

INTEGER POINTS ON SPHERES AND THEIR ORTHOGONAL LATTICES

MENNY AKA, MANFRED EINSIEDLER, AND URI SHAPIRA
(WITH AN APPENDIX BY RUIXIANG ZHANG)

ABSTRACT. Linnik proved in the late 1950's the equidistribution of integer points on large spheres under a congruence condition. The congruence condition was lifted in 1988 by Duke (building on a break-through by Iwaniec) using completely different techniques. We conjecture that this equidistribution result also extends to the pairs consisting of a vector on the sphere and the shape of the lattice in its orthogonal complement. We use a joining result for higher rank diagonalizable actions to obtain this conjecture under an additional congruence condition.

1. INTRODUCTION

A theorem of Legendre, whose complete proof was given by Gauss in [Gau86], asserts that an integer D can be written as a sum of three squares if and only if D is not of the form $4^m(8k + 7)$ for some $m, k \in \mathbb{N}$. Let $\mathbb{D} = \{D \in \mathbb{N} : D \not\equiv 0, 4, 7 \pmod{8}\}$ and $\mathbb{Z}_{\text{prim}}^3$ be the set of primitive vectors in \mathbb{Z}^3 . Legendre's Theorem also implies that the set

$$\mathbb{S}^2(D) \stackrel{\text{def}}{=} \left\{ v \in \mathbb{Z}_{\text{prim}}^3 : \|v\|_2^2 = D \right\}$$

is non-empty if and only if $D \in \mathbb{D}$. This important result has been refined in many ways. We are interested in the refinement known as Linnik's problem.

Let $\mathbb{S}^2 \stackrel{\text{def}}{=} \{x \in \mathbb{R}^3 : \|x\|_2 = 1\}$. For a subset S of rational odd primes we set

$$\mathbb{D}(S) = \left\{ D \in \mathbb{D} : \text{for all } p \in S, -D \pmod{p} \in (\mathbb{F}_p^\times)^2 \right\}.$$

In the late 1950's Linnik [Lin68] proved that $\left\{ \frac{v}{\|v\|} : v \in \mathbb{S}^2(D) \right\}$ equidistribute to the uniform measure on \mathbb{S}^2 when $D \rightarrow \infty$ under the restrictive assumption $D \in \mathbb{D}(p)$ where p is an odd prime. As we will again recall in this paper (see equation (3.4)) the condition $D \in \mathbb{D}(p)$ should be thought of as a splitting condition for an associated torus subgroup over \mathbb{Q}_p , which enables one to use dynamical arguments. Assuming GRH Linnik was able

M.A. acknowledges the support of ISEF, Advanced Research Grant 228304 from the ERC, and SNF Grant 200021-152819.

M.E. acknowledges the support of the SNF Grant 200021-127145 and 200021-152819.

U.S. acknowledges the support of the Chaya fellowship and ISF grant 357/13.

R.Z. acknowledges the support of Math Department of Princeton University.

to remove the congruence condition. A full solution of Linnik's problem was given by Duke [Duk88] (following a breakthrough by Iwaniec [Iwa87]), who used entirely different methods.

In this paper we concern ourself not just with the direction of the vector $v \in \mathbb{S}^2(D)$ but also with the shape of the lattice $\Lambda_v \stackrel{\text{def}}{=} \mathbb{Z}^3 \cap v^\perp$ in the orthogonal complement v^\perp . To discuss this refinement in greater detail we introduce the following notation. Fix a copy of $\mathbb{R}^2 \stackrel{\text{def}}{=} \mathbb{R}^2 \times \{0\}$ in \mathbb{R}^3 . To any primitive vector $v \in \mathbb{S}^2(D)$ we attach an orthogonal lattice $[\Lambda_v]$ and an orthogonal grid $[\Delta_v]$ in \mathbb{R}^2 by the following procedure.

First, note that

$$(1.1) \quad [\mathbb{Z}^3 : (\mathbb{Z}v \oplus \Lambda_v)] = D$$

since primitivity of v implies that the homomorphism $\mathbb{Z}^3 \rightarrow \mathbb{Z}$ defined by $u \mapsto (u, v)$ is surjective and $v \oplus \Lambda_v$ is the preimage of $D\mathbb{Z}$. Now we choose an orthogonal transformation k_v in $\text{SO}_3(\mathbb{R})$ that maps v to $\|v\|e_3$ and so maps v^\perp to our fixed copy of \mathbb{R}^2 . We rotate $\mathbb{Z}^3 \cap v^\perp$ by k_v and obtain a lattice in \mathbb{R}^2 , which has covolume \sqrt{D} by (1.1). In order to normalize the covolume we also multiply by the diagonal matrix $a_v = \text{diag}(D^{-\frac{1}{4}}, D^{-\frac{1}{4}}, D^{\frac{1}{2}})$. This defines a unimodular lattice $[\Lambda_v]$ in \mathbb{R}^2 , which is well defined up to planar rotations and so defines an element

$$[\Lambda_v] \in \mathcal{X}_2 \stackrel{\text{def}}{=} \text{SO}_2(\mathbb{R}) \backslash \text{SL}_2(\mathbb{R}) / \text{SL}_2(\mathbb{Z}).$$

We will refer to $[\Lambda_v]$ as “the shape of the orthogonal lattice” attached to v .

We may still obtain a bit more geometric information from the given vector v as follows. We choose a basis v_1, v_2 of the lattice Λ_v such that $\det(v_1, v_2, v) > 0$. Choose $w \in \mathbb{Z}^3$ with $(w, v) = 1$ and let g_v denote the matrix whose columns are v_1, v_2, w . Note that $g_v \in \text{SL}_3(\mathbb{Z})$ and that the set of choices of g_v is the coset $g_v \text{ASL}_2(\mathbb{Z})$, where $\text{ASL}_2 = \left\{ \begin{pmatrix} g & * \\ 0 & 1 \end{pmatrix} \mid g \in \text{SL}_2 \right\}$. Also note that the set of choices for k_v is the coset $\text{Stab}_{\text{SO}_3(\mathbb{R})}(e_3)k_v = \text{SO}_2(\mathbb{R})k_v$. As a_v commutes with $\text{SO}_2(\mathbb{R})$, we obtain the double coset

$$[\Delta_v] = \text{SO}_2(\mathbb{R})a_vk_vg_v\text{ASL}_2(\mathbb{Z}).$$

It does not depend on the choices made above and belongs to the space

$$\mathcal{Y}_2 \stackrel{\text{def}}{=} \text{SO}_2(\mathbb{R}) \backslash \text{ASL}_2(\mathbb{R}) / \text{ASL}_2(\mathbb{Z}),$$

where we used that $a_vk_vg_v \in \text{ASL}_2(\mathbb{R})$. Elements of the form $[\Delta_v]$ will be referred to as “orthogonal grids” and can be identified with two-dimensional lattices together with a marked point on the associated torus, defined up to a rotation.

Let $\tilde{\nu}_D$ denote the normalized counting measure on the set

$$\left\{ \left(\frac{v}{\|v\|}, [\Delta_v] \right) : v \in \mathbb{S}^2(D) \right\} \subset \mathbb{S}^2 \times \mathcal{Y}_2.$$

We are interested to find $A \subset \mathbb{D}$ for which

$$(1.2) \quad \tilde{\nu}_D \xrightarrow{\text{weak}^*} m_{\mathbb{S}^2} \otimes m_{\mathcal{Y}_2} \text{ as } D \rightarrow \infty \text{ with } D \in A$$

where $m_{\mathbb{S}^2} \otimes m_{\mathcal{Y}_2}$ is the product of the natural uniform measures on \mathbb{S}^2 and \mathcal{Y}_2 . We propose the following conjecture as a generalization of Linnik's problem and Theorem 1.2 below as a generalization of Linnik's theorem:

Conjecture 1.1. *The convergence in (1.2) holds for the subset $A = \mathbb{D} = \{D : D \not\equiv 0, 4, 7 \pmod{8}\}$.*

Consider the natural projection $\pi : \mathcal{Y}_2 \rightarrow \mathcal{X}_2$ induced by the natural map $\phi : \text{ASL}_2 \rightarrow \text{SL}_2$. Then $\tilde{\mu}_D \stackrel{\text{def}}{=} (Id \times \pi)_* \tilde{\nu}_D$ is the normalized counting measure on

$$\left\{ \left(\frac{v}{\|v\|}, [\Lambda_v] \right) : v \in \mathbb{S}^2(D) \right\} \subset \mathbb{S}^2 \times \mathcal{X}_2.$$

Slightly simplifying the above problem we are interested to find $A \subset \mathbb{D}$ for which

$$(1.3) \quad \tilde{\mu}_D \xrightarrow{\text{weak}^*} m_{\mathbb{S}^2} \otimes m_{\mathcal{X}_2} \text{ as } D \rightarrow \infty \text{ with } D \in A.$$

Using two splitting conditions (see §4) we are able to prove:

Theorem 1.2 (Main Theorem). *Let \mathbb{F} denote the set of square free integers and p, q denote two distinct odd prime numbers. Then the convergence (1.3) holds for $A = \mathbb{D}(\{p, q\}) \cap \mathbb{F}$.*

Remarks 1.3. Our interest in the above problem arose via the work of Marklof [Mar10] and W. Schmidt [Sch98] (see also [EMSS]), but as we later learned from P. Sarnak and R. Zhang, the question is closely related to the work of Maass [Maa56].

Our method of proof builds on the equidistribution on \mathbb{S}^2 and on \mathcal{X}_2 (respectively on related covering spaces) as obtained by Linnik [Lin68] or Duke [Duk88] (and in one instance more precisely the refinement of Duke's theorem obtained by Harcos and Michel [HM06]). The crucial step is to upgrade these statements to the joint equidistribution. To achieve that we apply the recent classification of joinings for higher rank actions obtained by E. Lindenstrauss and the second named author in [EL15]. As such a classification is only possible in higher rank we need to require Linnik's splitting condition at two different primes.

The restriction to square-free numbers can be avoided but appears currently in our proof through the work of Harcos and Michel [HM06], see also Remark 4.3. As Theorem 1.2 is assuming a splitting condition (actually two) Linnik's method [Lin68] could (most likely) be used to overcome the square-free condition. We refer also to [ELMV09, EMV10], where the Linnik method is used for slightly different problems.

Using a break-through of Iwaniec [Iwa87], it was shown by Duke [Duk88] that the congruence condition $D \in \mathbb{D}(p)$ in Linnik's work is redundant. In Conjecture 1.1 we expressed our belief that the congruence condition $D \in \mathbb{D}(\{p, q\})$ in Theorem 1.2 is also superfluous. It is possible that analytic methods can again be used to eliminate these congruence conditions in the

future although it does not seem to be a straightforward matter. We refer to Appendix A for some findings in this direction.

As we explain in §4.1 the equidistribution of $\{[\Lambda_v] : v \in \mathbb{S}^2(D)\}$ on \mathcal{X}_2 follows from a (refined) version of Duke’s Theorem. In this context it is not clear how to establish equidistribution of $\{[\Delta_v] : v \in \mathbb{S}^2(D)\}$ on \mathcal{Y}_2 using the analytic methods. Using the methods below any such equidistribution result on \mathcal{Y}_2 will imply a corresponding convergence in (1.2) for $A = \mathbb{D}(\{p, q\})$.

The higher dimensional analogues are more accessible. In fact working with spheres in \mathbb{R}^d we use unipotent dynamics in [AES14] to establish the equidistribution if $d \geq 6$. The cases $d = 4, 5$ are slightly harder and need a mild congruence condition (namely that $p \nmid D$ for a fixed odd prime p) for the method of [AES14]. In an upcoming paper [ERW14] of Ph. Wirth, R. Rühr, and the second named author the full result is obtained for $d = 4, 5$ by using effective dynamical arguments.

Acknowledgements: We would like to thank Elon Lindenstrauss, Philippe Michel, and Akshay Venkatesh for many fruitful conversations over the last years on various topics and research projects that lead to the current paper. While working on this project the authors visited the Israel Institute of Advanced Studies (IIAS) at the Hebrew University and its hospitality is deeply appreciated. We thank Peter Sarnak and Ruixiang Zhang for many conversations on these topics at the IIAS.

2. NOTATION AND ORGANIZATION OF THE PAPER

We first fix some common notation from algebraic number theory: Let $V_{\mathbb{Q}}$ be the set of places on \mathbb{Q} containing all primes p and the archimedean place ∞ . Let \mathbb{Z}_p denote the p -adic numbers and for $S \subset V_{\mathbb{Q}}$ we let $\mathbb{Q}_S = \prod'_{p \in S} \mathbb{Q}_p$ be the restricted direct product w.r.t. the compact open subgroups \mathbb{Z}_p . Finally, we set $\mathbb{A}_f = \prod'_{p \in V_{\mathbb{Q}} \setminus \{\infty\}} \mathbb{Q}_p$, $\widehat{\mathbb{Z}} = \prod_{p \in V_{\mathbb{Q}} \setminus \{\infty\}} \mathbb{Z}_p$ and $\mathbb{Z}^S = \mathbb{Z}[\{\frac{1}{p} : p \in S \setminus \{\infty\}\}]$. Recall that $\mathbb{Q} = \mathbb{Z}^{V_{\mathbb{Q}}}$ is a cocompact lattice in the adèles $\mathbb{A} = \mathbb{Q}_{V_{\mathbb{Q}}}$. The letter e with or without a subscript will denote the identity element of a group which is clear from the context.

A sequence of probability measures μ_n on a measurable space X is said to equidistribute to a probability measure μ as $n \rightarrow \infty$ if the sequence converges to μ in the weak* topology on the space of probability measures on X . A probability measure μ is called a weak* limit of a sequence of measures μ_n if there exists a subsequence (n_k) such that μ_{n_k} equidistribute to μ as $k \rightarrow \infty$.

Given a locally compact group L and a subgroup $M < L$ such that L/M admits an L -invariant probability measure, it is unique and we denote it by $m_{L/M}$ and call it the *uniform measure* on L/M . Finally, the letter π (with or without some decorations) is used to denote various projection maps whose definition will be clear from the context. E.g. if $M < L$ are as above and $K < L$ is a compact subgroup, there is a canonical projection

map $\pi : L/M \rightarrow K \backslash L/M$ and we will still refer to $\pi_*(m_{L/M})$ as the uniform measure on $K \backslash L/M$.

We now give an overview of our proof of Theorem 1.2 and discuss the organization of the paper. In §3, we establish that the convergence (1.3) follows from an equidistribution of "joined" adelic (or S -adic) torus orbits on a product of two homogeneous spaces. In §4.1, we use Duke's Theorem (resp. [HM06]) to deduce that these orbits equidistribute to a joining (see §4 for the definition). Then, in §4.2 we show that this joining must be the trivial joining. This will imply Theorem 1.2.

3. JOINED ADELIC, S -ADIC AND REAL TORUS ORBITS

In this section we show that Conjecture 1.1 and Theorem 1.2 follow from the equidistribution of a sequence of "adelic diagonal" torus orbits on a product of homogeneous spaces. We first explain this connection for Conjecture 1.1, involving a homogeneous space for ASL_2 .

Let $\mathbb{G}_1 = \text{SO}_3$, $\mathbb{G}_2 = \text{ASL}_2$ and $\mathbb{G} = \mathbb{G}_1 \times \mathbb{G}_2$, $G_j = \mathbb{G}_j(\mathbb{R})$, $\Gamma_j = \mathbb{G}_j(\mathbb{Z})$ for $j = 1, 2$ and $G = \mathbb{G}(\mathbb{R})$, $\Gamma = \mathbb{G}(\mathbb{Z})$, $K = \text{SO}_2(\mathbb{R})$ and fix $v \in \mathbb{S}^2(D)$, $D \in \mathbb{D}$ throughout this section. We wish to identify $K \backslash G_1 \cong \mathbb{S}^2$ so we let $k \in G_1$ act on \mathbb{S}^2 by the right action $(k, u) \mapsto k.u = k^{-1}u$; we find it simpler to think of \mathbb{S}^2 as row vectors and use the definition $(k, u^t) \mapsto k.u^t = u^t k$. Note that this defines a transitive action satisfying $K = \text{Stab}_{G_1}(e_3)$. Recall the definition of $g_v, k_v, a_v, [\Delta_v]$ from the introduction and note that $e_3^t k_v = \|v\|^{-1} v^t$.

Let $\mathbf{S}^2 \stackrel{\text{def}}{=} \mathbb{S}^2/\Gamma_1$ and $\mathbf{S}^2(D) \stackrel{\text{def}}{=} \mathbb{S}^2(D)/\Gamma_1$ and $\mathbf{v} = v^t \Gamma_1$ and set $[\Delta_{\mathbf{v}}] = [\Delta_v]$ which is well-defined as $[\Delta_{\gamma.v}] = [\Delta_v]$ for all $\gamma \in \Gamma_1$. The map $\mathbf{v} \in \mathbf{S}^2(D) \mapsto \frac{\mathbf{v}}{\|\mathbf{v}\|} \in \mathbf{S}^2$ is also well-defined. It follows that the following double coset

$$(3.1) \quad K \times K(k_v, a_v k_v g_v) \Gamma_1 \times \Gamma_2$$

represents the pair

$$\left(\frac{\mathbf{v}}{\|\mathbf{v}\|}, [\Delta_{\mathbf{v}}] \right) \in \mathbf{S}^2 \times \mathcal{Y}_2.$$

Note that all the measures appearing in equation (1.2) (resp. equation (1.3)) are Γ_1 -invariant so if we consider their projection ν_D (resp. μ_D) of $\tilde{\nu}_D$ (resp. $\tilde{\mu}_D$) to $\mathbf{S}^2 \times \mathcal{Y}_2$ (resp. $\mathbf{S}^2 \times \mathcal{X}_2$) we have that the convergence (1.2) is equivalent to

$$(3.2) \quad \nu_D \xrightarrow{\text{weak-*}} m_{\mathbf{S}^2} \otimes m_{\mathcal{Y}_2}, D \rightarrow \infty, D \in A$$

and the convergence (1.3) is equivalent to

$$(3.3) \quad \mu_D \xrightarrow{\text{weak-*}} m_{\mathbf{S}^2} \otimes m_{\mathcal{X}_2}, D \rightarrow \infty, D \in A.$$

Roughly speaking, integral orbits on the \mathbb{Z} -points of a variety admitting a \mathbb{Z} -action of an algebraic group \mathbb{P} may be parametrized by an adelic quotient of the stabilizer. E.g., as we will see below, Γ_1 -orbits of $\mathbb{S}^2(D)$, can be parametrized as an adelic quotient of the stabilizer of v . The interested

reader may consult [EV08, §3], [EMV10, §6.1] and [PR94, Theorem 8.2]. The novelty here is that we consider a “joint parametrization” and combine this with a recent work of the second named author with E. Lindenstrauss [EL15].

More concretely, consider the above right action of G_1 on $K \setminus G_1 \cong \mathbb{S}^2$ and set $\mathbb{H}_v \stackrel{\text{def}}{=} \text{Stab}_{G_1}(v)$. The group \mathbb{H}_v is defined over $\mathbb{Z} \subset \mathbb{Q}$ as $v \in \mathbb{Z}^3$. Naturally, $k_v^{-1} \text{Stab}_{G_1}(e_3) k_v = k_v^{-1} K k_v = \mathbb{H}_v(\mathbb{R})$.

In the proofs below we will frequently use the ternary quadratic form $Q_0((v_1, v_2, v_3)) = v_1^2 + v_2^2 + v_3^2 = \|(v_1, v_2, v_3)\|_2^2$ for (v_1, v_2, v_3) belonging to \mathbb{Q}^3 or one of its completions. The following lemma explains the congruence condition $D \in \mathbb{D}(p)$.

Lemma 3.1. *Let $v \in \mathbb{Z}_p^3$ and $D = Q_0(v)$. We have that*

$$(3.4) \quad -D = x^2 \text{ for some } x \in \mathbb{Z}_p \Rightarrow \mathbb{H}_v(\mathbb{Q}_p) \text{ is a split torus.}$$

Proof. Let w_1, w_2 be a basis of the orthogonal complement of v within \mathbb{Q}_p^3 . Notice first that $\mathbb{H}_v(\mathbb{Q}_p) \cong \text{SO}(aX^2 + bXY + cY^2)$, where $a = \|w_1\|_2^2, c = \|w_2\|_2^2, b = 2(w_1, w_2)$. The determinant of the companion matrix of Q_0 w.r.t. the basis v, w_1, w_2 is 1 up-to $(\mathbb{Q}_p^\times)^2$, that is, $D(ac - \frac{1}{4}b^2) \in (\mathbb{Q}_p^\times)^2$. By the assumption on D , $-\frac{4}{D} \in (\mathbb{Q}_p^\times)^2$ so $b^2 - 4ac \in (\mathbb{Q}_p^\times)^2$ which shows that $aX^2 + bXY + cY^2$ is isotropic over \mathbb{Q}_p . This implies the lemma. \square

Similarly, consider the action of G_2 on $K \setminus G_2$ and note that

$$\text{Stab}_{G_2}(K a_v k_v g_v) = g_v^{-1} k_v^{-1} a_v^{-1} K a_v k_v g_v = g_v^{-1} \mathbb{H}_v(\mathbb{R}) g_v.$$

Define the “diagonally embedded” algebraic torus \mathbb{L}_v by

$$\mathbb{L}_v(R) := \{(h, g_v^{-1} h g_v) : h \in \mathbb{H}_v(R)\}$$

for any ring R . It is defined over $\mathbb{Z} \subset \mathbb{Q}$ as so is \mathbb{H}_v and $g_v \in \text{SL}_3(\mathbb{Z})$.

In what follows we consider projections of an adelic orbit onto S -arithmetic homogeneous spaces. In order to define these projections note that \mathbb{G}_1 and \mathbb{G}_2 have class number one, that is, for $j = 1, 2$ and for any $T \subset V_{\mathbb{Q}} \setminus \{\infty\}$ we have

$$(3.5) \quad \mathbb{G}_j \left(\prod_{p \in T} \mathbb{Z}_p \right) \mathbb{G}_j(\mathbb{Z}^T) = \mathbb{G}_j(\mathbb{Q}_T).$$

Indeed, for \mathbb{G}_1 see [EMV10, §5.2] and for \mathbb{G}_2 it follows from the same, well-known (see [PR94]), assertions for the simply-connected algebraic group SL_2 and for \mathbb{G}_a^2 . This implies that for $\{\infty\} \subset S \subset S' \subset V_{\mathbb{Q}}$, if we let $X_j^S \stackrel{\text{def}}{=} \mathbb{G}_j(\mathbb{Q}_S) / \mathbb{G}_j(\mathbb{Z}^S)$, $X^S \stackrel{\text{def}}{=} X_1^S \times X_2^S$ we have a well-defined projection map $\pi_{S', S} : X^{S'} \rightarrow X^S$. The map $\pi_{S', S}$ is given by dividing by $\mathbb{G}(\prod_{p \in S' \setminus S} \mathbb{Z}_p)$ from the left and using (3.5). Now, consider the following adelic orbit

$$\mathcal{O}_D^{\mathbb{A}} := (k_v, e_f, a_v k_v g_v, e_f) \mathbb{L}_v(\mathbb{A}) \mathbb{G}(\mathbb{Q}) \subset X^{V_{\mathbb{Q}}},$$

where e_f denotes the identity element in $\mathbb{G}_j(\widehat{\mathbb{Z}})$ for $j = 1, 2$. Fix $\{\infty\} \subset S \subset V_{\mathbb{Q}}$ and set $\mathcal{O}_D^S \stackrel{\text{def}}{=} \pi_{V_{\mathbb{Q}}, S}(\mathcal{O}_D^{\mathbb{A}})$ and $\mu_{\mathcal{O}_D^S} = (\pi_{V_{\mathbb{Q}}, S})_*(\mu_{\mathcal{O}_D^{\mathbb{A}}})$ where $\mu_{\mathcal{O}_D^{\mathbb{A}}}$ is the uniform measure on this orbit. Although strictly speaking \mathcal{O}_D^S depends on v we omit v from the notation as we will see below that it will not play a crucial role.

We now describe \mathcal{O}_D^{∞} . Take a complete set of representatives $M_v \subset \mathbb{H}_v(\mathbb{A}_f)$ for the double coset space

$$\mathbb{H}_v(\mathbb{R} \times \widehat{\mathbb{Z}}) \backslash \mathbb{H}_v(\mathbb{A}) / \mathbb{H}_v(\mathbb{Q}) \cong \mathbb{H}_v(\widehat{\mathbb{Z}}) \backslash \mathbb{H}_v(\mathbb{A}_f) / \mathbb{H}_v(\mathbb{Q}),$$

which is finite by [PR94, Theorem 5.1]. For $h \in M_v$, using (3.5) we decompose $h = c_1(h)\gamma_1(h)^{-1}$ and $g_v^{-1}hg_v = c_2(h)\gamma_2(h)^{-1}$ with

$$(3.6) \quad c_j(h) \in \mathbb{G}_j(\widehat{\mathbb{Z}}), \gamma_j(h) \in \mathbb{G}_j(\mathbb{Q}), j = 1, 2.$$

We will use the abbreviation $\Theta_K \stackrel{\text{def}}{=} \{(k, k) : k \in K\}$. Moreover, let us write

$$\mathcal{O}_h \stackrel{\text{def}}{=} \Theta_K(k_v\gamma_1(h), a_vk_vg_v\gamma_2(h))\mathbb{G}(\mathbb{Z})$$

for $h \in M_v$.

Proposition 3.2. *Let $p : G/\Gamma \rightarrow (K \times K) \backslash G/\Gamma$ be the natural projection. Then,*

- (1) $\mathcal{O}_D^{\infty} = \bigsqcup_{h \in M_v} \mathcal{O}_h$.
- (2) For any $h \in M_v$ the orbit \mathcal{O}_h projects under p to a single point in $\text{supp}(\nu_D)$. Moreover, the correspondence $h \mapsto p(\mathcal{O}_h)$ is a bijection between M_v and $\text{supp}(\nu_D)$.
- (3) $p_*(\mu_{\mathcal{O}_D^{\infty}}) = \nu_D$.

Proof. (1) Using the set M_v of representatives we can write $\mathcal{O}_D^{\mathbb{A}}$ as a disjoint union of $\mathbb{L}_v(\mathbb{R} \times \widehat{\mathbb{Z}})$ -orbits:

$$\mathcal{O}_D^{\mathbb{A}} = \bigsqcup_{h \in M_v} (k_v, e_f, a_vk_vg_v, e_f)\mathbb{L}_v(\mathbb{R} \times \widehat{\mathbb{Z}})(e_{\infty}, h, e_{\infty}, g_v^{-1}hg_v)\mathbb{G}(\mathbb{Q}).$$

Decomposing each $h \in M_v$ and $g_v^{-1}hg_v$ as in (3.6) and using that

$$(\gamma_1(h), \gamma_1(h), \gamma_2(h), \gamma_2(h)) \in \mathbb{G}(\mathbb{Q})$$

we arrive at

$$\mathcal{O}_D^{\mathbb{A}} = \bigsqcup_{h \in M_v} (k_v, e_f, a_vk_vg_v, e_f)\mathbb{L}_v(\mathbb{R} \times \widehat{\mathbb{Z}})(\gamma_1(h), c_1(h), \gamma_2(h), c_2(h))\mathbb{G}(\mathbb{Q}).$$

Recalling that $\pi_{V_{\mathbb{Q}}, \{\infty\}}$ is given by dividing by $\mathbb{G}(\widehat{\mathbb{Z}})$ from the left we get

$$(3.7) \quad \mathcal{O}_D^{\infty} = \bigsqcup_{h \in M_v} (k_v, a_vk_vg_v)\mathbb{L}_v(\mathbb{R})(\gamma_1(h), \gamma_2(h))\mathbb{G}(\mathbb{Z}).$$

As $\mathbb{G}(\widehat{\mathbb{Z}}) \cap \mathbb{L}_v(\mathbb{A}_f) = \mathbb{L}_v(\widehat{\mathbb{Z}})$ this is indeed a disjoint union. Noting that $\Theta_K = (k_v, a_vk_vg_v)\mathbb{L}_v(\mathbb{R})(k_v^{-1}, (a_vk_vg_v)^{-1})$ we arrive at (1).

(2) We analyze $p(\mathcal{O}_h)$ for $h \in M_v$. We first concentrate on the \mathbb{G}_1 component. Identifying $K \backslash G_1/\Gamma_1 \cong \mathbf{S}^2$ we claim that $h \xrightarrow{\phi} Kk_v\gamma_1(h)\Gamma_1$ is a well-defined bijection between M_v and the set $\mathbf{S}^2(D)$. Indeed, it is shown in the proof of [PR94, Theorem 8.2] that under the above identification, ϕ is well-defined bijection between M_v and the set of all $\mathbf{w} \in \mathbf{S}^2(D)$ such that for all primes p there exists $g_p \in \mathbb{G}_1(\mathbb{Z}_p)$ with $g_p.v = w$ for some $v \in \mathbf{v}, w \in \mathbf{w}$ (where one uses the facts that \mathbb{G}_1 has class number 1 and that by Witt's Theorem $G_1(\mathbb{Q})$ act transitively on $\mathbb{S}^2(D)$). Now, by [EMV10, Lemma 5.4.1] the latter holds for any $\mathbf{w} \in \mathbf{S}^2(D)$, so ϕ is in fact a bijection from M_v to $\mathbf{S}^2(D)$ ¹.

To conclude the proof of (2) we show that if the first coordinate of $p(\mathcal{O}_h)$ is \mathbf{u} then the second one is $[\Lambda_{\mathbf{u}}]$. Let $h \in M_v$ and denote $\gamma_j = \gamma_j(h), c_j = c_j(h)$ for $j = 1, 2$ so that $\mathcal{O}_h = \Theta_K(k_v\gamma_1, a_vk_v g_v\gamma_2)\Gamma_1 \times \Gamma_2$. Note that $e_3^t k_v\gamma_1 = v^t\gamma_1 = (\gamma_1^{-1}v)^t$. We denote $u = \gamma_1^{-1}v$. We need to show that

$$(3.8) \quad Ka_vk_v g_v\gamma_2\Gamma_2 \stackrel{?}{=} [\Delta_u] = Ka_uk_u g_u\Gamma_2.$$

To see this note first that $a_v = a_u$ and that $k_v\gamma_1$ is a legitimate choice of k_u . With these choices, (3.8) (using the identity element of K on both sides) will follow once we show $g_u^{-1}\gamma_1^{-1}g_v\gamma_2 \in \Gamma_2$. The element $g_u^{-1}\gamma_1^{-1}g_v\gamma_2$ is certainly a determinant 1 element which maps \mathbb{R}^2 to itself. Furthermore, the third entry of its third column is positive by the orientation requirement in the definition of g_v and g_u . Therefore, it will be enough to show that this element maps \mathbb{Z}^3 to itself. Using that $\mathbb{Z} = \widehat{\mathbb{Z}} \cap \mathbb{Q} \subset \mathbb{A}_f$, we can see this as follows:

$$\begin{aligned} \mathbb{Q}^3 \supset g_u^{-1}\gamma_1^{-1}g_v\gamma_2\mathbb{Z}^3 &= g_u^{-1}c_1^{-1}(c_1\gamma_1^{-1})g_v(\gamma_2c_2^{-1})c_2\mathbb{Z}^3 = \\ &= g_u^{-1}c_1^{-1}hg_v g_v^{-1}h^{-1}g_v c_2\mathbb{Z}^3 = g_u^{-1}c_1^{-1}g_v c_2\mathbb{Z}^3 \subset \widehat{\mathbb{Z}}^3. \end{aligned}$$

(3) Recalling that $\mu_{\mathcal{O}_D^\infty} = (\pi_{V_{\mathbb{Q}, \infty}})_*(\mu_{\mathcal{O}_D^\Delta})$, we see that $\mu_{\mathcal{O}_D^\infty}(\mathcal{O}_h)$ is controlled by

$$\left| \text{Stab}_{\mathbb{L}_v(\mathbb{R} \times \widehat{\mathbb{Z}})}((e, h, e, g_v^{-1}hg_v)\mathbb{G}(\mathbb{Q})) \right|$$

which is independent of h as \mathbb{L}_v is commutative. This together with (2) shows that $p_*(\mu_{\mathcal{O}_D^\infty})$ is the normalized counting measure on its support. To show the same statement for ν_D we need to show that $|\text{Stab}_{\Gamma_1}(Kk_v\gamma_1(h))|$ is independent of h . For large enough D this is clear since Γ_1 is finite and every nontrivial $\gamma \in \Gamma_1$ fixes only two integer primitive points. The remaining cases can easily be checked (and are not really important for us). \square

3.1. From ASL_2 to SL_2 . Let us *momentarily* (see Remark 3.4) denote $\overline{\mathbb{G}}_2 = \text{SL}_2$ and let $\overline{X}_j^S, \overline{\mu}_{X_j^S}, \overline{\mathcal{O}}_D^S, \overline{\mu}_{\overline{\mathcal{O}}_D^S}$ be the analogous objects to the ones defined above. Note that $\overline{\mathbb{G}}_2$ also has class number 1. Simplified version of

¹Strictly speaking this is not needed but slightly simplifies the argument in §4.1.1 (cf. the higher dimensional case in [AES14]).

the discussion above implies analogous results for these analogous objects. In particular we have:

Corollary 3.3. *In order to establish the convergence (3.3) for a subset $A \subset \mathbb{N}$, it is enough to show that for some $\{\infty\} \subset S$, $\mu_{\overline{\mathcal{O}_D^S}}$ equidistribute to $\mu_{\overline{X_1^S}} \otimes \mu_{\overline{X_2^S}}$ when $D \rightarrow \infty, D \in A$.*

Remark 3.4. Since in the rest of the paper we will only prove results regarding SL_2 and in order not to burden the notation we change the notation introduced above and denote the objects related to SL_2 without the overline. For example, from now on, $\mathbb{G}_2 = \mathrm{SL}_2$.

4. DUKE'S THEOREM AND JOININGS

Choose any two distinct odd prime numbers p, q and define $S_0 = \{\infty, p, q\}$. Let η be a weak* limit of $(\mu_{\mathcal{O}_D^{S_0}})_{D \in \mathbb{D}(\{p, q\}) \cap \mathbb{F}}$ and let $\pi_j : X^{S_0} \rightarrow X_j^{S_0}$ denote the natural projections for $j = 1, 2$. Corollary 3.3 reduces the proof of Theorem 1.2 to the statement that $\eta = \mu_{X_1^{S_0}} \otimes \mu_{X_2^{S_0}}$. Roughly speaking, the latter will be obtained in two steps: the first, which relies on Duke's Theorem, is to show that $(\pi_j)_* \eta = \mu_{X_j^{S_0}}$ for $j = 1, 2$. The second uses [EL15] to bootstrap the information furnished by the first step to deduce that $\eta = \mu_{X_1^{S_0}} \otimes \mu_{X_2^{S_0}}$ (and it is this final step that requires the splitting condition at two places). For both steps (but mainly for the second step) we will need the following preliminary lemma:

Lemma 4.1. *Let η be a weak* limit as above. There exist $0 \neq v_p \in \mathbb{Z}_p^3, 0 \neq v_q \in \mathbb{Z}_q^3$ and $g_p \in \mathrm{SL}_3(\mathbb{Z}_p), g_q \in \mathrm{SL}_3(\mathbb{Z}_q)$ such that η is invariant under a diagonalizable subgroup of the form*

$$(4.1) \quad \mathbf{T} \stackrel{\mathrm{def}}{=} \{(h_p, h_q, g_p^{-1} h_p g_p, g_q^{-1} h_q g_q) : (h_p, h_q) \in \mathbb{H}_{v_p}(\mathbb{Q}_p) \times \mathbb{H}_{v_q}(\mathbb{Q}_q)\}.$$

Furthermore, $\mathbb{H}_{v_\ell}(\mathbb{Q}_\ell), \ell = p, q$ are split tori, and so $\mathbb{H}_{v_p}(\mathbb{Q}_p) \times \mathbb{H}_{v_q}(\mathbb{Q}_q)$ contains a group isomorphic to \mathbb{Z}^2 which is generated by an element $a_p \in \mathbb{H}_{v_p}(\mathbb{Q}_p)$ with eigenvalues $p, 1, p^{-1}$ and an element $a_q \in \mathbb{H}_{v_q}(\mathbb{Q}_q)$ with eigenvalues $q, 1, q^{-1}$.

Proof. By Hensel's lemma any vector v_D with $D \in \mathbb{D}(S_0)$ has the property that $D = Q_0(v_D) \in -(\mathbb{Z}_\ell^\times)^2$ for $\ell = p, q$. Moreover, $g_{v_D} \in \mathrm{SL}_3(\mathbb{Z}_\ell)$ for any prime ℓ . We assume that η is the weak* limit of $\mu_{\mathcal{O}_{D_n}^{S_0}}$ and let v_{D_n} denote the integral vector defining the orbit $\mathcal{O}_{D_n}^{S_0}$.

For any prime ℓ , \mathbb{Z}_ℓ^3 and $\mathrm{SL}_3(\mathbb{Z}_\ell)$ are compact sets. Thus we may choose a subsequence or, to simplify the notation, simply assume that (v_{D_n}) converges in \mathbb{Z}_p^3 to the vector v_p , in \mathbb{Z}_q^3 to v_q , $(g_{v_{D_n}})$ converges in $\mathrm{SL}_3(\mathbb{Z}_p)$ to g_p , and in $\mathrm{SL}_3(\mathbb{Z}_q)$ to g_q . Note that $\mathcal{O}_{D_n}^{S_0}$ admits a description, which is similar to Proposition 3.2(1), as a union of $\Theta_K \times \mathbb{L}_{v_{D_n}}(\mathbb{Q}_{\{p, q\}})$ -orbits. In particular

$\mu_{\mathcal{O}_{D_n}^{S_0}}$ is $\mathbb{L}_{v_{D_n}}(\mathbb{Q}_{\{p,q\}})$ -invariant. It readily follows that η is invariant under the group appearing in (4.1).

For the second assertion note that \mathbb{H}_{v_ℓ} is the (split) orthogonal group of the quadratic form Q_{v_ℓ} and that $Q_0(v_\ell) \in -(\mathbb{Z}_\ell^\times)^2$ for $\ell = p, q$. Here Q_{v_ℓ} is the isotropic (see the proof of (3.4)) quadratic form on the orthogonal complement of $v_\ell \in \mathbb{Q}_p^3$. The last assertion follows since $\mathbb{G}_1(\mathbb{Q}_\ell) \cong \mathrm{PGL}_2(\mathbb{Q}_\ell)$ for $\ell = p, q$ and any split torus is conjugated to the diagonal group. \square

4.1. Two instances of Duke's Theorem. In this section we prove the following proposition (which would hold for any S with $\infty \in S$):

Proposition 4.2. *For $j = 1, 2$ let $\mu_{i,D}$ denote the normalized probability measures on $\pi_j(\mathcal{O}_D^{S_0})$. Then $\mu_{i,D}$ equidistribute to $\mu_{X_j^{S_0}}$ when $D \rightarrow \infty$ with $D \in \mathbb{D}(\{p, q\}) \cap \mathbb{F}$. In particular, $(\pi_j)_* \eta = \mu_{X_j^{S_0}}$ for $j = 1, 2$.*

Both cases are special cases of the so-called Duke's Theorem [Duk88] and its refinements [HM06] (cf. [MV06] where Theorem 1 there corresponds to $j = 1$ and Theorem 2 to $j = 2$).

4.1.1. *Proof for $j = 1$.* As we wish to show equidistribution on the S_0 -adic space, we will use the formulation in [ELMV11, §4.6], with $\mathbf{G} = \mathbb{G}_1 = \mathrm{SO}_3$ being the projectivized group of units in the Hamiltonian quaternions.

Let μ be a weak* limit of a subsequence of $\mu_{1,D}$. Lemma 4.1 implies that μ is invariant under a product of two split tori $T = T_p \times T_q \subset \mathbb{G}_1(\mathbb{Q}_p) \times \mathbb{G}_1(\mathbb{Q}_q)$. By [ELMV11, §4.6] μ is also invariant under $\mathbb{G}_1(\mathbb{Q}_{S_0})^+ \stackrel{\mathrm{def}}{=} \Pi(\tilde{\mathbb{G}}_1(\mathbb{Q}_{S_0}))$ where $\Pi : \tilde{\mathbb{G}}_1 \rightarrow \mathbb{G}_1$ is the natural morphism from the simply-connected cover of \mathbb{G}_1 . We will be done once we show the following claim: $\mathbb{G}_1(\mathbb{Q}_{S_0})$ is generated by $\mathbb{G}_1(\mathbb{Q}_{S_0})^+$ and T . To this end, note that $\tilde{\mathbb{G}}_1(\mathbb{R}) \rightarrow \mathbb{G}_1(\mathbb{R})$ is surjective and so by [PR94, §8.2] there exists a homomorphism Ψ mapping the group $\mathbb{G}_1(\mathbb{Q}_{S_0})/\mathbb{G}_1(\mathbb{Q}_{S_0})^+$ to $S \stackrel{\mathrm{def}}{=} \mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2 \times \mathbb{Q}_q^\times/(\mathbb{Q}_q^\times)^2$. Furthermore, under the natural isomorphisms $\mathbb{G}_1(\mathbb{Q}_\ell) \cong \mathrm{PGL}_2(\mathbb{Q}_\ell)$, $\ell = p, q$, the coboundary map Ψ is nothing but the determinant map. With this it is easy to verify that the torus T is mapped surjectively onto S . Hence the proposition follows for $j = 1$.

4.1.2. *Proof for $j = 2$.* In this case, equidistribution follows from a subtler argument. For more details on the classical number theory constructions we are considering below see [Coh93, §5.2]. Recall that a binary quadratic form $q = aX^2 + bXY + cY^2$ over \mathbb{Z} is called primitive if $(a, b, c) = 1$ and that $\mathrm{disc}(q) \stackrel{\mathrm{def}}{=} b^2 - 4ac$. Primitivity and discriminant are stable under the usual $\mathrm{SL}_2(\mathbb{Z})$ -equivalence. Let $\mathrm{Bin}_L = \{[q] : \mathrm{disc}(q) = L\}$ denote the set of primitive positive definite binary quadratic forms of discriminant $L < 0$ considered up-to $\mathrm{SL}_2(\mathbb{Z})$ -equivalence. Finally recall that a number is called a fundamental discriminant if it is the discriminant of the maximal order in a quadratic field.

Claim 1. Let $v \in \mathbb{S}^2(D)$. If $D \equiv 1, 2 \pmod{4}$ then the two dimensional quadratic lattice $q_v \stackrel{\text{def}}{=} (\Lambda_v, x^2 + y^2 + z^2)$ defines an element in Bin_{-4D} . If $D \equiv 3 \pmod{4}$ then $q_v \stackrel{\text{def}}{=} (\Lambda_v, \frac{1}{2}(x^2 + y^2 + z^2))$ defines an element in Bin_{-D} .

Proof of Claim 1. The possible choices for an oriented basis of Λ_v give rise to the $\text{SL}_2(\mathbb{Z})$ -equivalence of binary quadratic forms. For calculating the discriminant and show primitivity, we choose v_1, v_2 as in the introduction as a \mathbb{Z} -basis for Λ_v and define Q_v to be the quadratic form $(\Lambda_v, x^2 + y^2 + z^2)$ with respect to this basis. That is, $Q_v = aX^2 + bXY + cY^2$, where $a = (v_1, v_1)$, $b = 2(v_1, v_2)$, $c = (v_2, v_2)$. It follows from Equation (1.1) that $ac - \frac{b^2}{4} = D$ or $\text{disc}(Q_v) = -4D < 0$. By construction Q_v is positive definite.

We will show that if $D \equiv 3 \pmod{4}$ then $2|a$ and $2|c$. Indeed, if $4 \nmid b$ the equation $ac - \frac{b^2}{4} = D$ implies that ac is divisible by 4. The claim follows since a and c are sums of three squares so if $4|a$ or $4|c$ we will have a contradiction to the primitivity of the vectors v_1 or v_2 . If $4|b$ then $ac \equiv 3 \pmod{4}$. So without loss of generality we may assume that $a \equiv 3, c \equiv 1 \pmod{4}$. This implies that all the coordinates of v_1 are odd and exactly two of the coordinates of v_2 are even. But then $\frac{b}{2} = (v_1, v_2)$ is odd, which is a contradiction. Primitivity of Q_v (resp. $\frac{1}{2}Q_v$ for $D \equiv 3 \pmod{4}$) and the last statement of the claim follow since for $D \in \mathbb{F}$ we have $\text{disc}(Q_v) = \text{disc}(\mathbb{Q}(\sqrt{-D}))$ (resp. $\text{disc}(\frac{1}{2}Q_v) = \text{disc}(\mathbb{Q}(\sqrt{-D}))$ for $D \equiv 3 \pmod{4}$), which implies the claim². \square

Due to Claim 1 we always set $L = -4D$ if $D \equiv 1, 2 \pmod{4}$ and $L = -D$ if $D \equiv 3 \pmod{4}$. Recall that $\mathcal{X}_2 \cong \Gamma_2 \backslash \mathbb{H}$ by sending $Kg\Gamma_2$ to $\Gamma_2 g^{-1} \cdot i \in \Gamma_2 \backslash \mathbb{H}$, where the action on $i \in \mathbb{H}$ is given by the regular Möbius transformation. For $\alpha \in \text{Bin}_L$ choose a quadratic form q such that $\alpha = [q]$ and we denote by z_q the unique root of $q(X, 1)$ belonging to the hyperbolic plane \mathbb{H} and by \mathbf{z}_q its Γ_2 -orbit. If $q = \frac{1}{2}Q$ (c.f. the case $D \equiv 3 \pmod{4}$ above), we may use the polynomial $q(X, 1)$ or $Q(X, 1)$ and obtain the same root — we may also write \mathbf{z}_Q for the Γ_2 -orbit of the root. Finally, we define $\mathbf{z}_\alpha = \mathbf{z}_q$ and note that this definition does not depend on the choice of q (within the Γ_2 -orbit). The set of Heegner points of discriminant L is $\mathcal{H}_L \stackrel{\text{def}}{=} \{\mathbf{z}_\alpha : \alpha \in \text{Bin}_L\}$.

Claim 2. Under the isomorphism $\mathcal{X}_2 \cong \Gamma_2 \backslash \mathbb{H}$ described above we have $\mathbf{z}_{q_v} = [\Lambda_v]$.

Proof of Claim 2. This follows from a straightforward calculation which is crucial to the argument, so we carry it out in details. Recall that $\phi : \text{ASL}_2 \rightarrow \text{SL}_2$ denotes the natural projection and let $M_v = \phi(a_v k_v g_v)$. The claim will follow once we show that $M_v^{-1} \cdot i = z_{Q_v}$ where Q_v is the quadratic form w.r.t. the basis v_1, v_2 used to define g_v . To this end, let $N_v = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ be the matrix whose columns are the first two entries of the vectors $k_v v_1, k_v v_2 \in \mathbb{R}^3$.

²The argument from [AES14, Lemma 3.3] could also be used to prove primitivity without the assumption $D \in \mathbb{F}$.

As scalar matrices act trivially as Möbius transformations, the action of a_v may be ignored and also the cases $D \equiv 3 \pmod{4}$ and $D \equiv 1, 2 \pmod{4}$ may be treated uniformly. In other words, it is enough to show that $N_v^{-1}.i = z_{Q_v}$. By the definition of k_v , the third entries of $k_v v_1, k_v v_2 \in \mathbb{R}^3$ are zeroes, so we have the following equalities: $\alpha^2 + \gamma^2 = \|v_1\|^2 = a$, $\beta^2 + \delta^2 = \|v_2\|^2 = c$ and $\alpha\beta + \gamma\delta = (v_1, v_2) = \frac{b}{2}$ and finally by (1.1) that $\det N_v = \alpha\delta - \beta\gamma = \sqrt{D}$. The claim now follows since

$$\begin{aligned} N^{-1}.i &= \frac{\delta i - \beta}{-\gamma i + \alpha} = \frac{-\frac{b}{2} + i\sqrt{D}}{a} \\ &= \frac{-b + \sqrt{-4D}}{2a} = \frac{-b + \sqrt{b^2 - 4ac}}{2a} = z_{Q_v}. \end{aligned}$$

□

It is well-known [Coh93, 5.2.8] that Bin_L , and therefore also \mathcal{H}_L , is parametrized by $\mathcal{C}_D \stackrel{\text{def}}{=} \text{Pic}(R_L)$, the class group of the unique order $R_L \subset \mathbb{Q}(\sqrt{-D})$ of discriminant L . By Claim 1, in both cases (regarding the definition of L in terms of D), \mathcal{C}_D is the class group of $\mathbb{Q}(\sqrt{-D})$.

Let

$$(4.2) \quad \mathcal{P}_D \stackrel{\text{def}}{=} \{\mathbf{z}_{q_v} : v \in \mathbb{S}^2(D)\} \subset \mathcal{H}_L.$$

Another instance of Duke's Theorem (see [MV06, Theorem 2]) implies that \mathcal{H}_L equidistribute on $\Gamma_2 \backslash \mathbb{H}$ when $D \rightarrow \infty$, $D \in \mathbb{D} \cap \mathbb{F}$. If \mathcal{P}_L would always be equal to \mathcal{H}_L , we could conclude in the same way as we did in the case $j = 1$ above (e.g. using [ELMV11, §4.6]). However, this is not always the case by the following claim.

Claim 3. Let \mathcal{C}_D^2 be the subgroup of squares in \mathcal{C}_D . Under the above mentioned parametrization of \mathcal{H}_L in terms of the class group \mathcal{C}_D the set \mathcal{P}_D corresponds to a coset of $\mathcal{C}_D^2 < \mathcal{C}_D$. We further note that $|\mathcal{C}_D^2| \asymp D^{\frac{1}{2}+o(1)}$ (and $\mathcal{C}_D^2 = \mathcal{C}_D$ if D is a prime).

Proof. This is shown in [EMV10, §4.2] as we now explain. Fix $D \in \mathbb{F} \cap \mathbb{D}$. As explained in [EMV10, §6], and in fact is proven implicitly in Proposition 3.2, the set $\mathbf{S}^2(D)$ is a torsor³ of \mathcal{C}_D . Also, Bin_L is naturally a torsor of \mathcal{C}_D . Note that $\alpha_{\mathbf{v}} \stackrel{\text{def}}{=} [q_v] \in \text{Bin}_L$ for $v \in \mathbf{v}$ is well-defined. It is shown in [EMV10, §4.2] that under these torsors structures, for any $\gamma \in \mathcal{C}_D, \mathbf{v} \in \mathbf{S}^2(D)$ we have

$$\alpha_{\gamma.\mathbf{v}} = \gamma^2.\alpha_{\mathbf{v}}.$$

Thus, it follows that the image of the map $\mathbf{v} \mapsto \alpha_{\mathbf{v}}$ in the torsor Bin_L corresponds to a coset of \mathcal{C}_D^2 . Thus, the same is true for $\mathcal{P}_D = \{\mathbf{z}_{q_v} : \mathbf{v} \in \mathbf{S}^2(D)\}$, which is the corresponding image in \mathcal{H}_L .

It is well-known [EMV10, (1.1)] that $\mathcal{C}_D, \mathbf{S}^2(D)$ and \mathcal{H}_L are asymptotically of size $D^{\frac{1}{2}+o(1)}$. Gauss' genus theory [Cas78, Chapter 14.4] tells us that

³A *torsor* of a group G is a set on which G acts freely and transitively.

$[\mathcal{C}_D : \mathcal{C}_D^2] = 2^{r(D)-1}$ where $r(D)$ is the number of distinct primes dividing D . Thus we also have $|\mathcal{C}_D^2| = |\mathcal{P}_D| \asymp D^{\frac{1}{2}+o(1)}$. \square

We can now establish the desired equidistribution on $X_2^{S_0}$. Recall from Proposition 3.2 that $p_*(\mu_{\mathcal{O}_D^\infty}) = \nu_D$. Let π_2 also denote the projection from X^∞ to X_2^∞ , and let π_K denote the projection from X_2^∞ to $K \backslash X_2^\infty = \mathcal{X}_2$. By Claim 2 we further get that $(\pi_K \circ \pi_2)_* \nu_D$ can be identified with the counting measure on $\mathcal{P}_D \subset \mathcal{X}_2 \cong \Gamma_2 \backslash \mathbb{H}$.

Therefore, the equidistribution of $(\pi_K \circ \pi_{S_0, \infty})_* \mu_{2,D}$ on \mathcal{X}_2 is equivalent to the equidistribution of \mathcal{P}_D on \mathcal{X}_2 . The equidistribution of such subsets, that is, subsets corresponding to cosets of large enough subgroups was established by [HM06, Theorem 6] (see also [Har, Corollary 1.4]) when $D \rightarrow \infty$ along $\mathbb{D} \cap \mathbb{F}$. This equidistribution comes in fact from a corresponding adelic statement. Since SL_2 is simply-connected (and in particular has class number 1) the desired S -arithmetic equidistribution for $j = 2$ follows from the proof of [HM06, Theorem 6]. \square

Remark 4.3. The only instance in which we use the assumption that $D \in \mathbb{F}$ is in the application of [HM06, Theorem 6]. Nevertheless it is known to experts that [HM06, Theorem 6] holds without the assumption that $D \in \mathbb{F}$, but such statement does not exist in print. A general adelic statement that will work for all discriminants is planned to appear in an appendix by Philippe Michel to an upcoming preprint ([AKA3]) of the first named author.

We also remark that as we assume the congruence condition $D \in \mathbb{D}(S_0)$ both equidistribution statements, i.e. for $\mu_{1,D}$ and $\mu_{2,D}$, may be deduced from the so-called Linnik’s Method (as it is done in slightly different context in [ELMV09, EMV10], see in particular [ELMV09, Prop. 3.6 (Basic lemma)] which only cares about the asymptotic size as in the last statement of Claim 3).

4.2. Joinings. From Proposition 4.2 we know that $(\pi_j)_* \eta = \mu_{X_j^{S_0}}$, $j = 1, 2$ and that η is a probability measure as π_2 has compact fibers and $\eta(X^{S_0}) = \mu_{X_2^{S_0}}(X_2^{S_0}) = 1$. Furthermore, by Lemma 4.1 η is invariant under the group \mathbf{T} that appears in (4.1). This means that η is a *joining* for the action of \mathbf{T} on the product space $X_1^{S_0} \times X_2^{S_0}$. Our goal, which is to show that $\eta = \mu_{X_1^{S_0}} \otimes \mu_{X_2^{S_0}}$, will follow from [EL15, Theorem 1.1]. Roughly speaking, it is shown there that a joining for a higher rank action (this is the reason we insist on S_0 to contain two primes) is always algebraic. As X_1^S is compact and X_2^S is non-compact, the only algebraic joining is given by the trivial joining. Below we will expand this argument in greater detail, where we will be more careful regarding the precise assumptions of [EL15, Theorem 1.1]. To satisfy these assumptions we need to reduce to the case where unipotents act ergodically, where we have a diagonally embedded action of \mathbb{Z}^2 by semisimple elements, and where the joining is ergodic. The precise definitions will be given below.

We fix some ad-hoc notation for this proof. Let $G^{S_0} = G_1^{S_0} \times G_2^{S_0}$ and $\Gamma^{S_0} = \Gamma_1^{S_0} \times \Gamma_2^{S_0}$ where $G_j^{S_0} = \mathbb{G}_j(\mathbb{Q}_{S_0})$ and $\Gamma_j^{S_0} = \mathbb{G}_j(\mathbb{Z}^{S_0})$ for $j = 1, 2$. Finally let $G^+ = G_1^+ \times G_2^{S_0}$ where $G_1^+ = \mathbb{G}_1(\mathbb{Q}_{S_0})^+$ is the (normal) open group defined in §4.1.1. Using G^+ we decompose X^{S_0} into finitely many disjoint G^+ -orbits $\mathbf{X}_r \stackrel{\text{def}}{=} G^+(g_r, e)\Gamma^{S_0}$, $r \in R$ for some $g_r \in G_1^{S_0}$ and an index set R .

By Proposition 4.2 for $j = 1$ we know that

$$(4.3) \quad \eta(\mathbf{X}_r) = \mu_{X_1^{S_0}}(G_1^+ g_r \Gamma_1^{S_0}) = \mu_{X^{S_0}}(G^+(g_r, e)\Gamma^{S_0}) > 0.$$

for all $r \in R$. Now fix some $r \in R$ and define the probability measure $\eta_r \stackrel{\text{def}}{=} \frac{1}{\eta(\mathbf{X}_r)} \eta|_{\mathbf{X}_r}$. It follows that

$$(\pi_1)_* \eta_r = \mu_1^r \stackrel{\text{def}}{=} \frac{1}{\eta(\mathbf{X}_r)} \mu_{X_1^{S_0}} \Big|_{G_1^+ g_r \Gamma_1^{S_0}},$$

where we may identify the latter with the normalized probability measure $\mu_{G_1^+ / (G_1^+ \cap g_r \Gamma_1^{S_0} g_r^{-1})}$. Also note that $(\pi_2)_* \eta_r = \mu_{X_2^{S_0}}$, that $G_1^+ \cap \mathbb{G}_1(\mathbb{R}) = \mathbb{G}_1(\mathbb{R})$ is connected, and that $G_1^+ \cap \mathbb{G}_1(\mathbb{Q}_{\{p,q\}})$ and $G_2^{S_0}$ are generated by one-parameter unipotent subgroups (see e.g. [BT73, §6.7]). Furthermore, G_1^+ (resp. $G_2^{S_0}$) act ergodically on the quotient $G_1^+ / (G_1^+ \cap g_r \Gamma_1^{S_0} g_r^{-1})$ (resp. on $X_2^{S_0}$) with respect to their uniform measure. This establishes one of the assumptions in [EL15, Thm. 1.1] — in the terminology of [EL15] the quotients $G_1^+ / (G_1^+ \cap g_r \Gamma_1^{S_0} g_r^{-1})$ and $G_2^{S_0} / \Gamma_2^{S_0}$ are “saturated by unipotents”.

Let

$$A = \{(a_1(\mathbf{n}), a_2(\mathbf{n})) : \mathbf{n} \in \mathbb{Z}^2\} < \mathbb{G}(\mathbb{Q}_{\{p,q\}})$$

be a subgroup isomorphic to \mathbb{Z}^2 as in Lemma 4.1. By construction $a_2(\mathbf{n}) = (g_p^{-1}, g_q^{-1})a_1(\mathbf{n})(g_p, g_q)$ for all $\mathbf{n} \in \mathbb{Z}^2$. Then, by Lemma 4.1 we have that η is invariant under A and that $a(\mathbf{n}) = (a_1(\mathbf{n}), a_2(\mathbf{n}))$ defines for $\mathbf{n} \in \mathbb{Z}^2$ a “class- \mathcal{A}' homomorphism”, in the terminology of [EL15]. Fix $r \in R$. As G_1^+ has finite-index in $G_1^{S_0}$, it follows that there exists a finite-index subgroup $\Lambda < \mathbb{Z}^2$ (again isomorphic to \mathbb{Z}^2) such that η_r is invariant under $B = a(\Lambda)$. The restriction of a to Λ is also of class- \mathcal{A}' . This establish another assumption of [EL15, Thm. 1.1].

In general η_r may not be B -ergodic, but a.e. ergodic component $\eta_{r,\tau}$ (with τ belonging to the probability space giving the ergodic decomposition) will now satisfy all assumptions in [EL15, Thm. 1.1]. In fact $\eta_{r,\tau}$ is an ergodic “joining for the higher rank action of $B = a(\Lambda)$ ” and we may conclude that $\eta_{r,\tau}$ is an algebraic joining. I.e. $\eta_{r,\tau}$ is the Haar measure on a closed orbit of the form $g_{r,\tau} M \Gamma$ where M is a finite index subgroup of a \mathbb{Q} -group $\mathbb{M} < \mathbb{G}_1 \times \mathbb{G}_2$ which projects onto \mathbb{G}_j for $j = 1, 2$. However, as both \mathbb{G}_1 and \mathbb{G}_2 are simple \mathbb{Q} -groups whose adjoint forms are different over \mathbb{Q} we obtain $\mathbb{M} = \mathbb{G}_1 \times \mathbb{G}_2$ and that $\eta_{r,\tau} = \mu_1^r \otimes \mu_{X_2^{S_0}}$ (for more details, see the comment after

[EL15, Theorem 1.1]). Using (4.3), it now follows that $\eta = \mu_{X_1^{S_0}} \otimes \mu_{X_2^{S_0}}$ as we wanted to show.

APPENDIX A. THE ASSOCIATED DIRICHLET SERIES
BY RUIXIANG ZHANG

In this appendix, we look at a sum related to the study of the equidistribution in Theorem 1.2, and explain some facts about them from the scope of classical analytic number theory. Theorem 1.2 has high dimensional twins, but we will concentrate on the theory in dimension 3, since we already saw that this is the most interesting dimension. Parallel theories have been developed in the references for higher dimensions.

Let \mathbb{H} be the usual upper half plane. Take ϕ on $\mathcal{X}_2 = \mathrm{SL}(2, \mathbb{Z}) \backslash \mathbb{H}$ to be a constituent of the spectrum decomposition, which can be a constant, a unitary Eisenstein series or a Maass cusp form, and then take a spherical harmonic ω on \mathbb{R}^3 . Assume k is the degree of the polynomial ω . We form the following Weyl sum for each positive integer n :

$$(A.1) \quad S(n, \omega, \phi) = \sum_{\mathbf{v} \in \mathbb{Z}_{\mathrm{prim}}^3, \|\mathbf{v}\|^2 = n} \omega\left(\frac{\mathbf{v}}{\|\mathbf{v}\|}\right) \phi(z_{\mathbf{v}}).$$

Here $z_{\mathbf{v}} \in \Gamma \backslash \mathbb{H}$ is defined as the following: Let the plane $b_{\mathbf{v}}$ be the orthogonal complement (with an orientation given by \mathbf{v}) of \mathbf{v} and $L_{\mathbf{v}}$ the lattice consisting of all the integer points on $b_{\mathbf{v}}$. The shape of $L_{\mathbf{v}}$ corresponds to a point $z_{\mathbf{v}} \in \Gamma \backslash \mathbb{H}$ in the usual sense. In other words, $z_{\mathbf{v}}$ in this appendix will denote the Heegner point attached to \mathbf{v} (previously defined by $z_{q_{\mathbf{v}}}$ in §4.1.2).

The motivation of this sum is the joint equidistribution Conjecture 1.1 in the paper. By a standard harmonic analysis argument (see the end), the pairs $(\frac{\mathbf{v}}{\|\mathbf{v}\|}, z_{\mathbf{v}})$ are jointly equidistributed if this sum, divided by the total number of \mathbf{v} 's, tend to zero (in some quantitative fashion) when either ω or ϕ is nontrivial.

As the first part of the appendix, we show that (A.1) is familiar to number theorists. In fact, this sum $S(n, \omega, \phi)$ can be interpreted as the n -th coefficient of the Dirichlet series obtained by taking the special value at the identity of a maximal parabolic Eisenstein series on $\mathrm{SL}(3, \mathbb{Z}) \backslash \mathrm{SL}(3, \mathbb{R})$ formed with respect to ϕ and ω . We now explain this correspondence and will state it as Theorem A.1.

In $G = \mathrm{SL}(3, \mathbb{R})$, let the discrete subgroup $\Gamma = \mathrm{SL}(3, \mathbb{Z})$. Take a maximal parabolic subgroup $P \subseteq G$ to be

$$(A.2) \quad P = \left\{ \begin{pmatrix} * & * & * \\ * & * & * \\ 0 & 0 & * \end{pmatrix} \in G \right\}.$$

According to the Langlands decomposition, we have $G = MANK$ where

$$\begin{aligned}
 M &= \left\{ \begin{pmatrix} * & * & 0 \\ * & * & 0 \\ 0 & 0 & 1 \end{pmatrix} \right\}, \\
 A &= \left\{ \begin{pmatrix} a^{-\frac{1}{4}} & 0 & 0 \\ 0 & a^{-\frac{1}{4}} & 0 \\ 0 & 0 & a^{\frac{1}{2}} \end{pmatrix}, a > 0 \right\}, \\
 N &= \left\{ \begin{pmatrix} 1 & 0 & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{pmatrix} \right\} \\
 K &= \mathrm{SO}(3, \mathbb{R}).
 \end{aligned}$$

Let

$$(A.3) \quad \Gamma_\infty = \left\{ \begin{pmatrix} * & * & * \\ * & * & * \\ 0 & 0 & 1 \end{pmatrix} \in \Gamma \right\}.$$

For an arbitrary $g \in G$ we can decompose it into

$$g = m(g)a(g)n(g)k(g), m(g) \in M, a(g) \in A, n(g) \in N, k(g) \in K.$$

This decomposition may not be unique. However, it is easy to see that $a(g)$ is unique, the bottom row $\mathbf{v}(g)$ of $k(g)$ is unique. By abuse of notation we will use $\omega(k(g))$ to denote $\omega(\mathbf{v}(g))$, and use $a(g)$ to denote the bottom right entry of (the matrix) $a(g)$. Moreover, $\phi(m(g))$ is well defined. It is also easy to verify that $\omega(k(g))$, $a(g)$ and $\phi(m(g))$ are invariant under the left multiplication by any element in Γ_∞ .

Therefore, for any $g \in G$, we form the sum

$$(A.4) \quad E(s, g, \omega, \phi) = \sum_{[\gamma] \in \Gamma_\infty \backslash \Gamma} \omega(k(\gamma g)) \phi(m(\gamma g)) a(\gamma g)^{-s}$$

which is the maximal parabolic Eisenstein series we mentioned above.

Since all elements in Γ have integral entries, when evaluated at the identity $g = I$, this series $E(s, I, \omega, \phi)$ become a Dirichlet series $\sum_{n=1}^{\infty} \frac{a_n}{n^s}$. We have

$$(A.5) \quad a_n = \sum_{[\gamma] \in \Gamma_\infty \backslash \Gamma: \text{the third row of } \gamma \text{ has length } \sqrt{n}} \omega(k(\gamma g)) \phi(m(\gamma g)).$$

We see some similarity between the summands of a_n and $S(n, \omega, \phi)$. Actually we have the following

Theorem A.1.

$$(A.6) \quad a_n = S(n, \omega, \phi).$$

Proof. First, note that all the primitive integer vectors of length \sqrt{n} have a natural 1-1 correspondence to the last rows of γ that have length \sqrt{n} , where $[\gamma] \in \Gamma_\infty \setminus \Gamma$. Thus with a primitive integer vector $\mathbf{v} = (a, b, c)$ of length \sqrt{n} we associated 1 summand in both sides. It suffices to show that both summands associated with \mathbf{v} are the same. It is obvious that the ω parts agree. We must show that the ϕ parts also agree. This is elementarily equivalent to the following statement: for the vector \mathbf{v} , the following two lattices have the same shape: (a) $\mathbb{Z}^3 \cap \mathbf{v}^\perp$ and (b) the projection of \mathbb{Z}^3 onto \mathbf{v}^\perp (which are both easily seen to be lattices of rank 2).

We now prove that for any vector $\mathbf{w} \in \mathbb{Z}^3 \cap \mathbf{v}^\perp$, there exists an integer vector \mathbf{u} such that $\mathbf{w} = \mathbf{v} \times \mathbf{u}$. In fact, we can assume $\mathbf{w} = (f, g, h)$ and without loss of generality assume that $c \neq 0$. Then we must find integers r, s, t such that $f = bt - cs, g = cr - at, h = as - br$. Note that by assumption we have $af + bg + ch = 0$. We deduce $\gcd(b, c) | af$. Since (a, b, c) is primitive, we have $\gcd(a, \gcd(b, c)) = 1$ and thus $\gcd(b, c) | f$. Hence we can choose t such that $c | f - bt$. In this situation $c | af + bg - a(f - bt)$, or $c | b(g + at)$. Hence we can change t by a multiple of $\frac{c}{\gcd(b, c)}$, if necessary, to make both $c | f - bt$ and $c | g + at$. Now we just set $s = \frac{bt-f}{c}, r = \frac{g+at}{c}$. It is then easy to deduce $h = as - br$ by the fact that $af + bg + ch = 0$.

By the last paragraph, the entire lattice (a) is the cross product of the lattice (b) and the vector \mathbf{v} . Hence they have the same shape and the theorem is proved. \square

It is not surprising that one could use the Dirichlet series $E(s, I, \omega, \phi)$ to study the analytic properties of the Weyl sum a_n , which would be naturally required if one wants to remove the congruence conditions of Theorem 1.2 and prove Conjecture 1.1.

To address the problem, we need a good estimate for all individual coefficients a_n . The work of Gauss (see e.g. [Ven70] for a nice account) shows that the total number of summands in a_n is given by the following theorem.

Theorem A.2 (Gauss[GM89]). *Given an integer $n > 3$. The number of coprime integer solutions (x, y, z) to the equation $n = x^2 + y^2 + z^2$ is $12h$ for $n \equiv 1, 2 \pmod{4}$, and is $24h'$ for $n \equiv 3 \pmod{8}$, where h and h' are the number of properly and improperly primitive classes of positive forms of determinant $-n$.*

By Siegel's theorem together with Dirichlet's class number formula (see [Dav67]), h and $h' \gg_\epsilon n^{\frac{1}{2}-\epsilon}$, and are usually around $n^{\frac{1}{2}}$ (with an arbitrary small error on the exponent). So we would like to have a power saving from the exponent $\frac{1}{2}$ for all a_n .

Remark A.3. We note that it suffices to consider *even* forms ω and ϕ . Otherwise it is obvious that $a_n = 0$. We assume this is the case for the rest of the discussion.

It is still not clear how to do this in the greatest generality. But there have been partial results. Part of the following brief account already appeared in §4.1 but we recall it once more for the reader’s convenience. In the special case $\phi = 1$, this reduces to a situation that could be treated with Iwaniec’s celebrated estimation of Fourier coefficients for half-integral weight holomorphic modular forms [Iwa87], as the series become a theta series. For the case $\omega = 1$ again by the work of Gauss [Ven70] we know we are summing the ϕ over a certain genus of quadratic forms of determinant $-n$. If we pretend that we are summing over all the quadratic forms (CM points), this can be settled using Duke’s generalization of Iwaniec’s argument to non-holomorphic forms [Duk88]. Using Waldspurger’s formula and subconvexity the power saving for the real problem is also known [HM06].

For general ϕ and ω , the connection of the series $E(s, I, \omega, \phi)$ to modular forms is still mysterious and we currently do not have the desired power saving. Nevertheless, since it is a specific value (meaning for the fixed $g = I$) of an Eisenstein series, the analytic continuation and the functional equation are known (see e.g. [Ter82]). Interestingly, Maass, when originally dealing with this very equidistribution problem (but in the ball, not on the sphere), also deduced these analytic properties [Maa59] [Maa71]. The following theorem could be easily derived from Maass’s work in [Maa71] (see Chapter 16).

Theorem A.4. *Let $\Xi(s, \omega, \phi) = E(s, I, \omega, \phi)\Lambda^*(s, \phi)$. Then $\Xi(s, \omega, \phi)$ is holomorphic on \mathbb{C} except for a possible pole at $s = \frac{3}{2}$. The pole exists if and only if both ω and ϕ are trivial. Also $\Xi(s, \omega, \phi)$ satisfies the functional equation*

$$(A.7) \quad \Xi\left(\frac{3}{2} - s, \omega, \phi\right) = \Xi(s, \omega, \phi).$$

Here $\Lambda^*(s, \phi)$ is a kind of “completed L -function of ϕ ” which we now define. Assume $\lambda(1 - \lambda)$ is the eigenvalue of the Laplacian $\Delta = -y^2(\frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2})$ for ϕ . When ϕ is a constant or unitary Eisenstein series, $\Lambda^*(s, \phi)$ factorizes:

$$(A.8) \quad \Lambda^*(s, \phi) = \Lambda(2s - \lambda, \zeta)\Lambda(2s - (1 - \lambda), \zeta)$$

where $\Lambda(s, \zeta) = \pi^{-\frac{s}{2}}\Gamma(\frac{s}{2})\zeta(s)$ is (up to normalization) the completed Riemann zeta function. When ϕ is a Maass cusp form, $\Lambda^*(s, \phi) = \Lambda(2s - \frac{1}{2}, \phi)$. Where $\Lambda(s, \phi)$ is the usual completed L -function of ϕ (we use the fact that ϕ is even):

$$(A.9) \quad \Lambda(s, \phi) = \pi^{-s}\Gamma\left(\frac{s}{2} + \frac{\lambda}{2} - \frac{1}{4}\right)\Gamma\left(\frac{s}{2} - \frac{\lambda}{2} + \frac{1}{4}\right)L(s, \phi).$$

With only the analytic properties stated in Theorem A.4, we cannot expect to get a good control of the size of each individual term $|a_n|$. However we can get an “average bound” for the sum of a_n . Next we will show one such bound.

We prove the following:

Theorem A.5.

(A.10)

$$\sum_{n \leq X} a_n = \left(\frac{1}{\text{Area}(\mathbb{S}^2)} \int_{\mathbb{S}^2} \omega \right) \left(\frac{1}{\text{Area}(\mathcal{X}_2)} \int_{\mathcal{X}_2} \phi \right) X^{\frac{3}{2}} + O_{\omega, \phi, \epsilon}(X^{\frac{15}{14} + \epsilon}).$$

Obviously, the product of the integrals (main term) in (A.10) is nonzero if and only if both ω and ϕ are trivial.

Proof. We fix ω, ϕ from the beginning. By lattice points counting, the theorem is obvious when ω and ϕ are trivial. Next we assume that this is not the case. To be explicit, let's assume ϕ is a Maass cusp form. Other cases are similar. We invoke a theorem, which is a general bound about sums of coefficients of Dirichlet series. We state the theorem in the form we need.

Theorem A.6 (A special case of Theorem 4.1 in [CN62]). *Assuming we have two Dirichlet series $f(s) = \sum_{n=1}^{\infty} \frac{c_n}{n^s}$ and $g(s) = \sum_{n=1}^{\infty} \frac{d_n}{n^s}$ and a product of Gamma factors $\Delta(s) = \prod_{\nu=1}^N \Gamma(\alpha_{\nu}s + \beta_{\nu})$, satisfying the functional equation*

$$(A.11) \quad \Delta(s)f(s) = \Delta(M-s)g(M-s)$$

for some $M > 0$. Also assume f is entire. Then

$$(A.12) \quad \sum_{n \leq X} c_n = O(X^{\frac{M}{2} - \frac{1}{4A} + 2A\eta u}) + O\left(\sum_{X < n \leq X'} |c_n|\right).$$

In (A.12), $A = \sum_{\nu=1}^N \alpha_{\nu} \geq 1$, $X' = X + O(X^{1-\eta-\frac{1}{2A}})$, $u = \beta - \frac{M}{2} - \frac{1}{4A}$ where β satisfies $\sum_{n=1}^{\infty} \frac{|d_n|}{n^{\beta}} < \infty$, η is any positive number at our disposal.

Take $f = g = E(s, I, \omega, \phi)L(2s - \frac{1}{2}, \phi)$. Maass proved $E(s, I, \omega, \phi)L(2s - \frac{1}{2}, \phi)$ is entire [Maa71], which enables us to do the substitution. We see here $M = \frac{3}{2}$. By Theorem A.4, $E(s, I, \omega, \phi)L(2s - \frac{1}{2}, \phi)$ has a functional equation with two Gamma factors, meaning $A = 2$. Finally we determine β . Assume $L(s, \phi) = \sum_{n=1}^{\infty} \frac{b_n}{n^s}$. Then $L(2s - \frac{1}{2}, \phi) = \sum_{n=1}^{\infty} \frac{b_n \sqrt{n}}{n^{2s}}$. Hence $|c_n| = |d_n| \leq \sum_{m^2 k = n} |a_k| |b_m| \sqrt{m} \leq \sum_{m^2 k = n} k^{\frac{1}{2} + \epsilon} m \ll n^{\frac{1}{2} + \epsilon}$. We can take $\beta = \frac{3}{2} + \epsilon$ and thus $u = \frac{5}{8} + \epsilon$.

We conclude that $\sum_{n \leq X} c_n = O(X^{\frac{5}{8} + (\frac{5}{2} + \epsilon)\eta}) + O(X^{\frac{5}{4} + \epsilon - \eta})$. After an optimization we get $\sum_{n \leq X} c_n = O(X^{\frac{15}{14} + \epsilon})$. Now if $\frac{1}{L(s, \phi)} = \sum_{n=1}^{\infty} \frac{h_n}{n^s}$, from the Euler product of $L(s, \phi)$ we easily get $|h_n| \ll n^{\frac{1}{2}}$. Hence

(A.13)

$$\left| \sum_{n \leq X} a_n \right| = \left| \sum_{n \leq X} h_n \sqrt{n} \sum_{mn^2 \leq X} c_m \right| \ll \left| \sum_{n \leq X} |h_n| \sqrt{n} \left(\frac{X}{n^2}\right)^{\frac{15}{14} + \epsilon} \right| \ll X^{\frac{15}{14} + \epsilon}.$$

□

We end the discussion with some further remarks concerning this approach. All the dependencies on ω and ϕ are polynomial in terms of their eigenvalues and can be made explicit by a slightly more careful treatment. It is then standard to do a spectral decomposition (of the smoothed characteristic function of the underlying domain) and take the Weyl law (see [Sel91]) into account, to get an estimate of the remainder term needed for the joint equidistribution result “in a big ball” — pairs $(\frac{\mathbf{v}}{\|\mathbf{v}\|}, z_{\mathbf{v}})$ get jointly equidistributed for $\|\mathbf{v}\| \leq n$ when $n \rightarrow \infty$. We can also get the joint equidistribution “in a thinner shell” (for some $X^{1-\theta} < \|\mathbf{v}\| < X$) where $\theta > 0$ depends on the remainder term we have. But the conjectured joint equidistribution result “on every sphere of a reasonable radius” (Conjecture 1.1) requires new ideas.

This type of (quantitative) bounds for the remainder term of the averaged size of a_n were also obtained by elementary methods by Schmidt [Sch98], in more general cases. Our approach will also have corresponding generalization for higher dimensional settings.

REFERENCES

- [AES14] M. Aka, M. Einsiedler, and U. Shapira, *Integer points on spheres and their orthogonal grids*, preprint (2014). [↑4, 8, 11](#)
- [BT73] A. Borel and J. Tits, *Homomorphismes “abstrait” de groupes algébriques simples*, Ann. of Math. (2) **97** (1973), 499–571. MR0316587 (47 #5134) [↑14](#)
- [Cas78] J. W. S. Cassels, *Rational quadratic forms*, London Mathematical Society Monographs, vol. 13, Academic Press Inc. [Harcourt Brace Jovanovich Publishers], London, 1978. [↑12](#)
- [CN62] K Chandrasekharan and R. Narasimhan, *Functional equations with multiple gamma factors and the average order of arithmetical functions*, Annals of Mathematics (1962), 93–136. [↑19](#)
- [Coh93] H. Cohen, *A course in computational algebraic number theory*, Vol. 138, Springer, 1993. [↑10, 12](#)
- [Dav67] H. Davenport, *Multiplicative number theory*, Englewood Cliffs, NJ (1967). [↑17](#)
- [Duk88] W. Duke, *Hyperbolic distribution problems and half-integral weight Maass forms*, Invent. Math. **92** (1988), no. 1, 73–90. MR931205 (89d:11033) [↑2, 3, 10, 18](#)
- [EL15] M. Einsiedler and E. Lindenstrauss, *Joinings of higher rank torus actions on homogeneous spaces*, preprint (2015). [↑3, 6, 9, 13, 14, 15](#)
- [ELMV09] M. Einsiedler, E. Lindenstrauss, P. Michel, and A. Venkatesh, *Distribution of periodic torus orbits on homogeneous spaces*, Duke Math. J. **148** (2009), no. 1, 119–174. MR2515103 (2010k:37004) [↑3, 13](#)
- [ELMV11] M. Einsiedler, E. Lindenstrauss, P. Michel, and A. Venkatesh, *Distribution of periodic torus orbits and Duke’s theorem for cubic fields*, Ann. of Math. (2) **173** (2011), no. 2, 815–885. MR2776363 (2012h:37006) [↑10, 12](#)
- [EMSS] M. Einsiedler, S. Mozes, S. Shah, and U. Shapira, *Equidistribution of primitive rational points on expanding horospheres*. Preprint. [↑3](#)
- [ERW14] M. Einsiedler, R. Rühr, and P. Wirth, *Effective equidistribution of shapes of orthogonal lattices*, preprint (2014). [↑4](#)
- [EMV10] J. S. Ellenberg, P. Michel, and A. Venkatesh, *Linnik’s ergodic method and the distribution of integer points on spheres*, arXiv preprint arXiv:1001.0897 (2010). [↑3, 6, 8, 12, 13](#)

- [EV08] J. S. Ellenberg and A. Venkatesh, *Local-global principles for representations of quadratic forms*, Invent. Math. **171** (2008), no. 2, 257–279. MR2367020 (2008m:11081) ↑[6](#)
- [Gau86] C. F. Gauss, *Disquisitiones arithmeticae*, Springer-Verlag, New York, 1986. Translated and with a preface by Arthur A. Clarke, Revised by William C. Waterhouse, Cornelius Greither and A. W. Grootendorst and with a preface by Waterhouse. MR837656 (87f:01105) ↑[1](#)
- [GM89] C. F. Gauss and H. Maser, *Untersuchungen über höhere arithmetik*, J. Springer, 1889. ↑[17](#)
- [Har] G. Harcos, *Subconvex bounds for automorphic L -functions and applications*. This is an unpublished dissertation available at <http://www.renyi.hu/gharcos/ertekezes.pdf>. ↑[13](#)
- [HM06] G. Harcos and P. Michel, *The subconvexity problem for Rankin-Selberg L -functions and equidistribution of Heegner points. II*, Invent. Math. **163** (2006), no. 3, 581–655. MR2207235 (2007j:11063) ↑[3](#), [5](#), [10](#), [13](#), [18](#)
- [Iwa87] H. Iwaniec, *Fourier coefficients of modular forms of half-integral weight*, Invent. Math. **87** (1987), no. 2, 385–401. MR870736 (88b:11024) ↑[2](#), [3](#), [18](#)
- [Lin68] Yu. V. Linnik, *Ergodic properties of algebraic fields*, Translated from the Russian by M. S. Keane. Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 45, Springer-Verlag New York Inc., New York, 1968. MR0238801 (39 #165) ↑[1](#), [3](#)
- [Maa56] H. Maass, *Spherical functions and quadratic forms*, J. Indian Math. Soc **20** (1956), 117–162. ↑[3](#)
- [Maa59] H. Maass, *Über die Verteilung der zweidimensionalen Untergitter in einem euklidischen Gitter*, Mathematische Annalen **137** (1959), 319–327. ↑[18](#)
- [Maa71] H. Maass, *Siegel’s modular forms and Dirichlet series*, Lecture Notes in Mathematics, Vol. 216, Springer-Verlag, Berlin-New York, 1971. ↑[18](#), [19](#)
- [Mar10] J. Marklof, *The asymptotic distribution of Frobenius numbers*, Invent. Math. **181** (2010), no. 1, 179–207. ↑[3](#)
- [MV06] P. Michel and A. Venkatesh, *Equidistribution, L -functions and ergodic theory: on some problems of Yu. Linnik*, International Congress of Mathematicians. Vol. II, 2006, pp. 421–457. MR2275604 (2008g:11085) ↑[10](#), [12](#)
- [PR94] V. Platonov and A. Rapinchuk, *Algebraic groups and number theory*, Pure and Applied Mathematics, vol. 139, Academic Press Inc., Boston, MA, 1994. Translated from the 1991 Russian original by Rachel Rowen. MR1278263 (95b:11039) ↑[6](#), [7](#), [8](#), [10](#)
- [Sch98] W. M. Schmidt, *The distribution of sublattices of \mathbf{Z}^m* , Monatsh. Math. **125** (1998), no. 1, 37–81. ↑[3](#), [20](#)
- [Sel91] A. Selberg, *Harmonic analysis, in “collected papers”, vol. i*, Springer-Verlag, 1991. ↑[20](#)
- [Ter82] A. Terras, *On automorphic forms for the general linear group*, JOURNAL OF MATHEMATICS **12** (1982), no. 1. ↑[18](#)
- [Ven70] B. A. Venkov, *Elementary number theory*, Wolters-Noordhoff, 1970. ↑[17](#), [18](#)

M.A. DEPARTEMENT MATHEMATIK, ETH ZÜRICH, RÄMISTRASSE 101, 8092 ZÜRICH, SWITZERLAND
E-mail address: menashe-hai.akka@math.ethz.ch

M.E. DEPARTEMENT MATHEMATIK, ETH ZÜRICH, RÄMISTRASSE 101, 8092 ZÜRICH, SWITZERLAND
E-mail address: manfred.einsiedler@math.ethz.ch

U.S. DEPARTMENT OF MATHEMATICS, TECHNION, HAIFA, ISRAEL
E-mail address: `ushapira@tx.technion.ac.il`

R.Z. DEPARTEMENT OF MATHEMATICS, PRINCETON UNIVERSITY, FINE HALL, WASHINGTON ROAD, PRINCETON, NJ USA 08544
E-mail address: `ruixiang@math.princeton.edu`