Canad. J. Math. Vol. **65** (6), 2013 pp. 1320–1383
http://dx.doi.org/10.4153/CJM-2013-027-0

Orbital L-functions for the Space of Binary Cubic Forms

Takashi Taniguchi and Frank Thorne

Abstract. We introduce the notion of orbital L-functions for the space of binary cubic forms and investigate their analytic properties. We study their functional equations and residue formulas in some detail. Aside from their intrinsic interest, the results from this paper are used to prove the existence of secondary terms in counting functions for cubic fields. This is worked out in a companion paper.

1 Introduction

The theory of *prehomogeneous vector spaces* was initiated by M. Sato in early 1960s. A finite dimensional representation of complex algebraic group (G, V) is called a prehomogeneous vector space if there exists a Zariski open orbit. One arithmetic significance of this is, that if (G, V) is defined over a number field, then there exist *zeta functions* associated to (G, V) which have analytic continuations and satisfy functional equations. This was discovered by M. Sato and T. Shintani [24] and numerous number-theoretic applications have been given (see, *e.g.*, [3, 10, 15, 25–27, 31, 32].)

Let (G, V) be the space of binary cubic forms:

$$G := \mathrm{GL}_2, \quad V := \{x(u, v) = x_1u^3 + x_2u^2v + x_3uv^2 + x_4v^3\}.$$

The discriminant $\mathrm{Disc}(x(u, v)) = x_2^2x_3^2 + 18x_1x_2x_3x_4 - 4x_1x_3^3 - 4x_2^3x_4 - 27x_1^2x_4^2$ is relatively invariant under the action of G, *i.e.*, $\mathrm{Disc}(gx) = (\det g)^2 \mathrm{Disc}(x)$. We denote by V^* the dual representation of G, which is similar to V but has a slightly different integral structure.

This (G, V) is an interesting example of a prehomogeneous vector space, and the associated zeta functions were studied extensively by Shintani [25]. He introduced the Dirichlet series

$$\xi_\pm(s) := \sum_{\substack{x\in \mathrm{SL}_2(\mathbb{Z})\backslash V(\mathbb{Z})\\ \pm \mathrm{Disc}(x)>0}} \frac{|\,\mathrm{Stab}(x)|^{-1}}{|\,\mathrm{Disc}(x)|^s}$$

associated to the positive and negative subsets of $V(\mathbb{Z})$, and the similarly associated $\xi^*_\pm(s)$ to $V^*(\mathbb{Z})$. (Here $|\,\mathrm{Stab}(x)|$ is the order of the stabilizer of x in $\mathrm{SL}_2(\mathbb{Z})$.) Then he established their notable analytic properties.

Received by the editors March 20, 2012.

Published electronically October 9, 2013.

The first author was partially supported by the Japan Society for the Promotion of Science, Grant-in-Aid No. 20740018, and a JSPS Postdoctoral Fellowship for Research Abroad. The second author was partially supported by the National Science Foundation, Grant DMS-0802967.

AMS subject classification: **11M41**, 11E76.

Keywords: binary cubic forms, prehomogeneous vector spaces, Shintani zeta functions, L-functions, cubic rings and fields.

Theorem 1.1 (Shintani) *The four Dirichlet series $\xi_\pm(s)$ and $\xi^*_\pm(s)$ have holomorphic continuations to the whole complex plane except for simple poles at $s = 1, 5/6$, and we have explicit formulas for their residues. Moreover, these Dirichlet series satisfy the functional equation*

$$\begin{pmatrix}\xi_+(1-s)\\ \xi_-(1-s)\end{pmatrix} = \frac{3^{3s-2}}{2\pi^{4s}}\Gamma(s)^2\Gamma\Big(s-\frac{1}{6}\Big)\Gamma\Big(s+\frac{1}{6}\Big)\begin{pmatrix}\sin 2\pi s & \sin \pi s\\ 3\sin\pi s & \sin 2\pi s\end{pmatrix}\begin{pmatrix}\xi^*_+(s)\\ \xi^*_-(s)\end{pmatrix}.$$

The purpose of this paper is to study L-functions corresponding to Shintani's zeta functions, extending Datskovsky and Wright's work [2]. Let us briefly explain our formulation. We fix a positive integer N. For any $a \in \mathbb{Z}$, the usual partial zeta function $\zeta(s,a)$ is defined by the formula $\zeta(s,a) = \sum_{n\in a+N\mathbb{Z}, n>0} n^{-s}$. Extending this idea, for any $a \in V(\mathbb{Z})$ we define the *partial zeta function* by

$$\xi_\pm(s,a) := \frac{1}{[\mathrm{SL}_2(\mathbb{Z}) : \Gamma(N)]}\sum_{\substack{x\in\Gamma(N)\backslash(a+NV(\mathbb{Z}))\\ \pm\,\mathrm{Disc}(x)>0}}\frac{|\,\mathrm{Stab}(x)|^{-1}}{|\,\mathrm{Disc}(x)|^s}.$$

Here $\Gamma(N)$ is the principal congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$, and now $|\,\mathrm{Stab}(x)|$ denotes the size of the group of stabilizers of x in $\Gamma(N)$. Since $\xi_\pm(s,a')$ counts the same orbits if $a' \equiv a \pmod N$, it is natural to regard a of $\xi_\pm(s,a)$ as an element of $V(\mathbb{Z}/N\mathbb{Z})$ rather than of $V(\mathbb{Z})$. We can easily check that $\xi_\pm(s) = \sum_{a\in V(\mathbb{Z}/N\mathbb{Z})}\xi_\pm(s,a)$, as expected.

Recall that the group $G(\mathbb{Z}/N\mathbb{Z})$ acts on $V(\mathbb{Z}/N\mathbb{Z})$. We may now define the *orbital L-function* by

$$\xi_\pm(s,\chi,a) := \sum_{g\in G(\mathbb{Z}/N\mathbb{Z})}\chi(\det g)\xi_\pm(s,ga)$$

for a Dirichlet character χ modulo N. We hope the analogy to the Dirichlet L-function $L(s,\chi) = \sum_{t\in(\mathbb{Z}/N\mathbb{Z})^\times}\chi(t)\zeta(s,t)$ is clear.[1] This orbital L-function seems to be a natural class of L-functions in the theory of prehomogeneous vector spaces, and we focus on this $\xi_\pm(s,\chi,a)$. We note that certain L-functions are introduced and studied in detail in the extensive works of Datskovsky and Wright [2, 29], and our orbital L-functions are closely related to theirs.

In this paper we prove three main results. The first one establishes fundamental analytic properties for our zeta functions.

Theorem 1.2 *For any congruence N, the orbital L-functions $\xi_\pm(s,\chi,a)$ and the partial zeta functions $\xi_\pm(s,a)$ have meromorphic continuations to whole complex plane and satisfy certain functional equations. They are holomorphic except for possible simple poles at $s = 1$ and $s = 5/6$, and their residues are described in terms of certain sums over the $G(\mathbb{Z}/N\mathbb{Z})$-orbit of $a \in V(\mathbb{Z}/N\mathbb{Z})$. We have explicit formulas of those residues in various cases. In particular, we have residue formulas when $a \in V(\mathbb{Z})$ detects cubic rings maximal at all primes dividing N, or when N is cube free.*

[1] As we will see in Lemma 3.3 (iii), strong approximation for SL_2 implies that the action of $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ on (the space of) partial zeta functions is trivial. Hence it is enough to work with one-dimensional representations $\chi\circ\det$ of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$; we can isolate each $\xi_\pm(s,a)$ by the orthogonality of characters on $(\mathbb{Z}/N\mathbb{Z})^\times$.

https://doi.org/10.4153/CJM-2013-027-0 Published online by Cambridge University Press

Hence, in principle we can understand the contributions of an arbitrary subset $X \subset V(\mathbb{Z})$ to the zeta function, as long as X is defined by a finite number of congruence conditions in $V(\mathbb{Z})$. We note that the first statement in this theorem is due to F. Sato [22]. This theorem is a combination of various results in this paper, and we give the proof in Remark 8.21. This result implies that there is a bias for the class numbers of integral binary cubic forms in arithmetic progressions, which seems to have been missed in the literature. We prove it in Theorem 9.2.

For a function f on $V(\mathbb{Z}/N\mathbb{Z})$, its finite Fourier transform $\widehat{f}$ is defined by

$$\widehat{f}(b) := N^{-4} \sum_{a \in V(\mathbb{Z}/N\mathbb{Z})} f(a) \exp\Big(2\pi\sqrt{-1} \cdot \frac{[a,b]}{N}\Big), \quad b \in V^*(\mathbb{Z}/N\mathbb{Z}),$$

where $[*,*]$ is the canonical pairing between V and V^*. Our second result is explicit formulas of the Fourier transforms of certain functions on $V(\mathbb{Z}/p^2\mathbb{Z})$.

Theorem 1.3 (Theorems 6.3, 6.4) *Let p be a prime not equal to 2 and 3. We have explicit formulas of the Fourier transforms of Φ_p and Φ'_p, where these are functions over $V(\mathbb{Z}/p^2\mathbb{Z})$ detecting nonmaximal and nonmaximal-or-totally-ramified cubic rings at p, respectively.*

See Theorems 6.3 and 6.4 for the exact formulas. These Fourier transforms occur in the explicit formulas for the zeta and L-functions dual to $\xi_\pm(s,a)$ and $\xi_\pm(s,\chi,a)$, and Theorem 1.3 allows us to write down these explicit formulas. This leads to an improved analytic understanding of $\xi_\pm(s,a)$ and $\xi_\pm(s,\chi,a)$.

Remark 1.4 Fouvry and Katz [7] have proved related bounds for such Fourier transforms, in a vastly more general context. As an application involving the space of binary cubic forms, they proved that there are infinitely many primes $p \equiv 1 \pmod 4$ for which $p+4$ is squarefree and $3 \nmid h(p+4)$.

Their bounds are stated only for exponential sums modulo p, and even if their methods could be used for sums over V_{p^2} it seems unlikely that their bounds would be sharp in the cases of our interest. That said, Fouvry and Katz's work predicts the phenomenon, observed in Theorems 6.3 and 6.4, that the Fourier transforms of Φ_p and Φ'_p are larger on the more singular orbits.

Theorem 1.2, in combination with explicit results such as Theorem 1.3, has fruitful arithmetic applications. To explain our motivation, we quote the main results of our companion paper [28]. Our primary purpose in proving Theorems 6.3 and 6.4 is to obtain the following density theorems.

Theorem 1.5 ([28])

(i) *The number of cubic fields K with $0 < \pm\operatorname{Disc}(K) < X$ is*

$$N_3^\pm(X) = \frac{C^\pm}{12\zeta(3)}X + K^\pm \frac{4\zeta(1/3)}{5\Gamma(2/3)^3\zeta(5/3)}X^{5/6} + O(X^{7/9+\epsilon}),$$

where $C^+ = K^+ = 1$ and $C^- = 3, K^- = \sqrt{3}$.

https://doi.org/10.4153/CJM-2013-027-0 Published online by Cambridge University Press

(ii) *For a quadratic field F, let $\mathrm{Cl}_3(F)$ denote the 3-torsion subgroup of the ideal class group of F. Then*

$$\sum_{\substack{[F:\mathbb{Q}]=2\\ 0<\pm\,\mathrm{Disc}(F)<X}} \#\,\mathrm{Cl}_3(F) = \frac{3+C^{\pm}}{\pi^2}X + K^{\pm}\frac{8\zeta(1/3)}{5\Gamma(2/3)^3}\prod_p\Bigl(1-\frac{p^{1/3}+1}{p(p+1)}\Bigr)X^{5/6} + O(X^{18/23+\epsilon}),$$

where the product in the secondary term is over all primes.

These secondary terms in Theorem 1.5 were also proved in independent work of Bhargava, Shankar, and Tsimerman [1]. Their paper studies the space (G,V) geometrically, and does not apply the theory of the associated zeta or L-functions.

We generalize this theorem to count these discriminants in arbitrary arithmetic progressions as well. In this case we discover a curious bias in the secondary term. For example, when the modulus m is not divisible by 4 we prove the following.

Theorem 1.6 ([28]) *Suppose m is a positive integer with $4 \nmid m$ and $a \in \mathbb{Z}$ arbitrary.*

(i) *The number of cubic fields K with*

$$0 < \pm\,\mathrm{Disc}(K) < X \quad \textit{and} \quad \mathrm{Disc}(K) \equiv a \pmod{m}$$

is

$$N_3^{\pm}(X;m,a) = C_1^{\pm}\bigl(m,(m,a)\bigr)X + K_1^{\pm}(m,a)X^{5/6} + O(X^{7/9+\epsilon}m^{8/9}).$$

The constant $C_1^{\pm}$ depends only on m and the greatest common divisor (m,a) of m and a, but $K_1^{\pm}$ may be different for different values of a, even when m and (m,a) are fixed, if there exist any nontrivial cubic characters modulo $m/(m,a)$.

(ii) *We have*

$$\sum_{\substack{[F:\mathbb{Q}]=2\\ 0<\pm\,\mathrm{Disc}(F)<X\\ \mathrm{Disc}(F)\equiv a \bmod m}} \#\,\mathrm{Cl}_3(F) = C_2^{\pm}\bigl(m,(m,a)\bigr)X + K_2^{\pm}(m,a)X^{5/6} + O(X^{18/23+\epsilon}m^{20/23}),$$

where $C_2^{\pm}$ and $K_2^{\pm}$ have the same properties as $C_1^{\pm}$ and $K_1^{\pm}$, respectively.

We refer to [28] for more explicit and general statements, including an explicit evaluation of the constants $C_i^{\pm}, K_i^{\pm}$, as well as associated numerical data. When $4 \mid m$ the statements change slightly (the discriminant of any field is $\equiv 0, 1 \pmod{4}$), but we treat this case as well.

Concerning Theorem 1.6, Datskovsky and Wright [2] proved that certain L-functions may have a pole if the character is cubic but are otherwise entire, and this is the origin of subtle behaviours of $K_i^{\pm}$. In Section 8 we refine their significant residue formulas [2] for $\xi_{\pm}(s,\chi,a)$, and in particular we complete all the cases where a detects cubic rings maximal at all primes dividing N. These formulas are used in [28] to obtain the explicit formulas for $K_i^{\pm}$. In Section 9, we briefly discuss how Theorem 1.6 relates to these residue formulas.

https://doi.org/10.4153/CJM-2013-027-0 Published online by Cambridge University Press

Besides these arithmetic applications, our explicit construction of L-functions is also motivated by work of Ohno and Nakagawa. In 1997, Ohno [16] conjectured the remarkably simple relations $\xi_+^*(s) = \xi_-(s)$ and $\xi_-^*(s) = 3\xi_+(s)$, and these relations were proved by Nakagawa [15]. As a consequence, Shintani's functional equation in Theorem 1.1 takes the following self-dual form.

Theorem 1.7 (Ohno–Nakagawa) *Let $\theta_\pm(s) := \sqrt{3}\xi_+(s) \pm \xi_-(s)$ for each sign. Then*

$$\Delta_\pm(1-s)\theta_\pm(1-s) = \Delta_\pm(s)\theta_\pm(s),$$

where

$$\Delta_+(s) := \left(\frac{2^4 3^3}{\pi^4}\right)^{s/2}\Gamma\left(\frac{s}{2}\right)\Gamma\left(\frac{s}{2}+\frac{1}{2}\right)\Gamma\left(\frac{s}{2}-\frac{1}{12}\right)\Gamma\left(\frac{s}{2}+\frac{1}{12}\right),$$
$$\Delta_-(s) := \left(\frac{2^4 3^3}{\pi^4}\right)^{s/2}\Gamma\left(\frac{s}{2}\right)\Gamma\left(\frac{s}{2}+\frac{1}{2}\right)\Gamma\left(\frac{s}{2}+\frac{5}{12}\right)\Gamma\left(\frac{s}{2}+\frac{7}{12}\right).$$

If we put $\Delta(s) = \left(\begin{smallmatrix}\Delta_+(s) & 0\\ 0 & \Delta_-(s)\end{smallmatrix}\right)$ $T = \left(\begin{smallmatrix}\sqrt{3} & 1\\ \sqrt{3} & -1\end{smallmatrix}\right)$ and $\xi(s) = \left(\begin{smallmatrix}\xi_+(s)\\ \xi_-(s)\end{smallmatrix}\right)$, then the formula is

$$\Delta(1-s)\cdot T\cdot\xi(1-s) = \Delta(s)\cdot T\cdot\xi(s).$$

Although the formulas $\xi_+^*(s) = \xi_-^*(s)$ and $\xi_-^*(s) = 3\xi_+(s)$ are very simple, Nakagawa's proof is quite technical; in particular, he used class field theory in a sophisticated manner. Analogous formulas were proved by Ohno, the first author, and Wakatsuki [17, 18] for zeta functions associated with other integral models for (G, V), leading to similar functional equations.

In this paper we will prove the following.

Theorem 1.8 (Theorem 7.6) *For a positive integer m, let*

$$\xi_{m,\pm}(s) := \sum_{\substack{x\in\mathrm{SL}_2(\mathbb{Z})\backslash V(\mathbb{Z})\\ m\mid\mathrm{Disc}(x)\\ \pm\,\mathrm{Disc}(x)>0}} \frac{|\,\mathrm{Stab}(x)|^{-1}}{|\,\mathrm{Disc}(x)|^s}, \qquad \xi_m(s) := \begin{pmatrix}\xi_{m,+}(s)\\ \xi_{m,-}(s)\end{pmatrix},$$

and for a square free integer N, write

$$\theta_N(s) := \sum_{m\mid N}\mu(m)m\xi_m(s).$$

With this notation, $\theta_N(s)$ satisfies the functional equation

$$N^{2(1-s)}\Delta(1-s)\cdot T\cdot\theta_N(1-s) = N^{2s}\Delta(s)\cdot T\cdot\theta_N(s).$$

Here $\mu(m)$ is the Möbius function. In Theorem 7.6, we also describe the residues of $\theta_N(s)$. The case $N = 1$ is Theorem 1.7, and we will in fact reduce the proof of this theorem to Ohno–Nakagawa's original formula. In the proof, we use Mori's explicit formulas [14] for certain orbital Gauss sums over $\mathbb{Z}/p\mathbb{Z}$.

https://doi.org/10.4153/CJM-2013-027-0 Published online by Cambridge University Press

As the terminology "orbital L-function" indicates, understanding the $G(\mathbb{Z}/N\mathbb{Z})$-orbit structure of $a \in V(\mathbb{Z}/N\mathbb{Z})$ is fundamental for the analysis of $\xi_{\pm}(s,\chi,a)$. We pursue the theory from this viewpoint. As we noted earlier, our L-functions are closely related to those studied by Datskovsky and Wright [2]. Although our work overlaps with theirs to some extent, our orbital L-functions have elementary and explicit descriptions, and we hope we have developed the theory to a point where it is quite usable in applications.

Although we focus on the particular example of the space of binary cubic forms, the definitions and basic properties studied in Sections 3 and 4 are applicable to general irreducible regular prehomogeneous vector spaces with a fixed integral model. Also, our arguments in Sections 5, 6 and 8, regarded as arguments over $\mathbb{Z}_p$, generalize to the integer ring of other local fields, and a version of Theorem 1.3 holds over an arbitrary local field with residue characteristic not 2 or 3. In a forthcoming paper (joint with Manjul Bhargava), this will be used to improve the error term in the function counting cubic extensions of any base number field, previously studied by Datskovsky and Wright [3].

We also discuss some related results and problems. When a Dirichlet series $\xi(s) = \sum a_n/n^s$ is given, it is natural to twist by a Dirichlet character χ, yielding the L-function $\xi(s,\chi) = \sum a_n\chi(n)/n^s$. L-functions of this type associated to prehomogeneous vector spaces have been previously discussed in the literature; see, *e.g.*, [11, 20–22]. For our case of the space of binary cubic forms, we discuss this $\xi(s,\chi)$ in Section 9. Since this $\xi(s,\chi)$ is expressed in terms of linear combinations of orbital L-functions of the form $\xi(s,\chi^2,a)$, in principle our theory contains the theory of $\xi(s,\chi)$. However, there are some rich stories involving $\xi(s,\chi)$ for which we do not yet have good analogues for $\xi(s,\chi,a)$. Among others, we mention the significant work of Denef and Gyoja [6], who proved an explicit formula for a certain Gauss sum. As a result, the functional equation of $\xi(s,\chi)$ turns out to have a nice simple form, as observed in [22]. Their work is notable because the formula is proved for a general prehomogeneous vector space. In this direction, although we obtain explicit formulas of orbital Gauss sums

$$W(\chi,a,b) := \sum_{g\in G(\mathbb{Z}/N\mathbb{Z})} \chi(\det g)\exp\Big(2\pi\sqrt{-1}\cdot\frac{[ga,b]}{N}\Big)$$

for some special $a \in V(\mathbb{Z}/N\mathbb{Z}), b \in V^*(\mathbb{Z}/N\mathbb{Z})$, it would be very interesting to further investigate the general case.

We also remark on the secondary pole of zeta functions for "cubic cases". What principle underlies the fact that the space of binary cubic forms (G,V) describes the family of cubic extensions? In 1992, Wright and Yukie [31] clarified that this is because the component group of the generic stabilizer is isomorphic to $\mathfrak{S}_3$, the permutation group of degree 3, and they studied the relationship of this fact to geometric interpretations of rational orbits. Among 29 types of irreducible regular prehomogeneous vector spaces classified by M. Sato and Kimura [23], 4 of them share this property, and hence they should be regarded as "cubic cases". One such cubic case is the representation $(\mathrm{GL}_2\times\mathrm{GL}_3^2, \mathrm{Aff}^2\otimes\mathrm{Aff}^3\otimes\mathrm{Aff}^3)$, and the global theory for a non-split form of this representation was given by the first author [27]. Interestingly, as

https://doi.org/10.4153/CJM-2013-027-0 Published online by Cambridge University Press

with the (G, V) studied in this paper, the secondary pole of the zeta function does not vanish under a twist by cubic characters. It is likely that this property is shared for all cubic case zeta functions, and ultimately this would reflect phenomena similar to Theorem 1.6.

This paper is organized as follows: in Section 2 we introduce the space of binary cubic forms V and its dual space V^*, with natural actions of $G = \mathrm{GL}_2$. We also recall the Delone–Faddeev correspondence. In Section 3 we introduce the orbital L-functions $\xi(s, \chi, a)$ and the orbital Gauss sums $W(\chi, a, b)$. In Section 4 we discuss the functional equations. These functional equations were obtained by F. Sato [22] in a general setting and we apply his result. We also introduce zeta functions $\xi(s, f)$ associated to G_N-relative invariant functions f, and express them in terms of orbital L-functions.

Later sections develop the more specific theory for (G, V). Let p be a prime. In Section 5, we give orbit descriptions over $\mathbb{Z}/p\mathbb{Z}$ and $\mathbb{Z}/p^2\mathbb{Z}$ which have arithmetic meanings. In Section 6, we discuss the orbital Gauss sums over $\mathbb{Z}/p\mathbb{Z}$ and $\mathbb{Z}/p^2\mathbb{Z}$ in detail. Over $\mathbb{Z}/p\mathbb{Z}$, this was studied by S. Mori [14] and we recall his result. After that, we compute various orbital Gauss sums over $\mathbb{Z}/p^2\mathbb{Z}$ for $p \neq 2, 3$, which is the main technical contribution of this paper, and we prove Theorem 1.3 as a consequence.

In Section 7, we study "divisible" zeta functions and prove Theorem 1.8.

In Section 8, we study the residues of the orbital L-functions $\xi(s, \chi, a)$. With a natural choice of the test function Φ_a, Wright's adelic zeta function [29] gives an integral expression for $\xi(s, \chi, a)$. Using the residue formula in [29], we compute the residues of $\xi(s, \chi, a)$ for the cases of our interest. The method as well as many of these results are due to Datskovsky and Wright [2], and our results refine theirs as needed for our application to Theorem 1.6. These computations lead to an explicit version of Theorem 1.2. In Section 9, we apply these results to prove residue formulas for $\xi(s, \chi)$ (Theorem 9.1) and we prove that class numbers of binary cubic forms are biased in arithmetic progressions (Theorem 9.2). We also compare our results to Theorem 1.6.

Notation

For a finite set X, we denote its cardinality by $|X|$. For a variety V defined over $\mathbb{Z}$ and a ring R, the set of R-rational points is denoted by V_R (rather than $V(R)$). The trivial Dirichlet character is denoted by $\mathbf{1}$. Our notation mostly matches the companion paper [28], but there are a few exceptions: the dual vector space V^* and the zeta function $\xi^*(s)$ for V^* in this paper are denoted by $\widehat{V}$ and $\widehat{\xi}(s)$ in [28], respectively. Also, $\xi_m(s)$ in this paper denotes the m-divisible zeta function, while $\xi_q(s)$ in [28] denotes the q-nonmaximal zeta function. We hope this does not confuse the reader.

2 The Space of Binary Cubic Forms and Cubic Rings

In this section, we introduce the space of binary cubic forms V and its dual space V^*, with natural actions of $G = \mathrm{GL}_2$. We regard G, V, and V^* as defined over $\mathbb{Z}$. After discussing their basic properties, we recall the Delone–Faddeev correspondence relating cubic forms to cubic rings.

https://doi.org/10.4153/CJM-2013-027-0 Published online by Cambridge University Press

Let $G = \mathrm{GL}_2$ and

$$V = \{x(u,v) = x_1u^3 + x_2u^2v + x_3uv^2 + x_4v^3 \mid x_1, x_2, x_3, x_4 \in \mathrm{Aff}\}.$$

We identify V with the four dimensional affine space Aff^4 via $x(u,v) = x_1u^3 + x_2u^2v + x_3uv^2 + x_4v^3 \leftrightarrow x = (x_1, x_2, x_3, x_4)$. We consider the following twisted action of G on V:

$$(g \cdot x)(u,v) = \frac{1}{\det g} x(\alpha u + \gamma v, \beta u + \delta v), \quad x \in V, \quad g = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in G.$$

We note that the scalar matrices act on V by the usual scalar multiplication. In terms of coordinates, the action is given by

$$ {}^t(g \cdot x) = \frac{1}{\alpha\delta - \beta\gamma} \begin{pmatrix} \alpha^3 & \alpha^2\beta & \alpha\beta^2 & \beta^3 \\ 3\alpha^2\gamma & \alpha^2\delta + 2\alpha\beta\gamma & \beta^2\gamma + 2\alpha\beta\delta & 3\beta^2\delta \\ 3\alpha\gamma^2 & \beta\gamma^2 + 2\alpha\gamma\delta & \alpha\delta^2 + 2\beta\gamma\delta & 3\beta\delta^2 \\ \gamma^3 & \gamma^2\delta & \gamma\delta^2 & \delta^3 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix}, $$
$$g = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}.$$

We usually omit $\cdot$ from $g \cdot x$ and write gx instead. Let

$$P(x) = x_2^2x_3^2 + 18x_1x_2x_3x_4 - 4x_1x_3^3 - 4x_2^3x_4 - 27x_1^2x_4^2,$$

which is the discriminant of $x(u,v)$. Then $P(gx) = (\det g)^2 P(x)$.

The dual representation V^* is the space of linear forms on V. In the dual coordinate system on V^*, we express elements of V^* as $y = (y_1, y_2, y_3, y_4)$. We denote the canonical pairing of V and V^* by $[x, y]$, so that $[x, y] = x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4$. We define the left action of G on V^* via $[x, g * y] = [(\det g)g^{-1} \cdot x, y]$. Then the scalar matrices also act by the usual scalar multiplication on V^*. In terms of coordinates, we have

$$ {}^t(g * y) = \frac{1}{\alpha\delta - \beta\gamma} \begin{pmatrix} \delta^3 & -3\gamma\delta^2 & 3\gamma^2\delta & -\gamma^3 \\ -\beta\delta^2 & \alpha\delta^2 + 2\beta\gamma\delta & -(\beta\gamma^2 + 2\alpha\gamma\delta) & \alpha\gamma^2 \\ \beta^2\delta & -(\beta^2\gamma + 2\alpha\beta\delta) & \alpha^2\delta + 2\alpha\beta\gamma & -\alpha^2\gamma \\ -\beta^3 & 3\alpha\beta^2 & -3\alpha^2\beta & \alpha^3 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{pmatrix}, $$
$$g = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}.$$

We usually omit $*$ from $g * y$ and write gy instead. Let

$$P^*(y) = 3y_2^2y_3^2 + 6y_1y_2y_3y_4 - 4y_1y_3^3 - 4y_2^3y_4 - y_1^2y_4^2.$$

Then $P^*(gy) = (\det g)^2 P^*(y)$.

https://doi.org/10.4153/CJM-2013-027-0 Published online by Cambridge University Press

We recall an embedding of V^* into V which is compatible with the action of G. Let

$$\iota \colon V^* \ni (y_1, y_2, y_3, y_4) \mapsto (y_4, -3y_3, 3y_2, -y_1) \in V.$$

Then we have $\iota(g * y) = g \cdot \iota(y)$. Hence if 3 is not a zero divisor in a ring R, we can realize V_R^* as a G_R-submodule of V_R. Moreover, if 3 is invertible in R then we can identify V_R^* with V_R in terms of ι. We use this identification in Section 6. Under this identification, the bilinear form on V induced by the pairing $[*, *]$ is given as

$$(2.1) \qquad [x, x'] = x_4x_1' - \frac{1}{3}x_3x_2' + \frac{1}{3}x_2x_3' - x_1x_4', \quad x, x' \in V,$$

and this satisfies $[gx, gx'] = (\det g)[x, x']$. We also note that $P\big(\iota(y)\big) = 27P^*(y)$.

We now recall the so-called *Delone–Faddeev correspondence*, which gives a ring-theoretic interpretation of rational orbits of (G, V). This was originally discovered by Levi in certain cases, was described in the textbook of Delone and Faddeev [5], and was then proved by Gan, Gross and Savin [8] in full generality.

Let R be an arbitrary (commutative) ring. A finite R-algebra S is called a *cubic ring over R* if S is free of rank 3 as an R-module.

Theorem 2.1 (Levi; [5], [8]) *There is a canonical discriminant-preserving bijection between the set of orbits $G_R \backslash V_R$ and the set of isomorphism classes of cubic rings over R. If $x \in V_R$ corresponds to a cubic ring S over R, then the group of stabilizers $G_{R,x}$ of x in G_R is isomorphic to* $\mathrm{Aut}_R(S)$, *the group of automorphisms of S as an R-algebra. Moreover if $x \in V_R$ is of the form $x(u, v) = u^3 + bu^2v + cuv^2 + dv^3$, then the corresponding cubic ring is $R[X]/(X^3 + bX^2 + cX + d)$. Also if x is of the form $x(u, v) = v(u^2 + cuv + dv^2)$, then the corresponding cubic ring is $R \times R[X]/(X^2 + cX + d)$.*

The proof of this theorem is well known. We simply recall the construction here. For $x = (x_1, x_2, x_3, x_4) \in V_R$, the corresponding cubic ring is the R-module $R1 \oplus R\omega \oplus R\theta$ with the commutative multiplicative structure so that 1 is the multiplicative identity and that

$$\omega^2 = -x_1x_3 - x_2\omega + x_1\theta, \quad \theta^2 = -x_2x_4 - x_4\omega + x_3\theta, \quad \omega\theta = -x_1x_4.$$

For more details, see [8] for example.

3 Orbital L-functions and Orbital Gauss Sums

In this section, we introduce the notion of *orbital L-functions* and *orbital Gauss sums*, and discuss their most basic properties. Further analytic properties are studied in later sections.

Let N be a positive integer. We put

$$G_N := G_{\mathbb{Z}/N\mathbb{Z}} = \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}), \quad V_N := V_{\mathbb{Z}/N\mathbb{Z}} \cong V_{\mathbb{Z}}/NV_{\mathbb{Z}}.$$

Then G_N acts on V_N. For $a \in V_N$, let $G_{N,a} := \{g \in G_N \mid ga = a\}$, the group of stabilizers. For each $a \in V_N$, $a + NV_{\mathbb{Z}}$ is invariant under the action of the principal

https://doi.org/10.4153/CJM-2013-027-0 Published online by Cambridge University Press

congruence subgroup $\Gamma(N) := \ker\big(\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})\big)$ of $\mathrm{SL}_2(\mathbb{Z})$. Let χ be a Dirichlet character whose conductor $m = m(\chi)$ is a divisor of N. As usual, we regard χ as a character modulo N via the reduction map $(\mathbb{Z}/N\mathbb{Z})^\times \to (\mathbb{Z}/m\mathbb{Z})^\times$.

For a congruence subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$ and a Γ-invariant subset X of $V_\mathbb{Z}$, we put

$$\xi_\pm(s, X, \Gamma) := \frac{1}{[\mathrm{SL}_2(\mathbb{Z}) : \Gamma]} \sum_{\substack{x \in \Gamma \backslash X \\ \pm P(x) > 0}} \frac{|\Gamma_x|^{-1}}{|P(x)|^s}$$

where $\Gamma_x = \{\gamma \in \Gamma \mid \gamma x = \gamma\}$, and

$$\xi(s, X, \Gamma) := \begin{pmatrix} \xi_+(s, X, \Gamma) \\ \xi_-(s, X, \Gamma) \end{pmatrix}.$$

We put

$$\xi(s) := \xi\big(s, V_\mathbb{Z}, \mathrm{SL}_2(\mathbb{Z})\big).$$

This is the zeta function introduced and studied by Shintani [25]. As a generalisation, we introduce the following.

Definition 3.1 We define

$$\xi(s, a) := \xi\big(s, a + NV_\mathbb{Z}, \Gamma(N)\big),$$

$$\xi(s, \chi, a) := \sum_{g \in G_N} \chi(\det g)\xi(s, ga).$$

We call $\xi(s, a)$ a *partial zeta function* and $\xi(s, \chi, a)$ an *orbital L-function* for the space of binary cubic forms.

Remark 3.2 We will observe in Propositions 4.6 and 4.7 that we can define $\xi(s, \chi, a)$ in terms of only $\mathrm{SL}_2(\mathbb{Z})$ and not $\Gamma(N)$.

For these zeta functions, the following basic properties hold.

Lemma 3.3

(i) *For* $g \in G_N$, $\xi(s, \chi, ga) = \chi(\det g)^{-1}\xi(s, \chi, a)$.
(ii) *We have* $\sum_{a \in V_N} \xi(s, a) = \xi(s)$.
(iii) *If* $g \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$, *then* $\xi(s, ga) = \xi(s, a)$.

Proof These are not too difficult to verify from the definitions. Alternatively, one can apply Proposition 3.3 of [17] as follows: (i) immediately follows from the definition, while (ii) follows from [17, Proposition 3.3 (1) and (4)]. For (iii), first note that the canonical map $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ is surjective. Take any lift $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ of $g \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$, then $\gamma(a + NV_\mathbb{Z}) = ga + NV_\mathbb{Z}$ by definition. By [17, Proposition 3.3 (2)], we have

$$\begin{aligned} \xi(s, ga) &= \xi\big(s, ga + NV_\mathbb{Z}, \Gamma(N)\big) = \xi\big(s, \gamma(a + NV_\mathbb{Z}), \Gamma(N)\big) \\ &= \xi\big(s, \gamma(a + NV_\mathbb{Z}), \gamma\Gamma(N)\gamma^{-1}\big) = \xi\big(s, a + NV_\mathbb{Z}, \Gamma(N)\big) = \xi(s, a). \end{aligned}$$

Note that $\Gamma(N)$ is a normal subgroup of $\mathrm{SL}_2(\mathbb{Z})$. ■

https://doi.org/10.4153/CJM-2013-027-0 Published online by Cambridge University Press

We put

$$T := \left\{ t = \begin{pmatrix} 1 & 0 \\ 0 & t_1 \end{pmatrix} \;\middle|\; t_1 \in \mathrm{GL}_1 \right\} \cong \mathrm{GL}_1$$

and $T_N = T_{\mathbb{Z}/N\mathbb{Z}} \cong (\mathbb{Z}/N\mathbb{Z})^\times$. Then since $G = \mathrm{SL}_2 \rtimes T$, we can write $\xi(s, \chi, a)$ as

$$\xi(s, \chi, a) = \frac{|G_N|}{|T_N|} \sum_{t \in T_N} \chi(\det t)\xi(s, ta). \tag{3.1}$$

Since T_N is an abelian group, by the orthogonality of characters we have the following.

Proposition 3.4 *We have*

$$\xi(s, a) = |G_N|^{-1} \sum_{\chi} \xi(s, \chi, a).$$

Here χ runs through all the Dirichlet characters of conductors dividing N.

Hence the study of partial zeta functions is equivalent to that of orbital L-functions. Since orbital L-functions are theoretically more natural to study, we concentrate on these for the rest of this paper.

We put $V_N^* = V_{\mathbb{Z}/N\mathbb{Z}}^* \cong V_{\mathbb{Z}}^*/NV_{\mathbb{Z}}^*$. Then G_N acts on V_N^* also. We define the zeta functions for the dual $\xi^*(s, b), \xi^*(s, \chi, b)$ for each $b \in V_N^*$ in exactly the same way; letting

$$\xi_{\pm}^*(s, Y, \Gamma) := \frac{1}{[\mathrm{SL}_2(\mathbb{Z}) : \Gamma]} \sum_{\substack{y \in \Gamma \backslash Y \\ \pm P^*(y) > 0}} \frac{|\Gamma_y|^{-1}}{|P^*(y)|^s}, \quad \xi^*(s, Y, \Gamma) := \begin{pmatrix} \xi_+^*(s, Y, \Gamma) \\ \xi_-^*(s, Y, \Gamma) \end{pmatrix},$$

we define

$$\xi^*(s, b) := \xi^*\left(s, b + NV_{\mathbb{Z}}^*, \Gamma(N)\right),$$

$$\xi^*(s, \chi, b) := \sum_{g \in G_N} \chi(\det g)\xi^*(s, gb).$$

They satisfy the same properties in Lemma 3.3. Namely, $\sum_{b \in V_N^*} \xi^*(s, b) = \xi^*(s)$, $\xi^*(s, gb) = \xi^*(s, b)$ for $g \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$, and $\xi^*(s, \chi, gb) = \chi(\det g)^{-1}\xi^*(s, \chi, b)$. Here we put $\xi^*(s) = \xi^*\left(s, V_{\mathbb{Z}}^*, \Gamma(1)\right)$.

We note that $\xi^*(s, Y, \Gamma) = 27^s\xi\left(s, \iota(Y), \Gamma\right)$ where $\iota\colon V_{\mathbb{Z}}^* \to V_{\mathbb{Z}}$ is the embedding introduced in Section 2. The factor 27^s comes from the relation $P\left(\iota(y)\right) = 27P^*(y)$ for $y \in Y \subset V_{\mathbb{Z}}^*$. Also if Y is defined by congruence conditions modulo N in $V_{\mathbb{Z}}^*$, then $\iota(Y)$ is determined by congruence conditions modulo $3N$ in $V_{\mathbb{Z}}$. Hence it is possible to write $\xi^*(s, b)$ (and hence $\xi^*(s, \chi, b)$) in terms of linear combinations of $\xi(s, a)$.

We conclude this section with the definition of the orbital Gauss sum. For $a \in V_N, b \in V_N^*$, we put $\langle a, b \rangle := \exp(2\pi i[a, b]/N)$. If we emphasize the dependence on N, we write $\langle a, b \rangle_N$ also.

https://doi.org/10.4153/CJM-2013-027-0 Published online by Cambridge University Press

Definition 3.5 For $a \in V_N$, $b \in V_N^*$ we define

$$W(\chi, a, b) := \sum_{g \in G_N} \chi(\det g)\langle ga, b\rangle = \sum_{g \in G_N} \chi(\det g)\langle a, gb\rangle$$

and call it the *orbital Gauss sum.*

The second equality holds because $[a, gb] = [(\det g)g^{-1}a, b]$. If we emphasize the dependence on N, we write $W_N(\chi, a, b)$ also. The following immediately follows from the definition.

Lemma 3.6 *For* $g_1, g_2 \in G_N$,

$$W(\chi, g_1 a, g_2 b) = \chi(\det g_1)^{-1}\chi(\det g_2)^{-1}W(\chi, a, b).$$

In particular, if $\chi \circ \det$ *is nontrivial either on* $G_{N,a}$ *or* $G_{N,b}$, *then* $W(\chi, a, b) = 0$.

The significance of this character sum will be clarified in the next section. In particular, this appears in the functional equation satisfied by $\xi(s, \chi, a)$ and $\xi^*(s, \chi^{-1}, b)$.

4 Functional equation

In this section we discuss the functional equation of the zeta functions. To begin, we recall Shintani's functional equation [25].

Theorem 4.1 (Shintani) *Let*

$$M(s) := \frac{3^{3s-2}}{2\pi^{4s}}\Gamma(s)^2\Gamma\left(s - \frac{1}{6}\right)\Gamma\left(s + \frac{1}{6}\right)\begin{pmatrix} \sin 2\pi s & \sin \pi s \\ 3\sin \pi s & \sin 2\pi s \end{pmatrix}.$$

Then

$$\xi(1-s) = M(s) \cdot \xi^*(s).$$

An extension necessary for us was given by F. Sato [22] in a general setting. We recall his formula and apply it to our orbital L-functions. Let $C(V_N)$ and $C(V_N^*)$ be the space of $\mathbb{C}$-valued functions on V_N and V_N^*, respectively.

Definition 4.2 For $f \in C(V_N)$, $f^* \in C(V_N^*)$ we define the associated zeta functions as follows:

$$\xi(s, f) := \sum_{a \in V_N} f(a)\xi(s, a), \quad \xi^*(s, f^*) := \sum_{b \in V_N^*} f^*(b)\xi^*(s, b).$$

This is the most general class of the zeta functions from our viewpoint and this class contains partial zeta functions and orbital L-functions as special cases. Our main interest is the orbital L-function but the functional equation is described most naturally for this class. For $f \in C(V_N)$, we define its Fourier transform $\widehat{f} \in C(V_N^*)$ by

$$\widehat{f}(b) = N^{-4}\sum_{a \in V_N} f(a)\langle a, b\rangle.$$

https://doi.org/10.4153/CJM-2013-027-0 Published online by Cambridge University Press

By the Fourier inversion formula, we have $f(a) = \sum_{b\in V_N^*} \widehat{f}(b)\langle -a, b\rangle$.

By [22, Theorem Q], we have the following functional equation.

Theorem 4.3 (F. Sato) *We have*

$$\xi(1-s, f) = N^{4s} M(s) \cdot \xi^*(s, \widehat{f}).$$

Sketch of Proof For the convenience of the reader, we give a brief review of Sato's proof. Let $\mathscr{S}(V_{\mathbb{R}})$ be the space of Schwarz–Bruhat functions on $V_{\mathbb{R}}$. We let $G_{\mathbb{R}}^+ = \{g \in G_{\mathbb{R}} \mid \det g > 0\}$ and denote by dg_∞ a fixed Haar measure on it. We define the (vector valued) local zeta function

$$(4.1)\quad \Gamma_\infty(\Phi_\infty, s) := \Big(\int_{G_{\mathbb{R}}^+} |P(g_\infty x_+)|_\infty^s \Phi_\infty(g_\infty x_+)\, dg_\infty, \int_{G_{\mathbb{R}}^+} |P(g_\infty x_-)|_\infty^s \Phi_\infty(g_\infty x_-)\, dg_\infty\Big),$$

where $\Phi_\infty \in \mathscr{S}(V_{\mathbb{R}})$. Here $x_\pm \in V_{\mathbb{R}}^\pm = \{x \in V_{\mathbb{R}} \mid \pm P(x) > 0\}$ is arbitrary.

As in the proof of [26, Theorem 5], we can take $\Phi_\infty \in \mathscr{S}(V_{\mathbb{R}})$ such that Φ_∞ vanishes on $\{x \in V_{\mathbb{R}} \mid P(x) = 0\}$ and $\widehat{\Phi}_\infty$ vanishes on $\{y \in V_{\mathbb{R}}^* \mid P^*(y) = 0\}$, where we put $\widehat{\Phi}_\infty(y) = \int_{V_{\mathbb{R}}} \Phi(x)\exp(-2\pi i[x,y])\, dx$. For $x \in V_{\mathbb{Z}}, y \in V_{\mathbb{Z}}^*$, let $f(x) = f(x \bmod N)$ and $\widehat{f}(y) = \widehat{f}(y \bmod N)$. Then by the standard unfolding method[2] (see the proof of Proposition 8.2 for details),

$$\int_{G_{\mathbb{R}}^+/\Gamma(N)} |\det g_\infty|_\infty^{2s} \sum_{x\in V_{\mathbb{Z}}} f(x)\Phi_\infty(g_\infty x)\, dg_\infty = \Gamma_\infty(\Phi_\infty, s)\xi(s, f).$$

On the other hand, by the Poisson summation formula,

$$\sum_{x\in V_{\mathbb{Z}}} f(x)\Phi_\infty(g_\infty x) = |\det g_\infty|_\infty^{-2} \sum_{y\in V_{\mathbb{Z}}^*} \widehat{f}(y)\widehat{\Phi}_\infty\big((\det g_\infty)^{-1} g_\infty y/N\big).$$

The rest of argument is standard in the theory of prehomogeneous vector spaces and we omit the details. ∎

Hence the study of the Fourier transform $\widehat{f}$ is fundamental for further analysis of the functional equation.

Let $N = N_1 N_2$, where N_1 and N_2 are coprime integers. For $f^i \in C(V_{N_i})$ for $i = 1, 2$, we define $f^1 \times f^2 \in C(V_N)$ by

$$(f^1 \times f^2)(a) = f^1(a \bmod N_1) f^2(a \bmod N_2), \qquad a \in V_N.$$

We use the similar notation for the dual space. We note that the Fourier transform $(f^1 \times f^2)^\wedge$ of $f^1 \times f^2$ does *not* coincide with $\widehat{f^1} \times \widehat{f^2}$ in general. Instead, we have the following. For $t \in (\mathbb{Z}/N\mathbb{Z})^\times$, let $f_t(a) = f(ta)$.

[2] Though we use another integral expression for $\xi(s, \chi, a)$ to compute residue formulas in Section 8, we find this more convenient for proving the functional equation.

Lemma 4.4 *With the notation above, we have*

$$(f^1 \times f^2)^\wedge = (f^1_{N_2})^\wedge \times (f^2_{N_1})^\wedge.$$

Proof Let $f = f^1 \times f^2$. Then

$$f^\wedge(b) = N_1^{-4} N_2^{-4} \sum_{a \in V_{N_1 N_2}} f(a) \langle a, b \rangle_{N_1 N_2}.$$

By the Chinese remainder theorem, the set of $a \in V_{N_1 N_2}$ is equal to the set of $N_2 a_1 + N_1 a_2$ for $a_1 \in V_1, a_2 \in V_2$. Therefore, the quantity above is

$$\begin{aligned} &N_1^{-4} N_2^{-4} \sum_{a_1 \in V_{N_1}} \sum_{a_2 \in V_{N_2}} f(N_2 a_1 + N_1 a_2) \langle N_2 a_1 + N_1 a_2, b \rangle_{N_1 N_2} \\ &\quad = N_1^{-4} N_2^{-4} \sum_{a_1 \in V_{N_1}} \sum_{a_2 \in V_{N_2}} f^1(N_2 a_1) f^2(N_1 a_2) \langle N_2 a_1, b \rangle_{N_1 N_2} \langle N_1 a_2, b \rangle_{N_1 N_2}. \end{aligned}$$

We have $\langle N_2 a_1, b \rangle_{N_1 N_2} = \langle a_1, b \rangle_{N_1}$ and $\langle N_1 a_2, b \rangle_{N_1 N_2} = \langle a_2, b \rangle_{N_2}$, where we reduce b modulo N_1 and N_2, respectively, and the result follows. ■

Let $N = \prod N_i$ where N_i and N_j are coprime for $i \neq j$ and $f^i \in C(V_{N_i})$. Then by the repeated use of this lemma, we have

$$\big(\prod f^i\big)^\wedge = \prod (f^i_{N/N_i})^\wedge,$$

where $\prod f^i \in C(V_N)$ is defined similarly.

We now introduce the following space of functions on V_N, which are our main interest.

Definition 4.5 We define

$$C(V_N, \chi) := \{ f \colon V_N \to \mathbb{C} \mid f(ga) = \chi(\det g) f(a) \text{ for all } g \in G_N, a \in V_N \},$$

the space of G_N-*relative invariant functions* with respect to χ.

Let $f \in C(V_N, \chi)$ and consider the associated zeta function $\xi(s, f)$. For $x \in V_{\mathbb{Z}}$, let $f(x) = f(x \bmod N)$. We note that for $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, $f(\gamma x) = f(x)$ since $(\gamma \bmod N) \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ is of determinant 1. For $f \in C(V_N, \chi)$, the zeta function $\xi(s, f)$ has the following description.

Proposition 4.6 *For* $f \in C(V_N, \chi)$,

$$\xi_\pm(s, f) = \sum_{\substack{x \in \mathrm{SL}_2(\mathbb{Z}) \backslash V_{\mathbb{Z}} \\ \pm P(x) > 0}} f(x) \frac{|\,\mathrm{SL}_2(\mathbb{Z})_x|^{-1}}{|P(x)|^s} \quad \textit{where } \xi(s, f) = \begin{pmatrix} \xi_+(s, f) \\ \xi_-(s, f) \end{pmatrix}.$$

https://doi.org/10.4153/CJM-2013-027-0 Published online by Cambridge University Press

Proof For $X \subset V_{\mathbb{Z}}$, let $X^{\pm} = \{x \in X \mid \pm P(x) > 0\}$. Then this follows from

$$\begin{aligned}\sum_{x \in \mathrm{SL}_2(\mathbb{Z}) \backslash V_{\mathbb{Z}}^{\pm}} & f(x) \frac{|\,\mathrm{SL}_2(\mathbb{Z})_x|^{-1}}{|P(x)|^s} \\ &= [\mathrm{SL}_2(\mathbb{Z}) : \Gamma(N)]^{-1} \sum_{x \in \Gamma(N) \backslash V_{\mathbb{Z}}^{\pm}} f(x) \frac{|\Gamma(N)_x|^{-1}}{|P(x)|^s} \\ &= [\mathrm{SL}_2(\mathbb{Z}) : \Gamma(N)]^{-1} \sum_{a \in V_N} f(a) \sum_{x \in \Gamma(N) \backslash (a + NV_{\mathbb{Z}})^{\pm}} \frac{|\Gamma(N)_x|^{-1}}{|P(x)|^s} \\ &= \xi_{\pm}(s, f). \qquad \blacksquare\end{aligned}$$

All the zeta functions we study in the rest of this paper will be of the form $\xi(s, f)$ for some $f \in C(V_N, \chi)$. We explain how $\xi(s, f)$ and $\widehat{f}$ for these f are related to the orbital L-functions and the orbital Gauss sums introduced in Section 3.

For $a \in V_N$, we define $f_{\chi,a} \in C(V_N)$ as follows: If $\chi \circ \det$ is trivial on $G_{N,a}$, we define

$$f_{\chi,a}(a') := \begin{cases} |G_{N,a}|\chi(\det g) & a' = ga, g \in G_N, \\ 0 & a' \notin G_N \cdot a. \end{cases}$$

Otherwise, we put $f_{\chi,a} = 0$. Then one can easily see that

$$\xi(s, f_{\chi,a}) = \xi(s, \chi, a) \quad \text{and} \quad \widehat{f_{\chi,a}}(b) = N^{-4} W(\chi, a, b).$$

We also check that $f_{\chi,a} \in C(V_N, \chi)$, and moreover if $f \in C(V_N, \chi)$, we have

$$f = |G_N|^{-1} \sum_{a \in V_N} f(a) f_{\chi,a}.$$

Hence we have the following.

Proposition 4.7 *Let $f \in C(V_N, \chi)$. Then*

$$\xi(s, f) = |G_N|^{-1} \sum_{a \in V_N} f(a) \xi(s, \chi, a),$$

$$\widehat{f}(b) = N^{-4} |G_N|^{-1} \sum_{a \in V_N} f(a) W(\chi, a, b).$$

So we will study $\xi(s, \chi, a)$ and $W(\chi, a, b)$, and then apply the results to prove analytic properties of $\xi(s, f)$.

For its own interest, we describe the functional equation of the orbital L-functions.

Proposition 4.8 *We have*

$$\begin{aligned}\xi(1 - s, \chi, a) &= N^{4s-4} M(s) \sum_{b \in G_N \backslash V_N^*} \frac{W(\chi, a, b)}{|G_{N,b}|} \xi^*(s, \chi^{-1}, b) \\ &= \frac{N^{4s-4}}{|G_N|} M(s) \sum_{b \in V_N^*} W(\chi, a, b) \xi^*(s, \chi^{-1}, b).\end{aligned}$$

https://doi.org/10.4153/CJM-2013-027-0 Published online by Cambridge University Press

Proof By applying $f_{\chi,a} \in C(V_N)$ to Theorem 4.3, we have

$$\begin{aligned}\xi(1-s,\chi,a) &= \frac{N^{4s-4}}{|G_N|} M(s) \sum_{b\in V_N^*} W(\chi,a,b)\xi^*(s,b)\\ &= \frac{N^{4s-4}}{|G_N|} M(s) \sum_{b\in G_N\backslash V_N^*} \frac{1}{|G_{N,b}|} \sum_{g\in G_N} W(\chi,a,gb)\xi^*(s,gb).\end{aligned}$$

Since $W(\chi,a,gb) = \chi(\det g)^{-1} W(\chi,a,b)$, we have the first equality. Since the product $W(\chi,a,b)\cdot\xi^*(s,\chi^{-1},b)$ depends only on the G_N-orbits of b, we have the second identity. ■

We discuss some general properties of the orbital Gauss sums. The following is easy to prove.

Lemma 4.9 *Let $d \mid N$, $a \in V_{N/d}$, $b \in V_N$ and let χ be a Dirichlet character whose conductor is a divisor of N/d. Regarding $da \in V_N$, we have*

$$W_N(\chi,da,b) = \frac{|G_N|}{|G_{N/d}|} W_{N/d}(\chi,a,b).$$

Proof Since the action of G_N on $da \in V_N$ factors through $G_N \to G_{N/d}$, we have

$$W_N(\chi,da,b) = \frac{|G_N|}{|G_{N/d}|} \sum_{g\in G_{N/d}} \chi(\det g)\langle gda,b\rangle_N.$$

Since $\langle gda,b\rangle_N = \langle ga,b\rangle_{N/d}$, we have the formula. ■

We give two further properties of orbital Gauss sums that are generalizations of those of the classical Gauss sum $\tau_N(\chi) = \sum_{t\in(\mathbb{Z}/N\mathbb{Z})^\times} \chi(t)\exp(2\pi i t/N)$. We do not use these results in this paper, but mention them because of their own interest. Recall that $\tau_N(\chi^{-1})\tau_N(\chi) = \chi(-1)N$ if the conductor of χ is N, and $\tau_N(\chi) = 0$ otherwise (see, *e.g.*, (3.15) of [12]). As a generalization, our Gauss sum satisfies the following.

Proposition 4.10 *Assume that $\chi \circ \det$ is trivial on $G_{N,a}$. Then*

$$\frac{1}{N^4} \sum_{b\in G_N\backslash V_N^*} \frac{W(\chi^{-1},-a',b)}{|G_{N,b}|}\frac{W(\chi,a,b)}{|G_{N,a}|} = \begin{cases}\chi(\det g) & a' = ga,\\ 0 & a' \notin G_N\cdot a.\end{cases}$$

https://doi.org/10.4153/CJM-2013-027-0 Published online by Cambridge University Press

Proof By the Fourier inversion formula,

$$\begin{aligned} f_{\chi,a}(a') &= \sum_{b\in V_N^*} \widehat{f_{\chi,a}}(b)\langle -a', b\rangle = N^{-4}\sum_{b\in V_N^*} W(\chi,a,b)\langle -a',b\rangle \\ &= N^{-4}\sum_{b\in G_N\backslash V_N^*} \frac{1}{|G_{N,b}|}\sum_{g\in G_N} W(\chi,a,gb)\langle -a',gb\rangle \\ &= N^{-4}\sum_{b\in G_N\backslash V_N^*} \frac{W(\chi,a,b)}{|G_{N,b}|}\sum_{g\in G_N} \chi^{-1}(\det g)\langle -a',gb\rangle \\ &= N^{-4}\sum_{b\in G_N\backslash V_N^*} \frac{W(\chi,a,b)}{|G_{N,b}|} W(\chi^{-1},-a',b). \end{aligned}$$

This is equivalent to the desired formula. ■

We next describe the decomposition formula. Assume $N = \prod_{1\le i\le r} N_i$, where $(N_i, N_j) = 1$ if $i \neq j$. Using the canonical isomorphism $(\mathbb{Z}/N\mathbb{Z})^\times \cong \prod(\mathbb{Z}/N_i\mathbb{Z})^\times$, we obtain a character χ_i on $(\mathbb{Z}/N_i\mathbb{Z})^\times$ by restricting χ. Then

$$\tau_N(\chi) = \prod_{1\le i\le r} \chi_i(N/N_i)\tau_{N_i}(\chi_i)$$

(see *e.g.*, (3.16) of [12]). This is generalized as follows.

Proposition 4.11 *For $a \in V_N$ and $b \in V_N^*$, let $a_i = (a \bmod N_i) \in V_{N_i}$ and $b_i = (b \bmod N_i) \in V_{N_i}^*$, respectively. Then*

$$W_N(\chi,a,b) = \prod_{1\le i\le r} \chi_i(N/N_i)^2 W_{N_i}(\chi_i,a_i,b_i).$$

Proof Let $f = f_{\chi,a} \in C(V_N)$ and $f_i = f_{i,\chi_i,a_i} \in C(V_{N_i})$ for each i. Then $f = \prod_{1\le i\le r} f_i$. Since $(f_{i,N/N_i})^\wedge = \chi_i(N/N_i)^2(f_i)^\wedge$, the result follows from Lemma 4.4. ■

5 Orbit Description

For the specific study of the orbital L-functions and orbital Gauss sums, it is indispensable to describe the G_N-orbit structure of V_N explicitly. By the Chinese remainder theorem, this is reduced to the case when N is a prime power. Let p be a prime. In this section, we study these orbit structures when $N = p$ and $N = p^2$. The theory over $\mathbb{Z}/p\mathbb{Z}$ is the base case and is well known, and the theory over $\mathbb{Z}/p^2\mathbb{Z}$ is a refinement of this. Besides its own interest, this is significant in the study of cubic fields, because the maximality criterion of cubic rings R over $\mathbb{Z}$ at p is given in terms of congruence conditions of the coefficients modulo p^2 of the corresponding integral binary cubic forms $x \in V_{\mathbb{Z}}$. We will in fact prove this criterion in Proposition 5.9.

https://doi.org/10.4153/CJM-2013-027-0 Published online by Cambridge University Press

5.1 The Case $N = p$

Let Σ_p be the following set of symbols:

$$\Sigma_p = \{(3), (21), (111), (1^2 1), (1^3), (0)\}.$$

For each $(\sigma) \in \Sigma_p$, we define $V_p(\sigma) \subset V_p$ as follows:

$$\begin{aligned}
V_p(3) &= \{a \in V_p \mid a(u,v) \text{ has no rational roots in } \mathbb{P}^1_{\mathbb{F}_p}\},\\
V_p(21) &= \{a \in V_p \mid a(u,v) \text{ has only one rational root in } \mathbb{P}^1_{\mathbb{F}_p}\},\\
V_p(111) &= \{a \in V_p \mid a(u,v) \text{ has three distinct rational roots in } \mathbb{P}^1_{\mathbb{F}_p}\},\\
V_p(1^2 1) &= \{a \in V_p \mid a(u,v) \text{ has one single root and one double root in } \mathbb{P}^1_{\mathbb{F}_p}\},\\
V_p(1^3) &= \{a \in V_p \mid a(u,v) \text{ has one triple root in } \mathbb{P}^1_{\mathbb{F}_p}\},\\
V_p(0) &= \{0\}.
\end{aligned}$$

So each cubic form in $V_p(3)$ is irreducible over $\mathbb{F}_p$, while each cubic form in $V_p(21)$ is the product of a linear form and an irreducible quadratic form over $\mathbb{F}_p$. We have $\{a \in V_p \mid P(a) = 0\} = V_p(1^2 1) \sqcup V_p(1^3) \sqcup V_p(0)$. We say $a \in V_p$ is of type (σ) if $a \in V_p(\sigma)$. The description of rational orbits over a field is well known (see *e.g.*, [29, Proposition 2.1]). Each $V_p(\sigma)$ consists of a single G_p-orbit. Moreover, under the Delone–Faddeev correspondence in Theorem 2.1, the corresponding cubic rings over $\mathbb{F}_p$ are $\mathbb{F}_{p^3}$, $\mathbb{F}_{p^2} \times \mathbb{F}_p$, $(\mathbb{F}_p)^3$, $\mathbb{F}_p \times \mathbb{F}_p[X]/(X^2)$, $\mathbb{F}_p[X]/(X^3)$ and $\mathbb{F}_p[X,Y]/(X^2, XY, Y^2)$, respectively. Note that $(0,1,0,0) \in V_p(1^2 1)$ and $(1,0,0,0) \in V_p(1^3)$. We always use them as orbital representatives of these orbits. The structure of the stabilizers for each orbit is given as follows.

Lemma 5.1 *The group of stabilizers of $G_{p,a}$ of a of type (3), (21), (111), $(1^2 1)$, (1^3), and (0) are isomorphic to $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}$, $\mathfrak{S}_3$, $\mathbb{F}_p^\times$, $\mathbb{F}_p^\times \ltimes \mathbb{F}_p$, and G_p, respectively. Moreover, for $(0,1,0,0) \in V_p(1^2 1)$ and $(1,0,0,0) \in V_p(1^3)$, the stabilizers are respectively given by*

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & t \end{pmatrix} \;\middle|\; t \in \mathbb{F}_p^\times \right\} \quad \textit{and} \quad \left\{ \begin{pmatrix} t & x \\ 0 & t^2 \end{pmatrix} \;\middle|\; t \in \mathbb{F}_p^\times, x \in \mathbb{F}_p \right\}.$$

Proof If $a \in V_p$ corresponds to a cubic ring R_a over $\mathbb{F}_p$ under the Delone–Faddeev correspondence, then $G_{p,a}$ is isomorphic to the automorphism group $\mathrm{Aut}(R_a)$ as an $\mathbb{F}_p$-algebra. It is easy to see that $\mathrm{Aut}(\mathbb{F}_{p^3}) \cong \mathbb{Z}/3\mathbb{Z}$, $\mathrm{Aut}(\mathbb{F}_p \times \mathbb{F}_{p^2}) \cong \mathbb{Z}/2\mathbb{Z}$ and $\mathrm{Aut}\big((\mathbb{F}_p)^3\big) \cong \mathfrak{S}_3$. If $g \in G_p$ stabilizes $a = (0,1,0,0)$, then g fixes $(1{:}0), (0{:}1) \in \mathbb{P}^1_{\mathbb{F}_p}$ and hence must be a diagonal matrix. Now an easy computation determines the stabilizers of a. The stabilizers of $(1,0,0,0)$ are similarly determined. ■

As a result, we see the cardinality of each orbit.

Lemma 5.2 *Let $n_p(\sigma) = |V_p(\sigma)|$. Then*

$$n_p(3) = 3^{-1}(p^2-1)(p^2-p), \qquad n_p(1^21) = (p^2-1)p,$$
$$n_p(21) = 2^{-1}(p^2-1)(p^2-p), \qquad n_p(1^3) = (p^2-1),$$
$$n_p(111) = 6^{-1}(p^2-1)(p^2-p), \qquad n_p(0) = 1.$$

Let $\mathbb{Q}_p$ be the p-adic field and $\mathbb{Z}_p$ its ring of integers. For $(\sigma) \in \Sigma_p$, we define

$$V_{\mathbb{Z}_p}(\sigma) := \{a \in V_{\mathbb{Z}_p} \mid a \bmod p \in V_p(\sigma)\},$$
$$V_{p^e}(\sigma) := \{a \in V_{p^e} \mid a \bmod p \in V_p(\sigma)\}, \quad (e \geq 1).$$

We say $a \in V_{\mathbb{Z}_p}$ or V_{p^e} is of type (σ) if $a \in V_{\mathbb{Z}_p}(\sigma)$ or $V_{p^e}(\sigma)$, respectively.

For the application in Section 7, we introduce the following function on V_p.

Definition 5.3 Let $f_p \in C(V_p)$ be the characteristic function of those $a \in V_p$ with $P(a) = 0$.

Obviously, $f_p \in C(V_p, \mathbf{1})$.

5.2 The Case $N = p^2$

In this subsection we study the G_{p^2}-orbit structure of V_{p^2}. We put $R := \mathbb{Z}/p^2\mathbb{Z}$, and also $pR := \{pu \mid u \in R\}$, $pR^\times := \{pu \mid u \in R^\times\} = pR \setminus \{0\}$.

Let Σ_{p^2} be the following set of symbols:

$$\Sigma_{p^2} = \{(3), (21), (111), (1^21_{\max}), (1^21_*), (1^3_{\max}), (1^3_*), (1^3_{**})\}.$$

We introduce $V_{p^2}(\sigma)$ for $(\sigma) = (1^21_{\max}), (1^21_*), (1^3_{\max}), (1^3_*), (1^3_{**})$ which we show that

$$V_{p^2}(1^21) = V_{p^2}(1^21_{\max}) \sqcup V_{p^2}(1^21_*),$$
$$V_{p^2}(1^3) = V_{p^2}(1^3_{\max}) \sqcup V_{p^2}(1^3_*) \sqcup V_{p^2}(1^3_{**}).$$

Let

$$\mathcal{D}_{p^2}(1^21_{\max}) := \{(0, a_2, a_3, a_4) \in V_{p^2} \mid a_2 \in R^\times, a_3 \in pR, a_4 \in pR^\times\},$$
$$\mathcal{D}_{p^2}(1^21_*) := \{(0, a_2, a_3, a_4) \in V_{p^2} \mid a_2 \in R^\times, a_3 \in pR, a_4 = 0\},$$
$$\mathcal{D}_{p^2}(1^3_{\max}) := \{(a_1, a_2, a_3, a_4) \in V_{p^2} \mid a_1 \in R^\times, a_2 \in pR, a_3 \in pR, a_4 \in pR^\times\},$$
$$\mathcal{D}_{p^2}(1^3_*) := \{(a_1, a_2, a_3, a_4) \in V_{p^2} \mid a_1 \in R^\times, a_2 \in pR, a_3 \in pR^\times, a_4 = 0\},$$
$$\mathcal{D}_{p^2}(1^3_{**}) := \{(a_1, a_2, a_3, a_4) \in V_{p^2} \mid a_1 \in R^\times, a_2 \in pR, a_3 = a_4 = 0\},$$

and

$$V_{p^2}(\sigma) := G_{p^2} \cdot \mathcal{D}_{p^2}(\sigma)$$

https://doi.org/10.4153/CJM-2013-027-0 Published online by Cambridge University Press

for these (σ). We say $a \in V_{p^2}$ is of type (σ) if $a \in V_{p^2}(\sigma)$. We put $n_{p^2}(\sigma) := |V_{p^2}(\sigma)|$.

One may notice that $\mathcal{D}_{p^2}(1^3_{\max})$ is the set of modulus classes of Eisenstein polynomials multiplied by units. We will prove in Proposition 5.9 that orbits containing these modulus classes correspond to cubic rings that are totally ramified at p. A similar interpretation in terms of partially ramified rings will be given for $\mathcal{D}_{p^2}(1^2 1_{\max})$ also. We also give an interpretation of these stratifications in terms of p-adic valuations of $P(x)$ in Proposition 5.7.

Let us study these sets.

Lemma 5.4 *We put*

$$\mathcal{D}_{p^2}(1^2 1) = \mathcal{D}_{p^2}(1^2 1_{\max}) \sqcup \mathcal{D}_{p^2}(1^2 1_*),$$
$$G_{p^2}(1^2 1) = \left\{ \begin{pmatrix} s & 0 \\ n & t \end{pmatrix} \in G_{p^2} \;\middle|\; s, t \in R^\times, n \in pR \right\}.$$

(i) *We have* $V_{p^2}(1^2 1) = G_{p^2} \cdot \mathcal{D}_{p^2}(1^2 1)$.

(ii) *Let* $a \in \mathcal{D}_{p^2}(1^2 1)$. *Then for* $g \in G_{p^2}$, $ga \in \mathcal{D}_{p^2}(1^2 1)$ *if and only if* $g \in G_{p^2}(1^2 1)$. *Moreover, both* $\mathcal{D}_{p^2}(1^2 1_{\max})$ *and* $\mathcal{D}_{p^2}(1^2 1_*)$ *are* $G_{p^2}(1^2 1)$*-invariant.*

(iii) *We have* $n_{p^2}(1^2 1_{\max}) = p^3(p^2-1)(p^2-p)$, $n_{p^2}(1^2 1_*) = p^4(p^2-1)$.

Proof (i) By definition $V_{p^2}(1^2 1) \supset G_{p^2}\mathcal{D}_{p^2}(1^2 1)$ and we consider the reverse inclusion. Let $a \in V_p(1^2 1)$. Then $(a \bmod p) \in V_p$ lies in the G_p-orbit of $(0,1,0,0)$. Hence by changing an element of its G_{p^2}-orbit if necessary, we may assume $a = (a_1, 1, a_3, a_4)$ where $a_1, a_3, a_4 \in pR$. Then the cubic form $a(u,v)$ decomposes as $a(u,v) = (a_1 u + v)(u^2 + a_3 uv + a_4 v^2)$ in $R[u,v]$. Hence for $g = \left(\begin{smallmatrix} 1 & -a_1 \\ 0 & 1 \end{smallmatrix}\right)$, we have $ga \in \mathcal{D}_{p^2}(1^2 1)$.

(ii) Let $a = (0, a_2, a_3, a_4) \in \mathcal{D}_{p^2}(1^2 1)$, $g \in G_{p^2}$ and assume $ga \in \mathcal{D}_{p^2}(1^2 1)$. By considering the reduction modulo p, we see that g must be of the form

$$g = \begin{pmatrix} s & m \\ n & t \end{pmatrix}, \quad s, t \in R^\times, m, n \in pR.$$

Moreover, since the first coordinate of ga is $(\det g)^{-1} s^2 m a_2$ and also $(\det g)^{-1} s^2 a_2 \in R^\times$, we have $m = 0$. Hence $g \in G_{p^2}(1^2 1)$. On the other hand, for this g, we have $ga = (0, sa_2, 2na_2 + ta_3, s^{-1}t^2 a_4)$. Note that $na_3 = 0$. Hence both $\mathcal{D}_{p^2}(1^2 1_{\max})$ and $\mathcal{D}_{p^2}(1^2 1_*)$ are $G_{p^2}(1^2 1)$-invariant.

(iii) By (ii), we have

$$n_{p^2}(1^2 1_{\max}) = \frac{|G_{p^2}|}{|G_{p^2}(1^2 1)|} |\mathcal{D}_{p^2}(1^2 1_{\max})| = p^3(p^2-p)(p^2-1).$$

The number $n_{p^2}(1^2 1_*)$ is computed similarly. ■

Lemma 5.5 *Let*

$$\mathcal{D}_{p^2}(1^3) = \mathcal{D}_{p^2}(1^3_{\max}) \sqcup \mathcal{D}_{p^2}(1^3_*) \sqcup \mathcal{D}_{p^2}(1^3_{**}),$$
$$G_{p^2}(1^3) = \left\{ \begin{pmatrix} s & m \\ n & t \end{pmatrix} \in G_{p^2} \;\middle|\; s, t \in R^\times, m \in R, n \in pR \right\}.$$

https://doi.org/10.4153/CJM-2013-027-0 Published online by Cambridge University Press

(i) *We have* $V_p(1^3) = G_{p^2} \cdot \mathcal{D}_{p^2}(1^3)$.

(ii) *Let* $a \in \mathcal{D}_{p^2}(1^3)$. *Then for* $g \in G_{p^2}$, $ga \in \mathcal{D}_{p^2}(1^3)$ *if and only if* $g \in G_{p^2}(1^3)$. *Moreover, all of* $\mathcal{D}_{p^2}(1^3_{\max})$, $\mathcal{D}_{p^2}(1^3_*)$, *and* $\mathcal{D}_{p^2}(1^3_{**})$ *are* $G_{p^2}(1^3)$*-invariant.*

(iii) *We have* $n_{p^2}(1^3_{\max}) = p^2(p^2-1)(p^2-p)$, $n_{p^2}(1^3_*) = p(p^2-p)(p^2-1)$, *and* $n_{p^2}(1^3_{**}) = p^2(p^2-1)$.

Since the proof is similar to the previous lemma, we omit the details. Note that for $a = (a_1, a_2, a_3, a_4) \in \mathcal{D}_{p^2}(1^3)$ and $g = \left(\begin{smallmatrix} s & m \\ n & t \end{smallmatrix}\right) \in G_{p^2}(1^3)$ (and hence $n \in pR$),

$$^t(ga) = \frac{1}{\det g} \begin{pmatrix} s^3a_1 + s^2ma_2 + sm^2a_3 + m^3a_4 \\ 3s^2na_1 + s^2ta_2 + 2stma_3 + 3m^2ta_4 \\ st^2a_3 + 3mt^2a_4 \\ t^3a_4 \end{pmatrix}.$$

We summarize the formulas for $n_p^2(\sigma)$ for convenience.

Lemma 5.6 *We have*

$$\begin{aligned}
&n_{p^2}(3) = 3^{-1}p^4(p^2-1)(p^2-p), && \\
&n_{p^2}(21) = 2^{-1}p^4(p^2-1)(p^2-p), && n_{p^2}(1^21_*) = p^4(p^2-1), \\
&n_{p^2}(111) = 6^{-1}p^4(p^2-1)(p^2-p), \qquad \textit{and} && n_{p^2}(1^3_*) = p(p^2-1)(p^2-p), \\
&n_{p^2}(1^21_{\max}) = p^3(p^2-1)(p^2-p), && n_{p^2}(1^3_{**}) = p^2(p^2-1). \\
&n_{p^2}(1^3_{\max}) = p^2(p^2-1)(p^2-p), &&
\end{aligned}$$

For $(\sigma) \in \Sigma_{p^2}$ and $e \geq 2$ we put

$$\begin{aligned}
V_{\mathbb{Z}_p}(\sigma) &:= \{a \in V_{\mathbb{Z}_p} \mid a \bmod p^2 \in V_{p^2}(\sigma)\}, \\
V_{p^e}(\sigma) &:= \{a \in V_{p^e} \mid a \bmod p^2 \in V_{p^2}(\sigma)\}.
\end{aligned}$$

By the definition of $\mathcal{D}_{p^2}(\sigma)$, we can easily see the following.

Proposition 5.7 *For* $p \neq 2$,

$$\begin{aligned}
V_{\mathbb{Z}_p}(1^21_{\max}) &= \left\{x \in V_{\mathbb{Z}_p}(1^21) \mid \operatorname{ord}_p\bigl(P(x)\bigr) = 1\right\}, \\
V_{\mathbb{Z}_p}(1^21_*) &= \left\{x \in V_{\mathbb{Z}_p}(1^21) \mid \operatorname{ord}_p\bigl(P(x)\bigr) \geq 2\right\},
\end{aligned}$$

and for $p \neq 2, 3$,

$$\begin{aligned}
V_{\mathbb{Z}_p}(1^3_{\max}) &= \left\{x \in V_{\mathbb{Z}_p}(1^3) \mid \operatorname{ord}_p\bigl(P(x)\bigr) = 2\right\}, \\
V_{\mathbb{Z}_p}(1^3_*) &= \left\{x \in V_{\mathbb{Z}_p}(1^3) \mid \operatorname{ord}_p\bigl(P(x)\bigr) = 3\right\}, \\
V_{\mathbb{Z}_p}(1^3_{**}) &= \left\{x \in V_{\mathbb{Z}_p}(1^3) \mid \operatorname{ord}_p\bigl(P(x)\bigr) \geq 4\right\}.
\end{aligned}$$

https://doi.org/10.4153/CJM-2013-027-0 Published online by Cambridge University Press

We now describe the ring-theoretic meaning of these orbits. We say that a cubic ring over $\mathbb{Z}_p$ is *maximal* if it is not isomorphic to a proper subring of another cubic ring. We say that a cubic ring R over $\mathbb{Z}$ is *maximal at p* if it is not contained in another cubic ring with finite index divisible by p, or equivalently if $R \otimes \mathbb{Z}_p$ is maximal as a cubic ring over $\mathbb{Z}_p$. We need the following auxiliary lemma.

Lemma 5.8 *Let R be a cubic ring over $\mathbb{Z}_p$ whose discriminant is zero. Then R is nonmaximal.*

Proof Let $K = R \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ and regard $R \subset K$. Since $\mathrm{Disc}(K) = 0$, K is isomorphic to $\mathbb{Q}_p \times \mathbb{Q}_p[X]/(X^2)$, $\mathbb{Q}_p[X]/(X^3)$ or $\mathbb{Q}_p[X,Y]/(X^2, XY, Y^2)$. In particular, K has a nilpotent element x. Take $y \in R$ such that $R \cap \mathbb{Q}_p x = \mathbb{Z}_p y$ and consider the ring $R[y/p] \subset K$. Since $y^3 = 0$, we have $R \subset R[y/p] \subset p^{-2}R$. This implies that $R[y/p]$ is free of rank 3 as a $\mathbb{Z}_p$-module. Since R is a proper subring of $R[y/p]$, R is nonmaximal. ■

Applying Theorem 2.1, we have the following interpretation of the set $V_{p^2}(\sigma)$ for $(\sigma) = (3), (21), (111), (1^2 1_{\max})$ and $(1^3_{\max})$ in terms of maximal cubic rings over $\mathbb{Z}_p$. This also explains why the maximality condition can be detected modulo p^2.

Proposition 5.9 *A maximal cubic ring over $\mathbb{Z}_p$ is one of the following: the integer ring $\mathcal{O}_L$ of the unramified cubic extension L of $\mathbb{Q}_p$; $\mathcal{O}_F \times \mathbb{Z}_p$, where $\mathcal{O}_F$ is the integer ring of the unramified quadratic extension F of $\mathbb{Q}_p$; $\mathbb{Z}_p^3$, the integer ring $\mathcal{O}_{L'}$ of a ramified cubic extension L' of $\mathbb{Q}_p$; or $\mathcal{O}_{F'} \times \mathbb{Z}_p$, where $\mathcal{O}_{F'}$ is the integer ring of a ramified quadratic extension F' of $\mathbb{Q}_p$. An element $x \in V_{\mathbb{Z}_p}$ corresponds to the above $\mathcal{O}_L, \mathcal{O}_F \times \mathbb{Z}_p, \mathbb{Z}_p^3, \mathcal{O}_{L'}$ or $\mathcal{O}_{F'} \times \mathbb{Z}_p$ if and only if $x \in V_{\mathbb{Z}_p}(\sigma)$, where $(\sigma) = (3), (21), (111), (1^3_{\max})$, or $(1^2 1_{\max})$, respectively. In particular, $V_{\mathbb{Z}_p}(\sigma)$ is a single $G_{\mathbb{Z}_p}$-orbit for $(\sigma) = (3), (21)$, and (111).*

Proof Let R be a maximal cubic ring over $\mathbb{Z}_p$. By the lemma above, the discriminant is nonzero. Hence $R \otimes \mathbb{Q}_p \supset R$ is a separable cubic algebra over $\mathbb{Q}_p$ and so it is a direct product $F_1 \times \cdots \times F_n$ of field extensions F_i of $\mathbb{Q}_p$ with $\sum_i [F_i : \mathbb{Q}_p] = 3$. Let $\mathcal{O}_{F_i}$ be the integer ring of F_i. Since any elements of $F_i \setminus \mathcal{O}_{F_i}$ generate $\mathbb{Z}_p$-algebras of infinite rank, any entries of elements of $R \subset F_1 \times \cdots \times F_n$ must be in $\mathcal{O}_{F_i}$. Hence we have $R \subset \mathcal{O}_{F_1} \times \cdots \times \mathcal{O}_{F_n}$. Since R is maximal, we have $R = \mathcal{O}_{F_1} \times \cdots \times \mathcal{O}_{F_n}$ and the first statement follows. Let $R = \mathbb{Z}_p \times \mathcal{O}_{F'}$ where F' is a ramified quadratic extension. Then $\mathcal{O}_{F'} = \mathbb{Z}_p[\theta]$ where $\theta \in F'$ is a root of an Eisenstein polynomial $X^2 + cX + d \in \mathbb{Z}_p[X]$. Hence $x(u,v) = v(u^2 + cuv + dv^2) \in V_{\mathbb{Z}_p}$ corresponds to R by Theorem 2.1 and we have $(x \bmod p^2) \in \mathcal{D}_{p^2}(1^2 1_{\max}) \subset V_{p^2}(1^2 1_{\max})$ by the definition of an Eisenstein polynomial. The other cases are proved similarly. ■

Let $V_{p^2}^{\max} \subset V_{p^2}$ be the set of elements of any of the types above. Then $V_{p^2}^{\max}$ is defined by a congruence condition modulo p^2 on $V_{\mathbb{Z}}$, and it detects cubic rings over $\mathbb{Z}$ maximal at p. Similarly we define $V_{\mathbb{Z}_p}^{\max} \subset V_{\mathbb{Z}_p}$ and $V_{p^e}^{\max} \subset V_{p^e}$.

Definition 5.10 We define the following subsets of V_{p^2}:

$$V_{p^2}^{\mathrm{nm}} := pV_{p^2} \sqcup V_{p^2}(1^3_{**}) \sqcup V_{p^2}(1^3_{*}) \sqcup V_{p^2}(1^2 1_{*}) = V_{p^2} \setminus V_{p^2}^{\max},$$

$$\tilde{V}_{p^2}^{\mathrm{nm}} := V_{p^2}^{\mathrm{nm}} \sqcup V_{p^2}(1^3_{\max}).$$

We denote by $\Phi_p, \Phi'_p \in C(V_{p^2})$ the characteristic functions of $V_{p^2}^{\mathrm{nm}}, \tilde{V}_{p^2}^{\mathrm{nm}}$, respectively.

Obviously $\Phi_p, \Phi'_p \in C(V_{p^2}, \mathbf{1})$. Φ_p detects cubic rings nonmaximal at p, and Φ'_p detects rings nonmaximal or totally ramified at p. The conditions corresponding to these functions were introduced in the seminal work of Davenport and Heilbronn [4], who originally proved the main terms of Theorem 1.5 by studying the space of binary cubic forms. These functions play important roles in our proof of Theorem 1.5 as well.

In Section 6, we will compute the Fourier transform of Φ_p, Φ'_p and hence the related orbital Gauss sums explicitly. For that purpose, we study the orbit structure of $V_{p^2}(\sigma)$ for $(\sigma) = (1^21_*)$, $(1^21_{\max})$, (1^3_{**}), (1^3_*), and $(1^3_{\max})$ more closely.

Lemma 5.11

(i) *Assume $p \neq 2$. The stabilizers of elements $a = (0,1,0,0) \in \mathcal{D}_{p^2}(1^21_*)$ and $a' = (0,1,0,a_4) \in \mathcal{D}_{p^2}(1^21_{\max})$ are respectively given by*

$$G_{p^2,a} = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & t \end{pmatrix} \;\middle|\; t \in R^\times \right\},$$

$$G_{p^2,a'} = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & t \end{pmatrix} \;\middle|\; t \in R^\times, t^2 \equiv 1 \pmod{p} \right\}.$$

Moreover, $b' = (0,1,0,b_4) \in \mathcal{D}_{p^2}(1^21_{\max})$ lies in the orbit $G_{p^2} \cdot a'$ if and only if $b_4 = t^2 a_4$ for some $t \in R^\times$.

(ii) *Assume $p \neq 3$. The stabilizers of elements $a = (1,0,0,0) \in \mathcal{D}_{p^2}(1^3_{**})$, $a' = (1,0,a_3,0) \in \mathcal{D}_{p^2}(1^3_*)$, and $a'' = (1,0,0,a_4) \in \mathcal{D}_{p^2}(1^3_{\max})$ are respectively given by*

$$G_{p^2,a} = \left\{ \begin{pmatrix} t & m \\ 0 & t^2 \end{pmatrix} \;\middle|\; t \in R^\times, m \in R \right\},$$

$$G_{p^2,a'} = \left\{ \begin{pmatrix} t & m \\ -2tma_3/3 & t^2 + m^2a_3/3 \end{pmatrix} \;\middle|\; t \in R^\times, m \in R, t^2 \equiv 1 \pmod{p} \right\},$$

$$G_{p^2,a''} = \left\{ \begin{pmatrix} t & m \\ 0 & t^2 \end{pmatrix} \;\middle|\; t \in R^\times, m \in pR, t^3 \equiv 1 \pmod{p} \right\}.$$

Moreover, $b' = (1,0,b_3,0) \in \mathcal{D}_{p^2}(1^3_*)$ lies in the orbit $G_{p^2} \cdot a'$ if and only if $b_3 = t^2 a_3$ for some $t \in R^\times$, and $b'' = (1,0,0,b_4) \in \mathcal{D}_{p^2}(1^3_{\max})$ lies in the orbit $G_{p^2} \cdot a''$ if and only if $b_4 = t^3 a_4$ for some $t \in R^\times$.

Proof (i) Let $g \in G_{p^2}$ satisfy $ga = a$, $ga' = a'$ or $ga' = b'$. Then $(g \bmod p) \in G_p$ stabilizes $(0,1,0,0) \in V_p$. Hence by Lemma 5.1, g must be of the form

$$g = \begin{pmatrix} 1+l & m \\ n & t \end{pmatrix}, \quad t \in R^\times, l, m, n \in pR.$$

For this g, we have

$$ga = \frac{1}{\det g}\left(m, (1+l)^2 t, 2nt, 0\right), \quad ga' = \frac{1}{\det g}\left(m, (1+l)^2 t, 2nt, a_4 t^3\right).$$

https://doi.org/10.4153/CJM-2013-027-0 Published online by Cambridge University Press

If $ga = a$, then by comparing the first and third entries, we have $m = n = 0$. Note that $2t \in R^\times$ since $p \neq 2$. Now by comparing the second entries, we have $(\det g)^{-1}(1+l)^2 t = 1 + l = 1$ and hence $l = 0$. If $ga' = b'$, by a similar argument we have $m = n = l = 0$ and $b_4 = t^2 a_4$. In particular, if $b_4 = a_4$, this holds if and only if $m = n = l = 0$ and $t^2 \equiv 1 \pmod p$. This proves (i).

(ii) Let $g \in G_{p^2}$ satisfy $ga = a$, $ga' = a'$, $ga' = b'$, $ga'' = a''$, or $ga'' = b''$. Then $(g \bmod p) \in G_p$ stabilizes $(1,0,0,0) \in V_p$. Hence by Lemma 5.1, g must be of the form

$$g = \begin{pmatrix} t & m \\ n & t^2 + l \end{pmatrix}, \quad t \in R^\times, m \in R, n, l \in pR.$$

For this g, we have

$$\begin{aligned} ga &= \frac{1}{\det g}(t^3, 3t^2 n, 0, 0), \\ ga' &= \Big(\frac{t^3 + tm^2 a_3}{t^3 + tl - mn}, \frac{3t^2 n + 2t^3 m a_3}{t^3 + tl - mn}, \frac{t^5 a_3}{t^3 + tl - mn}, 0\Big) \\ &= \Big(1 + \frac{tm^2 a_3 + mn - tl}{t^3}, \frac{3n + 2ta_3 m}{t}, t^2 a_3, 0\Big), \\ ga'' &= \frac{1}{\det g}(t^3 + m^3 a_4, 3t^2(n + m^2 a_4), 3mt^4 a_4, t^6 a_4). \end{aligned}$$

By the first formula, $ga = a$ holds if and only if $n = 0$ and $l = 0$. Note that $3t^2 \in R^\times$ since $p \neq 3$. Similarly by the second formula, $ga' = b'$ holds if and only if

$$n = -2ta_3 m/3, \quad l = m^2 a_3 + mnt^{-1} = m^2 a_3/3, \quad b_3 = t^2 a_3.$$

Let $ga'' = b''$. Then by comparing the third and second entries, we have $m \in pR$ and $n = 0$. Also since $t^3/(\det g) = 1$, we have $l = 0$. Now comparing the last coefficient, we have $b_4 = t^3 a_4$. Hence we have (ii). ■

Now we are ready to prove the following.

Proposition 5.12

(i) *Let $p \neq 2$.*

  (i) *We have $V_{p^2}(1^2 1_*) = G_{p^2} \cdot (0,1,0,0)$.*

  (ii) *The set $V_{p^2}(1^2 1_{\max})$ consists of two G_{p^2}-orbits, and each orbit has the same cardinality $2^{-1}|V_{p^2}(1^2 1_{\max})|$. For any $u_1, u_2 \in \mathbb{F}_p^\times$ such that u_1/u_2 is not a square, $(0,1,0,pu_1)$ and $(0,1,0,pu_2)$ are representatives of the two orbits.*

(ii) *Let $p \neq 3$.*

  (i) *We have $V_{p^2}(1^3_{**}) = G_{p^2} \cdot (1,0,0,0)$.*

  (ii) *If $p \equiv 2 \pmod 3$, $V_{p^2}(1^3_{\max})$ consists of single G_{p^2}-orbit.*

  (iii) *Let $p \equiv 1 \pmod 3$. Then $V_{p^2}(1^3_{\max})$ consists of three G_{p^2}-orbits and each orbit has the same cardinality $3^{-1}|V_{p^2}(1^3_{\max})|$. Let $\{u_1, u_2, u_3\} \subset \mathbb{F}_p^\times$ be a set of representatives of $\mathbb{F}_p^\times/(\mathbb{F}_p^\times)^3$. Then we can take $(1,0,0,pu_i)$, $i = 1,2,3$ as representatives of the three orbits.*

https://doi.org/10.4153/CJM-2013-027-0 Published online by Cambridge University Press

(iii) *Let $p \neq 2, 3$. The set $V_{p^2}(1^3_*)$ consists of two G_{p^2}-orbits and each orbit has the same cardinality $2^{-1}|V_{p^2}(1^3_*)|$. If $u_1, u_2 \in \mathbb{F}_p^\times$ are such that u_1/u_2 is not a square, then $(1, 0, pu_1, 0)$ and $(1, 0, pu_2, 0)$ are representatives of the two orbits.*

Proof (i) Let $a = (0, 1, 0, 0) \in V_{p^2}(1^2 1_*)$. By Lemma 5.11, we have $|G_{p^2,a}| = p^2 - p$. Hence

$$|G_{p^2} \cdot a| = \frac{|G_{p^2}|}{|G_{p^2,a}|} = \frac{p^4(p^2 - p)(p^2 - 1)}{(p^2 - p)} = p^4(p^2 - 1) = |V_{p^2}(1^2 1_*)|$$

and we have $V_{p^2}(1^2 1_*) = G_{p^2} \cdot a$. Let $a' = (0, 1, 0, a_4) \in V_{p^2}(1^2 1_{\max})$. Then we have $|G_{p^2,a'}| = 2p$ and hence we have $|G_{p^2} \cdot a'| = 2^{-1}p^3(p^2 - p)(p^2 - 1) = 2^{-1}|V_{p^2}(1^2 1_{\max})|$. Hence $V_{p^2}(1^2 1_*)$ consists of two orbits. Combined with Lemma 5.11 (i), we have (i).

(ii) and (iii) are proved in the same way. Let $p \neq 3$ and let a, a', a'' be as in Lemma 5.11 (ii). Then

$$|G_{p^2,a}| = p^2(p^2 - p), \quad |G_{p^2,a''}| = \begin{cases} p^2 & p \equiv 2 \pmod 3, \\ 3p^2 & p \equiv 1 \pmod 3. \end{cases}$$

If further $p \neq 2$, then $|G_{p^2,a'}| = 2p^3$. The rest of the argument proceeds similarly. ■

We conclude this section with supplementary results which we use in residue computations.

Proposition 5.13 *Let R be a non-degenerate cubic ring over $\mathbb{Z}_p$ and let $V_{\mathbb{Z}_p,R} \subset V_{\mathbb{Z}_p}$ be the set of elements corresponding to R under the Delone–Faddeev correspondence. Normalize the Haar measure on $V_{\mathbb{Z}_p}$ such that the total volume is 1. Then the volume of $V_{\mathbb{Z}_p,R}$ is $|\operatorname{Aut}_{\mathbb{Z}_p}(R)|^{-1} |\operatorname{Disc}(R)|^{-1}(1 - p^{-1})(1 - p^{-2})$, where $|\operatorname{Disc}(R)|$ is the discriminant of R as a power of p.*

Proof Recall that for any $x \in V_{\mathbb{Q}_p}$ with $P(x) \neq 0$, $G_{\mathbb{Q}_p} \cdot x$ is an open orbit in $V_{\mathbb{Q}_p}$. Let dg be the Haar measure on $G_{\mathbb{Q}_p}$ such that the volume of $G_{\mathbb{Z}_p}$ is 1. Then by the computation of the Jacobian determinant [2, p. 38], we have

$$\int_{G_{\mathbb{Q}_p} \cdot x} \phi(y) \frac{dy}{|P(y)|_p} = \frac{(1 - p^{-1})(1 - p^{-2})}{|G_{\mathbb{Q}_p,x}|} \int_{G_{\mathbb{Q}_p}} \phi(gx)\, dg$$

for an integrable function ϕ on $G_{\mathbb{Q}_p} \cdot x \subset V_{\mathbb{Q}_p}$. Hence the same computation shows that

$$\int_{G_{\mathbb{Z}_p} \cdot x} \phi(y) \frac{dy}{|P(y)|_p} = \frac{(1 - p^{-1})(1 - p^{-2})}{|G_{\mathbb{Z}_p,x}|} \int_{G_{\mathbb{Z}_p}} \phi(gx)\, dg.$$

Now let $x \in V_{\mathbb{Z}_p,R}$ and let ϕ be the characteristic function of $V_{\mathbb{Z}_p,R} = G_{\mathbb{Z}_p} \cdot x$. Then since $G_{\mathbb{Z}_p,x} \cong \operatorname{Aut}_{\mathbb{Z}_p}(R)$ and $|P(y)|_p = |\operatorname{Disc}(R)|^{-1}$ for all $y \in V_{\mathbb{Z}_p,R}$, we have the result. ■

https://doi.org/10.4153/CJM-2013-027-0 Published online by Cambridge University Press

Proposition 5.14

(i) *For $a \in V_p$ of type* (3), (21), *or* (111), *$G_p a + pV_{\mathbb{Z}_p}$ is a single $G_{\mathbb{Z}_p}$-orbit.*
(ii) *For $p \neq 2$ and $a \in V_{p^2}$ of type $(1^2 1_{\max})$, $G_{p^2} a + p^2 V_{\mathbb{Z}_p}$ is a single $G_{\mathbb{Z}_p}$-orbit.*
(iii) *For $p \neq 3$ and $a \in V_{p^2}$ of type $(1^3_{\max})$, $G_{p^2} a + p^2 V_{\mathbb{Z}_p}$ is a single $G_{\mathbb{Z}_p}$-orbit.*

Proof (i) follows from Proposition 5.9. Alternatively, we can prove this as follows. Let $\tilde{a} \in V_{\mathbb{Z}_p}$ be a lift of a and R the corresponding (unramified) cubic ring. Then obviously $G_{\mathbb{Z}_p} \tilde{a} \subseteq G_p a + pV_{\mathbb{Z}_p}$. On the other hand, by Lemma 5.1 and Proposition 5.13 we see that the volumes of these sets are equal:

$$\int_{G_p a + pV_{\mathbb{Z}_p}} dx = p^{-4} |G_p a| = \frac{p^{-4} |G_p|}{|G_{p,a}|} = \frac{(1 - p^{-1})(1 - p^{-2})}{|\operatorname{Aut}_{\mathbb{Z}_p}(R)|} = \int_{G_{\mathbb{Z}_p} \tilde{a}} dx.$$

Since both $G_{\mathbb{Z}_p} \tilde{a}$ and $G_p a + pV_{\mathbb{Z}_p}$ are open, they coincide.

(ii) and (iii) are proved similarly. We recall the classification of ramified quadratic and cubic extensions of $\mathbb{Q}_p$. If $p \neq 2$, then there are two ramified quadratic extensions of discriminant p. If $p \equiv 1 \pmod 3$, then there are three cyclic ramified cubic extensions, and if $p \equiv 2 \pmod 3$ there is a unique non-cyclic ramified cubic extension, and the discriminants of all these extensions are p^2. Let R be the (maximal ramified) cubic ring corresponding to a lift $\tilde{a}$ of a. Since R is maximal in $R \otimes \mathbb{Q}_p$, $\operatorname{Aut}_{\mathbb{Z}_p}(R) \cong \operatorname{Aut}_{\mathbb{Q}_p}(R \otimes \mathbb{Q}_p)$. Lemma 5.11 asserts that

$$|G_{p^2,a}| = |\operatorname{Aut}_{\mathbb{Q}_p}(R \otimes \mathbb{Q}_p)| \, |\operatorname{Disc}(R)|^{-1}$$

for each case and hence we have the result. ■

The following result, proved with the aid of PARI/GP [19], will be used in Section 8.5.

Proposition 5.15 *For $p = 3$ and $a \in V_{p^3}$ of type $(1^3_{\max})$, $G_{p^3} a + p^3 V_{\mathbb{Z}_p}$ is a single $G_{\mathbb{Z}_p}$-orbit.*

Proof It is known that there are 9 ramified cubic extensions of $\mathbb{Q}_3$ (see, *e.g.*, [13]) and hence $V_{\mathbb{Z}_p}(1^3_{\max})$ consists of 9 $G_{\mathbb{Z}_p}$-orbits. We list a set of representatives in a table in Proposition 8.20. Using PARI/GP [19] to explicitly calculate the stablizer group in $G_{\mathbb{Z}/27\mathbb{Z}}$ for each representative $a \in V_{\mathbb{Z}/27\mathbb{Z}}(1^3_{\max})$, we confirm the identity $|G_{p^3,a}| = |\operatorname{Aut}_{\mathbb{Q}_p}(R \otimes \mathbb{Q}_p)| \, |\operatorname{Disc}(R)|^{-1}$ as above. This finishes the proof. ■

6 Computation of Singular Gauss Sums

In this section, we explicitly compute the Fourier transforms of the functions $f_p \in C(V_p, \mathbf{1})$ and $\Phi_p, \Phi'_p \in C(V_{p^2}, \mathbf{1})$ introduced in Definitions 5.3 and 5.10. By Proposition 4.7, it suffices to evaluate the orbital Gauss sum $W(\mathbf{1}, a, b)$ for all b and for a in the support of these functions. We call these Gauss sums singular because $P(a)$ is not invertible for any such a.

For $N = p$, these Gauss sums were computed by S. Mori [14]. We first review his results and then study the case $N = p^2$ by extending Mori's approach.

https://doi.org/10.4153/CJM-2013-027-0 Published online by Cambridge University Press

6.1 The Case $N = p$

In this subsection we will prove the following.

Proposition 6.1 *The Fourier transform of $f_p \in C(V_p)$ is given by*

$$\widehat{f_p}(b) = \begin{cases} -p^{-3} & P^*(b) \neq 0, \\ p^{-2} - p^{-3} & P^*(b) = 0, b \neq 0, \\ p^{-1} + p^{-2} - p^{-3} & b = 0. \end{cases}$$

By Proposition 4.7,

$$\widehat{f_p}(b) = p^{-4}|G_p|^{-1} \sum_{a \in V_p} f_p(a) W(\mathbf{1}, a, b) = p^{-4}|G_p|^{-1} \sum_{P(a)=0} W(\mathbf{1}, a, b)$$

and so we are interested in $W(\mathbf{1}, a, b)$ for those a with $P(a) = 0$. Let $p \neq 3$. Then the map $\iota\colon V_p^* \to V_p$ is an isomorphism of G_p-modules, so we may and do identify V_p^* with V_p. Hence the orbital Gauss sum $W(\chi, a, b)$ is defined for a character χ on $\mathbb{F}_p^\times$ and $a, b \in V_p$. Since the bilinear form (2.1) is alternating, we have $W(\chi, b, a) = \chi(-1)W(\chi, a, b)$. As mentioned above, explicit formulas for these Gauss sums were proved by Mori [14]. Here we quote some of his results with his permission.

Proposition 6.2 (Mori) *Let $p \neq 3$. Assume $\chi = \mathbf{1}$ and $P(a) = 0$, $a \neq 0$. Then $W(\mathbf{1}, a, b)$ is given by the following table.*

type of b	*a: of type* (1^3)	*a: of type* $(1^2 1)$
(0)	$(p^2 - p)(p^2 - 1)$	$(p^2 - p)(p^2 - 1)$
(1^3)	$-p(p-1)$	$p(p-1)^2$
$(1^2 1)$	$p(p-1)^2$	$p(p-1)(p-2)$
(111)	$p(p-1)(2p-1)$	$-3p(p-1)$
(21)	$-p(p-1)$	$-p(p-1)$
(3)	$-p(p-1)(p+1)$	0

Since Mori's preprint is not yet available, we will give a brief outline of his proof in Remark 6.8 in the next subsection.

Proof of Proposition 6.1 The case $p = 3$ can be checked numerically, so we assume $p \neq 3$. As above, we identify V_p^* with V_p. When b is of type (111), by Lemma 5.2 and Propositions 4.7 and 6.2,

$$\begin{aligned} \widehat{f_p}(b) &= p^{-4}|G_p|^{-1} \sum_{a \in V_p(0) \sqcup V_p(1^3) \sqcup V_p(1^2 1)} W(\mathbf{1}, a, b) \\ &= \frac{(p^2-1)(p^2-p) \cdot 1 + p(p-1)(2p-1) \cdot (p^2-1) - 3p(p-1) \cdot p(p^2-1)}{p^4(p^2-1)(p^2-p)} \\ &= -p^{-3}. \end{aligned}$$

All the other cases are computed similarly. ■

https://doi.org/10.4153/CJM-2013-027-0 Published online by Cambridge University Press

6.2 The Case $N = p^2$

In this subsection we assume $p \neq 2, 3$. We identify $V_{p^2}^*$ with V_{p^2} via ι. Recall that we defined $\Phi_p, \Phi'_p \in C(V_{p^2}, \mathbf{1})$ in Definition 5.10. In this subsection we will prove the following.

Theorem 6.3 *The Fourier transform of Φ_p is given as follows:*

(i) *Let $b \in pV_{p^2}$. We write $b = pb'$ and regard b' as an element of V_p. Then*

$$\widehat{\Phi_p}(pb') = \begin{cases} p^{-2} + p^{-3} - p^{-5} & \text{for } b' \text{ of type } (0), \\ p^{-3} - p^{-5} & \text{for } b' \text{ of type } (1^3), (1^2 1), \\ -p^{-5} & \text{for } b' \text{ of type } (111), (21), (3). \end{cases}$$

(ii) *For $b \in V_{p^2} \setminus pV_{p^2}$,*

$$\widehat{\Phi_p}(b) = \begin{cases} p^{-3} - p^{-5} & \text{for } b \text{ of type } (1^3_{**}), \\ -p^{-5} & \text{for } b \text{ of type } (1^3_{*}), (1^3_{\max}), \\ 0 & \text{otherwise.} \end{cases}$$

Theorem 6.4 *The Fourier transform of Φ_p is given as follows:*

(i) *Let $b \in pV_{p^2}$ and write $b = pb'$ as above. Then*

$$\widehat{\Phi'_p}(pb') = \begin{cases} 2p^{-2} - p^{-4} & \text{for } b' \text{ of type } (0), \\ p^{-3} - p^{-4} & \text{for } b' \text{ of type } (1^3), \\ 2p^{-3} - 2p^{-4} & \text{for } b' \text{ of type } (1^2 1), \\ 2p^{-3} - 3p^{-4} & \text{for } b' \text{ of type } (111), \\ -p^{-4} & \text{for } b' \text{ of type } (21), \\ -p^{-3} & \text{for } b' \text{ of type } (3). \end{cases}$$

(ii) *For $b \in V_{p^2} \setminus pV_{p^2}$,*

$$\widehat{\Phi'_p}(b) = \begin{cases} p^{-3} - p^{-4} & \text{for } b \text{ of type } (1^3_{**}), \\ -p^{-4} & \text{for } b \text{ of type } (1^3_{*}), \\ 0 & \text{otherwise.} \end{cases}$$

Remark 6.5 We may check that our results are consistent with the Parseval formula

$$\sum_{b \in V_{p^2}} |\widehat{\Phi_p}(b)|^2 = p^{-8} \sum_{a \in V_{p^2}} |\Phi_p(a)|^2,$$

and similarly for Φ'_p.

Remark 6.6 As noted in the introduction, it is interesting to compare these results with the results of Fouvry and Katz [7] and in particular their Lemma 9.3. In particular, we observe the same phenomenon, *i.e.*, the cubic Gauss sums are larger on highly singular orbits.

To prove these theorems, we evaluate $W(\mathbf{1}, a, b)$ for $a \in \tilde{V}^{\mathrm{nm}}_{p^2}$.

Proposition 6.7 *Assume $b \in V_{p^2} \setminus pV_{p^2}$. Then for $a \in \tilde{V}^{\mathrm{nm}}_{p^2}$, the orbital Gauss sum $W(\mathbf{1}, a, b)$ is given by the following table.*

type of b	*a: of type* (1^3_{**})	*a: of type* (1^3_{*})	*a: of type* (1^3_{max})	*a: of type* $(1^2 1_{*})$
(1^3_{**})	$p^5(p-1)^2$	$p^5(p-1)^2$	$-p^5(p-1)$	$p^5(p-1)^2$
(1^3_{*})	$p^5(p-1)^2$	$p^5(p-1)^2$	$-p^5(p-1)$	$-p^5(p-1)$
(1^3_{max})	$-p^5(p-1)$	$-p^5(p-1)$	p^5 on average	0
$(1^2 1_{*})$	$p^5(p-1)^2$	$-p^5(p-1)$	0	0
$(1^2 1_{\mathrm{max}})$	$-p^5(p-1)$	p^5 on average	0	0
(111)	0	0	0	0
(21)	0	0	0	0
(3)	0	0	0	0

Here, when we say "on average", we fix b and take the average of $W(\mathbf{1}, a, b)$ over all a of the given type. For example, if b is of type $(1^2 1_{\mathrm{max}})$, "p^5 on average" in the second entry means $|V_{p^2}(1^3_*)|^{-1} \sum_{a \in V_{p^2}(1^3_*)} W(\mathbf{1}, a, b) = p^5$. (The individual values are described in the proof.)

The theorems follow from Propositions 6.2 and 6.7.

Proof of Theorems 6.3 and 6.4 Assume $b = pb'$, $b' \in V_p$. Then $W_{p^2}(1, a, pb') = p^4 W_p(1, a, b')$ by Lemma 4.9. There are respectively p^4, $p^3(p^2-1)$, and $p^4(p^2-1)$ elements in $V^{\mathrm{nm}}_{p^2}$ whose reductions modulo p are of type (0), (1^3), and $(1^2 1)$, respectively. Similarly there are respectively p^4, $p^4(p^2-1)$, and $p^4(p^2-1)$ in $\tilde{V}^{\mathrm{nm}}_{p^2}$. Hence by Propositions 4.7 and 6.2, if b' is of type (111), we have

$$\begin{aligned}
\widehat{\Phi}_p(pb') &= \frac{1}{p^4|G_{p^2}|} \sum_{a \in V^{\mathrm{nm}}_{p^2}} W_p(1, a, b') \\
&= \frac{p^3(p^2-p)(p^2-1)\{p + (2p-1) - 3p\}}{p^4|G_{p^2}|} = -p^{-5}, \\
\widehat{\Phi'_p}(pb') &= \frac{1}{p^4|G_{p^2}|} \sum_{a \in \tilde{V}^{\mathrm{nm}}_{p^2}} W_p(1, a, b') \\
&= \frac{p^4(p^2-p)(p^2-1)\{1 + (2p-1) - 3\}}{p^4|G_{p^2}|} = 2p^{-3} - 3p^{-4}.
\end{aligned}$$

https://doi.org/10.4153/CJM-2013-027-0 Published online by Cambridge University Press

Other cases of $b \in pV_{p^2}$ are handled similarly. Now let $b \in V_{p^2} \setminus pV_{p^2}$. Then since $(b \bmod p) \neq 0$, we have

$$\sum_{a \in pV_{p^2}} W_{p^2}(\mathbf{1}, a, b) = p^4 \sum_{a' \in V_p} W_p(\mathbf{1}, a', b) = 0.$$

Hence by Proposition 4.7,

$$\widehat{\Phi_p}(b) = \frac{1}{p^8 |G_{p^2}|} \sum_{a \in V^{\mathrm{nm}}_{p^2} \setminus pV_{p^2}} W_{p^2}(\mathbf{1}, a, b) \quad \text{and}$$

$$\widehat{\Phi'_p}(b) = \frac{1}{p^8 |G_{p^2}|} \sum_{a \in \tilde{V}^{\mathrm{nm}}_{p^2} \setminus pV_{p^2}} W_{p^2}(\mathbf{1}, a, b).$$

Our formulas now follow from Proposition 6.7 and Lemma 5.6. ■

We now come to the proof of Proposition 6.7.

Proof of Proposition 6.7 We prove this by case by case direct computations. We begin by introducing some notation and explaining our approach. Since $W(\mathbf{1}, a, b)$ depends only on the G_{p^2}-orbits of a and b, we will take a specific representative from each orbit and compute for those a and b. Let $R = \mathbb{Z}/p^2\mathbb{Z}$, as in Section 5.2. We will choose b according to its type, as follows:

type of b	b	condition on the coefficients
(1^3_{**})	$(1, 0, 0, 0)$	–
(1^3_{*})	$(1, 0, l, 0)$	$l \in pR^\times$
$(1^3_{\max})$	$(1, 0, k, -l)$	$k \in pR, l \in pR^\times$
$(1^2 1_{*})$	$(0, -1, 0, 0)$	–
$(1^2 1_{\max})$	$(0, -1, 0, -l)$	$l \in pR^\times$
(111)	$(0, -1, 1, 0)$	–
(21)	$(0, -1, 0, -l)$	$u^2 + l \in R[u]$ is irreducible
(3)	$(1, 0, k, -l)$	$u^3 + ku - l \in R[u]$ is irreducible

For b of type $(1^3_{\max})$, we can let $k = 0$, but we sometimes leave it as is to treat types $(1^3_{\max})$ and (3) simultaneously. We will choose $a \in V_{p^2}$ later.

We put

$$G_{p^2,1} := \left\{ g_1 := t(1 - mn) \begin{pmatrix} s & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & n \\ m & 1 \end{pmatrix} \;\middle|\; s, t \in R^\times, n \in R, m \in pR \right\} \subset G_{p^2},$$

$$G_{p^2,2} := \left\{ g_2 := -t \begin{pmatrix} s & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} m & 1 + mn \\ 1 & n \end{pmatrix} \;\middle|\; s, t \in R^\times, n, m \in R \right\} \subset G_{p^2}.$$

Then $G_{p^2} = G_{p^2,1} \sqcup G_{p^2,2}$. We also drop p^2 and write $G_1 = G_{p^2,1}, G_2 = G_{p^2,2}$. We write $\langle t \rangle := \exp(2\pi i t/p^2)$, hence $\langle a, b \rangle = \langle [a, b] \rangle$. We put

$$W_i(a, b) := \sum_{g_i \in G_i} \langle [g_i a, b] \rangle \quad i = 1, 2,$$

and compute this value for each choice of a, b. We recall the formula (2.1),

$$[a, b] = a_4 b_1 - \frac{1}{3} a_3 b_2 + \frac{1}{3} a_2 b_3 - a_1 b_4,$$

for $a = (a_1, a_2, a_3, a_4), b = (b_1, b_2, b_3, b_4) \in V_{p^2}$, which will be used throughout. When convenient, we write an element of V_{p^2} as a row vector via its transpose.

We immediately see that

$$\sum_{t \in R^\times} \langle t \rangle = 0, \quad \sum_{t \in R^\times} \langle pt \rangle = -p, \quad \sum_{n \in R} \langle n \rangle = \sum_{n \in R} \langle pn \rangle = \sum_{n \in pR} \langle n \rangle = 0.$$

We use these formulas and their variations very often. For example, if $f(s, m, n) \in R$ is a function independent of t and $f(s, m, n) \in R^\times$ for all s, m, n, then

$$\sum_{t \in R^\times} \sum_{s,m,n} \langle t \cdot f(s, m, n) \rangle = \sum_{s,m,n} \sum_{t \in R^\times} \langle t \rangle = 0.$$

Also, if $g(s, m) \in pR$ is independent of n and $\alpha \in pR^\times$ is a constant, then

$$\sum_{n \in R} \sum_{t \in R^\times} \sum_{s,m} \Big\langle t\big(g(s, m) + \alpha n\big) \Big\rangle = \sum_{t \in R^\times} \sum_{s,m} \sum_{n \in R} \langle \alpha n \rangle = 0.$$

These are typical examples of change of variables, and we omit the explanation of such modifications when they are easy and natural. Finally, note that $W(\mathbf{1}, a, b) = W(\mathbf{1}, b, a)$.

We now carry out the computation. In what follows, we see that $W_2(a, b) = 0$ and $W_1(a, b)$ is given by the table given in Proposition 6.7 for all of our chosen representatives.

(I) ***a* is of type** (1^3_{**})**.** We choose $a = (1, 0, 0, 0)$. To make the computation easier we replace the variables t, m of g_1 by $s^{-2}t, st^{-1}m$ and t, m of g_2 by st and $s^{-1}m$. Then since the variable m of g_1 is in pR and hence $m^2 = 0$, we have

$$g_1 a = \begin{pmatrix} t \\ 3m \\ 0 \\ 0 \end{pmatrix}, \quad g_2 a = t \begin{pmatrix} m^3 \\ 3m^2 \\ 3m \\ 1 \end{pmatrix}.$$

If $b = (1, 0, 0, 0)$, then since $|G_1| = p^5(p-1)^2$,

$$W_1(a, b) = \sum_{g_1 \in G_1} 1 = p^5(p-1)^2, \quad W_2(a, b) = \sum_{g_2 \in G_2} \langle t \rangle = \sum_{s,m,n} \sum_{t \in R^\times} \langle t \rangle = 0.$$

https://doi.org/10.4153/CJM-2013-027-0 Published online by Cambridge University Press

If $b = (0, -1, 0, 0)$, then

$$W_1(a,b) = \sum_{g_1 \in G_1} 1 = p^5(p-1)^2, \quad W_2(a,b) = \sum_{g_2 \in G_2} \langle tm \rangle = \sum_{s,t,n} \sum_{m \in R} \langle tm \rangle = 0.$$

If $b = (1, 0, l, 0)$ is of type (1^3_*), then since $1 + lm^2 \in R^\times$ for any $m \in R$, we have

$$W_1(a,b) = \sum_{g_1 \in G_1} 1 = p^5(p-1)^2, \quad W_2(a,b) = \sum_{g_2 \in G_2} \langle t(1+lm^2) \rangle = \sum_{g_2 \in G_2} \langle t \rangle = 0.$$

If $b = (0, -1, 1, 0)$, then $W_1(a,b) = \sum_{g_1 \in G_1} \langle m \rangle = 0$ and

$$\begin{aligned} W_2(a,b) &= \sum_{g_2 \in G_2} \langle t(m+m^2) \rangle = \Bigl(\sum_{m+m^2 \in R^\times} + \sum_{m+m^2 \in pR^\times} + \sum_{m+m^2=0} \Bigr) \langle t(m+m^2) \rangle \\ &= 0 + 2(p-1) \sum_{n \in R, s \in R^\times} (-p) + 2 \sum_{n \in R, s,t \in R^\times} 1 \\ &= -2p^4(p-1)^2 + 2p^4(p-1)^2 = 0. \end{aligned}$$

Let $b = (0, -1, 0, -l)$ be either of type $(1^2 1_{\max})$ or (21). Then $l \in pR^\times$ if b is of type $(1^2 1_{\max})$ and $l \in R^\times$ if b is of type (21). Also $1 + lm^2 \in R^\times$ for any m, since $1 + lX^2 \in R[X]$ is an irreducible polynomial. Hence we have

$$\begin{aligned} W_1(a,b) &= \sum_{g_1 \in G_1} \langle tl \rangle = \begin{cases} \sum_{s,m,n} (-p) = -p^5(p-1) & (1^2 1_{\max}), \\ \sum_{s,m,n} 0 = 0 & (21), \end{cases} \\ W_2(a,b) &= \sum_{g_2 \in G_2} \langle tm(1+lm^2) \rangle = \sum_{g_2 \in G_2} \langle tm \rangle = \sum_{s,t,n} \sum_{m \in R} \langle tm \rangle = 0. \end{aligned}$$

Finally, if $b = (1, 0, k, -l)$ is of type $(1^3_{\max})$ or (3), then by a similar consideration as above,

$$\begin{aligned} W_1(a,b) &= \sum_{s,m,n} \langle km \rangle \sum_{t} \langle tl \rangle = \begin{cases} \sum_{s,m,n} (-p) = -p^5(p-1) & (1^3_{\max}), \\ \sum_{s,m,n} 0 = 0 & (3), \end{cases} \\ W_2(a,b) &= \sum_{g_2 \in G_2} \langle t(1 + km^2 + lm^3) \rangle = 0. \end{aligned}$$

(II) ***a* is of type** $(1^2 1_*)$**.** We consider this case next. We choose $a = (0, 1, 0, 0)$. Then

$$g_1 a = t \begin{pmatrix} s^2 n \\ s(1+2nm) \\ 2m \\ 0 \end{pmatrix}, \quad g_2 a = t \begin{pmatrix} s^2(m^2 + nm^3) \\ s(2m + 3nm^2) \\ 1 + 3nm \\ s^{-1} n \end{pmatrix}.$$

If $b = (0, -1, 0, 0)$, then

$$W_1(a,b) = \sum_{g_1\in G_1} \left\langle \frac{2tm}{3} \right\rangle = \sum_{s,t,n}\sum_{m\in pR} \langle m\rangle = 0,$$

$$W_2(a,b) = \sum_{g_2\in G_2} \left\langle t\left(\frac{1}{3} + nm\right) \right\rangle = \sum_{t,s}\left\langle \frac{t}{3}\right\rangle \sum_{m,n}\langle tnm\rangle = \sum_{t,s}\langle t\rangle \sum_{m,n}\langle nm\rangle$$

$$= \sum_{m,n,s}\langle nm\rangle \sum_{t\in R^\times}\langle t\rangle = 0.$$

Let $b = (1, 0, l, 0)$ be of type (1^3_*). Since $l \in pR^\times$ and $1 + ls^2m^2$ is always a unit, we have

$$W_1(a,b) = \sum_{g_1\in G_1}\left\langle \frac{tsl}{3}\right\rangle = \sum_{s,m,n}\sum_{t\in R^\times}\langle tl\rangle = \sum_{s,m,n}(-p) = -p^5(p-1),$$

$$W_2(a,b) = \sum_{g_2\in G_2}\left\langle t\left\{ \frac{2mls}{3} + n\left(\frac{1}{s} + lsm^2\right)\right\}\right\rangle$$

$$= \sum_{s,t,r}\left\langle \frac{2mlts}{3}\right\rangle \sum_{n}\left\langle \frac{t}{s}n(1 + ls^2m^2)\right\rangle = 0.$$

Let $b = (0, -1, 1, 0)$ be of type (111). Then

$$W_1(a,b) = \sum_{g_1\in G_1}\left\langle \frac{t}{3}(2m + s(1+2nm))\right\rangle = \sum_{g_1\in G_1}\langle t\rangle = 0.$$

For $W_2(a,b)$, we have

$$W_2(a,b) = \sum_{s,t,m}\sum_{n}\left\langle \frac{t}{3}\left(1 + 2ms + 3n(m+sm^2)\right)\right\rangle.$$

We divide the sum according as $m + sm^2 = m(1+sm) \in R^\times$ or not. The former is

$$\sum_{m+sm^2\in R^\times}\left\langle \frac{t}{3}(1+2ms)\right\rangle \left\langle tn(m+m^2s)\right\rangle = \sum_{m+sm^2\in R^\times}\left\langle \frac{t}{3}(1+2ms)\right\rangle \langle n\rangle = 0.$$

Let $m + sm^2 \in pR$. Then either $m \in pR$ or $ms \in -1 + pR$. Hence

$$\left(1 + 2ms + 3n(m+sm^2)\right) \in R^\times,$$

and so the latter sum is 0 as well. Hence $W_2(a,b) = 0$.

Let $b = (0, -1, 0, -l)$ be of type $(1^21_{\max})$ or (21). If b is of type $(1^21_{\max})$ then $s^2nl \in pR$, and if b is of type (21) then $s^2l \in R^\times$ for any s, n. Hence

$$W_1(a,b) = \sum_{g_1\in G_1}\left\langle t\left(\frac{2m}{3} + s^2nl\right)\right\rangle = \begin{cases} \sum_{t,s,n}\sum_{m\in pR}\langle tm\rangle = 0 & (1^21_{\max}),\\ \sum_{t,s,m}\sum_{n\in R}\langle tn\rangle = 0 & (21).\end{cases}$$

https://doi.org/10.4153/CJM-2013-027-0 Published online by Cambridge University Press

For $W_2(a,b)$, since $1+s^2m^2l \in R^\times$, we have

$$W_2(a,b) = \sum_{g_2\in G_2} \Big\langle t\Big(\frac{1}{3}+s^2m^2l\Big)\Big\rangle \langle tnm(1+s^2m^2l)\rangle = \sum_{t,s,m}\Big\langle t\Big(\frac{1}{3}+s^2m^2l\Big)\Big\rangle \sum_{n}\langle nm\rangle.$$

Since $\sum_{n\in R}\langle nm\rangle = 0$ unless $m=0$, we have $W_2(a,b)=\sum_{t,s,n}\langle t/3\rangle = 0$.

Let $b=(1,0,k,-l)$ be of type $(1^3_{\max})$ or (3). If b is of type $(1^3_{\max})$, since $l \in pR^\times$,

$$W_1(a,b) = \sum_{g_1\in G_1}\Big\langle t\Big(\frac{sk}{3}+s^2ln\Big)\Big\rangle = \sum_{t,s,m}\Big\langle \frac{tsk}{3}\Big\rangle \sum_{n}\langle ts^2ln\rangle = 0.$$

If b is of type (3), then since $s^2l+\frac{2sk}{3}m \in R^\times$,

$$W_1(a,b) = \sum_{g_1\in G_1}\Big\langle tn\Big(s^2l+\frac{2sk}{3}m\Big)\Big\rangle\Big\langle\frac{tsk}{3}\Big\rangle = \sum\langle n\rangle\Big\langle\frac{tsk}{3}\Big\rangle = 0.$$

Moreover for both types,

$$W_2(a,b) = \sum_{g_2\in G_2}\langle tn(s^{-1}+sm^2k+s^2m^3l)\rangle\Big\langle t\Big(\frac{2msk}{3}+s^2m^2l\Big)\Big\rangle.$$

Since $s^{-1}+sm^2k+s^2m^3l \in R^\times$, $W_2(a,b)=\sum_{g_2}\langle n\rangle\langle t(\frac{2msk}{3}+s^2m^2l)\rangle = 0$.

(III) ***a*** **is of type** (1^3_*)**.** Let $a=(1,0,\alpha,0)$, where $\alpha\in pR^\times$. By replacing m of g_1 with $s^{-1}m-2\alpha n/3$, we have

$$g_1a = t\begin{pmatrix} s^2(1+\alpha n^2)\\ 3m\\ \alpha\\ 0\end{pmatrix}, \quad g_2a = t\begin{pmatrix} s^2\big(m^3+\alpha(n^2m^3+2nm^2+m)\big)\\ s\big(3m^2+\alpha(3n^2m^2+4nm+1)\big)\\ 3m+\alpha(3n^2m+2n)\\ s^{-1}(1+\alpha n^2)\end{pmatrix}.$$

Let $b=(1,0,l,0)$ be of type (1^3_*). Then

$$W_1(a,b)=\sum_{g_1\in G_1}1 = p^5(p-1)^2, \quad W_2(a,b)=\sum_{g_2\in G_2}\Big\langle t\Big(\frac{1}{s}(1+\alpha n^2)+slm^2\Big)\Big\rangle$$
$$= \sum_{g_2\in G_2}\langle t\rangle = 0.$$

Let $b=(0,-1,1,0)$ be of type (111). Then $W_1(a,b)=\sum_{t,s,n}\langle t\alpha/3\rangle\sum_m\langle tm\rangle = 0$, and

$$\begin{aligned} W_2(a,b) &= \sum_{g_2\in G_2}\Big\langle\frac{t}{3}\big(3m+\alpha(3n^2m+2n)\big)\Big\rangle\Big\langle\frac{ts}{3}\big(3m^2+\alpha(3n^2m^2+4nm+1)\big)\Big\rangle\\ &= \sum_{t,s,n}\Big(\sum_{m\in R^\times}\langle t\rangle\langle ts\rangle + \sum_{m\in pR}\Big\langle t\Big(m+\frac{2\alpha n}{3}\Big)\Big\rangle\Big\langle\frac{ts\alpha}{3}\Big\rangle\Big)\\ &= \sum_{m\in R^\times}\sum_{s,n}\sum_{t\in R^\times}\langle s\rangle\langle t\rangle + \sum_{m\in pR}\sum_{s,t}\sum_{n\in R}\langle m\rangle\langle t\rangle = 0+0=0.\end{aligned}$$

Let $b = (1, 0, k, -l)$ be either of type $(1^3_{\max})$ or (3). Then

$$W_1(a,b) = \begin{cases} \sum_{g_1\in G_1} \langle ts^2 l\rangle = -p^5(p-1) & (1^3_{\max}),\\ \sum_{g_1\in G_1} \left\langle t\left(ls^2 + (km + \alpha s^2 n^2 l)\right)\right\rangle = \sum_{g_1\in G_1}\langle t\rangle = 0 & (3),\end{cases}$$

$$W_2(a,b) = \sum_{g_2\in G_2} \langle t\{s^{-1}(1 + ks^2m^2 + ls^3m^3) + \alpha f(s,n,m)\}\rangle = \sum_{g_2\in G_2}\langle t\rangle = 0.$$

Note that $1 + ks^2m^2 + ls^3m^3 = b(1, sm) \in R^\times$ for all s, m.

Let $b = (0, -1, 0, -l)$ be of type $(1^2 1_{\max})$ or (21). Then

$$W_2(a,b) = \sum_{G_2}\left\langle t\left\{ m(1 + lm^2s^2) + \frac{\alpha}{3} f(s,m,n)\right\}\right\rangle,$$

where $f(s,m,n) = 3n^2m + 2n + s^2(n^2m^3 + 2nm^2 + m)l$. Note that $1 + lm^2s^2 \in R^\times$. If $m \in pR$, then $\alpha f(s,m,n) = 2n\alpha$. Hence

$$W_2(a,b) = \sum_{m\in R^\times}\langle t\rangle + \sum_{m\in pR}\left\langle t\left(m + \frac{2n\alpha}{3}\right)\right\rangle = 0 + 0 = 0.$$

If b is of type (21),

$$W_1(a,b) = \sum_{G_1}\left\langle t\left(ls^2 + \frac{\alpha}{3} + ls^2n^2\alpha\right)\right\rangle = 0.$$

If b is of type $(1^2 1_{\max})$,

$$W_1(a,b) = \sum_{g_1\in G_1}\left\langle t\left(\frac{\alpha}{3} + ls^2\right)\right\rangle = \sum_{s,m,n}\sum_{t\in R^\times}\langle t(\alpha + 3ls^2)\rangle.$$

We consider whether $\alpha + 3ls^2 \in pR$ is 0 or not for $s \in R^\times$. Note that since $\alpha, 3l \in pR^\times$, we can regard $\alpha/3l \in \mathbb{F}_p^\times$. If $-\alpha/3l$ is not a square in $\mathbb{F}_p^\times$, then $\alpha + 3ls^2 \in pR^\times$ for any $s \in R^\times$. If $-\alpha/3l$ is a square in $\mathbb{F}_p^\times$, then $\alpha + 3ls^2 = 0$ for $2p$ choices of $s \in R^\times$, and $\alpha + 3ls^2 \in pR^\times$ otherwise. Hence

$$W_1(a,b) = \begin{cases} \sum_{s,m,n}(-p) = p^5 - p^6 & \text{if } -\alpha/3l \notin (\mathbb{F}_p^\times)^2,\\ 2p\sum_{m,n}(p^2 - p) + (p^2 - 3p)\sum_{m,n}(-p) & \\ \qquad = p^5 + p^6 & \text{if } -\alpha/3l \in (\mathbb{F}_p^\times)^2.\end{cases}$$

By Proposition 5.12 (ii), for $a \in V_{p^2}(1^3_*)$, $-\alpha/3l \in (\mathbb{F}_p^\times)^2$ or $-\alpha/3l \notin (\mathbb{F}_p^\times)^2$ occurs with equal probability. Hence the average value of $W_1(a,b)$ with respect to $a \in V_{p^2}(1^3_*)$ is p^5.

https://doi.org/10.4153/CJM-2013-027-0 Published online by Cambridge University Press

(IV) a is of type $(1^3_{\max})$. By Proposition 5.12, we can take $a=(1,0,0,\alpha)$ for some $\alpha \in pR^\times$. Then

$$g_1a = t\begin{pmatrix} s^2(1+\alpha n^3) \\ 3s(m+\alpha n^2) \\ 3\alpha n \\ s^{-1}\alpha \end{pmatrix}, \quad g_2a = t\begin{pmatrix} s^2\big(m^3+\alpha(mn+1)^3\big) \\ 3s\big(m^2+\alpha n(mn+1)^2\big) \\ 3\big(m+\alpha n^2(mn+1)\big) \\ s^{-1}(1+\alpha n^3) \end{pmatrix}.$$

Let $b=(0,-1,1,0)$. Then

$$\begin{aligned} W_1(a,b) &= \sum_{s,t,n}\sum_{m\in pR}\langle t(sm+\alpha n+\alpha sn^2)\rangle = \sum_{s,t,n}\sum_{m\in pR}\langle m\rangle = 0, \\ W_2(a,b) &= \sum_{g_2\in G_2}\Big\langle t\big(m+\alpha n^2(mn+1)\big)\Big\rangle\Big\langle st\big(m^2+\alpha n(mn+1)^2\big)\Big\rangle \\ &= \sum_{s,t,n}\sum_{m\in R^\times}\langle t\rangle\langle ts\rangle + \sum_{s,t,n}\sum_{m\in pR}\langle t(m+\alpha n^2)\rangle\langle \alpha tsn\rangle = 0+0=0. \end{aligned}$$

Let $b=(0,-1,0,-l)$ be of type $(1^21_{\max})$ or (21). Then

$$\begin{aligned} W_1(a,b) &= \sum_{g_1\in G_1}\langle t(\alpha n+ls^2(1+\alpha n^3))\rangle = \begin{cases} \sum_{s,t,m}\sum_n\langle t(\alpha n+ls^2)\rangle = 0 & (1^21_{\max}), \\ \sum_{s,m,n}\sum_t\langle t\rangle = 0 & (21), \end{cases} \\ W_2(a,b) &= \sum_{g_2\in G_2}\Big\langle t\Big\{m(1+ls^2m^2)+\alpha\big(n^2(mn+1)+ls^2(mn+1)^3\big)\Big\}\Big\rangle \\ &= \sum_{s,t,n}\sum_{m\in R^\times}\langle t\rangle + \sum_{s,t,n}\sum_{m\in pR}\Big\langle t\big(m+\alpha(n^2+s^2l)\big)\Big\rangle = 0+0=0. \end{aligned}$$

Let $b=(1,0,k,-l)$ be of type (3). Then

$$\begin{aligned} W_1(a,b) &= \sum_{g_1\in G_1}\Big\langle t\big(ls^2+ksm+\alpha(s^{-1}+kn^2+ls^2n^3)\big)\Big\rangle = \sum_{s,m,n}\sum_{t\in R^\times}\langle t\rangle = 0, \\ W_2(a,b) &= \sum_{g_2\in G_2}\langle t\{s^{-1}(1+ks^2m^2+ls^3m^3)+\alpha f(s,m,n)\}\rangle = \sum_{s,m,n}\sum_{t\in R^\times}\langle t\rangle = 0. \end{aligned}$$

Note that $1+ks^2m^2+ls^3m^3 \in R^\times$ for any s,m.

Let $b=(1,0,0,-l)$ be of type $(1^3_{\max})$. (By Proposition 5.12, we may assume $k=0$.) Similarly to as above, we have $W_2(a,b)=0$. For $W_1(a,b)$, we have

$$W_1(a,b) = \sum_{g_1\in G_1}\Big\langle \frac{t}{s}(\alpha+s^3l)\Big\rangle = \sum_{t,m,n}\sum_s\langle t(\alpha+s^3l)\rangle.$$

We consider whether $\alpha+s^3l\in pR$ is 0 or not for $s\in R^\times$.

https://doi.org/10.4153/CJM-2013-027-0 Published online by Cambridge University Press

First, let $p \equiv 2 \pmod 3$. Then $\alpha + s^3 l = 0$ for p choices of s and $\alpha + s^3 l \in pR^\times$ otherwise. Hence

$$W_1(a,b) = p \sum_{m,n,t} 1 + (p^2 - 2p) \sum_{m,n} (-p) = p(p^2 - p)p^3 - (p^2 - 2p)p^4 = p^5.$$

Next let $p \equiv 1 \pmod 3$. If $-\alpha/l$ is not a cube in $\mathbb{F}_p^\times$, then $\alpha + s^3 l \in pR^\times$ for all s. If $-\alpha/l$ is a cube in $\mathbb{F}_p^\times$, $\alpha + s^3 l = 0$ for $3p$ choices of s and $\alpha + s^3 l \in pR^\times$ otherwise. Hence

$$W_1(a,b) = \begin{cases} (p^2 - p) \sum_{m,n} (-p) = p^5 - p^6 & -\alpha/l \notin (\mathbb{F}_p^\times)^3, \\ 3p \sum_{m,n,t} 1 + (p^2 - 4p) \sum_{m,n} (-p) = p^5 + 2p^6 & -\alpha/l \in (\mathbb{F}_p^\times)^3. \end{cases}$$

By Proposition 5.12 (iv), the average value of $W_1(a,b)$ with respect to $a \in V_{p^2}(1^3_{\max})$ is $\frac{2}{3}(p^5 - p^6) + \frac{1}{3}(p^5 + 2p^6) = p^5$. ■

Remark 6.8 We briefly review Mori's proof [14] of Proposition 6.2. The outline is quite similar to the proof above. We fix a prime $p \neq 3$. Let

$$G_{p,1} := \left\{ g_1 := t \begin{pmatrix} s & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \;\middle|\; s, t \in \mathbb{F}_p^\times, n \in \mathbb{F}_p \right\} \subset G_p,$$

$$G_{p,2} := \left\{ g_2 := -t \begin{pmatrix} s & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} m & 1 + mn \\ 1 & n \end{pmatrix} \;\middle|\; s, t \in \mathbb{F}_p^\times, n, m \in \mathbb{F}_p \right\} \subset G_p.$$

Then $G_p = G_{p,1} \sqcup G_{p,2}$. We drop p and write $G_1 = G_{p,1}, G_2 = G_{p,2}$. We write $\langle t \rangle := \exp(2\pi i t/p)$, hence $\langle a, b \rangle = \langle [a,b] \rangle$. We put $W_i(a,b) := \sum_{g_i \in G_i} \langle [g_i a, b] \rangle$ and compute this value. Note that $W(\mathbf{1}, a, b) = W_1(a,b) + W_2(a,b)$. In this case of $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, we have

$$\sum_{t \in \mathbb{F}_p^\times} \langle t \rangle = -1, \qquad \sum_{n \in \mathbb{F}_p} \langle n \rangle = 0.$$

Let $a = (1,0,0,0)$ be of type (1^3). Then, with a change of variables similar to that in (I) in the previous proof, we have $g_1 a = (t,0,0,0)$, $g_2 a = t(m^3, 3m^2, 3m, 1)$. If $b = (1,0,0,0)$, then

$$W_1(a,b) = \sum_{g \in G_1} 1 = |G_1| = p(p-1)^2,$$

$$W_2(a,b) = \sum_{g \in G_2} \langle t \rangle = \sum_{s,m,n} (-1) = -p^2(p-1),$$

and hence $W(\mathbf{1}, a, b) = -p(p-1)$. If $b = (0,1,0,0)$, then

$$W_1(a,b) = \sum_{g \in G_1} 1 = p(p-1)^2, \quad W_2 = \sum_{g \in G_2} \langle tm \rangle = \sum_{s,t,n} \sum_{m} \langle m \rangle = 0$$

and $W(\mathbf{1},a,b) = p(p-1)^2$ follows. If $b = (1,0,k,-l)$ is of type (3), then $l \in \mathbb{F}_p^\times$ and also $1 + m^2k + m^3l \in \mathbb{F}_p^\times$ for all $m \in \mathbb{F}_p$. Hence

$$W_1(a,b) = \sum_{g\in G_1} \langle tl \rangle = -p(p-1), \quad W_2(a,b) = \sum_{g\in G_2} \langle t(1+km^2+lm^3) \rangle = -p^2(p-1)$$

and so $W(\mathbf{1},a,b) = -p(p^2-1)$. Let $a = (0,1,0,0)$. Then as in (II) in the previous proof,

$$g_1 a = t \begin{pmatrix} s^2 n \\ s \\ 0 \\ 0 \end{pmatrix}, \quad g_2 a = t \begin{pmatrix} s^2(m^2+nm^3) \\ s(2m+3nm^2) \\ 1+3nm \\ s^{-1}n \end{pmatrix}.$$

Let $b = (0,-1,1,0)$ be of type (111). Then $W_1(a,b) = \sum_{g\in G_1} \langle ts/3 \rangle = -p(p-1)$. For $W_2(a,b)$, by exactly the same consideration as in (II) in the previous proof,

$$\begin{aligned} W_2(a,b) &= \sum_{m+sm^2\in\mathbb{F}_p^\times} \left\langle \frac{t}{3}(1+2ms) \right\rangle \langle n \rangle + \sum_{m=0} \left\langle \frac{t}{3} \right\rangle + \sum_{1+ms=0} \left\langle -\frac{t}{3} \right\rangle \\ &= 0 - p(p-1) - p(p-1) = -2p(p-1). \end{aligned}$$

Hence we have $W(\mathbf{1},a,b) = -3p(p-1)$. Let $b = (0,-1,0,-l)$ be of type (21). Then similarly,

$$W_1(a,b) = \sum_{t,s,n,m} \langle ts^2nl \rangle = 0, \quad W_2(a,b) = \sum_{t,s,n,m} \langle t/3 \rangle = -p(p-1)$$

and hence $W(\mathbf{1},a,b) = -p(p-1)$. The other cases are obtained similarly and we omit the details.

7 The Ohno–Nakagawa Formula

25 years after Shintani introduced the zeta functions $\xi(s)$ and $\xi^*(s)$, Ohno [16] conjectured a remarkably simple formula satisfied by $\xi(s)$ and $\xi^*(s)$. This was proved by Nakagawa [15].

Theorem 7.1 (Ohno, Nakagawa) *We have*

$$\xi^*(s) = A \cdot \xi(s), \quad A = \begin{pmatrix} 0 & 1 \\ 3 & 0 \end{pmatrix}.$$

By plugging this formula into Shintani's functional equation $\xi(1-s) = M(s)\xi^*(s)$ in Theorem 4.1, the functional equation is rewritten in the following symmetric form.

Theorem 7.2 (Ohno, Nakagawa) *We have*

$$\Delta(1-s) \cdot T \cdot \xi(1-s) = \Delta(s) \cdot T \cdot \xi(s),$$

where $\Delta(s)$ and T are as in Theorem 1.7.

Theorem 7.2 follows from Theorem 7.1 simply because $\Delta(1-s)TM(s) = \Delta(s)TA^{-1}$. We note that this "diagonalization" of $M(s)$ is due to Datskovsky and Wright [2, Proposition 4.1]. Recently, Ohno, Wakatsuki, and the first author [17, 18] classified all $\mathrm{SL}_2(\mathbb{Z})$-invariant lattices L in $V_{\mathbb{Z}}$ and showed that the associated zeta function $\xi(s, L, \mathrm{SL}_2(\mathbb{Z}))$ for each L satisfies a functional equation in a self-dual form as in Theorem 7.2. In this section we establish a similar formula for the "N-divisible zeta function" when N is square free. We also state residue formulas that we will prove in Section 8.

In this section we assume that N is a square free integer. Let $f_N \in C(V_N, \mathbf{1})$ be the characteristic function of $\{a \in V_N \mid P(a) = 0\}$. This definition agrees with Definition 5.3, and $f_N = \prod_{p|N} f_p$.

Definition 7.3 We define the *N-divisible zeta function*

$$\xi_N(s) := \xi(s, f_N) = \sum_{a \in V_N, P(a)=0} \xi(s, a).$$

This function counts the $V_{\mathbb{Z}}$-orbits whose discriminants are multiples of N, and we study its analytic properties.

We first describe the residues; these formulas follow from Proposition 8.6 and Corollary 8.14.

Proposition 7.4 *We have*

$$\operatorname{Res}_{s=1} \xi_N(s) = \prod_{p|N} \Big(\frac{1}{p} + \frac{1}{p^2} - \frac{1}{p^3} \Big) \cdot (\alpha + \beta),$$

$$\operatorname{Res}_{s=5/6} \xi_N(s) = \prod_{p|N} \Big(\frac{1}{p} + \frac{1}{p^{4/3}} - \frac{1}{p^{7/3}} \Big) \cdot \zeta(\frac{1}{3})\gamma,$$

where α, β and γ are as in Definition 8.3.

We next prove the functional equation. For a square free integer m, we put

$$\xi_m^*(s) := \sum_{b \in V_m^*, P^*(b)=0} \xi^*(s, b).$$

Proposition 7.5 *If N is square free, we have*

$$\xi_N(1-s) = N^{4s-3} M(s) \sum_{m_1 m_2 m_3 = N} \mu(m_1) m_2 m_3^{2-4s} \xi_{m_2}^*(s).$$

Proof By Theorem 4.3 and Proposition 6.1, we have

$$\xi_N(1-s) = N^{4s} M(s) \sum_{b \in V_N^*} \widehat{f_N}(b) \xi^*(s, b)$$

https://doi.org/10.4153/CJM-2013-027-0 Published online by Cambridge University Press

where $\widehat{f_N}(b)$ is multiplicative in N, and for a prime p is equal to $p^{-1}+p^{-2}-p^{-3}$ if $b=0$, $p^{-2}-p^{-3}$ if $b\neq 0$ but $P^*(b)=0$, and $-p^{-3}$ otherwise. We rewrite $\widehat{f_p}(b)$ as

$$\widehat{f_p}(b) = -p^{-3} + g_{p,2}(b)p^{-2} + g_{p,3}(b)p^{-1},$$

where $g_{p,3}(b)$ is the characteristic function of $b=0$, and $g_{p,2}(b)$ is the characteristic function of those b with $P^*(b)=0$. Then we have

$$\begin{aligned}
\xi_N(1-s) &= N^{4s}M(s)\sum_{b\in V_N^*}\prod_{p|N}\bigl(-p^{-3}+g_{p,2}(b)p^{-2}+g_{p,3}(b)p^{-1}\bigr)\,\xi^*(s,b)\\
&= N^{4s}M(s)\sum_{m_1m_2m_3=N}\mu(m_1)m_1^{-3}m_2^{-2}m_3^{-1}\Bigl(\sum_{\substack{b\in V_N^*\\ m_2|P^*(b),b\in m_3V_N^*}}\xi^*(s,b)\Bigr)\\
&= N^{4s-3}M(s)\sum_{m_1m_2m_3=N}\mu(m_1)m_2m_3^2\Bigl(m_3^{-4s}\sum_{\substack{b\in V_N^*\\ m_2|P^*(b)}}\xi^*(s,b)\Bigr),
\end{aligned}$$

as desired. ■

Let φ and μ be the Euler function and Möbius function, respectively. Similarly to [17], we find a functional equation in self dual form for certain linear combinations of zeta functions.

Theorem 7.6 *For a square free integer N, let*

$$\theta_N(s) := \sum_{m|N}\mu(m)m\xi_m(s).$$

Then

$$\operatorname{Res}_{s=1}\theta_N(s) = \mu(N)\frac{\varphi(N)}{N^2}\cdot(\alpha+\beta),\qquad \operatorname{Res}_{s=5/6}\theta_N(s) = \mu(N)\frac{\varphi(N)\zeta(1/3)}{N^{4/3}}\cdot\gamma,$$

and

$$N^{2(1-s)}\Delta(1-s)\cdot T\cdot\theta_N(1-s) = N^{2s}\Delta(s)\cdot T\cdot\theta_N(s).$$

Proof By Proposition 7.4,

$$\operatorname{Res}_{s=1} m\xi_m(s) = \prod_{p|m}\Bigl(1+\frac{1-p^{-1}}{p}\Bigr)\cdot(\alpha+\beta),$$

$$\operatorname{Res}_{s=5/6} m\xi_m(s) = \prod_{p|m}\Bigl(1+\frac{1-p^{-1}}{p^{1/3}}\Bigr)\cdot\zeta(1/3)\gamma.$$

Since

$$\prod_{p|N}(1-a_p) = \sum_{m|N}\mu(m)\prod_{p|m}a_p$$

for any a_p and $\prod_{p|N}(1-p^{-1}) = \varphi(N)/N$, the residue formulas follow. We consider the functional equation. By Proposition 7.5,

$$\begin{aligned} M(s)^{-1}\cdot\theta_N(1-s) &= M(s)^{-1}\sum_{m|N}\mu(m)m\xi_m(1-s)\\ &= \sum_{m|N}\mu(m)m^{4s-2}\sum_{m_1m_2m_3=m}\mu(m_1)m_2m_3^{2-4s}\xi^*_{m_2}(s)\\ &= \sum_{m_1m_2m_3m_4=N}\mu(m_2m_3)m_2(m_1m_2)^{4s-2}\xi^*_{m_2}(s)\\ &= \sum_{m_1m_2|N}\mu(m_2)(m_1m_2)^{4s-2}m_2\xi^*_{m_2}(s)\sum_{m_3m_4=\frac{N}{m_1m_2}}\mu(m_3). \end{aligned}$$

By the Möbius inversion formula, $\sum_{m_3m_4=\frac{N}{m_1m_2}}\mu(m_3)$ is 1 if $N=m_1m_2$ and 0 otherwise. Hence

$$M(s)^{-1}\cdot\theta_N(1-s) = N^{4s-2}\sum_{m|N}\mu(m)m\xi^*_m(s).$$

By the Ohno–Nakagawa formula, we have $\xi^*_m(s) = A\cdot\xi_m(s)$ for any m. Hence

$$M(s)^{-1}\cdot\theta_N(1-s) = N^{4s-2}A\cdot\theta_N(s).$$

Since $\Delta(1-s)TM(s) = \Delta(s)TA^{-1}$, we have the formula. ■

8 Computation of Residues

In this section we compute the residues of our orbital L-functions and related zeta functions. We start by showing that for a suitable choice Φ_a of test function, the adelic Shintani zeta function studied by Wright [29] gives an integral expression for $\xi(s,\chi,a)$. Hence its residues are described in terms of certain integrals that have Euler products. The local analysis is carried out in later subsections. We note that a number of the results of this section are already obtained in the extensive work of Datskovsky–Wright [2], and we follow their approach to give refinements of their results.

Recall that $\xi(s,\chi,a)$ is a vector consisting of two Dirichlet series. When we talk about the analytic properties of $\xi(s,\chi,a)$, we mean so entrywise. The locations of the poles coincide for the two series, so we hope our meaning is clear. In particular, for $z_0\in\mathbb{C}$, we denote by $\operatorname{Res}_{z=z_0}\xi(s,\chi,a)$ the column vector of residues of these Dirichlet series at $z=z_0$.

We fix some notation for adelic analysis. Let $\mathbb{R}_+^\times = \{t\in\mathbb{R}\mid t>0\}$ and $\mathbb{C}_1^\times = \{z\in\mathbb{C}^\times\mid |z|=1\}$. For $t\in\mathbb{Q}_p^\times$, let $\operatorname{ord}_p(t)$ be the unique integer m satisfying $t\in p^m\mathbb{Z}_p^\times$. Let $|\cdot|_p\colon\mathbb{Q}_p^\times\to\mathbb{R}_+^\times$ be the normalized absolute value, hence $|t|_p = p^{-\operatorname{ord}_p(t)}$. We normalize the Haar measure du (resp. $d^\times t$) on $\mathbb{Q}_p$ (resp. $\mathbb{Q}_p^\times$) so that the volume of $\mathbb{Z}_p$ (resp. of $\mathbb{Z}_p^\times$) is 1. We put $\widehat{\mathbb{Z}} := \prod_{p:\text{finite}}\mathbb{Z}_p$, so that $\widehat{\mathbb{Z}}^\times = \prod_{p:\text{finite}}\mathbb{Z}_p^\times$. As usual, let $\mathbb{A}_{\mathrm{f}} := \widehat{\mathbb{Z}}\otimes\mathbb{Q}$ and $\mathbb{A} = \mathbb{A}_{\mathrm{f}}\times\mathbb{R}$. Let $\mathscr{S}(V_{\mathbb{R}}), \mathscr{S}(V_{\mathbb{Q}_p}), \mathscr{S}(V_{\mathbb{A}_{\mathrm{f}}}), \mathscr{S}(V_{\mathbb{A}})$ be the

https://doi.org/10.4153/CJM-2013-027-0 Published online by Cambridge University Press

space of Schwarz–Bruhat functions on each of the indicated domains. For a Dirichlet character χ, let $\delta(\chi)$ be 1 if χ is trivial and 0 otherwise.

For the rest of this section we fix a (primitive) Dirichlet χ of conductor m. We introduce notation related to χ. The usual L-function and the local L-factors for χ are defined by

$$L(s,\chi) := \prod_p L_p(s,\chi), \quad L_p(s,\chi) := \begin{cases} 1 & p \mid m, \\ \bigl(1-\chi(p)/p^s\bigr)^{-1} & p \nmid m. \end{cases}$$

Recall the direct product decomposition $\mathbb{A}^\times = \mathbb{R}_+^\times \cdot \widehat{\mathbb{Z}}^\times \cdot \mathbb{Q}^\times$. We lift χ to an idele class character $\tilde{\chi}\colon \mathbb{A}^\times/\mathbb{Q}^\times \to \mathbb{C}_1^\times$ by using the compositum

$$\tilde{\chi}\colon \mathbb{A}^\times = \mathbb{R}_+^\times \cdot \widehat{\mathbb{Z}}^\times \cdot \mathbb{Q}^\times \twoheadrightarrow \widehat{\mathbb{Z}}^\times \twoheadrightarrow (\widehat{\mathbb{Z}}/m\widehat{\mathbb{Z}})^\times \cong (\mathbb{Z}/m\mathbb{Z})^\times \xrightarrow{\chi} \mathbb{C}_1^\times.$$

Let $\tilde{\chi}_p$ be the local character on $\mathbb{Q}_p^\times$ induced from $\tilde{\chi}$:

$$\tilde{\chi}_p := \tilde{\chi}|_{\mathbb{Q}_p^\times} \colon \mathbb{Q}_p^\times \to \mathbb{C}_1^\times.$$

Let $m = \prod p^{c_p}$. Then χ has a unique decomposition, $\chi = \prod \chi_p$, corresponding to the decomposition $(\mathbb{Z}/m\mathbb{Z})^\times = \prod (\mathbb{Z}/p^{c_p}\mathbb{Z})^\times$, where χ_p is a primitive character on $(\mathbb{Z}/p^{c_p}\mathbb{Z})^\times$. (If $p \nmid m$, this means $c_p = 0$ and χ_p is the trivial character.) We put $\chi'_p := \prod_{p' \neq p} \chi_{p'}$. This is a primitive character of conductor m/p^{c_p} that is coprime to p. Hence $\chi'_p(p)$ makes sense.

Let us describe $\tilde{\chi}_p$ explicitly in terms of χ. Since $\mathbb{Q}_p^\times = \mathbb{Z}_p^\times \times p^{\mathbb{Z}}$, it is enough to describe $\tilde{\chi}_p|_{\mathbb{Z}_p^\times}$ and $\tilde{\chi}_p(p)$, and by definition these are given as follows.

Lemma 8.1 *The character $\tilde{\chi}_p$ restricted to $\mathbb{Z}_p^\times$ agrees with the pullback of χ_p via the canonical surjection $\mathbb{Z}_p^\times \to (\mathbb{Z}_p/p^{c_p}\mathbb{Z}_p)^\times \cong (\mathbb{Z}/p^{c_p}\mathbb{Z})^\times$. Also we have $\tilde{\chi}_p(p) = \chi'_p(p)^{-1}$.*

If $p \nmid m$, then $\chi'_p = \chi_p$ and so $\tilde{\chi}_p(p) = \chi(p)^{-1}$.

8.1 An Integral Expression for Orbital L-functions

We now return to the analysis of zeta functions. In this subsection we fix a positive integer N that is a multiple of m, and we also fix $a \in V_N$. Let $V'_{\mathbb{Q}} := \{x \in V_{\mathbb{Q}} \mid P(x) \neq 0\}$. For $\Phi \in \mathscr{S}(V_{\mathbb{A}})$, Wright [29] introduced the global zeta function

$$Z(\Phi,s,\chi) := \int_{G_{\mathbb{A}}/G_{\mathbb{Q}}} |\det g|_{\mathbb{A}}^{2s} \tilde{\chi}(\det g) \sum_{x \in V'_{\mathbb{Q}}} \Phi(gx)\, dg.$$

Here dg is a Haar measure on $G_{\mathbb{A}}$ normalized as in [29, p. 514].

Let $\Phi_a = \Phi_\infty \times \Phi_{\mathrm{f},a}$ where $\Phi_\infty \in \mathscr{S}(V_{\mathbb{R}})$ is arbitrary and $\Phi_{\mathrm{f},a} \in \mathscr{S}(V_{\mathbb{A}_{\mathrm{f}}})$ is the characteristic function of $\tilde{a} + NV_{\widehat{\mathbb{Z}}} \subset V_{\widehat{\mathbb{Z}}}$, where $\tilde{a}$ is a lift of a under the surjection $V_{\widehat{\mathbb{Z}}} \twoheadrightarrow V_{\widehat{\mathbb{Z}}/N\widehat{\mathbb{Z}}} \cong V_N$. Let $G_{\mathbb{R}}^+ := \{g \in G_{\mathbb{R}} = \mathrm{GL}_2(\mathbb{R}) \mid \det g > 0\}$ with Haar measure dg_∞ normalized as in [29], and let $\Gamma_\infty(\Phi_\infty, s)$ be the local zeta function defined in (4.1).

Proposition 8.2 *We have*

$$Z(\Phi_a, s, \chi) = |G_N|^{-1}\Gamma_\infty(\Phi_\infty, s)\xi(s, \chi^{-1}, a).$$

If $\chi = \mathbf{1}$, $\xi(s, \chi, a)$ is holomorphic except for simple poles at $s = 1$ and $5/6$. If $\chi \neq \mathbf{1}$ and $\chi^3 = \mathbf{1}$, then $\xi(s, \chi, a)$ is holomorphic except for a simple pole at $s = 5/6$; otherwise it is entire.

Proof Let $\mathcal{K}_N := \ker(G_{\widehat{\mathbb{Z}}} \to G_{\mathbb{Z}/N\mathbb{Z}})$. This is an open subgroup of $G_{\mathbb{A}_{\mathrm{f}}}$. Note that $G_{\mathbb{R}}^+\mathcal{K}_N \cap G_{\mathbb{Q}} = \Gamma(N)$. For $t \in T_N \subset G_N = G_{\mathbb{Z}/N\mathbb{Z}}$, we denote by $\tilde{t} \in G_{\widehat{\mathbb{Z}}}$ its (arbitrary) lift. Then $\mathcal{K}_N\tilde{t}$ does not depend on the choice of $\tilde{t}$. By strong approximation for SL_2, it is known (see, *e.g.*, [9]) that $G_{\mathbb{A}} = G_{\mathbb{R}}^+\mathcal{K}G_{\mathbb{Q}}$ for any subgroup $\mathcal{K} \subset G_{\widehat{\mathbb{Z}}}$ such that the determinant map is surjective onto $\widehat{\mathbb{Z}}^\times$. One checks that the union $\bigcup_{t\in T_N} \mathcal{K}_N\tilde{t}$ is such a $\mathcal{K}$, and it is not difficult to check that the union $G_{\mathbb{A}} = \bigcup_{t\in T_N} G_{\mathbb{R}}^+\mathcal{K}_N\tilde{t}G_{\mathbb{Q}}$ is disjoint.

Corresponding to this decomposition, for each $t \in T_N$ we put

$$Z_t(\Phi_a, s, \widetilde{\chi}) := \int_{G_{\mathbb{R}}^+\mathcal{K}_N\tilde{t}G_{\mathbb{Q}}/G_{\mathbb{Q}}} |\det g|_{\mathbb{A}}^{2s}\widetilde{\chi}(\det g) \sum_{x\in V'_{\mathbb{Q}}} \Phi_a(gx)\, dg.$$

Let dg_{f} be the Haar measure on $G_{\mathbb{A}_{\mathrm{f}}}$ normalized so that the volume of $G_{\widehat{\mathbb{Z}}}$ is 1. Then $dg = dg_\infty dg_{\mathrm{f}}$. For this integral, we have the following process of modification:

$$\begin{aligned}
Z_t(\Phi_a, s, \widetilde{\chi}) &= \int_{G_{\mathbb{R}}^+\mathcal{K}_N G_{\mathbb{Q}}/G_{\mathbb{Q}}} |\det \tilde{t}g|_{\mathbb{A}}^{2s}\widetilde{\chi}(\det \tilde{t}g) \sum_{x\in V'_{\mathbb{Q}}} \Phi_a(\tilde{t}gx)\, dg \\
&= \chi(\det t) \int_{G_{\mathbb{R}}^+\mathcal{K}_N G_{\mathbb{Q}}/G_{\mathbb{Q}}} |\det g|_{\mathbb{A}}^{2s}\widetilde{\chi}(\det g) \sum_{x\in V'_{\mathbb{Q}}} \Phi_{t^{-1}a}(gx)\, dg \\
&= \chi(\det t) \int_{G_{\mathbb{R}}^+\mathcal{K}_N/G_{\mathbb{R}}^+\mathcal{K}_N\cap G_{\mathbb{Q}}} |\det g|_{\mathbb{A}}^{2s}\widetilde{\chi}(\det g) \sum_{x\in V'_{\mathbb{Q}}} \Phi_{t^{-1}a}(gx)\, dg \\
&= \chi(\det t) \int_{G_{\mathbb{R}}^+/\Gamma(N)\times\mathcal{K}_N} |\det g_\infty|_\infty^{2s} \sum_{x\in V'_{\mathbb{Q}}} \Phi_\infty(g_\infty x)\Phi_{\mathrm{f},t^{-1}a}(g_{\mathrm{f}}x)\, dg_\infty dg_{\mathrm{f}} \\
&= \chi(\det t) \int_{\mathcal{K}_N} dg_{\mathrm{f}} \int_{G_{\mathbb{R}}^+/\Gamma(N)} |\det g_\infty|_\infty^{2s} \sum_{x\in V'_{\mathbb{Q}}} \Phi_\infty(g_\infty x)\Phi_{\mathrm{f},t^{-1}a}(x)\, dg_\infty \\
&= \frac{\chi(\det t)}{|G_N|} \int_{G_{\mathbb{R}}^+/\Gamma(N)} |\det g_\infty|_\infty^{2s} \sum_{x\in V'_{\mathbb{Q}}\cap(t^{-1}a+NV_{\widehat{\mathbb{Z}}})} \Phi_\infty(g_\infty x)\, dg_\infty \\
&= \frac{\chi(\det t)}{|T_N|} \frac{1}{[\Gamma(1):\Gamma(N)]} \int_{G_{\mathbb{R}}^+/\Gamma(N)} |\det g_\infty|_\infty^{2s} \sum_{x\in V'_{\mathbb{Q}}\cap(t^{-1}a+NV_{\mathbb{Z}})} \Phi_\infty(g_\infty x)\, dg_\infty \\
&= \frac{\chi(\det t)}{|T_N|}\Gamma_\infty(\Phi_\infty, s)\xi(s, t^{-1}a).
\end{aligned}$$

By (3.1), the formula is obtained by summing this formula over all $t \in T_N$. We now explain the process of modifications above.

The first equality follows from $G_{\mathbb{R}}^{+}\mathcal{K}_N\tilde{t} = \tilde{t}G_{\mathbb{R}}^{+}\mathcal{K}_N$. Since $\widetilde{\chi}$ and $\tilde{t}$ are both lifts, $\widetilde{\chi}(\det\tilde{t}) = \chi(\det t)$ and $\tilde{t} \in G_{\widehat{\mathbb{Z}}}$ implies $|\det\tilde{t}|_{\mathbb{A}} = 1$. Also by definition $\Phi_a(\tilde{t}x) = \Phi_{t^{-1}a}(x)$. Hence the second equality follows. The third equality is obvious. Since $|\det(\mathcal{K}_N)|_{\mathbb{A}} = \widetilde{\chi}(\det(G_{\mathbb{R}}^{+}\mathcal{K}_N)) = 1$, we have the fourth. The fifth equality is because $\Phi_{\mathrm{f},t^{-1}a}$ is $\mathcal{K}_N$-invariant. Since $\int_{\mathcal{K}_N} dg_{\mathrm{f}} = [G_{\widehat{\mathbb{Z}}} : \mathcal{K}_N]^{-1} \cdot \int_{G_{\widehat{\mathbb{Z}}}} dg_{\mathrm{f}} = |G_N|^{-1}$ and $\Phi_{\mathrm{f},t^{-1}a} \in \mathscr{S}(V_{\mathbb{A}_f})$ is the characteristic function of $t^{-1}a + NV_{\widehat{\mathbb{Z}}}$, we have the sixth equality. By $V_{\mathbb{Q}} \cap (t^{-1}a + NV_{\widehat{\mathbb{Z}}}) = t^{-1}a + NV_{\mathbb{Z}}$, we have the seventh. For the last equality, we divide $V'_{\mathbb{Q}} \cap (t^{-1}a + NV_{\widehat{\mathbb{Z}}})$ into its $\Gamma(N)$-orbits and consider each integral separately. Then this equality follows from the unfolding method. Note that

$$\int_{G_{\mathbb{R}}^{+}/\Gamma(N)_x} |\det g_\infty|_\infty^{2s}\,\Phi_\infty(g_\infty x)\,dg_\infty = \frac{|\Gamma(N)_x|^{-1}}{|P(x)|^s}\int_{G_{\mathbb{R}}^{+}} |P(g_\infty x)|_\infty^{s}\,\Phi_\infty(g_\infty x)\,dg_\infty.$$

The second statement of the proposition follows from Wright's study of $Z(\Phi, s, \omega)$ in [29], combined with the standard argument treating $\Gamma_\infty(\Phi_\infty, s)$. For this, see the proof of [25, Theorem 2.1], for example. ■

8.2 Residues as Integrals

We now start to compute the residues of $\xi(s, \chi, a)$. We introduce the following constants.

Definition 8.3 We define

$$\alpha := \frac{\pi^2}{36}\begin{pmatrix}1\\3\end{pmatrix}, \quad \beta := \frac{\pi^2}{12}\begin{pmatrix}1\\1\end{pmatrix}, \quad \gamma := \frac{2\pi^2}{9\Gamma(2/3)^3}\begin{pmatrix}1\\\sqrt{3}\end{pmatrix}. \tag{8.1}$$

Shintani [25] proved the following.

Theorem 8.4 (Shintani) *The residues of* $\xi(s)$ *are*

$$\mathrm{Res}_{s=1}\,\xi(s) = \alpha + \beta, \qquad \mathrm{Res}_{s=5/6}\,\xi(s) = \zeta(1/3)\gamma.$$

We define an averaging operator $\mathcal{M}_{\mathrm{f},\chi}$ on $\mathscr{S}(V_{\mathbb{A}_{\mathrm{f}}})$ by

$$\mathcal{M}_{\mathrm{f},\chi}\Phi_{\mathrm{f}}(x) = \int_{G_{\widehat{\mathbb{Z}}}} \tilde{\chi}(\det g_{\mathrm{f}})\Phi_{\mathrm{f}}(g_{\mathrm{f}}x)\,dg_{\mathrm{f}} \quad \big(\Phi_{\mathrm{f}} \in \mathscr{S}(V_{\mathbb{A}_{\mathrm{f}}})\big). \tag{8.2}$$

If χ is trivial then we write $\mathcal{M}_{\mathrm{f}}$ as well. For $\Phi_{\mathrm{f}} \in \mathscr{S}(V_{\mathbb{A}_{\mathrm{f}}})$, let

$$\mathcal{B}_{\mathrm{f}}(\Phi_{\mathrm{f}}) := \zeta(2)^{-1}\int_{\mathbb{A}_{\mathrm{f}}^{\times}\times\mathbb{A}_{\mathrm{f}}^{2}} |t|_{\mathrm{f}}^{2}\mathcal{M}_{\mathrm{f}}\Phi_{\mathrm{f}}(0, t, u_3, u_4)\,d^{\times}t\,du_3du_4,$$

$$\mathcal{C}_{\mathrm{f}}(\Phi_{\mathrm{f}}, \chi, s) := \int_{\mathbb{A}_{\mathrm{f}}^{\times}\times\mathbb{A}_{\mathrm{f}}^{3}} \tilde{\chi}(t)|t|_{\mathrm{f}}^{s}\mathcal{M}_{\mathrm{f},\chi^{-1}}\Phi_{\mathrm{f}}(t, u_2, u_3, u_4)\,d^{\times}t\,du_2du_3du_4,$$

$$\mathcal{C}_{\mathrm{f}}(\Phi_{\mathrm{f}}, \chi) := \mathcal{C}_{\mathrm{f}}(\Phi_{\mathrm{f}}, \chi, 1/3).$$

https://doi.org/10.4153/CJM-2013-027-0 Published online by Cambridge University Press

We note that $\mathcal{C}_{\mathrm{f}}(\Phi_{\mathrm{f}}, \chi, s)$ is defined for $\Re(s) \leq 1$ by analytic continuation. Then for $a \in V_N$, by [29, Theorem 6.1] and Proposition 8.2 (see [2, pp. 69–70] also), we have

$$\begin{aligned} \operatorname{Res}_{s=1} \frac{\xi(s,\chi,a)}{|G_N|} &= \delta(\chi)\Big(\frac{1}{N^4}\alpha + \mathcal{B}_{\mathrm{f}}(\Phi_{\mathrm{f},a})\beta\Big), \\ \operatorname{Res}_{s=5/6} \frac{\xi(s,\chi,a)}{|G_N|} &= \delta(\chi^3)\mathcal{C}_{\mathrm{f}}(\Phi_{\mathrm{f},a},\chi)\gamma. \end{aligned} \tag{8.3}$$

Hence we will compute these values explicitly. We define a local averaging operator $\mathcal{M}_{p,\chi}$ on $\mathcal{S}(V_{\mathbb{Q}_p})$ similarly to (8.2):

$$\mathcal{M}_{p,\chi}\Phi_p(x) = \int_{G_{\mathbb{Z}_p}} \tilde{\chi}_p(\det g_p)\Phi_p(g_p x)\, dg_p \quad \big(\Phi_p \in \mathcal{S}(V_{\mathbb{Q}_p})\big). \tag{8.4}$$

Here we normalize the measure dg_p on $G_{\mathbb{Q}_p}$ such that the volume of $G_{\mathbb{Z}_p}$ is 1. For $a \in V_{p^e}$ or $a \in V_{\mathbb{Z}_p}$ and $e \geq 0$, let $\Phi_{p,a} \in \mathcal{S}(V_{\mathbb{Z}_p})$ be the characteristic function of $a + p^e V_{\mathbb{Z}_p}$. We put

$$\mathcal{B}_{p^e}(a) := p^{4e}(1-p^{-2}) \int_{\mathbb{Q}_p^\times \times \mathbb{Q}_p^2} |t|_p^2 \mathcal{M}_p \Phi_{p,a}(0,t,u_3,u_4)\, d^\times t\, du_3 du_4, \tag{8.5}$$

$$\begin{aligned} \mathcal{C}_{p^e}(a,\chi) := {}& p^{4e} L_p\Big(\frac{1}{3},\chi^{-1}\Big)^{-1} \\ & \times \int_{\mathbb{Q}_p^\times \times \mathbb{Q}_p^3} \tilde{\chi}_p(t)|t|_p^{1/3} \mathcal{M}_{p,\chi^{-1}} \Phi_{p,a}(t,u_2,u_3,u_4)\, d^\times t\, du_2 du_3 du_4. \end{aligned} \tag{8.6}$$

Note that these are 1 if $e = 0$ and χ is unramified at p. Let $N = \prod p^{e_p}$ be the prime decomposition of N. For $a \in V_N$, we define

$$\mathcal{B}_N(a) := \prod_{p|N} \mathcal{B}_{p^{e_p}}(a_p), \qquad \mathcal{C}_N(a,\chi) := \prod_{p|N} \mathcal{C}_{p^{e_p}}(a_p,\chi), \tag{8.7}$$

where $a_p = (a \bmod p^e) \in V_{p^e}$. Then

$$\mathcal{B}_{\mathrm{f}}(\Phi_{\mathrm{f},a}) = N^{-4}\mathcal{B}_N(a), \qquad \mathcal{C}_{\mathrm{f}}(\Phi_{\mathrm{f},a},\chi) = N^{-4}\mathcal{C}_N(a,\chi)L(1/3,\chi^{-1}).$$

Hence by (8.3) we have the following generalization of Theorem 8.4.

Theorem 8.5 *We have*

$$\begin{aligned} \operatorname{Res}_{s=1} \frac{\xi(s,\chi,a)}{|G_N|} &= \delta(\chi)\Big(\frac{1}{N^4}\alpha + \frac{\mathcal{B}_N(a)}{N^4}\beta\Big), \\ \operatorname{Res}_{s=5/6} \frac{\xi(s,\chi,a)}{|G_N|} &= \delta(\chi^3)\frac{\mathcal{C}_N(a,\chi)}{N^4} L\Big(\frac{1}{3},\chi^{-1}\Big)\gamma. \end{aligned}$$

https://doi.org/10.4153/CJM-2013-027-0 Published online by Cambridge University Press

We now describe the residues of $\xi(s,f)$ for $f \in C(V_N,\chi)$. For $f \in C(V_N)$ we define

$$\mathcal{A}_N(f) = \sum_{a\in V_N} \frac{f(a)}{N^4}, \quad \mathcal{B}_N(f) = \sum_{a\in V_N} \frac{f(a)\mathcal{B}_N(a)}{N^4}, \tag{8.8}$$
$$\mathcal{C}_N(f,\chi) = \sum_{a\in V_N} \frac{f(a)\mathcal{C}_N(a,\chi)}{N^4}.$$

By definition these are multiplicative. By Theorem 8.5 and Proposition 4.7, we have the following.

Proposition 8.6 *Let $f \in C(V_N,\chi)$. Then*

$$\operatorname{Res}_{s=1} \xi(s,f) = \delta(\chi)\big(\mathcal{A}_N(f)\alpha + \mathcal{B}_N(f)\beta\big),$$
$$\operatorname{Res}_{s=5/6} \xi(s,f) = \delta(\chi^3)\mathcal{C}_N(f,\chi)L\Big(\frac{1}{3},\chi^{-1}\Big)\gamma.$$

Since $\xi(s,\chi,a)$ and $\xi(s,f)$ for $f \in C(V_N,\chi)$ are holomorphic if χ^3 is nontrivial, we assume that χ^3 is trivial for the rest of this section:

Assumption 8.7 The Dirichlet character χ is either trivial or cubic.

This of course implies that $\tilde{\chi}$, $\tilde{\chi}_p$, χ_p and χ'_p are trivial or cubic characters also.

8.3 Preliminaries for Explicit Computation

Now our aim is to compute $\mathcal{B}_{p^e}(a)$ and $\mathcal{C}_{p^e}(a,\chi)$ explicitly. In this subsection we prepare several lemmas for the computation. We fix a prime p and denote the p-part of the conductor of χ by p^c. We assume $e \geq c$.

We first describe some basic properties satisfied by $\mathcal{B}_{p^e}(a)$ and $\mathcal{C}_{p^e}(a,\chi)$.

Lemma 8.8

(i) *For $g \in G_{p^e}$,*

$$\mathcal{B}_{p^e}(ga) = \mathcal{B}_{p^e}(a), \quad \mathcal{C}_{p^e}(ga,\chi) = \chi_p(\det g)^{-1}\mathcal{C}_{p^e}(a,\chi). \tag{8.9}$$

(ii) *If χ is unramified at p, then*

$$p^{-4e}\sum_{a\in V_{p^e}} \mathcal{B}_{p^e}(a) = 1, \quad p^{-4e}\sum_{a\in V_{p^e}} \mathcal{C}_{p^e}(a,\chi) = 1. \tag{8.10}$$

(iii) *Let $m \leq e-c$. For $a \in V_{p^{e-m}}$, we regard $p^m a \in V_{p^e}$. Then*

$$\mathcal{B}_{p^e}(p^m a) = \mathcal{B}_{p^{e-m}}(a), \quad \mathcal{C}_{p^e}(p^m a,\chi) = \tilde{\chi}_p(p)^m p^{2m/3}\mathcal{C}_{p^{e-m}}(a,\chi).$$

https://doi.org/10.4153/CJM-2013-027-0 Published online by Cambridge University Press

Proof These immediately follow from the definitions (8.5) and (8.6). For (ii), we note that if χ is unramified, $\sum_{a\in V_{p^e}} \mathcal{M}_{p,\chi^{-1}}\Phi_{p,a} = \sum_{a\in V_{p^e}} \Phi_{p,a}$ is the characteristic function of $V_{\mathbb{Z}_p}$. ■

Lemma 8.9 *Let $a \in V_{p^e}$. Assume that $G_{p^e}a + p^eV_{\mathbb{Z}_p}$ is a single $G_{\mathbb{Z}_p}$-orbit and that $\chi_p \circ \det$ is trivial on $G_{p^e,a}$. Then*

$$\mathcal{B}_{p^e}(a) = \mathcal{B}_{p^{e'}}(a'), \quad \mathcal{C}_{p^e}(a,\chi) = \mathcal{C}_{p^{e'}}(a',\chi),$$

for all $e' \geq e$ and $a' \in V_{p^{e'}}$ such that $a' \bmod p^e = a$.

Proof By (8.5) and (8.6), it is enough to show that

$$p^{4e}\mathcal{M}_{p,\chi^{-1}}\Phi_{p,a} = p^{4e'}\mathcal{M}_{p,\chi^{-1}}\Phi_{p,a'}.$$

Let $\tilde{a} \in V_{\mathbb{Z}_p}$ be a lift of a. Then by assumption $G_{p^e}a + p^eV_{\mathbb{Z}_p} = G_{\mathbb{Z}_p}\tilde{a}$. We claim that

$$\mathcal{M}_{p,\chi^{-1}}\Phi_{p,a}(x) = \begin{cases} |G_{p^e,a}||G_{p^e}|^{-1}\chi_p(\det k) & x = k\tilde{a}, k \in G_{\mathbb{Z}_p}, \\ 0 & x \notin G_{\mathbb{Z}_p}\tilde{a}. \end{cases} \tag{8.11}$$

By (8.4) and Lemma 8.1,

$$\mathcal{M}_{p,\chi^{-1}}\Phi_{p,a} = |G_{p^e}|^{-1}\sum_{g\in G_{p^e}} \chi_p(\det g)\Phi_{p,ga}. \tag{8.12}$$

Hence $\mathcal{M}_{p,\chi^{-1}}\Phi_{p,a}(x)$ vanishes unless $x \in G_{p^e}a + p^eV_{\mathbb{Z}_p}$. Let $x = k\tilde{a}, k \in G_{\mathbb{Z}_p}$. Then

$$\begin{aligned} \mathcal{M}_{p,\chi^{-1}}\Phi_{p,a}(k\tilde{a}) &= \chi_p(\det k)|G_{p^e}|^{-1}\sum_{g\in G_{p^e}} \chi_p(\det g)\Phi_{p,ga}(\tilde{a}) \\ &= \chi_p(\det k)|G_{p^e}|^{-1}\sum_{g\in G_{p^e,a}} \chi_p(\det g) = |G_{p^e,a}|\,|G_{p^e}|^{-1}\chi_p(\det k), \end{aligned}$$

where the last equality follows from the assumption and hence we have (8.11). Now it is enough to show that $|G_{p^{e'},a'}| = |G_{p^e,a}|$. For this, note the identity $G_{p^{e'}}a' + p^{e'}V_{\mathbb{Z}_p} = G_{p^e}a + p^eV_{\mathbb{Z}_p}$. These volumes are $p^{-4e'}|G_{p^{e'}}|/|G_{p^{e'},a'}|$ and $p^{-4e}|G_{p^e}|/|G_{p^e,a}|$ respectively, and hence we have $|G_{p^{e'},a'}| = |G_{p^e,a}|$. This finishes the proof. ■

To begin our computation of $\mathcal{B}_{p^e}(a)$ and $\mathcal{C}_{p^e}(a,\chi)$, we introduce the following notation.

Definition 8.10

(i) For $a = (a_1,a_2,a_3,a_4) \in V_{\mathbb{Z}_p}$, we define

$$\mathcal{B}'_{p^e}(a) := \begin{cases} 0 & a_1 \notin p^eV_{\mathbb{Z}_p}, \\ p^e(1+p^{-1})|a_2|_p & a_1 \in p^eV_{\mathbb{Z}_p}, a_2 \notin p^eV_{\mathbb{Z}_p}, \\ 1 & a_1, a_2 \in p^eV_{\mathbb{Z}_p}. \end{cases} \tag{8.13}$$

https://doi.org/10.4153/CJM-2013-027-0 Published online by Cambridge University Press

(ii) For $y \in \mathbb{Z}_p$, we define $I_{p^e}(y,\chi)$ as follows. If $c = 0$, we put

$$(8.14) \qquad I_{p^e}(y,\chi) := \begin{cases} p^{2e/3}\tilde{\chi}_p(p)^e & \operatorname{ord}_p(y) \geq e, \\ \dfrac{1-\tilde{\chi}_p(p)p^{-1/3}}{1-p^{-1}}\tilde{\chi}_p(y)|y|_p^{-2/3} & \operatorname{ord}_p(y) < e. \end{cases}$$

If $c \geq 1$, then we put

$$(8.15) \qquad I_{p^e}(y,\chi) := \begin{cases} (1-p^{-1})^{-1}\tilde{\chi}_p(y)|y|_p^{-2/3} & \operatorname{ord}_p(y) \leq e-c, \\ 0 & \operatorname{ord}_p(y) > e-c. \end{cases}$$

Since these quantities respectively depend only on $(a \bmod p^e) \in V_{p^e}$ or $(y \bmod p^e) \in \mathbb{Z}/p^e\mathbb{Z}$, we use the same notation for $a \in V_{p^e}$ or $y \in \mathbb{Z}/p^e\mathbb{Z}$ as well.

An easy computation shows that

$$(8.16) \qquad \mathcal{B}'_{p^e}(a) = p^{4e}(1-p^{-2})\int_{\mathbb{Q}_p^\times \times \mathbb{Q}_p^2} |t|_p^2 \Phi_{p,a}(0,t,u_3,u_4)\, d^\times t du_3 du_4,$$

$$(8.17) \qquad I_{p^e}(y,\chi) = p^e L_p(\frac{1}{3},\chi^{-1})^{-1}\int_{y+p^e\mathbb{Z}_p} \tilde{\chi}_p(t)|t|_p^{1/3}\, d^\times t.$$

Let $W = \mathrm{Aff}^2$ be the affine space of 2-dimensional row vectors. The G naturally acts on W from the right. We put $W_{p^e} := W_{\mathbb{Z}/p^e\mathbb{Z}} = (\mathbb{Z}/p^e\mathbb{Z})^2$ and

$$W'_{p^e} := \{(u,v) \in (\mathbb{Z}/p^e\mathbb{Z})^2 \mid u \in (\mathbb{Z}/p^e\mathbb{Z})^\times \text{ or } v \in (\mathbb{Z}/p^e\mathbb{Z})^\times\},$$

which is the G_{p^e}-orbit of $(1,0) \in W_{p^e}$. The following formulas for $\mathcal{B}_{p^e}(a)$ and $\mathcal{C}_{p^e}(a,\chi)$ hold.

Lemma 8.11

(i) *We have*

$$(8.18) \qquad \mathcal{B}_{p^e}(a) = |G_{p^e}|^{-1}\sum_{g \in G_{p^e}} \mathcal{B}'_{p^e}(ga).$$

(ii) *If χ is unramified at p* (i.e., *if $c = 0$*), *we have*

$$(8.19) \qquad \mathcal{C}_{p^e}(a,\chi) = |G_{p^e}|^{-1}\sum_{g \in G_{p^e}} I_{p^e}\big((ga)_1,\chi\big),$$

where $(ga)_1 \in \mathbb{Z}/p^e\mathbb{Z}$ is the first entry of $ga \in V_{p^e}$. Moreover for any χ,

$$(8.20) \qquad \mathcal{C}_{p^e}(a,\chi) = |W'_{p^e}|^{-1}\sum_{(u,v) \in W'_{p^e}} I_{p^e}\big(a(u,v),\chi\big).$$

Here we are plugging particular values of u and v into the binary cubic form a.

Proof (i) is obtained by (8.12) with χ_p trivial and (8.16). We consider (ii). Let

$$\mathcal{C}'_{p^e}(a,\chi) = p^{4e} L_p\Big(\frac{1}{3},\chi^{-1}\Big)^{-1}\int_{\mathbb{Q}_p^\times\times\mathbb{Q}_p^3}\tilde{\chi}_p(t)|t|_p^{1/3}\Phi_{p,a}(t,u_2,u_3,u_4)\,d^\times t du_2 du_3 du_4.$$

Then by (8.17) we have $\mathcal{C}'_{p^e}(a,\chi) = I_{p^e}(a_1,\chi)$. Hence by (8.12) we have

$$\begin{aligned}\mathcal{C}_{p^e}(a,\chi) &= |G_{p^e}|^{-1}\sum_{g\in G_{p^e}}\chi_p(\det g)\mathcal{C}'_{p^e}(ga,\chi)\\ &= |G_{p^e}|^{-1}\sum_{g\in G_{p^e}}\chi_p(\det g) I_{p^e}\big((ga)_1,\chi\big).\end{aligned}$$

In particular we have (8.19). Moreover, note that $(ga)_1 = (\det g)^{-1}a\big((1,0)g\big)$. Since $I_{p^e}(ty,\chi) = \chi_p(t)I_{p^e}(y,\chi)$ for $t\in(\mathbb{Z}/p^e\mathbb{Z})^\times$, we have

$$\mathcal{C}_{p^e}(a,\chi) = |G_{p^e}|^{-1}\sum_{g\in G_{p^e}} I_{p^e}\Big(a\big((1,0)g\big),\chi\Big) = |W'_{p^e}|^{-1}\sum_{(u,v)\in W'_{p^e}} I_{p^e}\big(a(u,v),\chi\big),$$

as desired. ■

8.4 Unramified Computation

In this subsection, we compute $\mathcal{B}_{p^e}(a)$ and $\mathcal{C}_{p^e}(a,\chi)$ for $p\nmid m$, that is, when χ is unramified at p. By (8.9), these depend only on the G_{p^e}-orbit of a. For $\mathcal{C}_{p^e}$, we list for convenience the values of $(1-p^{-2})\mathcal{C}_{p^e}(a,\chi)$.

When $e=1$, we have the following.

Proposition 8.12 *For $e=1$, $\mathcal{B}_p(a)$ and $(1-p^{-2})\mathcal{C}_p(a,\chi)$ are given by the following table.*

Type of a	$\mathcal{B}_p(a)$	$(1-p^{-2})\mathcal{C}_p(a,\chi)$
(3)	0	$(1-\chi(p)^2p^{-1/3})(1+p^{-1})$
(21)	1	$1-\chi(p)^2p^{-4/3}$
(111)	3	$(1-\chi(p)p^{-2/3})(1+\chi(p)^2p^{-1/3})^2$
(1^21)	$\frac{p+2}{p+1}$	$(1+\chi(p)^2p^{-1/3})(1-p^{-1})$
(1^3)	$\frac{1}{p+1}$	$1-\chi(p)^2p^{-4/3}$
(0)	1	$(1-p^{-2})\chi(p)^2p^{2/3}$.

Proof For the computation of $\mathcal{C}_{p^e}(a,\chi)$, it is convenient to put

$$x := \tilde{\chi}_p(p)p^{-1/3} = \chi(p)^2p^{-1/3}. \tag{8.21}$$

We note that since χ is a cubic character, $x^3 = p^{-1}$. Let

$$n_p^0(\sigma) = |\{a\in V_p(\sigma)\mid a_1\neq 0\}|,\quad n_p^1(\sigma) = |\{a\in V_p(\sigma)\mid a_1 = 0, a_2\neq 0\}|,$$

https://doi.org/10.4153/CJM-2013-027-0 Published online by Cambridge University Press

and

$$n_p^2(\sigma) = |\{a \in V_p(\sigma) \mid a_1 = a_2 = 0\}|.$$

Note that $\sum_{0 \leq i \leq 2} n_p^i(\sigma) = n_p(\sigma)$. Then for $a \in V_p(\sigma)$, by (8.18) and (8.13) (respectively by (8.19) and (8.14)), we have

$$\mathcal{B}_p(a) = \frac{n_p^0(\sigma)}{n_p(\sigma)} \cdot 0 + \frac{n_p^1(\sigma)}{n_p(\sigma)} \cdot p(1 + p^{-1}) + \frac{n_p^2(\sigma)}{n_p(\sigma)} \cdot 1,$$

$$\mathcal{C}_p(a, \chi) = \frac{n_p^0(\sigma)}{n_p(\sigma)} \cdot \frac{1 - x}{1 - x^3} + \frac{n_p^1(\sigma) + n_p^2(\sigma)}{n_p(\sigma)} \cdot \frac{1}{x^2}.$$

For $(\sigma) = (1^2 1)$, we see that the ratio $n_p^0(\sigma) : n_p^1(\sigma) : n_p^2(\sigma)$ is $(p - 1) : 1 : 1$ and hence

$$\mathcal{B}_p(a) = \frac{1}{p+1} \cdot p(1 + p^{-1}) + \frac{1}{p+1} \cdot 1 = \frac{p+2}{p+1},$$

$$\mathcal{C}_p(a, \chi) = \frac{p-1}{p+1} \cdot \frac{1-x}{1-x^3} + \frac{2}{p+1} \cdot \frac{1}{x^2} = \frac{1-x^3}{1+x^3} \cdot \frac{1-x}{1-x^3} + \frac{2x^3}{1+x^3} \cdot \frac{1}{x^2} = \frac{1+x}{1+x^3}.$$

The other cases are computed similarly. For $(\sigma) = (3), (21), (111), (1^2 1), (1^3)$, and (0), the ratio $n_p^0(\sigma){:}n_p^1(\sigma){:}n_p^2(\sigma)$ is $1{:}0{:}0$, $p{:}1{:}0$, $(p - 2){:}3{:}0$, $(p - 1){:}1{:}1$, $p{:}0{:}1$, and $0{:}0{:}1$ respectively, and the result follows. ■

We now consider the case $e \geq 2$. In connection with counting cubic fields, we mainly work for $a \in V_{p^e}^{\max}$, *i.e.*, of type $(3), (21), (111), (1^2 1_{\max})$, or $(1^3_{\max})$. This is a generalization of results of Datskovsky and Wright [2, Theorem 5.2 and Proposition 5.3] to unramified characters.

Proposition 8.13 *Let $e \geq 2$ and $a \in V_{p^e}^{\max}$. Then $\mathcal{B}_{p^e}(a)$ and $(1 - p^{-2})\mathcal{C}_{p^e}(a, \chi)$ are given by the following table.*

Type of a	$\mathcal{B}_{p^e}(a)$	$(1 - p^{-2})\mathcal{C}_{p^e}(a, \chi)$
(3)	0	$(1 - \chi(p)^2 p^{-1/3})(1 + p^{-1})$
(21)	1	$1 - \chi(p)^2 p^{-4/3}$
(111)	3	$(1 - \chi(p) p^{-2/3})(1 + \chi(p)^2 p^{-1/3})^2$
$(1^2 1_{\max})$	1	$(1 + \chi(p)^2 p^{-1/3})(1 - \chi(p) p^{-2/3})$
$(1^3_{\max})$	0	$1 - \chi(p) p^{-2/3}.$

In particular, they depend only on the orbital type of a.

Proof For $(\sigma) = (3), (21), (111)$, $V_{\mathbb{Z}_p}(\sigma)$ is a single $G_{\mathbb{Z}_p}$-orbit. Hence, if a is of one of these types, Lemma 8.9 reduces our calculation to the case $e = 1$, handled in Proposition 8.12. Therefore we consider the remaining cases. We put $R = \mathbb{Z}/p^e\mathbb{Z}$, and again write $x = \chi(p)^2 p^{-1/3}$ as in (8.21).

First let a be of type $(1^2 1_{\max})$. By Theorem 2.1, each orbit in $V_{p^e}(1^2 1_{\max})$ contains some $a = (0, 1, a_3, a_4)$ where $a_3 \in pR$ and $a_4 \in pR^\times$. Let $g = \left(\begin{smallmatrix} q & r \\ s & t \end{smallmatrix}\right) \in G_{p^e}$. Then

https://doi.org/10.4153/CJM-2013-027-0 Published online by Cambridge University Press

the first coordinate $(ga)_1$ of ga is $(ga)_1 = (\det g)^{-1} r(q^2 + a_3qr + a_4r^2)$. Since $a_3 \in pR$ and $a_4 \in pR^\times$,

$$\operatorname{ord}_p(q^2 + a_3qr + a_4r^2) = \begin{cases} 0 & \operatorname{ord}_p(q) = 0, \\ 1 & \operatorname{ord}_p(q) \geq 1. \end{cases}$$

Hence $(ga)_1 = 0$ if and only if $r = 0$, and in this case, $(ga)_2 = q \in R^\times$. Hence by (8.13), $\mathcal{B}'_{p^e}(ga) = p^e(1 + p^{-1})$ if $r = 0$ and 0 otherwise. Since

$$|\{g \in G_{p^e} \mid r = 0\}| = p^{3e}(1 - p^{-1})^2,$$

by (8.18) we have $\mathcal{B}_{p^e}(a) = 1$.

We compute $\mathcal{C}_{p^e}(a, \chi)$ using (8.20) and (8.14). Let $(u, v) \in W'_{p^e}$. Then $a(u, v) = v(u^2 + a_3uv + a_4v^2)$. If $u^2 + a_3uv + a_4v^2 \notin R^\times$, then $u \notin R^\times$ and hence $v \in R^\times$. Therefore,

$$\operatorname{ord}_p\bigl(a(u, v)\bigr) = \begin{cases} 1 & \operatorname{ord}_p(u) \geq 1, \\ \operatorname{ord}_p(v) & \operatorname{ord}_p(u) = 0. \end{cases}$$

The cardinalities of the subsets $\{\operatorname{ord}_p(u) \geq 1\}$, $\{\operatorname{ord}_p(u) = 0, \operatorname{ord}_p(v) = m < e\}$, and $\{v = 0\}$ of W'_{p^e} are $p^{2e-1}(1 - p^{-1})$, $p^{2e-m}(1 - p^{-1})^2$, and $p^e(1 - p^{-1})$, respectively. Hence by (8.20) and (8.14),

$$\mathcal{C}_{p^e}(a, \chi) = \frac{p^{2e-1}(1 - p^{-1})}{p^{2e}(1 - p^{-2})} \cdot \frac{(1 - x)px}{1 - p^{-1}} + \sum_{0 \leq m < e} \frac{p^{2e-m}(1 - p^{-1})^2}{p^{2e}(1 - p^{-2})} \cdot \frac{(1 - x)p^m x^m}{1 - p^{-1}} + \frac{p^e(1 - p^{-1})}{p^{2e}(1 - p^{-2})} \cdot p^e x^e = \frac{(1 + x)(1 - x^2)}{1 - p^{-2}}.$$

Next let a be of type $(1^3_{\max})$. We may assume $a = (1, a_2, a_3, a_4)$ where $a_2, a_3 \in pR$, $a_4 \in pR^\times$. Let $g \in G_{p^e}$ as above. Then $(ga)_1 = (\det g)^{-1}(q^3 + a_2q^2r + a_3qr^2 + a_4r^3)$. Since $a_2, a_3 \in pR$ and $a_4 \in pR^\times$, $\operatorname{ord}_p(q^3 + a_2q^2r + a_3qr^2 + a_4r^3) \leq 1$, and hence $(ga)_1$ is always nonzero. Hence $\mathcal{B}_{p^e}(a) = 0$. Also the order of $\operatorname{ord}_p\bigl(a(u, v)\bigr)$ is 0 if $\operatorname{ord}_p(u) = 0$ and 1 otherwise. Hence

$$\mathcal{C}_{p^e}(a, \chi) = \frac{p^{2e}(1 - p^{-1})}{p^{2e}(1 - p^{-2})} \cdot \frac{(1 - x)}{1 - p^{-1}} + \frac{p^{2e-1}(1 - p^{-1})}{p^{2e}(1 - p^{-2})} \cdot \frac{(1 - x)px}{1 - p^{-1}} = \frac{1 - x^2}{1 - p^{-2}}.$$

This finishes the proof. ■

As corollaries we have the following. Recall that we introduced $f_p \in C(V_p)$, $\Phi_p, \Phi'_p \in C(V_{p^2})$ in Definitions 5.3, 5.10 and the distributions $\mathcal{A}_N, \mathcal{B}_N, \mathcal{C}_N$ in (8.8).

Corollary 8.14 *Assume that χ is unramified at p. We have*

$$\mathcal{A}_p(f_p) = \mathcal{B}_p(f_p) = \frac{1}{p} + \frac{1}{p^2} - \frac{1}{p^3}, \quad \mathcal{C}_p(f_p, \chi) = \frac{1}{p} + \frac{\chi(p)^2}{p^{4/3}} - \frac{\chi(p)^2}{p^{7/3}}.$$

https://doi.org/10.4153/CJM-2013-027-0 Published online by Cambridge University Press

Proof Let x be as in (8.21). By Lemma 5.2 and Proposition 8.12, we have

$$\begin{aligned}\mathcal{A}_p(f_p) &= \frac{p(p^2-1)}{p^4} + \frac{(p^2-1)}{p^4} + \frac{1}{p^4} = \frac{1}{p} + \frac{1}{p^2} - \frac{1}{p^3},\\ \mathcal{B}_p(f_p) &= \frac{p(p^2-1)}{p^4}\frac{p+2}{p+1} + \frac{(p^2-1)}{p^4}\frac{1}{p+1} + \frac{1}{p^4} = \frac{1}{p} + \frac{1}{p^2} - \frac{1}{p^3},\\ \mathcal{C}_p(f_p,\chi) &= \frac{p(p^2-1)}{p^4}\frac{1+x}{1+x^3} + \frac{(p^2-1)}{p^4}\frac{1-x^4}{1-x^6} + \frac{1}{p^4}\frac{1}{x^2} = x^3+x^4-x^7,\end{aligned}$$

as desired. Again we note that $x^3 = p^{-1}$. ■

Corollary 8.15 *Assume that χ is unramified at p. Then*

$$\begin{aligned}\mathcal{A}_{p^2}(\Phi_p) &= \frac{1}{p^2} + \frac{1}{p^3} - \frac{1}{p^5}, & \mathcal{A}_{p^2}(\Phi'_p) &= \frac{2}{p^2} - \frac{1}{p^4},\\ \mathcal{B}_{p^2}(\Phi_p) &= \frac{2}{p^2} - \frac{1}{p^4}, & \mathcal{B}_{p^2}(\Phi'_p) &= \frac{2}{p^2} - \frac{1}{p^4},\\ \mathcal{C}_{p^2}(\Phi_p,\chi) &= \frac{\chi(p)}{p^{5/3}} + \frac{1}{p^2} - \frac{\chi(p)}{p^{11/3}}, & \mathcal{C}_{p^2}(\Phi'_p,\chi) &= \frac{\chi(p)}{p^{5/3}} + \frac{2}{p^2} - \frac{\chi(p)}{p^{8/3}} - \frac{1}{p^3}.\end{aligned}$$

Proof Let x be as in (8.21). By (8.10), we have

$$\mathcal{C}_{p^2}(\Phi_p,\chi) = p^{-8}\sum_{a\in V^{\mathrm{nm}}_{p^2}} \mathcal{C}_{p^2}(a,\chi) = 1 - p^{-8}\sum_{a\in V^{\max}_{p^2}} \mathcal{C}_{p^2}(a,\chi).$$

Hence by Lemma 5.6 and Proposition 8.13,

$$\begin{aligned}\mathcal{C}_{p^2}(\Phi_p,\chi) = 1 - &\frac{p^4(p^2-1)(p^2-p)}{p^8}\frac{1-x^2}{1-x^6}\\ &\times\Big(\frac{1-x+x^2}{3} + \frac{1+x^2}{2} + \frac{(1+x)^2}{6} + \frac{1+x}{p} + \frac{1}{p^2}\Big)\\ = 1 - &(1-x^3)(1-x^2)(1+x^2+x^3+x^4+x^6) = x^5+x^6-x^{11},\end{aligned}$$

and the result follows. By adding the contribution from $V_{p^2}(1^3_{\max})$, we also have

$$\mathcal{C}_{p^2}(\Phi'_p,\chi) = 1-(1-x^3)(1-x^2)(1+x^2+x^3+x^4) = x^5+2x^6-x^8-x^9,$$

as desired. The other formulas are proved similarly. ■

For its own interest, when $e = 2$ we compute $\mathcal{B}_{p^e}(a)$ and $\mathcal{C}_{p^2}(a,\chi)$ for $a \in V^{\mathrm{nm}}_{p^2}$ also. By Lemma 8.8 (iii), we may assume $a \in V^{\mathrm{nm}}_{p^2} \setminus pV_{p^2}$.

Proposition 8.16 *Let $a \in V_{p^2}$ be of type $(1^2 1_*)$, (1^3_*) or (1^3_{**}). Then $\mathcal{B}_{p^e}(a)$ and $(1-p^{-2})\mathcal{C}_{p^2}(a,\chi)$ are given in the following table.*

Type of a	$\mathcal{B}_{p^2}(a)$	$(1-p^{-2})\mathcal{C}_{p^2}(a,\chi)$
$(1^2 1_*)$	$\frac{2p+1}{p+1}$ $(p \neq 2)$ $\frac{4}{3}$ $(p=2, a=(0,1,0,0))$ $\frac{5}{3}$ $(p=2, a=(0,1,2,0))$	$\big(1+\chi(p)p^{1/3}\big)\,(1-p^{-1})$
(1^3_*)	1	$\big(1+\chi(p)p^{1/3}\big)\,\big(1-\chi(p)p^{-2/3}\big)$
(1^3_{**})	$\frac{1}{p+1}$	$\big(1+\chi(p)p^{1/3}\big)\,\big(1-\chi(p)p^{-2/3}\big)$.

Proof Since the proof is quite similar to Proposition 8.13, we shall be brief. Let $R = \mathbb{Z}/p^2\mathbb{Z}$.

Let $a = (0,1,a_2,0) \in \mathcal{D}_{p^2}(1^2 1_*)$. We first compute $\mathcal{C}_{p^2}(a,\chi)$. Let $(u,v) \in W'_{p^2}$. Then

$$\operatorname{ord}_p\big(a(u,v)\big) = \operatorname{ord}_p\big(uv(u+a_2 v)\big) = \begin{cases} 2 & u \in pR, \\ \operatorname{ord}_p(v) & u \in R^\times. \end{cases}$$

Hence by (8.20) and (8.14),

$$\begin{aligned}\mathcal{C}_{p^2}(a,\chi) &= \frac{(1-p^{-1})^2}{1-p^{-2}} \cdot \frac{1-x}{1-p^{-1}} + \frac{p^{-1}(1-p^{-1})^2}{1-p^{-2}} \cdot \frac{(1-x)px}{1-p^{-1}} \\ &\quad + \frac{p^{-1}(1-p^{-2})}{1-p^{-2}} \cdot p^2 x^2 \\ &= \frac{1+x^{-1}}{1+p^{-1}}.\end{aligned}$$

We consider $\mathcal{B}_{p^2}(a)$. Let $a = (0,1,0,0)$ and $g = \left(\begin{smallmatrix} q & r \\ s & t \end{smallmatrix}\right) \in G_{p^2}$. Then $(ga)_1 = 0$ if and only if $r = 0$ or $q \in pR$. Moreover, if $r = 0$ then $(ga)_2 \in R^\times$, and if $q \in pR$ then $(ga)_2 \in 2qR^\times$. Then by (8.18) and (8.13), if $p \neq 2$ we have

$$\begin{aligned}\mathcal{B}_{p^2}(a) &= \frac{p^{-2}(1-p^{-1})}{1-p^{-2}} \cdot p^2(1+p^{-1}) + \frac{p^{-1}(1-p^{-1})^2}{1-p^{-2}} \cdot p(1+p^{-1}) \\ &\quad + \frac{p^{-2}(1-p^{-1})}{1-p^{-2}} \cdot 1 \\ &= \frac{2p+1}{p+1},\end{aligned}$$

and if $p = 2$ we have

$$\mathcal{B}_{p^2}(a) = \frac{p^{-2}(1-p^{-1})}{1-p^{-2}} \cdot p^2(1+p^{-1}) + \frac{p^{-1}(1-p^{-1})}{1-p^{-2}} \cdot 1 = \frac{p+2}{p+1} = \frac{4}{3}.$$

When $p \neq 2$, $V_{p^2}(1^2 1_*)$ is a single orbit by Proposition 5.12, and hence this is enough. When $p = 2$ we see numerically that there is one other orbit represented by $a = (0,1,2,0)$ in $V_{p^2}(1^2 1_*)$, and by a similar consideration we have $\mathcal{B}_{p^2}(a) = \frac{5}{3}$ for this a.

This finishes the proof for type $(1^2 1_*)$. The arguments for types (1^3_*) and (1^3_{**}) are similar and easier, so we omit the details. ■

https://doi.org/10.4153/CJM-2013-027-0 Published online by Cambridge University Press

8.5 Ramified Computation

In this subsection, we compute $\mathcal{C}_{p^e}(a,\chi)$ for $p \mid m$, that is, at the primes p where χ is ramified. Since χ is cubic, either $p \equiv 1 \pmod 3$ or $p = 3$, and the conductor p^c of χ is

$$p^c = \begin{cases} p & p \equiv 1 \pmod 3, \\ p^2 & p = 3. \end{cases}$$

We assume $e \geq c$. We mainly work for $p \equiv 1 \pmod 3$. For $p = 3$, the computation seems to be more complicated theoretically. Fortunately there are only finitely many cases, so we simply use PARI/GP [19] for evaluation.

We first treat the case $e = 1$ and (hence) $p \equiv 1 \pmod 3$. The following is a refinement of [2, Proposition 5.4]. As in [2], we encounter a curious "cubic character sum of a cubic polynomial" which was evaluated by Wright [30].

Proposition 8.17 *Assume $p \equiv 1 \pmod 3$. Let $e = 1$. We have*

$$(1-p^{-2})\mathcal{C}_p(a,\chi)$$
$$= \begin{cases} p^{-2}\tau(\chi_p)^3\chi_p\big(P(a)\big) & \text{for } a \text{ of type } (3), (111), \\ -p^{-2}\tau(\chi_p)^3\chi_p\big(P(a)\big) & \text{for } a \text{ of type } (2), \\ 0 & \text{for } a \text{ of type } (1^21), (0), \\ \chi_p(\det g)^2 & \text{for } a \text{ of type } (1^3),\ a = g(1,0,0,0), g \in G_p. \end{cases}$$

Here $\tau(\chi_p) = \sum_{t\in\mathbb{F}_p^\times} \chi_p(t)\exp(2\pi i t/p)$ is the usual Gauss sum.

Proof If a is of type (1^21) or (0), then $\chi_p \circ \det$ is nontrivial on $G_{p,a}$ and hence $\mathcal{C}_p(a,\chi) = 0$. We consider the other cases. By (8.20) and (8.15) we have

$$\mathcal{C}_p(a,\chi) = \frac{1}{(p^2-1)(1-p^{-1})} \sum_{(u,v)\in\mathbb{F}_p^2, a(u,v)\neq 0} \chi_p\big(a(u,v)\big).$$

The sum in the right hand side was studied by Wright [30]. Let

$$J(\chi_p,\chi_p) = \sum_{t\in\mathbb{F}_p^\times, t\neq 1} \chi_p(t)\chi_p(1-t)$$

be the Jacobi sum. If a is of type (3), (21) or (111), then by [30, Theorem 1],

$$\sum_{(u,v)\in\mathbb{F}_p^2, a(u,v)\neq 0} \chi_p\big(a(u,v)\big) = \pm(p-1)\chi_p\big(P(a)\big)\, J(\chi_p,\chi_p),$$

where the sign is + if a is of type (3) or (111), and − if a is of type (2). Since $\chi_p^2 = \overline{\chi}_p \neq \mathbf{1}$, we have

$$J(\chi_p,\chi_p) = \tau(\chi_p)^2/\tau(\overline{\chi}_p) = \tau(\chi_p)^2\cdot\chi_p(-1)\tau(\chi_p)/p = \tau(\chi_p)^3/p,$$

https://doi.org/10.4153/CJM-2013-027-0 Published online by Cambridge University Press

and the result follows. Let a be of type (1^3). We have $a = ga_0$ for some $g \in G_p$, where $a_0 = (1, 0, 0, 0)$. Then $\mathcal{C}_p(a, \chi) = \chi_p(\det g)^2 \mathcal{C}_p(a_0, \chi)$ and

$$\sum_{(u,v)\in\mathbb{F}_p^2, a_0(u,v)\neq 0} \chi_p\big(a_0(u, v)\big) = \sum_{u\in\mathbb{F}_p^\times, v\in\mathbb{F}_p} \chi_p(u^3) = \sum_{u\in\mathbb{F}_p^\times, v\in\mathbb{F}_p} 1 = p(p-1).$$

Hence we have the formula. ■

We now study the case $e \geq 2$. When $e = 2$ and $a \in V_{p^2}^{\mathrm{nm}}$, this is fairly easy. As before we may assume $a \notin pV_{p^2}$.

Proposition 8.18 *If a is of type $(1^2 1_*)$, then $\mathcal{C}_{p^2}(a, \chi) = 0$. Let a be of type (1^3_*) or (1^3_{**}). We may assume $a = (1, a_2, a_3, 0)$ is in $\mathcal{D}_{p^2}(1^3_*)$ or $\mathcal{D}_{p^2}(1^3_{**})$, and for these a,*

$$(1-p^{-2})\mathcal{C}_{p^2}(a, \chi) = \begin{cases} 1 & p \equiv 1 \pmod 3, \\ \frac{1}{3}\big(1 + \chi_p(1 + a_2 + a_3) + \chi_p(1 - a_2 + a_3)\big) & p = 3. \end{cases}$$

Proof If a is of type $(1^2 1_*)$, then by Lemma 5.11 (i), $\chi \circ \det$ is nontrivial on $G_{p^2,a}$. Hence Lemma 8.8 (i) implies that $\mathcal{C}_{p^2}(a, \chi)$ must vanish.

We put $R = \mathbb{Z}/p^2\mathbb{Z}$. Let $a = (1, a_2, a_3, 0)$ with $a_2, a_3 \in pR$. Depending on the type of a, a_3 is in $pR^\times$ or 0. For $(u, v) \in W'_{p^2}$, $a(u, v) = 0$ if $u \in pR$. Hence by (8.20) and (8.15),

$$(1 - p^{-2})\mathcal{C}_{p^2}(a, \chi) = p^{-4}(1 - p^{-1})^{-1} \sum_{u\in R^\times, v\in R} \chi_p(u^3 + a_2u^2v + a_3uv^2).$$

By changing v to uv and using that χ_p is cubic,

$$(1 - p^{-2})\mathcal{C}_{p^2}(a, \chi) = p^{-2} \sum_{v\in R} \chi_p(1 + a_2v + a_3v^2).$$

If $p \equiv 1 \pmod 3$, then $\chi_p(1 + a_2v + a_3v^2) = 1$ since the conductor of χ_p is p. If $p = 3$, then $\chi_p(1+a_2v+a_3v^2)$ is determined by $(v \bmod 3) \in \{0, \pm 1\}$. Hence we have the formula. ■

For $e \geq 2$, we now compute $\mathcal{C}_{p^e}(a, \chi)$ for $a \in V_{\mathbb{Z}_p}^{\max}$ or $a \in V_{p^e}^{\max}$. For stating our result as well as applications to counting cubic fields [28], it is convenient to instead compute a quantity closely related to $\mathcal{C}_{p^e}(a, \chi)$. Let $a \in V_{\mathbb{Z}_p}^{\max}$. We choose $e \geq c$ such that

(i) $G_{p^e}a + p^eV_{\mathbb{Z}_p}$ is a single $G_{\mathbb{Z}_p}$-orbit,

(ii) the value $\tilde{\chi}_p\big(P(a)/p^{\mathrm{ord}_p(P(a))}\big)$ depends only on $a \bmod p^e$,

and define

$$\tilde{\mathcal{C}}_{p^e}(a, \chi) := (1 - p^{-2})\frac{\mathcal{C}_{p^e}(a, \chi)}{\tilde{\chi}_p\big(P(a)/p^{\mathrm{ord}_p(P(a))}\big)}.$$

This depends only on the $G_{\mathbb{Z}_p}$-orbit of a, and only on $a \bmod p^e$. Hence this depends only on the G_{p^e}-orbit of $a \bmod p^e$. For each a, we can choose such $e \geq c$ satisfying (i) and (ii) as follows.

https://doi.org/10.4153/CJM-2013-027-0 Published online by Cambridge University Press

Lemma 8.19

- (i) *Let* $p \equiv 1 \pmod 3$. *For a of type* (3), (21), *or* (111), $e = 1$ *is enough. For a of type* $(1^2 1_{\max})$ *or* $(1^3_{\max})$, $e = 2$ *is enough.*
- (ii) *Let* $p = 3$. *For a of type* (3), (21), *or* (111), $e = 2$ *is enough. For a of type* $(1^2 1_{\max})$ *or* $(1^3_{\max})$, $e = 3$ *is enough.*

Proof By Propositions 5.14, 5.15, these e satisfy (i). We check (ii) for each orbit individually. For elements of type $(3), (21), (111)$ this is trivial, so we work for the remaining cases. Assume $p = 3$ and $a \in V_{\mathbb{Z}_p}(1^3_{\max})$. A set of representatives of the various $G_{\mathbb{Z}_p}$-orbits are given in the second table of the next proposition. If a lies, say, in the orbit of $a_{\mathrm{rep}} = (1,3,0,3)$ and $a' \equiv a \pmod{p^3}$, then $\operatorname{ord}_p\big(P(a)\big) = 4$. Let $a = g a_{\mathrm{rep}}$. Then $g^{-1}a' \equiv a_{\mathrm{rep}} \pmod{p^3}$. If we write $g^{-1}a' = (a_1, a_2, a_3, a_4)$, then by the definition of the polynomial P, we have

$$P(g^{-1}a') \equiv -4a_2^3 a_4 - 27a_1^2 a_4^2 \equiv P(a_{\mathrm{rep}}) \pmod{p^6}.$$

This shows that $P(a')/p^4 \equiv P(a)/p^4 \pmod{p^2}$. Hence the values of $\tilde{\chi}_p$ for a, a' coincide; recall that the conductor of $\tilde{\chi}_p$ is p^2. This proves (ii) for this $G_{\mathbb{Z}_p}$-orbit.

The elements a in other orbits are treated similarly, and we omit the detailss. ■

We now give the value of $\tilde{\mathfrak{C}}_{p^e}(a, \chi)$ for each $G_{\mathbb{Z}_p}$-orbit in $V_{\mathbb{Z}_p}^{\max}$. We also list the minimal e, $|P(a)|_p^{-1}$ and $|G_{\mathbb{Z}_p,a}|$ for convenience. The result for $p \equiv 1 \pmod 3$ is due to Datskovsky and Wright [2, Proposition 5.4].

Proposition 8.20 *Let* $a \in V_{\mathbb{Z}_p}^{\max}$. *If* $p \equiv 1 \pmod 3$, *we have the following table.*

Type of a	$a \in V_{\mathbb{Z}_p}$	$e \geq$	$\tilde{\mathfrak{C}}_{p^e}(a, \chi)$	$\lvert P(a)\rvert_p^{-1}$	$\lvert G_{\mathbb{Z}_p,a}\rvert$
(3)	a	1	$\tau(\chi_p)^3/p^2$	1	3
(21)	a	1	$-\tau(\chi_p)^3/p^2$	1	2
(111)	a	1	$\tau(\chi_p)^3/p^2$	1	6
$(1^2 1_{\max})$	$(0,1,0,p\alpha), \alpha \in \mathbb{Z}_p^\times$	2	$\chi_p(2)\chi'_p(p)^2 p^{-1/3}$	p	2
$(1^3_{\max})$	$(1,0,0,p\alpha), \alpha \in \mathbb{Z}_p^\times$	2	$\chi_p(\alpha) + \chi_p(\alpha)^2\chi'_p(p)^2 p^{-1/3}$	p^2	3

If $p = 3$, *we have the following table.*

Type of a	$a \in V_{\mathbb{Z}_p}$	$e \geq$	$\tilde{\mathfrak{C}}_{p^e}(a, \chi)$	$\lvert P(a)\rvert_p^{-1}$	$\lvert G_{\mathbb{Z}_p,a}\rvert$
(3)	a	2	$\tau(\chi_p)^3/p^4 = \chi_p(2)/p$	1	3
(21)	a	2	$\tau(\chi_p)^3/p^4 = \chi_p(2)/p$	1	2
(111)	a	2	$\tau(\chi_p)^3/p^4 = \chi_p(2)/p$	1	6
$(1^2 1_{\max})$	$(0,1,0,\pm 3)$	3	$\pm\big(1 - \chi_p(4)\big)\,\chi'_p(p)^2 p^{-4/3}$	p	2
$(1^3_{\max})$	$(1,0,3,3)$	3	$\big(\chi_p(2) - 1\big)/p$	p^3	1
	$(1,0,6,3)$	3	$\big(2\chi_p(2) + 1\big)/p$	p^3	1
	$(1,3,0,3)$	3	$\chi_p(4)\chi'_p(p)^2 p^{-1/3}$	p^4	1
	$(1,-3,0,3\alpha), \alpha = 1,4,7$	3	$\chi_p(\alpha)^2 + \chi'_p(p)^2 p^{-1/3}$	p^4	3
	$(1,0,0,3\alpha), \alpha = 1,4,7$	3	$\chi_p(\alpha)^2\chi'_p(p)^2 p^{-1/3}$	p^5	1

https://doi.org/10.4153/CJM-2013-027-0 Published online by Cambridge University Press

Proof Let $p \equiv 1 \pmod 3$. By Lemma 8.9, for orbits of type $(3), (21), (111)$ this follows from Proposition 8.17. We consider orbits of type $(\sigma) = (1^2 1_{\max})$ or $(1^3_{\max})$. By Lemma 8.9 we may assume $e = 2$, but for potential further applications of our argument we let $e \geq 2$ be arbitrary. We use (8.20) and (8.15) for computation. Let $R = \mathbb{Z}/p^e\mathbb{Z}$. For $0 \neq x \in R$, let $\tilde{\chi}_p(x) = \tilde{\chi}_p(\tilde{x})$ where $\tilde{x} \in \mathbb{Z}_p$ is an arbitrary lift of x. This is well defined since the conductor of χ_p is p. Also if $x \in p^m R^\times$ for some $0 \leq m < e$ and $y \in x + p^{m+1}R$, then $\tilde{\chi}_p(y) = \tilde{\chi}_p(x)$.

(i) Let $a \in V_{p^e}(1^2 1_{\max})$. We may assume $a = (0, 1, a_3, a_4)$ where $a_3 \in pR$ and $a_4 \in pR^\times$. Let $(u, v) \in W'_{p^e}$. If $u \in pR$, then $v \in R^\times$ and hence $a(u, v) \in a_4 v^3 + p^2 R$. This implies $\tilde{\chi}_p\big(a(u, v)\big) = \tilde{\chi}_p(a_4 v^3) = \tilde{\chi}_p(a_4)$. If $u \in R^\times$, then $a(u, v) \neq 0$ if and only if $v \neq 0$, and in this case $a(u, v) \in v(u^2 + pR)$ and hence $\tilde{\chi}_p\big(a(u, v)\big) = \tilde{\chi}_p(u^2 v)$. Hence by (8.20), (8.15),

$$\begin{aligned}
\mathcal{C}_{p^e}(a, \chi) &= \frac{1}{p+1}\frac{\tilde{\chi}_p(a_4)p^{2/3}}{1 - p^{-1}} + \frac{1}{p^{2e}(1 - p^{-2})} \sum_{u \in R^\times, v \in R \setminus \{0\}} \frac{\tilde{\chi}_p(u^2 v)|v|^{-2/3}}{1 - p^{-1}} \\
&= \frac{\tilde{\chi}_p(a_4)p^{-1/3}}{1 - p^{-2}} + \frac{1}{p^{2e}(1 - p^{-2})(1 - p^{-1})} \\
&\qquad \times \sum_{u \in R^\times} \tilde{\chi}_p(u^2) \sum_{0 \leq m < e} p^{2m/3} \sum_{v \in p^m R^\times} \tilde{\chi}_p(v).
\end{aligned}$$

Since $\tilde{\chi}_p$ induces a nontrivial character on each $(\mathbb{Z}/p^{e-m}\mathbb{Z})^\times$ for $m < e$, we have

$$\sum_{v \in p^m R^\times} \tilde{\chi}_p(v) = \tilde{\chi}_p(p)^m \sum_{v' \in (\mathbb{Z}/p^{e-m}\mathbb{Z})^\times} \tilde{\chi}_p(v') = 0.$$

Hence $\mathcal{C}_{p^e}(a, \chi) = (1 - p^{-2})^{-1}\tilde{\chi}_p(a_4)p^{-1/3}$. In particular for $a = (0, 1, 0, p\alpha) \in V_{\mathbb{Z}_p}$, $\alpha \in \mathbb{Z}_p^\times$,

$$\tilde{\mathcal{C}}_{p^e}(a, \chi) = \frac{\tilde{\chi}_p(p\alpha)p^{-1/3}}{\tilde{\chi}_p(-4\alpha)} = \tilde{\chi}_p(2p)p^{-1/3} = \chi_p(2)\chi'_p(p^2)p^{-1/3}.$$

Note that the last equality follows from Lemma 8.1.

(ii) Let $a \in V_{p^e}(1^3_{\max})$. We may assume $a = (1, a_2, a_3, a_4)$ where $a_2, a_3 \in pR$ and $a_4 \in pR^\times$. If $u \in R^\times$, then $a(u, v) \in u^3 + pR$ and hence $\tilde{\chi}_p\big(a(u, v)\big) = 1$. If $u \in pR$, then $a(u, v) \in a_4 v^3 + p^2 R$ and hence $\tilde{\chi}_p\big(a(u, v)\big) = \tilde{\chi}_p(a_4)$. Hence by (8.20), (8.15),

$$\mathcal{C}_{p^e}(a, \chi) = \frac{p}{p+1}\frac{1}{1 - p^{-1}} + \frac{1}{p+1}\frac{\tilde{\chi}_p(a_4)p^{2/3}}{1 - p^{-1}} = \frac{1 + \tilde{\chi}_p(a_4)p^{-1/3}}{1 - p^{-2}}.$$

The result in the table follows from this. This finishes the proof for $p \equiv 1 \pmod 3$.

Let $p = 3$. Then since $\mathbb{Q}_p^\times = p^{\mathbb{Z}} \times \mathbb{Z}_p^\times$ and $(\mathbb{Z}_p/p^2\mathbb{Z}_p)^\times \cong (\mathbb{Z}/9\mathbb{Z})^\times$ is generated by $2 \in \mathbb{Z}_p^\times$, $\tilde{\chi}_p$ is determined uniquely by $\tilde{\chi}_p(p)$ and $\tilde{\chi}_p(2)$. Now the results in the second table are verified by explicitly evaluating the sum (8.20) using PARI/GP [19]. Note the identity $\chi_p(2) = p^{-3}\tau(\chi_p)^3$. ■

Remark 8.21 We now explain how Theorem 1.2 follows from our arguments. The functional equations of $\xi(s,a)$ and $\xi(s,\chi,a)$ are obtained as special cases of Theorem 4.3, due to F. Sato, and for $\xi(s,\chi,a)$ we stated this as Proposition 4.8. By Proposition 3.4, the residues of $\xi(s,a)$ are obtained from those of $\xi(s,\chi,a)$. By Proposition 8.2, $\xi(s,\chi,a)$ is entire if χ^3 is nontrivial, and Theorem 8.5 and Lemma 8.11 express the residues of $\xi(s,\chi,a)$ as a sum over G_N for χ cubic. When a corresponds to a maximal cubic ring for all $p \mid N$, explicit residue formulas are proved in Propositions 8.13 and 8.20. When N is cube-free, explicit formulas are proved in Propositions 8.12, 8.17 for $p \mid\mid N$, and Propositions 8.13, 8.16, 8.18, 8.20 for $p^2 \mid\mid N$.

9 Examples: Bias of Class Numbers in Arithmetic Progressions

Let χ be a primitive Dirichlet character of conductor m. For each sign we define

$$\xi_{\pm}(s,\chi) := \sum_{\substack{x\in \mathrm{SL}_2(\mathbb{Z})\backslash V_{\mathbb{Z}}^{\pm} \\ (P(x),m)=1}} \frac{|\operatorname{Stab}(x)|^{-1}\chi\bigl(P(x)\bigr)}{|P(x)|^s}, \tag{9.1}$$

where $V_{\mathbb{Z}}^{\pm} = \{x \in V_{\mathbb{Z}} \mid \pm P(x) > 0\}$ and $\operatorname{Stab}(x)$ denotes the stabilizer group of x in $\mathrm{SL}_2(\mathbb{Z})$. This is also a standard construction of L-functions from Shintani's zeta functions $\xi_{\pm}(s)$. In this section we apply our analysis to describe the residues of these zeta functions and their relatives, and prove biases of class numbers in arithmetic progressions. We also discuss how these results relate to Theorem 1.6.

Let $h \in C(V_m)$ be the function defined for $a \in V_m$ by

$$h(a) = \begin{cases} \chi\bigl(P(a)\bigr) & \text{if } P(a) \in (\mathbb{Z}/m\mathbb{Z})^{\times}, \\ 0 & \text{otherwise.} \end{cases}$$

Then $h \in C(V_m,\chi^2)$, and by Proposition 4.6, $\xi(s,h) = {}^t\bigl(\xi_+(s,\chi),\xi_-(s,\chi)\bigr)$. Proposition 8.6 asserts that each of $\xi_{\pm}(s,\chi)$ is holomorphic if χ^6 is nontrivial.

Assume $\chi^6 = \mathbf{1}$. We consider the case where m is a power of an odd prime p. (Since m is the conductor of χ, $\chi^6 = \mathbf{1}$ implies that $m = p$ except for the case $p = 3$, and χ is not quadratic where $m = p^2$.) Let $\lambda_p \in C(V_p)$ be as follows: $\lambda_p(a) = 1$ if a is of type (3) or (111), $\lambda_p(a) = -1$ if a is of type (21), and $\lambda_p(a) = 0$ otherwise.

If χ is quadratic, then Proposition 8.6 implies that $\xi_{\pm}(s,\chi)$ has possible simple poles at $s = 1$ and $5/6$. We compute the quantity $\mathcal{C}_p(h,\mathbf{1})$ defined in (8.8). In this case $h = \lambda_p$, and by Proposition 8.12 with Lemma 5.2,

$$\begin{aligned}\mathcal{C}_p(h,\mathbf{1}) = (1-p^{-1})\Bigl\{ \frac{(1-p^{-1/3})(1+p^{-1})}{3} - \frac{1-p^{-4/3}}{2} \\ + \frac{(1-p^{-2/3})(1+p^{-1/3})^2}{6}\Bigr\} = 0.\end{aligned}$$

Similarly $\mathcal{A}_p(h) = \mathcal{B}_p(h) = 0$. Hence $\xi_{\pm}(s,h)$ is in fact entire.

https://doi.org/10.4153/CJM-2013-027-0 Published online by Cambridge University Press

Now assume that $\chi^2 \neq \mathbf{1}$ but $\chi^6 = \mathbf{1}$, *i.e.*, χ is either cubic or sextic. Then $\xi_\pm(s,\chi)$ has a possible simple pole at $s = 5/6$ and is holomorphic elsewhere. Let $m = p \neq 3$. By Proposition 8.20,

$$\mathcal{C}_p(h,\chi^2) = p^{-4} \sum_{P(a)\neq 0} \chi\big(P(a)\big)\, \mathcal{C}_p(a,\chi^2) = \frac{p^{-6}\tau(\chi^2)^3}{1-p^{-2}} \sum_{P(a)\neq 0} \lambda_p(a)\chi\big(P(a)\big)^3$$
$$= \begin{cases} 0 & \text{if } \chi \text{ is cubic,} \\ p^{-2}(1-p^{-1})\tau(\chi^2)^3 & \text{if } \chi \text{ is sextic.} \end{cases}$$

If $m = p^2 = 3^2$, we have

$$\mathcal{C}_{p^2}(h,\chi^2) = \begin{cases} p^{-4}(1-p^{-1})\tau(\chi^2)^3 & \text{if } \chi \text{ is cubic,} \\ 0 & \text{if } \chi \text{ is sextic.} \end{cases}$$

So $\xi_\pm(s,\chi)$ has a pole at $s = 5/6$ when $\mathcal{C}_{p^e}(h,\chi^2)$ does not vanish.

Now let m be an arbitrary odd integer. Since $\mathcal{A}, \mathcal{B}, \mathcal{C}$ have Euler products, based on the computations above we get the following residue formula. Recall the decomposition $\chi = \prod \chi_p$ we introduced at the beginning of Section 8.

Theorem 9.1 *Assume that the conductor m of χ is odd and $m \neq 1$. Then the $\xi_\pm(s,\chi)$ are holomorphic except for a simple pole at $s = 5/6$, which occurs if χ_p is of order 6 for all $3 \neq p \mid m$ and in addition χ_3 is of order 3 if $3 \mid m$. In this case the residues are*

$$\operatorname{Res}_{s=5/6} \xi_\pm(s,\chi) = K_\pm \frac{2\pi^2 \prod_{p\mid m}(1-p^{-1})}{9\Gamma(2/3)^3 m^2} \tau(\chi^2)^3 L(1/3,\chi^{-2}).$$

Here $K_+ = 1, K_- = \sqrt{3}$, $\tau(\chi^2) = \sum_{t\in(\mathbb{Z}/m\mathbb{Z})^\times} \chi^2(t)\exp(2\pi i t/m)$ is the Gauss sum, and $L(s,\chi)$ is the usual Dirichlet L-function. If χ is of odd conductor $m > 1$ but does not satisfy the properties above, then the $\xi_\pm(s,\chi)$ are entire.

Proof We assume $\chi^6 = \mathbf{1}$ and compute the residue at $s = 5/6$; the residue computation at $s = 1$ is similar. Since χ is primitive, $\chi^6 = \mathbf{1}$ implies that each χ_p is quadratic, cubic, or sextic.

We first consider the case $3 \nmid m$. Then m is square free. Let us write $h = \prod_{p\mid m} h_p$, where $h_p \in C(V_p)$ satisfies $h_p(a) = \chi_p\big(P(a)\big)$ if $P(a) \in (\mathbb{Z}/p\mathbb{Z})^\times$ and $h_p(a) = 0$ if $P(a) = 0$. Then by (8.7) and (8.8), $\mathcal{C}_N(h,\chi^2) = \prod_{p\mid m} \mathcal{C}_p(h_p,\chi^2)$. $\mathcal{C}_p(h_p,\chi^2)$ is computed as above; it is $p^{-2}(1-p^{-1})\tau(\chi_p^2)^3$ if χ_p is sextic and 0 if χ_p is quadratic or cubic. Hence $\mathcal{C}_N(h,\chi^2) = 0$ if any χ_p is not sextic. Thus assume that all χ_p are sextic. Then by the decomposition formula for the classical Gauss sum (recalled before Proposition 4.11),

$$\frac{1}{m^2}\cdot\tau(\chi^2)^3 = \frac{1}{m^2}\prod_{p\mid m}\chi_p(m/p)^6\tau(\chi_p^2)^3 = \prod_{p\mid m}\frac{\tau(\chi_p^2)^3}{p^2},$$

https://doi.org/10.4153/CJM-2013-027-0 Published online by Cambridge University Press

and we conclude that

$$\mathcal{C}_N(h,\chi^2) = \frac{\tau(\chi^2)^3}{m^2}\prod_{p\mid m}(1-p^{-1}).$$

Hence (9.1) follows from Proposition 8.6 and (8.1).

The case $3\mid m$ is similarly done; $\mathcal{C}_N(h,\chi^2)=0$ unless χ_3 is cubic and χ_p is sextic for all $3\neq p\mid m$, and in this case we have (9.1) because of the identity

$$\frac{1}{m^2}\cdot\tau(\chi^2)^3 = \frac{\tau(\chi_3^2)^3}{3^4}\prod_{p\mid m}\frac{\tau(\chi_p^2)^3}{p^2}. \qquad \blacksquare$$

From this result we can prove the two main terms of the function counting the class numbers of integral binary cubic forms in arithmetic progressions. This result implies that there is a bias in the second main term if and only if the odd modulus admits a character of order 6.

Theorem 9.2 *Let $h_\pm(n)$ be the coefficients of Shintani's original zeta function $\xi_\pm(s)$,* i.e., $\xi_\pm(s)=\sum h_\pm(n)/n^s$. *Let N be an odd integer and a an integer coprime to N. Then*

$$\sum_{\substack{0<n<X\\ n\equiv a (\operatorname{mod} N)}} h_\pm(n) = C'_\pm\frac{\pi^2\prod_{p\mid N}(1-p^{-2})}{9N}\cdot X$$
$$+K_1(N,a)\frac{2K_\pm\pi^2}{9\Gamma(2/3)^3N}\cdot\frac{X^{5/6}}{5/6}+O_{N,\epsilon}(X^{3/5+\epsilon}),$$

where $C'_+=1, C'_-=3/2, K_+=1, K_-=\sqrt{3}$, and

$$K_1(N,a)=\sum_{\chi^6=\mathbf{1}}{}' \chi(a)^{-1}\frac{\tau(\chi^2)^3L(1/3,\chi^{-2})}{m_\chi^2}\prod_{p\mid N,p\nmid m_\chi}\bigl(1-\chi(p)^{-2}p^{-4/3}\bigr).$$

Here the sum above is over primitive characters χ whose conductor m_χ is a divisor of N (including the trivial character modulo 1) such that if we write $\chi=\prod_{p\mid m_\chi}\chi_p$, then each χ_p has exact order 6 for $p\neq 3$ and χ_3 has exact order 3 if $3\mid m_\chi$.

By the Delone–Faddeev correspondence, we can also state Theorem 9.2 as a formula counting discriminants of cubic rings in arithmetic progressions.

Proof Let χ be a primitive Dirichlet character whose conductor m_χ is a divisor of N. We define $\xi^N_\pm(s,\chi)$ by the formula (9.1) with the sum restricted to those x with $P(x)$ coprime to N (rather than m_χ). Then Proposition 8.6 and Corollary 8.14 imply

$$\operatorname{Res}_{s=1}\xi^N_\pm(s,\mathbf{1}) = \operatorname{Res}_{s=1}\xi_\pm(s,\mathbf{1})\prod_{p\mid N}(1-p^{-1})(1-p^{-2}),$$

$$\operatorname{Res}_{s=5/6}\xi^N_\pm(s,\chi) = \operatorname{Res}_{s=5/6}\xi_\pm(s,\chi)\prod_{p\mid N,p\nmid m_\chi}(1-p^{-1})\bigl(1-\chi(p)^{-2}p^{-4/3}\bigr),$$

where if $\chi^6 \neq \mathbf{1}$, the second formula means the formal equality $0 = 0$. On the other hand, Sato–Shintani's Tauberian theorem [24, Theorem 3] asserts that

$$\sum_{0<n<X,(n,N)=1} h_\pm(n)\chi(n) = \operatorname{Res}_{s=1} \xi^N_\pm(s,\chi)X + \operatorname{Res}_{s=5/6} \xi^N_\pm(s,\chi)\frac{X^{5/6}}{5/6} + O_{N,\epsilon}(X^{3/5+\epsilon}).$$

Now the theorem follows from the residue formulas in Theorems 8.4 and 9.1 with the orthogonality of characters. Note that $\varphi(N) = N\prod_{p\mid N}(1-p^{-1})$. ■

Let $\mathcal{P}$ be a finite set of primes. We define the $\mathcal{P}$-maximal L-function $\xi^{\mathcal{P}}_\pm(s,\chi)$ by the formula (9.1) with the sum restricted to those x satisfying $(x \bmod p^2) \in V^{\max}_{p^2}$ for all $p \in \mathcal{P}$. Note that $\bigl(P(x), m\bigr) = 1$ implies $(x \bmod p^2) \in V^{\max}_{p^2}$ for $p \mid m$, hence only primes $p \in \mathcal{P}$ coprime to m are relevant for the definition. Then $\xi^{\mathcal{P}}_\pm(s,\chi)$ again has a pole under the same condition for $\xi_\pm(s,\chi)$, and by Proposition 8.6 and Corollary 8.15 the residues are

$$\operatorname{Res}_{s=5/6} \xi^{\mathcal{P}}_\pm(s,\chi) = \operatorname{Res}_{s=5/6} \xi_\pm(s,\chi) \prod_{p\in\mathcal{P}, p\nmid m} (1-p^{-2})(1-\chi^2(p)p^{-5/3}). \tag{9.2}$$

The poles at $s = 5/6$ of $\xi^{\mathcal{P}}_\pm(s,\chi)$, as well as of $\xi_\pm(s,\chi)$, are the source of the biases we described in Theorem 1.6. Indeed, for χ as in Theorem 9.1, we prove in [28] that

$$\sum_{\substack{[F:\mathbb{Q}]=3, 0<\pm\operatorname{Disc}(F)<X \\ (\operatorname{Disc}(F),m)=1}} \chi\bigl(\operatorname{Disc}(F)\bigr) = \frac{K_\pm(\chi)}{2}\frac{X^{5/6}}{5/6} + O(m^{8/9}X^{7/9+\epsilon}), \tag{9.3}$$

where $K_\pm(\chi)$ is the limit of (9.2) as $\mathcal{P}$ tends to the set of all primes:

$$K_\pm(\chi) := \frac{4K_\pm\tau(\chi^2)^3}{3\Gamma(2/3)^3 m^2 \prod_{p\mid m}(1+p^{-1})} \frac{L(1/3,\chi^{-2})}{L(5/3,\chi^2)}.$$

The 2 in the denominator of $\frac{K_\pm(\chi)}{2}$ in (9.3) is the index $[\mathrm{GL}_2(\mathbb{Z})\colon \mathrm{SL}_2(\mathbb{Z})]$. This appears because the Shintani zeta functions count $\mathrm{SL}_2(\mathbb{Z})$-orbits, while cubic fields correspond to $\mathrm{GL}_2(\mathbb{Z})$-orbits.

We briefly explain other variations as well. Suppose first that the conductor m is a power of $p = 2$. Then there are no cubic nor sextic characters, but are three quadratic characters χ. One is of conductor 4, and the two others are of conductor 8. To compute the residues, we note that for $a \in V_{\mathbb{Z}_2}$ of type (3), (21), or (111), $P(a) \bmod 8$ is given by

$$P(a) \equiv \begin{cases} 1 \bmod 8 & \text{for } a \text{ of type } (3), (111), \\ 5 \bmod 8 & \text{for } a \text{ of type } (21). \end{cases} \tag{9.4}$$

This is easily verified for the representatives

$$(1,0,1,1) \in V_{\mathbb{Z}_2}(3), \quad (0,1,1,1) \in V_{\mathbb{Z}_2}(21), \quad (0,1,1,0) \in V_{\mathbb{Z}_2}(111),$$

https://doi.org/10.4153/CJM-2013-027-0 Published online by Cambridge University Press

and hence is true for any element a, because $P(ga) = (\det g)^2 P(a)$ and $(\det g)^2 \in (\mathbb{Z}_2^\times)^2 = 1 + 8\mathbb{Z}_2$. Let χ be of conductor $4 = p^2$. By (9.4), $h(a) = \chi\big(P(a)\big)$ is always 1 when $P(a) \in (\mathbb{Z}/4\mathbb{Z})^\times$, and we have

$$\mathcal{A}_{p^2}(h) = \mathcal{B}_{p^2}(h) = (1-p^{-1})(1-p^{-2}), \quad \mathcal{C}_{p^2}(h,\mathbf{1}) = (1-p^{-1})(1-p^{-4/3}).$$

Hence $\xi_\pm(s,\chi)$ has poles both at $s = 1$ and $s = 5/6$ for this χ. But this is fairly reasonable, because $P(x)$ is always $\equiv 0, 1 \pmod 4$ for $x \in V_\mathbb{Z}$, and so $\xi_\pm(s,\chi)$ simply counts orbits with $P(x) \equiv 1 \pmod 4$ without a twist. On the other hand, if χ is either character of conductor $8 = p^3$, by (9.4) $h(a) = 1$ if a is of type (3) or (111), $h(a) = -1$ if a is of type (21), and $h(a) = 0$ otherwise. Hence we have $\mathcal{A}_{p^3}(h) = \mathcal{B}_{p^3}(h) = \mathcal{C}_{p^3}(h,\mathbf{1}) = 0$, and the $\xi_\pm(s,\chi)$ are entire.

Second, this observation for $m = 2^c$ allows us to extend Theorem 9.1 to m even. This consists of case by case descriptions corresponding to conditions on χ_2, and we omit the details.

Third, let r be a positive integer. Then

$$\xi_\pm(s,r,\chi) := \sum_{\substack{x\in \mathrm{SL}_2(\mathbb{Z})\backslash V_\mathbb{Z}^\pm \\ r\mid P(x),(P(x)/r,m)=1}} \frac{|\operatorname{Stab}(x)|^{-1}\chi\big(P(x)/r\big)}{|P(x)|^s} \tag{9.5}$$

is also a natural L-function. Since ${}^t\big(\xi_+(s,r,\chi), \xi_-(s,r,\chi)\big) = \xi(s,h)$ for an appropriate $h \in C(V_N,\chi^2)$, we can study these as well. In particular it is entire if $\chi^6 \neq \mathbf{1}$, and we can describe their residues explicitly when $\chi^6 = \mathbf{1}$ for the case we can apply the residual computations. This includes the case when r is cubefree and $p \nmid m$ for all $p^2 \mid r$. As a simplest example, let $m = r = p \neq 2, 3$. Then $h \in C(V_{p^2},\chi^2)$ is given by

$$h(a) = \begin{cases} \chi(P(a)/p) & \text{if } a \in V_{p^2}(1^2 1_{\max}), \\ 0 & \text{otherwise.} \end{cases}$$

For χ quadratic, by Proposition 8.13 with Proposition 5.12 (i) (ii), we see that $\mathcal{A}_{p^2}(h) = \mathcal{B}_{p^2}(h) = \mathcal{C}_{p^2}(h,\mathbf{1}) = 0$. For χ cubic or sextic, by Proposition 8.20 we have

$$\begin{aligned}\mathcal{C}_{p^2}(h,\chi^2) &= \sum_{a\in V_{p^2}(1^2 1_{\max})} \chi\big(P(a)/p\big)\,\mathcal{C}_p(a,\chi^2) = \frac{\chi(4)p^{-1/3}}{1-p^{-2}} \sum_{a\in V_{p^2}(1^2 1_{\max})} \chi^3\big(P(a)/p\big) \\ &= \begin{cases} \chi(4)(1-p^{-1})p^{-4/3} & \text{if } \chi \text{ is cubic,} \\ 0 & \text{if } \chi \text{ is sextic.} \end{cases}\end{aligned}$$

Hence the $\xi_\pm(s,p,\chi)$ are entire unless χ is cubic, in which case their residues at $s = 5/6$ are

$$\operatorname{Res}_{s=5/6} \xi_\pm(s,p,\chi) = K_\pm \frac{2\pi^2\chi(4)(1-p^{-1})}{9\Gamma(2/3)^3 p^{4/3}} L(1/3,\chi^{-2}).$$

https://doi.org/10.4153/CJM-2013-027-0 Published online by Cambridge University Press

This again is a source of the bias in Theorem 1.6 for $m = p^2$ and $(m, a) = p$.

Moreover, if $r = r(X_N)$ for a union of G_N-orbits X_N in V_N is well defined, then we can define $\xi_{\pm}(s, X_N, \chi)$ by (9.5) with the sum restricted to those x satisfying $(x \bmod N) \in X_N$. This is in fact possible if X_N detects certain maximal cubic rings over $\mathbb{Z}_p$ for each $p \mid N$, and as we computed the contributions to the residues for all $a \in V_{p^e}^{\max}$ in Propositions 8.13 and 8.20, we can describe the residues explicitly. This enables us to impose local specifications while counting cubic fields in arithmetic progressions. For details, see [28, Section 6.4].

Acknowledgement The first author would like to thank Shingo Mori for many discussions, which became the starting point of this work, and the Princeton Mathematics Department for their support during his stay.

References

[1] M. Bhargava, A. Shankar, and J. Tsimerman, *On the Davenport–Heilbronn theorem and second order terms.* Invent. Math. **193**(2013), 439–499. http://dx.doi.org/10.1007/s00222-012-0433-0

[2] B. Datskovsky and D. J. Wright, *The adelic zeta function associated with the space of binary cubic forms II: Local theory.* J. Reine Angew. Math. **367**(1986), 27–75.

[3] ———, *Density of discriminants of cubic extensions.* J. Reine Angew. Math. **386**(1988), 116–138.

[4] H. Davenport and H. Heilbronn, *On the density of dsicriminants of cubic fields. II.* Proc. Roy. Soc. London Ser. A **322**(1971), no. 1551, 405–420.

[5] B. N. Delone and D. K. Faddeev, *The theory of irrationalities of the third degree.* Transl. Math. Monogr. **10**, American Mathematical Society, Providence, 1964.

[6] J. Denef and A. Gyoja, *Character sums associated to prehomogeneous vector spaces.* Compositio Math. **113**(1998), 273–346. http://dx.doi.org/10.1023/A:1000404921277

[7] E. Fouvry and N. Katz, *A general stratification theorem for exponential sums, and applications.* J. Reine Angew. Math. **540**(2001), 115–166.

[8] W. T. Gan, B. Gross, and G. Savin, *Fourier coefficients of modular forms on G_2.* Duke Math. J. **115**(2002), 105–169. http://dx.doi.org/10.1215/S0012-7094-02-11514-2

[9] S. Gelbart, *Automorphic Forms on Adele Groups*. Princeton University Press, Princeton, 1975.

[10] T. Ibukiyama and H. Saito, *On zeta functions associated to symmetric matrices and an explicit conjecture on dimensions of Siegel modular forms of general degree.* Internat. Math. Res. Notices **8**(1992), 161–169.

[11] T. Ibukiyama and H. Saito, *On zeta functions associated to symmetric matrices III: An explicit form of L-functions.* Nagoya Math. J. **146**(1997), 149–183.

[12] H. Iwaniec and E. Kowalski, *Analytic Number Theory.* Amer. Math. Soc. Colloq. Publ. **53**, Amer. Math. Soc., Providence, Rhode Island, 2004.

[13] J. Jones and D. Roberts, *A database of local fields.* J. Symbolic Comput. **41**(2006), 80–97. Accompanying database available online at http://math.la.asu.edu/~jj/localfields/. http://dx.doi.org/10.1016/j.jsc.2005.09.003

[14] S. Mori, *Orbital Gauss sums for the space of binary cubic forms over a finite field.* In preparation.

[15] J. Nakagawa, *On the relations among the class numbers of binary cubic forms.* Invent. Math. **134**(1998), 101–138. http://dx.doi.org/10.1007/s002220050259

[16] Y. Ohno, *A conjecture on coincidence among the zeta functions associated with the space of binary cubic forms.* Amer. J. Math. **119**(1997), 1083–1094. http://dx.doi.org/10.1353/ajm.1997.0032

[17] Y. Ohno and T. Taniguchi, *Relations among Dirichlet series whose coefficients are class numbers of binary cubic forms II.* Preprint, 2009. arxiv:1112.5029

[18] Y. Ohno, T. Taniguchi, and S. Wakatsuki, *Relations among Dirichlet series whose coefficients are class numbers of binary cubic forms.* Amer. J. Math. **131**(2009), 1525–1541. http://dx.doi.org/10.1353/ajm.0.0080

[19] PARI/GP. version 2.3.4, Bordeaux, 2008. Available from http://pari.math.u-bordeaux.fr/.

[20] H. Saito, *A generalization of Gauss sums and its applications to Siegel modular forms and L-functions associated with the vector space of quadratic forms.* J. Reine Angew. Math. **416**(1991), 91–142.

[21] ———, *On L-functions associated with the vector space of binary quadratic forms.* Nagoya Math. J. **130**(1993), 149–176.

https://doi.org/10.4153/CJM-2013-027-0 Published online by Cambridge University Press

[22] F. Sato, *On functional equations of zeta distributions.* Adv. Studies in Pure Math. **15**(1989), 465–508.

[23] M. Sato and T. Kimura, *A classification of irreducible prehomogeneous vector spaces and their relative invariants.* Nagoya Math. J. **65**(1977), 1–155.

[24] M. Sato and T. Shintani, *On zeta functions associated with prehomogeneous vector spaces.* Ann. of Math. **100**(1974), 131–170. http://dx.doi.org/10.2307/1970844

[25] T. Shintani, *On Dirichlet series whose coefficients are class-numbers of integral binary cubic forms.* J. Math. Soc. Japan **24**(1972), 132–188. http://dx.doi.org/10.2969/jmsj/02410132

[26] ______, *On zeta-functions associated with vector spaces of quadratic forms.* J. Fac. Sci. Univ. Tokyo, Sect. IA **22**(1975), 25–66.

[27] T. Taniguchi, *On the zeta functions of prehomogeneous vector spaces for a pair of simple algebras.* Ann. Inst. Fourier **57**(2007), 1331–1358. http://dx.doi.org/10.5802/aif.2296

[28] T. Taniguchi and F. Thorne, *Secondary terms in counting functions for cubic fields.* Duke Math. J., to appear.

[29] D. J. Wright, *The adelic zeta function associated to the space of binary cubic forms part I: Global theory.* Math. Ann. **270**(1985), 503–534. http://dx.doi.org/10.1007/BF01455301

[30] D. J. Wright, *Cubic character sums of cubic polynomials.* Proc. Amer. Math. Soc. **100**(1987), 409–413. http://dx.doi.org/10.1090/S0002-9939-1987-0891136-3

[31] D. J. Wright and A. Yukie, *Prehomogeneous vector spaces and field extensions.* Invent. Math. **110**(1992), 283–314. http://dx.doi.org/10.1007/BF01231334

[32] A. Yukie, *Shintani Zeta Functions.* London Math. Soc. Lecture Note Ser. **183**, Cambridge University Press, Cambridge, 1993.

Department of Mathematics, Graduate School of Science, Kobe University, Kobe 657-8501, Japan

and

Department of Mathematics, Princeton University, Princeton, NJ 08540, USA
e-mail: tani@math.kobe-u.ac.jp

Department of Mathematics, University of South Carolina, Columbia, SC 29208, USA
e-mail: thorne@math.sc.edu

https://doi.org/10.4153/CJM-2013-027-0 Published online by Cambridge University Press