1, 2, 3)$ for $\sigma \in [\frac{1}{2}, 1]$ as before. It is easy to see that $\frac{1}{2} \leqslant \sigma_3 \leqslant \sigma_2 \leqslant \sigma_1 < 1$.

We shall use the weak version (4.1).

Case 1: We first consider the case $3(a_2 + a_3) \leqslant 7a_1$ and we put

$$\sigma := 1 - \frac{5}{4(a_1 + a_2 + a_3)}.$$

Clearly $\sigma < 1 - 1/(a_1 + a_2 + a_3)$. Since $3a_3 \leqslant 7a_1 - 3a_2 \leqslant (2a_1 + 5a_2) - 3a_2 = 2(a_1 + a_2)$, we have $\sigma \geqslant 1 - \frac{1}{2a_3}$ and $\sigma_1 \leqslant \frac{5}{8}$. By (4.1) we have

$$H(\sigma) = \sum_{j=1}^{3} \frac{1}{m(\sigma_j)} \leqslant \frac{3 - 4\sigma_1}{4} + \frac{3 - 4\sigma_2}{4} + \frac{3 - 4\sigma_3}{4} = \frac{1}{2}.$$

Hence we get $\sigma^* \leqslant \sigma$.

Case 2: When $3(a_2 + a_3) > 7a_1$, $3a_3 + a_1 \leqslant 5a_2$ and $3a_3 < a_1 + 3a_2$, we put

$$\sigma := 1 - \frac{3}{a_1 + 3a_2 + 3a_3}.$$

It is clear that $\sigma < 1 - 1/(a_1 + a_2 + a_3)$ and $\sigma > 1 - \frac{1}{2a_3}$ by the last condition. One can check that the first two conditions imply that $\frac{5}{8} < \sigma_1 < 1$ and $\frac{1}{2} \leqslant \sigma_3 \leqslant \sigma_2 \leqslant \frac{5}{8}$. Hence

$$H(\sigma) = \sum_{j=1}^{3} \frac{1}{m(\sigma_j)} \leqslant \frac{1 - \sigma_1}{3} + \frac{3 - 4\sigma_2}{4} + \frac{3 - 4\sigma_3}{4} = \frac{1}{2}.$$

Hence we get $\sigma^* \leqslant \sigma$.

Case 3: We consider the case $3(a_2 + a_3) > 7a_1$, $3a_3 + a_1 \leqslant 5a_2$ and $3a_3 \geqslant a_1 + 3a_2$. In this case we put

$$\sigma := 1 - \frac{1}{2a_3}.$$

Note that this is the best possible choice. Using the last condition we easily check that

$$3a_3 \geqslant a_1 + 3a_2 \geqslant 4a_1$$

and hence

$$\sigma_1 = a_1 \left(1 - \frac{1}{2a_3}\right) - a_1 + 1 = 1 - \frac{a_1}{2a_3} \geqslant \frac{5}{8}.$$

Now we consider two cases.

(i) If $3a_3 \leqslant 4a_2$, then $\sigma_2 \leqslant \frac{5}{8}$. By the third condition we get

$$H(\sigma) = \sum_{j=1}^{3} \frac{1}{m(\sigma_j)} \leqslant \frac{1 - \sigma_1}{3} + \frac{3 - 4\sigma_2}{4} + \frac{1}{4} = \frac{a_1 + 3a_2}{6a_3} \leqslant \frac{1}{2}.$$

(ii) If $3a_3 > 4a_2$, then $\sigma_2 > \frac{5}{8}$. By the third condition we have $3a_3 \geqslant a_1 + 3a_2 \geqslant 2(a_1 + a_2)$. Hence

$$\begin{aligned} H(\sigma) = \sum_{j=1}^{3} \frac{1}{m(\sigma_j)} &\leqslant \frac{1 - \sigma_1}{3} + \frac{1 - \sigma_2}{3} + \frac{1}{4} \\ &= \frac{1}{4} + \frac{a_1 + a_2}{6a_3} \leqslant \frac{1}{4} + \frac{1}{6} \cdot \frac{3}{2} = \frac{1}{2}. \end{aligned}$$

Combining the two cases (i) and (ii), we have $\sigma^* = \sigma = 1 - 1/(2a_3)$.

Case 4: Finally we consider the case $3(a_2+a_3) > 7a_1$, $3a_3+a_1 > 5a_2$, where we put

$$\sigma := 1 - \frac{1}{2a_3}.$$

In this case, using the second condition, we easily check that

$$3a_3 > 5a_2 - a_1 \geqslant 4a_2$$

and hence

$$\sigma_2 = a_2\left(1-\frac{1}{2a_3}\right) - a_2 + 1 = 1 - \frac{a_2}{2a_3} > \frac{5}{8}.$$

We have $1 > \sigma_2 > \frac{5}{8}, 1 > \sigma_1 > \frac{5}{8}$, and $\sigma_3 = \frac{1}{2}$. Hence

$$H(\sigma) = \sum_{j=1}^{3} \frac{1}{m(\sigma_j)} \leqslant \frac{1-\sigma_1}{3} + \frac{1-\sigma_2}{3} + \frac{1}{4} \leqslant \frac{1}{8} + \frac{1}{8} + \frac{1}{4} = \frac{1}{2}.$$

Therefore we have $\sigma^* = \sigma = 1 - 1/(2a_3)$. ■

Proof of Theorem 3. Now the proof of Theorem 3 is immediate by substituting each value on the right hand side of (4.2) to (1.12). ■

Remark. From Lemma 7 we have

$$\sigma^*(3,4,5) = \frac{9}{10}, \qquad \sigma^*(2,3,4) = \frac{7}{8},$$

which are the best possible results . By Theorem 8.4 of Ivić[7] we also note the following slightly better results

$$\sigma^*(4,5,6) \leqslant \frac{214}{233}, \qquad \sigma^*(1,2,2) \leqslant \frac{41761}{54522} = 0.765948\ldots.$$

References

[1] X. Cao, Y. Tanigawa and W. Zhai, *On a conjecture of Chowla and Walum*, Science China Mathematics **53** (2010), 2755–2771.

[2] X. Cao, Y. Tanigawa and W. Zhai, *Tong-type identity and the mean square of the error term for an extended Selberg class*, to appear in Science China Mathematics, see arXiv:1501.04269.

[3] K. Corrádi and I. Kátai, *A comment of K. S. Ganggadharan's paper entitled "Two classical lattice point problems"*, Magyar Tud. Akad. Mat. Fiz.Oszt. Közl. **17** (1967), 89–97.

[4] H. Cramér, *Über zwei Sätze von Hern G. H. Hardy*, Math. Z. **15** (1922), 201–210.

[5] J.L. Hafner, *New omega theorems for two classical lattice point problems*, Invent. Math. **63** (1981), 181-186.

[6] M.N. Huxley, *Exponential sums and lattice points III*, Proc. London Math. Soc. **87** (2003), 591–609.
[7] A. Ivić, *The Riemann Zeta-Function*, John Wiley and Sons, 1985.
[8] A. Ivić, *The general divisor problem*, J. Number Theory **27** (1987), 73–91.
[9] A. Ivić, E. Krätzel, M. Kühleitner and W. G. Nowak, *Lattice points in large regions and related arithmetic functions: recent developments in a very classic topic*,(English summary) Elementare und analytische Zahlentheorie, 89–128, Schr.Wiss. Ges. Johann Wolfgang Goethe Univ.Frankfurt am Main, 20, Franz Steiner Verlag Stuttgart, Stuttgart, 2006.
[10] E. Krätzel, *Lattice Points*, Kluwer Academic Publishers, Dordrecht 1988.
[11] Y.-K. Lau and K.-M. Tsang, *On the mean square formula of the error term in the Dirichlet divisor problem*, Math. Proc. Camb. Phil. Soc. **146** (2009), 277–287.
[12] K.-C. Tong, *On divisor problem III*, Acta Math. Sinica **6** (1956), 515–541.
[13] W. Zhai and X. Cao, *On the mean square of the error term for the asymmeric two-dimensional divisor problem (I)*, Monatsh. Math. **159** (2010), 185–209.

Addresses: Xiaodong Cao: Department of Mathematics and Physics, Beijing Institute of Petro-Chemical Technology, Beijing, 102617, P.R. China;
Yoshio Tanigawa: Graduate School of Mathematics, Nagoya University, Nagoya, 464-8602, Japan;
Wenguang Zhai: Department of Mathematics, China University of Mining and Technology, Beijing 100083, P.R. China.

E-mail: caoxiaodong@bipt.edu.cn, tanigawa@math.nagoya-u.ac.jp, zhaiwg@hotmail.com

Received: 18 December 2014; **revised:** 11 September 2015

Functiones et Approximatio
54.2 (2016), 195–226
doi: 10.7169/facm/2016.54.2.5

THE AMPLIFICATION METHOD IN THE CONTEXT OF $GL(n)$ AUTOMORPHIC FORMS

Guillaume Ricotta

Abstract: In [SV] and [BMb], the authors proved the existence of a so-called higher rank amplifier and in [HRRa], the authors described an explicit version of a $GL(3)$ amplifier. This article provides, for $n \geqslant 4$, a totally explicit $GL(n)$ amplifier and gives all the results required to use it effectively.

Keywords: amplification method, Hecke operators, Hecke algebras.

1. Introduction and statement of the results

1.1. Motivation

The general philosophy of the amplification method

The amplification method was set up by W. Duke, J. Friedlander and H. Iwaniec (see [FI92], [Iwa92] and [DFI94] for example).

When bounding say a complex number z, which satisfies for obvious reasons depending on the context

$$|z| \leqslant M \tag{1.1}$$

for some positive real number M but, which is expected to satisfy

$$|z| \leqslant M^{1-\delta} \tag{1.2}$$

for some $0 < \delta < 1$, it is sometimes profitable to include z in a finite family[1] of complex numbers of the same nature, say

$$z = z_{j_0} \in \{z_j, j \in J\} \coloneqq \mathcal{Z}_J$$

2010 Mathematics Subject Classification: primary: 11F99, 20C08; secondary: 15A21

[1] Note that choosing a family containing z may be highly non-trivial. In particular, it should be large enough in order to be able to use the powerful tools of harmonic analysis but not too large such that bounding a moment of small order, like the second one, has a chance to be successful.

where J is a finite set of cardinality $\asymp M$, $j_0 \in J$ is the index of our favourite complex number z and to estimate all the quantities occuring in this family on average.

For instance, one can try to bound the second moment of this family given by

$$M_2(\mathcal{Z}_J) \coloneqq \sum_{j\in J} |z_j|^2.$$

By (1.1), the second moment satisfies

$$M_2(\mathcal{Z}_J) \leqslant |J| M^2,$$

which does not help us to prove (1.2) by positivity.

One can try to bound instead an amplified second moment given by

$$\mathcal{M}_2(\mathcal{Z}_J, \overrightarrow{\alpha}) \coloneqq \sum_{j\in J} |M_j(\overrightarrow{\alpha})|^2 |z_j|^2$$

where $M_j(\overrightarrow{\alpha})$ is a short Dirichlet polynomial given by

$$M_j(\overrightarrow{\alpha}) \coloneqq \sum_{i\in I} \alpha_i a_j(i)$$

for $j \in J$ and where I is a small finite set. Here, $\overrightarrow{\alpha} = (\alpha_i)_{i\in I}$ is a finite sequence of complex numbers, which will be specified later on, and $(a_j(i))_{i\in I}$ are some complex numbers naturally related to z_j for $j \in J$. In practice, the currently known techniques enable us to prove

$$\mathcal{M}_2(\mathcal{Z}_J, \overrightarrow{\alpha}) \leqslant M^{\varepsilon} \left(M^2 ||\overrightarrow{\alpha}||_2^2 + |I|^{\beta} ||\overrightarrow{\alpha}||_1 \right) \tag{1.3}$$

for some possibly large $\beta > 0$ and for all $\varepsilon > 0$, where as usual $||\overrightarrow{\alpha}||_1$ and $||\overrightarrow{\alpha}||_2$ stand for the L^1 and L^2 norms of $\overrightarrow{\alpha}$, respectively.

The whole point of the amplification method is to choose a sequence $\overrightarrow{\alpha}$, which amplifies the contribution of the complex number z in the amplified second moment $\mathcal{M}_2(\mathcal{Z}_J, \overrightarrow{\alpha})$. More explicitely, one has to construct a sequence $\overrightarrow{\alpha}$ satisfying[2]

$$||\overrightarrow{\alpha}||_2 \leqslant |I|^{\varepsilon}, \qquad |M_{j_0}(\overrightarrow{\alpha})|^2 \geqslant |I|^{\gamma}$$

for some possibly small $\gamma > 0$ and for all $\varepsilon > 0$. In general, cooking such sequence $\overrightarrow{\alpha}$ is based on the fact that some of the complex numbers $a_{j_0}(i)$, $i \in I$, cannot be small simultaneously. For such sequence, (1.3) entails by positivity

$$|z|^2 = |z_{j_0}|^2 \leqslant (M|I|)^{\varepsilon} \left(\frac{M^2}{|I|^{\gamma}} + |I|^{\beta+1/2-\gamma} \right) \tag{1.4}$$

for all $\varepsilon > 0$, which implies (1.2) by an optimal choice of $|I|$.

[2]Obviously one should also expect that $|M_j(\overrightarrow{\alpha})|^2$ is not too large when $j \neq j_0$ in J for the amplification method to be successful. This generally follows in concrete cases, at least conditionally, from a suitable version of the Riemann Hypothesis. Hopefully, one does not this in practice.

The very natural first step towards the proof of (1.3) is to open the square and to switch the order of summation, which leads us to bounding

$$\sum_{(i_1,i_2)\in I^2} \alpha_{i_1}\overline{\alpha_{i_2}} \sum_{j\in J} a_j(i_1)\overline{a_j(i_2)}|z_j|^2. \tag{1.5}$$

The diagonal term, namely the contribution from $i_1 = i_2$ in (1.5), is generally bounded by the first term in the right-hand side of (1.4), whereas the non-diagonal term, namely the contribution from $i_1 \neq i_2$ in (1.5), is generally bounded by the second term in the right-hand side of (1.4).

Getting these bounds heavily relies in practice on linearising the products $a_j(i_1)\overline{a_j(i_2)}$ for i_1 and i_2 in I, namely these products can be often written in relevant cases as a linear combination of the $a_j(i)$'s. Such linearisations in the context of $GL(n)$ automorphic forms are the core of this article.

In practice, the complex numbers $a_j(i)$ and $\overline{a_j(i)}$, $(i,j) \in I \times J$, are the eigenfunctions of some specific endomorphisms. Thus, linearising the products $a_j(i_1)\overline{a_j(i_2)}$ boils down to linearising the composition of the relevant endomorphisms.

The amplification method in $GL(n)$

Let p and q be two prime numbers.

In the context of $GL(n)$ automorphic forms defined in Section 2, our favourite complex number z is related to a $GL(n)$ Hecke-Maaß cusp form f, say $z = z(f)$. For instance, $z = f(g)$ for g in the generalised upper-half plane or $z = L(f,s)$, the value of the Godement-Jacquet L-function attached to f on the critical line $\mathrm{Re}\,(s) = 1/2$.

Hence z can be included, with a slight abuse of notations, in a finite subset of an orthonormal basis $(f_j)_{j\geqslant 1}$ of $GL(n)$ Hecke-Maaß cusp forms, namely those whose analytic conductors, the Laplace eigenvalue or the level or the imaginary part of s for instance, is bounded by some parameter $Q > 0$, which is devoted to tend to infinity, say

$$z(f) = z(f_{j_0}) \in \{z(f_j), j \geqslant 1, Q(f_j) \leqslant Q\}.$$

In [SV], the authors proved the existence of an abstract higher rank amplifier and in [BMb], the authors proved that there exists, at least asymptotically (p large), a non-trivial linear combination of $GL(n)$ Hecke operators equal to the identity operator (see [BMb, Lemma 4.2]). The whole point of this work is to give a totally explicit and ready to use version of a $GL(n)$ amplifier.

The choice of our amplifier $\overrightarrow{\alpha}$ relies on the fundamental identity

$$a_{j_0}(p, \underbrace{1,\dots,1}_{n-2 \text{ terms}})a_{j_0}(\underbrace{1,\dots,1}_{n-2 \text{ terms}}, p) = a_{j_0}(p, \underbrace{1,\dots,1}_{n-3 \text{ terms}}, p) + 1,$$

where $a_j(m_1,\dots,m_{n-1})$ stands for the $(m_1,\dots,m_{n-1})$'th Fourier coefficient of f_j (see (2.1) and [Gol06, Theorem 9.3.11, p. 271]). This identity essentially says that

$a_{j_0}(p,\underbrace{1,\dots,1}_{n-2\text{ terms}})a_{j_0}(\underbrace{1,\dots,1}_{n-2\text{ terms}},p)$ and $a_{j_0}(p,\underbrace{1,\dots,1}_{n-2\text{ terms}},p)$ cannot be simultaneously small . At the level of Hecke operators, this identity reflects the fact that

$$T_{\mathrm{diag}(1,\underbrace{p,\dots,p}_{n-1\text{ terms}})}\circ T_{\mathrm{diag}(\underbrace{1,\dots,1}_{n-1\text{ terms}},p)}=T_{\mathrm{diag}(1,\underbrace{p,\dots,p}_{n-2\text{ terms}},p^2)}+\frac{p^n-1}{p-1}\mathrm{Id}, \tag{1.6}$$

itself a consequence of the identity

$$\Lambda_n\mathrm{diag}\left(\underbrace{1,\dots,1}_{n-1\text{ terms}},p\right)\Lambda_n * \Lambda_n\mathrm{diag}\left(1,\underbrace{p,\dots,p}_{n-1\text{ terms}}\right)\Lambda_n$$
$$=\Lambda_n\mathrm{diag}\left(1,\underbrace{p,\dots,p}_{n-2\text{ terms}},p^2\right)\Lambda_n+\frac{p^n-1}{p-1}\Lambda_n\mathrm{diag}\left(\underbrace{p,\dots,p}_{n\text{ terms}}\right)\Lambda_n$$

at the level of Λ_n double cosets, where $\Lambda_n:=GL_n(\mathbb{Z})$ (see [AZ95, Lemma 2.18, p. 114]).

The coefficients $a_j(i)$'th will be some Hecke eigenvalues of f_j. More precisely, being inspired by [HRRa] and by (1.6), we set

$$a_j(p):=a_j(p,\underbrace{1,\dots,1}_{n-1\text{ terms}})=\text{the eigenvalue of } T_p=p^{-(n-1)/2}T_{\mathrm{diag}(\underbrace{1,\dots,1}_{n-1\text{ terms}},p)},$$
$$a_j\left(p^2\right):=\text{the eigenvalue of } p^{-(n-1)}T_{\mathrm{diag}(1,\underbrace{p,\dots,p}_{n-2\text{ terms}},p^2)}\in\mathbb{R}$$

when acting on f_j and we recall that

$$\overline{a_j(p)}=\text{the eigenvalue of } T_p^*=p^{-(n-1)/2}T_{\mathrm{diag}(1,\underbrace{p,\dots,p}_{n-1\text{ terms}})}$$

still when acting on f_j (see (2.4)). Thus, I is a subset of the prime numbers and of the squares of the prime numbers.

A very natural candidate for a $GL(n)$ amplifier is

$$M_j\left(\overrightarrow{\alpha}\right):=\sum_{i\in I}\alpha_i a_j(i)$$

where

$$\alpha_i:=\begin{cases}\overline{a_{j_0}(p)} & \text{if } i=p\leqslant\sqrt{L} \text{ is a prime number,}\\ -1 & \text{if } i=p^2\leqslant L \text{ is the square of a prime number}\\ 0 & \text{otherwise.}\end{cases}$$

This amplifier satisfies, as in the $GL(2)$ and $GL(3)$ case, $|M_{j_0}\left(\overrightarrow{\alpha}\right)|^2\ll_\varepsilon L^{1-\varepsilon}$ since $|I|\ll_\varepsilon L^{1-\varepsilon}$ for all $\varepsilon>0$.

Glancing at (1.5) and applying the inequality[3]

$$|M_{j_0}(\overrightarrow{\alpha})|^2 \leqslant 2\left|\sum_{p\leqslant\sqrt{L}}\alpha_p a_j(p)\right|^2 + 2\left|\sum_{p\leqslant\sqrt{L}}\alpha_{p^2}a_j(p^2)\right|^2,$$

it becomes crucial to linearise the products

$$T_{\mathrm{diag}(1,\underbrace{p,\dots,p}_{n-1\text{ terms}})}\circ T_{\mathrm{diag}(\underbrace{1,\dots,1}_{n-1\text{ terms}},q)} \text{ and } T_{\mathrm{diag}(1,\underbrace{p,\dots,p}_{n-2\text{ terms}},p^2)}\circ T_{\mathrm{diag}(1,\underbrace{q,\dots,q}_{n-2\text{ terms}},q^2)}$$

where p and q are two prime numbers. The results are given in the next section and reveal that the relevant Hecke operators when applying the amplification method in $GL(n)$ are

$$T_{\mathrm{diag}(1,\underbrace{p,\dots,p}_{n-2\text{ terms}},pq)},\qquad T_{\mathrm{diag}(1,\underbrace{pq,\dots,pq}_{n-2\text{ terms}},(pq)^2)},\qquad T_{\mathrm{diag}(1,\underbrace{p,\dots,p}_{n-2\text{ terms}},p^2)}$$

and

$$T_{\mathrm{diag}(1,\underbrace{p^2,\dots,p^2}_{n-3\text{ terms}},p^3,p^3)},\qquad T_{\mathrm{diag}(1,1,\underbrace{p,\dots,p}_{n-3\text{ terms}},p^3)},\qquad T_{\mathrm{diag}(1,1,\underbrace{p,\dots,p}_{n-4\text{ terms}},p^2,p^2)}.$$

1.2. Statement of the results

Theorem A. *Let $n\geqslant 4$, $\Lambda_n = GL_n(\mathbb{Z})$ and p be a prime number.*

1. *The finite set $R^{(n)}(p)$ of cardinality*

$$\deg\left(\mathrm{diag}\left(1,\underbrace{p,\dots,p}_{n-2\text{ terms}},p^2\right)\right) = p\frac{\left(p^{n-1}-1\right)\left(p^n-1\right)}{(p-1)^2}$$

defined in Proposition 3.1 is a complete system of representatives of the distinct Λ_n right cosets of

$$\Lambda_n\mathrm{diag}\left(1,\underbrace{p,\dots,p}_{n-2\text{ terms}},p^2\right)\Lambda_n$$

modulo Λ_n.

2. *The following formulas for the degrees[4] hold:*

$$\deg\left(\mathrm{diag}\left(p,\underbrace{p^2,\dots,p^2}_{n-2\text{ terms}},p^3\right)\right) = p\frac{\left(p^{n-1}-1\right)\left(p^n-1\right)}{(p-1)^2}, \tag{1.7}$$

[3]Such inequality, used for the first time in the amplification method in [BHM], enabled the authors to avoid mixing squares of prime numbers and prime numbers in their diophantine analysis.

[4]The degree of a matrix is defined in (1.16). See also Section 2 for more details.

$$\deg\left(\mathrm{diag}\left(1,\underbrace{p^2,\dots,p^2}_{n-3\text{ terms}},p^3,p^3\right)\right)=p^{n+1}\frac{\left(p^{n-2}-1\right)\left(p^{n-1}-1\right)\left(p^n-1\right)}{(p-1)^2(p^2-1)},\tag{1.8}$$

$$\deg\left(\mathrm{diag}\left(1,\underbrace{p^2,\dots,p^2}_{n-2\text{ terms}},p^4\right)\right)=p^{2n-1}\frac{\left(p^{n-1}-1\right)\left(p^n-1\right)}{(p-1)^2},\tag{1.9}$$

$$\deg\left(\mathrm{diag}\left(p,p,\underbrace{p^2,\dots,p^2}_{n-3\text{ terms}},p^4\right)\right)=p^{n+1}\frac{\left(p^{n-2}-1\right)\left(p^{n-1}-1\right)\left(p^n-1\right)}{(p-1)^2(p^2-1)},\tag{1.10}$$

and

$$\deg\left(\mathrm{diag}\left(p,p,\underbrace{p^2,\dots,p^2}_{n-4\text{ terms}},p^3,p^3\right)\right)=p^4\frac{\left(p^{n-3}-1\right)\left(p^{n-2}-1\right)\left(p^{n-1}-1\right)\left(p^n-1\right)}{(p-1)^2\left(p^2-1\right)^2}.\tag{1.11}$$

3. *Finally,*

$$\begin{aligned}
&\Lambda_n\mathrm{diag}\left(1,\underbrace{p,\dots,p}_{n-2\text{ terms}},p^2\right)\Lambda_n * \Lambda_n\mathrm{diag}\left(1,\underbrace{p,\dots,p}_{n-2\text{ terms}},p^2\right)\Lambda_n\\
&\quad=\frac{2p^n-p^2-2p+1}{p-1}\Lambda_n\mathrm{diag}\left(p,\underbrace{p^2,\dots,p^2}_{n-2\text{ terms}},p^3\right)\Lambda_n\\
&\qquad+p\frac{\left(p^{n-1}-1\right)\left(p^n-1\right)}{(p-1)^2}\Lambda_n\mathrm{diag}\left(\underbrace{p^2,\dots,p^2}_{n\text{ terms}}\right)\Lambda_n\\
&\qquad+\Lambda_n\mathrm{diag}\left(1,\underbrace{p^2,\dots,p^2}_{n-2\text{ terms}},p^4\right)\Lambda_n\\
&\qquad+(p+1)\Lambda_n\mathrm{diag}\left(1,\underbrace{p^2,\dots,p^2}_{n-3\text{ terms}},p^3,p^3\right)\Lambda_n\\
&\qquad+(p+1)\Lambda_n\mathrm{diag}\left(p,p,\underbrace{p^2,\dots,p^2}_{n-3\text{ terms}},p^4\right)\Lambda_n\\
&\qquad+(p+1)^2\Lambda_n\mathrm{diag}\left(p,p,\underbrace{p^2,\dots,p^2}_{n-4\text{ terms}},p^3,p^3\right)\Lambda_n.
\end{aligned}\tag{1.12}$$

Corollary B. *Let $n \geqslant 4$. If p and q are two prime numbers then*

$$T_{\mathrm{diag}(1,\underbrace{p,\dots,p}_{n-1 \text{ terms}})} \circ T_{\mathrm{diag}(\underbrace{1,\dots,1}_{n-1 \text{ terms}},q)} = T_{\mathrm{diag}(1,\underbrace{p,\dots,p}_{n-2 \text{ terms}},pq)} + \delta_{p=q}\frac{p^n-1}{p-1}\mathrm{Id} \tag{1.13}$$

and

$$\begin{aligned} T_{\mathrm{diag}(1,\underbrace{p,\dots,p}_{n-2 \text{ terms}},p^2)} &\circ T_{\mathrm{diag}(1,\underbrace{q,\dots,q}_{n-2 \text{ terms}},q^2)} \qquad (1.14)\\ &= T_{\mathrm{diag}(1,\underbrace{pq,\dots,pq}_{n-2 \text{ terms}},(pq)^2)} + \delta_{p=q}\frac{2p^n-p^2-2p+1}{p-1}T_{\mathrm{diag}(1,\underbrace{p,\dots,p}_{n-2 \text{ terms}},p^2)}\\ &\quad + \delta_{p=q}p\frac{\left(p^{n-1}-1\right)(p^n-1)}{(p-1)^2}\mathrm{Id} + \delta_{p=q}(p+1)T_{\mathrm{diag}(1,\underbrace{p^2,\dots,p^2}_{n-3 \text{ terms}},p^3,p^3)}\\ &\quad + \delta_{p=q}(p+1)T_{\mathrm{diag}(1,1,\underbrace{p,\dots,p}_{n-3 \text{ terms}},p^3)} + \delta_{p=q}(p+1)^2T_{\mathrm{diag}(1,1,\underbrace{p,\dots,p}_{n-4 \text{ terms}},p^2,p^2)}. \end{aligned}$$

When $p \neq q$, the previous corollary follows from (2.13) whereas when $p = q$, it comes from Theorem A, [AZ95, Lemma 2.18, p. 114] and (2.9). This corollary generalizes the case $n = 2$, well-known for a long time, and the case $n = 3$ done in [HRRa].

1.3. On the possible applications of this higher rank amplifier

Subconvexity bounds for *L*-functions

Let f be a $GL(n)$ Hecke Maaß cusp form. A very classical problem considered by analytic number theorists is the size of the Godement-Jacquet L-function associated to f, say $L(f,s)$ with s on the critical line $\mathrm{Re}\,(s) = 1/2$ when the analytic conductor $C(f)$ of f tends to infinity. The bound

$$L(f,s) \ll C(f)^{1/4+\varepsilon},$$

for any $\varepsilon > 0$ is named the convexity or trivial bound, even if this is not a trivial result in general. Improving this bound, namely proving a subconvexity bound, was proved in the past to be useful to solve many arithmetical questions, such as equidistribution results.

The $GL(2)$ case was intensively investigated in the last decades, culminating in the work of P. Michel and A. Venkatesh in [MV10], who used the amplification method in $GL(2)$. It seems that the best subconvexity bounds in the $GL(2)$ case intrinsic to the amplification method are the Weyl exponent $1/4(1-1/3)$ ([Wey21]) and the Burgess exponent $1/4(1-1/4)$ ([Bur62]).

Very few examples of subconvexity bounds for L-functions of $GL(n)$ automorphic forms, which are not lifts of $GL(2)$ ones, are known. One can quote [Li11], [Blo12], [Muna], [BB] in the rank 2 case, and an extremely recent and elaborate subconvexity bound for twisted L-functions of $GL(3)$ automorphic forms by R. Munshi in [Munb]. As far as we know, the Weyl and Burgess exponents have never appeared in this higher rank case.

We hope that the completely explicit $GL(n)$ amplifier built in this paper will sheld some new lights on these questions in the close future.

Subconvexity bounds for sup-norms of automorphic forms

Let f be a L^2-normalized $GL(n)$ Hecke-Maaß cusp form.

The spectral aspect. Let K be a fixed compact subset of $SL_n(\mathbb{R})/SO_n(\mathbb{R})$. The convexity bound for the sup-norm of f restricted to K is given by

$$||f|_K||_\infty \ll \lambda_f^{n(n-1)/8}$$

where λ_f is the Laplace eigenvalue of f. More details can be found in [Sar]. It is important to mention that F. Brumley and N. Templier discovered in [BT] that this convexity bound does not hold when $n \geqslant 6$ if f is not restricted to a compact.

The convexity bound is not expected to be sharp, essentially because there are some additional symmetries on $SL_n(\mathbb{R})/SO_n(\mathbb{R})$: the Hecke correspondences. More precisely, one should be able to prove a subconvexity bound, namely finding an absolute positive constant $\delta_n > 0$ such that

$$||f|_K||_\infty \ll \lambda_f^{n(n-1)/8-\delta_n} \tag{1.15}$$

The pioneering work done by H. Iwaniec and P. Sarnak in [IS95] is the bound given in (1.15) when $n = 2$ for $\delta_2 = 1/24$. This constant δ_2 seems to be intrinsic to the amplification method in $GL(2)$. The case $n = 3$ was completed in [HRRb]. The general case was done in a series of impressive works by V. Blomer and P. Maga in [BMb] and in [BMa]. One could also quote [Marb].

All these achievements were done thanks to the amplification method. Determining what should be the best subconvexity exponent intrinsic to the amplification method is an interesting question, which should reveal new types of analytic problems. Needless to say that the explicit $GL(n)$ amplifier could be useful to do so.

The level aspect. Let us say that f is of level q and let us speak about the growth of the sup-norm of f as q gets large.

For $GL(2)$ and when the level q is squarefree, the convexity bound is

$$||f||_\infty \ll q^\varepsilon$$

for all $\varepsilon > 0$ but one expects that the correct order of magnitude is

$$||f||_\infty \ll q^{-1/2+\varepsilon}$$

This rank 1 case in prime level was intensively studied during the last years after the foundational work of V. Blomer and R. Holowinsky in [BH10], particularly in [Tem10], [HT12] and [HR]. In [HT13], the authors proved the bound

$$||f||_\infty \ll q^{-1/6+\varepsilon}$$

which seems to be the best possible subconvexity exponent intrinsic to the amplification method. Note that the authors really used the **shape** of the explicit $GL(2)$ amplifier in order to get this bound. When the level q is not squarefree, the situation is more delicate since the Atkin-Lehner group has more than one orbit when acting on the cusps. See [Sah] and [Mara] for more details.

For $GL(n)$, as far as we know, these questions remain completely open. We hope that the explicit $GL(n)$ amplifier constructed in this work will make possible an investigation of these questions in a higher rank setting.

1.4. Organization of the paper

The general background on $GL(n)$ Maaß cusp forms and on the $GL(n)$ Hecke algebra is given in Section 2. The proof of part (1) in Theorem A is done in Section 3 (see Proposition 3.1). The proofs of parts (2) and (3) in Theorem A are detailed in Section 4.

Notations. $n \geqslant 2$ is an integer and p, q are prime numbers. Λ_n stands for the group $GL_n(\mathbb{Z})$ of $n \times n$ invertible matrices with integer entries, whose unity element is the identity matrix I_n. For g a $n \times n$ matrix with rational coefficients, the degree of g is defined by

$$\deg(g) = \operatorname{card}\left(\Lambda_n \setminus \Lambda_n g \Lambda_n\right). \tag{1.16}$$

If $a_1, \ldots, a_n$ are real numbers then $\operatorname{diag}(a_1, \ldots, a_n)$ denotes the $n \times n$ diagonal matrix with $a_1, \ldots, a_n$ as diagonal entries. The following double Λ_n cosets will occur throughout this article:

$$\pi_i^{(n)}(p) \coloneqq \Lambda_n D_i^{(n)}(p) \Lambda_n, \qquad D_i^{(n)}(p) = \operatorname{diag}\left(1, \ldots, 1, \underbrace{p, \ldots, p}_{i \text{terms}}\right),$$

$$\pi^{(n)}(p) \coloneqq \Lambda_n D^{(n)}(p) \Lambda_n, \qquad D^{(n)}(p) = \operatorname{diag}\left(1, \underbrace{p, \ldots, p}_{n-2 \text{ terms}}, p^2\right),$$

$$\pi_{i,j}^{(n)}(p) \coloneqq \Lambda_n D_{i,j}^{(n)}(p) \Lambda_n, \qquad D_{i,j}^{(n)}(p) = \operatorname{diag}\left(1, \ldots, 1, \underbrace{p, \ldots, p}_{i \text{terms}}, \underbrace{p^2, \ldots, p^2}_{j \text{ terms}}\right)$$

for $0 \leqslant i, j \leqslant n$ with $i + j \leqslant n$. The following polynomials in x will occur when computing the degrees of some relevant Λ_n double cosets for this work:

$$\varphi_r(x) \coloneqq \prod_{k=1}^{r} \left(x^k - 1\right), \qquad \varphi_0(x) = 1$$

for $r \geqslant 1$. Let us define the n-tuple

$$\boldsymbol{d}_n(p) \coloneqq \left(1, p, p^2, \dots, \underbrace{p^{k-1}}_{k\text{'th term}}, \dots, p^{n-2}, p^n\right).$$

Finally, if $\mathcal{P}$ is a property then $\delta_{\mathcal{P}}$ is the Kronecker symbol, namely 1 if $\mathcal{P}$ is satisfied and 0 otherwise.

Acknowledgements. The author heartily thanks the anonymous referee for her or his long list of constructive suggestions, which greatly improved both the presentation and the arguments in some proofs.

He would like to thank R. Holowinsky and E. Royer for fruitful discussions related to this work.

The author's research was partially supported by a Marie Curie Intra European Fellowship within the 7th European Community Framework Programme. The grant agreement number of this project, whose acronym is ANERAUTOHI, is PIEF-GA-2009-251271. He would like to thank E. Kowalski, ETH and its entire staff for the excellent working conditions.

Last but not least, he would like to express his gratitude to K. Belabas for his crucial but isolated support for Analytic Number Theory among the Number Theory research team A2X (Institut de Mathématiques de Bordeaux, Université de Bordeaux).

2. Background on the $GL(n)$ Hecke algebra

In this section, $n \geqslant 2$. The convenient references for this section are [AZ95], [Gol06], [Kri90], [New72] and [Shi94].

Let f be a $GL(n)$ Maaß cusp form of level 1. Such f admits a Fourier expansion

$$f(g) = \sum_{\gamma \in U_{n-1}(\mathbb{Z}) \backslash SL_{n-1}(\mathbb{Z})} \sum_{\substack{m_1, \dots, m_{n-2} \geqslant 1 \\ m_{n-1} \in \mathbb{Z}^*}} \frac{a_f(m_1, \dots, m_{n-1})}{\prod_{1 \leqslant k \leqslant n-1} |m_k|^{k(n-k)/2}} \tag{2.1}$$

$$\times W_{\mathrm{Ja}}\left(\mathrm{diag}(m_1 \dots m_{n-2}|m_{n-1}|, \dots, m_1 m_2, m_1, 1) \begin{pmatrix} \gamma & \\ & 1 \end{pmatrix} g, \nu_f, \psi_{\underbrace{1, \dots, 1}_{n-2 \text{ terms}}, \frac{m_{n-1}}{|m_{n-1}|}}\right)$$

for $g \in GL_n(\mathbb{R})$ (see [Gol06, Equation (9.1.2)]. Here $U_{n-1}(\mathbb{Z})$ stands for the $\mathbb{Z}$-points of the group of $(n-1) \times (n-1)$ upper-triangular unipotent matrices. $\nu_f \in \mathbb{C}^{n-1}$ is the type of f, whose components are complex numbers characterized by the property that, for every invariant differential operator D in the center of the universal enveloping algebra of $GL_n(\mathbb{R})$, the cusp form f is an eigenfunction of D with the same eigenvalue as the power function I_{ν_f}, which is defined in [Gol06, Equation (5.1.1)]. $\psi_{\underbrace{1, \dots, 1}_{n-2 \text{ terms}}, \pm 1}$ is the character of the group of $n \times n$

upper-triangular unipotent real matrices defined by

$$\psi_{\underbrace{1,\dots,1}_{n-2 \text{ terms}},\pm 1}(u) = e^{2i\pi(u_{1,2}+\cdots+u_{n-2,n-1}\pm u_{n-1,n})}.$$

for $u = [u_{i,j}]_{1\leqslant i,j\leqslant n}$. $W_{Ja}\left(*, \nu_f, \psi_{\underbrace{1,\dots,1}_{n-2 \text{ terms}},\pm 1}\right)$ stands for the $GL(n)$ Jacquet Whittaker function of type ν_f and character $\psi_{\underbrace{1,\dots,1}_{n-2 \text{ terms}},\pm 1}$ defined in [Gol06, Equation 6.1.2]. The complex number $a_f(m_1,\dots,m_{n-1})$ is the $(m_1,\dots,m_{n-1})$'th *Fourier coefficient* of f for $m_1,\dots,m_{n-2}$ some positive integers and m_{n-1} a non-vanishing integer.

For $g \in GL_n(\mathbb{Q})$, one knows (see [AZ95, Lemma 1.2, p. 94 and Lemma 2.1, p. 105]) that the Λ_n double coset $\Lambda_n g \Lambda_n$ is a finite union of Λ_n right cosets such that it makes sense to define the *Hecke operator* T_g by

$$T_g(f)(h) = \sum_{\delta \in \Lambda_n \backslash \Lambda_n g \Lambda_n} f(\delta h)$$

for $h \in GL_n(\mathbb{R})$ (see [AZ95, Chapter 3, Sections 1.1 and 1.5]. The *degree* of g or T_g is defined by

$$\deg(g) = \deg(T_g) = \operatorname{card}\left(\Lambda_n \setminus \Lambda_n g \Lambda_n\right).$$

Obviously,

$$\deg(rg) = \deg(g). \tag{2.2}$$

for $r \in \mathbb{Q}^\times$. By [AZ95, Lemma 2.18 Equation (2.32), p. 114],

$$\deg\left(D^{(n)}_{i,j}(p)\right) = p^{j(n-i-j)} \frac{\varphi_n(p)}{\varphi_{n-i-j}(p)\varphi_i(p)\varphi_j(p)} \tag{2.3}$$

for $0 \leqslant i, j \leqslant n$ with $i + j \leqslant n$.

Remark 2.1. The equations (2.2) and (2.3) prove (1.7) and (1.11) in Theorem A.

The adjoint of T_g for the Peterson inner product is $T_{g^{-1}}$. The algebra of Hecke operators $\mathbb{T}$ is the ring of endomorphisms generated by all the T_g's with $g \in GL_n(\mathbb{Q})$, a commutative algebra of normal endomorphisms (see [Gol06, Theorem 9.3.6]), which contains the m'th normalised Hecke operator

$$T_m = \frac{1}{m^{(n-1)/2}} \sum_{\substack{g=\operatorname{diag}(y_1,\dots,y_n)\\ y_1|y_2|\cdots|y_n\\ y_1y_2\dots y_n=m}} T_g$$

for all positive integer m. A *Hecke-Maaß cusp form* f of level 1 is a Maaß cusp form of level 1, which is an eigenfunction of $\mathbb{T}$. In particular, it satisfies

$$T_m(f) = a_f(m, \underbrace{1,\dots,1}_{n-2 \text{ terms}})f \text{ and } T^*_m(f) = a_f(\underbrace{1,\dots,1}_{n-2 \text{ terms}}, m)f \tag{2.4}$$

according to [Gol06, Theorem 9.3.11].

The algebra $\mathbb{T}$ is isomorphic to the *absolute Hecke algebra*, the free $\mathbb{Z}$-module generated by the double cosets $\Lambda_n g \Lambda_n$ where g ranges over $\Lambda_n \setminus GL_n(\mathbb{Q})/\Lambda_n$ and endowed with the following multiplication law. If g_1 and g_2 belong to $GL_n(\mathbb{Q})$ and

$$\Lambda_n g_1 \Lambda_n = \bigcup_{i=1}^{\deg(g_1)} \Lambda_n \alpha_i \text{ and } \Lambda_n g_2 \Lambda_n = \bigcup_{j=1}^{\deg(g_2)} \Lambda_n \beta_j$$

then

$$\Lambda_n g_1 \Lambda_n * \Lambda_n g_2 \Lambda_n = \sum_{\Lambda_n h \Lambda_n \subset \Lambda_n g_1 \Lambda_n g_2 \Lambda_n} m(g_1, g_2; h) \Lambda_n h \Lambda_n \tag{2.5}$$

where $h \in GL_n(\mathbb{Q})$ ranges over a system of representatives of the Λ_n-double cosets contained in the set $\Lambda_n g_1 \Lambda_n g_2 \Lambda_n$ and

$$\begin{aligned} & m(g_1, g_2; h) \\ & \quad = \operatorname{card}\left(\{(i,j) \in \{1, \dots, \deg(g_1)\} \times \{1, \dots, \deg(g_2)\}, \alpha_i \beta_j \in \Lambda_n h\}\right), \qquad (2.6) \\ & \quad = \frac{1}{\deg(h)} \operatorname{card}\left(\{(i,j) \in \{1, \dots, \deg(g_1)\} \times \{1, \dots, \deg(g_2)\}, \alpha_i \beta_j \in \Lambda_n h \Lambda_n\}\right), \qquad (2.7) \\ & \quad = \frac{\deg(g_2)}{\deg(h)} \operatorname{card}\left(\{i \in \{1, \dots, \deg(g_1)\}, \alpha_i g_2 \in \Lambda_n h \Lambda_n\}\right) \qquad (2.8) \end{aligned}$$

by [AZ95, Lemma 1.5, p. 96]. In particular,

$$\Lambda_n r I_n \Lambda_n * \Lambda_n g \Lambda_n = \Lambda_n r g \Lambda_n \tag{2.9}$$

for $g \in GL_n(\mathbb{Q})$ and $r \in \mathbb{Q}^\times$ ([AZ95, Lemma 2.4, p. 107]).

For $g \in GL_n(\mathbb{Q})$ with integer entries, the Λ_n right coset $\Lambda_n g$ contains a unique upper-triangular column reduced matrix, namely

$$\Lambda_n g = \Lambda_n C \tag{2.10}$$

where $C = [c_{i,j}]_{1 \leqslant i,j \leqslant n}$ is an upper-triangular matrix with integer entries satisfying

$$\forall j \in \{2, \dots, n\}, \forall i \in \{1, j-1\}, \quad 0 \leqslant c_{i,j} < c_{j,j}$$

by [AZ95, Lemma 2.7].

Let g be a $n \times n$ matrix with integer entries. Let $1 \leqslant k \leqslant n$. Let $I_{n,k}$ be the set of all k-tuples $\{i_1, \dots, i_n\}$ satisfying $1 \leqslant i_1 < i_2 < \cdots < i_k \leqslant n$. Obviously, $I_{n,k}$ is of cardinal $\binom{n}{k}$. If ω and τ are two elements of $I_{n,k}$ then $g(\omega, \tau)$ will denote the $k \times k$ determinantal minor of g whose row indices are the elements of ω and whose column indices are the elements of τ. Obviously, there are $\binom{n}{k}^2$ such minors. The k'th *determinantal divisor* of g, say $d_k(g)$, is the non-negative integer defined by

$$d_k(g) = \begin{cases} 0 & \text{if } \forall (\omega, \tau) \in I_{n,k}^2, g(\omega, \tau) = 0, \\ gcd_{(\omega,\tau) \in I_{n,k}^2} g(\omega, \tau) & \text{otherwise} \end{cases} \tag{2.11}$$

and the *determinantal vector* of g is $\boldsymbol{d}_n(g) = (d_1(g), \ldots, d_n(g))$. The determinantal divisors turn out to be useful since if h is another $n \times n$ matrix with integer entries then

$$h \in \Lambda_n g \Lambda_n \qquad \text{if and only if} \qquad \boldsymbol{d}(h) = \boldsymbol{d}(g) \tag{2.12}$$

according to [New72].

By [AZ95, Proposition 2.5, p. 107], if g_1, g_2 belong to $GL_n(\mathbb{Q})$ with integer entries then

$$\Lambda_n g_1 \Lambda_n * \Lambda_n g_2 \Lambda_n = \Lambda_n g_1 g_2 \Lambda_n \tag{2.13}$$

provided $d_1(g_1) = d_1(g_2) = 1$ and $(d_n(g_1), d_n(g_2)) = 1$.

Finally, we will use the following result on the local integral Hecke algebra at the prime p, say $\underline{\underline{H}}_p^n$, defined as the Λ_n double cosets $\Lambda_n g \Lambda_n$, where g ranges over the matrices in $GL_n(\mathbb{Z}[1/p])$ with integer entries. By [AZ95, Lemma 2.16, p. 112], the $\mathbb{Q}$-linear map $\Psi : \underline{\underline{H}}_p^n \to \underline{\underline{H}}_p^{n-1}$ defined by

$$\begin{aligned} &\Psi\left(\Lambda_n \mathrm{diag}\left(p^{\delta_1}, \ldots, p^{\delta_n}\right) \Lambda_n\right) \\ &\qquad = \begin{cases} \Lambda_n \mathrm{diag}\left(p^{\delta_2}, \ldots, p^{\delta_n}\right) \Lambda_n & \text{if } 0 = \delta_1 \leqslant \delta_2 \leqslant \ldots \leqslant \delta_n, \\ 0 & \text{otherwise} \end{cases} \end{aligned} \tag{2.14}$$

is a morphism of rings.

3. Decomposition of $\pi^{(n)}(p)$ into Λ_n right cosets

In this section, $n \geqslant 2$. The main purpose of this section is to prove part (1) in Therorem A, namely to find a convenient complete system of representatives for the distinct Λ_n right cosets of $\pi^{(n)}(p)$ modulo Λ_n. Let us denote by $R_0^{(n)}(p)$ the set of $n \times n$ upper-triangular matrices $C = [c_{i,j}]_{1 \leqslant i,j \leqslant n}$ with integer entries satisfying

$$\boldsymbol{d}_n(C) = \boldsymbol{d}_n(p), \tag{3.1}$$

$$\forall i \in \{1, \ldots, n\}, \qquad c_{i,i} = p, \tag{3.2}$$

and

$$\forall j \in \{2, \ldots, n\}, \forall i \in \{1, \ldots, j-1\}, \qquad 0 \leqslant c_{i,j} < p. \tag{3.3}$$

Let us also denote by $R_1^{(n)}(p)$ the set of $n \times n$ upper-triangular matrices $C = [c_{i,j}]_{1 \leqslant i,j \leqslant n}$ with integer entries satisfying

$$\forall i \in \{1, \ldots, n\}, \quad c_{i,i} \in \left\{1, p, p^2\right\}, \tag{3.4}$$

$$\exists! i \in \{1, \ldots, n\}, \quad c_{i,i} = 1 \qquad \text{and} \qquad \exists! i \in \{1, \ldots, n\}, \quad c_{i,i} = p^2, \tag{3.5}$$

$$\forall j \in \{2, \ldots, n\}, \forall i \in \{1, \ldots, j-1\}, \qquad 0 \leqslant c_{i,j} < c_{j,j} \tag{3.6}$$

and

$$\forall i \in \{1, \ldots, n-1\}, \ p \mid c_{i,i} \Rightarrow \forall j \in \{i+1, \ldots, n\}, \ p \mid c_{i,j}. \tag{3.7}$$

Proposition 3.1. *Let $n \geqslant 2$. The set $R^{(n)}(p) = R_0^{(n)}(p) \sqcup R_1^{(n)}(p)$ is a complete system of representatives of the distinct Λ_n right cosets of $\pi^{(n)}(p)$ modulo Λ_n. In other words,*

$$\pi^{(n)}(p) = \left(\bigsqcup_{C_0 \in R_0^{(n)}(p)} \Lambda_n C_0 \right) \bigsqcup \left(\bigsqcup_{C_1 \in R_1^{(n)}(p)} \Lambda_n C_1 \right).$$

In addition,

$$\begin{aligned} card\left(R_0^{(n)}(p)\right) &= \frac{(n-1)p^n - np^{n-1} + 1}{p-1}, \\ card\left(R_1^{(n)}(p)\right) &= \frac{p^{2n} - np^{n+1} + 2(n-1)p^n - np^{n-1} + 1}{(p-1)^2}. \end{aligned}$$

Remark 3.2. Proposition 3.1 proves part (1) in Theorem A.

Proof of Proposition 3.1. By (3.7), all the matrices C_1 in $R_1^{(n)}(p)$ can be decomposed as

$$C_1 = \mathrm{diag}\left(p^{\alpha_1}, \dots, p^{\alpha_n}\right) C_1'$$

for some non negative integers $\alpha_1, \dots, \alpha_n$ and with $C_1' \in \Lambda_n$, hence

$$C_1 \in \Lambda \mathrm{diag}\left(p^{\alpha_1}, \dots, p^{\alpha_n}\right) \Lambda = \pi^{(n)}(p)$$

by (3.4) and (3.5).

All the matrices C_0 in $R_0^{(n)}(p)$ belong to $\pi^{(n)}(p)$ since their determinantal vectors match the determinantal vector of $D^{(n)}(p)$ by (3.1).

All the matrices in $R^{(n)}(p)$ are upper-triangular column reduced matrices by (3.3), (3.6) and belong to different Λ_n right cosets according to the unicity statement given in (2.10).

Let $C = [c_{i,j}]_{1 \leqslant i,j \leqslant n}$ be any upper-triangular column reduced matrix that lies in $\pi^{(n)}(p)$ and let us prove that C belongs to $R^{(n)}(p)$. First of all, the determinant of C is p^n, hence

$$\forall i \in \{1, \dots, n\}, \exists \alpha_i \in \mathbb{N}, \quad c_{i,i} = p^{\alpha_i}.$$

Then, $C = \lambda_1 D^{(n)}(p) \lambda_2$ with λ_1, λ_2 in Λ_n, which entails that $C^{-1} = \lambda_2^{-1} D^{(n)}(p)^{-1} \lambda_1^{-1}$. As a consequence, $p^2 C^{-1}$ has integer entries and

$$\forall i \in \{1, \dots, n\}, \qquad \alpha_i \in \{0, 1, 2\}.$$

If all the diagonal entries of C are equal to p then C belongs to $R_0^{(n)}(p)$ since its determinantal vector must be equal to the determinantal vector of $D^{(n)}(p)$, namely $\boldsymbol{d}_n(p)$. Assume that one of its diagonal coefficient is not equal to p. The condition $d_2(C) = p$ implies that there must be at most one diagonal coefficient of C equal

to 1. Let us prove that C has a single diagonal coefficient equal to 1 and a single coefficient equal to p^2. Let σ be the permutation of $\{1,\dots,n\}$ satisfying

$$0 \leqslant \alpha_{\sigma(1)} \leqslant \dots \leqslant \alpha_{\sigma(n)} \leqslant 2.$$

The determinant condition is

$$\alpha_{\sigma(1)} + \dots + \alpha_{\sigma(n)} = n.$$

If $\alpha_{\sigma(1)} = 0$ then one easily gets $\alpha_{\sigma(2)} = \dots = \alpha_{\sigma(n-1)} = 1$ and $\alpha_{\sigma(n)} = 2$. If $\alpha_{\sigma(1)} \geqslant 1$ then all the diagonal entries of C are equal to p, which is a contradiction. Thus, (3.5) is satisfied. Let us prove (3.7). Assume on the contrary that there exist i_0 in $\{1,\dots,n-1\}$ and j_0 in $\{i_0+1,\dots,n\}$ such that $p \mid c_{i_0,i_0}$ and $p \nmid c_{i_0,j_0}$. The fact that $p \nmid c_{i_0,j_0}$ implies that $c_{j_0,j_0} \neq 1$. Let $j_1 \neq j_0$ be the index of the column of C, for which $c_{j_1,j_1} = 1$. Let us prove that the columns $C[j_1]$ of C of index j_1 and $C[j_0]$ of C of index j_0 are linearly independent modulo p. If

$$0 = \lambda_0 C[j_0] + \lambda_1 C[j_1] \pmod p$$

then the i_0'th component implies that

$$0 = \lambda_0 c_{i_0,j_0} + \lambda_1 c_{i_0,j_1} = \lambda_0 c_{i_0,j_0} \pmod p$$

such that $\lambda_0 = 0 \pmod p$ since c_{i_0,j_0} is invertible modulo p and $\lambda_1 = 0 \pmod p$. This is a contradiction since C is of rank 1 modulo p. Thus, C belongs to $R_1^{(n)}(p)$.

Let us compute the cardinality of $R_1^{(n)}(p)$. Obviously,

$$\begin{aligned}\operatorname{card}\left(R_1^{(n)}(p)\right) &= p^{n-1} \sum_{1\leqslant\alpha_1\neq\alpha_2\leqslant n} p^{\alpha_2-\alpha_1} \\ &= \left(\sum_{0\leqslant\alpha\leqslant n-1} p^{\alpha}\right)^2 - np^{n-1} \\ &= \frac{p^{2n} - np^{n+1} + 2(n-1)p^n - np^{n-1} + 1}{(p-1)^2}.\end{aligned}$$

Let us compute the cardinality of $R_0^{(n)}(p)$. Obviously,

$$\begin{aligned}\operatorname{card}\left(R_0^{(n)}(p)\right) &= \operatorname{card}\left(R^{(n)}(p)\right) - \operatorname{card}\left(R_1^{(n)}(p)\right) \\ &= \deg\left(D^{(n)}(p)\right) - \operatorname{card}\left(R_1^{(n)}(p)\right) \\ &= p\frac{\varphi_n(p)}{\varphi_1(p)^2\varphi_{n-2}(p)} - \frac{p^{2n} - np^{n+1} + 2(n-1)p^n - np^{n-1} + 1}{(p-1)^2} \\ &= p\frac{\left(p^{n-1}-1\right)\left(p^n-1\right)}{(p-1)^2} - \frac{p^{2n} - np^{n+1} + 2(n-1)p^n - np^{n-1} + 1}{(p-1)^2}\end{aligned}$$

by (2.3), which is the expected result. ■

We will need more details, stated in the following proposition, on the matrices in $R_0^{(n)}(p)$.

Proposition 3.3. *Let $n \geqslant 4$ and $C_0 = [c_{i,j}]_{1 \leqslant i,j \leqslant n} \in R_0^{(n)}(p)$. On the one hand, $C_0 \neq pI_n$. On the other hand, for all positive integers i, j, k, ℓ, one has*

$$1 \leqslant i < k < j < \ell \leqslant n \Rightarrow c_{i,j}c_{k,\ell} \equiv c_{i,\ell}c_{k,j} \pmod{p}$$
$$1 \leqslant i < j \leqslant k < \ell \leqslant n \Rightarrow c_{i,j}c_{k,\ell} = 0.$$

Remark 3.4. One can check that

$$R_0^{(2)}(p) = \bigsqcup_{0<c_{1,2}<p} \left\{ \begin{pmatrix} p & c_{1,2} \\ & p \end{pmatrix} \right\},$$

$$R_0^{(3)}(p) = \bigsqcup_{\substack{0 \leqslant c_{1,2}, c_{1,3}, c_{2,3} < p \\ c_{1,2}c_{2,3} = 0 \\ (c_{1,2}, c_{1,3}, c_{2,3}) \neq (0,0,0)}} \left\{ \begin{pmatrix} p & c_{1,2} & c_{1,3} \\ & p & c_{2,3} \\ & & p \end{pmatrix} \right\}.$$

Proof of Proposition 3.3. The fact that $C_0 \neq pI_n$ is obvious since the first determinantal divisor of C_0, whose value is 1, is nothing else than the greatest common divisor of the entries of C_0, which are non-negative integers strictly less than p.

Recall that $d_2(C_0) = p$. As a consequence, p divides the determinantal minors of C_0 of size 2 given by

$$c_{i,j}c_{k,\ell} - c_{i,\ell}c_{k,j} \tag{3.8}$$

for all $1 \leqslant i < k < j < \ell \leqslant n$. It also divides the determinantal divisors of C_0 of size 2 given by

$$c_{i,j}c_{j,\ell} - c_{i,\ell}c_{j,j} = c_{i,j}c_{j,\ell} - pc_{i,\ell} \tag{3.9}$$

for $1 \leqslant i < j < \ell \leqslant n$. The fact that the prime number p divides $c_{i,j}c_{j,\ell}$implies that $c_{i,j}c_{j,\ell} = 0$ because the non-diagonal entries of C_0 are non-negative and strictly less than p. Similarly, p divides the determinantal divisors of C_0 of size 2 given by

$$c_{i,j}c_{k,\ell} - c_{i,\ell}c_{k,j} = c_{i,j}c_{k,\ell} \tag{3.10}$$

for $1 \leqslant i < j < k < \ell \leqslant n$, such that $c_{i,j}c_{k,\ell} = 0$ too. ∎

4. End of the proof of Theorem A

In this section, $n \geqslant 4$. The following lemma, whose proof can be skipped in a first reading, will be used in Proposition 4.2.

Lemma 4.1. *Let $n \geqslant 4$ and $2 \leqslant k \leqslant n-2$. Let $C = [c_{i,j}]_{1 \leqslant i,j \leqslant n}$ be an upper-triangular matrix with integer entries satisfying*

$$\forall i \in \{1, \ldots, n\}, \quad c_{i,i} = p \tag{4.1}$$

and

$$1 \leqslant i < j \leqslant k < \ell \leqslant n \Rightarrow c_{i,j}c_{k,\ell} = 0 \tag{4.2}$$

for all positive integer i, j, k, ℓ. *Let*

$$2 \leqslant i_0 < j_0 \leqslant n-1. \tag{4.3}$$

Then, there exists ω_{i_0,j_0}, τ_{i_0,j_0} *in* $I_{n,k}$ *and* $\varepsilon_{i_0,j_0} = \pm 1$ *such that*

$$\left(CD^{(n)}(p)\right)(\omega_{i_0,j_0}, \tau_{i_0,j_0}) = \varepsilon_{i_0,j_0} p^{2k-2} c_{i_0,j_0}. \tag{4.4}$$

Proof of Lemma 4.1. Let $a_2 < a_3 < \cdots < a_{k-1}$ be an ordered sequence of indices in $\{2, \ldots, n-1\}$ not containing i_0 and j_0 and let

$$\omega_0 = \{1, a_2, \ldots, a_{k-1}, a_k \coloneqq i_0\},$$
$$\tau_0 = \{1, a_2, \ldots, a_{k-1}, j_0\}.$$

Such a choice is possible by (4.3). Note that ω_0 and τ_0 do not belong a priori to $I_{n,k}$ since they are not necessarily ordered (see (2.11)) but on the one hand, this will only change the determinant occuring in the left-hand side of (4.4) by ± 1 and on the other hand, this abuse of notations has the advantage of minimizing a lot the notations involved.

By the Cauchy-Binet formula,

$$\left(CD^{(n)}(p)\right)(\omega_0, \tau_0) = \sum_{\alpha \in I_{n,k}} C_0(\omega, \alpha) D^{(n)}(p)(\alpha, \tau) \tag{4.5}$$
$$= C_0(\omega, \tau) D^{(n)}(p)(\tau, \tau) \tag{4.6}$$
$$= p^{k-1} C_0(\omega, \tau) \tag{4.7}$$
$$= p^k \sum_{\sigma \in \sigma_{k-1}} \varepsilon(\sigma) c_{a_{\sigma(2)}, a_2} \cdots c_{a_{\sigma(k-1)}, a_{k-1}} c_{a_{\sigma(k)}, j_0} \tag{4.8}$$

where σ_{k-1} stands for the group of permutations of $\{2, \ldots, k\}$.

Obviously, the contribution to the previous sum of the permutation Id in σ_{k-1} equals

$$p^{2k-2} c_{i_0,j_0}$$

by (4.1). This is exactly the right-hand side of (4.4), up to the abuse of notations recalled above.

Let us show that all the other terms vanish. Let $\sigma \neq \mathrm{Id}$ in σ_{k-1}. One can assume that $a_{\sigma(k)} \leqslant j_0$ and

$$a_{\sigma(\ell)} \leqslant a_\ell \tag{4.9}$$

for $\ell \in \{2, \ldots, k-1\}$ since otherwise, the contribution of σ trivially vanishes, C being upper-triangular. Let us say that

$$2 \leqslant a_2 < \cdots < a_{u_0 - 1} < a_k = i_0 < a_{u_0} < \cdots < a_{v_0} < j_0 < a_{v_0+1} < \cdots < a_{k-1} \leqslant n-1 \tag{4.10}$$

where $2 \leqslant u_0 - 1 < v_0 \leqslant k-1$. (4.9) immediately implies that

$$\sigma(\ell) = \ell$$

for $2 \leqslant \ell \leqslant u_0 - 1$.

The fact that σ is different from the identity permutation Id entails that there exists at least two integers $\ell \geqslant u_0$ satisfying $\sigma(\ell) \neq \ell$. Let $u_0 \leqslant \ell_0 < \ell_1$ be the two consecutive smallest of them. One has

$$\sigma(\ell) = \ell$$

if $u_0 \leqslant \ell \leqslant \ell_0 - 1$ or $\ell_0 + 1 \leqslant \ell \leqslant \ell_1 - 1$ by (4.9), hence

$$\sigma(\ell_0) = k \qquad \text{and} \qquad \sigma(\ell_1) = \ell_0$$

by (4.10). Consequently, the contribution of σ equals

$$p^k \varepsilon(\sigma) c_{i_0, a_{\ell_0}} c_{a_{\ell_0}, a_{\ell_1}} \times \cdots = 0$$

by (4.2) since

$$1 \leqslant i_0 < a_{\ell_0} \leqslant a_{\ell_0} < a_{\ell_1}.$$

■

Then, we need the following intermediate result.

Proposition 4.2. *Let $n \geqslant 4$. Let $C_0 = [c_{i,j}]_{1 \leqslant i,j \leqslant n}$ in $R_0^{(n)}(p)$. If*

$$\forall (i,j) \in \{1, \dots, n\}^2, \quad 2 \leqslant i < j \leqslant n-1 \Rightarrow c_{i,j} = 0 \tag{4.11}$$

then

$$C_0 D^{(n)}(p) \in \Lambda_n \, diag\left(p, \underbrace{p^2, \dots, p^2}_{n-2 \text{ terms}}, p^3\right) \Lambda_n.$$

Otherwise,

$$C_0 D^{(n)}(p) \in \Lambda_n \, diag\left(p, p, \underbrace{p^2, \dots, p^2}_{n-4 \text{ terms}}, p^3, p^3\right) \Lambda_n.$$

In addition,

$$card\left(\left\{ C_0 \in R_0^{(n)}(p), C_0 D^{(n)}(p) \in \Lambda_n \, diag\left(p, \underbrace{p^2, \dots, p^2}_{n-2 \text{ terms}}, p^3\right) \Lambda_n \right\}\right) = 2p^{n-1} - p - 1$$

and

$$card\left(\left\{ C_0 \in R_0^{(n)}(p), C_0 D^{(n)}(p) \in \Lambda_n \, diag\left(p, p, \underbrace{p^2, \dots, p^2}_{n-4 \text{ terms}}, p^3, p^3\right) \Lambda_n \right\}\right) = \frac{p^2\left((n-3)p^{n-2} - (n-2)p^{n-3} + 1\right)}{p-1}.$$

Remark 4.3. One can easily check that when $n = 3$

$$C_0 D^{(3)}(p) \in \Lambda_3 \mathrm{diag}\left(p, p^2, p^3\right) \Lambda_3$$

for all matrix $C_0 \in R_0^{(3)}(p)$ whereas when $n = 2$

$$C_0 D^{(2)}(p) \in \Lambda_2 \mathrm{diag}\left(p, p^3\right) \Lambda_2$$

for all matrix $C_0 \in R_0^{(2)}(p)$.

Proof of Proposition 4.2. Recall that

$$\boldsymbol{d}_n\left(\mathrm{diag}\left(p, \underbrace{p^2, \dots, p^2}_{n-2 \text{ terms}}, p^3\right)\right) = \left(p, p^3, \dots, \underbrace{p^{2k-1}}_{k\text{'th term}}, \dots, p^{2n-5}, p^{2n-3}, p^{2n}\right),$$

$$\boldsymbol{d}_n\left(\mathrm{diag}\left(p, p, \underbrace{p^2, \dots, p^2}_{n-4 \text{ terms}}, p^3, p^3\right)\right) = \left(p, p^2, \dots, \underbrace{p^{2k-2}}_{k\text{'th term}}, \dots, p^{2n-6}, p^{2n-3}, p^{2n}\right),$$

$$\boldsymbol{d}_n(C_0) = \boldsymbol{d}_n(p) = \left(1, p, \dots, \underbrace{p^{\ell-1}}_{\ell\text{'th term}}, \dots, p^{n-2}, p^n\right)$$

for $2 \leqslant k \leqslant n-2$ and $2 \leqslant \ell \leqslant n-1$.

Obviously, $d_1(C_0 D^{(n)}(p)) = p$ and $d_n(C_0 D^{(n)}(p)) = p^{2n}$.

Let us show that $d_{n-1}(C_0 D^{(n)}(p)) = p^{2n-3}$. Of course, p^{2n-3} is a determinantal minor of $C_0 D^{(n)}(p)$ of size $n-1$ such that it remains to show that the other determinantal minors of $C_0 D^{(n)}(p)$ of size $n-1$ are all divisible by p^{2n-3}. Let $\omega = \{1, \dots, n\} \setminus \{i_0\}$ and $\tau = \{1, \dots, n\} \setminus \{j_0\}$ two elements in $I_{n,n-1}$ (see (2.11) for the notations used). By the Cauchy-Binet formula,

$$\begin{aligned}\left(C_0 D^{(n)}(p)\right)(\omega, \tau) &= \sum_{\alpha \in I_{n,n-1}} C_0(\omega, \alpha)\, D^{(n)}(p)(\alpha, \tau) \\ &= C_0(\omega, \tau)\, D^{(n)}(p)(\tau, \tau)\end{aligned}$$

since $D^{(n)}(p)$ is a diagonal matrix. If $j_0 = 1$ then $C_0(\omega, \tau)$ is divisible by p^{n-2}, since $d_{n-1}(C_0) = p^{n-2}$, and $D^{(n)}(p)(\tau, \tau) = p^n$. If $2 \leqslant j_0 \leqslant n-1$ then $C_0(\omega, \tau)$ is divisible by p^{n-2} and $D^{(n)}(p)(\tau, \tau) = p^{n-1}$. The only remaining case is when $j_0 = n$. The minor obtained when erasing the i_0'th row and the n'th column of $C_0 D^{(n)}(p)$ has its last row equal to 0 but when $i_0 = n$, in which case

$$\left(C_0 D^{(n)}(p)\right)(\omega, \tau) = p^{2n-3}.$$

Let $2 \leqslant k \leqslant n-2$. Of course, p^{2k-1} is a determinantal minor of $C_0 D^{(n)}(p)$ of size k. Then, by Lemma 4.1, all the integers

$$p^{2k-2} c_{i,j}$$

for $2 \leqslant i < j \leqslant n-1$ also belong to the list of determinantal minors of $C_0 D^{(n)}(p)$ of size k. Let $\omega = \{i_1, \dots, i_k\}$ with $1 \leqslant i_1 < \cdots < i_k \leqslant n$ and $\tau = \{j_1, \dots, j_k\}$ with $1 \leqslant j_1 < \cdots < j_k \leqslant n$ two elements in $I_{n,k}$. Once again, by the Cauchy-Binet formula,

$$\begin{aligned}\left(C_0 D^{(n)}(p)\right)(\omega,\tau) &= \sum_{\alpha \in I_{n,k}} C_0(\omega,\alpha)\, D^{(n)}(p)(\alpha,\tau) \\ &= C_0(\omega,\tau)\, D^{(n)}(p)(\tau,\tau) \\ &= C_0(\omega,\tau) \times \begin{cases} p^{k+1} & \text{if } 2 \leqslant j_1 < \cdots < j_{k-1} < j_k = n, \\ p^k & \text{if } 2 \leqslant j_1 < \cdots < j_k \leqslant n-1, \\ p^k & \text{if } 1 = j_1 < j_2 \cdots < j_{k-1} < j_k = n, \\ p^{k-1} & \text{if } 1 = j_1 < j_2 \cdots < j_k \leqslant n-1. \end{cases}\end{aligned}$$

$C_0(\omega,\tau)$ being divisible by p^{k-1}, since $d_k(C_0) = p^{k-1}$, all these determinantal minors are divisible by p^{2k-1} except a priori when $1 = j_1 < j_2 \cdots < j_k \leqslant n-1$. Let us investigate this last case. First of all,

$$\begin{aligned}C_0(\omega,\tau) &= \sum_{\sigma \in \sigma_k} \varepsilon(\sigma) c_{i_{\sigma(1)},1} c_{i_{\sigma(2)},j_2} \dots c_{i_{\sigma(k)},j_k} \\ &= \sum_{\substack{\sigma \in \sigma_k \\ i_{\sigma(1)}=1}} \varepsilon(\sigma) c_{i_{\sigma(1)},1} c_{i_{\sigma(2)},j_2} \dots c_{i_{\sigma(k)},j_k} \\ &= \begin{cases} p \sum_{\substack{\sigma \in \sigma_k \\ \sigma(1)=1}} \varepsilon(\sigma) c_{i_{\sigma(2)},j_2} \dots c_{i_{\sigma(k)},j_k} & \text{if } i_1 = 1, \\ 0 & \text{otherwise} \end{cases}\end{aligned}$$

where σ_k stands for the permutation group on k letters and since the condition $i_{\sigma(1)} = 1$ is equivalent to $i_1 = \sigma(1) = 1$. We can focus on the case $i_1 = 1$, in which case

$$C_0(\omega,\tau) = \sum_{L=0}^{k-1} p^{1+L} \sum_{\substack{\sigma \in \sigma_k \\ \sigma(1)=1 \\ \forall \ell \in \{2,\dots,k\}, i_{\sigma(\ell)} \leqslant j_\ell \\ \operatorname{card}\left(\left\{\ell \in \{2,\dots,k\}, i_{\sigma(l)} = j_\ell\right\}\right) = L}} \varepsilon(\sigma) \prod_{\substack{2 \leqslant \ell \leqslant k \\ i_{\sigma(\ell)} \neq j_\ell}} c_{i_{\sigma(\ell)},j_\ell}$$

is a polynomial in a subset of

$$c_{i,j}, \quad 2 \leqslant i < j \leqslant n-1$$

divisible by p^{k-1}, since $d_k(C_0) = p^{k-1}$, whose constant term is divisible by p^k. One can now conclude as follows. If (4.11) holds then $d_k\left(C_0 D^{(n)}(p)\right)$ is the greatest common divisor of 0, p^{2k-1} and of a finite list of integers divisible by p^{2k-1}, hence

$$d_k\left(C_0 D^{(n)}(p)\right) = p^{2k-1}.$$

If (4.11) does not hold then $d_k\left(C_0 D^{(n)}(p)\right)$ is the greatest common divisors of p^{2k-1}, of the integers $p^{2k-2}c_{i,j}$, $2 \leqslant i < j \leqslant n-1$, and of a finite list of integers divisible by p^{2k-2}, hence

$$d_k\left(C_0 D^{(n)}(p)\right) = p^{2k-2}.$$

Let us compute the first cardinality, say $c_0^{(n)}(p)$, given in the previous proposition. The set

$$\left\{C_0 \in R_0^{(n)}(p), \forall (i,j) \in \{1,\dots,n\}^2, \quad 2 \leqslant i < j \leqslant n-1 \Rightarrow c_{i,j} = 0\right\}$$

can be decomposed into the disjoint union of the three following sets.

- The set of matrices C_0 in $R_0^{(n)}(p)$ satisfying (4.11) and $c_{1,2} \neq 0$, $c_{n-1,n} = 0$, which implies that
$$c_{2,n} = \cdots = c_{n-2,n} = 0.$$
There are $(p-1)p^{n-2}$ such matrices.
- The set of matrices C_0 in $R_0^{(n)}(p)$ satisfying (4.11) and $c_{1,2} = 0$, $c_{n-1,n} \neq 0$, which implies that
$$c_{1,3} = \cdots = c_{1,n-1} = 0.$$
There are $(p-1)p^{n-2}$ such matrices.
- The set of matrices C_0 in $R_0^{(n)}(p)$ satisfying (4.11) and $c_{1,2} = c_{n-1,n} = 0$, which can be identified to the set of matrices C_0 in $R_0^{(n-1)}(p)$ satisfying (4.11), by erasing the diagonal of zeros above the main diagonal. There are $c_0^{(n-1)}(p)$ such matrices.

In total,

$$c_0^{(n)}(p) = 2(p-1)p^{n-2} + c_0^{(n-1)}(p).$$

One can conclude by induction on $n \geqslant 4$. If the formula holds for $n \geqslant 4$ then

$$c_0^{(n+1)}(p) = 2(p-1)p^{n-1} + 2p^{n-1} - p - 1 = 2p^n - p - 1.$$

Let us briefly check that $c_0^{(4)}(p) = 2p^3 - p - 1$. If C_0 in $R_0^{(4)}(p)$ satisfies (4.11) then five cases can occur.

- $c_{1,2} = c_{1,3} = c_{1,4} = c_{2,4} = 0$ and $c_{3,4} \neq 0$. There are $p-1$ such matrices.
- $c_{1,2} = c_{1,3} = c_{1,4} = 0$ and $c_{2,4} \neq 0$. There are $p(p-1)$ such matrices.
- $c_{1,2} = c_{1,3} = 0$ and $c_{1,4} \neq 0$. There are $p^2(p-1)$ such matrices.
- $c_{1,2} = c_{2,4} = c_{3,4} = 0$ and $c_{1,3} \neq 0$. There are $p(p-1)$ such matrices.
- $c_{2,4} = c_{3,4} = 0$ and $c_{1,2} \neq 0$. There are $p^2(p-1)$ such matrices.

The computation of the second cardinality is a consequence of Proposition 3.1, which gives the cardinal of $R_0^{(n)}(p)$. ■

Let us now complete the proof of Theorem A.

Proof of Theorem A. By (2.5),

$$\pi^{(n)}(p) * \pi^{(n)}(p) = \sum_{\Lambda_n h \Lambda_n \subset \pi^{(n)}(p)\pi^{(n)}(p)} m_n(h;p)\Lambda_n h \Lambda_n$$

where $h \in GL_n(\mathbb{Q})$ ranges over a system of representatives of the Λ_n right cosets contained in the set

$$\pi^{(n)}(p)\pi^{(n)}(p)$$

and

$$m_n(h;p) \coloneqq \frac{\deg\left(D^{(n)}(p)\right)}{\deg(h)} c_n(h;p),$$
$$c_n(h;p) \coloneqq \operatorname{card}\left(\left\{C \in R^{(n)}(p), CD^{(n)}(p) \in \pi^{(n)}(p)\right\}\right).$$

Recall that

$$\deg\left(D^{(n)}(p)\right) = p\frac{\varphi_n(p)}{\varphi_1(p)^2\varphi_{n-2}(p)} = p\frac{\left(p^{n-1}-1\right)\left(p^n-1\right)}{(p-1)^2} \tag{4.12}$$

by (2.3).

Let us determine the different matrices h occuring in this decomposition.

If C_1 in $R_1^{(n)}(p)$ then we have already seen that

$$C_1 = \operatorname{diag}\left(p^{\delta_1}, \dots, p^{\delta_n}\right) C_1'$$

with C_1' an upper-triangular matrix in Λ_n and $0 \leqslant \delta_1, \dots, \delta_n \leqslant 2$ with

$$\operatorname{card}\left(\{i \in \{1, \dots, n\}, \delta_i = 0\}\right) = \operatorname{card}\left(\{i \in \{1, \dots, n\}, \delta_i = 2\}\right) = 1.$$

As a consequence,

$$C_1 D^{(n)}(p) = \operatorname{diag}\left(p^{\delta_1}, \underbrace{p^{1+\delta_2}, \dots, p^{1+\delta_{n-1}}}_{n-2 \text{ terms}}, p^{2+\delta_n}\right) D^{(n)}(p)^{-1} C_1' D^{(n)}(p)$$
$$\in \Lambda_n \operatorname{diag}\left(p^{\delta_1}, \underbrace{p^{1+\delta_2}, \dots, p^{1+\delta_{n-1}}}_{n-2 \text{ terms}}, p^{2+\delta_n}\right) \Lambda_n$$

since $D^{(n)}(p)^{-1} C_1' D^{(n)}(p)$ belongs to Λ_n. Let $1 \leqslant \alpha_1 \neq \alpha_2 \leqslant n$ the integers satisfying

$$\delta_{\alpha_1} = 0 \qquad \text{and} \qquad \delta_{\alpha_2} = 2.$$

Let us list the different cases that can occur.

First case: $\alpha_1 = 1$ and $2 \leqslant \alpha_2 \leqslant n-1$. In this case, one has

$$C_1 D^{(n)}(p) \in \Lambda_n \mathrm{diag}\left(1, \underbrace{p^2, \dots, p^2}_{n-3 \text{ terms}}, p^3, p^3\right) \Lambda_n.$$

The number of such matrices C_1 is

$$\sum_{2 \leqslant \alpha_2 \leqslant n-1} p^{n+\alpha_2-2} = p^n \frac{p^{n-2}-1}{p-1}. \tag{4.13}$$

Second case: $\alpha_1 = 1$ and $\alpha_2 = n$. In this case, one has

$$C_1 D^{(n)}(p) \in \Lambda_n \mathrm{diag}\left(1, \underbrace{p^2, \dots, p^2}_{n-2 \text{ terms}}, p^4\right) \Lambda_n.$$

The number of such matrices C_1 is

$$p^{2n-2}. \tag{4.14}$$

Third case: $2 \leqslant \alpha_1 \leqslant n-1$ and $\alpha_2 = 1$. In this case, one has

$$C_1 D^{(n)}(p) \in \Lambda_n \mathrm{diag}\left(p, \underbrace{p^2, \dots, p^2}_{n-2 \text{ terms}}, p^3\right) \Lambda_n.$$

The number of such matrices C_1 is

$$\sum_{2 \leqslant \alpha_1 \leqslant n-1} p^{n-\alpha_1} = p \frac{p^{n-2}-1}{p-1}. \tag{4.15}$$

Fourth case:[5] $2 \leqslant \alpha_1 \neq \alpha_2 \leqslant n-1$. In this case, one has

$$C_1 D^{(n)}(p) \in \Lambda_n \mathrm{diag}\left(p, p, \underbrace{p^2, \dots, p^2}_{n-4 \text{ terms}}, p^3, p^3\right) \Lambda_n.$$

The number of such matrices C_1 is

$$\begin{aligned} \sum_{2 \leqslant \alpha_1 \neq \alpha_2 \leqslant n-1} p^{n-1+\alpha_2-\alpha_1} &= \left(\sum_{1 \leqslant \alpha \leqslant n-2} p^\alpha\right)^2 - (n-2)p^{n-1} \\ &= \frac{p^2\left(p^{2(n-2)} - (n-2)p^{n-1} + 2(n-3)p^{n-2} - (n-2)p^{n-3} + 1\right)}{(p-1)^2}. \end{aligned} \tag{4.16}$$

[5]Note that this case does not occur if $n < 4$.

Fifth case: $2 \leqslant \alpha_1 \leqslant n-1$ and $\alpha_2 = n$. In this case, one has

$$C_1 D^{(n)}(p) \in \Lambda_n \mathrm{diag}\left(p, p, \underbrace{p^2, \dots, p^2}_{n-3 \text{ terms}}, p^4\right) \Lambda_n.$$

The number of such matrices C_1 is

$$\sum_{2 \leqslant \alpha_1 \leqslant n-1} p^{2n-1-\alpha_1} = p^n \frac{p^{n-2}-1}{p-1}. \tag{4.17}$$

Sixth case: $\alpha_1 = n$ and $\alpha_2 = 1$. In this case, one has

$$C_1 D^{(n)}(p) \in \Lambda_n \mathrm{diag}\left(\underbrace{p^2, \dots, p^2}_{n \text{ terms}}\right) \Lambda_n = \Lambda_n p^2 I_n \Lambda_n.$$

The number of such matrices C_1 is

$$1. \tag{4.18}$$

Seventh case: $\alpha_1 = n$ and $2 \leqslant \alpha_2 \leqslant n-1$. In this case, one has

$$C_1 D^{(n)}(p) \in \Lambda_n \mathrm{diag}\left(p, \underbrace{p^2, \dots, p^2}_{n-2 \text{ terms}}, p^3\right) \Lambda_n.$$

The number of such matrices C_1 is

$$\sum_{2 \leqslant \alpha_2 \leqslant n-1} p^{\alpha_2 - 1} = p \frac{p^{n-2}-1}{p-1}. \tag{4.19}$$

If C_0 in $R_0^{(n)}(p)$ then two cases can occur by Proposition 4.2.
Eighth case: $\forall (i,j) \in \{1, \dots, n\}^2, 2 \leqslant i < j \leqslant n \Rightarrow c_{i,j} = 0$. In this case,

$$C_0 D^{(n)}(p) \in \Lambda_n \mathrm{diag}\left(p, \underbrace{p^2, \dots, p^2}_{n-2 \text{ terms}}, p^3\right) \Lambda_n$$

and the number of such matrices is

$$2p^{n-1} - p - 1. \tag{4.20}$$

Nineth case: $\exists (i,j) \in \{1, \dots, n\}^2, 2 \leqslant i < j \leqslant n$ and $c_{i,j} \neq 0$. In this case,

$$C_0 D^{(n)}(p) \in \Lambda_n \mathrm{diag}\left(p, p, \underbrace{p^2, \dots, p^2}_{n-4 \text{ terms}}, p^3, p^3\right) \Lambda_n$$

and the number of such matrices is

$$\frac{p^2\left((n-3)p^{n-2}-(n-2)p^{n-3}+1\right)}{p-1}. \tag{4.21}$$

In particular, we have just proved that

$$\begin{aligned}
\pi^{(n)}(p)*\pi^{(n)}(p) &= m_n(1;p)\Lambda_n p^2 I_n \Lambda_n \\
&+ m_n(2;p)\Lambda_n \mathrm{diag}\left(p, \underbrace{p^2,\dots,p^2}_{n-2 \text{ terms}}, p^3\right)\Lambda_n \\
&+ m_n(3;p)\Lambda_n \mathrm{diag}\left(1, \underbrace{p^2,\dots,p^2}_{n-3 \text{ terms}}, p^3, p^3\right)\Lambda_n \\
&+ m_n(4;p)\Lambda_n \mathrm{diag}\left(1, \underbrace{p^2,\dots,p^2}_{n-2 \text{ terms}}, p^4\right)\Lambda_n \\
&+ m_n(5;p)\Lambda_n \mathrm{diag}\left(p, p, \underbrace{p^2,\dots,p^2}_{n-3 \text{ terms}}, p^4\right)\Lambda_n \\
&+ m_n(6;p)\Lambda_n \mathrm{diag}\left(p, p, \underbrace{p^2,\dots,p^2}_{n-4 \text{ terms}}, p^3, p^3\right)\Lambda_n.
\end{aligned} \tag{4.22}$$

where

$$\begin{aligned}
m_n(1;p) &\coloneqq m_n\left(p^2 I_n; p\right), \\
m_n(2;p) &\coloneqq m_n\left(\mathrm{diag}\left(p, \underbrace{p^2,\dots,p^2}_{n-2 \text{ terms}}, p^3\right); p\right), \\
m_n(3;p) &\coloneqq m_n\left(\mathrm{diag}\left(1, \underbrace{p^2,\dots,p^2}_{n-3 \text{ terms}}, p^3, p^3\right); p\right)
\end{aligned}$$

and

$$\begin{aligned}
m_n(4;p) &\coloneqq m_n\left(\mathrm{diag}\left(1, \underbrace{p^2,\dots,p^2}_{n-2 \text{ terms}}, p^4\right); p\right), \\
m_n(5;p) &\coloneqq m_n\left(\mathrm{diag}\left(p, p, \underbrace{p^2,\dots,p^2}_{n-3 \text{ terms}}, p^4\right); p\right), \\
m_n(6;p) &\coloneqq m_n\left(\mathrm{diag}\left(p, p, \underbrace{p^2,\dots,p^2}_{n-4 \text{ terms}}, p^3, p^3\right); p\right).
\end{aligned}$$

One has,

$$m_n(1;p)=\frac{\deg\left(D^{(n)}(p)\right)}{\deg(p^2I_n)}c_n\left(p^2I_n;p\right)=p\frac{\left(p^{n-1}-1\right)\left(p^n-1\right)}{(p-1)^2}$$

by (4.12) and (4.18) since $\deg(p^2I_n)=1$.

Then,

$$\begin{aligned}m_n(2;p)&=\frac{\deg\left(D^{(n)}(p)\right)}{\deg\left(\mathrm{diag}\left(p,\underbrace{p^2,\dots,p^2}_{n-2\text{ terms}},p^3\right)\right)}c_n\left(\mathrm{diag}\left(p,\underbrace{p^2,\dots,p^2}_{n-2\text{ terms}},p^3\right);p\right)\\&=c_n\left(\mathrm{diag}\left(p,\underbrace{p^2,\dots,p^2}_{n-2\text{ terms}},p^3\right);p\right)\\&=2p\frac{p^{n-2}-1}{p-1}+2p^{n-1}-p-1\\&=\frac{2p^n-p^2-2p+1}{p-1}\end{aligned}$$

by (2.2), (4.15), (4.19), (4.20).

Let us compute simultaneously the values of $m_n(3;p)$ and $m_n(4;p)$. On the one hand, applying the map Ψ (see (2.14)) to (4.22), one gets

$$\begin{aligned}\pi_{n-2,1}^{(n-1)}(p)*\pi_{n-2,1}^{(n-1)}(p)&=m_n(3;p)\Lambda_n\mathrm{diag}\left(\underbrace{p^2,\dots,p^2}_{n-3\text{ terms}},p^3,p^3\right)\Lambda_n\\&\quad+m_n(4;p)\Lambda_n\mathrm{diag}\left(\underbrace{p^2,\dots,p^2}_{n-2\text{ terms}},p^4\right)\Lambda_n.\end{aligned}$$

On the other hand, by [AZ95, Lemma 2.18 Equation (2.30), p. 115], one gets

$$\begin{aligned}\pi_{n-2,1}^{(n-1)}(p)*\pi_{n-2,1}^{(n-1)}(p)&=\Lambda_np^2I_n\Lambda_n*\pi_1^{(n-1)}(p)*\pi_1^{(n-1)}(p)\\&=\Lambda_np^2I_n\Lambda_n*\left(\pi_{0,1}^{(n-1)}(p)+(p+1)\pi_{2,0}^{(n-1)}(p)\right)\\&=\Lambda_n\mathrm{diag}\left(\underbrace{p^2,\dots,p^2}_{n-2\text{ terms}},p^4\right)\Lambda_n\\&\quad+(p+1)\Lambda_n\mathrm{diag}\left(\underbrace{p^2,\dots,p^2}_{n-3\text{ terms}},p^3,p^3\right)\Lambda_n\end{aligned}$$

by (2.9). Distinct Λ_n double cosets being linearly independent by [AZ95, Lemma 1.5, p. 96], we get

$$m_n(3;p) = p+1, \qquad m_n(4;p) = 1.$$

Then,

$$\begin{aligned}\deg\left(\operatorname{diag}\left(1,\underbrace{p^2,\dots,p^2}_{n-3 \text{ terms}},p^3,p^3\right)\right)&\\ = \frac{\deg\left(D^{(n)}(p)\right)}{m_n(3;p)} c_n\left(\operatorname{diag}\left(1,\underbrace{p^2,\dots,p^2}_{n-3 \text{ terms}},p^3,p^3\right);p\right)&\\ = p^{n+1}\frac{\left(p^{n-2}-1\right)\left(p^{n-1}-1\right)\left(p^n-1\right)}{(p-1)^2\left(p^2-1\right)}&\end{aligned}$$

by (4.12) and (4.13). This proves (1.8) in Theorem A. Similarly,

$$\begin{aligned}\deg\left(\operatorname{diag}\left(1,\underbrace{p^2,\dots,p^2}_{n-2 \text{ terms}},p^4\right)\right) &= \frac{\deg\left(D^{(n)}(p)\right)}{m_n(4;p)} c_n\left(\operatorname{diag}\left(1,\underbrace{p^2,\dots,p^2}_{n-2 \text{ terms}},p^4\right);p\right)\\ &= p^{2n-1}\frac{\left(p^{n-1}-1\right)\left(p^n-1\right)}{(p-1)^2}\end{aligned}$$

by (4.12) and (4.14). This proves (1.9) in Theorem A.

Let us consider $m_n(5;p)$. First, let us compute the value of

$$\deg\left(\operatorname{diag}\left(p,p,\underbrace{p^2,\dots,p^2}_{n-3 \text{ terms}},p^4\right)\right) = \deg\left(\operatorname{diag}\left(1,1,\underbrace{p,\dots,p}_{n-3 \text{ terms}},p^3\right)\right)$$

by (2.2). This is done by a semi-explicit computation of

$$\pi_{n-2}^{(n)}(p) * \pi_{0,1}^{(n)}(p) = \sum_{\Lambda_n h \Lambda_n \subset \pi_{n-2}^{(n)}(p)\pi_{0,1}^{(n)}(p)} m\left(D_{n-2}^{(n)}(p), D_{0,1}^{(n)}(p); h\right)\Lambda_n h \Lambda_n$$

where $h \in GL_n(\mathbb{Q})$ ranges over a system of representatives of the Λ_n right cosets contained in the set

$$\pi_{n-2}^{(n)}(p)\pi_{0,1}^{(n)}(p)$$

and

$$\begin{aligned}m\left(D_{n-2}^{(n)}(p), D_{0,1}^{(n)}(p); h\right)&\\ = \frac{\deg\left(D_{0,1}^{(n)}(p)\right)}{\deg(h)} \operatorname{card}\left(\left\{C \in R_{1,1,\underbrace{p,\dots,p}_{n-2}}, CD_{0,1}^{(n)}(p) \in \Lambda_n h \Lambda_n\right\}\right)&\end{aligned}$$

where $R_{1,1,\underbrace{p,\dots,p}_{n-2}}$ is the complete system of representatives for the distinct Λ_n right cosets of $\pi_{n-2}^{(n)}(p)$ modulo Λ_n given by the set of upper-triangular column reduced matrices C satisfying

$$\forall i \in \{1,\dots,n\}, \quad c_{i,i} \in \{1,p\}, \tag{4.23}$$

$$\operatorname{card}\left(\{i \in \{1,\dots,n\}, c_{i,i}=1\}\right)=2 \tag{4.24}$$

and

$$\forall i \in \{1,\dots,n-1\}, p \mid c_{i,i} \Rightarrow \forall j \in \{i+1,\dots,n\}, \quad c_{i,j}=0 \tag{4.25}$$

according to [AZ95, Lemma 2.18, p. 115]. Let C be an element of $R_{1,1,\underbrace{p,\dots,p}_{n-2}}$ and let $1 \leqslant \alpha_1 < \alpha_2 \leqslant n$ be the indices of the diagonal elements of C equal to 1 by (4.24). By (4.23) and (4.25), C can be decomposed into

$$C = \operatorname{diag}\left(p^{\delta_1},\dots,p^{\delta_n}\right) C'$$

for some upper-triangular matrix C' in Λ_n and integers $0 \leqslant \delta_1,\dots,\delta_n \leqslant 1$ such that

$$CD_{0,1}^{(n)}(p) \in \begin{cases} \Lambda_n \operatorname{diag}\left(1,1,\underbrace{p,\dots,p}_{n-3 \text{ terms}},p^3\right)\Lambda_n & \text{if } 1 \leqslant \alpha_1 < \alpha_2 \leqslant n-1 \\ \pi_{n-2,1}^{(n)}(p) & \text{if } 1 \leqslant \alpha_1 < \alpha_2 = n. \end{cases}$$

Thus,

$$\begin{aligned} \pi_{n-2}^{(n)}(p) * \pi_{0,1}^{(n)}(p) &= m\left(D_{n-2}^{(n)}(p), D_{0,1}^{(n)}(p); D_{n-2,1}^{(n)}(p)\right)\pi_{n-2,1}^{(n)}(p) \\ &\quad + m\left(D_{n-2}^{(n)}(p), D_{0,1}^{(n)}(p); \operatorname{diag}\left(1,1,\underbrace{p,\dots,p}_{n-3 \text{ terms}},p^3\right)\right) \\ &\quad \times \Lambda_n \operatorname{diag}\left(1,1,\underbrace{p,\dots,p}_{n-3 \text{ terms}},p^3\right)\Lambda_n. \end{aligned}$$

Applying the map $\Psi^{\circ 2}$ (see (2.14)) to the previous equality, one gets

$$\begin{aligned} &\Lambda_n \operatorname{diag}\left(\underbrace{p,\dots,p}_{n-3 \text{ terms}},p^3\right)\Lambda_n \\ &= m\left(D_{n-2}^{(n)}(p), D_{0,1}^{(n)}(p); \operatorname{diag}\left(\underbrace{p,\dots,p}_{n-3 \text{ terms}},p^3\right)\right)\Lambda_n \operatorname{diag}\left(\underbrace{p,\dots,p}_{n-3 \text{ terms}},p^3\right)\Lambda_n, \end{aligned}$$

hence

$$m\left(D_{n-2}^{(n)}(p), D_{0,1}^{(n)}(p); \operatorname{diag}\left(\underbrace{p, \dots, p}_{n-3 \text{ terms}}, p^3\right)\right) = 1$$

by the linear independence of distinct Λ_n double cosets ([AZ95, Lemma 1.5 Equation (2.32), p. 96]). As a consequence,

$$\begin{aligned}
\deg\left(\operatorname{diag}\left(1, 1, \underbrace{p, \dots, p}_{n-3 \text{ terms}}, p^3\right)\right) &= \deg\left(D_{0,1}^{(n)}(p)\right) \sum_{1 \leqslant \alpha_1 < \alpha_2 \leqslant n-1} p^{2n-1-\alpha_1-\alpha_2} \\
&= p^{n-1} \frac{\varphi_n(p)}{\varphi_{n-1}(p)\varphi_1(p)} p^{2n-1} \sum_{1 \leqslant \alpha_1 < \alpha_2 \leqslant n-1} \left(\frac{1}{p}\right)^{\alpha_1+\alpha_2} \\
&= p^{n-1} \frac{\varphi_n(p)}{\varphi_{n-1}(p)\varphi_1(p)} p^{2n-4} \frac{\varphi_{n-1}(1/p)}{\varphi_2(1/p)\varphi_{n-3}(1/p)} \\
&= p^{n-1} \frac{\varphi_n(p)}{\varphi_{n-1}(p)\varphi_1(p)} p^2 \frac{\varphi_{n-1}(p)}{\varphi_2(p)\varphi_{n-3}(p)} \\
&= p^{n+1} \frac{\varphi_n(p)}{\varphi_1(p)\varphi_2(p)\varphi_{n-3}(p)}
\end{aligned}$$

by (4.12), [AZ95, Equation (2.33), p. 115] and since

$$\varphi_r(1/x) = (-1)^r x^{-r(r+1)/2} \varphi_r(x)$$

for $r \geqslant 1$ and $x \neq 0$ a real number. This proves (1.10) in Theorem A. As a consequence,

$$\begin{aligned}
m_n(5; p) &= \frac{\deg\left(D^{(n)}(p)\right)}{\deg\left(\operatorname{diag}\left(p, p, \underbrace{p^2, \dots, p^2}_{n-3 \text{ terms}}, p^4\right)\right)} c_n\left(\operatorname{diag}\left(p, p, \underbrace{p^2, \dots, p^2}_{n-3 \text{ terms}}, p^4\right); p\right) \\
&= \frac{\varphi_2(p)}{\varphi_1(p)^2} \\
&= p + 1
\end{aligned}$$

by (4.17).

Finally, let us compute the value of $m_n(6;p)$. One has

$$\begin{aligned} m_n(6;p) &= \frac{\deg\left(D^{(n)}(p)\right)}{\deg\left(\operatorname{diag}\left(p,p,\underbrace{p^2,\dots,p^2}_{n-4 \text{ terms}},p^3,p^3\right)\right)} \\ &\quad \times c_n\left(\operatorname{diag}\left(p,p,\underbrace{p^2,\dots,p^2}_{n-4 \text{ terms}},p^3,p^3\right);p\right) \\ &= \frac{\deg\left(D^{(n)}(p)\right)}{\deg\left(D^{(n)}_{n-4,2}(p)\right)} c_n\left(\operatorname{diag}\left(p,p,\underbrace{p^2,\dots,p^2}_{n-4 \text{ terms}},p^3,p^3\right);p\right) \\ &= \frac{(p+1)^2(p-1)^2}{p^3\left(p^{n-2}-1\right)\left(p^{n-3}-1\right)} \frac{p^3\left(p^{2n-5}-p^{n-2}-p^{n-3}+1\right)}{(p-1)^2} \\ &= (p+1)^2 \end{aligned}$$

by (2.2), (2.3), (4.16) and (4.21).

Equation (4.22) and the explicit values of the constants $m_n(i;p)$ $(1 \leqslant i \leqslant 6)$ prove (1.12) in Theorem A. ∎

References

[AZ95] A.N. Andrianov and V.G. Zhuravlëv, *Modular forms and Hecke operators*, volume 145 of Translations of Mathematical Monographs, American Mathematical Society, Providence, RI, 1995, Translated from the 1990 Russian original by Neal Koblitz.

[BB] V. Blomer and J. Buttcane, *On the subconvexity problem for L-functions on GL*(3), available at http://arxiv.org/abs/1504.02667.

[BH10] V. Blomer and R. Holowinsky, *Bounding sup-norms of cusp forms of large level*, Invent. Math. **179**(3) (2010), 645–681.

[BHM] V. Blomer, G. Harcos, and D. Milicevic, *Eigenfunctions on arithmetic hyperbolic* 3*-manifolds*, Duke Math. J. **165**(4) (2016), 625–659.

[Blo12] V. Blomer, *Subconvexity for twisted L-functions on* GL(3), Amer. J. Math. **134**(5) (2012), 1385–1421.

[BMa] V. Blomer and P. Maga, *Subconvexity for sup-norms of automorphic forms on PGL*(n), available at http://arxiv.org/pdf/1405.6691.pdf.

[BMb] V. Blomer and P. Maga, *The sup-norm problem for PGL*(4), Int. Math. Res. Not. **14** (2015), 5311–5332.

[BT] F. Brumley and N. Templier, *Large values of cusp forms on GL*(n), available at http://arxiv.org/abs/1411.4317.

[Bur62] D.A. Burgess, *On character sums and L-series*, Proc. London Math. Soc. (3) **12** (1962), 193–206.

[DFI94] W. Duke, J.B. Friedlander, and H.Iwaniec, *Bounds for automorphic L-functions. II*, Invent. Math. **115**(2) (1994), 219–239.

[FI92] J. Friedlander and H. Iwaniec, *A mean-value theorem for character sums*, Michigan Math. J. **39**(1) (1992), 153–159.

[Gol06] D. Goldfeld, *Automorphic forms and L-functions for the group* $GL(n, \mathbb{R})$, volume 99 of Cambridge Studies in Advanced Mathematics, Cambridge University Press, Cambridge, 2006 (with an appendix by Kevin A. Broughan).

[HR] H. Helfgott and G. Ricotta, *A new bound for the sup-norm of automorphic forms on non-compact modular curves in the level aspect*, available at http://www.math.u-bordeaux1.fr/gricotta/supnorm.htm.

[HRRa] R. Holowinsky, G. Ricotta, and E. Royer, *The amplification method in the* $GL(3)$ *Hecke algebra*, available at http://arxiv.org/abs/1412.5022.

[HRRb] R. Holowinsky, G. Ricotta, and E. Royer, *On the sup-norm of* $SL(3)$ *Hecke-Maass cusp form*, available at http://arxiv.org/abs/1411.4317.

[HT12] G. Harcos and N. Templier, *On the sup-norm of Maass cusp forms of large level: II*, Int. Math. Res. Not. IMRN **20** (2012), 4764–4774.

[HT13] G. Harcos and N. Templier, *On the sup-norm of Maass cusp forms of large level. III*, Math. Ann. **356**(1) (2013), 209–216.

[IS95] H. Iwaniec and P. Sarnak, L^∞ *norms of eigenfunctions of arithmetic surfaces*, Ann. of Math. (2) **141**(2) (1995), 301–320.

[Iwa92] H. Iwaniec, *The spectral growth of automorphic L-functions*, J. Reine Angew. Math. **428** (1992), 139–159.

[Kri90] A. Krieg, *Hecke algebras*, Mem. Amer. Math. Soc. **87**(435) (1990), x+158.

[Li11] X. Li, *Bounds for* $\mathrm{GL}(3) \times \mathrm{GL}(2)$ *L-functions and* $\mathrm{GL}(3)$ *L-functions*, Ann. of Math. (2) **173**(1) (2011), 301–336.

[Mara] S. Marshall, *Local bounds for* L^p *norms of Maass forms in the level aspect*, available at http://arxiv.org/abs/1502.01006.

[Marb] S. Marshall, *Sup norms of Maass forms on semisimple groups*, available at http://arxiv.org/abs/1405.7033.

[Muna] R. Munshi, *The circle method and bounds for L-functions - III: t-aspect subconvexity for* $GL(3)$ *L-functions*, . Amer. Math. Soc. **28**(4) (2015), 913–938.

[Munb] R. Munshi, *The circle method and bounds for L-functions - IV: subconvexity for twists of* $\mathrm{GL}(3)$ *L-functions*, Ann. of Math. (2) **182** (2015), 617–672.

[MV10] P. Michel and A. Venkatesh, *The subconvexity problem for* GL_2, Publ. Math. Inst. Hautes Études Sci. **111** (2010), 171–271.

[New72] M. Newman, *Integral matrices*, Academic Press, New York, 1972. Pure and Applied Mathematics, Vol. 45.

[Sah] A. Saha, *On sup-norms of cusp forms of powerful level*, available at http://arxiv.org/abs/1404.3179.

[Sar] P. Sarnak, *Letter to Morawetz*, available at http://www.math.princeton.edu/sarnak.

[Shi94] G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, volume 11 of Publications of the Mathematical Society of Japan, Princeton University Press, Princeton, NJ, 1994. Reprint of the 1971 original, Kanô Memorial Lectures 1.

[SV] L. Silberman and A. Venkatesh, *Entropy bounds for Hecke eigenfunctions on division algebras*, preprint available at http://www.math.ubc.ca/lior/work/.

[Tem10] N. Templier, *On the sup-norm of Maass cusp forms of large level*, Selecta Math. (N.S.) **16**(3) (2010), 501–531.

[Wey21] H. Weyl, *Zur abschatzung von* $\zeta(1+ti)$, Math. Z. **10** (1921), 88–101.

Address: Guillaume Ricotta: Université de Bordeaux, Institut de Mathématiques de Bordeaux, 351 cours de la libération, 33405 Talence Cedex, France.

E-mail: Guillaume.Ricotta@math.u-bordeaux1.fr

Received: 16 March 2015; **revised:** 19 November 2015

Functiones et Approximatio
54.2 (2016), 227–239
doi: 10.7169/facm/2016.54.2.6

CLASSES LOGARITHMIQUES ET CAPITULATION

Jean-François Jaulent

Résumé: Nous étudions un analogue logarithmique du Théorème d'Artin-Furtwängler sur la capitulation en transposant dans le cadre des classes logarithmiques les arguments mis en œuvre dans la preuve algébrique classique du Théorème de l'idéal principal.

Abstract: We study a logarithmic version of the classical result of Artin-Furwängler on principalization of ideal classes in the Hilbert class-field by applying the group theoretic description of the transfert map to logarithmic class-groups of degree 0.

Keywords: capitulation, logarithmic class group, principalization.

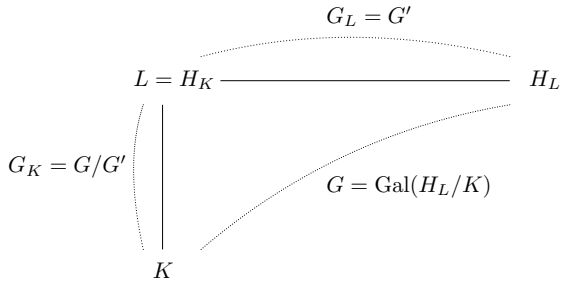
1. Introduction

Le célèbre Théorème d'Artin-Furwängler (*cf.* [2, 4, 3]) affirme que le groupe des classes d'idéaux Cl_K d'un corps de nombres K capitule dans son corps des classes de Hilbert $L = H_K$; en d'autres termes que les idéaux de K se principalisent dans son extension abélienne non ramifiée maximale L.

Et, comme l'extension des classes d'idéaux est injective pour les ℓ-parties dans une extension de degré étranger à ℓ, cela revient à dire que, pour tout nombre premier ℓ, le ℓ-sous-groupe de Sylow du groupe des classes d'idéaux d'un corps de nombres capitule dans le ℓ-corps des classes de Hilbert de ce corps *i.e.* dans sa ℓ-extension abélienne non ramifiée maximale.

La preuve du Théorème d'Artin-Furwängler repose sur deux éléments, le premier de nature arithmétique, le second purement algébrique : d'une part, la Théorie du corps de classes interprète le groupe de classes d'idéaux Cl_K comme groupe de Galois G_K de l'extension abélienne H_K/K, l'homomorphisme d'extension $j_{L/K} : Cl_K \to Cl_L$ correspondant dans cette description au morphisme de transfert $\mathrm{Ver}_{L/K} : G_K \to G_L$; d'autre part, des considérations de théorie des groupes montrent alors que le transfert est nul dans la situation étudiée :

2010 Mathematics Subject Classification: primary: 11R37

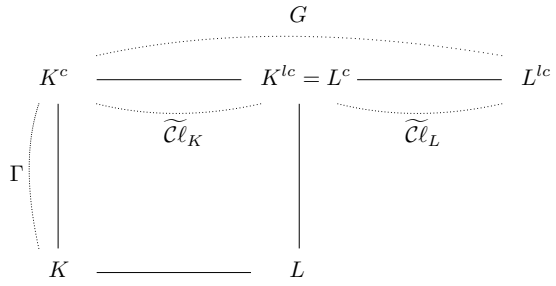


Comme noté dans [7], ce résultat s'étend à diverses situations arithmétiques, notamment aux groupes de classes de rayons, qui conduisent à des situations formellement comparables. Il était donc tentant d'essayer de le transposer à des groupes de classes présentant des analogies remarquables avec les objets précédents.

Il est ainsi défini dans [9], pour chaque nombre premier ℓ et tout corps de nombres K, un groupe de classes logarithmiques noté $\mathcal{C}\ell_K$, obtenu en remplaçant les valuations ordinaires $\nu_{\mathfrak{p}}$ attachées à chaque place finie $\mathfrak{p}$ de K par leurs analogues formels $\widetilde{\nu}_{\mathfrak{p}}$ définis à partir du logarithme ℓ-adique de la valeur absolue ℓ-adique attachée à la place $\mathfrak{p}$. La Théorie ℓ-adique du corps de classes (*cf.* [10, 5]) interprète alors le groupe de classes $\mathcal{C}\ell_K$ comme groupe de Galois de la pro-ℓ-extension abélienne localement cyclotomique maximale K^{lc} du corps K.

Mais une première difficulté apparaît alors : la pro-ℓ-extension abélienne K^{lc} contient évidemment la $\mathbb{Z}_\ell$-extension cyclotomique K^c de K, de sorte que le groupe $\mathcal{C}\ell_K \simeq \mathrm{Gal}(K^{lc}/K)$ n'est jamais fini. Pour obtenir un groupe fini, il est ainsi nécessaire de se restreindre au sous-groupe des classes logarithmiques de degré nul $\widetilde{\mathcal{C}\ell}_K \simeq \mathrm{Gal}(K^{lc}/K^c)$. Et la *conjecture de Gross-Kuz'min*, souvent appelée *conjecture de Gross généralisée* (*cf.* [8, 9, 10, 12])– affirme que cette restriction nécessaire est aussi suffisante, *i.e.* que le groupe obtenu $\widetilde{\mathcal{C}\ell}_K$ est effectivement un ℓ-groupe fini.

Lorsqu'elle est satisfaite, l'extension localement cyclotomique K^{lc} provient alors, par composition avec K^c, d'une extension abélienne L de K (que l'on peut supposer linéairement disjointe de K^c) et il est naturel d'introduire la pro-ℓ-extension abélienne localement cyclotomique maximale L^{lc} du corps L et de considérer le morphisme d'extension $\widetilde{j}_{L/K} : \widetilde{\mathcal{C}\ell}_K \to \mathcal{C}\ell_L$. Dans le schéma obtenu cependant arrive une deuxième difficulté :



le sous-corps $K^{lc} = L^c$ de L^{lc} n'est plus alors le sous-corps maximal de L^{lc} qui est abélien sur K^c, mais celui qui est abélien sur K ; de sorte qu'on ne peut plus écrire comme plus haut $\widetilde{\mathcal{C}\ell}_L \simeq G'$ et $\widetilde{\mathcal{C}\ell}_K \simeq G/G'$ avec $G = \mathrm{Gal}(L^{lc}/K^c)$, mais qu'il nous faut prendre en compte aussi l'action du groupe procyclique $\Gamma = \mathrm{Gal}(K^c/K)$.

Le but de cette note est d'étudier la transposition dans ce contexte logarithmique des résultats classiques d'Artin-Furtwängler et de Tannaka-Terada sur la capitulation dans le corps des classes de Hilbert ou dans le corps des genres relatif à une extension cyclique non ramifiée (devenant ici procyclique).

2. Bref rappel sur les classes logarithmiques

Classiquement, le groupe des classes d'idéaux d'un corps de nombres K est défini comme conoyau Cl_K du morphisme naturel partant du groupe multiplicatif $K^\times$ à valeurs dans le groupe des idéaux Id_K donné par la famille des valuations $\nu = (\nu_\mathfrak{p})_{\mathfrak{p} \in Pl_K}$ attachées aux places finies de K.

$$1 \to E_K \to K^\times \xrightarrow{\nu} Id_K \to Cl_K \to 1.$$

Par produit tensoriel avec $\mathbb{Z}_\ell$, son ℓ-sous-groupe de Sylow apparaît comme conoyau du morphisme ν étendu au tensorisé $\mathcal{R}_K = \mathbb{Z}_\ell \otimes_\mathbb{Z} K^\times$ et à valeurs dans le $\mathbb{Z}_\ell$-module libre construit sur ces mêmes places : $\mathcal{D}\ell = \oplus_{\mathfrak{p} \in Pl_K} \mathbb{Z}_\ell \mathfrak{p}$.

Le groupe des classes logarithmiques est le groupe analogue $\mathcal{C}\ell_K$ obtenu en remplaçant les valuations classiques $\nu_\mathfrak{p}$ par leurs homologues ℓ-adiques $\widetilde{\nu}_\mathfrak{p}$ définis à partir des logarithmes des valeurs absolues ℓ-adiques (*cf.* [9]) :

$$1 \to \mathcal{E}_K \to \mathcal{R}_K \xrightarrow{\widetilde{\nu}} \mathcal{D}\ell_K \to \mathcal{C}\ell_K \to 1.$$

Contrairement au groupe de classes d'idéaux, c'est donc un objet ℓ-adique.

Pour chaque place finie $\mathfrak{p}$ de K, soit $\mathcal{R}_\mathfrak{p} = \varprojlim K_\mathfrak{p}^\times / K_\mathfrak{p}^{\times \ell^n}$ le compactifié ℓ-adique du groupe $K_\mathfrak{p}^\times$ et $\mathcal{J}_K = \prod_\mathfrak{p}^{res} \mathcal{R}_\mathfrak{p}$ le ℓ-adifié du groupe des idèles de K.

Du point de vue local, le noyau $\mathcal{U}_\mathfrak{p}$ de $\nu_\mathfrak{p}$ dans $\mathcal{R}_\mathfrak{p}$ (autrement dit le sous-groupe des unités de $\mathcal{R}_\mathfrak{p}$) est le groupe de normes associé à la $\mathbb{Z}_\ell$-extension non ramifiée de $K_\mathfrak{p}$; tandis que le noyau $\widetilde{\mathcal{U}}_\mathfrak{p}$ de $\widetilde{\nu}_\mathfrak{p}$ (*i.e.* le sous-groupe des unités logarithmiques) correspond, lui, à sa $\mathbb{Z}_\ell$-extension cyclotomique. Par la Théorie ℓ-adique du corps de classes (*cf.* [5, 9, 10]), le ℓ-goupe des classes d'idéaux s'interprète comme groupe de Galois de la ℓ-extension abélienne non ramifiée maximale K^{nr} de K ; et le ℓ-groupe des classes logarithmiques $\mathcal{C}\ell_K \simeq \mathcal{J}_K / \prod_\mathfrak{p} \widetilde{\mathcal{U}}_\mathfrak{p} \mathcal{R}_K$ comme groupe de Galois de sa pro-ℓ-extension abélienne localement cyclotomique maximale K^{lc}. Le corps K^{lc} est ainsi la plus grande pro-ℓ-extension abélienne de K qui est complètement décomposée au-dessus de la $\mathbb{Z}_\ell$-extension cyclotomique K^c. En particulier K^{lc} contient K^c et $\mathcal{C}\ell_K$ n'est jamais fini.

La surjection canonique du ℓ-adifié $\mathcal{J}_K$ du groupe des idèles de K dans le groupe procycliqe $\mathrm{Gal}(K^c/K) \simeq \mathbb{Z}_\ell$ fournit cependant un morphisme *degré* :

$$\deg : \mathcal{J}_K \to \mathbb{Z}_\ell \, ;$$

dont le noyau $\widetilde{\mathcal{J}}_K$ est, par construction, le sous-groupe normique de $\mathcal{J}_K$ attaché à K^c. Le noyau

$$\widetilde{\mathcal{C}\ell}_K \simeq \widetilde{\mathcal{J}}_K / \prod_{\mathfrak{p}} \widetilde{\mathcal{U}}_{\mathfrak{p}} \mathcal{R}_K \simeq \mathrm{Gal}(K^{lc}/K^c)$$

de l'application induite sur $\mathcal{C}\ell_K$ est ainsi le *groupe des classes logarithmiques de degré nul*, qui est l'objet de cette note.

La *Conjecture de Gross-Kuz'min* (pour le corps K et le premier ℓ) postule précisément la finitude de ce groupe. Comme expliqué dans [8], c'est une conséquence d'une conjecture plus générale d'indépendance ℓ-adique de nombres algébriques, qui résulte elle-même de la conjecture de Schanuel ℓ-adique.

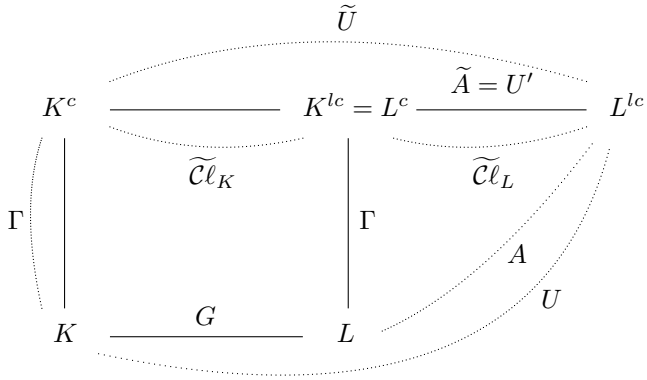
Comme établi par Greenberg, les résultats de transcendance de Baker-Brumer (*cf. e.g.* [5, 6, 8]) assurent que la conjecture de Gross-Kuz'min vaut en particulier dès que le corps considéré K est abélien sur $\mathbb{Q}$. La même conclusion vaut encore sous des hypothèses plus larges, lorsque K est totalement réel, en vertu d'un raffinement du théorème de Baker-Brumer dû à M. Waldschmidt et précisé par M. Laurent puis D. Roy (*cf.* [11]). Le cas général reste actuellement ouvert.

3. Le schéma galoisien de la capitulation

Partons donc d'un corps de nombre arbitraire, vérifiant la conjecture de Gross-Kuz'min pour un premier donné ℓ. Notons K^c sa $\mathbb{Z}_\ell$-extension cyclotomique de K et K^{lc} la pro-ℓ-extension abélienne localement cyclotomique de K. Comme expliqué plus haut, le groupe $\mathrm{Gal}(K^{lc}/K)$ s'identifie alors au pro-ℓ-groupe des classes logarithmiques $\mathcal{C}\ell_K$ de K et le sous-groupe $\mathrm{Gal}(K^{lc}/K^c)$ au ℓ-groupe $\widetilde{\mathcal{C}\ell}_K$ des classes logarithmiques de degré nul.

Soit maintenant L une ℓ-extension abélienne de K telle qu'on ait $LK^c = K^{lc}$ et $\widetilde{\mathcal{C}\ell}_L$ son (pro)-ℓ-groupe des classes logarithmiques de degré nul. Il s'agit de voir que $\widetilde{\mathcal{C}\ell}_K$ capitule dans $\widetilde{\mathcal{C}\ell}_L$. Quitte à remplacer L par un sous-corps convenable L', nous pouvons supposer L/K linéairement disjointe de K^c/K sans restreindre aucunement la généralité de notre preuve, puisque la capitulation dans $\widetilde{\mathcal{C}\ell}_{L'}$ entraînera la capitulation dans $\widetilde{\mathcal{C}\ell}_L$.

Cela fait, introduisons la pro-ℓ-extension abélienne localement cyclotomique maximale L^{lc} de L et notons G le groupe de Galois $\mathrm{Gal}(L/K)$. Le corps L^{lc} est lui-même une pro-ℓ-extension de K ; soit donc $U = \mathrm{Gal}(L^{lc}/K)$ son groupe de Galois et A le sous-groupe $\mathrm{Gal}(L^{lc}/L)$, qui s'identfie au pro-ℓ-groupe des classes logarithmiques $\mathcal{C}\ell_L$. Les sous-groupes de degré nul respectifs de U et de A (*i.e.* les noyaux des morphismes de restriction à K^c) sont respectivement $\widetilde{U} = \mathrm{Gal}(L^{lc}/K^c)$ et $\widetilde{A} = \mathrm{Gal}(L^{lc}/L^c) \simeq \widetilde{\mathcal{C}\ell}_L$; et $\widetilde{A}$ est aussi le sous-groupe dérivé de U, puisque $L^c = LK^c$ est, par construction la sous-extension maximale de L^{lc} qui est abélienne sur K. L'ensemble de cette discussion peut donc se résumer par le schéma de corps :



Maintenant, dans le formalisme du corps de classes, l'extension des idèles (côté arithmétique) correspond au transfert (côté théorie des groupes) ; de sorte que pour montrer que $\widetilde{\mathcal{C}\ell}_K$ capitule dans $\widetilde{\mathcal{C}\ell}_L$, il s'agit de vérifier que le transfert

$$\mathrm{Ver}_{U/A} : U/U' \to A$$

envoie le sous-groupe $\widetilde{U}/U'$ de degré nul de U/U' sur le sous-groupe nul de $\widetilde{A}$.

Il est classique de partir pour cela de l'isomorphisme $G = U/A \simeq \widetilde{U}/\widetilde{A}$ en faisant choix de représentants des classes de G formé d'éléments de $\widetilde{U}$, disons $(u_\tau)_{\tau \in G}$ (avec la convention $u_{\tau^{-1}} = u_\tau^{-1}$) et d'introduire le système de facteurs

$$a_{\sigma,\tau} = u_\sigma u_\tau u_{\sigma\tau}^{-1} \in \widetilde{A}$$

dont la classe dans $H^2(G, A)$ définit la loi sur U à isomorphisme près.

4. Interprétation en termes d'algèbre linéaire

En analogie avec le cas classique, nous pouvons alors constuire un $\mathbb{Z}_\ell$-module résolvant B en formant la somme directe :

$$B = A \oplus I_G = A \oplus (\underset{\tau \neq 1}{\oplus} \mathbb{Z}_\ell(\tau - 1)),$$

munie de l'action de G définie par :

$$\sigma * a = a^\sigma \qquad \& \qquad \sigma * (\tau - 1) = a_{\sigma,\tau} + \sigma(\tau - 1).$$

Suivant Artin-Tate (*cf.* [3], Ch. 13, §4), nous avons un diagramme commutatif :

$$\begin{array}{ccccc} \mathcal{C}\ell_K & \xrightarrow{\sim} & U/U' & \xrightarrow{\sim} & B/I_G * B \\ \downarrow{\scriptstyle j_{L/K}} & & \downarrow{\scriptstyle \mathrm{Ver}_{U/A}} & & \downarrow{\scriptstyle \mathrm{Tr}_{B/A}} \\ \mathcal{C}\ell_L & \xrightarrow{\sim} & A & = & A \end{array}$$

où l'isomorphime en haut à droite est donné par le *logarithme* :

$$au_\tau U' \mapsto a + (\tau - 1) + I_G * B\,;$$

de sorte que l'homomorphisme d'extension $j_{L/K}$ à gauche correspond au morphisme de transfert $\mathrm{Ver}_{U/A}$ au centre et à la trace $\mathrm{Tr}_{B/A} = \sum_{\tau\in G}\tau$ à droite.

Comme indiqué dans l'introduction, nous sommes intéressés par la restriction de $j_{L/K}$ au sous-groupe des classes logarithmiques de degré nul. Définissons donc le degré d'un élément $b = a + \sum \lambda_\tau(\tau - 1)$ de B par la formule : $\deg b = \deg a$. Le sous-module des éléments de degré nul dans B est alors :

$$\widetilde{B} = \widetilde{A} \oplus I_G = \widetilde{A} \oplus (\underset{\tau\neq 1}{\oplus} \mathbb{Z}_\ell(\tau - 1)).$$

Observons que $\widetilde{B}$ contient $I_G * B$; et que le quotient $\widetilde{B}/I_G * B$ est encore l'image par le logarithme du sous-groupe $\widetilde{U}/U'$ des éléments de degré nul du quotient U/U' ; ce que nous pouvons résumer par le diagramme commutatif :

$$\begin{array}{ccccc}
\widetilde{\mathcal{C}\ell}_K & \xrightarrow{\sim} & \widetilde{U}/U' & \xrightarrow{\sim} & \widetilde{B}/I_G * B \\
\Big\downarrow{\scriptstyle j_{L/K}} & & \Big\downarrow{\scriptstyle \mathrm{Ver}_{U/A}} & & \Big\downarrow{\scriptstyle \mathrm{Tr}_{B/A}} \\
\widetilde{\mathcal{C}\ell}_L & \xrightarrow{\sim} & \widetilde{A} & = & \widetilde{A}
\end{array}$$

En fin de compte, montrer que les classes logarithmiques de degré nul du corps K capitulent dans L revient à vérifier que pour $B = A \oplus I_G$, muni de l'action de G définie plus haut, l'opérateur trace $\mathrm{Tr}_{B/A} = \sum_{\tau\in G}\tau$ est nul sur le sous-module $\widetilde{B} = \widetilde{A} \oplus I_G$.

Avant d'aller plus loin, il peut être intéressant de préciser le dénominateur $I_G * B$ qui intervient dans le quotient à droite du diagramme : l'isomomorphisme canonique de $\mathbb{Z}_\ell[G]$-modules $B/A \simeq I_G$ nous donne l'inclusion : $I_G * B \subset A \oplus I_G^2$.

Pour établir l'égalité, il suffit par conséquent de comparer les deux indices $(\widetilde{B} : I_G * B)$ et $(\widetilde{B} : \widetilde{A} \oplus I_G^2)$. Or, nous avons :

- d'un côté $\widetilde{B}/I_G * B \simeq \widetilde{U}/U' \simeq \widetilde{\mathcal{C}\ell}_K \simeq G$, conformément au diagramme ;
- et directement : $\widetilde{B}/(\widetilde{A} \oplus I_G^2) = (\widetilde{A} \oplus I_G)/(\widetilde{A} \oplus I_G^2) \simeq I_G/I_G^2 \simeq G$;

d'où l'égalité annoncée :

$$I_G * B = \widetilde{A} \oplus I_G^2.$$

5. Approche par la méthode d'Artin-Furtwängler

La méthode classique, telle qu'exposée dans [3], consiste à écrire le ℓ-groupe G comme produit direct de s sous-groupes cycliques $\langle\tau_i\rangle$ d'ordres respectifs e_i ; et à considérer les éléments $b_i = \tau_i - 1$ de $\widetilde{B}$ pour $i = 1, \cdots, s$.

Dans le cas classique le module résolvant B est engendré par les $(b_i)_i$; dans le cadre logarithmique qui nous intéresse ici, c'est plus compliqué, du fait qu'il nous faut considérer le sous-module $\widetilde{B}$ des éléments de degré nul.

Relevons $\Gamma = \mathrm{Gal}(K^c/K)$ dans $U = \mathrm{Gal}(L^{lc}/K$ en faisant choix d'un prolongement γ à L^{lc} d'un progénérateur arbitraire de Γ. L'isomorphisme

$$B/I_G * B \simeq U/U' \simeq \Gamma \times G$$

montre que B est engendré, comme $\mathbb{Z}_\ell[G]$-module, conjointement par γ et les $(b_i)_i$. Et les identités $e_j b_i \in I_G * B$ s'écrivent ainsi :

$$e_i b_i = \sum_{j=1}^{s} \lambda_{ij} * b_j + \mu_i * \gamma$$

avec les λ_{ij} et les μ_i dans I_G. Notant alors M la matrice de terme général $m_{ij} = e_i\delta_{ij} - \lambda_{ij}$, nous obtenons :

$$M * \begin{bmatrix} b_1 \\ \vdots \\ b_s \end{bmatrix} = \begin{bmatrix} \mu_1 \\ \vdots \\ \mu_s \end{bmatrix} * \gamma\,;$$

puis, par multiplication à gauche par la transcomatrice $\widetilde{M}$ de M :

$$\det M * \begin{bmatrix} b_1 \\ \vdots \\ b_s \end{bmatrix} = \widetilde{M}M * \begin{bmatrix} b_1 \\ \vdots \\ b_s \end{bmatrix} = \widetilde{M} \begin{bmatrix} \mu_1 \\ \vdots \\ \mu_s \end{bmatrix} * \gamma = \begin{bmatrix} \nu_1 \\ \vdots \\ \nu_s \end{bmatrix} * \gamma$$

c'est-à-dire : $\det M * b_i = \nu_i * \gamma$ pour un ν_i de I_G, pour chaque $i = 1, \cdots, s$.

L'isomorphisme $\widetilde{B}/\widetilde{A} \simeq I_G$ montre alors que $\det M \in \mathbb{Z}_\ell[G]$ est un multiple de la trace, disons : $\det M = \kappa\,\mathrm{Tr}_{B/A}$, pour un κ dans $\mathbb{Z}_\ell$. Et un calcul de degré dans l'algèbre de groupe donne alors directement :

$$\deg(\det M) = \det([\deg(m_{ij})]_{ij}) = \det([e_i\delta_{ij}]_{ij}) = \prod e_i = \mid G \mid = \deg \mathrm{Tr}_{B/A}\,;$$

d'où, comme attendu : $\det M = \mathrm{Tr}_{B/A}$ et finalement l'inclusion :

$$\mathrm{Tr}_{B/A}(\widetilde{B}) \subset I_G * \gamma$$

puisque $\widetilde{B}$ est $\mathbb{Z}_\ell[G]$-engendré par les b_i (pour $i = 1, \ldots, s$) et $I_G * \gamma$; de sorte que $\mathrm{Tr}_{B/A}(\widetilde{B})$ est engendré par les $\mathrm{Tr}_{B/A}(b_i)$ pour $i = 1, \ldots, s$. Ainsi :

Proposition 1. *Avec les notations ci-dessus, l'image dans $\mathcal{C}\ell_L$ du sous-groupe des classes logarithmiques de degré nul $\widetilde{\mathcal{C}\ell}_K$ s'identifie au sous-module $\mathrm{Tr}_{B/A}(\widetilde{B})$ du $\mathbb{Z}_\ell[G]$-module $I_G * \gamma$ construit sur un relèvement du groupe procyclique Γ.*

Remarque. La méthode ne donne donc pas la trivialité du groupe $\mathrm{Tr}_{B/A}(\widetilde{B})$, comme dans le cas classique, mais seulement une inclusion.

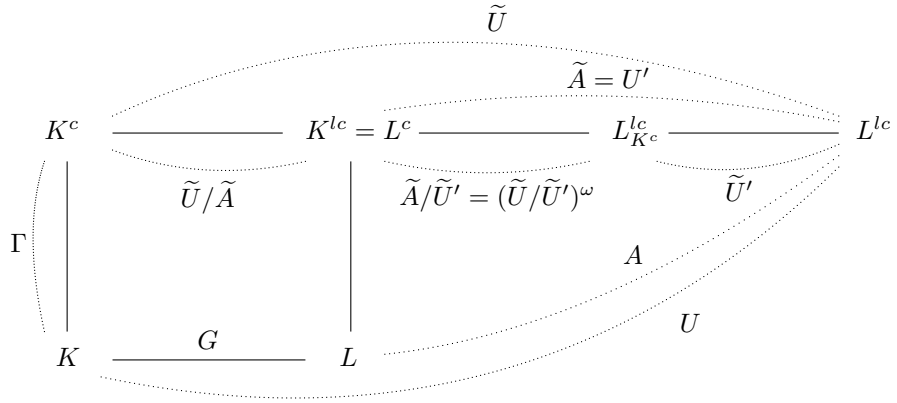
6. Interprétation en termes de théorie des genres

Pour aller plus loin dans la description de la capitulation logarithmique, nous pouvons nous inspirer des méthodes initiées par T. Tannaka et F. Terada pour généraliser le *Théorème de l'idéal principal* dans le contexte de la théorie cyclique des genres (*cf.* [13, 14, 15, 16]).

Introduisons le sous-corps $L^{lc}_{K^c}$ de L^{lc} fixé par le sous-groupe dérivé $\widetilde{U}'$ de $\widetilde{U} = \mathrm{Gal}(L^{lc}/K^c)$. Par construction $L^{lc}_{K^c}/K^c$ est la plus grande sous-extension de L^{lc}/K^c qui est abélienne sur K^c et nous avons : $\mathrm{Gal}(L^{lc}_{K^c}/L^c) \simeq \widetilde{A}/\widetilde{U}'$. Cela étant, L^c, qui est la plus grande sous-extension de $L^{lc}_{K^c}/K^c$ qui provient par composition avec K^c d'une extension abélienne de K, est donc le corps des genres de $L^{lc}_{K^c}$ relativement à l'extension procyclique K^c/K ; en particulier $\mathrm{Gal}(L^c/K^c)$ est le plus grand quotient de $\widetilde{U}/\widetilde{U}' = \mathrm{Gal}(L^{lc}_{K^c}/K^c)$ sur lequel $\Gamma = \mathrm{Gal}(K^c/K)$ opère trivialement ; et nous avons donc : $\mathrm{Gal}(L^{lc}_{K^c}/L^c) \simeq (\widetilde{U}/\widetilde{U}')^{\omega}$; d'où, finalement :

$$\widetilde{A}/\widetilde{U}' = (\widetilde{U}/\widetilde{U}')^{(\gamma-1)},$$

si γ désigne un relèvement arbitraire dans $A = \mathrm{Gal}(L^{lc}/K)$ d'un générateur topologique de Γ. Et l'ensemble de cette discussion peut être résumé par le schéma de corps :



où nous avons noté $\omega = \gamma - 1$.

Précisons quelques points. Comme $\Gamma \simeq \gamma^{\mathbb{Z}_\ell}$ opère trivialement sur le quotient $U/A \simeq G$, nous pouvons écrire :

$$u_\tau^\gamma = \gamma u_\tau \gamma^{-1} = a_\tau u_\tau$$

pour tout $\tau \in G$, avec

$$a_\tau = u_\tau^\gamma u_\tau^{-1} = [\gamma, u_\tau] = \gamma^{1-\tau} ;$$

Convenons de noter $\widetilde{U}^\omega$ le sous-groupe de $\widetilde{A}$ qui est engendré par les a_τ lorsque τ décrit G. Cela étant, nous avons :

Lemme 2. *Avec ces conventions, il vient :* $\widetilde{A} = \widetilde{U}'\widetilde{U}^{\omega}$.

Preuve. C'est une conséquence immédiate de l'égalité $\widetilde{A}/\widetilde{U}' = (\widetilde{U}/\widetilde{U}')^{(\omega)}$ donnée par la théorie des genres. ■

7. Approche par la méthode de Tannaka-Terada

Revenons maintenant sur le module résolvant B. Rappelons que nous avons fait choix d'un relèvement γ dans $A = \mathrm{Gal}(L^{lc}/L)$ d'un générateur topologique de Γ, ce qui nous a permis de définir les éléments a_τ pour $\tau \in G$. En termes d'algèbre linéaire, *i.e.* en notations additives, il vient ainsi :

$$a_\tau = u_\tau^{\gamma} u_\tau^{-1} = [\gamma, u_\tau] = \gamma^{1-\tau} = (1-\tau) * \gamma \in I_G * \gamma \subset \widetilde{A}\,;$$

et nous pouvons transporter l'action de Γ sur U au module B en posant :

$$\gamma * (\tau - 1) = a_\tau + (\tau - 1).$$

En particulier B peut ainsi être regardé comme un module sur l'algèbre $\Lambda[G]$ construite sur l'algèbre d'Iwasawa $\Lambda = \mathbb{Z}_\ell[[\omega]]$ en l'indéterminée $\omega = \gamma - 1$. De fait l'identité ci-dessus donne immédiatement :

$$\omega^2 * (\tau - 1) = \omega * a_\tau = 0,$$

de sorte que B est annulé par ω^2. Plus précisément :

Lemme 3. *Avec les conventions précédentes, on a :* $\omega * \widetilde{B} = \widetilde{U}^{\omega} = I_G * \gamma$. *Et* $\widetilde{B}$ *est* $\Lambda[G]$*-engendré par les éléments* $b_i = \tau_i - 1$*, pour* $i = 1, \ldots, s$.

Preuve. Il vient, effet :

$$\omega * \widetilde{B} = \omega * (\widetilde{A} \oplus I_G) = \omega * I_G = \sum_{\tau \in G} \mathbb{Z}_\ell\ \omega * (\tau - 1) = \sum\nolimits_{\tau \in G} \mathbb{Z}_\ell\ a_\tau = \widetilde{U}^{\omega}\,;$$

d'où, par passage au quotient à partir de l'isomorphisme : $\widetilde{B}/I_G * \widetilde{B} \simeq \widetilde{U}/\widetilde{U}'$:

$$\widetilde{B}/(I_G * \widetilde{B} + \omega * \widetilde{B}) \simeq \widetilde{U}/\widetilde{U}'\widetilde{U}^{\omega} = \widetilde{U}/\widetilde{A} \simeq G\,;$$

de sorte que $\widetilde{B}$, regardé comme $\Lambda[G]$-module, est engendré par les s éléments $b_i = \tau_i - 1$ construits sur un système minimal de générateurs de G. ■

Ce point acquis, les identités $e_j b_i \in I_G * B + \omega * \widetilde{B}$ s'écrivent :

$$e_i b_i = \sum_{j=1}^{s} \mu_{ij} * b_j + \omega * \sum_{j=1}^{s} \nu_{ij} * b_j$$

avec les μ_{ij} dans I_G et les ν_{ij} dans $\mathbb{Z}_\ell[G]$. Notant alors M la matrice de terme général $m_{ij} = e_i\delta_{ij} - \lambda_{ij}$ et N celle de terme général ν_{ij}, nous obtenons :

$$[M - \omega N] * \begin{bmatrix} b_1 \\ \vdots \\ b_s \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix} ; \qquad \text{donc : } \det[M - \omega N] * \widetilde{B} = 0.$$

Un calcul modulo $\widetilde{A}$ montre alors, comme précédemment, que le déterminant de la matrice M coïncide avec la trace $\mathrm{Tr}_{B/A}$, de sorte que le déterminant $d = \det[M - \omega N]$ (calculé modulo ω^2) est de la forme :

$$d = \mathrm{Tr}_{B/A} - \omega\delta$$

pour un certain $\delta \in \mathbb{Z}_\ell[G]$. En particulier :

Proposition 4. *Comme opérateur sur $\widetilde{B}$, la trace s'écrit : $\mathrm{Tr}_{B/A} = \omega\delta$; et il suit :*

$$\mathrm{Tr}_{B/A}(\widetilde{B}) = \delta\omega * \widetilde{B} = \delta I_G * \gamma.$$

8. Capitulation des classes invariantes

La Proposition 4 ci-dessus précise naturellement le résultat obtenu à la fin de la section 5 par le procédé d'Artin-Furtwängler, puisqu'elle décrit précisément le sous-module image $\mathrm{Tr}_{B/A}(\widetilde{B})$ des classes logarithmique étendues ; mais elle ne donne pas d'information directe sur le sous-groupe de $\widetilde{\mathcal{C}\ell}_K$ qui capitule dans $\widetilde{\mathcal{C}\ell}_L$. Nous allons voir que la méthode de Tannaka-Terada donne cependant des éléments de réponse :

Théorème 5. *Le noyau de la trace $\mathrm{Tr}_{B/A}$ regardé dans le quotient $\widetilde{B}/I_G * \widetilde{B}$ contient le sous-groupe ambige $(\widetilde{B}/I_G * \widetilde{B})^\Gamma = {}^{-1}\omega(I_G * \widetilde{B})/I_G * \widetilde{B}$.*

En d'autres termes, on a l'implication :

$$\omega(\widetilde{b}) \in I_G * \widetilde{B} \Rightarrow \mathrm{Tr}_{B/A}(\widetilde{b}) = 0.$$

Remarque. Le quotient $\widetilde{B}/I_G * \widetilde{B} \simeq \widetilde{U}/\widetilde{U}'$ est annulé par ω^2. Le théorème affirme seulement que le sous-groupe annulé par ω est contenu dans le noyau de $\mathrm{Tr}_{B/A}$.

Preuve. Le noyau $\widetilde{A} \cap I_G * \widetilde{B}$ du morphisme naturel $A \to \widetilde{B}/I_G * \widetilde{B} \simeq \widetilde{U}/\widetilde{U}'$ étant $\widetilde{U}'$, nous avons $\widetilde{A} \cap I_G * \widetilde{B} = \widetilde{U}'$, donc :

$$\omega\widetilde{B} \cap I_G * \widetilde{B} = \omega\widetilde{B} \cap \widetilde{A} \cap I_G * \widetilde{B} = \widetilde{U}^\omega \cap \widetilde{U}'.$$

Et le Théorème sera établi si nous montrons que l'opérateur δ est nul sur $\widetilde{U}'$.

Observons pour cela que le groupe $\widetilde{U}$ est engendré par $\widetilde{A}$ et les $(u_\tau)_{\tau\in G}$; de sorte que son sous-groupe dérivé $\widetilde{U}'$, lui, est engendré conjointement

- par les commutateurs $[a, u_\tau] = a^{(1-\tau)}$ avec $a \in \widetilde{A}$ et $\tau \in G$ et
- par les $[u_\sigma, u_\tau]$, lorsque σ et τ parcourent un système générateur de G.

Introduisons le sous-module $\partial\widetilde{B}$ de $\widetilde{B}$ qui est engendré par les commutateurs :

$$[b_i, b_j] = b_i * b_j - b_j * b_i = (\tau_i - 1)*(\tau_j - 1) - (\tau_j - 1)*(\tau_i - 1) = a_{\tau_i,\tau_j} - a_{\tau_j,\tau_i}.$$

Traduites en notations additives, les observations précédentes nous donnent l'identité :

$$\widetilde{U}' = I_G * A + \partial\widetilde{B}.$$

Supposons établie la trivialité de δ sur le sous-module $\partial\widetilde{B}$. Il vient alors :

$$\delta * \widetilde{U}' = \delta * I_G * \widetilde{A} = \delta I_G * (\widetilde{U}' + \omega * \widetilde{B}) = I_G * (\delta * \widetilde{U}') ;$$

d'où :

$$\delta * \widetilde{U}' = 0,$$

ce qui est précisément le résultat attendu. ■

Ainsi, le Théorème résulte du :

Lemme 6 (Lemme d'Adachi). *L'opérateur δ est nul sur le sous-module $\partial\widetilde{B}$.*

Preuve. Il s'agit de vérifier que l'on a : $\delta b_i * b_j = \delta b_j * b_i$, pour tout (i, j) ; ce qui se fait en transposant *mutatis mutandis* dans le cadre procyclique considéré ici les calculs de déterminants effectués par N. Adachi dans son rapport sur le Théorème de l'idéal principal [1] consacré au Théorème de Tannaka-Terada. ■

Remarque. Le quotient $\widetilde{B}/I_G*\widetilde{B} \simeq \widetilde{U}/\widetilde{U}'$ étant réputé fini, le noyau de ω regardé comme endomorphisme de $\widetilde{B}/I_G * \widetilde{B}$, a même ordre que son conoyau. On a donc :

$$({}^{-1}\omega(I_G * \widetilde{B}) : I_G * \widetilde{B}) = (\widetilde{U} : \widetilde{U}'\widetilde{U}^{\omega}) = (\widetilde{U} : \widetilde{A}) = |G|.$$

Et le *noyau de capitulation* est au moins d'ordre $|G| = |\widetilde{\mathcal{C}\ell}_K|$ (mais dans $\widetilde{U}/\widetilde{U}'$).

9. Conclusion

Contrairement à ce qui se produit pour les ℓ-groupes de classes au sens habituel, on voit que les méthodes classiques, même très élaborées, ne permettent pas de conclure dans le cadre logarithmique à un analogue complet du résultat d'Artin-Furtwängler, puique la capitulation y apparait comme un sous-groupe éventuellement strict du groupe des classes total.

De fait cette observation, a priori décevante, se trouve confirmée par l'expérimentation numérique. Donnons un contre-exemple simple qui ruine clairement tout espoir de transposer naïvement dans le cadre logarithmique le classique théorème 94 de Hilbert sur la capitulation :

Scolie 7. *Pour $\ell = 3$, il existe des corps quadratiques imaginaires K dont le 3-groupe des classes logarithmiques de degré nul est cyclique d'ordre 3 et qui possèdent une extension cyclique L de degré $[L : K] = 3$ logarithmiquement non ramifiée pour lesquelles l'homomorphisme $j_{L/K} : \widetilde{\mathcal{C}\ell}_K \to \widetilde{\mathcal{C}\ell}_L$ est injectif.*

Preuve. Sous la conjecture de Gross-Kuz'min (et donc en pratique dans tous les exemples numériques étudiés), le quotient de Herbrand $q(G,\widetilde{\mathcal{E}}_L)$ attaché aux unités logarithmiques dans une extension cyclique L/K vaut 1, en vertu de l'expression du caractère du $\mathbb{Z}_\ell[G]$-module $\widetilde{\mathcal{E}}_L$ donnée dans [9]. En particulier, dès que le groupe $H^2(G,\widetilde{\mathcal{E}}_L)$ est trivial, il en est de même du groupe $H^1(G,\widetilde{\mathcal{E}}_L)$ qui s'identifie précisément à la capitulation logarithmique Ker $j_{L/K}$. Les calculs numériques effectués par Karim Belabas avec PARI, montrent que c'est, par exemple, le cas pour $K=\mathbb{Q}[\sqrt{-31}]$ et $L=K[x]$, où x est racine du polynôme $X^3+3X+(\theta+9)/2$ avec $\theta^2=-31$. ■

On voit par là une différence essentielle d'avec le cas des groupes de classes au sens habituel : pour les unités au sens ordinaire, le quotient de Herbrand $q(G,E_L)$ relatif à une extension cyclique de corps de nombres L/K n'est jamais trivial ; il est égal au degré $[L:K]$ de l'extension, de sorte que le premier groupe de cohomologie $H^1(G,E_L)$, qui mesure précisément la capitulation dès lors que l'extension considérée L/K est non ramifiée, n'est pas trivial non plus. Et c'est la clef du théorème 94. Dans le cadre logarithmique en revanche, la trivialité du quotient de Herbrand interdit toute minoration de la capitulation ; ce que confirme le calcul.

A contrario, le même argument fournit une majoration de la capitulation logarithmique meilleure que celle que l'on a dans le cas classique :

Proposition 8. *Soient L/K une ℓ-extension cyclique de corps de nombres logarithmiquement non ramifiée et G son groupe de Galois. Sous la conjecture de Gross-Kuz'min, l'ordre du sous-groupe des classes logarithmiques de K qui capitulent dans L satisfait la majoration :*

$$|\widetilde{Cap}_{L/K}| = |H^1(G,\widetilde{\mathcal{E}}_L)| = |H^2(G,\widetilde{\mathcal{E}}_L)| \leqslant (r_K + c_K + \delta_K)^{[L:K]},$$

où r_K et c_K représentent les nombres de places réelles et complexes du corps K et δ_K vaut 0 ou 1 suivant que K contient ou pas les racines ℓ-ièmes de l'unité.

Preuve. Le groupe $\widetilde{\mathcal{E}}_K$ des unités logarithmiques de K est alors, en effet, le produit du sous-groupe μ_K des racines d'ordre ℓ-primaire de l'unité contenues dans K et d'un $\mathbb{Z}_\ell$-module libre de dimension r_K+c_K (cf. [9], §3). ■

Références

[1] N. Adachi, *Reports on principal ideal theorems*, Mem. School Sci. Engin., Waseda Univ. **37** (1973), 81–90.

[2] E. Artin, *Idealklassen in Oberkörpern und allgemeine Rezprozitätsgesetz*, Abh. Math. Sem. Hamburg **7** (1930), 46–51.

[3] E. Artin & J. Tate *Class Field Theory*, Addison-Wesley (1968).

[4] P. Furtwängler, *Beweis des Hauptidealsatzes für die Klassenkörper algebraischer Zahlkörper*, Abh. Math. Sem. Hamburg **7** (1930), 14–36.

[5] G. Gras, *Class Field Theory: From Theory To Practice*, Springer-Verlag, 2003.

[6] R. Greenberg, *On a certain ℓ-adic representation*, Inv. Math. **21** (1973) 117–124.
[7] J. Herbrand, *Sur les théorèmes du genre principal et des idéaux principaux*, Abh. Math. Sem. Hamburg **9** (1932), 84–92.
[8] J.-F. Jaulent, *Sur l'indépendance ℓ-adique de nombres algébriques*, J. Numb. Th. **20** (1985), 149–158 .
[9] J.-F Jaulent, *Classes logarithmiques des corps de nombres*, J. Théor. Nombres Bordeaux **10** (1994), 301–325.
[10] J.-F. Jaulent, *Théorie ℓ-adique globale du corps de classes*, J. Théor. Nombres Bordeaux **10** (1998), 355–397.
[11] J.-F. Jaulent, *Classes logarithmiques des corps totalement réels*, Acta Arithmetica **103** (2002), 1–7.
[12] L. V. Kuz'min, *The Tate module of algebraic number fields*, Izv. Akad. Nauk SSSR Ser. Mat. **36** (1972), 267-327.
[13] T. Tannaka & F. Terada, *A generalization of the principal ideal theorem*, Proc. Japan Acad. **25** (1949), 7–8.
[14] T. Tannaka, *Some remarks concerning the principal ideal theorem*, Tôhoku Math. J. **1** (1949), 270–278.
[15] F. Terada, *On a generalization of the principal ideal theorem*, Tôhoku Math. J. **1** (1949), 229–269.
[16] F. Terada, *A principal ideal theorem in the genus field*, Tôhoku Math. J. **23** (1971), 697–718.

Address: Jean-François Jaulent: Univ. Bordeaux & CNRS, Institut de Mathématiques de Bordeaux, UMR 5251, 351 Cours de la Libération, F-33405 Talence cedex, France.

E-mail: jean-francois.jaulent@math.u-bordeaux1.fr

Received: 30 March 2015; **revised:** 11 September 2015

Functiones et Approximatio
54.2 (2016), 241–250
doi: 10.7169/facm/2016.54.2.7

COMPARING LOCAL CONSTANTS OF ORDINARY ELLIPTIC CURVES IN DIHEDRAL EXTENSIONS

Sunil Chetty

Abstract: We establish, for a substantial class of elliptic curves, that the arithmetic local constants introduced by Mazur and Rubin agree with quotients of analytic root numbers.

Keywords: elliptic curves, rank, Selmer groups, parity conjecture.

1. Introduction

Let E/k be an elliptic curve over a number field k. Fix a rational prime $p > 3$ for which E is ordinary[1] and a quadratic extension K of k. Next, fix a character ρ of $\mathrm{Gal}(\overline{k}/K)$ of order p^n and let $\tau_\rho = \mathrm{ind}_{K/k}\,\rho$ and $\tau_1 = \mathrm{ind}_{K/k}\,1$ be the induced representations[2] from $\mathrm{Gal}(\overline{k}/K)$ to $\mathrm{Gal}(\overline{k}/k)$. With ρ we define $L = \overline{k}^{\ker\rho}$, a cyclic extension L/K of degree p^n, and we assume ρ is such that L/k is Galois and that the non-trivial element $c \in \mathrm{Gal}(K/k)$ acts on $g \in \mathrm{Gal}(L/k)$ via conjugation as $cgc^{-1} = g^{-1}$. Following [9] we refer to such extensions L/k as dihedral.

Let v denote a prime of K, u the prime of k below v, w a prime of L above v, and denote k_u, K_v and L_w for the completions at u, v, and w. We consider $\mathrm{Gal}(L_w/k_u) \leqslant \mathrm{Gal}(L/k)$, and we set $\tau_{\rho,u}$ (resp. $\tau_{1,u}$) to be τ_ρ (resp. τ_1) restricted to $\mathrm{Gal}(L_w/k_u)$.

For a self-dual complex representation τ of $\mathrm{Gal}(L/k)$, one has a conjectural functional equation for the completed L-function $\Lambda(E/k,\tau,s)$ (see [12, §21])

$$\Lambda(E/k,\tau,s) = \left(\prod_u W(E/k_u,\tau_u)\right)\Lambda(E/k,\tau,2-s), \tag{1.1}$$

This material is based upon work supported by the National Science Foundation under grant DMS-0457481. The author would like to thank Karl Rubin for his many helpful conversations on this material and reading of initial drafts of this paper.

2010 Mathematics Subject Classification: primary: 11G05; secondary: 11G07, 11G40

[1] There is, to date and to our knowledge, only one result [9, Theorem 5.7] at supersingular primes analogous to our considerations.

[2] Context will determine the field of values. See [7, §5] for a discussion of this.

with $W(E/k_u, \tau_u) \in \{\pm 1\}$ and the product taken over places u of k. Even though the functional equation is conjectural, the $W(E/k_u, \tau_u)$ can often be made explicit.

In [9] Mazur and Rubin define constants δ_v, for each prime v of K, which relate the ρ-part and 1-part of the pro-p-Selmer $\mathrm{Gal}(\bar{k}/K)$-module $\mathcal{S}_p(E/L)$ (see §2.2)

$$\dim_{\overline{\mathbb{Q}}_p} \mathcal{S}_p(E/L)^\rho - \dim_{\overline{\mathbb{Q}}_p} \mathcal{S}_p(E/L)^1 \equiv \sum_v \delta_v \mod 2. \tag{1.2}$$

Defining γ_u by $(-1)^{\gamma_u} = W(E/k_u, \tau_{\rho,u})/W(E/k_u, \tau_{1,u})$, for each prime u of k, the invariance of $\Lambda(E/k, \tau, s)$ under induction (see [12, §8]) and (1.1) give

$$\mathrm{ord}_{s=1}\, \Lambda(E/k, \tau_\rho, s) - \mathrm{ord}_{s=1}\, \Lambda(E/k, \tau_1, s) \equiv \sum_u \gamma_u \mod 2. \tag{1.3}$$

With the Shafarevic-Tate and Birch-Swinnerton-Dyer Conjectures in mind, the left-hand sides of (1.2) and (1.3) are equal, and so we aim to show in as many cases as possible that $\gamma_u = \sum_{v|u} \delta_v$.

Our main new result is Theorem 4.1, and it yields a new proof of a case of a relative version of the Parity Conjecture, Corollary 4.2. This Corollary is already known by different methods via work by de la Rochefoucauld in [1], Dokchitser and Dokchitser in [3] and [2], and can also be recovered from work by Greenberg in [5, §13]. Our calculations of δ_v in bad reduction also provide a new extension of the results of [9, §7-8] regarding growth in rank of $\mathcal{S}_p(E)$ over dihedral L/K, for example by relaxing the conditions in Theorem 8.5 of [9].

2. Local constants of elliptic curves

In this section we recall the relevant parts of [13] and [9].

2.1. Analytic local constants

We denote ω_u for the standard valuation on k_u and c_6 for the constant appearing in a simplified Weierstrauss model for E/k_u (see [17, §III.1]). For τ a representation of $\mathrm{Gal}(\bar{k}_u/k_u)$ with real-valued character, we call $W(E/k_u, \tau) \in \{\pm 1\}$ the analytic local root number for the pair $(E/k_u, \tau)$. We call the constants $\gamma_u \in \mathbb{Z}/2\mathbb{Z}$ defined as quotients of local root numbers in §1 the analytic local constants.

When τ has finite image, set $\mathfrak{c}(\tau) := \det \tau(-1)$ and for two representations τ and τ' of $\mathrm{Gal}(\bar{k}_u/k_u)$ with finite image define $\langle \tau, \tau' \rangle := \langle \mathrm{tr}(\tau), \mathrm{tr}(\tau') \rangle$, with the right-hand side the usual inner product on characters.

Let H be the unramified quadratic extension of k_u and η the unramified quadratic character of $\mathrm{Gal}(\bar{k}_u/k_u)$, i.e. the character of $\mathrm{Gal}(\bar{k}_u/k_u)$ with kernel $\mathrm{Gal}(\bar{k}_u/H)$. For $e = 3,\ 4$, or 6 and $q \equiv -1 \mod e$, where $q = \#(k_u/u)$, let ϕ_e be a tamely ramified character of $\mathrm{Gal}(\bar{k}_u/H)$ with $\phi_e|_{\mathcal{O}_H^\times}$ of exact order e and such that $\sigma_e = \mathrm{ind}_{H/k}\, \phi_e$ is irreducible and symplectic. For θ the unramified quadratic character of $\mathrm{Gal}(\bar{k}_u/H)$ set $\hat{\sigma}_e := \mathrm{ind}_{H/k_u}(\phi_e \theta)$, which is a dihedral representation of $\mathrm{Gal}(\bar{k}_u/k_u)$ (see p. 316-318 of [13]).

Define a representation σ_{E/k_u} by applying the results of [12, §4] to

$$\sigma_{E/k_u,\ell} : \mathrm{Gal}(\overline{k}_u/k_u) \to \mathrm{GL}(V_\ell(E)^*),$$

where $V_\ell(E)^*$ is the dual of $V_\ell(E) = T_\ell(E) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$. From

$$W(E/k_u, \tau) = W(\sigma_{E/k_u} \otimes \tau),$$

Rohrlich proves the following formulae.

Theorem 2.1 (Theorem 2 of [13]). *Suppose $\tau = \bar{\tau}$ is a 2-dimensional representation of $\mathrm{Gal}(\overline{k}_u/k_u)$ and denote ℓ for the residue characteristic of k_u.*

(i) *If $\ell = \infty$ then $W(E/k_u, \tau) = (-1)^{dim\ \tau} = 1$.*
(ii) *If $\ell < \infty$ and E has good reduction over k_u then $W(E/k_u, \tau) = \mathfrak{c}(\tau)$.*
(iii) *If $\ell < \infty$ and $\omega_u(j) < 0$ then*

$$W(E/k_u, \tau) = \mathfrak{c}(\tau)(-1)^{\langle \chi, \tau \rangle}$$

where χ is the character associated to the extension $k_u(\sqrt{-c_6})$.
(iv) *If $5 \leqslant \ell < \infty$, $\omega_u(j) \geqslant 0$, and $e = \frac{12}{gcd(\omega_u(\Delta_E), 12)}$*

$$W(E/k_u, \tau) = \begin{cases} \mathfrak{c}(\tau) & \text{if } q \equiv 1 \mod e \\ \mathfrak{c}(\tau)(-1)^{\langle 1, \tau \rangle + \langle \eta, \tau \rangle + \langle \hat{\sigma}_e, \tau \rangle} & \text{if } e > 2,\ q \equiv -1 \mod e. \end{cases}$$

Proposition 2.2 (Proposition 7 of [13]). *If $\sigma_{E/k_u} = \psi \oplus \psi^{-1}$ for some character ψ of $k_u^\times$ and τ is as in Theorem 2.1, then $W(E/k_u, \tau) = \mathfrak{c}(\tau)$.*

2.2. Arithmetic local constants

Let $\mathrm{Sel}_{p^\infty}(E/K)$ be the p^∞-Selmer group of E (see [9, §2] or [4, §2]). Define the pro-p Selmer group of E over K as the Pontrjagin dual of $\mathrm{Sel}_{p^\infty}(E/K)$

$$\mathcal{S}_p(E/K) := \mathrm{Hom}(\mathrm{Sel}_{p^\infty}(E/K), \mathbb{Q}_p/\mathbb{Z}_p),$$

and consider it as a $\bar{\mathbb{Q}}_p$-module by tensoring with $\bar{\mathbb{Q}}_p$.

When $L_w \neq K_v$, let L'_w be the unique subfield of L_w containing K_v with $[L_w : L'_w] = p$, and otherwise let $L'_w := L_w = K_v$.

Definition 2.3 (Corollary 5.3 of [9])**.** For each prime v of K, define the arithmetic local constant $\delta_v = \delta(v, E, \rho) \in \mathbb{Z}/2\mathbb{Z}$ to be

$$\delta_v := \dim_{\mathbb{F}_p} E(K_v)/(E(K_v) \cap \mathrm{N}_{L_w/L'_w} E(L_w)) \mod 2.$$

Theorem 2.4 (Theorem 6.4 of [9]). *If S is a set of primes of K containing all primes above p, all primes ramified in L/K, and all primes where E has bad reduction, then*

$$\dim_{\overline{\mathbb{Q}}_p} \mathcal{S}_p(E/L)^\rho - \dim_{\overline{\mathbb{Q}}_p} \mathcal{S}_p(E/L)^1 \equiv \sum_{v \in S} \delta_v \mod 2.$$

Proof. Following the notation of [9, §3], let R be the maximal order in in the cyclotomic field of p^n-roots of unity, so R has a unique prime $\mathfrak{p}$ above p. Define $\mathcal{I} := \mathfrak{p}^{p^{n-1}}$ and define the $\mathcal{I}$-twist of E by $A := \mathcal{I} \otimes E$ (in the sense of [10] and [9]), an abelian variety with $R \subset \mathrm{End}_K(A)$. We then have

$$\dim_{\overline{\mathbb{Q}}_p} \mathcal{S}_p(E/L)^\rho = \mathrm{corank}_{R\otimes\mathbb{Z}_p} \mathrm{Sel}_{p^\infty}(A/K),$$
$$\dim_{\overline{\mathbb{Q}}_p} \mathcal{S}_p(E/L)^1 = \mathrm{corank}_{\mathbb{Z}_p} \mathrm{Sel}_{p^\infty}(E/K).$$

Thus the conclusion above is equivalent to Theorem 6.4 of [9]

$$\mathrm{corank}_{R\otimes\mathbb{Z}_p} \mathrm{Sel}_{p^\infty}(A/K) - \mathrm{corank}_{Z_p} \mathrm{Sel}_{p^\infty}(E/K) \equiv \sum_{v\in S} \delta_v \mod 2. \qquad \blacksquare$$

3. Local computations

We keep the setting and notation of Theorem 2.1 and §1. Recall that c is the non-trivial element of $\mathrm{Gal}(K/k)$.

3.1. Preliminary calculations

Proposition 3.1. *If $v^c \neq v$, then $\gamma_u \equiv \delta_v + \delta_{v^c} \equiv 0$.*

Proof. When $v \neq v^c$, we have $\mathrm{Gal}(L_w/k_u) = \mathrm{Gal}(L_w/K_v)$. It follows that $\tau_{\rho,u} = \rho \oplus \rho^{-1}$ and $\tau_{1,u} = 1 \oplus 1$, so $\det \tau(-1) = 1$ for $\tau = \tau_{\rho,u}$ or $\tau = \tau_{1,u}$. Also $\langle \psi, \tau \rangle \equiv 0 \mod 2$ for $\psi = 1$, η, χ, or $\hat{\sigma}_e$, and by Theorem 2.1, we have $W(E/k_u, \tau) = 1$. Applying Lemma 5.1 of [9] for δ_v finishes the claim. $\blacksquare$

Proposition 3.2. *If $v^c = v$, v is unramified in L/K then $\gamma_u \equiv \sum_{v|u} \delta_v \equiv 0$.*

Proof. In this case, v splits completely in L/K by [9, 6.5(i)], i.e. for every prime w of L lying above v, $L_w = K_v$. Now, we have

$$\tau_{\rho,u}, \tau_{1,u} : \mathrm{Gal}(L_w/k_u) = \mathrm{Gal}(K_v/k_u) \to \mathrm{GL}_2(\mathbb{C})$$

viewing $\mathrm{Gal}(K_v/k_u)$ as the v-decomposition subgroup of $\mathrm{Gal}(L/k)$. One sees by direct calculation (see for example [14, §5.3]) that $\tau_{\rho,u} \cong \tau_{1,u}$, and by applying Corollary 5.3 of [9] for δ_v the claim follows. $\blacksquare$

3.2. Good reduction

In the case of good reduction, the arithmetic local constant has been determined by Mazur and Rubin in [9].

Theorem 3.3 (Theorem 5.6 and 6.6 of [9]). *If v is a prime of K with $v \nmid p$, $v = v^c$, v is ramified in L/K, and E has good reduction at v, then $\delta_v \equiv 0$.*

Theorem 3.4 (Theorem 6.7 of [9]). *If $v \mid p$ and E has good ordinary reduction at v, then $\delta_v \equiv 0$.*

For the corresponding situation on the analytic side:

Proposition 3.5. *If E has good reduction over K_v then $\gamma_u \equiv 0$.*

Proof. By Theorem 2.1(ii), it suffices to see $\det \tau_{\rho,u} \equiv \det \tau_{1,u} \mod \mathfrak{p}$ for some $\mathfrak{p} \mid p$. Fixing a basis for the spaces of ρ and 1 respectively, we have $\rho \equiv 1 \mod \mathfrak{p}$ since L/K is a cyclic p-power extension. This implies $\tau_{\rho,u} \equiv \tau_{1,u} \mod \mathfrak{p}$ (component-wise), viewed as matrices with function-valued entries, and $\det \tau_{\rho,u} \equiv \det \tau_{1,u} \mod \mathfrak{p}$. ■

3.3. Potential multiplicative reduction

Here, in view of Propositions 3.1-3.2, we assume $v^c = v$ and v ramifies in L/K, i.e. $L_w \neq K_v$.

Analytic

Proposition 3.6. *If E/k_u has potential multiplicative reduction, then $\gamma_u \equiv 0$ if and only if E does not have split multiplicative reduction over K_v.*

Proof. Applying the arguments of Proposition 3.5, it remains to determine $\langle \chi, \tau \rangle$. If E has split multiplicative reduction at u, $\chi = 1$ and since $L_w \neq K_v$, $\dim \tau = 2$. We have $\tau = \tau_{1,u} = 1 \oplus \mu$, with μ the character associated to the extension K_v/k_u. When E has split multiplicative reduction at u, $\chi = 1 \ncong \mu$ and so $\langle \chi, \tau \rangle = 1$. For the other cases, $\chi \cong \mu$ if and only if K_v/k_u is the quadratic extension over which E acquires split multiplicative reduction. ■

Arithmetic

Proposition 3.7. *If E has potential multiplicative reduction over k_u, then $\delta_v \equiv 0$ if and only if E does not have split multiplicative reduction over K_v.*

Proof. Let H be the quadratic extension over which E attains split multiplicative reduction. If $H = K_v$, there is a $q \in k_u^\times$ such that $E(L_w) \cong L_w^\times / q^{\mathbb{Z}}$ as $\mathrm{Gal}(L_w/K_v)$-modules, and with the isomorphism defined over K_v (loc. cit. [17]). This case is Lemma 8.4 of [9].

Suppose now that $H \neq K_v$. Define E' to be the quadratic twist of E associated to H/k_u, so that E' has split multiplicative reduction at u, and $E \xrightarrow{\phi} E'$ is an isomorphism over H. As before, we have a $\mathrm{Gal}(HL_w/k_u)$-isomorphism

$$\lambda : E'(HL_w) \to HL_w^\times / q^{\mathbb{Z}},$$

with $q \in k^\times$. Let $\mathrm{Gal}(HL_w/L_w) = \langle \sigma \rangle$ and define the minus-part of $HL_w^\times$ to be

$$(HL_w^\times)^- := \{ z \in HL_w^\times \ : \ z^\sigma = z^{-1} \}$$

and similarly for all other $\mathrm{Gal}(HL_w/L_w)$-modules[3]. The map obtained by precomposing λ with ϕ restricts to

$$E(L_w) \xrightarrow{\phi} E'(HL_w)^- \xrightarrow{\lambda} ((HL_w^\times)/q^{\mathbb{Z}})^-.$$

If $q \notin \mathrm{N}_{HL_w/L_w}$ then we also have $((HL_w^\times)/q^{\mathbb{Z}})^- \cong (HL_w^\times)^-$. If $q \in \mathrm{N}_{HL_w/L_w}$ then the projection of $(HL_w^\times)^-$ has index 2 in $((HL_w^\times)/q^{\mathbb{Z}})^-$, hence prime to p. Both cases will be similar, so we proceed with the former. One has a similar situation with $E(L'_w) \to (HL'^\times_w)^-$.

Since these maps commute with $N := \mathrm{N}_{HL_w/HL'_w}$, the snake lemma gives

$$[E(L'_w) : N(E(L_w))] = [(HL'^\times_w)^- : N((HL_w^\times)^-)].$$

We claim that this index is 1, implying $E(K_v) \subseteq E(L'_w) = N(E(L_w))$ and hence

$$\dim_{\mathbb{F}_p} E(K_v)/(E(K_v) \cap \mathrm{N}_{L_w/L'_w} E(L_w)) = 0.$$

To see that the index is 1, we note that local class field theory gives an injection

$$((HL'_w)^\times)^-/N((HL_w^\times)^-) \hookrightarrow \mathrm{Gal}(HL_w/HL'_w) = \mathrm{Gal}(L_w/L'_w)^-.$$

Since we know that σ conjugates $\mathrm{Gal}(L_w/L'_w)$ trivially, $\mathrm{Gal}(L_w/L'_w)^-$ is trivial. ■

3.4. Potential good reduction

Again, we assume $v^c = v$ and v ramifies in L/K, so $L_w \neq K_v$ as before.

Analytic

Denote ℓ for the common residue characteristic of k_u, K_v, L_w, and suppose E/k_u has additive and potential good reduction. Throughout we set H to be the unique unramified quadratic extension of k_u.

Proposition 3.8. *Suppose $v \nmid 6$. If $v \nmid p$ or K_v/k_u is unramified then $\gamma_u \equiv 0$.*

Proof. Here, we use the notation of Theorem 2.1, and from $v \nmid 6$, we have $\ell \geqslant 5$. For $\tau = \tau_{\rho,u}$ or $\tau = \tau_{1,u}$, we have $\langle 1, \tau\rangle + \langle \eta, \tau\rangle \equiv 0 \mod 2$, using that K_v/k_u is unramified for the latter.

In this setting $\hat{\sigma}_e$ is the representation of $\mathrm{Gal}(\bar{k}_u/k_u)$ induced from a character $\hat{\phi}_e$ of order $e = 3$, 4, or 6 (see [13, p. 332]). Hence, we may view $\hat{\sigma}_e$ as a representation of $\mathrm{Gal}(K_1/k_u)$ for some extension K_1/K_v.

Consider $\tau = \tau_{\rho,u}$. Lifting $\hat{\sigma}_e$ and τ to some appropriate extension K_2/k_u, since τ is irreducible, we see $\langle \hat{\sigma}_e, \tau\rangle = 1$ if and only if $\hat{\sigma}_e \cong \tau$. Restricting τ and $\hat{\sigma}_e$ to $\mathrm{Gal}(K_2/K_v)$, these representations decompose as $\tau = \rho \oplus \rho^c$ and $\hat{\sigma}_e = \phi_e \oplus \phi_e^c$. The order of ρ is a power of $p \geqslant 5$ and the order of ϕ_e is 3, 4, or 6, so $\langle \hat{\sigma}_e, \tau\rangle = 0$. For $\tau = \tau_{1,u}$, we have $\tau = 1 \oplus \eta$ and so $\langle \hat{\sigma}_e, \tau\rangle = 0$. ■

[3]For example, restriction of σ gives $\mathrm{Gal}(HL_w/L_w) \cong \mathrm{Gal}(HL'_w/L'_w)$, providing HL'_w a $\mathrm{Gal}(HL_w/L_w)$-module structure.

Proposition 3.9. *Suppose $v \nmid 6$ and K_v/k_u is ramified. If E acquires good reduction over an abelian extension of k_u, then $\gamma_u \equiv 0$.*

Proof. Here $\ell \geqslant 5$, so we are in case (iii) of Theorem 2.1, and the condition that E acquires good reduction over an abelian extension of k_u is equivalent to (see [11, Prop 2]) $\mathcal{W}(M/k_u)$ being abelian, where M is the minimal extension of k_u^{ur} over which E acquires good reduction, and in turn to $\sigma_{E/k_u} = \psi \oplus \psi^{-1}$ for some character ψ of $k_u^\times$. This gives

$$W(E/k_u, \tau) = \mathfrak{c}(\tau) = \det \tau(-1).$$

Applying Proposition 3.5 then gives the result. ∎

Proposition 3.10. *If $v \mid 6$ then $\gamma_u \equiv 0$.*

Proof. This is case 2(b) of [1]. De la Rochefoucauld proves this in terms of ϵ-factors as Rohrlich's formula (Theorem 2.1 above) do not apply when E is wildly ramified (see [6, §4]). We note that the dihedral setting is essential in his proof. ∎

Arithmetic

Proposition 3.11. *If $v \nmid p$ and E has additive reduction over K_v then $\delta_v \equiv 0$.*

Proof. If E has additive reduction, then

$$E_0(K_v)/E_1(K_v) \cong \tilde{E}_{ns}(\kappa) \cong \kappa^+, \tag{3.1}$$

with κ, the residue field of K_v, a finite field of characteristic $\ell \neq p$. We recall two facts (see §VII.3 and §VII.6 of [17]),

(1) $E_1(K_v) \cong \mathbb{Z}_\ell^r \oplus T$ for some finite ℓ-group T.
(2) $|E(K_v)/E_0(K_v)| \leqslant 4$.

Since $p \nmid 6\ell$ these two facts yield

$$E(K_v)/pE(K_v) \cong E_0(K_v)/pE_0(K_v) \cong E_1(K_v)/pE_1(K_v) = 0,$$

showing that $E(K_v)$ has no p-subgroups and so $\delta_v \equiv 0$. ∎

For $\mathcal{K}$ a finite extension of k_u, denote $\tilde{E}$ for the reduction of E at the prime of $\mathcal{K}$. If κ is the residue field of $\mathcal{K}$ and E has good ordinary reduction over $\mathcal{K}$ then we say that E has *anomalous* reduction over $\mathcal{K}$ if $\tilde{E}(\kappa)[p] \neq 0$, and we say E has *non-anomalous* reduction otherwise (see [9, App. B], also [8, §1.b]).

Proposition 3.12. *If $v \mid p$, E has additive reduction over K_v, and E attains good, ordinary, non-anomalous reduction over a Galois extension M/K_v, then $\delta_v \equiv 0$.*

Proof. Since E has potential good reduction, M can be chosen so that $[M : K_v]$ is prime to p (see [15, §2] and [16, p.2]). Let E^k denote a model for E defined over k_u, and let E^M denote a model of E defined over M for which E has good, ordinary, non-anomalous reduction. We have an isomorphism $E^k \to E^M$ defined over M, giving $E^k(\mathcal{M}) \cong E^M(\mathcal{M})$, where $\mathcal{M} = ML_w$, and similarly for $\mathcal{M}' = ML'_w$. We denote $\Gamma = \mathrm{Gal}(M/K_v)$ and $H = \mathrm{Gal}(L_w/L'_w)$, and note that

$$\mathrm{Gal}(M/K_v) \cong \mathrm{Gal}(\mathcal{M}'/L'_w) \cong \mathrm{Gal}(\mathcal{M}/L_w), \qquad \mathrm{Gal}(L_w/L'_w) \cong \mathrm{Gal}(\mathcal{M}/\mathcal{M}').$$

By Propositions B.2 and B.3 of [9], we have that $N_H : E^M(\mathcal{M}) \to E^M(\mathcal{M}')$ is surjective, and hence $N_H : E^k(\mathcal{M}) \to E^k(\mathcal{M}')$ is surjective also. From this and $N_\Gamma \circ N_H = N_H \circ N_\Gamma$ we have

$$\begin{aligned}[E^k(L'_w) : N_\Gamma(E^k(\mathcal{M}'))] &= [E^k(L'_w) : N_\Gamma \circ N_H(E^k(\mathcal{M}))] \\ &= [E^k(L'_w) : N_H \circ N_\Gamma(E^k(\mathcal{M}))].\end{aligned} \tag{3.2}$$

Since Γ has order prime to p and

$$|\Gamma| \cdot E^k(L'_w) \subset N_\Gamma(E^k(\mathcal{M}')) \subset E^k(L'_w),$$

the first term in (3.2) is prime to p. Since H has order p and

$$N_H \circ N_\Gamma(E^k(\mathcal{M})) \subset N_H(E^k(L_w)) \subset E^k(L'_w),$$

the last term in (3.2) is divisible by some power of p when $N_H(E^k(L_w)) \neq E^k(L'_w)$. Since this is impossible, we must have $N_H(E^k(L_w)) \supset E^k(K_v)$ and $\delta_v \equiv 0$. ∎

4. Main result

Recall E/k is an elliptic curve ordinary at p. Also recall that γ_u is defined by

$$(-1)^{\gamma_u} = W(E/k_u, \tau_{\rho,u})/W(E/k_u, \tau_{1,u}).$$

Define $\mathfrak{S} = \{\text{primes } v \text{ of } K : v^c = v,\ v \text{ ramifies in } L/K, \text{ and } v \mid 6p\}$.

Theorem 4.1. *Fix primes u of k and v of K with $v \mid u$. If $v \in \mathfrak{S}$ suppose that one of the following holds:*

(a) *E has good reduction at v.*
(b) *E has potential multiplicative reduction at v,*
(c) *E has additive, potential good reduction at v, and acquires good, non-anomalous reduction over an abelian extension of k_u when $v \mid p$.*

Then $\gamma_u \equiv \sum_{v|u} \delta_v \mod 2$.

Corollary 4.2. *If E/k satisfies the hypothesis of Theorem 4.1, then* mod 2

$$\dim_{\overline{\mathbb{Q}}_p} \mathcal{S}_p(E/L)^\rho - \dim_{\overline{\mathbb{Q}}_p} \mathcal{S}_p(E/L)^1 \equiv \mathrm{ord}_{s=1}\, \Lambda(E/k, \rho, s) - \mathrm{ord}_{s=1}\, \Lambda(E/k, 1, s).$$

Proof of 4.1. Let v, v^c the primes of K above u. If $v \notin \mathfrak{S}$ then $v^c \neq v$, v is unramified in L/K, or $v \nmid 6p$. If $v^c \neq v$ then we use Proposition 3.1, and if $v^c = v$ is unramified in L/K, Proposition 3.2 gives the claim. For the remainder we may assume $v^c = v$.

In the case $v \nmid 6p$, we have $v \nmid 6$ and $v \nmid p$. If E has good reduction at v then Theorem 3.3 shows $\delta_v \equiv 0$, and Proposition 3.5 gives $\gamma_u \equiv 0$. If E has potential multiplicative reduction then Proposition 3.7 and Proposition 3.6, for δ_v and γ_u, respectively, give the result. Lastly, if E has potential good reduction, then we apply Proposition 3.11 and Proposition 3.8.

For $v \in \mathfrak{S}$, case (a) follows from Theorem 3.4 for δ_v and Proposition 3.5 for γ_u. Case (b) is covered by Proposition 3.7 for δ_v and Proposition 3.6 for γ_u.

For case (c), first consider $v \mid 6$. We apply Proposition 3.10 for γ_u, and since $v \nmid p$, we can apply Proposition 3.11 for δ_v. When $v \mid p$ the condition that E acquries ordinary, non-anomalous reduction allows us to apply Proposition 3.12 for δ_v. In this case, $v \nmid 6$ and so for γ_u we use Proposition 3.8 when K_v/k_u is unramified or the 'abelian' condition and Proposition 3.9 when K_v/k_u is ramified. ■

References

[1] T. De la Rochefoucauld, *Invariance of the parity conjecture for p-Selmer groups of elliptic curves in a D_{2p^n}-extension*, arXiv:1002.0554v1 [math.NT], preprint.

[2] T. Dokchitser and V. Dokchitser, *Regulator constants and the parity conjecture*, Invent. Math. **178**(1) (2009), 23–71.

[3] T. Dokchitser and V. Dokchitser, *On the Birch-Swinnerton-Dyer quotients modulo squares*, Annals of Mathematics **172**(1) (2010), 567–596.

[4] R. Greenberg, *Introduction to Iwasawa theory*, in B. Conrad and K. Rubin, editors, Arithmetic Algebraic Geometry, volume 9 of Park City Mathematics Series, American Mathematical Society, 2001.

[5] R. Greenberg, *Iwasawa theory, projective modules, and modular representations*, http://www.math.washington.edu/ greenber/personal.html, preprint.

[6] S. Kobayashi, *The local root number of elliptic curves with wild ramification*, Mathematische Annalen **323** (2002), 609–623.

[7] B. Mazur, *An Arithmetic Theory of Local Constants*, http://www.cirm.univ-mrs.fr/videos/2006/exposes/17w2/Mazur.pdf.

[8] B. Mazur, *Rational points of abelian varieties with values in towers of number fields*, Inventiones Math. **18** (1972), 183–266.

[9] B. Mazur and K. Rubin, *Finding large Selmer rank via an arithmetic theory of local constants*, Annals of Mathematics **166**(2) (2007), 581–614.

[10] B. Mazur, K. Rubin, and A. Silverberg, *Twisting commutative algebraic groups*, Journal of Algebra **314**(1) (2007), 419–438.

[11] D. Rohrlich, *Variation of the root number in families of elliptic curves*, Compositio Mathematica **87** (1993), 119–151.

[12] D. Rohrlich, *Elliptic Curves and the Weil-Deligne Group*, in Elliptic Curves and Related Topics, volume 4 of CRM Proceedings and Lecture Notes, pages 125–157, Amer. Math. Soc. 1994.

[13] D. Rohrlich, *Galois theory, elliptic curves, and root numbers*, Composito Mathematica **100** (1996), 311–349.
[14] J-P. Serre, *Linear Representations of Finite Groups*, volume 67 of Graduate Texts in Mathematics, Springer, 1979.
[15] J-P. Serre and J. Tate, *Good Reduction of Abelian Varieties*, Annals of Mathematics **88**(3) (1968), 492–517.
[16] J. Silverman, *The Néron fiber of abelian varieties with potential good reduction*, Math. Ann. **264** (1983), 1–3.
[17] J. Silverman, *Arithmetic of Elliptic Curves*, volume 106 of Graduate Texts in Mathematics, Springer, 1986.

Address: Sunil Chetty: Mathematics Department, College of St. Benedict and St. John's University.

E-mail: schetty@csbsju.edu

Received: 10 October 2010; **revised:** 4 January 2016

Functiones et Approximatio
54.2 (2016), 251–274
doi: 10.7169/facm/2016.54.2.8

LEVEL STRIPPING FOR VECTOR-VALUED SIEGEL MODULAR FORMS OF GENUS 2

Rodney Keaton

Abstract: In this paper, we present a method by which one can strip primes from the level of a vector-valued genus 2 Siegel modular form while preserving a congruence modulo this prime. An application of this result to four-dimensional Galois representations will also be presented.

Keywords: congruence of modular forms, Galois representations, Siegel modular forms.

1. Introduction

Throughout, we fix a rational prime $\ell \geqslant 5$ and let $G_{\mathbb{Q}}$ denote the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Furthermore, we fix embeddings of $\overline{\mathbb{Q}}$ into $\overline{\mathbb{Q}}_\ell$ and into $\mathbb{C}$.

In [23], J-P. Serre poses two conjectures which provid precise conditions under which a Galois representation of the form

$$\overline{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell) \tag{1.1}$$

arises from a cuspidal elliptic eigenform. The "weak" conjecture simply states when such an eigenform exists, while the "strong" conjecture gives the precise character, level, and weight of such an eigenform. Through the late eighties and early nineties a large body of work was dedicated to showing that the weak conjecture implies the strong conjecture. Hence, one now simply refers to both as Serre's conjecture. The reader is referred to [9] for a nice overview of these results. Among this body of work, we have the following theorem due to Ribet which provides a "level stripping" result for Galois representations of the above type, and serves as the primary motivation for the results in this paper.

Theorem 1 ([22, Theorem 2.1]). *Suppose that $\overline{\rho}$ is as in Equation 1.1 and arises from an elliptic eigenform of level $\ell^r N$ with $r > 0$ and $(N, \ell) = 1$. Then, $\overline{\rho}$ arises from an elliptic eigenform of level N.*

2010 Mathematics Subject Classification: primary: 11F33, 11F46; secondary: 11F80

It should also be noted that this theorem holds for $\ell = 3$ as well and was further extended to the case $\ell = 2$ by Hatada in [11] using slightly different methods. Finally, as one of the monumental achievements in modern number theory, we have that Serre's conjecture is now a theorem due to Khare and Wintenberger, see [15],[16].

In recent work of Herzig and Tilouine, see [12], a "Serre type" conjecture is made for Galois representations of the form

$$\overline{\rho} : G_{\mathbb{Q}} \to \mathrm{GSp}_4(\overline{\mathbb{F}}_\ell).$$

For a precise statement of this conjecture the reader is referred to Section 4. In this setting, the Galois representations are conjectured to arise from vector-valued Siegel modular forms of genus 2. While the conjecture in this setting is not as precise as Serre's conjecture concerning the character, level, and weight, Herzig and Tilouine do mention that the level should be prime to ℓ. Bearing this in mind, the main result of this paper is a level stripping result for Siegel modular forms analogous to Theorem 1. Such results have been previously been obtained by Taylor in [27] under an ordinarity condition, by Brown and the author in [7] for Siegel modular forms which are lifted from elliptic modular forms, and by the author in [14] for scalar valued Siegel modular forms.

In particular, the level-stripping result of this paper and the subsequent application to Galois representations can be viewed as a direct generalization of the results in [14] to the vector-valued setting. The techniques used to prove the main results in this paper are identical to the techniques employed in [14], but the primary obstacle lies in the fact that the arithmetic of vector-valued Siegel modular forms can be quite a bit more delicate. Furthermore, it is important to remark that this paper seeks to correct a mistake which was overlooked in [14]. For more details see the end of Section 3.3. Finally, it is the goal of the author to provide convenient references for arithmetic results which may be common knowledge to the experts, but have yet to explicitly appear in the literature for vector-valued Siegel modular forms with level.

2. Background

In this section we will introduce some basic facts about vector-valued Siegel modular forms of genus 2. For more details the interested reader is referred to [3] for a thorough treatment of scalar valued forms of arbitrary level and [30] for a quite readable exposition of the theory of arbitrary genus vector-valued forms in the level 1 setting.

Let $\mathfrak{h}_2$ denote the genus 2 Siegel upper half plane, and let $\mathrm{GSp}_4^+(\mathbb{R})$ denote the set of 4×4 symplectic matrices with real entries and positive similitude factor. Note, we will denote the similitude factor by μ throughout. We have an action of $\mathrm{GSp}_4^+(\mathbb{R})$ on $\mathfrak{h}_2$ given by,

$$\gamma \cdot Z = (aZ + b)(cZ + d)^{-1}, \qquad \text{for } \ Z \in \mathfrak{h}_2, \ \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GSp}_4^+ \mathbb{R}).$$

In order to define vector-valued Siegel modular forms, we will need to generalize the notion of the "automorphy factor" from the classical theory of modular forms. To this end, consider an irreducible representation,

$$\rho : \mathrm{GL}_2(\mathbb{C}) \to \mathrm{GL}(V),$$

with V some finite dimensional $\mathbb{C}$-vector space. Representations of this type have been completely classified and are, in fact, in bijective correspondence with tuples of the form $(k_1, k_2) \in \mathbb{Z}^2$ with $k_1 \geqslant k_2$ by Proposition 15.47 in [10]. We call (k_1, k_2) the highest weight vector of ρ.

To be more precise, we let $V' = \mathbb{C}x_1 \oplus \mathbb{C}x_2$ be the standard representation of $\mathrm{GL}_2(\mathbb{C})$. Then, the highest weight vector (k_1, k_2) corresponds to the representation $\mathrm{Sym}^{k_1-k_2}(V') \otimes \det^{k_2}(V')$, where $\mathrm{Sym}^k(V')$ is the k^{th} symmetric power of V', which we can identify with the space of degree $k_1 - k_2$ homogeneous polynomials in $\mathbb{C}[x_1, x_2]$.

With V as above, let $F : \mathfrak{h}_2 \to V$ be a holomorphic function. Then, for $\gamma \in \mathrm{GSp}_4^+(\mathbb{R})$, we define the weight ρ slash operator by

$$(F|_\rho \gamma)(Z) = \rho(cZ + d)^{-1} F(\gamma \cdot Z).$$

We are interested in functions which are invariant under the action of certain subgroups of $\mathrm{GSp}_4^+(\mathbb{R})$ by the slash operator. In particular, we define $\mathrm{Sp}_4(\mathbb{Z})$ to be elements of $\mathrm{GSp}_4^+(\mathbb{R})$ which have integral entries and lie within the kernel of the similitude factor. This group serves as the analogue to the group $\mathrm{SL}_2(\mathbb{Z})$ in the setting of elliptic modular forms. We also have the analogues of the level N congruence subgroups in this setting, i.e., the subgroups

$$\Gamma_0^2(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{Sp}_4(\mathbb{Z}) : c \equiv 0_2 \pmod{N} \right\},$$
$$\Gamma_1^2(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0^2(N) : a \equiv d \equiv 1_2 \pmod{N} \right\},$$

where we are writing the entries as 2×2 blocks.

We are now prepared to define Siegel modular forms.

Definition 2. Let N be a positive integer, χ be a Dirichlet character modulo N, and V a finite dimensional complex vector space. Let $F : \mathfrak{h}_2 \to V$ be a holomorphic function and $\rho : \mathrm{GL}_2(\mathbb{C}) \to \mathrm{GL}(V)$ be an irreducible representation. Then, we say that F is a *Siegel modular form of character χ, genus 2, level N, and weight ρ* if

$$F|_\rho \gamma = \chi(\gamma) F, \qquad \text{for all } \gamma \in \Gamma_0^2(N),$$

where we set $\chi(\gamma) = \chi(\det d)$. We denote the space of all such functions as $M_\rho^2(N, \chi)$.

If $\dim_{\mathbb{C}}(V) > 1$ then the modular forms in the definition above are typically referred to as vector-valued Siegel modular forms in the literature, and if $\dim_{\mathbb{C}}(V) = 1$ then they are typically called classical or scalar-valued Siegel modular forms.

We have that for $F \in M^2_{\rho_1}(N,\chi)$ and $G \in M^2_{\rho_2}(N,\chi)$, the product

$$F(Z)G(Z) := F(Z) \otimes_{\mathbb{C}} G(Z)$$

is in $M^2_{\rho_1\otimes\rho_2}(N,\chi)$, where if (k_1,k_2) and (k_1',k_2') are the highest weight vectors of ρ_1 and ρ_2, respectively, then the highest weight vector of $\rho_1\otimes\rho_2$ is (k_1+k_1', k_2+k_2'). Hence,

$$\bigoplus_{\rho} M^2_{\rho}(N,\chi)$$

is a graded $\mathbb{C}$-algebra, where the sum is taken over all irreducible representations of $\mathrm{GL}_2(\mathbb{C})$.

It follows from the transformation property satisfied by $F \in M^2_{\rho}(N,\chi)$ and the Koecher principle that F admits a Fourier expansion of the form

$$F(Z) = \sum_{\substack{T\in\Lambda_2\\ T\geqslant 0}} a_F(T)\exp(\mathrm{Tr}(TZ)) \text{ with } a_F(T) \in V,$$

where Λ_2 denotes the set of all 2×2 half-integral symmetric matrices, i.e., $2T$ is an integral matrix with even diagonal entries, $T \geqslant 0$ means that T is positive definite, and $\mathrm{Tr}(TZ)$ is the trace of the matrix TZ. Furthermore, if $a_{F|_\rho\gamma}(T) = 0$ for every $\gamma \in \mathrm{Sp}_4(\mathbb{Z})$ when T is not strictly positive definite, we say that F is a cusp form. We denote the subspace of cusp forms by $S^2_{\rho}(N,\chi)$.

Next, we recall some facts from the theory of Hecke operators for Siegel modular forms. Let $F \in M^2_{\rho}(N,\chi)$. We define the weight ρ double coset operator by

$$F[\Gamma^2_0(N)\alpha\Gamma^2_0(N)]_\rho = \sum_i \chi(\det(a_{\alpha_i}))F|_\rho\alpha_i,$$

where the summation runs over a complete set of representatives for

$$\Gamma^2_0(N)\backslash\Gamma^2_0(N)\alpha\Gamma^2_0(N).$$

We have a natural multiplication of these double coset operators given by

$$F[(\Gamma^2_0(N)\alpha\Gamma^2_0(N))\cdot(\Gamma^2_0(N)\beta\Gamma^2_0(N))]_\rho = \sum_{i,j}\chi(\det(a_{\alpha_i\beta_j}))F|_\rho\alpha_i\beta_j,$$

which makes the collection of double coset operators into an algebra over $\mathbb{Q}$, which is called the Hecke algebra, and denoted $H(\Gamma^2_0(N))$. The following proposition is quite helpful in working with elements of the Hecke algebra.

Proposition 3 ([30, Prop. 16.4]). *Let $\alpha \in \mathrm{GSp}_4^+(\mathbb{Q}) \cap M_4(\mathbb{Z})$. Then, the double coset $\Gamma_0^2(N)\alpha\Gamma_0^2(N)$ has a unique representative of the form*

$$\gamma = \mathrm{diag}(a_1, a_2, d_1, d_2)$$

with integers a_j, d_j satisfying $a_j > 0, a_j d_j = \mu(\gamma)$ for $j = 1, 2$ and $a_2 | d_2, a_1 | a_2$.

For a prime p, if we define $H_p(\Gamma_0^2(N))$ to be the subring of double cosets in $H(\Gamma_0^2(N))$ whose representatives have only powers of p in the denominators of the entries, then this proposition gives us that any element of $H(\Gamma_0^2(N))$ can be written as a finite product of elements, each coming from a distinct $H_p(\Gamma_0^2(N))$. In other words, we have a decomposition $H(\Gamma_0^2(N)) = \otimes_p' H_p(\Gamma_0^2(N))$, where $\otimes_p'$ is called the restricted tensor product, and means that all but finitely many elements of the product should be the identity. We will also use $H_p^{\mathbb{Z}}(\Gamma_0^2(N))$ to denote the subring of $H_p(\Gamma_0^2(N))$ whose representatives have only integral entries. We call $H_p^{\mathbb{Z}}(\Gamma_0^2(N))$ the local Hecke algebra at p. Let $H^{\mathbb{Z}}(\Gamma_0^2(N)) = \otimes_p' H_p^{\mathbb{Z}}(\Gamma_0^2(N))$. Concerning the generators of $H_p^{\mathbb{Z}}(\Gamma_0^2(N))$, we have the following theorem.

Theorem 4 ([30, Thm. 9]). *The local Hecke algebra at p, for $p \nmid N$, is a $\mathbb{Z}$-algebra generated by the following elements*

$$T(p) = \Gamma_0^2(N) \begin{pmatrix} I_2 & 0_2 \\ 0_2 & pI_2 \end{pmatrix} \Gamma_0^2(N),$$

and,

$$T_i(p^2) = \Gamma_0^2(N) \begin{pmatrix} I_{2-i} & 0 & 0 & 0 \\ 0 & p1_i & 0 & 0 \\ 0 & 0 & p^2 I_{2-i} & 0 \\ 0 & 0 & 0 & pI_i \end{pmatrix} \Gamma_0^2(N),$$

for $i = 1, 2$. Furthermore, $H_p(\Gamma_0^2(N)) = H_p^{\mathbb{Z}}(\Gamma_0^2(N))[1/T_2(p^2)]$.

Note, from Lemma 4.2 in [3] we have that the spaces $M_k^2(N, \chi)$, $S_k^2(N, \chi)$ are stable under the action of the Hecke operators, and it is not difficult to see that this proof extends to arbitrary weight ρ.

Moreover, adapting the scalar weight techniques from [3] to our vector-valued setting, we immediately obtain the following theorem, which gives an explicit action of the Hecke operators on Fourier coefficients.

Theorem 5. *Let $F \in M_\rho^2(N, \chi)$. Then, we have the following expression for $a_{T(p)F}(T)$,*

$$\chi(p^2) a_F\left(\frac{T}{p}\right) + p^3 \rho(\mathrm{diag}(p,p))^{-1} a_F(pT) + p\chi(p) \sum_{D \in S(p)} \rho(D)^{-1} a_F\left(\frac{DT\ {}^T D}{p}\right).$$

and for $a_{T_1(p^2)F}(T)$,

$$\chi(p^2)\sum_{D\in S(p)}\rho(D)^{-1}\left(a_F\left(\frac{DT\,{}^TD}{p^2}\right)+p^3\chi(p)\rho(\mathrm{diag}(p,p))^{-1}a_F(DT\,{}^TD)\right)$$
$$+p\chi(p^2)\left(\left(\sum_{D\in S(p)}\rho(D)^{-1}a_F\left(\frac{DT\,{}^TD}{p}\right)\right)^2-\sum_{D\in S(p^2)}\rho(D)^{-1}a_F\left(\frac{DT\,{}^TD}{p^2}\right)\right)$$
$$-(p+1)\chi(p)\rho(\mathrm{diag}(p,p))^{-1}a_f(T).$$

Note, as the verification of this theorem is quite lengthy and fairly routine, we have simply included the proof of this result in Section 5 so as not to take the reader too far afield.

In addition to the Hecke operators, the space $S^2_\rho(N,\chi)$ also comes equipped with an inner product, known as the Petersson inner product. The reader is referred to [25] for the formulation in the setting of arbitrary genus vector-valued Siegel modular forms, where one needs to change the domain integrated over in the case of non-trivial level.

Let $V=\mathbb{C}x_1\oplus\mathbb{C}x_2$ be the standard representation of $\mathrm{GL}_2(\mathbb{C})$. This space comes with a natural inner product given by

$$\langle a_1x_1+a_2x_2,b_1x_1+b_2x_2\rangle=a_1\bar{b}_1+a_2\bar{b}_2,$$

which induces an inner product on $\mathrm{Sym}^{k_1-k_2}(V)$ given by

$$\langle v_1\dots v_{k_1-k_2},w_1\dots w_{k_1-k_2}\rangle=\frac{1}{(k_1-k_2)!}\sum_{\sigma\in S_{k_1-k_2}}\prod_{j=1}^{k_1-k_2}\langle v_{\sigma(j)},w_j\rangle,$$

where $v_i,w_i\in V$. From [25] we have that this inner product satisfies

1. $\langle v,w\rangle=\overline{\langle w,v\rangle}$, for all $v,w\in\mathrm{Sym}^{k_1-k_2}(V)$.
2. $\langle\rho(\gamma_1)v,\rho(\gamma_2)w\rangle=\langle\rho({}^T\overline{\gamma_2}\gamma_1)v,w\rangle$ for all $\gamma_1,\gamma_2\in\mathrm{GL}_2(\mathbb{C})$, $v,w\in\mathrm{Sym}^{k_1-k_2}(V)$, where
$$\rho:\mathrm{GL}_2(\mathbb{C})\to\mathrm{GL}(\mathrm{Sym}^{k_1-k_2}(V)).$$

Using this, we define the Petersson inner product of $F,G\in M^2_\rho(N,\chi)$, with at least one a cusp form, to be

$$\langle F,G\rangle_{\Gamma^2_1(N)}=*\int_{\Gamma^2_1(N)\backslash\mathfrak{h}_2}\langle\rho(Z)F(Z),G(Z)\rangle\det(\mathrm{Im}(Z))^{-3}dZ,$$

where $\Gamma^2_1(N)\backslash\mathfrak{h}_2$ is a fundamental domain for $\Gamma^2_1(N)$, and the normalizing factor $*$ is given by

$$\frac{1}{[\mathrm{Sp}_4(\mathbb{Z}):\{\pm I_4\}\,\Gamma^2_1(N)]}.$$

From [4] we have that the Hecke operators are self-adjoint with respect to this inner product in the level 1, arbitrary genus case. Furthermore, using the formulas derived in Theorem 5, this can be shown to hold for level N and genus 2 for all Hecke operators in $H_N^{\mathbb{Z}}(\Gamma_0^2(N)) := \otimes'_{p\nmid N} H_p^{\mathbb{Z}}(\Gamma_0^2(N))$. These formulas are precisely the same, regardless of the level, so the self-adjointness follows immediately. From this, it follows that $S_\rho^2(N,\chi)$ has an orthogonal basis which consists of simultaneous eigenvectors for $T(p)$ and $T_i(p^2)$ for $i = 1, 2$ and for all $p \nmid N$. We refer to such an eigenvector as an eigenform. Note, by our definition of modular forms, any element of $M_\rho^2(N,\chi)$ is automatically an eigenvector for the Hecke operators $T_2(p^2)$ for $p \nmid N$ and has eigenvalue given by $\chi(p)$ up to some normalization factor.

We can also associate an L-function to a genus 2 Siegel modular form as well. Assume that $F \in S_\rho^2(N,\chi)$ is an eigenform, with ρ having highest weight vector (k_1, k_2). Then, the associated L-function is given by

$$L(s,F) = \prod_{p\nmid N} L_p(p^{-s},F)^{-1} \prod_{p|N} (1-\lambda_F(p)p^{-s})^{-1},$$

with

$$\begin{aligned} L_p(X,F) = 1 &- \lambda_F(p)X + (\lambda_F(p)^2 - \lambda_F(p^2;1) - \chi(p^2)p^{k_1+k_2-4})X^2 \\ &- \chi(p^2)\lambda_F(p)p^{k_1+k_2-3}X^3 + \chi(p^4)p^{2k_1+2k_2-6}X^4, \end{aligned}$$

where $T(p)F = \lambda_F(p)F$ and $T_1(p^2)F = \lambda_F(p^2;1)F$. Note, there are actually two distinct L-functions associated to F, however, the L-function presented above, referred to as the spinor L-function, is all we will be concerned with. By Theorem 1 in [1], it is known that this L-function is absolutely convergent in some right half plane and satisfies a functional equation in the scalar weight case.

3. Level stripping of Siegel modular forms

In this section, the goal is to prove our level stripping result. Before this is possible, we need quite a few preliminaries that will go in to the proof.

3.1. Arithmetic properties of Siegel modular forms

In this section, we give some important arithmetic properties of Siegel modular forms, and cuspidal eigenforms in particular, which will be needed for discussing congruences.

In order to discuss arithmetic properties of Siegel modular forms, we need to consider Siegel modular forms with Fourier coefficients lying in a certain ring. We make this precise here and set some notation. Recall, we can identify the representation space V with the homogeneous polynomials $\mathbb{C}[x_1, x_2]$ of degree $k_1 - k_2$, where (k_1, k_2) is the highest weight vector of ρ. For any subring $R \subset \mathbb{C}$, let V_R denote the homogeneous polynomials in $R[x_1, x_2]$ of degree $k_1 - k_2$. Let $S_\rho^2(N,\chi)_R$ denote the subset of $S_\rho^2(N,\chi)$ whose elements have Fourier coefficients in V_R at each cusp. Note, in [13], it is shown that vector-valued modular forms satisfy a "q-expansion principle," i.e., if the Fourier coefficients at one cusp lie in V_R then so do the Fourier coefficients at all of the other cusps.

We begin with the following lemma which will be needed throughout this section. Note the proof follows immediately from the explicit formulas given in Theorem 5.

Lemma 6. *Let $F \in S^2_\rho(N,\chi)_{\mathbb{Q}(\chi)}$. Then, $TF \in S^2_\rho(N,\chi)_{\mathbb{Q}(\chi)}$, for any $T \in H^{\mathbb{Z}}_N(\Gamma^2_0(N))$, where $\mathbb{Q}(\chi)$ is defined to be the number field obtained by adjoining all of the values of χ to $\mathbb{Q}$.*

We should also mention that similar results have been obtained in [13] using techniques from arithmetic geometry.

Using this lemma, we obtain the following result concerning the field of definition of the Hecke eigenvalues for a given eigenform.

Proposition 7. *Let $F \in S^2_\rho(N,\chi)$ be an eigenform. Define $\mathbb{Q}(\lambda_F)$ to be the field generated by adjoining all of the eigenvalues of F with respect to the Hecke operators $T(p)$ and $T_i(p^2)$ for $1 \leqslant i \leqslant 2$ and $p \nmid N$. Then, $\mathbb{Q}(\lambda_F)/\mathbb{Q}$ is a totally real finite extension.*

Note, this result is certainly well known to the experts, but we record the proof for the sake of completeness in the literature.

Proof. For any $t \in H^{\mathbb{Z}}_N(\Gamma^2_0(N))$, let $\lambda(t)$ satisfy $tF = \lambda(t)F$. Note, $\lambda(t)$ is algebraic as it is the root of the characteristic polynomial of t, and as t is self-adjoint, we have that $\lambda(t)$ is totally real.

To obtain that $\mathbb{Q}(\lambda_F)/\mathbb{Q}$ is a finite extension, we proceed as in the proofs of Theorem 1 in [18] where this lemma is proven for classical Siegel modular forms of arbitrary genus and of level 1 and Theorem 1 in [26] where this lemma is proven for vector valued Siegel modular forms of genus 2 and level 1.

By Lemma 2.1 in [27], we have that

$$S^2_\rho(N,\chi)_{\mathcal{O}_K} \otimes_{\mathcal{O}_K} \mathbb{C} = S^2_\rho(N,\chi),$$

where $\mathcal{O}_K$ is the ring of integers of some finite abelian extension $K/\mathbb{Q}$. Without loss of generality, we assume that $\mathbb{Q}(\chi) \subseteq K$.

Let $\mathrm{Aut}(\mathbb{C}/K)$ denote the field automorphisms of $\mathbb{C}$ which fix elements of K. Let $\sigma \in \mathrm{Aut}(\mathbb{C}/K)$. We define

$$F^\sigma(Z) = \sum_T \sigma(a_F(T)) \exp(\mathrm{Tr}(TZ)),$$

and σ acts on $a_F(T)$ by considering $a_F(T) \in \mathbb{C}[x_1,x_2]$ and acting on the the coefficients, i.e., for $a_F(T) = \sum_{i,j} a_{ij} x_1^i x_2^j$ we have $\sigma(a_F(T)) := \sum_{i,j} \sigma(a_{ij}) x_1^i x_2^j$.

We can decompose F as the sum

$$F = \sum_n c_n (F_n \otimes z_n),$$

where $c_n \in \mathcal{O}_K$, $z_n \in \mathbb{C}$, and $F_n \in S_\rho^2(N,\chi)_{\mathcal{O}_K}$. Recall, by Lemma 6, we have that $tF_n \in S_\rho^2(N,\chi)_{\mathcal{O}_K}$ for any $t \in H_N^{\mathbb{Z}}(\Gamma_0^2(N))$. Furthermore, for any $t \in H_N^{\mathbb{Z}}(\Gamma_0^2(N))$, we have

$$tF = \sum_n c_n(tF_n \otimes z_n).$$

It follows that $(tF)^\sigma = t(F^\sigma)$ for any $t \in H_N^{\mathbb{Z}}(\Gamma_0^2(N))$. In particular, $tF^\sigma = \sigma(\lambda_F(t))F^\sigma$. We notice from this that $F^\sigma \in S_\rho^2(N,\sigma\circ\chi)$ and that $\mathbb{Q}(\lambda_{F^\sigma}) = \sigma(\mathbb{Q}(\lambda_F))$.

Let $\mathcal{B}_\chi$ denote a basis of eigenforms for $S_\rho^2(N,\chi)$ and set

$$\mathcal{B} := \bigcup_{\chi \,(\mathrm{mod}\ N)} \mathcal{B}_\chi,$$

where the union is over all Dirichlet characters modulo N. Note, $\mathcal{B}$ is a finite set. From the discussion above, we have a map

$$\mathrm{Aut}(\mathbb{C}/K) \to S_{|\mathcal{B}|},$$

where $S_{|\mathcal{B}|}$ is the symmetric group on $|\mathcal{B}|$ letters. Thus, the action of $\mathrm{Aut}(\mathbb{C}/K)$ on each the direct sum over χ of all $S_\rho^2(N,\chi)$ factors through a finite quotient. Hence, $\mathbb{Q}(\lambda_F)/\mathbb{Q}$ is a finite extension. ■

Finally, to conclude this section, we have the following result concerning the field of definition of the Fourier coefficients of an eigenform.

Lemma 8. *Let $F \in S_\rho^2(N,\chi)$ be an eigenform and let K denote $\mathbb{Q}(\lambda_F,\chi)$, i.e., the field obtained by adjoining all of the values of χ to $\mathbb{Q}(\lambda_F)$. Set*

$$S_\rho^2(N,\chi;F) = \left\{G \in S_\rho^2(N,\chi) : \lambda_G(t) = \lambda_F(t) \text{ for all } t \in H_N^{\mathbb{Z}}(\Gamma_0^2(N))\right\}.$$

Then,

$$S_\rho^2(N,\chi;F) = S_\rho^2(N,\chi;F)_{\mathcal{O}_{KL}} \otimes_{\mathcal{O}_{KL}} \mathbb{C},$$

where $\mathcal{O}_{KL}$ is the ring of integers of the compositum of K and L where $L/\mathbb{Q}$ is some finite extension.

Proof. Recall, by Lemma 2.1 in [27] we have

$$S_\rho^2(N,\chi) = S_\rho^2(N,\chi)_{\mathcal{O}_L} \otimes_{\mathcal{O}_L} \mathbb{C},$$

where we are using the same notation which was defined before Corollary 6 and $L/\mathbb{Q}$ is a finite abelian extension. We assume that L contains the values of χ. Let $\{F_1,\ldots,F_r\}$ be an $\mathcal{O}_L$-basis for $S_\rho^2(N,\chi)_{\mathcal{O}_L}$. By Theorem 6, we have that

$$tF_i = \sum_{j=1}^r c_{ij}(t)F_j, \qquad \text{for all } \ t \in H_N^{\mathbb{Z}}(\Gamma_0^2(N)),$$

where $c_{ij}(t) \in \mathcal{O}_L$.

For each $z = (z_1, \ldots, z_r) \in \mathbb{C}^r$ we put

$$f(z) = \sum_{i=1}^{r} z_i F_i.$$

We set $V(F) = \{z \in \mathbb{C}^r : f(z) \in S_\rho^2(N, \chi; F)\}$. Note, $V(F)$ is a finite dimensional $\mathbb{C}$-vector space and we denote the dimension by d. It is clear that f defines a $\mathbb{C}$-linear isomorphism

$$f : V(F) \to S_\rho^2(N, \chi; F).$$

Take S to be a generating set for $H_N^{\mathbb{Z}}(\Gamma_0^2(N))$ as a $\mathbb{Z}$-algebra , which we know is finite because $H_N^{\mathbb{Z}}(\Gamma_0^2(N)) \hookrightarrow \mathrm{End}_{\mathbb{C}}(S_\rho^2(N, \chi))$. For $z \in V(F)$ it is clear that $tf(z) = \lambda_F(t) f(z)$ for all $t \in S$, i.e.,

$$\sum_{i=1}^{r} c_{ij}(t) z_i = \lambda_F(t) z_i.$$

Since the coefficients $\lambda_F(t), c_{ij}(t)$ are in KL, there exists a basis $\{v_1, \ldots, v_d\}$ of $V(F)$ such that $v_j \in (KL)^r$. Take a non-zero $\gamma_j \in \mathcal{O}_{KL}$ such that $v_j' = \gamma_j v_j \in \mathcal{O}_{KL}^r$. Then, $f(v_j') \in S_k^n(N, \chi; F)_{\mathcal{O}_{KL}}$ and $V(F) = \bigoplus_{i=1}^{d} \mathbb{C} v_i'$. ∎

3.2. Congruences of genus 2 Siegel modular forms

In this section we define two distinct notions of congruences between genus 2 Siegel modular forms. We then show a relationship between the two notions.

Let F and G be genus 2 eigenforms of level N and M respectively. For any prime $p \nmid MN$, we let $\lambda_F(p), \lambda_F(p^2; i), \lambda_G(p), \lambda_G(p^2; i)$ denote the eigenvalues of F and G with respect to $T(p)$ and $T_i(p^2)$ for $i = 1, 2$, i.e.,

$$T(p)F = \lambda_F(p)F,\ T_i(p^2)F = \lambda_F(p^2; i)F,$$

$$T(p)G = \lambda_G(p)G,\ T_i(p^2)G = \lambda_G(p^2; i)G.$$

We let $\mathbb{Q}(\lambda_F, \lambda_G)$ denote the compositum of $\mathbb{Q}(\lambda_F)$ and $\mathbb{Q}(\lambda_G)$, where $\mathbb{Q}(\lambda_F)$ and $\mathbb{Q}(\lambda_G)$ were defined in Proposition 7. By Proposition 7, $\mathbb{Q}(\lambda_F, \lambda_G)$ is a totally real number field. Let Σ denote a finite set of primes. Then, we write $F \equiv_\Sigma G \pmod{\ell}$ if for all primes $p \notin \Sigma$ we have

$$\lambda_F(p) \equiv \lambda_G(p) \pmod{\nu}, \qquad \lambda_F(p^2; i) \equiv \lambda_G(p^2; i) \pmod{\nu} \quad \text{for } i = 1, 2,$$

where ν is a prime lying above ℓ in $\mathbb{Q}(\lambda_F, \lambda_G)$. This is referred to as a congruence of eigenvalues.

Our second notion will be the congruence of Fourier coefficients, which we define as in [6]. Define the following field,

$$\mathbb{Q}(F) = \prod_{T \in \Lambda_2} \mathbb{Q}(a_F(T)),$$

where

$$\mathbb{Q}(a_F(T)) := \mathbb{Q}\left(\left\{a_{ij} : a_F(T) = \sum_{i,j} a_{ij} x_1^i x_2^j\right\}\right).$$

As in Section 2, we have identified V with the homogeneous polynomials of degree $k_2 - k_1$ in $\mathbb{C}[x_1, x_2]$, where (k_1, k_2) is the highest weight vector of ρ. Then, Lemma 8 gives that after some normalization, we may assume that $\mathbb{Q}(F)$ is a finite extension. We make the same assumption for the field $\mathbb{Q}(G)$.

Define the ℓ-adic valuation of F as

$$\operatorname{ord}_\ell(F) = \inf_{T \in \Lambda_2} \{\operatorname{ord}_\nu(a_F(T))\},$$

where

$$\operatorname{ord}_\nu(a_F(T)) = \min_{i,j}\left\{\operatorname{ord}_\nu(a_{ij}) : a_F(T) = \sum_{i,j} a_{ij} x_1^i x_2^j\right\},$$

and ν is a prime lying above ℓ in $\mathbb{Q}(F)$. Using this, we say that F and G have congruent Fourier coefficients, denoted $F \equiv_{\text{fc}} G \pmod{\ell^r}$, if $\operatorname{ord}_\ell(F - G) \geqslant r$.

For the genus 1 case, it is clear that these two notions of congruence are equivalent, as the Fourier coefficients of a normalized elliptic eigenform are precisely the eigenvalues. This equivalence is not necessarily true for any higher genus. However, we do have the following lemma, which gives that a congruence of Fourier coefficients implies a congruence of eigenvalues.

Lemma 9. *Let F, G be as defined above and let Σ be the set of rational primes dividing MN. If $F \equiv_{\text{fc}} G \pmod{\ell}$ then $F \equiv_\Sigma G \pmod{\ell}$.*

Proof. This proof follows the same argument as in Theorem A.1 in [21], however we include it here to emphasize that this result works for vector-valued forms of arbitrary level, not just the classical forms of level one case as was proven in [21].

Set K to be the compositum of $\mathbb{Q}(F)$ and $\mathbb{Q}(G)$. Also, we adjoin the values of the characters of F and G if necessary and continue to denote this field by K. Let $c \in K$ so that at least one component of one Fourier coefficient of cF is an ℓ-unit, i.e., for some $T \in \Lambda_2$ and $i, j \in \mathbb{N}$ we have that $\operatorname{ord}_\nu(a_{ij}) = 0$, where $a_F(T) = \sum_{i,j} a_{ij} x_1^i x_2^j$ and ν is a prime lying above ℓ in K. Without loss of generality, we replace F and G by cF and cG, respectively. Denote this component by $a_F(T)_{ij}$. Let $t \in H_N^{\mathbb{Z}}(\Gamma_0^2(N))$ with $tF = \lambda_F(t)F$ and $tG = \lambda_G(t)G$. Define the form $H = F - G$. Then,

$$\lambda_F(t)F - \lambda_G(t)G = t(F - G) = tH.$$

By Theorem 6, we have that $\mathbb{Q}(tH) \subseteq K$. Hence,

$$\lambda_F(t) a_F(T)_{ij} \equiv \lambda_G(t) a_G(T)_{ij} \pmod{\nu},$$

where ν is a prime lying above ℓ in K. Since $a_F(T)_{ij}$ is an ℓ-unit and $a_F(T)_{ij} \equiv a_G(T)_{ij} \pmod{\nu}$, we have that $\lambda_F(t) \equiv \lambda_G(t) \pmod{\nu}$, which completes the proof. ∎

3.3. The $U(\ell)$ operator

In this section, we introduce a certain operator on the space of Siegel modular forms which is analogous to the U_ℓ^N operator in [20] and then give the relevant properties which will be important for our purposes. Furthermore, we will provide a correction to the proof of the main result in [14].

We define the operator $U(\ell)$ by its action on Fourier expansions,

$$U(\ell) : \sum_{0 \leqslant T \in \Lambda_2} a_F(T) \exp(\mathrm{Tr}(TZ)) \mapsto \sum_{0 \leqslant T \in \Lambda_2} a_F(\ell T) \exp(\mathrm{Tr}(TZ)).$$

For our main result we will need the following two properties of the $U(\ell)$ operator.

Lemma 10 ([5, Thm 3.1]). *If $\ell || M$, the operator $U(\ell)$ is an injective map from $M_\rho^2(M, \chi)$ to itself.*

Proof. We give a sketch of the proof here, as the result is only shown for the scalar weight case in [5].

Let $F \in M_\rho^2(M, \chi)$ with $\ell || M$. Following d) in Remark 1 of [5], we consider the operator

$$tF = F| \sum_{\substack{M \in M_2(\mathbb{F}_\ell) \\ AEFBM = {}^T M}} \begin{pmatrix} 0 & -I_2 \\ I_2 & M \end{pmatrix}.$$

Note that this is the operator denoted $\tau(1, n)$ in [5]. This operator is invertible by Proposition 2.1 in [5].

From Equation 3.2 in [5], we can decompose t as follows

$$tF = F| \sum_{\substack{M \in M_2(\mathbb{F}_\ell) \\ AEFBM = {}^T M}} \begin{pmatrix} 0 & -I_2 \\ I_2 & M \end{pmatrix} = p^{3-k} F | W_\ell | U(\ell),$$

where

$$W_\ell = \begin{pmatrix} 0_2 & -I_2 \\ \ell I_2 & 0_2 \end{pmatrix}.$$

Note, W_ℓ is an involution. Furthermore, W_ℓ normalizes the group $\Gamma_0^2(M)$, which gives that $F|W_\ell \in M_\rho^2(M, \chi)$. Combining this with the invertibility of t, we have that $U(\ell)$ is injective. ∎

Lemma 11. *If $\ell^2 | M$ and χ is defined modulo $\frac{M}{\ell}$, the operator $U(\ell)$ maps $M_\rho^2(M, \chi)$ to $M_\rho^2(M/\ell, \chi)$.*

Proof. Here we have adapted a proof of Andrianov from [2].

Let $F \in M_\rho^2(M, \chi)$. From [5] we have that the operator $U(\ell)$ is given by,

$$U(\ell)F = \ell^3 \sum_S F| \begin{pmatrix} 1 & S \\ 0 & \ell \end{pmatrix},$$

where the summation runs over all symmetric matrices in $M_2(\mathbb{Z}/\ell\mathbb{Z})$. We have

$$U(\ell)F = \ell^3 \sum_S F| \begin{pmatrix} 1 & S \\ 0 & \ell \end{pmatrix} = \ell^3 F| \begin{pmatrix} 1 & 0 \\ 0 & \ell \end{pmatrix} \sum_S \begin{pmatrix} 1 & S \\ 0 & 1 \end{pmatrix}.$$

Define the following subgroup of $\Gamma_0^2(M/\ell)$,

$$\Gamma(M/\ell, \ell) := \left\{ \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \Gamma_0^2(M/\ell) : B \equiv 0 \pmod{\ell} \right\}.$$

Then, for $\gamma \in \Gamma(M/\ell, \ell)$ we have

$$\begin{aligned} F| \begin{pmatrix} 1 & 0 \\ 0 & \ell \end{pmatrix} | \begin{pmatrix} a_\gamma & b_\gamma \\ c_\gamma & d_\gamma \end{pmatrix} &= F| \begin{pmatrix} a_\gamma & b_\gamma \\ \ell c_\gamma & \ell d_\gamma \end{pmatrix} \\ &= F| \begin{pmatrix} a_\gamma & \frac{b_\gamma}{\ell} \\ \ell c_\gamma & d_\gamma \end{pmatrix} | \begin{pmatrix} 1 & 0 \\ 0 & \ell \end{pmatrix} \\ &= \chi(\gamma) F| \begin{pmatrix} 1 & 0 \\ 0 & \ell \end{pmatrix}. \end{aligned}$$

Note, a complete set of right coset representatives for

$$\Gamma(M/\ell, \ell) \backslash \Gamma_0^2(M/\ell)$$

is given by

$$\left\{ \begin{pmatrix} 1 & S \\ 0 & 1 \end{pmatrix} : {}^T S = S, S \in M_2(\mathbb{Z}/\ell\mathbb{Z}) \right\}.$$

Let $\gamma \in \Gamma_0(M/\ell)$, and let $S \in M_2(\mathbb{Z}/\ell\mathbb{Z})$ be symmetric. Set S' to be the unique symmetric matrix in $M_2(\mathbb{Z}/\ell\mathbb{Z})$ which is congruent to $(a_\gamma + Sc_\gamma)^{-1}(b_\gamma + Sd_\gamma) \pmod{\ell}$. Then, from Lemma 13 in [2], there exists $\gamma_S \in \Gamma(M/\ell, \ell)$ such that

$$\begin{pmatrix} 1 & S \\ 0 & 1 \end{pmatrix} \gamma = \gamma_S \begin{pmatrix} 1 & S' \\ 0 & 1 \end{pmatrix}.$$

Note, such a γ_S also satisfies $\chi(\gamma) = \chi(\gamma_S)$. Thus,

$$\begin{aligned} U(\ell)F|\gamma &= \ell^3 \sum_S F| \begin{pmatrix} 1 & 0 \\ 0 & \ell \end{pmatrix} \begin{pmatrix} 1 & S \\ 0 & 1 \end{pmatrix} \gamma \\ &= \ell^3 \sum_S F| \begin{pmatrix} 1 & 0 \\ 0 & \ell \end{pmatrix} \gamma_S \begin{pmatrix} 1 & S' \\ 0 & 1 \end{pmatrix} \\ &= \ell^3 \chi(\gamma_S) F| \begin{pmatrix} 1 & 0 \\ 0 & \ell \end{pmatrix} \sum_{S'} \begin{pmatrix} 1 & S' \\ 0 & 1 \end{pmatrix} \\ &= \chi(\gamma) U(\ell) F. \end{aligned}$$

This completes the proof. ∎

Corollary 12. *Let $F \in S^2_\rho(N\ell^r, \chi)$ be an eigenform with χ defined modulo N, $r > 1$, and $\ell \nmid N$. Then, for some ρ' and some χ' defined modulo N, there is a form $G \in S^2_{\rho'}(N\ell^{r-1}, \chi')$ satisfying*

$$F \equiv_{\text{fc}} G \pmod{\ell}.$$

Proof. We begin by letting $\sigma \in \text{Gal}(\mathbb{Q}(F)/\mathbb{Q})$ be a Frobenius element for ν a prime over ℓ in $\mathbb{Q}(F)$, i.e., $\sigma x \equiv x^\ell \pmod{\nu}$ for all $x \in \mathcal{O}_{\mathbb{Q}(F)}$. By realizing σ as an element of $\text{Aut}(\mathbb{C})$, we can apply Theorem 1 in [26] to see that $F^{\sigma^{-1}}$, as defined in the proof of Lemma 7, is an eigenform in $S^2_\rho(N\ell^r, \sigma^{-1} \circ \chi)$. Define a form $G = U(\ell)(F^{\sigma^{-1}})^\ell$. Then, we have

$$\begin{aligned} U(\ell)(F^{\sigma^{-1}})^\ell &\equiv U(\ell) \sum_{\substack{T>0 \\ T \in \Lambda_2}} \sigma^{-1}(a_F(T))^\ell \exp(\ell \operatorname{Tr}(TZ)) \pmod{\nu} \\ &= \sum_{\substack{T>0 \\ T \in \Lambda_2}} \sigma^{-1}(a_F(T))^\ell \exp(\operatorname{Tr}(TZ)) \\ &\equiv \sum_{\substack{T>0 \\ T \in \Lambda_2}} a_F(T) \exp(\operatorname{Tr}(TZ)) \pmod{\nu}. \end{aligned}$$

Thus, G is congruent in Fourier coefficients to F. Moreover, by Lemma 11, $G \in S^2_{\rho'}(N\ell^{r-1}, \chi')$ for some ρ' and χ'. ∎

We remark here on a mistake in the proof of Theorem 8 in [14]. In this proof, the author makes use of of the property given in Lemma 11. However, it was brought to the attention of the author by R. Schmidt, that it is possible that upon applying the $U(\ell)$ operator, the resulting form may be identically zero. The previous corollary allows the author to avoid this error.

3.4. Main result

In this section, we will prove the following theorem. Note, the corresponding result for scalar valued forms can be found in [14].

Theorem 13. *Let $F \in S^2_\rho(\ell^r N, \chi)$ be an eigenform with the highest weight vector of ρ satisfying $k_2 \geqslant 3$ and χ defined modulo ℓN with $\ell \nmid N$. Let Σ be the set of rational primes which divide ℓN. Then, for some χ' and ρ', there exists an eigenform $G \in S^2_{\rho'}(N, \chi')$ such that $F \equiv_\Sigma G \pmod{\ell}$.*

Proof. Throughout we are working with genus 2 Siegel modular forms, so we will drop the superscript. Furthermore, throughout the proof we will not be explicit about the weights of the intermediate forms, but we will make a note about the final weight ρ' at the end. Finally, we will tacitly take finite extensions of $\mathbb{Q}$ as needed.

As χ is a character modulo ℓN we obtain a factorization $\chi = \omega^i \kappa$, where ω is the unique character of conductor ℓ and order $\ell - 1$, i.e., the Teichmüller character, and κ is a character modulo N.

Let $E \in M_k(\ell, \omega^{-i})$ be a form from the sequence in Theorem 1.2 in [17] such that $E \equiv_{\text{fc}} 1 \pmod{\ell}$. Consider the product of Siegel modular forms FE.

We first want to show that this product transforms correctly under the action of $\Gamma_0(\ell^r) \cap \Gamma_1(N)$. Let $\gamma \in \Gamma_0(\ell^r) \cap \Gamma_1(N)$. Then,

$$\begin{aligned}(F(Z)E(Z))|\gamma &= \kappa\omega^i(\gamma)\omega^{-i}(\gamma)\det(cZ+d)^{-k}\rho(cZ+d)^{-1}F(\gamma Z)E(\gamma Z)\\ &= F(Z)E(Z).\end{aligned}$$

Thus, the product is a form of the desired level and of character κ. We will denote the weight of this form by ρ'. Furthermore, as $E \equiv_{\text{fc}} 1 \pmod{\ell}$ we have that

$$FE \equiv_{\text{fc}} F \pmod{\ell}.$$

Thus, FE is an eigenform when reduced modulo ν for a prime ν lying above ℓ in $\mathbb{Q}(F)$, and Lemma 9 gives us

$$FE \equiv_{\Sigma} F \pmod{\ell}.$$

Let $\mathcal{O}_\nu$ be an extension of $\mathbb{Z}_\ell$ which has ν as its maximal ideal. As $S_{\rho'}(N\ell^r, \kappa)$ is a finite, free $\mathcal{O}_\nu$ module, we can apply the Deligne-Serre lifting lemma (Lemme 6.11, [8]) to obtain an eigenform $F_1 \in S_{\rho'}(N\ell^r, \kappa)$ such that

$$F_1 \equiv_{\Sigma} F \pmod{\ell}.$$

We can now apply Corollary 12 repeatedly to F_1 in order to obtain a form $F_2 \in S_{\rho'}(N\ell, \chi')$ for some ρ' and χ', which is congruent in Fourier coefficients modulo ℓ to F. By the same argument used above we can find an eigenform in $S_{\rho'}(N\ell, \chi')$ satisfying this same congruence.

Before proceeding, we state the following lemma whose proof is precisely the same as the proof of Proposition 3.1 in [6].

Lemma 14. *Let $F \in S^2_\rho(N\ell, \chi)$ be an eigenform with associated character χ defined modulo N. Then, for some ρ' there exists $G \in S^2_{\rho'}(N, \chi)$ such that $F \equiv_{\text{fc}} G \pmod{\ell}$.*

Applying this lemma to F_2 to obtain a form $F_3 \in S_{\rho'}(N, \chi')$ which is congruent in Fourier coefficients to F modulo ν. Just as before, this yields the desired eigenform G.

Finally, with regards to the weight ρ' of G, if we let the highest weight vector of ρ be (k_1, k_2), then the highest weight vector of ρ' is

$$(\ell(k_1 + i\ell^{m_1} + \ell^{m_2-1}(\ell-1)), \ell(k_2 + i\ell^{m_1} + \ell^{m_2-1}(\ell-1)),$$

where m_1 and m_2 are both sufficiently large integers. In particular, we have that

$$(k_1', k_2') \equiv (k_1 + i, k_2 + i) \pmod{\ell - 1},$$

where (k_1', k_2') is the highest weight vector of ρ'. ∎

4. Application to Galois representations

In this section, we present an application of Theorem 13 which provides evidence for a conjecture of Herzig and Tilouine.

We begin with the following result which gives the existence of a Galois representation attached to a cuspidal Siegel eigenform of genus 2 as well as the characteristic polynomial of the images of the Frobenius elements with respect to this representation. Note that this result is stated in [24], however the proof is essentially due to Laumon in [19] and Weissauer in [31],[32]. The last reference is necessary to conclude that the associated Galois representation is symplectic in the case that the Siegel eigenform does not arise as a Saito-Kurokawa lift.

Theorem 15. *Let $F \in S^2_\rho(M,\chi)$ be an eigenform with ρ having highest weight vector (k_1,k_2) which satisfies $k_2 \geqslant 3$. Let $K = \mathbb{Q}(\lambda_F)$ and let ν be a prime lying above ℓ in K. Then, there exists a continuous, semi-simple Galois representation*

$$\rho_{F,\nu} : G_{\mathbb{Q}} \to \mathrm{GL}_4(\mathcal{O}_{K_\nu})$$

such that for all primes $p \nmid \ell M$ we have

$$\det(X \cdot 1_4 - \rho_{F,\nu}(\mathrm{Frob}_{\mathfrak{p}})) = L_p(X,F).$$

and $\rho_{F,\nu}$ is unramified at p, and we remind the reader that $L_p(X,F)$ is the local factor at p of the spinor L-function as defined in Section 2.

Throughout the remainder of the section, we will suppose that F is not a Saito-Kurokawa lift, so that we may assume the image of $\rho_{F,\nu}$ is contained in $\mathrm{GSp}_4(\mathcal{O}_{K_\nu})$. Furthermore, we will denote the weight ρ by its highest weight vector (k_1,k_2) in order to avoid confusion.

As we our representation takes values in $\mathrm{GSp}_4(\mathcal{O}_{K_\nu})$, we may form the residual representation of $\rho_{F,\nu}$ at ℓ, i.e., the representation

$$\overline{\rho}_{F,\nu} : G_{\mathbb{Q}} \to \mathrm{GSp}_4\left(\mathcal{O}_{K_\nu}/\nu\mathcal{O}_{K_\nu}\right) \hookrightarrow \mathrm{GSp}_4(\overline{\mathbb{F}}_\ell),$$

by reducing the image of $\rho_{F,\nu}$ modulo ν. We will take the semisimplification of the residual representation and continue to denote it as $\overline{\rho}_{F,\nu}$. We say that any representation arising in this way is *modular*.

With this in mind, we can ask when is a representation $\overline{\rho} : G_{\mathbb{Q}} \to \mathrm{GSp}_4(\overline{\mathbb{F}}_\ell)$ modular?

In a partial answer to this question, Herzig and Tilouine have given conditions under which $\overline{\rho}$ is conjectured to be modular. The reason this is a partial answer is that Herzig and Tilouine restrict to the ordinary setting. In order to state precisely the conjecture of Herzig and Tilouine we need a bit of background. For more details the reader is referred to [12].

First, we say that $\overline{\rho}$ is odd if $\mu \circ \overline{\rho}(c) = -1$, where $c \in G_{\mathbb{Q}}$ is complex conjugation and μ is the similitude factor. Note, to see that this is necessary for a representation to be modular, the reader is referred to Section 9 of [28].

Second, we need the following definition.

Definition 16. Let $F \in S^2_{(k_1,k_2)}(M,\chi)$ be an eigenform. We say that F is *ordinary at* ℓ if it satisfies one of the following two equivalent conditions

1. $\mathrm{ord}_\ell(\lambda_F(\ell)) = 0$ and $\mathrm{ord}_\ell(\lambda_F(\ell^2;1)) = k_2 - 3$.
2. The roots of the characteristic polynomial of $\rho_{F,\nu}(\mathrm{Frob}_\ell)$, which we denote by r_1, r_2, r_3, r_4, satisfy

$$\mathrm{ord}_\ell(r_1) = 0, \quad \mathrm{ord}_\ell(r_2) = k_2 - 2, \quad \mathrm{ord}_\ell(r_3) = k_1 - 1, \quad \mathrm{ord}_\ell(r_4) = k_1 + k_2 - 3.$$

Note that the equivalence in the above definition comes directly from the characteristic polynomial in Theorem 15.

Let D_ν be the decomposition group of ℓ in $G_{\mathbb{Q}}$, where ν is any prime lying above ℓ in $\overline{\mathbb{Z}}$. Let χ_ℓ denote the ℓ-adic cyclotomic character and for an ℓ-adic number u, we set $\epsilon(u)$ to be the unramified character of D_ν which sends Frob_ℓ to u. Then, for F ordinary at ℓ, we have from [29] that

$$\rho_{F,\nu}|_{D_\nu} \sim \begin{pmatrix} \chi_\ell^{k_1+k_2-3}\epsilon\left(\frac{r_4}{\ell^{k_1+k_2-3}}\right) & * & * & * \\ 0 & \chi_\ell^{k_1-1}\epsilon\left(\frac{r_3}{\ell^{k_1-1}}\right) & * & * \\ 0 & 0 & \chi_\ell^{k_2-2}\epsilon\left(\frac{r_2}{\ell^{k_2-2}}\right) & * \\ 0 & 0 & 0 & \epsilon(r_1) \end{pmatrix},$$

where $\sim$ denotes that the representations are isomorphic.

With this in mind, for a representation

$$\overline{\rho} : G_{\mathbb{Q}} \to \mathrm{GSp}_4(\overline{\mathbb{F}}_\ell),$$

we will say $\overline{\rho}$ is ordinary at ℓ if up to conjugation we have

$$\overline{\rho}|_{D_\nu} \sim \begin{pmatrix} \overline{\chi}_\ell^{e_3}\epsilon(u_3) & * & * & * \\ 0 & \overline{\chi}_\ell^{e_2}\epsilon(u_2) & * & * \\ 0 & 0 & \overline{\chi}_\ell^{e_1}\epsilon(u_1) & * \\ 0 & 0 & 0 & \overline{\chi}_\ell^{e_0}\epsilon(u_0) \end{pmatrix},$$

where $\overline{\chi}_\ell$ is the reduction of χ_ℓ modulo ℓ, the exponents satisfy $e_3 \geqslant e_2 \geqslant e_1 \geqslant e_0$, ϵ is as above, and $u_3, u_2, u_1, u_0 \in \overline{\mathbb{F}}_\ell^\times$. We denote such a representation by $(\overline{\rho}, \{e_j\})$. After twisting by an appropriate power of $\overline{\chi}_\ell$ we may assume $e_0 = 0$ and that $e_j \leqslant j(\ell-2)$ for $j = 1, 2, 3$. This brings us to the next definition.

Definition 17. For a representation $(\overline{\rho}, \{e_j\})$, we say that the exponents $\{e_j\}$ are ℓ-small if we can twist $\overline{\rho}$ by a power of $\overline{\chi}_\ell$ so that $0 = e_0 \leqslant e_1 \leqslant e_2 \leqslant e_3 < \ell - 1$.

Furthermore, if we can write $e_1 = k_2 - 2$ and $e_2 = k_1 - 1$ for some integers $k_1 \geqslant k_2 \geqslant 3$ then we call (k_1, k_2) the modular weight of $(\overline{\rho}, \{e_j\})$.

We are now prepared to state the following conjecture.

Conjecture 18 ([12, Conj. 0]). *Let $(\overline{\rho}, \{e_j\})$ be an irreducible, odd Galois representation which is ordinary at ℓ and has modular weight (k_1, k_2). Suppose further that the exponents $\{e_j\}$ are ℓ-small. Then, $\overline{\rho}$ is modular of level N with $\ell \nmid N$.*

As evidence for this conjecture, we can state the following corollary which follows from Theorem 13.

Corollary 19. *Suppose that $\overline{\rho}$ is modular of level $\ell^r N$ and character χ of conductor ℓN with $\ell \nmid N$. Then, $\overline{\rho}$ is modular of level N.*

Proof. Suppose that $\overline{\rho}$ arises from $F \in S^2_{(k_1,k_2)}(\ell^r N, \chi)$. Then, we can apply Theorem 13 to obtain a representation $\overline{\rho}'$ of level N such that the characteristic polynomials of $\overline{\rho}(\mathrm{Frob}_p)$ and $\overline{\rho}'(\mathrm{Frob}_p)$ are equal for all $p \nmid \ell N$. Thus, the characteristic polynomials of $\overline{\rho}$ and $\overline{\rho}'$ are equal everywhere by the Chebotarev Density Theorem. The Brauer-Nesbitt Theorem gives that $\overline{\rho}$ is isomorphic to $\overline{\rho}'$. ■

Note, this result allows one to remove the $\ell \nmid N$ condition from Conjecture 18 after placing the necessary restriction on the corresponding character.

To conclude the section, we make a brief comment concerning the ℓ-small condition on the exponents. In a recent paper, Yamauchi presents the following theorem.

Theorem 20 ([33, Thm. 1.1]). *Let $\overline{\rho}$ be an irreducible, odd Galois representation. Assume that $\overline{\rho}$ is modular. Then, there is some integer $0 \leqslant \alpha \leqslant \ell - 2$ and a (mod ℓ) eigenform F of weight (k,k) or $(k+1,k)$, for $k \geqslant 1$, such that F is not identically zero and $\overline{\rho} \cong \overline{\chi}_\ell^\alpha \otimes \overline{\rho}_F$.*

We should stress that that the eigenform F in the theorem is only defined modulo ℓ. Hence, it may not be realizable as a genuine eigenform. However, in the discussion following this theorem in [33], Yamauchi mentions that a forthcoming result of Boxer may allow one to show that $k \leqslant \ell + 1$, and then he provides an argument which would allow one to lift the form F to characteristic zero, i.e., to realize F as a genuine eigenform. If one had such a result, then the condition on the exponents being ℓ-small in Conjecture 18 could be removed.

5. Action of Hecke operators on Fourier coefficients

In this section, we provide explicit formulas for the action of Hecke operators on genus 2 Siegel modular forms. In particular, we provide a proof of Theorem 5. We will adapt techniques used by Andrianov in [3] for scalar weight modular forms to the vector valued setting.

First, we derive a basic property of Fourier coefficients, which will help motivate our technique. Let $F \in M^2_\rho(N,\chi)$. As we have seen, the Fourier expansion of F of the form

$$F(Z) = \sum_{T \in \Lambda_2} a_F(T) \exp(\mathrm{Tr}(TZ)) \qquad \text{with} \quad a_F(T) \in V,$$

where $\rho : \mathrm{GL}_2(\mathbb{C}) \to \mathrm{GL}(V)$. Furthermore, each Fourier coefficient is given by the integral

$$\int_{X \pmod 1} F(Z) \exp(-\mathrm{Tr}(TZ)) dX,$$

where we write $Z = X + iY$, dX is the Euclidean volume of the space of X coordinates, and the integral runs over $-1/2 \leqslant X_{ij} \leqslant 1/2$ for all i, j. This integral formula allows us to derive the following relationship between the Fourier coefficients of F,

$$\begin{aligned} a_F(MT\,{}^TM) &= \int_{X \pmod 1} F(Z)\exp(-\operatorname{Tr}(MT\,{}^TMZ))dX \\ &= \int_{X \pmod 1} F(Z)\exp(-\operatorname{Tr}(T\,{}^TMZM))dX \\ &= \chi(\det(M))\rho(M)\int_{X \pmod 1} F({}^TMZM)\exp(-\operatorname{Tr}(T\,{}^TMZM))dX \\ &= \chi(\det(M))\rho(M)a_F(T), \end{aligned}$$

where $M \in \mathrm{GL}_2(\mathbb{Z})$. Note, to move from the second line to the third line we use that

$$F(Z) = \chi(\det(M))\rho(M)F({}^TMZM),$$

which follows from the transformation property of F and noticing that

$$\begin{pmatrix} {}^TM & 0 \\ 0 & M^{-1} \end{pmatrix} \in \Gamma_0^2(N).$$

In summary, the desired property of the Fourier coefficients of F is

$$a_F(MT\,{}^TM) = \chi(\det(M))\rho(M)a_F(T), \text{ for all } M \in \mathrm{GL}_2(\mathbb{Z}). \tag{5.1}$$

With this property in mind, we define a more general space of functions. Let $\mathcal{F}(V)$ denote the space of holomorphic functions $F : \mathfrak{h}_2 \to V$ which have a Fourier expansion of the form

$$F(Z) = \sum_{T \in \Lambda_2} a_F(T)\exp(\operatorname{Tr}(TZ)) \qquad \text{with} \quad a_F(T) \in V.$$

Let ϵ be a character of the group $\mathrm{GL}_2(\mathbb{Z})$. Define a subspace $\mathcal{F}_\epsilon(V) \subset \mathcal{F}(V)$ by considering only functions $F \in \mathcal{F}(V)$ which satisfy

$$\epsilon(M)F(({}^TMZ + M')M) = F(Z), \qquad \text{for all} \quad \begin{pmatrix} {}^TM & M' \\ 0 & M^{-1} \end{pmatrix} \in P_4,$$

where P_4 is the Siegel parabolic subgroup. To summarize, we have defined the space $\mathcal{F}_\epsilon(V)$ to behave like modular forms with respect to the Siegel parabolic subgroup, rather than congruence subgroups. Using an argument as in the pre-

ceding paragraph we have that for $F \in \mathcal{F}_\epsilon(V)$, the Fourier coefficients satisfy

$$a_F(MT\ {}^TM) = \epsilon(M)a_F(T),$$

where $M \in \mathrm{GL}_2(\mathbb{Z})$. Note, by Equation 5.1, we have that $M^2_\rho(N,\chi) \subseteq \mathcal{F}_\epsilon(V)$ if $\epsilon(M) = \chi(\det(M))\rho(M)$. Throughout, we will fix a ρ, χ and set $\epsilon = \chi\rho$.

As our functions in $\mathcal{F}_\epsilon(V)$ behave like modular forms with respect to the Siegel parabolic subgroup, it makes sense to define the double coset operator in this setting

$$P_4\alpha P_4 : \mathcal{F}_\epsilon(V) \to \mathcal{F}_\epsilon(V),$$

given by

$$F[P_4\alpha P_4]_\epsilon = \sum_i \chi(\alpha_i)F|_\epsilon\alpha_i,$$

where we are summing over a complete set of coset representatives for $P_4\backslash P_4\alpha P_4$, $\alpha \in \mathrm{GSp}_4^+(\mathbb{Q})$ satisfies $c_\alpha = 0$, and the slash operator is defined to be

$$(F|_\epsilon\gamma)(Z) = \rho(d_\gamma)^{-1}F(\gamma Z).$$

In [3], Andrianov defines a map, ι, from $H^{\mathbb{Z}}(\Gamma_0^2(N))$ to the double coset operators of the type listed above. This map is defined by

$$\iota : \sum_i \Gamma_0^2(N)\alpha_i \mapsto \sum_i P_4\alpha_i.$$

The benefit of this map lies in the following lemma, which provides us with a compatibility between the Hecke operators on $M^2_\rho(N,\chi)$ and the double coset operators on $\mathcal{F}_\epsilon(V)$.

Lemma 21. *Let $F \in M^2_\rho(N,\chi)$. Then,*

$$TF = \iota(T)F, \qquad \textit{for every } \ T \in H^{\mathbb{Z}}(\Gamma_0^2(N)).$$

Proof. Note, this is stated as part of Lemma 4.12 from [3], we simply restate it here to emphasize that we are interested in vector valued modular forms, not just the scalar valued case.

The lemma follows from the fact that we can find coset representatives, $\{\alpha_i\}$ for T which have $c_{\alpha_i} = 0$ for all i. ■

With this lemma in mind, we use explicit coset representatives computed for double cosets of the form $P_4\backslash P_4\alpha P_4$ to compute formulas for the action of elements of $H^{\mathbb{Z}}(\Gamma_0^2(N))$. In fact, it is enough for our purposes to give coset representatives for ι applied to the generators of $H_p^{\mathbb{Z}}(\Gamma_0^2(N))$ taken from Theorem 4 for each $p \nmid N$. First, we give the image of these generators as double cosets, then we will give their explicit decompositions.

Lemma 22 ([3, Lemma 3.64]).

$$\begin{aligned}
\iota(T(p)) &= [P_4 \operatorname{diag}(p,p,1,1)P_4] + [P_4 \operatorname{diag}(p,1,1,p)P_4] + [P_4 \operatorname{diag}(1,1,p,p)P_4],\\
\iota(T_1(p^2)) &= \frac{1}{p}[P_4 \operatorname{diag}(p,p,1,1)P_4][P_4 \operatorname{diag}(p,1,1,p)P_4]\\
&\quad + \frac{1}{p}[P_4 \operatorname{diag}(p,1,1,p)P_4][P_4 \operatorname{diag}(1,1,p,p)P_4]\\
&\quad + \frac{1}{p}[P_4 \operatorname{diag}(p,1,1,p)P_4]^2 - [P_4 \operatorname{diag}(p^2,1,1,p^2)P_4]\\
&\quad - \frac{p+1}{p^3}[P_4 \operatorname{diag}(p,p,1,1)P_4][P_4 \operatorname{diag}(1,1,p,p)P_4],\\
\iota(T_2(p^2)) &= \frac{1}{p^3}[P_4 \operatorname{diag}(p,p,1,1)P_4][P_4 \operatorname{diag}(1,1,p,p)P_4].
\end{aligned}$$

Combining Lemma 3.60 and Proposition 3.61 from [3], we obtain the following left coset decompositions for the double coset operators in the previous lemma,

$$\begin{aligned}
P_4\backslash P_4 \operatorname{diag}(p,p,1,1)P_4 &= P_4 \begin{pmatrix} pI_2 & 0_2 \\ 0_2 & I_2 \end{pmatrix},\\
P_4\backslash P_4 \operatorname{diag}(1,1,p,p)P_4 &= \bigcup_{B={}^TB\in M_2(\mathbb{Z})/p\mathbb{Z})} P_4 \begin{pmatrix} I_2 & B \\ 0_2 & pI_2 \end{pmatrix},\\
P_4\backslash P_4 \operatorname{diag}(p,1,1,p)P_4 &= \bigcup_{\substack{D\in S(p)\\ B(D)\,(\mathrm{mod}\ D)}} P_4 \begin{pmatrix} p\,{}^TD^{-1} & B \\ 0_2 & D \end{pmatrix},\\
P_4\backslash P_4 \operatorname{diag}(p^2,1,1,p^2)P_4 &= \bigcup_{\substack{D\in S(p^2)\\ B(D)\,(\mathrm{mod}\ D)}} P_4 \begin{pmatrix} p^2\,{}^TD^{-1} & B \\ 0_2 & D \end{pmatrix},
\end{aligned}$$

where $S(d) = \operatorname{SL}_2(\mathbb{Z})\backslash \operatorname{SL}_2(\mathbb{Z}) \operatorname{diag}(1,d) \operatorname{SL}_2(\mathbb{Z})$, $B(D) = \left\{B : {}^TBD = {}^TDB\right\}$, and $B \equiv B' \pmod D$ if $(B-B')D^{-1} \in M_2(\mathbb{Z})$.

With these left cosets, we are able to compute the action of each of these double cosets on the Fourier coefficients of elements of $M^2_\rho(N,\chi)$. We will only require the action for primes not dividing N.

Lemma 23. *Let $F \in M^2_\rho(N,\chi)$ and let $p \nmid N$ be a prime. Then,*

1. $a_{F[P_4 \operatorname{diag}(p,p,1,1)P_4]_\epsilon}(T) = \chi(p^2)a_F\left(\frac{T}{p}\right)$.
2. $a_{F[P_4\backslash P_4 \operatorname{diag}(1,1,p,p)P_4]_\epsilon}(T) = p^3\rho(\operatorname{diag}(p,p))^{-1}a_F(pT)$.
3. $a_{F[P_4\backslash P_4 \operatorname{diag}(p,1,1,p)P_4]_\epsilon}(T) = p\chi(p)\displaystyle\sum_{D\in S(p)} \rho(D)^{-1}a_F\left(\frac{DT\,{}^TD}{p}\right)$
4. $a_{F[P_4\backslash P_4 \operatorname{diag}(p,1,1,p)P_4]_\epsilon}(T) = p^2\chi(p^2)\displaystyle\sum_{D\in S(p^2)} \rho(D)^{-1}a_F\left(\frac{DT\,{}^TD}{p^2}\right)$.

We set $a_F(T) = 0$ if $T \notin \Lambda_2$.

Proof. This is essentially the proof of Lemma 4.14 in [3].

Number 1 follows immediately. Number 2 follows by decomposing

$$\begin{pmatrix} I_2 & B \\ 0_2 & pI_2 \end{pmatrix} = \begin{pmatrix} I_2 & 0_2 \\ 0_2 & pI_2 \end{pmatrix} \begin{pmatrix} I_2 & B \\ 0_2 & I_2 \end{pmatrix},$$

applying the definition of the slash operator, and noticing that there are p^3 elements of $M_2(\mathbb{Z}/p\mathbb{Z})$ which are symmetric.

To show the formula in Number 3, we begin by applying the appropriate left coset representatives to the Fourier expansion to obtain that

$$\chi(p) \sum_{\substack{D \in S(p) \\ B(D) \,(\mathrm{mod}\ D)}} \rho(D)^{-1} \sum_{T \in \Lambda_2} a_F(T) \exp(\mathrm{Tr}(T(p\,({}^T D^{-1} Z + B) D^{-1}))$$

is equal to

$$\chi(p) \sum_{\substack{D \in S(p) \\ B(D) \,(\mathrm{mod}\ D)}} \rho(D)^{-1} \sum_{T \in \Lambda_2} a_F\left(\frac{DT\,{}^T D}{p}\right) \exp(\mathrm{Tr}(TZ)) \exp\left(\mathrm{Tr}\left(\frac{DT\,{}^T DBD^{-1}}{p}\right)\right).$$

Thus, by fixing T, we have that $a_{F[P_4 \backslash P_4 \,\mathrm{diag}(1,1,p,p) P_4]_\epsilon}(T)$ is equal to

$$\chi(p) \sum_{\substack{D \in S(p) \\ B(D) \,(\mathrm{mod}\ D)}} \rho(D)^{-1} a_F\left(\frac{DT\,{}^T D}{p}\right) \exp\left(\mathrm{Tr}\left(\frac{DT\,{}^T DBD^{-1}}{p}\right)\right).$$

Furthermore, in the proof of Lemma 4.14 in [3], it is shown that for any $D \in S(p)$ we have

$$\sum_{B(D) \,(\mathrm{mod}\ D)} \exp\left(\mathrm{Tr}\left(\frac{DT\,{}^T DBD^{-1}}{p}\right)\right) = p.$$

Thus, our expression becomes

$$a_{F[P_4 \backslash P_4 \,\mathrm{diag}(1,1,p,p) P_4]_\epsilon}(T) = p\chi(p) \sum_{D \in S(p)} \rho(D)^{-1} a_F\left(\frac{DT\,{}^T D}{p}\right),$$

as desired. Note, the proof of Number 4 follows precisely the same argument as the proof of Number 3. ∎

We can combine Lemma 21, Lemma 22, and Lemma 23 to give formulas for the action of the Hecke operators in $H_p^{\mathbb{Z}}(\Gamma_0^2(N))$ on the Fourier coefficients of elements in $M_\rho^2(N, \chi)$ for all $p \nmid N$. Note, we will only be concerned with the action of $T(p)$ and $T_1(p^2)$, as we have already restricted to the eigenspace of $T_2(p^2)$. The explicit action of these operators on Fourier coefficients is given in Theorem 5.

Acknowledgements. The author would like to thank J. Brown for posing this this problem and for all of the helpful discussions along the way. Furthermore, the author would like to thank S. Böcherer and S. Nagaoka for providing a preprint which was crucial for the main result of this paper. Finally, the author would like to thank A. Pitale and R. Schmidt for the many helpful conversations concerning the main result of this paper.

References

[1] A. Andrianov, *On functional equations satisfied by spinor Euler products for Siegel modular forms of genus 2 with characters*, Abh. Math. Sem. Univ. Hamburg **71** (2001), 123–142.

[2] A. Andrianov, *On diagonalization of singular Frobenius operators on Siegel modular forms*, Amer. J. Math. **125** (2003), 139–165.

[3] A. Andrianov, *Introduction to Siegel modular forms and Dirichlet series*, Universitext. Springer, New York, NY, 2009.

[4] T. Arakawa, *Vector values Siegel's modular forms of degree two and the associated Andrianov l-functions*, Manuscripta Math. **44** (1983), 155–186.

[5] S. Böcherer, *On the Hecke operator U(p)*, J. Math. Kyoto Univ. **45-4** (2005), 807–829.

[6] S. Böcherer and S. Nagaoka, *On p-adic properties of Siegel modular forms*, In Automorphic Forms, volume 115 of Springer proceedings in mathematics and statistics, pages 47–66. Springer, 2014.

[7] J. Brown and R. Keaton, *Level stripping for Siegel modular forms with reducible Galois representations*, J. Number Theory **133**(5) (2013), 1492–1501.

[8] P. Deligne and J-P. Serre, *Formes modulaires de poids 1*, Ann. scient. Ec. Norm. Sup. **7** (1974), 507–530.

[9] F. Diamond, *The refined conjecture of Serre*, In J. Coates and S.-T. Yau, editors, Elliptic Curves and Fermat's Last Theorem, pages 172–186. International Press, 1997.

[10] W. Fulton and J. Harris, *Representation theory: A first course*, volume 129 of Graduate Texts in Mathematics, Springer-Verlag, 1991.

[11] K. Hatada, *On classical and ℓ-adic modular forms of levels $N\ell^m$ and N*, J. Number Theory **87** (2001), 1–14.

[12] F. Herzig and J. Tilouine, *Conjecture de type de Serre et formes compagnons pour GSp_4*, J. Reine Angew. Math. **676** (2013), 1–32.

[13] T. Ichikawa, *Vector valued p-adic Siegel modular forms*, J. reine angew. Math. **690** (2014), 35–49.

[14] R. Keaton, *Level stripping for degree 2 Siegel modular forms*, Math. Res. Lett. **20**(5) (2013), 919–932.

[15] C. Khare and J-P. Wintenberger, *Serre's modularity conjecture (I)*, Invent. Math. **178** (2009), 485–504.

[16] C. Khare and J-P. Wintenberger, *Serre's modularity conjecture (II)*, Invent. Math. **178** (2009), 505–586.

[17] T. Kikuta, *On p-adic Siegel modular forms of non-real nebentypus of degree 2*, Acta Arith. **152** (2012), 175–183.
[18] N. Kurokawa, *On Siegel eigenforms*, Proc. Japan Acad. Ser. A **57** (1981), 47–50.
[19] G. Laumon, *Fonctions zéta des variétés de Siegel de dimension trois*, Astérisque **302** (2005), 1–66.
[20] W. Li, *Newforms and functional equations*, Math. Ann. **212** (1975), 285–315.
[21] S. Mizumoto, *Congruences for Fourier coefficients of lifted Siegel modular forms I: Eisenstein lifts*, Abh. Math. Sem. Univ. Hamburg **75** (2005), 97–120.
[22] K. Ribet, *Report on mod ℓ representations of $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$*, in Motives, volume 55 of Proc. Sympos. Pure. Math, pages 639–676, Providence, RI, 1994. Amer. Math. Soc.
[23] J-P. Serre, *Sur les représentations modulaires de degré 2 de $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$*, Duke Math. J. **54**(1) (1987), 179–230.
[24] C. Skinner and E. Urban, *Sur les deformations p-adiques de certain representations automorphes*, J. Inst. Math. Jussieu **5** (2006), 629–698.
[25] H. Takayanagi, *Vector valued Siegel modular forms and their L-functions; Application of a differential operator*, Japan J. Math. **19** (1994), 251–297.
[26] Y. Takei, *On algebraicity of vector valued Siegel modular forms*, Kodai Math. J. **15** (1992), 445–457.
[27] R. Taylor, *On congruences between modular forms*, PhD thesis, Princeton University, 1988.
[28] J. Tilouine, *Deformations of Galois representations and Hecke algebras*, Narosa Publishing House, 1996.
[29] E. Urban, *Sur les représentations p-adiques associées aux représentations cuspidales de $GSp_4(\mathbb{Q})$*, Astérisque **302** (2005), 151–176.
[30] G. van der Geer, *Siegel modular forms and their applications*, in 1-2-3 of Modular Forms, Lectures at a Summer School in Nordfjordeid, Norway, pages 181–246. Universitext, 2008.
[31] R. Weissauer, *Four dimensional Galois representations*, Astérisque **302** (2005), 67–150.
[32] R. Weissauer, *Existence of Whittaker models related to four dimensional symplectic Galois representations*, in Modular Forms on Schiermonnikoog, pages 285–310, Cambridge Univ. Press, 2008.
[33] T. Yamauchi, *The weight in Serre's conjecture for GSp_4*, arXiv:1410.7894, 2014.

Address: Rodney Keaton: Department of Mathematics, University of Oklahoma, Norman, Oklahoma, USA.

E-mail: rkeaton@math.ou.edu

Received: 4 September 2015; **revised:** 19 October 2015

INFORMATION FOR AUTHORS

Functiones et Approximatio Commentarii Mathematici publishes original papers in mathematics with special attention to analysis (in a broad sense) and number theory. Submission of a manuscript implies that the work has not been published before (except in the form of an abstract), that it is not under consideration for publication elsewhere, and that it will not be submitted elsewhere unless it has been rejected by the editors of Functiones et Approximatio. On the proof stage, the author will be asked to transfer copyright of the article to the publisher.

Manuscripts should be submitted electronically, preferably by sending a PDF file to fa@amu.edu.pl. Sending two hard copies is also possible, but electronic submission is preferred. On acceptance of the paper the authors will be also asked to transmit the TEX source file. The authors affiliation should be given at the end of the manuscript.

An abstract of not more than 200 words, 2010 Mathematical Subject Classification and key words are required.

References should be arranged in alphabetical order and labeled with numbers. The theorems, lemmas, ect. should be numbered consecutively within sections. The formulas must be numbered in similar but independent way. Figures must be arranged in a form suitable for direct reproducing, EPS (min. 1200 dpi) files are preferred. The use of very thin lines should be avoided.

The corresponding author may request 25 free offprints or the final PDF file of the article when sending the proof corrections.

Publikacja sfinansowana przez Wydział Matematyki i Informatyki UAM

Redaktor techniczny: Elżbieta Rygielska

Łamanie komputerowe: Łukasz Pańkowski

ISBN 978-83-232-3031-1
ISSN 0208-6573

WYDAWNICTWO NAUKOWE UNIWERSYTETU IM. ADAMA MICKIEWICZA W POZNANIU
61-701 POZNAŃ, UL. FREDRY 10
www.press.amu.edu.pl
Sekretariat: tel. 61 829 46 46, faks 61 829 46 47, e-mail: wydnauk@amu.edu.pl
Dział sprzedaży: tel. 61 829 46 40, e-mail: press@amu.edu.pl

Ark. wyd. 11,00. Ark. druk. 8,875.

DRUK I OPRAWA: EXPOL, WŁOCŁAWEK, UL. BRZESKA 4

ISBN 978-83-232-3031-1
ISSN 0208-6573