L'Enseignement Mathématique (2) 57 (2011), 393–422

SIEGEL'S MASS FORMULA AND AVERAGES OF DIRICHLET L-FUNCTIONS OVER FUNCTION FIELDS

by Piotr MACIAK and Jorge MORALES

ABSTRACT. Let $\mathfrak{G}$ be a genus of definite ternary lattices over $\mathbf{F}_q[t]$ of square-free determinant. In this paper we give self-contained and relatively elementary proofs of Siegel's formulas for the weighted sum of primitive representation numbers over the classes of $\mathfrak{G}$ and for the mass of $\mathfrak{G}$. Our proof of the mass formula shows an interesting and seemingly new relation with certain averages of Dirichlet L-functions.

1. INTRODUCTION

Let $\mathbf{F}_q$ be the finite field with q elements, where q is odd. Let $K = \mathbf{F}_q(t)$ be the field of rational functions over $\mathbf{F}_q$, and $A = \mathbf{F}_q[t]$ the polynomial ring. We denote by K_∞ the completion of K "at infinity", that is $K_\infty = \mathbf{F}_q((t^{-1}))$, the field of Laurent series in t^{-1} over $\mathbf{F}_q$.

A quadratic space (V, Q) over K is *definite* if the extended space $(V \otimes K_\infty, Q)$ is anisotropic, that is if Q has no nontrivial zeros over K_∞. If (V, Q) is definite, then the dimension of V is at most four since the field K_∞ is C_2 by a theorem of Lang [11, Theorem 8].

Let $D \in A$ be a square-free polynomial and let (V, Q) be a ternary definite quadratic space over K that contains integral lattices of determinant D. Let $\mathfrak{G}$ denote the genus of such lattices. In this paper we give self-contained and relatively elementary proofs for the Siegel-Minkowski formulas for the weighted sum of primitive representation numbers over the classes in $\mathfrak{G}$ (see (1.1) below) and the formula for the mass of $\mathfrak{G}$ (see (1.3) below). Both formulas are obtained directly in a completely explicit form that does not involve Euler products of local densities.

Let $L_1, \ldots, L_h$ be representatives of all isometry classes in $\mathfrak{G}$. Let $n_i = |SO(L_i)|$ for $i = 1, \ldots, h$. For $a \in A$ we denote by $R(L_i, a)$ the number of *primitive* solutions of the equation $Q(\mathbf{x}) = a$ with $\mathbf{x} \in L_i$. We begin by establishing a formula for the weighted sum of the $R(L_i, a)$

$$\sum_{i=1}^{h} \frac{1}{n_i} R(L_i, a) = \frac{1}{2^r} \left|\mathrm{Pic}(A[\sqrt{-aD}])\right|, \tag{1.1}$$

where a is prime to the determinant D and such that $-aD$ is not a square in K_∞ and r is the number of irreducible polynomials dividing D (Theorem 5.7). Here $\mathrm{Pic}(A[\sqrt{-aD}])$ is the *Picard group* of the order $A[\sqrt{-aD}]$. Formula (1.1) is established from the action of a suitable idèle group on a set of lattices of $\mathfrak{G}$ that represent a primitively. Formula (1.1) was already known to Gauss [4, §292] for the number of primitive solutions of the equation $x^2 + y^2 + z^2 = a$ over $\mathbf{Z}$. Interpretations of Gauss' formula in terms of the Hurwitz quaternions have been given by Venkov [20] and Rehm [14]. Shemanske [18] generalized this to the norm form of a quaternion algebra of class number one over $\mathbf{Q}$. Our approach uses a correspondence between lattices and quaternion orders that goes back to work of Brandt and Latimer (see the thorough exposition by Llorente [12] on this topic).

Recall that the quantity $\sum_{i=1}^{h} 1/n_i$ is called the *mass* of $\mathfrak{G}$. We obtain an explicit expression for the mass using an argument that is specific to function fields. We compute the limit of "averages" of $R(L_i, a)$ as a varies over a fixed degree

$$\lim_{m\to\infty} \frac{1}{q^{3m}} \sum_{\substack{\deg a = 2m+\delta+1 \\ (a,D)=1}} R(L_i, a), \tag{1.2}$$

where $\delta = \deg D$. We show that this limit does not depend on the representative L_i of the genus. Denoting this limit by ℓ and using (1.1) we get

$$\sum_{i=1}^{h} \frac{1}{n_i} = \frac{1}{2^r \ell} \lim_{m\to\infty} \frac{1}{q^{3m}} \sum_{\substack{\deg a = 2m+\delta+1 \\ (a,D)=1}} \left|\mathrm{Pic}(A[\sqrt{-aD}])\right|.$$

The evaluation of the limit on the right-hand side reveals an interesting connection with work by Hoffstein and Rosen [8] on averages of L-functions over function fields (see Theorem 7.5 and Remark 7.6). The computation of this limit in our situation requires the use of the "Riemann Hypothesis" for curves over finite fields, which was first proved by A. Weil [21]. Elementary proofs have since then been offered by Stepanov [19] (for hyperelliptic curves, the only case needed here), Schmidt [17], Bombieri [1]. See [15, Appendix] for an exposition of Bombieri's proof and interesting historical remarks.

In order to state the final formula for the mass we introduce the function

$$M_e(s) = \sum_{\substack{d|e \\ d \text{ monic}}} \mu(d)|d|^{-s},$$

where μ is the Möbius function and $e \in A \setminus \{0\}$.

With this notation, the formula for the mass that we obtain is

$$\sum_{i=1}^{h} \frac{1}{n_i} = \frac{q^{\delta} M_D(1) M_{D_0}(2)}{2^r(q^2-1)(2M_{D_0}(1) - M_{D_0}(2))}, \tag{1.3}$$

where D is the determinant and δ is its degree. The polynomial D_0 is the product of prime divisors of D at which Q is isotropic, and D_1 is the product of prime divisors of D at which Q is anisotropic, and r is the total number of prime divisors of D (Theorem 8.1).

In the last section we apply (1.3) to obtain an exact formula for the class number h in the case where D is irreducible (Theorem 9.2).

2. Preliminaries and notation

The following notation will be used throughout this paper:

$\mathbf{F}_q$	:	the finite field with q elements, where q is odd
A	:	the polynomial ring $\mathbf{F}_q[t]$
K	:	the field of fractions of A
$\mathbf{A}_K$	:	the adèle ring of K
(V,Q)	:	a regular quadratic space over K
$C(V,Q)$	:	the Clifford algebra of (V,Q)
$C_0(V,Q)$	:	the even Clifford algebra of (V,Q)

Recall that a quadratic form Q over K is *definite* if it is anisotropic (i.e. does not have nontrivial zeros) over $K_\infty = \mathbf{F}_q((t^{-1}))$. Notice that definite forms exist only in rank ≤ 4.

In this paper, we shall limit ourselves to the case $\dim_K V = 3$ and all quadratic forms are assumed to be definite. This implies in particular that $C_0(V,Q)$ is a quaternion algebra over K ramified at $\mathfrak{p} = \infty$.

If $\mathfrak{p}$ is a prime of A then $A_\mathfrak{p}$, $K_\mathfrak{p}$ will denote $\mathfrak{p}$-adic completions of A, K respectively. Similar notation will be used to denote localizations of any considered modules.

If L is an A-lattice in V, the *determinant* $\det(L)$ of L is defined as

$$\det(B(\mathbf{e}_i, \mathbf{e}_j)) \in A/(\mathbf{F}_q^\times)^2,$$

where $B(\mathbf{x}, \mathbf{y}) = \frac{1}{2}\big(Q(\mathbf{x}+\mathbf{y}) - Q(\mathbf{x}) - Q(\mathbf{y})\big)$ and $(\mathbf{e}_1, \ldots, \mathbf{e}_n)$ is a basis of L over A.

A lattice $L \subset V$ is called *maximal* if it is maximal for the property that $B(L, L) \subset A$.

Recall that two lattices L and L' of V are in the *same genus* if their completions $L_\mathfrak{p}$ and $L'_\mathfrak{p}$ are isometric for all primes $\mathfrak{p}$ of K.

LEMMA 2.1. *All maximal lattices in V are in the same genus.*

Proof. This follows from [13, Theorem 91:2].

LEMMA 2.2. *Let (V, Q) be a ternary definite quadratic space over K and let $L \subset V$ be an integral lattice of square-free determinant D. Let $a \in A$ be a polynomial relatively prime to D. The following conditions are equivalent:*

(i) *The equation $Q(\mathbf{x}) = a$ has a solution with $\mathbf{x} \in V$.*

(ii) *The equation $Q(\mathbf{x}) = a$ has a solution with $\mathbf{x} \in V_\infty$.*

(iii) *The equation $Q(\mathbf{x}) = a$ has a primitive solution $\mathbf{x} \in L_\mathfrak{p}$ for all primes $\mathfrak{p}$ of K (including $\mathfrak{p} = \infty$).*

(iv) *The equation $Q(\mathbf{x}) = a$ has a primitive solution $\mathbf{x} \in M$, where M is some lattice in the genus of L.*

(v) *$-aD$ is not a square in K_∞.*

(vi) *The extension $K(\sqrt{-aD})/K$ does not split at $\mathfrak{p} = \infty$ (i.e. is "imaginary").*

Proof. (i) $\Longrightarrow$ (ii) is trivial.

(ii) $\Longrightarrow$ (iii). Let $\mathfrak{p}$ be a finite prime. If $\mathfrak{p} \nmid D$ then $(L_\mathfrak{p}, Q)$ has a binary hyperbolic orthogonal factor $\langle 1, -1 \rangle$ and hence $(L_\mathfrak{p}, Q)$ represents primitively any element of $A_\mathfrak{p}$. If $\mathfrak{p} \mid D$ then $(L_\mathfrak{p}, Q)$ has a binary unimodular orthogonal factor and hence represents all $\mathfrak{p}$-units, in particular a.

(iii) $\Longrightarrow$ (i) follows from the Hasse-Minkowski Theorem.

(iii) $\Longleftrightarrow$ (iv) follows from [3, Ch. 9, Theorem 5.1].

(v) $\Longleftrightarrow$ (ii). It is clear that a is represented by V_∞ if and only if $F = Q \perp \langle -a \rangle$ is isotropic over K_∞. By [6, Proposition 4.24] this condition holds if and only if $-aD \notin {K_\infty^\times}^2$ or $S_\infty(F) = 1$, where S_∞ denotes the *Hasse invariant* at ∞. Since Q is anisotropic over K_∞

we have $S_\infty(Q) = -(-1,D)_\infty$ (see e.g. [6, Proposition 4.21]). Hence $S_\infty(F) = S_\infty(Q)(D,-a)_\infty = -(D,a)_\infty$. If $-aD \in {K_\infty^\times}^2$ then $S_\infty(F) = -1$, which would imply that a is not represented by V_∞.

(v) $\iff$ (vi) is trivial.

3. Correspondence between lattices and orders

We assume throughout this section that (V,Q) is a ternary definite quadratic space over K.

Recall that the *Clifford algebra* $C(V,Q)$ is the quotient of the tensor algebra $T(V)$ by the two-sided ideal generated by the set $\{\mathbf{x}\otimes\mathbf{x} - Q(\mathbf{x}) : \mathbf{x} \in V\}$. We refer to [16, Chapter 9, §2] or [3, Chapter 10, §2] for the general properties of this construction.

If $L \subset V$ is an integral A-lattice we denote by $C(L)$ the Clifford algebra of L, which we view as the A-order of $C(V,Q)$ generated by L. Its center $Z(C(L))$ is a quadratic order over A, hence of the form $A[\delta_L]$, where $\delta_L^2 \in A$. Notice that δ_L is defined only up to a multiplicative constant. It is easy to see that $\delta_L^2 = -\det L$ (up to squares of $\mathbf{F}_q^\times$).

Lemma 3.1. *Let $L, M \subset V$ be integral lattices with the same determinant. Then $\delta_L = \delta_M u$, where $u \in \mathbf{F}_q^\times$.*

Proof. δ_L and δ_M generate the quadratic extension $Z(C(V,Q))/K$, so $\delta_L = \delta_M u$ with $u \in K^\times$. Since $\delta_M^2 = -\det M \equiv -\det L = \delta_L^2 \pmod{{\mathbf{F}_q^\times}^2}$, we have $u \in \mathbf{F}_q^\times$.

We denote by $C_0(V,Q)$ the *even Clifford algebra* of (V,Q) (see [16, Chapter 9, §2] for the definition). The algebra $C_0(V,Q)$ comes naturally equipped with the *trace form* $\langle x,y\rangle = \frac{1}{2}\mathrm{Tr}(x\bar{y})$, where Tr is the reduced trace and $\bar{\ }$ is the canonical involution on $C_0(V,Q)$. The associated quadratic form is the *norm form* of $C_0(V,Q)$ and will be denoted by N. If $L \subset V$ is an integral lattice, we denote by $C_0(L)$ its even Clifford algebra, which is an A-order in $C_0(V,Q)$. An order in $C_0(V,Q)$ is in particular an A-lattice, so it makes sense to speak about its determinant with respect to $\langle\ ,\ \rangle$.

PROPOSITION 3.2. *Let L be an integral A-lattice in (V,Q). Then*

$$\det(C_0(L)) = \det(L)^2 .$$

Proof. Let $\mathfrak{p}$ be a prime of A and let $\{\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3\}$ be an orthogonal basis of $L_\mathfrak{p}$. It is easy to check that $\{1, \mathbf{e}_1\mathbf{e}_2, \mathbf{e}_1\mathbf{e}_3, \mathbf{e}_2\mathbf{e}_3\}$ is an orthogonal basis of $C_0(L_\mathfrak{p})$. Then

$$\begin{aligned}\det(C_0(L_\mathfrak{p})) &= N(\mathbf{e}_1\mathbf{e}_2)N(\mathbf{e}_1\mathbf{e}_3)N(\mathbf{e}_2\mathbf{e}_3)\\ &= \mathbf{e}_1^2\mathbf{e}_2^2\mathbf{e}_1^2\mathbf{e}_3^2\mathbf{e}_2^2\mathbf{e}_3^2\\ &= Q(\mathbf{e}_1)^2Q(\mathbf{e}_2)^2Q(\mathbf{e}_3)^2\\ &= \det(L_\mathfrak{p})^2 .\end{aligned}$$

The result follows.

LEMMA 3.3. *Let $L^\sharp \subset V$ be the lattice dual to L. Then*

$$\delta_L L^\sharp = \Lambda_0 ,$$

where $\Lambda_0 = \{\, x \in C_0(L) \,:\, \mathrm{Tr}\,(x) = 0 \,\}$.

Proof. It is enough to prove the equality $\delta L^\sharp = \Lambda_0$ locally at all primes. Let $\mathfrak{p}$ be a prime of A and let $\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3$ be an orthogonal basis of $L_\mathfrak{p}$. Then $\{\mathbf{e}_1\mathbf{e}_2, \mathbf{e}_1\mathbf{e}_3, \mathbf{e}_2\mathbf{e}_3\}$ is a basis of $(\Lambda_0)_\mathfrak{p}$. Let $\mathbf{e}_i^\sharp = Q(\mathbf{e}_i)^{-1}\mathbf{e}_i$ for $i = 1,2,3$. It is easy to see that $\{\mathbf{e}_1^\sharp, \mathbf{e}_2^\sharp, \mathbf{e}_3^\sharp\}$ is a basis of $L_\mathfrak{p}^\sharp$ (in fact the dual basis). Since $\delta_L = u\mathbf{e}_1\mathbf{e}_2\mathbf{e}_3$, where $u \in A_\mathfrak{p}^\times$, we see by direct calculation $\delta_L\mathbf{e}_1^\sharp = u\mathbf{e}_2\mathbf{e}_3$, $\delta_L\mathbf{e}_2^\sharp = -u\mathbf{e}_1\mathbf{e}_3$, $\delta_L\mathbf{e}_3^\sharp = u\mathbf{e}_1\mathbf{e}_2$. This shows the desired equality.

PROPOSITION 3.4. *Let L, M be integral A-lattices of V. If $C_0(L) = C_0(M)$, then $M = L$.*

Proof. Recall that δ_L denotes the element of $C(L)$ such that $Z(C(L)) = A[\delta_L]$ and $\delta_L^2 = -\det L$. With this notation, if $C_0(L) = C_0(M)$ then by Lemma 3.3, we have $\delta_L L^\sharp = \delta_M M^\sharp$. Since $\delta_L = \delta_M\alpha$ for some $\alpha \in K^\times$, we have $L = \alpha M$. Now, by Proposition 3.2, we have $\det L = \det M$. This immediately implies $\alpha \in A^\times$ and hence $L = M$.

It is a standard fact (see e.g. [3, Theorem 3.1 and Corollary 2, Ch. 10]) that $uVu^{-1} = V$ for each $u \in C_0(V,Q)^\times$ and that the map $c_u \colon V \to V$ defined by $c_u(x) = uxu^{-1}$ is an automorphism of (V,Q). Moreover, the map $c \colon C_0(V,Q)^\times \to O(V)$ given by $u \mapsto c_u$ is a group homomorphism inducing the exact sequence

$$(3.1) \qquad 1 \longrightarrow K^{\times} \xrightarrow{i} C_0(V,Q)^{\times} \xrightarrow{c} \mathbf{SO}(V,Q) \longrightarrow 1\,.$$

PROPOSITION 3.5. *Let L and M be integral A-lattices in V. Then L and M are isometric if and only if the A-orders $C_0(L)$ and $C_0(M)$ are conjugate in $C_0(V,Q)$.*

Proof. Assume that L, M are isometric. Then $M = \sigma L$ for some $\sigma \in \mathbf{SO}(V,Q)$. By (3.1) we have $\sigma = c_u$ for some $u \in C_0(V,Q)^{\times}$. Thus $M = uLu^{-1}$, which implies that $C_0(M) = uC_0(L)u^{-1}$. Conversely, assume that $C_0(M) = uC_0(L)u^{-1}$. Then

$$C_0(uLu^{-1}) = uC_0(L)u^{-1} = C_0(M)\,.$$

By Proposition 3.4, $uLu^{-1} = M$.

THEOREM 3.6. *Let D be the determinant of a maximal lattice in (V,Q) and let Λ be an A-order of $C_0(V,Q)$ such that* $\det(\Lambda) = b^4D^2$ *for some $b \in A$. Then there exists an integral A-lattice $L \subset V$ such that $\Lambda = C_0(L)$.*

Proof. Let $M \subset V$ be a maximal lattice and let $\delta = b\delta_M$, so $\delta^2 = -b^2D$. Define $L = \delta{\Lambda_0}^{\sharp}$, where $\Lambda_0 = \{x \in \Lambda \,:\, \mathrm{Tr}\,(x) = 0\}$ and let ${\Lambda_0}^{\sharp}$ be the dual of Λ_0 with respect to the norm form N. By Lemma 3.3, it is enough to show that $\delta L^{\sharp} = \Lambda_0$. Let $C_0(V,Q)_0 = \{x \in C_0(V,Q) \,:\, \mathrm{Tr}\,(x) = 0\}$. For $x \in C_0(V,Q)_0$ we have $Q(\delta x) = (\delta x)^2 = \delta^2x^2 = -\delta^2N(x)$, so multiplication by δ in $C(V,Q)$ induces an isomorphism of quadratic spaces $(C_0(V,Q)_0, -\delta^2N) \xrightarrow{\simeq} (V,Q)$. It follows immediately from this observation that $\delta^{-1}L^{\sharp} = \delta^{-2}({\Lambda_0}^{\sharp})^{\sharp} = \delta^{-2}\Lambda_0$. Thus $\delta L^{\sharp} = \Lambda_0$ as desired.

COROLLARY 3.7. *Let $D \in A$ be a square-free polynomial and assume that V admits integral lattices of discriminant D. Suppose further that Q is anisotropic at all prime divisors of D. Then an integral lattice $L \subset V$ is maximal if and only if its even Clifford algebra $C_0(L)$ is a maximal order.*

Proof. Let L be a maximal lattice in V. Then $\det(L) = D$ and therefore by Proposition 3.2 we have $\det C_0(L) = D^2$. Notice that D^2 is the determinant of a maximal order since all its prime divisors are ramified in $C_0(V,Q)$ (Q is anisotropic at all these primes) and D is square-free. This is enough to ensure that $C_0(L)$ is maximal.

Conversely, if Λ is a maximal order, then by Theorem 3.6, $\Lambda = C_0(L)$ for some lattice L of determinant D.

PROPOSITION 3.8. *An element $a \in A$ relatively prime to* $\det L$ *is represented primitively by L if and only if $C_0(L)$ contains a primitive element λ such that $\lambda^2 = -aD$.*

Proof. Let $\Lambda = C_0(L)$. Suppose that $a \in A$ is such that $a = \mathbf{x}^2$ for some primitive $\mathbf{x} \in L$. Since a is prime to $\det L$, $\mathbf{x}$ is primitive in $L^\sharp$ as well. It follows that $\delta\mathbf{x}$ is primitive in $\delta L^\sharp = \Lambda_0$. Clearly $(\delta\mathbf{x})^2 = \delta^2\mathbf{x}^2 = -aD$. The converse is obvious.

4. AN IDÈLE ACTION ON PRIMITIVE REPRESENTATIONS

As in previous sections, (V, Q) denotes a ternary definite quadratic space over K. We assume throughout that the maximal lattices in V have square-free determinant that we denote by D. Recall that $\mathbf{A}_K$ denotes the *adèle ring* of K.

Let $a \in A$ relatively prime to D and let $\mathbf{v} \in V$ be a fixed vector with $Q(\mathbf{v}) = a$. We consider the set

$$\mathcal{L}_{\mathbf{v}} = \{L \, : \, L \subset V \text{ integral lattice}; \ \det L = D\, ; \ L \ni \mathbf{v} \text{ primitively}\}\,.$$

We denote by $\mathbf{SO}(V, Q)$ the group of orientation-preserving automorphisms of (V, Q), which we view as an algebraic group defined over K. Let $\mathbf{G}$ be the stabilizer of $\mathbf{v}$, which is a closed subgroup of $\mathbf{SO}(V, Q)$. It is clear that $\mathbf{G}(\mathbf{A}_K)$ acts on $\mathcal{L}_{\mathbf{v}}$ by restriction of the natural action of $\mathbf{SO}(V, Q)(\mathbf{A}_K)$ on the set of all A-lattices of V.

PROPOSITION 4.1. *The action of $\mathbf{G}(\mathbf{A}_K)$ on $\mathcal{L}_{\mathbf{v}}$ is transitive.*

Proof. Let $\mathfrak{p}$ be a prime of A and let $L, L' \in \mathcal{L}_{\mathbf{v}}$. Assume first that $\mathfrak{p} \nmid a$, where $a = Q(\mathbf{v})$. Then $A_\mathfrak{p}\mathbf{v}$ is an orthogonal factor of both $L_\mathfrak{p}$ and $L'_\mathfrak{p}$. Write $L_\mathfrak{p} = A_\mathfrak{p}\mathbf{v} \perp M_\mathfrak{p}$ and $L'_\mathfrak{p} = A_\mathfrak{p}\mathbf{v} \perp M'_\mathfrak{p}$. Since $L_\mathfrak{p}$ and $L'_\mathfrak{p}$ are isometric, so must be $M_\mathfrak{p}$ and $M'_\mathfrak{p}$ and hence there exists $\sigma_\mathfrak{p} \in \mathbf{G}(K_\mathfrak{p})$ such that $\sigma_\mathfrak{p} L_\mathfrak{p} = L'_\mathfrak{p}$.

Assume now that $\mathfrak{p} \mid a = Q(\mathbf{v})$. Since $\mathbf{v}$ is primitive in $L_\mathfrak{p}$, there exists $\mathbf{v}_2 \in L_\mathfrak{p}$ such that $B(\mathbf{v}, \mathbf{v}_2) \equiv 1 \pmod{\mathfrak{p}}$ and $Q(\mathbf{v}_2) \equiv 0 \pmod{\mathfrak{p}}$. Since $L_\mathfrak{p}$ is unimodular (recall that a and D are relatively prime), we can assume further by Hensel's Lemma that $Q(\mathbf{v}_2) = 0$. Replacing $\mathbf{v}_2$ by a suitable scalar multiple, we can also assume that $B(\mathbf{v}, \mathbf{v}_2) = 1$. Hence $\mathbf{v}$ and $\mathbf{v}_2$ span a unimodular binary lattice $N_\mathfrak{p}$ of determinant -1. Taking the orthogonal complement of $N_\mathfrak{p}$ in $L_\mathfrak{p}$ we get a vector $\mathbf{v}_3 \in L_\mathfrak{p}$ such that $\{\mathbf{v}, \mathbf{v}_2, \mathbf{v}_3\}$ is a basis of $L_\mathfrak{p}$.

The Gram matrix of Q in this basis is

$$\begin{pmatrix} a & 1 \\ 1 & 0 \end{pmatrix} \perp \langle -D \rangle . \tag{4.1}$$

The same construction yields vectors $\mathbf{v}_2', \mathbf{v}_3' \in L_\mathfrak{p}'$ such that $\{\mathbf{v}, \mathbf{v}_2', \mathbf{v}_3'\}$ is a basis of $L_\mathfrak{p}'$ and the Gram matrix of Q in this basis is also as in (4.1). Clearly the linear map $\sigma_\mathfrak{p} \colon V_\mathfrak{p} \to V_\mathfrak{p}$ given by $\sigma_\mathfrak{p}\mathbf{v} = \mathbf{v}, \sigma_\mathfrak{p}\mathbf{v}_2 = \mathbf{v}_2', \sigma_\mathfrak{p}\mathbf{v}_3 = \mathbf{v}_3'$ is in $\mathbf{G}(K_\mathfrak{p})$ and satisfies $\sigma_\mathfrak{p} L_\mathfrak{p} = L_\mathfrak{p}'$.

Consider now the natural exact sequence of algebraic groups over K (see e.g. [10, Ch. 8, §23] for the general case)

$$1 \longrightarrow \mathbf{GL}_1(K) \xrightarrow{i} \mathbf{GL}_1(C_0(V,Q)) \xrightarrow{c} \mathbf{SO}(V,Q) \longrightarrow 1 , \tag{4.2}$$

where i is the natural inclusion and $c_u(\mathbf{x}) = u\mathbf{x}u^{-1}$.

Let $E = Z_{C_0(V,Q)}(\mathbf{v})$. Restricting c to $\mathbf{GL}_1(E)$ we get an exact sequence of algebraic groups over K

$$1 \longrightarrow \mathbf{GL}_1(K) \xrightarrow{i} \mathbf{GL}_1(E) \xrightarrow{c} \mathbf{G} \longrightarrow 1 . \tag{4.3}$$

LEMMA 4.2. *Let $\mathbf{J}_K$ and $\mathbf{J}_E$ denote the idèle groups of K and E respectively. Then we have an exact sequence*

$$1 \longrightarrow \mathbf{J}_K \xrightarrow{i} \mathbf{J}_E \xrightarrow{c} \mathbf{G}(\mathbf{A}_K) \longrightarrow 1 . \tag{4.4}$$

Proof. The result follows easily by taking points over the adèle ring $\mathbf{A}_K$ in (4.3) and taking the natural identifications $\mathbf{J}_K = \mathbf{GL}_1(K)(\mathbf{A}_K)$ and $\mathbf{J}_E = \mathbf{GL}_1(E)(\mathbf{A}_K)$. The surjectivity of $c \colon \mathbf{J}_E \to \mathbf{G}(\mathbf{A}_K)$ is easy to verify directly.

We let now $\mathbf{J}_E$ act on $\mathcal{L}_\mathbf{v}$ via $c \colon \mathbf{J}_E \to \mathbf{G}(\mathbf{A}_K)$. It is clear from Proposition 4.1 that this action is transitive. We shall now investigate the stabilizer of a lattice $L \in \mathcal{L}_\mathbf{v}$ for this action. Let $B = A[\delta_L \mathbf{v}] \subset E$.

PROPOSITION 4.3. *Let $L \in \mathcal{L}_\mathbf{v}$ and let $\mathfrak{p}$ be a prime of A. Let $H_\mathfrak{p} = \{u \in E_\mathfrak{p}^\times : uL_\mathfrak{p}u^{-1} = L_\mathfrak{p}\}$.*

(i) *If $\mathfrak{p} \nmid D$, then $H_\mathfrak{p} = K_\mathfrak{p}^\times B_\mathfrak{p}^\times$.*

(ii) *If $\mathfrak{p} \mid D$, then $H_\mathfrak{p} = E_\mathfrak{p}^\times$.*

Proof. (i) Suppose $\mathfrak{p} \nmid D$. Then $\det C_0(L_\mathfrak{p})$ is a $\mathfrak{p}$-unit by Proposition 3.2 and hence $C_0(L_\mathfrak{p})$ is a maximal order in $C_0(V_\mathfrak{p}) \simeq M_2(K_\mathfrak{p})$. Thus $H_\mathfrak{p} = (K_\mathfrak{p}^\times C_0(L_\mathfrak{p})^\times) \cap E_\mathfrak{p}^\times = K_\mathfrak{p}^\times (C_0(L_\mathfrak{p})^\times \cap E_\mathfrak{p}^\times)$. By the proof of Proposition 3.8, $\delta\mathbf{v}$ is primitive in $C_0(L_\mathfrak{p})$, which implies $C_0(L_\mathfrak{p})^\times \cap E_\mathfrak{p}^\times = B_\mathfrak{p}^\times$.

(ii) Suppose $\mathfrak{p} \mid D$. We have an orthogonal decomposition $V = K\mathbf{v} \perp W$ and since $\mathfrak{p} \nmid a$ (a and D are assumed to be relatively prime), we have a corresponding integral orthogonal decomposition $L_\mathfrak{p} = A_\mathfrak{p}\mathbf{v} \perp N_\mathfrak{p}$. Hence we can identify $E_\mathfrak{p}$ with $C_0(W)$ and $B_\mathfrak{p}$ with $C_0(N_\mathfrak{p})$. Multiplication by $C_0(N_\mathfrak{p}) = B_\mathfrak{p}$ in $C(V,Q)$ makes $N_\mathfrak{p}$ into a $B_\mathfrak{p}$-module (see [9]) which is free of rank one ($B_\mathfrak{p}$ is a maximal order since D is square-free). It is easy to see by direct computation that for $u \in E_\mathfrak{p} = C_0(W_\mathfrak{p})$ and $\mathbf{x} \in W_\mathfrak{p}$ we have $\mathbf{x}u = \overline{u}\mathbf{x}$, where $u \mapsto \overline{u}$ is the canonical involution of $E_\mathfrak{p}$.

For $u \in E_\mathfrak{p}^\times$ we have the following chain of equivalences

$$\begin{aligned} u \in H_\mathfrak{p} &\iff uN_\mathfrak{p}u^{-1} = N_\mathfrak{p} \\ &\iff u\overline{u}^{-1}N_\mathfrak{p} = N_\mathfrak{p} \\ &\iff u\overline{u}^{-1} \in B_\mathfrak{p}^\times . \end{aligned}$$

Since $B_\mathfrak{p}$ is ramified over $A_\mathfrak{p}$, all $u \in E_\mathfrak{p}^\times$ fulfill the last condition.

We can now describe the *stability subgroups* for the action of $\mathbf{J}_E$ on $\mathcal{L}_\mathbf{v}$:

PROPOSITION 4.4. *Let $L \in \mathcal{L}_\mathbf{v}$ and let $S = \{\mathfrak{p} : \mathfrak{p} \mid D\} \cup \{\infty\}$. Then*

$$(\mathbf{J}_E)_L = \mathbf{J}_K\Bigg(\prod_{\mathfrak{p}\in S} E_\mathfrak{p}^\times \times \prod_{\mathfrak{p}\notin S} B_\mathfrak{p}^\times\Bigg).$$

Proof. This is an immediate consequence of Proposition 4.3.

COROLLARY 4.5. *The Picard group* Pic$(B[1/D])$ *acts simply transitively on the set $\mathcal{L}_\mathbf{v}/E^\times$. In particular*

$$\left|\mathcal{L}_\mathbf{v}/E^\times\right| = \left|\mathrm{Pic}(B[1/D])\right|.$$

Proof. It follows from Propositions 4.1 and 4.4 that $\mathbf{J}_E/E^\times(\mathbf{J}_E)_L$ acts simply transitively on $\mathcal{L}_\mathbf{v}/E^\times$. Since A is a PID, we have

$$\mathbf{J}_K = K^\times(K_\infty \times \prod_{\mathfrak{p}\neq\infty} A_\mathfrak{p}^\times) \subset E^\times\Bigg(\prod_{\mathfrak{p}\in S} E_\mathfrak{p}^\times \times \prod_{\mathfrak{p}\notin S} B_\mathfrak{p}^\times\Bigg).$$

Using the inclusion above and Proposition 4.4, we get

$$E^\times(\mathbf{J}_E)_L = E^\times\Bigg(\prod_{\mathfrak{p}\in S} E_\mathfrak{p}^\times \times \prod_{\mathfrak{p}\notin S} B_\mathfrak{p}^\times\Bigg),$$

which proves the corollary.

5. Weighted sum of representation numbers

Let $L_1, L_2, \dots, L_h \in \mathcal{L}_{\mathbf{v}}$ be representatives of all isometry classes in $\mathcal{L}_{\mathbf{v}}$. Let

$$R_i = \{\mathbf{x} \in L_i \, : \, Q(\mathbf{x}) = a \ \text{ and } \ \mathbf{x} \text{ is primitive in } L_i\}.$$

We define a map $\psi_i \colon R_i \to \mathcal{L}_{\mathbf{v}}/E^\times$ as follows: for $\mathbf{x} \in R_i$, choose $\sigma \in \mathbf{SO}(V, Q)$ such that $\sigma(\mathbf{x}) = \mathbf{v}$ and set

$$\psi_i(\mathbf{x}) = (\sigma L_i), \tag{5.1}$$

where (σL_i) denotes the image of σL_i in $\mathcal{L}_{\mathbf{v}}/E^\times$. It is readily checked that (σL_i) does not depend on the choice of σ. Indeed, if $\sigma, \tau \in \mathbf{SO}(V, Q)$ are such that $\sigma(\mathbf{x}) = \tau(\mathbf{x}) = \mathbf{v}$, then $\sigma\tau^{-1} = c_u$ for some $u \in E^\times$ and hence $\sigma L_i = c_u \tau L_i$. This shows that $(\sigma L_i) = (\tau L_i)$.

The group $SO(L_i)$ acts naturally on R_i and we denote by $R_i/SO(L_i)$ the orbit space for this action.

Proposition 5.1. *Let $\psi_i \colon R_i \to \mathcal{L}_{\mathbf{v}}/E^\times$ ($i = 1, \dots, h$) be the maps defined in* (5.1).

(i) *Each ψ_i induces an injective map $\overline{\psi}_i \colon R_i/SO(L_i) \hookrightarrow \mathcal{L}_{\mathbf{v}}/E^\times$.*

(ii) *$\mathcal{L}_{\mathbf{v}}/E^\times$ is the disjoint union of the images $\psi_i(R_i)$ ($i = 1, \dots, h$).*

Proof. (i) It is clear from the definition (5.1) of ψ_i that $\psi_i(\rho\mathbf{x}) = \psi_i(\mathbf{x})$ for $\rho \in SO(L_i)$, so ψ_i induces a map $\overline{\psi}_i \colon R_i/SO(L_i) \to \mathcal{L}_{\mathbf{v}}/E^\times$. We shall see that this map is injective. Suppose $\psi_i(\mathbf{x}) = \psi_i(\mathbf{y})$ and let $\sigma, \tau \in \mathbf{SO}(V, Q)$ be such that $\sigma(\mathbf{x}) = \tau(\mathbf{y}) = \mathbf{v}$. Then, by the definition of ψ_i, we have $\sigma L_i = c_u \tau L_i$ for some $u \in E^\times$. Replacing τ by $c_u\tau$ does not affect the condition $\tau(\mathbf{y}) = \mathbf{v}$, so we can assume that $\sigma L_i = \tau L_i$. Thus $\tau^{-1}\sigma \in SO(L_i)$ and $\tau^{-1}\sigma(\mathbf{x}) = \mathbf{y}$.

(ii) It is enough to observe that each of the sets $\psi_i(R_i)$ consists exactly of the classes of $\mathcal{L}_{\mathbf{v}}/E^\times$ represented by lattices isometric to L_i, so these sets are pairwise disjoint. Since $L_1, \dots, L_h$ represent all isometry classes in $\mathcal{L}_{\mathbf{v}}$, their union is $\mathcal{L}_{\mathbf{v}}/E^\times$.

Corollary 5.2. *Let $\rho_i = |R_i/SO(L_i)|$, where $i = 1, \dots, h$. Then*

$$\sum_{i=1}^{h} \rho_i = |\mathrm{Pic}(B[1/D])|, \tag{5.2}$$

where $B = A[\delta\mathbf{v}] \simeq A[\sqrt{-aD}]$.

Proof. This follows immediately from Corollary 4.5 and Proposition 5.1.

LEMMA 5.3. (i) *If* $\deg(a) > 0$ *then the group* $SO(L_i)$ *acts freely on* R_i. (ii) *If* $\deg(a) = 0$ *then the stabilizers* $SO(L_i)_{\mathbf{x}}$ *have order* 2 *for all* $\mathbf{x} \in R_i$.

Proof. (i) Set $L = L_i$ for simplicity of the notation. We have a natural embedding $SO(L)_{\mathbf{v}} \hookrightarrow SO(M)$. Notice that M cannot be unimodular since in this case $A\mathbf{v}$ would be an orthogonal factor of L, which would cause a and D to differ by a unit of A, contradicting that a and D are relatively prime. So M is a primitive definite binary lattice over A with $\deg(\det M) > 0$. It is an easy exercise to show that in this case $SO(M) = \{\pm 1_M\}$. Hence $|SO(L)_{\mathbf{v}}| \leq 2$.

(ii) Suppose that a is a unit. Then $L = A\mathbf{v} \perp M$ and $SO(L)_{\mathbf{v}} \simeq SO(M)$. Conversely, if $SO(L)_{\mathbf{v}} \simeq SO(M)$, let σ be the nontrivial element of $SO(L)_{\mathbf{v}}$ and let $e = (1+\sigma)/2$ and $f = (1-\sigma)/2$. It is clear that e, f are idempotents and $e + f = 1$. Since 2 is invertible in A, we have $L = eL + fL$ and this decomposition is orthogonal since σ is an isometry. Also $A\mathbf{v}$ is contained in eL, but since $\mathbf{v}$ is primitive we must have $A\mathbf{v} = eL$. Hence $A\mathbf{v}$ is an orthogonal factor of L, which implies that a divides D. Since a and D are relatively prime, this is possible only if a is a unit.

COROLLARY 5.4. *The numbers* ρ_i *of Corollary* 5.2 *are given by*

$$\rho_i = \begin{cases} \dfrac{|R_i|}{|SO(L_i)|} & \textit{if } \deg(a) > 0\,, \\[2ex] \dfrac{2|R_i|}{|SO(L_i)|} & \textit{if } \deg(a) = 0\,. \end{cases}$$

Proof. The result follows immediately from Lemma 5.3 and the orbit-stabilizer theorem.

We shall now describe the right-hand side of (5.2). Recall that $B \simeq A[\lambda]$, where $\lambda^2 = -aD$. To simplify the notation, let $C = B[1/D]$. There is a natural map $\mathrm{Pic}(B) \to \mathrm{Pic}(C)$, which is readily seen to be surjective. We shall investigate its kernel.

LEMMA 5.5. *With the notation above,*
(i) *if* $\deg(a) > 0$, *then* $C^\times = A[1/D]^\times$;
(ii) *if* $\deg(a) = 0$, *then* $C^\times = A[1/D]^\times \langle \lambda \rangle$, *where* $\langle \lambda \rangle$ *is the multiplicative subgroup generated by* λ.

Proof. Let $z \in C^\times$. Multiplying z by a suitable unit of $A[1/D]$, we can assume without loss of generality that z is of the form $z = x + y\lambda$ with $x, y \in A$

and $\gcd(x,y,D)=1$. Since z is a unit, its norm $e:=N(z)=x^2+aDy^2$ is a product of primes dividing D. If p is a prime divisor of e, then p divides x and we get the equation $px_0^2+aD_0y^2=e_0$, where $x_0=x/p$, $D_0=D/p$ and $e_0=e/p$. If $p\mid e_0$, then $p\mid D_0$ since a and D are relatively prime, but this is a contradiction with the fact that D is square-free. Hence e is square-free and therefore e divides D. Letting $x_1=x/e$ and $D_1=D/e$ in the original equation, we get $ex_1^2+aD_1y^2=1$. Since the form $ex_1^2+aD_1y^2$ is definite ($-aD$ is not a square in K_∞) we have that either e and x_1 are units and $y=0$ or y and aD_1 are units and $x_1=0$. In the first case $z=x\in A^\times$. The second case holds only if a is a unit and in this situation $z=y\lambda$ with $y\in A^\times$.

LEMMA 5.6. *Let r be the number of prime divisors of D. The kernel of the natural map* $\operatorname{Pic}(B)\to\operatorname{Pic}(C)$ *is an elementary 2-group of order 2^r if* $\deg(a)>0$ *and of order 2^{r-1} if* $\deg(a)=0$. *In particular*

$$|\operatorname{Pic}(C)|=\begin{cases}2^{-r}\,|\operatorname{Pic}(B)| & \textit{if } \deg(a)>0\,,\\ 2^{-r+1}\,|\operatorname{Pic}(B)| & \textit{if } \deg(a)=0\,.\end{cases}\tag{5.3}$$

Proof. We shall reduce the proof to the case where a is square-free, or equivalently, to the case where the orders involved are integrally closed.

Let $\overline{B}$ and $\overline{C}$ be the integral closures of B and C in E respectively. Write $a=a_0a_1^2$, where a_0 is square-free. We have a commutative diagram where the rows are exact and the vertical maps f and $\overline{f}$ are onto:

$$\begin{tikzcd}
1 \arrow[r] & \overline{B}^\times/B^\times \arrow[r] \arrow[d] & \prod_{p|a_1}\overline{B}_{\mathfrak{p}}^\times/B_{\mathfrak{p}}^\times \arrow[r] \arrow[d, equal] & \operatorname{Pic}(B) \arrow[r] \arrow[d, "f"] & \operatorname{Pic}(\overline{B}) \arrow[r] \arrow[d, "\overline{f}"] & 1 \\
1 \arrow[r] & \overline{C}^\times/C^\times \arrow[r] & \prod_{p|a_1}\overline{C}_{\mathfrak{p}}^\times/C_{\mathfrak{p}}^\times \arrow[r] & \operatorname{Pic}(C) \arrow[r] & \operatorname{Pic}(\overline{C}) \arrow[r] & 1\,.
\end{tikzcd}$$

Note that since a and D are relatively prime, $B_{\mathfrak{p}}=C_{\mathfrak{p}}$ for $p\mid a_1$. Clearly $\overline{B}^\times=B^\times=A^\times$ since $\deg(D)>0$. Since $\overline{C}=A[1/D,\lambda_0]$, where $\lambda_0^2=-a_0D$, by Lemma 5.5 we have $\overline{C}^\times/C^\times=\{1\}$ except when $\deg(a_0)=0$ and $\deg(a)>0$, in which case we have $\overline{C}^\times/C^\times=\langle\lambda_0\rangle/\langle\lambda_0^2\rangle\simeq\mathbf{Z}/2\mathbf{Z}$. It follows immediately from the diagram that

$$|\ker f|=\begin{cases}2\,\left|\ker\overline{f}\right| & \text{if } \deg(a_0)=0 \text{ and } \deg(a)>0\,,\\ \left|\ker\overline{f}\right| & \text{in all other cases}\,.\end{cases}\tag{5.4}$$

We shall now determine $\ker\bar{f}$. Let p_i $(i = 1, \dots, r)$ be the prime divisors of D. Since $\bar{B} = A[\lambda_0]$, where $\lambda_0^2 = a_0 D$, these primes are ramified in $\bar{B}$, i.e. $p_i \bar{B} = \mathfrak{p}_i^2$, where $\mathfrak{p}_i$ is a prime of $\bar{B}$. The elements of $\ker\bar{f}$ are represented by ideals $\mathfrak{a}$ of $\bar{B}$ satisfying $\mathfrak{a}\bar{C} = \bar{C}$, so such an ideal is a product of primes diving D. This shows that $\ker\bar{f}$ is a 2-elementary abelian group generated by the classes of the $\mathfrak{p}_i$ in $\mathrm{Pic}(\bar{B})$, which we will denote by $[\mathfrak{p}_i]$.

Any relation among the $[\mathfrak{p}_i]$ must be of the form

$$[\mathfrak{p}_{i_1}][\mathfrak{p}_{i_2}]\dots[\mathfrak{p}_{i_k}] = 1\,,$$

where $\{i_1, i_2, \dots, i_k\} \subset \{1, 2, \dots, r\}$. Equivalently,

$$\mathfrak{p}_{i_1}\mathfrak{p}_{i_2}\dots\mathfrak{p}_{i_k} = \omega\bar{B} \tag{5.5}$$

for some $\omega \in \bar{B}$. Since $\mathfrak{p}_i^2 = p_i\bar{B}$, it follows that $\omega^2 u \in A$ for some $u \in \bar{B}^{\times}$. But $\bar{B}^{\times} = A^{\times}$ since $-a_0 D$ is not a square in K_∞ and $\deg(D) > 0$. Consequently, $\omega^2 \in A$ and $\omega^2 \mid a_0 D$. The second condition ensures that $\omega \notin A$, so $\omega = b\lambda_0$ for some $b \in A$. Then we also have $a_0 D \mid \omega^2$; this is possible only if $\{i_1, i_2, \dots, i_k\} = \{1, 2, \dots, r\}$ and $\deg a_0 = 0$. Thus

$$\left|\ker\bar{f}\right| = \begin{cases} 2^{r-1} & \text{if } \deg(a_0) = 0\,, \\ 2^r & \text{if } \deg(a_0) > 0\,. \end{cases} \tag{5.6}$$

We conclude by putting together (5.4) and (5.6).

We can now state and prove the formula for the weighted sum of primitive representation numbers. For a definite A-lattice (L, Q) and a polynomial $a \in A$, we denote by $R(L, a)$ the number of solutions of the equation $Q(\mathbf{x}) = a$ with $\mathbf{x}$ *primitive* in L.

THEOREM 5.7. *Let D be a square-free non-constant polynomial and let (V, Q) be a ternary quadratic space over K of determinant D. Let $L_1, \dots, L_h$ be representatives of all the isometry classes of integral A-lattices in V of determinant D and let a be a polynomial relatively prime to D such that $-aD \notin K_\infty^{\times 2}$. Then*

$$\sum_{i=1}^{h} \frac{R(L_i, a)}{|SO(L_i)|} = 2^{-r}\left|\mathrm{Pic}(A[\sqrt{-aD}])\right|\,, \tag{5.7}$$

where r is the number of prime factors of D.

Proof. The formula follows from Corollaries 5.4 and 5.2 together with (5.3). The case $\deg(a) = 0$ requires special consideration in the computations, but the end formula turns out to be the same in both cases.

6. THE EPSTEIN ZETA FUNCTION

In this and the next sections we will encounter functions of a complex variable s that are naturally functions of q^{-s}. If F is such a function, we shall write F^* for the unique function such that $F(s) = F^*(q^{-s})$.

As in previous sections, (V, Q) denotes a definite ternary quadratic space over K. Let $L \subset V$ be an integral A-lattice. The *Epstein zeta function* of L is defined by

$$Z_L(s) = \sum_{\mathbf{x} \in L \setminus \{0\}} |Q(\mathbf{x})|^{-s}. \tag{6.1}$$

Collecting the terms of the same degree, we have

$$Z_L(s) = \sum_{k=0}^{\infty} \alpha_k(L) q^{-ks},$$

where

$$\alpha_k(L) = \left|\{\mathbf{x} \in L \,:\, \deg Q(\mathbf{x}) = k\}\right|.$$

PROPOSITION 6.1. *Let $\delta = \deg \det(L)$. For $k > \delta$ we have*

$$\alpha_k(L) = \begin{cases} (1 - q^{-1})\, q^{(3k-\delta+4)/2} & \text{if } k \equiv \delta \pmod 2, \\ (1 - q^{-2})\, q^{(3k-\delta+5)/2} & \text{if } k \not\equiv \delta \pmod 2. \end{cases}$$

Proof. Let μ_i $(i = 1, 2, 3)$ be the successive minima of L and let $L_k = \{\mathbf{x} \in L : \deg Q(\mathbf{x}) \leq k\}$. It is easy to see that for $k \geq \delta$,

$$\dim_{\mathbf{F}_q} L_k = \lfloor (k - \mu_1)/2 \rfloor + \lfloor (k - \mu_2)/2 \rfloor + \lfloor (k - \mu_3)/2 \rfloor + 3$$

(see [2, §3]). Since $\delta = \mu_1 + \mu_2 + \mu_3$, we have

$$|L_k| = \begin{cases} q^{(3k-\delta+4)/2} & \text{if } k \equiv \delta \pmod 2, \\ q^{(3k-\delta+5)/2} & \text{if } k \not\equiv \delta \pmod 2. \end{cases}$$

The proposition follows from the simple observation that $\alpha_k(L) = |L_k| - |L_{k-1}|$.

COROLLARY 6.2. *$Z_L(s)$ is a rational function of $u = q^{-s}$ with simple poles at $u = \pm q^{-3/2}$.*

Proof. Let $Z_L^*(u) = Z_L(s)$ and let $P(u) = \sum_{k=0}^{\delta-1} \alpha_k(L) u^k$. Thus, using

Proposition 6.1, we have:

$$\begin{aligned} Z_L^*(u) &= P(u) + q^{\delta+2}(1-q^{-1})u^{\delta}\sum_{l=0}^{\infty}(q^3u^2)^l + q^{\delta+4}(1-q^{-2})\,u^{\delta+1}\sum_{l=0}^{\infty}(q^3u^2)^l \\ &= P(u) + q^{\delta}(q-1)\,q\frac{(1+qu+q^2u)u^{\delta}}{1-q^3u^2}\,. \end{aligned}$$

DEFINITION 6.3. We shall say that two formal power series $f(u)$ and $g(u)$ in u are *equivalent* if $f(u)-g(u)$ is a polynomial in u. We shall denote this equivalence relation by $f(u)\sim g(u)$. Similarly, two meromorphic functions $F(s)$ and $G(s)$ will be said to be *equivalent* if $F(s)-G(s)$ is a polynomial in q^{-s}.

PROPOSITION 6.4. *Let M and L be A-lattices in V and assume that $L\subset M$. Then*

$$Z_M(s)\sim [M:L]\;Z_L(s)\,,$$

where $[M:L]$ is the index of L in M.

Proof. Let k be large enough so that the restriction of the canonical projection $M\to M/L$ to M_k is onto. Then $[M_k:L_k]=[M:L]$ for all k large enough. It follows that $\alpha_k(M)=|M_k|-|M_{k-1}|=[M:L]\,(|L_k|-|L_{k-1}|)=[M:L]\alpha_k(L)$ for k large enough.

DEFINITION 6.5. Let $\chi\colon L\to \mathbf{C}$ be any function. The *Epstein zeta function twisted by χ* is defined by

$$Z_L(s,\chi)=\sum_{\mathbf{x}\in L\setminus\{0\}}\chi(\mathbf{x})|Q(\mathbf{x})|^{-s}. \tag{6.2}$$

LEMMA 6.6. *Let $L\subset V$ be an integral lattice of square-free determinant D. For $d\mid D$, let χ_d be the characteristic function of the set $\{\mathbf{x}\in L\,:\,Q(\mathbf{x})\equiv 0 \pmod d\}$. Let d_0 be the product of the primes dividing d at which Q is isotropic and let d_1 be the product of the primes dividing d at which Q is anisotropic. Then*

$$Z_L(s,\chi_d)\sim (2|d_0|^{-1}|d_1|^{-2}-|d|^{-2})Z_L(s)\,.$$

Proof. Let $\mathfrak{p}$ be a prime divisor of D. If Q is isotropic at $\mathfrak{p}$ then $L_{\mathfrak{p}}$ has a basis $\{\mathbf{v}_1,\mathbf{v}_2,\mathbf{v}_3\}$ over $A_{\mathfrak{p}}$ such that $Q(x\mathbf{v}_1+y\mathbf{v}_2+z\mathbf{v}_3)=xy-Dz^2$. For each $d\mid D$ we define two sublattices $L^{(d,i)}$ $(i=1,2)$ of L by their local components as follows:

$$L_{\mathfrak{p}}^{(d,i)} = \begin{cases} A_{\mathfrak{p}}\mathbf{v}_i + \mathfrak{p}L_{\mathfrak{p}}^{\sharp} & \text{if } \mathfrak{p} \mid d_0\,, \\ \mathfrak{p}L_{\mathfrak{p}}^{\sharp} & \text{if } \mathfrak{p} \mid d_1\,, \\ L_{\mathfrak{p}} & \text{if } \mathfrak{p} \nmid d\,. \end{cases}$$

It is easy to see from the definition of $L^{(d,i)}$ that for $\mathbf{x} \in L$

$$Q(\mathbf{x}) \equiv 0 \pmod{d} \iff \mathbf{x} \in L^{(d,1)} \cup L^{(d,2)}.$$

Hence

$$Z_L(s,\chi_d)(s) = Z_{L^{(d,1)}}(s) + Z_{L^{(d,2)}}(s) - Z_{L^{(d,1)}\cap L^{(d,2)}}(s)\,.$$

Since $d = d_0 d_1$ we also have

$$[L : L^{(d,i)}] = |d_0|\,|d_1|^2 \quad \text{and} \quad [L : L^{(d,1)} \cap L^{(d,2)}] = |d|^2\,.$$

We finish by applying Proposition 6.4.

For $d \in A \setminus \{0\}$ we define

$$M_d(s) = \sum_{e|d} \mu(e)|e|^{-s}, \tag{6.3}$$

where μ is the *Möbius function*. It is easy to see that $M_d(s)$ has a product decomposition

$$M_d(s) = \prod_{p|d}(1 - |p|^{-s})\,.$$

The function $M_d(s)$ defined in (6.3) will play an important role in many subsequent computations.

LEMMA 6.7. *Write $D = D_0D_1$, where D_0 is the product of the isotropic primes dividing D and D_1 is the product of the anisotropic primes dividing D. Let ψ be the characteristic function of the set $\{\mathbf{x} \in L \,:\, \gcd(Q(\mathbf{x}), D) = 1\}$. Then*

$$Z_L(s,\psi) \sim \big(2M_{D_0}(1)M_{D_1}(2) - M_D(2)\big)\, Z_L(s)\,.$$

Proof. Recall that χ_d denotes the characteristic function of the set

$$\{\mathbf{x} \in L \setminus \{0\} \,:\, Q(\mathbf{x}) \equiv 0 \pmod{d}\}.$$

Notice that χ_d as a function of d is multiplicative, i.e. if $(d,e) = 1$, then

$\chi_{de} = \chi_d \chi_e$. The functions ψ and χ_d are related by the identity

$$\begin{aligned}\psi &= \prod_{\substack{p \mid D \\ p \text{ prime}}} (1 - \chi_p) \\ &= \sum_{d \mid D} \mu(d) \chi_d \,.\end{aligned}$$

It follows immediately that

$$Z_L(s, \psi) = \sum_{d \mid D} \mu(d) Z_L(s, \chi_d) \,.$$

Hence, by Lemma 6.6, we have

$$\begin{aligned} Z_L(s, \psi) &\sim \sum_{\substack{d_0 \mid D_0 \\ d_1 \mid D_1}} \mu(d_0 d_1)(2|d_0|^{-1}|d_1|^{-2} - |d|^{-2}) Z_L(s) \\ &= \big(2M_{D_0}(1) M_{D_1}(2) - M_D(2)\big) \, Z_L(s) \,.\end{aligned}$$

Recall that the *content* of a vector $\mathbf{x} \in L \setminus \{0\}$ is the monic polynomial $c(\mathbf{x}) \in A$ such that $c(\mathbf{x}) A\mathbf{x} = K\mathbf{x} \cap L$. A vector $\mathbf{x} \in L$ is *primitive* if $c(\mathbf{x}) = 1$.

LEMMA 6.8. *Let ϕ be the characteristic function of the set $\{\mathbf{x} \in L : \mathbf{x}$ is primitive$\}$. Then*

$$Z_L(s, \psi) = M_D(2s) \, \zeta(2s) \, Z_L(s, \phi\psi) \,,$$

where ζ is the zeta function of A.

Proof. Collecting the terms of equal content in the defining sum for $Z_L(s, \psi)$ we have

$$\begin{aligned} Z_L(s, \psi) &= \sum_{(d,D)=1} \sum_{c(\mathbf{x})=d} \psi(\mathbf{x}) |Q(\mathbf{x})|^{-s} \\ &= \sum_{(d,D)=1} \sum_{c(\mathbf{y})=1} \psi(\mathbf{y}) |Q(\mathbf{y})|^{-s} |d|^{-2s} \\ &= \Big(\sum_{(d,D)=1} |d|^{-2s} \Big) \, Z_L(s, \phi\psi) \\ &= \Big(\prod_{p \mid D} (1 - |p|^{-2s}) \Big) \, \zeta(2s) Z_L(s, \phi\psi) \\ &= M_D(2s) \, \zeta(2s) \, Z_L(s, \phi\psi) \,.\end{aligned}$$

In order to prove the main theorem of this section, we need the following easy lemma from complex analysis.

LEMMA 6.9. *Let g be a function analytic on the disk $|z| < R$, where $R > 1$, and let $g^+(z) = (g(z) + g(-z))/2$ and $g^-(z) = (g(z) - g(-z))/2$. Let $f(z) = g(z)/(1 - z^2)$ and consider the Taylor series expansion of $f(z)$ at $z = 0$:*

$$f(z) = \sum_{n=0}^{\infty} a_n z^n \quad \textit{for } |z| < 1 .$$

Then the sequences $\{a_{2k}\}$ and $\{a_{2k+1}\}$ converge, and

$$\lim_{k\to\infty} a_{2k} = g^+(1) \qquad \textit{and} \qquad \lim_{k\to\infty} a_{2k+1} = g^-(1) .$$

Proof. We leave the proof as an exercise.

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

THEOREM 6.10. *Let*

$$\beta_k(L) = \#\{\mathbf{x} \in L \setminus \{0\} : \deg Q(\mathbf{x}) = k,\ (Q(\mathbf{x}), D) = 1,\ c(\mathbf{x}) = 1\}.$$

Then the sequences $\beta_{\delta+2m}(L)\, q^{-3m}$ and $\beta_{\delta+2m+1}(L)\, q^{-3m}$ converge and

$$\lim_{m\to\infty} \frac{\beta_{\delta+2m}(L)}{q^{3m}} = \frac{2M_{D_0}(1)M_{D_1}(2) - M_D(2)}{M_D(3)\zeta(3)}(1 - q^{-1})q^{\delta+2}$$

$$\lim_{m\to\infty} \frac{\beta_{\delta+2m+1}(L)}{q^{3m}} = \frac{2M_{D_0}(1)M_{D_1}(2) - M_D(2)}{M_D(3)\zeta(3)}(1 - q^{-2})q^{\delta+4}.$$

Proof. Notice that $\beta_k(L)$ is the coefficient of order k of $Z^*_L(u, \phi\psi)$. To simplify notation, we let $C = 2M_{D_0}(1)M_{D_1}(2) - M_D(2)$. Putting together Lemmas 6.7 and 6.8 we get

$$M^*_D(u^2)\zeta^*(u^2)Z^*_L(u, \phi\psi) = CZ^*_L(u) + F(u) ,$$

where $F(u)$ is a polynomial in u. Notice that the zeros of $M^*_D(u^2)$ lie on the circle $|u| = 1$ and that $\zeta^*(u^2) = 1/(1 - qu^2)$ has no zeros. We get

$$Z^*_L(u, \phi\psi) = \frac{CZ^*_L(u)}{M^*_D(u^2)\zeta^*(u^2)} + G(u) , \tag{6.4}$$

where $G(u)$ is analytic on the disk $|u| < 1$. The only poles of $Z^*_L(u, \phi\psi)$ on this disk are $u = \pm q^{-3/2}$.

Notice that $G(q^{-3/2}z)$ is analytic on the disk $|z| < q^{3/2}$, so its Taylor series at the origin converges for $z = 1$. Hence the Taylor coefficients of $G(q^{-3/2}z)$ tend to 0. Multiplying (6.4) throughout by u^δ and applying Lemma 6.9 to $u^\delta Z_L^*(u)/(M_D^*(u^2)\zeta^*(u^2))$ with $u = q^{-3/2}z$, we get

$$\begin{aligned}\lim_{m\to\infty} \frac{\beta_{\delta+2m}(L)}{q^{3m}} &= \frac{C}{M_D(3)\zeta(3)} \lim_{m\to\infty} \frac{\alpha_{\delta+2m}(L)}{q^{3m}} \\ &= \frac{C}{M_D(3)\zeta(3)}(1-q^{-1})q^{\delta+2}.\end{aligned}$$

Similarly,

$$\begin{aligned}\lim_{m\to\infty} \frac{\beta_{\delta+2m+1}(L)}{q^{3m}} &= \frac{C}{M_D(3)\zeta(3)} \lim_{m\to\infty} \frac{\alpha_{\delta+2m+1}(L)}{q^{3m}} \\ &= \frac{C}{M_D(3)\zeta(3)}(1-q^{-2})q^{\delta+4}.\end{aligned}$$

7. Averages of class numbers

Let $D \in A$ be a square-free polynomial of degree δ. Throughout this section, the symbol $\sum^\bullet$ will denote a sum restricted to polynomials relatively prime to D. Define

$$\Psi_D(k,l) = \left|\{(x,y) \in A^2 \ : \ x,y \text{ monic}, \ \gcd(x,y) = 1 \text{ and } \gcd(D,xy) = 1\}\right|.$$

LEMMA 7.1. *The following identity holds in the ring of iterated power series* $\mathbf{Q}[[u]][[v]]$ *:*

$$\sum_{k,l\geq 0} \Psi_D(k,l)u^k v^l = \frac{M_D^*(u)M_D^*(v)(1-quv)}{M_D^*(uv)(1-qu)(1-qv)}. \tag{7.1}$$

Proof. Define

$$\eta_D(s) = \sum_{a \ \text{monic}}^\bullet |a|^{-s}.$$

It follows immediately from the Euler product decomposition of $\zeta(s)$ that we have a factorization

$$\eta_D(s) = M_D(s)\zeta(s), \tag{7.2}$$

where $M_D(s)$ is the polynomial in q^{-s} defined in (6.3).

With this notation, we have

$$\begin{aligned}\eta_D(s)\eta_D(t) &= \sum_{a,\,b\ \text{monic}}^{\bullet} |a|^{-s}|b|^{-t}\\ &= \sum_{d\ \text{monic}}^{\bullet} \sum_{\substack{a,\,b\ \text{monic}\\ \gcd(a,b)=d}}^{\bullet} |a|^{-s}|b|^{-t}\\ &= \sum_{d\ \text{monic}}^{\bullet} |d|^{-(s+t)} \sum_{\substack{a,\,b\ \text{monic}\\ \gcd(a,b)=1}}^{\bullet} |a|^{-s}|b|^{-t}\\ &= \eta_D(s+t) \sum_{\substack{a,\,b\ \text{monic}\\ \gcd(a,b)=1}}^{\bullet} |a|^{-s}|b|^{-t}.\end{aligned}$$

Letting $u = q^{-s}$ and $v = q^{-t}$ we get

$$\eta_D^*(u)\eta_D^*(v) = \eta_D^*(uv) \sum_{k,l\geq 0} \Psi_D(k,l)u^k v^l,$$

which, combined with (7.2), shows the lemma.

For the next computation, we shall need the following variant of Lemma 6.9.

LEMMA 7.2. *Let g be an analytic function on the disk $|z| < R$, where $R > 1$. Let $f(z) = g(z)/(1-z)$ and consider the Taylor series expansion of $f(z)$ at $z = 0$:*

$$f(z) = \sum_{n=0}^{\infty} a_n z^n \quad \textit{for } |z| < 1\ .$$

Then the sequence $\{a_n\}$ converges and $\lim_{n\to\infty} a_n = g(1)$.

Proof. We leave the proof as an exercise.

LEMMA 7.3.

$$\lim_{l\to\infty} q^{-l} \sum_{k=0}^{\infty} \Psi_D(k,l) q^{-2k} = \frac{M_D(1)M_D(2)}{M_D(3)} \cdot \frac{\zeta(2)}{\zeta(3)}\,. \tag{7.3}$$

Proof. Let $u = q^{-2}$ and $v = q^{-1}z$, where z is a complex variable, and substitute in (7.1). We get

$$\sum_{l=0}^{\infty} \left[q^{-l} \sum_{k=0}^{\infty} \Psi_D(k,l) q^{-2k} \right] z^l = \frac{M_D^*(q^{-2})M_D^*(q^{-1}z)(1-q^{-2}z)}{M_D^*(q^{-3}z)(1-q^{-1})(1-z)}\,. \tag{7.4}$$

It is easy to see that the inner sum converges uniformly in l since $\Psi_D(k,l)q^{-l}$ is bounded by q^k. Notice that the function on the right-hand side of (7.4) has a simple pole at $z=1$ and that all other poles lie on the circle $|z|=q^3$. Hence, applying Lemma 7.2, we get

$$\begin{aligned}\lim_{l\to\infty} q^{-l}\sum_{k=0}^{\infty}\Psi_D(k,l)q^{-2k} &= \frac{M_D^*(q^{-2})M_D^*(q^{-1}z)(1-q^{-2}z)}{M_D^*(q^{-3}z)(1-q^{-1})}\bigg|_{z=1} \\ &= \frac{M_D(1)M_D(2)}{M_D(3)}\cdot\frac{\zeta(2)}{\zeta(3)}\,.\end{aligned}$$

For each $b\in A\setminus\{0\}$, we define

$$\chi_b(a)=\left(\frac{b}{a}\right)$$

for all monic polynomials a, where $\left(\frac{b}{a}\right)$ is the *Legendre symbol*. The *Dirichlet L-series* $L(s,\chi_b)$ attached to χ_b is defined by

$$L(s,\chi_b)=\sum_{a\ \text{monic}}\chi_b(a)\,|a|^{-s}.$$

If b is not a square, $L(s,\chi_b)$ is actually a polynomial of degree at most $\deg b-1$ in q^{-s} (see [15, Proposition 4.3]). In this case we write

$$L(s,\chi_b)=\sum_{k=0}^{\deg b-1}c_k(\chi_b)q^{-sk},$$

where

$$c_k(\chi_b)=\sum_{\substack{a\ \text{monic}\\ \deg a=k}}\chi_b(a)\,.$$

Our task will be to compute sums of coefficients $c_k(\chi_{Dm})$ as m runs over all polynomials of fixed degree l prime to D. We have

$$\sum_{\deg m=l}{}^{\bullet}\, c_k(\chi_{Dm})=\sum_{\substack{a\ \text{monic}\\ \deg a=k}}{}^{\bullet}\sum_{\deg m=l}{}^{\bullet}\left(\frac{m}{a}\right)\left(\frac{D}{a}\right). \tag{7.5}$$

(Recall that a bullet $^{\bullet}$ with the summation symbol indicates that the sum is restricted to polynomials prime to D.)

Assume that $\deg m = l \geq k+\delta$. If a is not a square, then

$$\sum_{\deg m=l}^{\bullet} \left(\frac{m}{a}\right) = 0\,,$$

since in this case $\left(\frac{-}{a}\right)$ is a nontrivial character on $(A/DaA)^{\times}$. If a is a square, then the summation above is just the number of polynomials m of degree l prime to D and a. Thus

$$\text{(7.6)} \qquad \sum_{\deg m=l}^{\bullet} c_k(\chi_{Dm}) = (q-1)\Psi_D(k/2,l) \quad \text{for } l \geq k+\delta\,,$$

with the convention that $\Psi_D(k/2,l)=0$ if $k/2$ is not an integer. The factor $q-1$ on the right-hand side accounts for the fact that the sum includes all polynomials m of degree l, not only the monic ones.

Thus we have so far

$$\text{(7.7)} \quad \sum_{\deg m=l}^{\bullet} L(s,\chi_{Dm}) = (q-1)\sum_{k=0}^{\lfloor (l-\delta)/2\rfloor} \Psi_D(k,l)q^{-2sk} + \sum_{k=l-\delta+1}^{l+\delta-1}\left(\sum_{\deg m=l}^{\bullet} c_k(\chi_{Dm})\right) q^{-sk}.$$

LEMMA 7.4. $|c_k(\chi_{Dm})| \leq \binom{l+\delta-1}{k} q^{k/2}$.

Proof. Let $L^*(u,\chi_{Dm}) = L(s,\chi_{Dm})$, where $u=q^{-s}$, and write $m=m_0m_1^2$, where m_0 is square-free. Let $E=K(\sqrt{Dm})$. We get from the Euler product factorization of $L(s,\chi_{Dm})$ the identity

$$L^*(u,\chi_{Dm}) = f(u)L_E(u)\prod_{p|m_1}\left(1-\left(\frac{m_0D}{p}\right)u^{\deg p}\right),$$

where $f(u)=(1-u^2)$, $(1-u)$ or $(1-u)^2$ according to whether the prime at infinity of K is *inert*, *ramified* or *split* in E and $L_E(u)$ is the L-function of E. The polynomial $L_E(u)$ has a factorization of the form

$$L_E(u) = \prod_{i=1}^{2g}(1-\pi_i u)\,,$$

where the g is the genus of E. By the Riemann Hypothesis (see [15, Theorem 5.10]), the inverse roots π_i of $L_E(u)$ satisfy $|\pi_i| = q^{1/2}$. Let $\pi_{2g+1},\ldots,\pi_n$ (where $n \leq l+\delta-1$) be the inverses of the remaining roots of $L^*(u, \chi_{Dm})$. Notice that $|\pi_i| = 1$ for $i = 2g+1, \dots, n$. With this notation we have

$$L^*(u, \chi_{Dm}) = \prod_{i=1}^{n} (1 - \pi_i u),$$

so the coefficient $c_k(\chi_{Dm})$ is given by

$$c_k(\chi_{Dm}) = s_k(\pi_1, \dots, \pi_n),$$

where s_k is the degree k *elementary symmetric function* in n variables. Hence

$$\begin{aligned} |c_k(\chi_{Dm})| &\leq \binom{n}{k} \sup\{|\pi_{i_1} \cdots \pi_{i_k}|\} \\ &\leq \binom{n}{k} q^{k/2} \\ &\leq \binom{l+\delta-1}{k} q^{k/2}. \end{aligned}$$

We can now prove the main theorem of this section.

THEOREM 7.5.

$$\lim_{l\to\infty} \frac{1}{q^l} \sum_{\deg m = l}^{\bullet} L(1, \chi_{Dm}) = \frac{M_D(1) M_D(2)}{M_D(3)} q (1 - q^{-2}). \tag{7.8}$$

Proof. We shall first estimate the second sum on the right-hand side of (7.7) at $s = 1$ using Lemma 7.4. Take l large enough so that $l - \delta + 1 > (l + \delta - 1)/2$ ($l \geq 3\delta$ suffices). For $l + \delta - 1 \geq k \geq l - \delta + 1$ we have

$$\binom{l+\delta-1}{k} \leq \binom{l+\delta-1}{l-\delta+1} = \binom{l+\delta-1}{2\delta-2}.$$

Using Lemma 7.4 we get

$$\left| \sum_{k=l-\delta+1}^{l+\delta-1} \Big(\sum_{\deg m = l}^{\bullet} c_k(\chi_{Dm}) \Big) q^{-k} \right| \leq q^l (q-1)(2\delta-1) \binom{l+\delta-1}{2\delta-2} q^{-(l-\delta+1)/2}. \tag{7.9}$$

Hence

$$\frac{1}{q^l} \left| \sum_{k=l-\delta+1}^{l+\delta-1} \Big(\sum_{\deg m = l}^{\bullet} c_k(\chi_{Dm}) \Big) q^{-k} \right| \leq P(l) q^{-l/2}, \tag{7.10}$$

where we have set

$$P(l) = (q-1)\, q^{(\delta-1)/2}(2\delta - 1)\binom{l+\delta-1}{2\delta-2}.$$

Notice that $P(l)$ is a polynomial in l of degree $2\delta - 2$, so taking limits in (7.10), we get

$$\lim_{l\to\infty} \frac{1}{q^l} \sum_{k=l-\delta+1}^{l+\delta-1} \Bigl(\sum_{\deg m=l}^{\bullet} c_k(\chi_{Dm}) q^{-k} \Bigr) = 0\,.$$

Therefore, from (7.7)

$$\lim_{l\to\infty} \frac{1}{q^l} \sum_{\deg m=l}^{\bullet} L(1,\chi_{Dm}) = (q-1) \lim_{l\to\infty} \frac{1}{q^l} \sum_{k=0}^{\lfloor (l-\delta)/2 \rfloor} \Psi_D(k,l) q^{-2k}. \tag{7.11}$$

In order to conclude, we inspect the "tail" of the series in (7.3). Using the obvious inequality $\Psi_D(k,l) \le q^{k+l}$ we get

$$\frac{1}{q^l} \sum_{k=\lfloor (l-\delta)/2 \rfloor +1}^{\infty} \Psi_D(k,l) q^{-2k} \le \sum_{k=\lfloor (l-\delta)/2 \rfloor +1}^{\infty} q^{-k}.$$

The right-hand side of the above inequality tends to zero as $l \to \infty$. The theorem follows from (7.11) and (7.3):

$$\begin{aligned} \lim_{l\to\infty} \frac{1}{q^l} \sum_{\deg m=l}^{\bullet} L(1,\chi_{Dm}) &= (q-1) \frac{M_D(1) M_D(2)}{M_D(3)} \cdot \frac{\zeta(2)}{\zeta(3)} \\ &= \frac{M_D(1) M_D(2)}{M_D(3)} q(1-q^{-2})\,. \end{aligned}$$

REMARK 7.6. Theorem 7.5 can be restated in perhaps a more suggestive way as a limit of averages. For $l \ge \delta$ the number of polynomials of degree l prime to D is $(q-1)q^l M_D(1)$. Thus (7.8) becomes

$$\lim_{l\to\infty} \frac{1}{(q-1)q^l M_D(1)} \sum_{\deg m=l}^{\bullet} L(1,\chi_{Dm}) = \frac{M_D(2)\zeta(2)}{M_D(3)\zeta(3)}\,. \tag{7.12}$$

(Compare with [8, Theorem 1.4].)

COROLLARY 7.7. *Let* $h(mD) = \bigl|\mathrm{Pic}(A[\sqrt{mD}])\bigr|$. *Then*

$$\lim_{l\to\infty} \frac{1}{q^{3l}} \sum_{\deg m=\delta+2l+1}^{\bullet} h(mD) = q^{2\delta}(q^2-1) \frac{M_D(1) M_D(2)}{M_D(3)}\,. \tag{7.13}$$

Proof. For $\deg m = \delta + 2l + 1$ we have the relation (see e.g. [8, Theorem 0.6 (i)])

$$\begin{aligned} L(1,\chi_{mD}) &= \frac{q^{1/2}}{|mD|^{1/2}} h(mD) \\ &= q^{-l-\delta} h(mD)\,. \end{aligned}$$

Thus

$$\begin{aligned} \lim_{l\to\infty} \frac{1}{q^{3l}} \sideset{}{^\bullet}\sum_{\deg m=\delta+2l+1} h(mD) &= q^{2\delta+1} \lim_{l\to\infty} \frac{1}{q^{\delta+2l+1}} \sideset{}{^\bullet}\sum_{\deg m=\delta+2l+1} L(1,\chi_{Dm}) \\ &= q^{2\delta}(q^2-1)\frac{M_D(1)M_D(2)}{M_D(3)}\,. \end{aligned}$$

8. The mass formula

We can use the results established in the previous sections to obtain Siegel's Mass Formula in the case where the determinant D is square-free.

THEOREM 8.1. *Let D be a square-free polynomial of degree δ and let $L_1,\dots,L_h$ be a complete list of representatives of the isometry classes of ternary definite lattices of determinant D. Then*

$$\sum_{i=1}^{h} \frac{1}{|SO(L_i)|} = \frac{q^\delta M_D(1)M_{D_0}(2)}{2^r(q^2-1)(2M_{D_0}(1)-M_{D_0}(2))}\,, \tag{8.1}$$

where r is the number of prime divisors of D.

Proof. We take sums in (5.7) over all polynomials a relatively prime to D with $\deg a = \delta+2l+1$ for a fixed positive integer l (we restrict ourselves to degrees of this form to ensure that $-aD$ is not a square in K_∞ so the equivalent conditions of Lemma 2.2 are satisfied). We get

$$\sideset{}{^\bullet}\sum_{\deg a=\delta+2l+1} \sum_{i=1}^{h} \frac{R(L_i,a)}{|SO(L_i)|} = \frac{1}{2^r} \sideset{}{^\bullet}\sum_{\deg a=\delta+2l+1} h(-aD)\,.$$

Interchanging the sums and using the notation of Theorem 6.10 we have

$$\frac{1}{q^{3l}} \sum_{i=1}^{h} \frac{\beta_{\delta+2l+1}(L_i)}{|SO(L_i)|} = \frac{1}{2^r}\frac{1}{q^{3l}} \sideset{}{^\bullet}\sum_{\deg a=\delta+2l+1} h(-aD)\,.$$

The formula follows from Theorem 6.10 and Corollary 7.7 by taking the limit as $l \to \infty$.

REMARK 8.2. In the special case where D is *irreducible*, formula (8.1) becomes

$$\sum_{i=1}^{h} \frac{1}{|SO(L_i)|} = \frac{q^\delta - 1}{2(q^2-1)}\,, \tag{8.2}$$

which is equivalent to the one proved by Gekeler [5, 5.11] using Drinfeld modules.

9. EXACT CLASS NUMBERS

Theorem 8.1 allows us also to give *exact* class numbers for definite forms of *irreducible* determinant D. We shall restrict ourselves for simplicity to the case where the degree of D is odd (a similar argument can be made in the case where D has even degree).

Assuming D is irreducible of odd degree, all definite ternary forms of determinant D are in the genus of the diagonal form $Q_0 = \langle 1, -\epsilon, -\epsilon D\rangle$, where ϵ is a nonsquare in $\mathbf{F}_q$. Since D is irreducible, a quadratic form Q of determinant D either represents a unit or is indecomposable. Let h_{dec} be the number of classes of *decomposable* forms of determinant D and let h_{ind} be the number of *indecomposable* ones (then $h = h_{\mathrm{dec}} + h_{\mathrm{ind}}$). If Q is decomposable then Q is of one of the types:

$$Q = \langle 1\rangle \perp (-\epsilon Q') \quad \text{or} \quad Q = \langle \epsilon\rangle \perp (-Q'')\,, \tag{9.1}$$

where Q' is a binary form in the principal genus of determinant D and Q'' is in the principal genus of determinant ϵD. The only class common to these two types is represented by the diagonal form Q_0.

Kneser [9] showed that the theory of Gauss for binary quadratic forms holds in great generality, and we can apply it in particular for forms over A (see also [7] for the specific case of polynomial rings) in order to count the possibilities for Q' and Q''. The proper equivalence classes of binary quadratic forms of determinant D in the principal genus are in one-to-one correspondence with elements of the ideal class group $\mathrm{Pic}(A[\sqrt{-D}])$ (this group has odd order since D is irreducible of odd degree). The number of improper nontrivial equivalence classes in the principal genus is then $(\left|\mathrm{Pic}(A[\sqrt{-D}])\right| - 1)/2$. Similarly for the forms of determinant ϵD. Thus:

$$\begin{aligned} h_{\mathrm{dec}} &= 1 + \frac{\left|\mathrm{Pic}(A[\sqrt{-D}])\right| - 1}{2} + \frac{\left|\mathrm{Pic}(A[\sqrt{-\epsilon D}])\right| - 1}{2} \\ &= \frac{L_{-D}(1) + L_{-D}(-1)}{2}\,, \end{aligned} \tag{9.2}$$

where L_{-D} is the numerator of the zeta function (see [15, Theorem 5.9]) of the hyperelliptic curve $y^2 = -D$. Here we use the well-known fact that $L_{-\epsilon D}(u) = L_{-D}(-u)$. Note that in the particular case of an elliptic curve ($\deg D = 3$) we have $h = h_{\mathrm{dec}} = q+1$.

LEMMA 9.1. *Denote by $SO(Q)$ the group of integral rotations of Q. Then we have:*

(i) *if $Q = Q_0$, then $|SO(Q)| = 2(q+1)$;*

(ii) *if Q is as in* (9.1) *with Q' and Q'' indecomposable, then $|SO(Q)| = 2$;*

(iii) *if Q is indecomposable, then $|SO(Q)| = 1$.*

Proof. We leave the proof as an easy exercise.

THEOREM 9.2. *Let D be a square-free irreducible polynomial of odd degree δ, let h be the number of isometry classes of definite ternary forms of determinant D and let h_{ind} be the number of those that are indecomposable. Then*

$$h = \frac{1}{2}\left[1 + \frac{q(q^{\delta-1}-1)}{q^2-1} + \frac{L_{-D}(1)+L_{-D}(-1)}{2}\right]; \tag{9.3}$$

$$h_{ind} = \frac{1}{2}\left[1 + \frac{q(q^{\delta-1}-1)}{q^2-1} - \frac{L_{-D}(1)+L_{-D}(-1)}{2}\right]. \tag{9.4}$$

Proof. This is a straightforward application of Theorem 8.1 together with (9.2) and Lemma 9.1

REMARK 9.3. In the case where D is irreducible, the form Q is anisotropic exactly at D and at ∞, so by Corollary 3.7, the maximal lattices in V are in one-to-one-correspondence with the maximal orders of the quaternion algebra $C_0(V,Q)$. So the number h of Theorem 9.2 is also the *type* of the quaternion algebra $C_0(V,Q)$, i.e. the number of conjugacy classes of maximal orders of $C_0(V,Q)$. Formula (9.3) is therefore equivalent to the formula proved by Gekeler [5, Theorem 7.6] using Drinfeld modules for the type of a quaternion algebra ramified at D and ∞.

REFERENCES

[1] BOMBIERI, E. Counting points on curves over finite fields (d'après S.A. Stepanov). Séminaire Bourbaki, 25ème année (1972/1973), Exp. No. 430, 234–241. Lecture Notes in Mathematics *383*. Springer, Berlin, 1974.

[2] BUREAU, J. and J. MORALES. Isospectral definite ternary $\mathbf{F}_q[t]$-lattices. *J. Number Theory 129* (2009), 2457–2473.

[3] CASSELS, J.W.S. *Rational Quadratic Forms*. London Mathematical Society Monographs *13*. Academic Press, Inc., Harcourt Brace Jovanovich, Publishers, London-New York, 1978.

[4] GAUSS, C.F. *Disquisitiones arithmeticae*. Königliche Gesellschaft der Wissenschaften, Göttingen, 1801, 1863.

[5] GEKELER, E.-U. On the arithmetic of some division algebras. *Comment. Math. Helv. 67* (1992), 316–333.

[6] GERSTEIN, L.J. *Basic Quadratic Forms*. Graduate Studies in Mathematics *90*. Amer. Math. Soc., Providence, RI, 2008.

[7] HELLEGOUARCH, Y. Positive definite binary quadratic forms over $k[X]$. In: *Number Theory (Ulm, 1987)*, 93–119. Lecture Notes in Mathematics *1380*. Springer, New York, 1989.

[8] HOFFSTEIN, J. and M. ROSEN. Average values of L-series in function fields. *J. Reine Angew. Math. 426* (1992), 117–150.

[9] KNESER, M. Composition of binary quadratic forms. *J. Number Theory 15* (1982), 406–413.

[10] KNUS, M.-A., A. MERKURJEV, M. ROST and J.-P. TIGNOL. *The Book of Involutions*. With a preface in French by J. Tits. Amer. Math. Soc. Colloquium Publications *44*. Amer. Math. Soc., Providence, RI, 1998.

[11] LANG, S. On quasi algebraic closure. *Ann. of Math. (2) 55* (1952), 373–390.

[12] LLORENTE, P. Correspondencia entre formas ternarias enteras y órdenes cuaterniónicos. Contributions to the algorithmic study of problems of arithmetic moduli (Spanish). *Rev. R. Acad. Cienc. Exactas Fís. Nat. (Esp.) 94* (2000), 397–416.

[13] O'MEARA, O.T. *Introduction to Quadratic Forms*. Reprint of the 1973 edition. Classics in Mathematics. Springer-Verlag, Berlin, 2000.

[14] REHM, H.P. On a theorem of Gauss concerning the number of integral solutions of the equation $x^2 + y^2 + z^2 = m$. In: *Ternary Quadratic Forms and Norms* (O. Taussky, ed.), 31–38. Lecture Notes in Pure and Applied Mathematics *79*. Marcel Dekker, Inc./New York-Basel, 1982.

[15] ROSEN, M. *Number Theory in Function Fields*. Graduate Texts in Mathematics *210*. Springer-Verlag, New York, 2002.

[16] SCHARLAU, W. *Quadratic and Hermitian Forms*. Grundlehren der mathematischen Wissenschaften *270*. Springer-Verlag, Berlin, 1985.

[17] SCHMIDT, W.M. Zur Methode von Stepanov. *Acta Arith. 24* (1973), 347–367.

[18] SHEMANSKE, T.R. Representations of ternary quadratic forms and the class number of imaginary quadratic fields. *Pacific J. Math. 122* (1986), 223–250.

[19] STEPANOV, S.A. An elementary proof of the Hasse-Weil theorem for hyperelliptic curves. *J. Number Theory 4* (1972), 118–143.

[20] VENKOV, B. A. On the arithmetic of quaternion algebras (Russian). *Izv. Akad. Nauk SSSR 16* (1922/24), 205–220.

[21] WEIL, A. *Sur les courbes algébriques et les variétés qui s'en déduisent*. Actualités Sci. Ind., no. 1041 = Publ. Inst. Math. Univ. Strasbourg *7* (1945), Hermann et Cie., Paris, 1948.

(Reçu le 20 août 2010)

Piotr Maciak

École Polytechnique Fédérale de Lausanne
EPFL-FSB-MATHGEOM-CSAG
Station 8
CH-1015 Lausanne
Switzerland
e-mail: piotr.maciak@epfl.ch

Jorge Morales

Mathematics Department
Louisiana State University
Baton Rouge, Louisiana 70808
U.S.A.
e-mail: morales@math.lsu.edu