Integer points on spheres and their orthogonal lattices

Journal Article

Author(s):
Aka, Menny; Einsiedler, Manfred; Shapira, Uri

Publication date:
2016-11

Permanent link:
https://doi.org/10.3929/ethz-b-000114302

Rights / license:
In Copyright - Non-Commercial Use Permitted

Originally published in:
Inventiones mathematicae 206(2), https://doi.org/10.1007/s00222-016-0655-7

Funding acknowledgement:
152819 - Equidistribution and dynamics on homogeneous spaces (SNF)
Integer points on spheres and their orthogonal lattices

Menny Aka¹ · Manfred Einsiedler¹ · Uri Shapira²

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 breakthrough 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.

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.

☑️ Manfred Einsiedler
manfred.einsiedler@math.ethz.ch

Menny Aka
menashe-hai.akka@math.ethz.ch

Uri Shapira
ushapira@tx.technion.ac.il

¹ Departement Mathematik, ETH Zürich, Rämistrasse 101, 8092 Zurich, Switzerland
² Department of Mathematics, Technion, Haifa, Israel
1 Introduction

A theorem of Legendre, whose complete proof was given by Gauss in [14], 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 \( \mathbb{D} = \{ D \in \mathbb{N} : D \not\equiv 0, 4, 7 \mod 8 \} \) and \( \mathbb{Z}_3^{\text{prim}} \) be the set of primitive vectors in \( \mathbb{Z}^3 \). Legendre’s Theorem also implies that the set

\[
S^2(D) \overset{\text{def}}{=} \left\{ v \in \mathbb{Z}_3^{\text{prim}} : \|v\|_2^2 = D \right\}
\]

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 \( S \subseteq \mathbb{P} \) be a subset of the odd prime numbers and set

\[
\mathbb{D}(S) = \left\{ D \in \mathbb{D} : \text{for all } p \in S, \ -D \mod p \in \left( \mathbb{F}_p^* \right)^2 \right\}.
\]

In the late 1950’s Linnik [18] proved that \( \left\{ \frac{v}{\|v\|} : v \in S^2(D) \right\} \) equidistribute to the uniform measure on \( \mathbb{S}^2 \) when \( D \to \infty \) under the restrictive assumption \( D \in \mathbb{D}(p) \) where \( p \) is an odd prime. As we will again recall in this paper [see Eq. (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 to remove the congruence condition. A full solution of Linnik’s problem was given by Duke [6] (following a breakthrough by Iwaniec [17]), who used entirely different methods.

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

First, note that

\[
[Z^3 : (Zv \oplus \Lambda_v)] = D \tag{1.1}
\]

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 \( \|v\| \mathbf{e}_3 \) 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

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

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. Up to \(\Lambda_v\), there is a unique vector \(w \in \mathbb{Z}^2\) with \((w, v) = 1\). Its well-defined orthogonal projection to the 2-dimensional torus \(v^\perp / \Lambda_v\) is a \(D\)-torsion point. In order to keep track of the information furnished by \(w\) and \(\Lambda_v\) in a corresponding homogeneous space we proceed as follows: First we choose a basis \(v_1, v_2\) of the lattice \(\Lambda_v\) with \(\det(v_1, v_2, v) > 0\). Then we 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 \(\text{ASL}_2 = \{(g \in \text{SL}_2) | g \in \text{ASL}_2(\mathbb{Z})\}\). Also note that the set of choices for \(k_v\) is the coset \(\text{StabSO}_3(\mathbb{R})(e_3)k_v = \text{SO}_2(\mathbb{R})k_v\). Finally, 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

\[
\mathcal{Y}_2 \overset{\text{def}}{=} \text{SO}_2(\mathbb{R}) \backslash \text{ASL}_2(\mathbb{R}) / \text{ASL}_2(\mathbb{Z}),
\]

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 \(\tilde{v}_D\) denote the normalized counting measure on the set

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

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

\[
\tilde{v}_D \overset{\text{weak}^*}{\longrightarrow} m_{S^2} \otimes m_{\mathcal{Y}_2} \quad \text{as} \quad D \to \infty \text{ with } D \in A \quad (1.2)
\]

where \(m_{S^2} \otimes m_{\mathcal{Y}_2}\) is the product of the natural uniform measures on \(S^2\) 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 $A = \mathbb{D} = \{D : D \equiv 0, 4, 7 \mod 8\}$.

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

$$\left\{ \left( \frac{v}{\|v\|}, [\Lambda v] \right) : v \in S_2^2(D) \right\} \subset S_2^2 \times \mathcal{X}_2.$$ 

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

$$\tilde{\mu}_D \overset{\text{weak}^*}{\longrightarrow} m_{S_2^2} \otimes m_{\mathcal{X}_2} \quad \text{as} \quad D \to \infty \text{ with } D \in A. \quad (1.3)$$

Using two splitting conditions (see Sect. 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 [21] and Schmidt [24] (see also [10]), but as we later learned from Sarnak and Zhang, the question is closely related to the work of Maass [19,20].

Our method of proof builds on the equidistribution on $S^2$ and on $\mathcal{X}_2$ (respectively on related covering spaces) as obtained by Linnik [18] or Duke [6] (and in one instance more precisely the refinement of Duke’s theorem obtained by Harcos and Michel [16]). 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 Lindenstrauss and the second named author in [7]. 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 [16], see also Remarks 4.4. As Theorem 1.2 is assuming a splitting condition (actually two) Linnik’s method [18] could (most likely) be used to overcome the square-free condition. We refer also to [8,12], where the Linnik method is used for slightly different problems.

Using a break-through of Iwaniec [17], it was shown by Duke [6] 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. Some findings in this direction appear in an appendix by Ruixiang Zhang [25] to the Arxived version of this paper.
As we explain in Sect. 4.1 the equidistribution of \( \{ [\Lambda_v] : v \in S^2(D) \} \) 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 \( \{ [\Delta_v] : v \in S^2(D) \} \) 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 [1] 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 [1]. In an upcoming paper [11] of Wirth, Rühr, and the second named author the full result is obtained for \( d = 4, 5 \) by using effective dynamical arguments.

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 \( \infty \). 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 \( \mathbb{A}_f = \prod_{p \in V_\mathbb{Q} \setminus \{ \infty \}} \mathbb{Q}_p, \hat{\mathbb{Z}} = \prod_{p \in V_\mathbb{Q} \setminus \{ \infty \}} \mathbb{Z}_p \) and \( \mathbb{Z}^S = \mathbb{Z}[\{\frac{1}{p} : p \in S \setminus \{ \infty \}\}] \).

Recall that \( \mathbb{Q} = \mathbb{Z}^\mathbb{V}_\mathbb{Q} \) is a cocompact lattice in the adeles \( \mathbb{A} = \mathbb{Q}_{V_\mathbb{Q}} \). 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 \( \mu_n \) on a locally compact space \( X \) is said to equidistribute to a probability measure \( \mu \) as \( n \to \infty \) if the sequence converges to \( \mu \) in the weak* topology on the space of probability measures on \( X \). A probability measure \( \mu \) is called a weak* limit of a sequence of measures \( \mu_n \) if there exists a subsequence \( (n_k) \) such that \( \mu_{n_k} \) equidistribute to \( \mu \) as \( k \to \infty \).

Given a locally compact group \( L \) and a closed 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 \( \pi \) (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 \( \pi : L/M \to K \backslash L/M \) 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 Sect. 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 Sect. 4.1, we use Duke’s Theorem (resp. [16]) to deduce that these orbits equidistribute to a joining (see Sect. 4
for the definition). Then, in Sect. 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 \( \text{ASL}_2 \).

Let \( G_1 = \text{SO}_3 \), \( G_2 = \text{ASL}_2 \) and \( G = G_1 \times G_2 \), \( G_j = G_j(\mathbb{R}) \), \( \Gamma_j = G_j(\mathbb{Z}) \) for \( j = 1, 2 \) and \( G = G(\mathbb{R}) \), \( \Gamma = \Gamma(\mathbb{Z}) \), \( K = \text{SO}_2(\mathbb{R}) \) and fix \( v \in S^2(D) \), \( D \in \mathbb{D} \) throughout this section. We wish to identify \( K \backslash G_1 \cong S^2 \) so we let \( k \in G_1 \) act on \( S^2 \) by the right action \( (k, u) \mapsto k.u = k^{-1}u \); we find it simpler to think of \( S^2 \) as row vectors and use the definition \( (k, u) \mapsto k.u = u'k \). 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 \( e_3^T k_v = \|v\|^{-1} v' \).

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

\[
K \times K (k_v, a_v k_v g_v) \Gamma_1 \times \Gamma_2
\]

represents the pair

\[
\left( \frac{v}{\|v\|}, [\Delta_v] \right) \in S^2 \times Y_2.
\]

Note that all the measures appearing in Eq. (1.2) (resp. Eq. (1.3)) are \( \Gamma_1 \)-invariant so if we consider their projections \( \nu_D \) (resp. \( \mu_D \)) of \( \tilde{\nu}_D \) (resp. \( \tilde{\mu}_D \)) to \( S^2 \times Y_2 \) (resp. \( S^2 \times X_2 \)) we have that the convergence (1.2) is equivalent to

\[
\nu_D \overset{\text{weak-}*}{\longrightarrow} m_{S^2} \otimes m_{Y_2}, \quad D \rightarrow \infty, \quad D \in A
\]

and the convergence (1.3) is equivalent to

\[
\mu_D \overset{\text{weak-}*}{\longrightarrow} m_{S^2} \otimes m_{X_2}, \quad D \rightarrow \infty, \quad D \in A.
\]

Roughly speaking, integral orbits on the \( \mathbb{Z} \)-points of a variety admitting a \( \mathbb{Z} \)-action of an algebraic group \( P \) may be parametrized by an adelic quotient of the stabilizer. E.g., as we will see below, \( \Gamma_1 \)-orbits of vectors in \( S^2(D) \), can be parametrized by an adelic quotient of the stabilizer of \( v \). The interested reader may consult [13, §3], [12, §6.1] and [23, 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 Lindenstrauss [7].

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

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 assume that $D = Q_0(v) \neq 0$. We have that

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

**Proof** Let $w_1, w_2$ be a basis of the orthogonal complement of $v$ within $\mathbb{Q}_p^3$. Notice first that $H_v(\mathbb{Q}_p) \cong \text{SO}(aX^2 + bXY + cY^2)$, 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, $D(ac - \frac{1}{4}b^2) \in (\mathbb{Q}_p^\times)^2$. Since $4 \in (\mathbb{Q}_p^\times)^2$ we have $-D(b^2 - 4ac) \in (\mathbb{Q}_p^\times)^2$. Now we see that $-D \in (\mathbb{Q}_p^\times)^2$ if and only if $b^2 - 4ac \in (\mathbb{Q}_p^\times)^2$. This happens if and only if $aX^2 + bXY + cY^2$ is isotropic over $\mathbb{Q}_p$ which is if and only if $H_v(\mathbb{Q}_p)$ is a split torus. \hfill $\square$

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

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

Define the “diagonally embedded” algebraic torus $L_v$ by

$$L_v(R) := \{(h, g_v^{-1}hg_v) : h \in H_v(R)\}$$

for any ring $R$. It is defined over $\mathbb{Z} \subset \mathbb{Q}$ as so is $H_v$ 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 $G_1$ and $G_2$ have class number one, that is, for $j = 1, 2$ and for any $T \subset V_Q \setminus \{\infty\}$ we have

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

Indeed, for $G_1$ see [12, §5.2] and for $G_2$ it follows from the same, well-known (see [23]), assertions for the simply-connected algebraic group $\text{SL}_2$ and for $G_2^\times$. This implies that for $\{\infty\} \subset S \subset S' \subset V_Q$, if we let $X^S_j \overset{\text{def}}{=} G_j(\mathbb{Q}_S)/G_j(\mathbb{Z}_S)$,
$X^S \overset{\text{def}}{=} X_1^S \times X_2^S$ we have a well-defined projection map $\pi_{S',S} : X^{S'} \to X^S$. The map $\pi_{S',S}$ is given by dividing by $G(\prod_{p \in S' \setminus S} \mathbb{Z}_p)$ from the left and using \((3.5)\). Now, consider the following adelic orbit

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

where $e_f$ denotes the identity element in $G_j(\hat{\mathbb{Z}})$ for $j = 1, 2$. Fix $\{\infty\} \subset S \subset V\mathbb{Q}$ and set $O_S^S := \pi_{V\mathbb{Q},S}(O_D^A)$ and $\mu_{O_S^S} = (\pi_{V\mathbb{Q},S})_*(\mu_{O_D^A})$ where $\mu_{O_D^A}$ is the uniform measure on this orbit. Although strictly speaking $O_S^S$ 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 $O_\infty^D$. Take a complete set of representatives $M_v \subset \mathbb{H}_v(\mathbb{A}_f)$ for the double coset space

$$H_v(\mathbb{R} \times \hat{\mathbb{Z}}) \backslash H_v(\mathbb{A}) / H_v(\mathbb{Q}) \cong H_v(\hat{\mathbb{Z}}) \backslash H_v(\mathbb{A}_f) / H_v(\mathbb{Q}),$$

which is finite by \([23, \text{Theorem } 5.1]\). For $h \in M_v$, using \((3.5)\) we decompose $h = c_1(h)\gamma_1(h)^{-1}$ and $g_v^{-1} h g_v = c_2(h)\gamma_2(h)^{-1}$ with

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

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

$$O_h \overset{\text{def}}{=} \Theta_K (k_v \gamma_1(h), a_v k_v g_v \gamma_2(h))G(\mathbb{Z})$$

for $h \in M_v$. Note that $\Theta_K = (k_v, a_v k_v g_v) \mathbb{L}_v(\mathbb{R})(k_v^{-1}, (a_v k_v g_v)^{-1})$ so

$$O_h = (k_v, a_v k_v g_v) \mathbb{L}_v(\mathbb{R})(\gamma_1(h), \gamma_2(h))G(\mathbb{Z}).$$

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

1. $O_\infty^D = \bigcup_{h \in M_v} O_h$.
2. For any $h \in M_v$ the orbit $O_h$ projects under $p$ to a single point in support($\nu_D$). Moreover, the correspondence $h \mapsto p(O_h)$ is a bijection between $M_v$ and support($\nu_D$). In particular, the union in (1) is a disjoint union.
3. $p_*(\mu_{O_\infty^D}) = \nu_D$. 

\(\square\) Springer
Proof (1) Using the set $M_v$ of representatives we can write $O^\Lambda_D$ as a disjoint union of $L_v(R \times \hat{\mathbb{Z}})$-orbits:

$$O^\Lambda_D = \bigcup_{h \in M_v} (k_v, e_f, a_v k_v g_v, e_f) L_v (R \times \hat{\mathbb{Z}}) (e_\infty, h, e_\infty, g_v^{-1} h g_v) G(\mathbb{Q}).$$

Decomposing each $h \in M_v$ and $g_v^{-1} h g_v$ as in (3.6) and using that $(\gamma_1(h), \gamma_1(h), \gamma_2(h), \gamma_2(h)) \in G(\mathbb{Q})$

we arrive at

$$O^\Lambda_D = \bigcup_{h \in M_v} (k_v, e_f, a_v k_v g_v, e_f) L_v (R \times \hat{\mathbb{Z}}) (\gamma_1(h), c_1(h), \gamma_2(h), c_2(h)) G(\mathbb{Q}).$$

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

$$O^\infty_D = \bigcup_{h \in M_v} (k_v, a_v k_v g_v) L_v (R) (\gamma_1(h), \gamma_2(h)) G(\mathbb{Z}).$$

With this we arrive at (1).

(2) We analyze $p(O_h)$ for $h \in M_v$. We first concentrate on the $G_1$ component. Identifying $K \setminus G_1 / \Gamma_1 \simeq S^2$ we claim that $h \mapsto K k_v \gamma_1(h) \Gamma_1$ is a well-defined bijection between $M_v$ and the set $S^2(D)$. Indeed, it is shown in the proof of [23, Theorem 8.2] that under the above identification, $\phi$ is well-defined bijection between $M_v$ and the set of all $w \in S^2(D)$ such that for all primes $p$ there exists $g_p \in G_1(\mathbb{Z}_p)$ with $g_p \cdot w = w$ for some $v \in v, w \in w$ [where one uses the facts that $G_1$ has class number 1 and that by Witt’s Theorem $G_1(\mathbb{Q})$ act transitively on $S^2(D)$]. Now, by [12, Lemma 5.4.1] the latter holds for any $w \in S^2(D)$, so $\phi$ is in fact a bijection from $M_v$ to $S^2(D).$ This already implies that the union in (1) is a disjoint union.

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

$$K a_v k_v g_v \gamma_2 \Gamma_2 \equiv [\Delta_u] = K a_u k_u g_u \Gamma_2.$$  

(3.8)

1 Strictly speaking this is not needed but slightly simplifies the argument in Sect. 4.1.1 (cf. the higher dimension case in [1]).
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 $\mathbb{Z} = \hat{\mathbb{Z}} \cap \mathbb{Q} \subset \mathbb{A}_f$, we can see this as follows:

\[
\mathbb{Q}^3 \supset g_u^{-1} \gamma_1^{-1} g_v \gamma_2 \mathbb{Z}^3 = g_u^{-1} c_1^{-1} (c_1 \gamma_1^{-1}) g_v (\gamma_2 c_2^{-1}) c_2 \mathbb{Z}^3
\]

\[
= g_u^{-1} c_1^{-1} h g_v g_v^{-1} h^{-1} g_v c_2 \mathbb{Z}^3 = g_u^{-1} c_1^{-1} g_v c_2 \mathbb{Z}^3 \subset \hat{\mathbb{Z}}^3.
\]

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

\[
|\text{Stab}_{L_v(\mathbb{R} \times \hat{\mathbb{Z}})}((e, h, e, g_v^{-1} h g_v) G(\mathbb{Q}))|
\]

which is independent of $h$ as $L_v$ is commutative. This together with (2) shows that $\rho_*(\mu_{\mathcal{O}_D^\infty})$ is the normalized counting measure on its support. To show the same statement for $\nu_D$ we need to show that $|\text{Stab}_{\Gamma_1}(K k_v \gamma_1(h))|$ is independent of $h$. For large enough $D$ this is clear since $\Gamma_1$ 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 $\overline{G}_2 = \text{SL}_2$ and let $\overline{X}_j^S, \mu_{\overline{X}_j^S}, \overline{\mathcal{O}}_D^S, \mu_{\overline{\mathcal{O}}_D^S}$ be the analogous objects to the ones defined above. Note that $\overline{G}_2$ also has class number 1. Simplified version of 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 $D \to \infty$, $D \in A$.

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

\[\square\] Springer
4 Duke’s theorem and joinings

Choose any two distinct odd prime numbers \(p, q\) and define \(S_0 = \{\infty, p, q\}\). Let \(\eta\) be a weak* limit of \((\mu_{\mathcal{O}^S_D})_{D \in \mathbb{D}(\{p, q\})} \cap \mathbb{F}\) and let \(\pi_j : X_{S_0} \to X_{S_0}^{s_j}\) denote the natural projections for \(j = 1, 2\). Corollary 3.3 reduces the proof of Theorem 1.2 to the statement that \(\eta = \mu_{X_1} \otimes \mu_{X_2}\). Roughly speaking, the latter will be obtained in two steps: the first, which relies on Duke’s Theorem, is to show that \((\pi_j)_* \eta = \mu_{X_0}\) for \(j = 1, 2\). The second uses [7] to bootstrap the information furnished by the first step to deduce that \(\eta = \mu_{X_1} \otimes \mu_{X_2}\) (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 \(\eta\) 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 \(g_p \in SL_3(\mathbb{Z}_p)\), \(g_q \in SL_3(\mathbb{Z}_q)\) such that \(\eta\) is invariant under a diagonalizable subgroup of the form

\[
T \overset{\text{def}}{=} \{(h_p, h_q, g_p^{-1}h_pg_p, g_q^{-1}h_qg_q) : (h_p, h_q) \in \mathbb{H}_{v_p}(\mathbb{Q}_p) \times \mathbb{H}_{v_q}(\mathbb{Q}_q)\}.
\]

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 \(\mathbb{Z}_2^2\) 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 \(D = Q_0(v_D) \in -(\mathbb{Z}_\ell^X)^2\) for \(\ell = p, q\). Moreover, \(g_{v_D} \in SL_3(\mathbb{Z}_\ell)\) for any prime \(\ell\). We assume that \(\eta\) is the weak* limit of \(\mu_{\mathcal{O}_{D_n}}\) and let \(v_{D_n}\) denote the integral vector defining the orbit \(\mathcal{O}_{D_n}^{S_0}\).

For any prime \(\ell\), \(\mathbb{Z}_\ell^3\) and \(SL_3(\mathbb{Z}_\ell)\) 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 \(SL_3(\mathbb{Z}_p)\) to \(g_p\), and in \(SL_3(\mathbb{Z}_q)\) 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 \(\mathcal{O}_K \times L_{v_{D_n}}(\mathbb{Q}(\ell))\)-orbits. In particular \(\mu_{\mathcal{O}_{D_n}^{S_0}}\) is \(L_{v_{D_n}}(\mathbb{Q}(\ell))\)-invariant. It readily follows that \(\eta\) is invariant under the group appearing in (4.1).

For the second assertion note that \(\mathbb{H}_{v_\ell}\) is the (split) orthogonal group of the quadratic form \(Q_{v_\ell}\) and that \(Q_0(v_\ell) \in -(\mathbb{Z}_\ell^X)^2\) for \(\ell = p, q\). Here \(Q_{v_\ell}\) is the isotropic [see the proof of (3.4)] quadratic form on the orthogonal complement of \(v_\ell \in \mathbb{Q}_\ell^3\). The last assertion follows since \(\mathbb{G}_1(\mathbb{Q}_\ell) \cong \text{PGL}_2(\mathbb{Q}_\ell)\) 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 $\mu_{j,D}$ denote the normalized probability measures on $\pi_j(O_D^{S_0})$. Then $\mu_{i,D}$ equidistribute to $\mu_{X_j^{S_0}}$ when $D \to \infty$ with $D \in \mathbb{D}(\{p, q\}) \cap \mathbb{F}$.

**Corollary 4.3** For any weak* limit $\eta$ of $(\mu_{O_D^{S_0}})_{D \in \mathbb{D}(\{p, q\}) \cap \mathbb{F}}$ we have that $(\pi_j)_*\eta = \mu_{X_j^{S_0}}$ for $j = 1, 2$.

Both cases are special cases of the so-called Duke’s Theorem [6] and its refinements [16] (cf. [22] where Theorem 1 there corresponds to $j = 1$ and Theorem 2 to $j = 2$). Note that $D \in \mathbb{F}$ implies the primitivity assumption that is sometimes used in the statement of Duke’s Theorem. This assumption is not needed (See [12, §10.1] and Remark 4.4). The proof of Proposition 4.2 is given in the next two subsections.

4.1.1 Proof of Proposition 4.2 for $j = 1$

As we wish to show equidistribution on the $S_0$-adic space, we will use the formulation in [9, §4.6], with $G = G_1 = \text{SO}_3$ being the projectivized group of units in the Hamiltonian quaternions.

Let $\mu$ be a weak* limit of a subsequence of $\mu_{1,D}$. Lemma 4.1 implies that $\mu$ is invariant under a product of two split tori $T = T_p \times T_q \subset G_1(\mathbb{Q}_p) \times G_1(\mathbb{Q}_q)$.

By [9, §4.6] $\mu$ is also invariant under $G_1(\mathbb{Q}_{S_0})^+ \overset{\text{def}}{=} \Pi((\tilde{G}_1(\mathbb{Q}_{S_0})))$ where $\Pi : \tilde{G}_1 \to G_1$ is the natural morphism from the simply-connected cover of $G_1$.

We will be done once we show the following claim: $G_1(\mathbb{Q}_{S_0})$ is generated by $G_1(\mathbb{Q}_{S_0})^+$ and $T$. To this end, note that $G_1(\mathbb{R}) \to G_1(\mathbb{R})$ is surjective. Furthermore, under the natural isomorphisms $G_1(\mathbb{Q}_\ell) \cong \text{PGL}_2(\mathbb{Q}_\ell), \ell = p, q$ the group

$$G_1(\mathbb{Q}_p \times \mathbb{Q}_q)/G_1(\mathbb{Q}_p \times \mathbb{Q}_q)^+ \cong \text{PGL}_2(\mathbb{Q}_p \times \mathbb{Q}_q)/\Pi(SL_2(\mathbb{Q}_p \times \mathbb{Q}_q))$$

is mapped to $S \overset{\text{def}}{=} \mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2 \times \mathbb{Q}_q^\times/(\mathbb{Q}_q^\times)^2$ via the determinant map. Since the determinant map maps the torus $T$ onto $S$, this implies Proposition 4.2 for $j = 1$. 

Springer
4.1.2 Proof of Proposition 4.2 for \( j = 2 \)

In this case, equidistribution follows from a subler argument. For more details on the classical number theory constructions we are considering below see [5, §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 \( \text{disc}(q) \overset{\text{def}}{=} b^2 - 4ac \). Primitivity and discriminant are stable under the usual \( \text{SL}_2(\mathbb{Z}) \)-equivalence. Let \( \text{Bin}_L = \{ [q] : \text{disc}(q) = L \} \) denote the set of primitive positive definite binary quadratic forms of discriminant \( L < 0 \) considered up-to \( \text{SL}_2(\mathbb{Z}) \)-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 \( v \in S^2(D) \). If \( D \equiv 1, 2 \pmod{4} \) then the two dimensional quadratic lattice \( q_v \overset{\text{def}}{=} (\Lambda_v, x^2 + y^2 + z^2) \) defines an element in \( \text{Bin}_{-4D} \). If \( D \equiv 3 \pmod{4} \) then \( q_v \overset{\text{def}}{=} (\Lambda_v, \frac{1}{2}(x^2 + y^2 + z^2)) \) defines an element in \( \text{Bin}_{-D} \).

Proof of Claim 1 The possible choices for an oriented basis of \( \Lambda_v \) 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 \( \Lambda_v \) 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 Eq. (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 claim.\(^2\) \( \square \)

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 \( K \Gamma_2 t \) to \( \Gamma_2 \gamma^{-1} i \in \Gamma_2 \backslash \mathbb{H} \), where the action on \( i \in \mathbb{H} \) is given by the regular M"{o}bius transformation.

\(^2\) The argument from [1, Lemma 3.3] could also be used to prove primitivity without the assumption \( D \in \mathbb{F} \).
For $\alpha \in \text{Bin}_L$ choose a quadratic form $q$ such that $\alpha = [q]$ and we denote by $z_q$ its $\Gamma_2$-orbit. If $q = \frac{1}{2}Q$ (c.f. the case $D \equiv 3 \mod 4$ above), we may use the polynomial $q(X, 1)$ or $Q(X, 1)$ and obtain the same root—we may also write $z_Q$ for the $\Gamma_2$-orbit of the root. Finally, we define $z_\alpha = z_q$ and note that this definition does not depend on the choice of $q$ (within the $\Gamma_1/2$-orbit). The set of Heegner points of discriminant $L$ is $\mathcal{H}_L \overset{\text{def}}{=} \{ z_\alpha : \alpha \in \text{Bin}_L \}$.

**Claim 2** Under the isomorphism $X_2 \cong \Gamma_2 \backslash \mathbb{H}$ described above we have $z_q \circ_i = [\Lambda_1]_v$.

**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 $M_v^{-1} \cdot i = z_Q$ 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 $N_v = \left( \begin{array}{cc} \alpha & \beta \\ \gamma & \delta \end{array} \right)$ be the matrix whose columns are the first two entries of the vectors $k_v v_1, k_v v_2 \in \mathbb{R}^3$. As scalar matrices act trivially as Möbius transformations, the action of $a_v$ may be ignored and also the cases $D \equiv 3 \mod 4$ and $D \equiv 1, 2 \mod 4$ may be treated uniformly. In other words, it is enough to show that $N_v^{-1} \cdot i = z_Q$. 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

$$
N^{-1} \cdot i = \frac{\delta i - \beta}{-\gamma i + \alpha} = \frac{-b + i \sqrt{D}}{a} = \frac{-b + \sqrt{-4D}}{2a} = z_Q.
$$

\[ \square \]

It is well-known [5, 5.2.8] that $\text{Bin}_L$, and therefore also $\mathcal{H}_L$, is parametrized by $C_D \overset{\text{def}}{=} \text{Pic}(R_L)$, 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 $D$), $C_D$ is the class group of $\mathbb{Q}(\sqrt{-D})$.

Let

$$
\mathcal{P}_D \overset{\text{def}}{=} \{ z_{q_v} : v \in S^2(D) \} \subset \mathcal{H}_L.
$$

(4.2)

Another instance of Duke’s Theorem (see [22, 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 [9, §4.6]). However, this is not always the case by the following claim.
Claim 3 Let $C_D^2$ be the subgroup of squares in $C_D$. Under the above mentioned parametrization of $\mathcal{H}_L$ in terms of the class group $C_D$ the set $P_D$ corresponds to a coset of $C_D^2 < C_D$. We further note that $|C_D^2| \asymp D^{\frac{1}{2} + o(1)}$ (and $C_D^2 = C_D$ if $D$ is a prime).

Proof This is shown in [12, §4.2] as we now explain. Fix $D \in \mathbb{F} \cap \mathbb{D}$. As explained in [12, §6], and in fact is proven implicitly in Proposition 3.2, the set $S^2(D)$ is a torsor\(^3\) of $C_D$. Also, $\text{Bin}_L$ is naturally a torsor of $C_D$. Note that $\alpha_v \overset{\text{def}}{=} [q_v] \in \text{Bin}_L$ for $v \in \mathfrak{v}$ is well-defined. It is shown in [12, §4.2] that under these torsors structures, for any $\gamma \in C_D$, $v \in S^2(D)$ we have $\alpha_{\gamma \cdot v} = \gamma^2 \cdot \alpha_v$.

Thus, it follows that the image of the map $v \mapsto \alpha_v$ in the torsor $\text{Bin}_L$ corresponds to a coset of $C_D^2$. Thus, the same is true for $P_D = \{z_{q_v} : v \in S^2(D)\}$, which is the corresponding image in $\mathcal{H}_L$.

It is well-known [12, (1.1)] that $C_D, S^2(D)$ and $\mathcal{H}_L$ are asymptotically of size $D^{\frac{1}{2} + o(1)}$. Gauss’ genus theory [4, Chapter 14.4] tells us that $[C_D : C_D^2] = 2^{r(D) - 1}$ where $r(D)$ is the number of distinct primes dividing $D$. Thus we also have $|C_D^2| = |P_D| \asymp D^{\frac{1}{2} + o(1)}$. $\square$

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

Therefore, the equidistribution of $(\pi_K \circ \pi_{S_0, \infty})_\ast \mu_{2, D}$ on $\mathcal{H}_2$ is equivalent to the equidistribution of $P_D$ on $\mathcal{H}_2$. The equidistribution of such subsets, that is, subsets corresponding to cosets of large enough subgroups was established by [16, Theorem 6] (see also [15, Corollary 1.4]) when $D \to \infty$ along $\mathbb{D} \cap \mathbb{F}$. This equidistribution comes in fact from a corresponding adelic statement. Since $\text{SL}_2$ is simply-connected (and in particular has class number 1) the desired $S$-arithmetic equidistribution for $j = 2$ follows from the proof of [16, Theorem 6]. This concludes the proof of Proposition 4.2 for $j = 2$. $\square$

Remark 4.4 The only instance in which we use the assumption that $D \in \mathbb{F}$ is in the application of [16, Theorem 6]. Nevertheless it is known to experts that [16, 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 ([2]) of the first named author.

\(^3\) A torsor of a group $G$ is a set on which $G$ acts freely and transitively.
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 [8,12], see in particular [8, Prop. 3.6 (Basic lemma)] which only cares about the asymptotic size as in the last statement of Claim 3).

### 4.2 Joinings

From Corollary 4.3 we know that \( (\pi_j)_* \eta = \mu_{X_{S_0}^j}, \; j = 1, 2 \) and in particular that \( \eta \) is a probability measure. Furthermore, by Lemma 4.1 \( \eta \) is invariant under the group \( T \) that appears in (4.1). This means that \( \eta \) is a joining for the action of \( T \) on the product space \( X_{S_0}^1 \times X_{S_0}^2 \). Our goal, which is to show that \( \eta = \mu_{X_{S_0}^1} \otimes \mu_{X_{S_0}^2} \), will follow from [7, 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 \( X_{S_0}^1 \) is compact and \( X_{S_0}^2 \) 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 [7, 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 \( G_{S_0}^1 = G_{S_0}^2 \times G_{S_0}^2 \) and \( \Gamma_{S_0} = \Gamma_{S_0}^1 \times \Gamma_{S_0}^2 \) where \( G_{j,S_0}^j = \mathbb{G}_j(\mathbb{Q}_{S_0}) \) and \( \Gamma_{j,S_0} = \mathbb{G}_j(\mathbb{Z}_{S_0}) \) for \( j = 1, 2 \).

Finally let \( G^+ = G_{1,S_0}^+ \times G_{2,S_0}^2 \) where \( G_{1,S_0}^1 = \mathbb{G}_1(\mathbb{Q}_{S_0})^+ \) is the (normal) open group defined in Sect. 4.1.1. Using \( G^+ \) we decompose \( X_{S_0}^1 \) into finitely many disjoint \( G^+\)-orbits \( X_r \), \( r \in R \) for some \( g_r \in G_{1,S_0}^1 \) and an index set \( R \).

By Proposition 4.2 for \( j = 1 \) we know that

\[
\eta(X_r) = \mu_{X_{S_0}^1}(G_{1,S_0}^1 g_r \Gamma_{1,S_0}^1) = \mu_{X_{S_0}^1}(G_{1,S_0}^+(g_r,e) \Gamma_{S_0}^1) > 0.
\]

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

\[
(\pi_1)_* \eta_r = \mu_{1,S_0}^r \overset{\text{def}}{=} \left. \frac{1}{\eta(X_r)} \mu_{X_{S_0}^1} \right|_{G_{1,S_0}^+ g_r \Gamma_{1,S_0}^1},
\]

where we may identify the latter with the normalized probability measure \( \mu_{G_{1,S_0}^+/G_{1,S_0}^1 g_r \Gamma_{1,S_0}^1} \). Also note that \((\pi_2)_* \eta_r = \mu_{X_{S_0}^2}, \) that \( G_{1,S_0}^1 \cap \mathbb{G}_2(\mathbb{R}) = \ldots \)
$G_1(\mathbb{R})$ is connected, and that $G_1^+ \cap G_1(\mathbb{Q}_{(p,q)})$ and $G_2^{S_0}$ are generated by one-parameter unipotent subgroups (see e.g. [3, §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 [7, Theorem. 1.1]—in the terminology of [7] 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 $A = \{(a_1(\mathbf{n}), a_2(\mathbf{n})) : \mathbf{n} \in \mathbb{Z}^2 \} < G(\mathbb{Q}_{(p,q)})$ 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 $\eta$ 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 [7]. 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 $\eta_r$ is invariant under $B = a(\Lambda)$. The restriction of $a$ to $\Lambda$ is also of class-$\mathcal{A}'$. This establish another assumption of [7, Theorem. 1.1].

In general $\eta_r$ may not be $B$-ergodic, but a.e. ergodic component $\eta_{r,\tau}$ (with $\tau$ belonging to the probability space giving the ergodic decomposition) will now satisfy all assumptions in [7, Theorem. 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 $M < G_1 \times G_2$ which projects onto $G_j$ for $j = 1, 2$. However, as both $G_1$ and $G_2$ are simple $\mathbb{Q}$-groups whose adjoint forms are different over $\mathbb{Q}$ we obtain $M = G_1 \times G_2$ and that $\eta_{r,\tau} = \mu_{r,\tau} = \mu_{S_0} \otimes \mu_X$ (for more details, see the comment after [7, Theorem 1.1]). Using (4.3), it now follows that $\eta = \mu_X \otimes \mu_X$ as we wanted to show.

Acknowledgments 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.

References

1. Aka, M., Einsiedler, M., Shapira, U.: Integer points on spheres and their orthogonal grids. J. Lond. Math. Soc. 93(1), 143–158 (2016)

Springer
2. Aka, M.: Continued fractions of arithmetic sequences of quadratics, in preparation. With an appendix by Philippe Michel (preprint)
3. Borel, A., Tits, J.: Homomorphismes “abstraits” de groupes algébriques simples. Ann. Math. 2(97), 499–571 (1973)
4. Cassels, J.W.S.: Rational Quadratic Forms, London Mathematical Society Monographs, vol. 13. Academic Press Inc. [Harcourt Brace Jovanovich Publishers], London (1978)
5. Cohen, H.: A Course in Computational Algebraic Number Theory, vol. 138. Springer, New York (1993)
6. Duke, W.: Hyperbolic distribution problems and half-integral weight Maass forms. Invent. Math. 92(1), 73–90 (1988)
7. Einsiedler, M., Lindenstrauss, E.: Joinings of higher rank torus actions on homogeneous spaces. http://arxiv.org/abs/1502.05133 (2015)
8. Einsiedler, M., Lindenstrauss, E., Michel, P., Venkatesh, A.: Distribution of periodic torus orbits on homogeneous spaces. Duke Math. J. 148(1), 119–174 (2009)
9. Einsiedler, M., Lindenstrauss, E., Michel, P., Venkatesh, A.: Distribution of periodic torus orbits and Duke’s theorem for cubic fields. Ann. Math. 173(2), 815–885 (2011)
10. Einsiedler, M., Mozes, S., Shah, S., Shapira, U.: Equidistribution of primitive rational points on expanding horospheres. doi:10.1112/S0010437X15007605
11. Einsiedler, M., Rühr, R., Wirth, P.: Effective equidistribution of shapes of orthogonal lattices (preprint)
12. Ellenberg, J.S., Michel, P., Venkatesh, A.: Linnik’s ergodic method and the distribution of integer points on spheres. Automorphic representations and L-functions. Tata Inst. Fundam. Res. Stud. Math. 22, 119–185 (2013)
13. Ellenberg, J.S., Venkatesh, A.: Local-global principles for representations of quadratic forms. Invent. Math. 171(2), 257–279 (2008)
14. Gauss, C.F.: 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
15. Harcos, G.: Subconvex bounds for automorphic L-functions and applications. This is an unpublished dissertation available at http://www.renyi.hu/gharcos/ertekezes.pdf
16. Harcos, G., Michel, P.: The subconvexity problem for Rankin-Selberg L-functions and equidistribution of Heegner points. II. Invent. Math. 163(3), 581–655 (2006)
17. Iwaniec, H.: Fourier coefficients of modular forms of half-integral weight. Invent. Math. 87(2), 385–401 (1987)
18. Linnik, Y.V.: 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 (1969)
19. Maass, H.: Spherical functions and quadratic forms. J. Indian Math. Soc 20, 117–162 (1956)
20. Maass, H.: Über die Verteilung der zweidimensionalen Untergitter in einem euklidischen Gitter. Mathematische Annalen 137, 319–327 (1959)
21. Marklof, J.: The asymptotic distribution of Frobenius numbers. Invent. Math. 181(1), 179–207 (2010)
22. Michel, P., Venkatesh, A.: Equidistribution, L-functions and ergodic theory: on some problems of Yu. Linnik. In: International congress of mathematicians, vol. II, p. 421–457 (2006)
23. Platonov, V., Rapinchuk, A.: Algebraic groups and number theory. Pure and Applied Mathematics, vol 139. Academic Press Inc., Boston (1994). Translated from the 1991 Russian original by Rachel Rowen
24. Schmidt, W.M.: The distribution of sublattices of $\mathbb{Z}^m$. Monath. Math. 125(1), 37–81 (1998)
25. Zhang, R.: Appendix to “integer points on spheres and their orthogonal lattices”- arxiv version. arXiv preprint arXiv:1502.04209 (2015)