Annals of Mathematics **189** (2019), 145–276
https://doi.org/10.4007/annals.2019.189.1.4

Joint equidistribution of CM points

By Ilya Khayutin

Abstract

We prove the mixing conjecture of Michel and Venkatesh for toral packets with negative fundamental discriminants and split at two fixed primes, assuming all splitting fields have no exceptional Landau-Siegel zero. As a consequence we establish for arbitrary products of indefinite Shimura curves the equidistribution of Galois orbits of generic sequences of CM points all of whose components have the same fundamental discriminant, assuming the CM fields are split at two fixed primes and have no exceptional zero.

The joinings theorem of Einsiedler and Lindenstrauss applies to the toral orbits arising in these results. Yet it falls short of demonstrating equidistribution due to the possibility of intermediate algebraic measures supported on Hecke correspondences and their translates.

The main novel contribution is a method to exclude intermediate measures for toral periods. The crux is a geometric expansion of the cross-correlation between the periodic measure on a torus orbit and a Hecke correspondence, expressing it as a short shifted convolution sum. The latter is bounded from above generalizing the method of Shiu and Nair to polynomials in two variables on smooth domains.

Contents

1. Introduction 146
2. Preliminaries 158
3. Principal results 169
4. Measure rigidity 175
5. Coordinates for quaternion algebras 181
6. The double quotient $\mathbf{G}^{\Delta}\backslash\mathbf{G}\times\mathbf{G}/\mathbf{T}^{\Delta}$ 191
7. Homogeneous Hecke sets 197
8. Geometric expansion of the pair cross-correlation 201

Keywords: equidistribution, mixing conjecture, torus orbit, André-Oort, relative trace-formula

AMS Classification: Primary: 11G18, 37A17.

9. Sums of multiplicative functions over polynomials in two variables 220
10. Proof of main theorem 237
Appendix A. Principal genus theory 256
Appendix B. Points on conics 265
References 271

1. **Introduction**

1.1. *The mixing conjecture of Michel and Venkatesh.* Let Y be a complex modular curve. Each CM point[1] on Y is an element of a finite *packet* of CM points, all of which have CM by the same quadratic order Λ and form a single orbit under $\operatorname{Pic}(\Lambda)$. For each integer i, let $\mathscr{P}_i \subset Y$ be a packet of CM points with discriminant $D_i < 0$. Denote by μ_i the normalized counting measure on $\mathscr{P}_i$. By a theorem of Duke [Duk88] and Iwaniec [Iwa87] and its generalizations *inter alios* by [Che04], [Mic04], [Zha05] we know that if $|D_i| \to_{i\to\infty} \infty$, then $\mu_i \xrightarrow[i\to\infty]{\text{weak}-*} \mathrm{m}_Y$, where m_Y is the normalized Haar measure on Y.

Michel and Venkatesh [MV06] have conjectured a variant of the following.

Conjecture 1.1 (Mixing Conjecture). *Let $\mathscr{P}_i \subset Y$ be a sequence of packets of* CM *points as above. Each $\mathscr{P}_i$ is a principal homogeneous space of $\operatorname{Pic}(\Lambda_i)$, where Λ_i is the* CM *order of the points in $\mathscr{P}_i$. For each $i \in \mathbb{N}$, fix $\sigma_i \in \operatorname{Pic}(\Lambda_i)$ and define*

$$\mathscr{P}_i^{\text{joint}} \coloneqq \{(z, \sigma_i.z) \mid z \in \mathscr{P}_i\} \subset Y \times Y.$$

Denote by μ_i^{joint} the normalized counting measure supported on $\mathscr{P}_i^{\text{joint}}$.

Set

$$\mathfrak{N}_i = \min_{\substack{\mathfrak{a}\subseteq\Lambda_i \text{ invertible ideal} \\ \mathfrak{a}\in\sigma_i}} \operatorname{Nr}\mathfrak{a}.$$

If $\mathfrak{N}_i \to_{i\to\infty} \infty$, then μ_i^{joint} converge weak-$*$ to $\mathrm{m}_Y \times \mathrm{m}_Y$.

Using the reciprocity map of class field theory this conjecture implies a special case of the following well-known conjecture about equidistribution of Galois orbits of special points on products of modular curves.

Conjecture 1.2. *Let X be a finite product of complex modular curves. Let $\{x_i\}_i$ be a sequence of special points on X; i.e., each coordinate of x_i is a*

[1] In the setting of modular curves, CM points are classically called Heegner points. We follow the terminology of *CM point* to differentiate between the points on the modular curve — which are the subject of this manuscript — and the corresponding point on a modular elliptic curve, which we do not discuss.

CM *point. Denote by μ_i the normalized counting measure on the finite Galois orbit of x_i.*

If the sequence $\{x_i\}_i$ has finite intersection with any proper special subvariety[2] *of X, then $\{\mu_i\}_i$ converges weak-$*$ to the uniform probability measure on X.*

The latter conjecture implies the André-Oort conjecture for products of modular curves, which has been settled by Pila [Pil11]; see also [And98], [Edi98], [Edi05]. The André-Oort conjecture in this setting states that the sequence $\{x_i\}_i$ above must be Zariski dense in X. The Pila-Zannier strategy that is behind the recent breakthroughs on the Anrdré-Oort conjecture [Pil11], [PT13], [Tsi18] does not seem to shed light on the question of equidistribution of Galois orbits.

1.2. *Summary of results.*

1.2.1. *Results for torus orbits.* We present a proof of the mixing conjecture of Michel and Venkatesh, conditional on several significant assumptions. Most importantly, we assume that all the CM fields E_i are split at two fixed primes p_1, p_2 and have no exceptional Landau-Siegel zero.

Einsiedler, Lindenstrauss, Michel and Venkatesh [ELMV11] have defined the notion of a toral packet. To each CM point or a closed geodesic on a modular curve corresponds an order Λ in a quadratic field $E/\mathbb{Q}$. A toral packet is a generalization of the notion of a single $\mathrm{Pic}(\Lambda)$-orbit of a CM point or a closed geodesic.

Let $\mathbf{G}$ be a form of $\mathbf{PGL}_2$ defined over $\mathbb{Q}$. Fix a compact-open subgroup $K_f < \mathbf{G}(\mathbb{A}_f)$, and consider the double quotient

$$\widetilde{Y} \coloneqq {}_{\mathbf{G}(\mathbb{Q})}\backslash^{\mathbf{G}(\mathbb{A})}/_{K_f}.$$

The action of the real group $\mathbf{G}(\mathbb{R})$ on $\widetilde{Y}$ induces an isomorphism between $\widetilde{Y}$ and a disjoint union of finitely many locally homogeneous spaces

$$\widetilde{Y} \simeq \bigsqcup_{\delta\in\mathbf{G}(\mathbb{Q})\backslash\mathbf{G}(\mathbb{A}_f)/K_f} {}_{\Gamma_\delta}\backslash^{\mathbf{G}(\mathbb{R})},$$

where $\Gamma_\delta \coloneqq \mathbf{G}(\mathbb{Q}) \cap \delta K_f \delta^{-1}$ is a congruence lattice in $\mathbf{G}(\mathbb{R})$. In the simplest case when $\mathbf{G} = \mathbf{PGL}_2$ and K_f is a maximal compact subgroup the space $\widetilde{Y}$ has a single component and can be identified with ${}_{\mathbf{PGL}_2(\mathbb{Z})}\backslash^{\mathbf{PGL}_2(\mathbb{R})}$.

[2] This condition implies that the size of the Galois orbit of x_i tends to infinity as $i \to \infty$ because of Brauer-Siegel and the fact that a special point is by itself a special subvariety.

A toral packet $\mathscr{P}$ is a finite collection of orbits in $\widetilde{Y}$ of a real torus $H < \mathbf{G}(\mathbb{R})$, which is a projection of a single adelic torus orbit; see Section 2.4.1 for an exact definition. The set of H-orbits in $\mathscr{P}$ has a natural structure as a principal homogeneous space for a finite abelian group C that is a quotient of the idèle class group of an associated quadratic field $E/\mathbb{Q}$. Moreover, there is an order $\Lambda < E$ attached to $\mathscr{P}$ and a canonical surjective homomorphism $C \to \operatorname{Pic}(\Lambda)$. If K_f is maximal, then this homomorphism is an isomorphism. To each packet one can attach a discriminant $D \in \mathbb{R}$ that measures the arithmetic complexity of the packet; cf. Section 2.4.4. This discriminant is a product of $\operatorname{disc}(\Lambda)$ and an archimedean contribution.

The following is a special case of Theorem 3.2.

Theorem 1.3. *Let $\mathbf{G}$ be a form of $\mathbf{PGL}_2$ defined over $\mathbb{Q}$, and let $K_f < \mathbf{G}(\mathbb{A}_f)$ be a compact-open subgroup. Fix a* compact *real torus $K_\infty < \mathbf{G}(\mathbb{R})$, and denote*

$$Y := \widetilde{Y}/K_\infty = \mathbf{G}(\mathbb{Q})\backslash \mathbf{G}(\mathbb{A})/K_\infty \times K_f \simeq \bigsqcup_{\delta\in\mathbf{G}(\mathbb{Q})\backslash\mathbf{G}(\mathbb{A}_f)/K_f} \Gamma_\delta\backslash \mathbf{G}(\mathbb{R})/K_\infty.$$

Let $\mathscr{P}_i \subset \widetilde{Y}$ be a sequence of toral packets invariant under K_∞ with a fundamental discriminant $D_i < 0$. By abuse of notation denote by $\mathscr{P}_i$ the projection of the packet to a finite set of points in Y. The set $\mathscr{P}_i \subset Y$ is a principal homogeneous space for an abelian group C_i.

Let $\Lambda_i < E_i$ be the order in an imaginary quadratic field $E_i/\mathbb{Q}$ attached to $\mathscr{P}_i$, and denote by $\sigma \mapsto [\sigma]$ the homomorphism $C_i \to \operatorname{Pic}(\Lambda_i)$. For every $i \in \mathbb{N}$, choose some $\sigma_i \in C_i$ and let μ_i^{joint} be the Borel probability measure on $Y \times Y$ defined as the normalized counting measure on the set

$$\mathscr{P}_i^{\mathrm{joint}} := \{(z, \sigma_i.z) \mid z \in \mathscr{P}_i\} \subset Y \times Y.$$

Fix two primes p_1, p_2, and for all $i \in \mathbb{N}$, assume

(1) *the primes p_1, p_2 are split in E_i;*
(2) *the Dedekind ζ-function of E_i has no exceptional Landau-Siegel zero.*

Set

$$\mathfrak{N}_i = \min_{\substack{\mathfrak{a}\subseteq\Lambda_i \text{ invertible ideal} \\ \mathfrak{a}\in[\sigma_i]}} \operatorname{Nr}\mathfrak{a},$$

and assume $\mathfrak{N}_i \to_{i\to\infty} \infty$. Then any weak-$*$ limit point of $\left\{\mu_i^{\mathrm{joint}}\right\}_i$ is a convex combination of the uniform probability measures on the connected components of $Y \times Y$.

The theorem above is a special case of Theorem 3.2, which together with Proposition 3.6 describes completely under the assumptions above the analogues weak-$*$ limit points in the adelic quotient

$$[(\mathbf{G}\times\mathbf{G})(\mathbb{A})] \coloneqq {}^{\textstyle(\mathbf{G}\times\mathbf{G})(\mathbb{Q})}\backslash^{\textstyle(\mathbf{G}\times\mathbf{G})(\mathbb{A})}.$$

The conclusion of Theorem 1.3 is the best possible in this setting. In particular, one cannot expect equidistribution on all of $Y\times Y$ because the joint packets $\mathscr{P}_i^{\mathrm{joint}}$ can avoid completely some connected components of $Y\times Y$. This phenomena can appear already for $\mathbf{G}=\mathbf{PGL}_2$ whenever K_f is non-maximal. This behavior is intimately related to the limit of the averages of the residual spectrum over $\mathscr{P}_i^{\mathrm{joint}}$, and it is easy to compute exactly which limit measures exactly occur using Proposition 3.6.

We also establish a generalization of Theorem 1.3 to n-fold products $Y^{\times n}$ — Theorem 3.9. This generalization follows from the 2-fold result and an auxiliary application of the Einsiedler-Lindenstrauss joining theorem [EL15a, Cor. 1.5].

1.2.2. *Results for Galois orbits.* Theorem 1.3 and its n-fold generalization Theorem 3.9 imply through the reciprocity map of class field theory a theorem about equidistribution of Galois orbits of special point in products of indefinite Shimura curves.

Theorem 1.4. *Let $\mathbf{G}$ be a form of $\mathbf{PGL}_2$ defined over $\mathbb{Q}$ and split over $\mathbb{R}$. Let X be a finite product of indefinite Shimura curves relative to $\mathbf{G}$. Assume $\{x_i\}_i$ is a sequence of special points on X such that all coordinates have* CM *by the same* maximal *order. Denote by μ_i the normalized counting measure on the finite Galois orbit of x_i.*

Fix two primes p_1, p_2, and denote by E_i the CM *field of x_i. Assume that for all $i\in\mathbb{N}$,*

(1) *the primes p_1, p_2 split in E_i;*
(2) *the Dedekind ζ-function of E_i has no exceptional Landau-Siegel zero.*

If the sequence $\{x_i\}_i$ has a finite intersection with any proper special subvariety, then any weak-$*$ limit point of $\{\mu_i\}_i$ is a convex combination of the uniform probability measures on the connected components of X.

1.3. *Previous results.* Conjecture 1.1 has been proved by Ellenberg, Michel and Venkatesh [EMV13] under the assumption of a single fixed split prime p_1 and if the following holds:

$$\exists\eta>0\,\forall i\gg 1\colon \mathfrak{N}_i \ll |D|^{1/2-\eta}. \tag{1}$$

The proof in [EMV13] used minor assumptions and applied verbatim only when $\mathbf{G}$ was ramified at infinity and $\gcd(\mathfrak{N}_i, p_1)=1$. The assumption on $\mathbf{G}(\mathbb{R})$ can be removed using [Kha17], and the condition $\gcd(\mathfrak{N}_i, p_1) = 1$ can be relaxed by restricting the range of η in (1) depending on the best available bounds towards the Ramanujan Conjecture for[3] $\mathbf{SL}_2$.

Condition (1) is essential to the method of [EMV13] and fails for the majority of possible twists $[\sigma_i] \in \mathrm{Pic}(\Lambda_i)$. The proof strategy of Ellenberg, Michel and Venkatesh is to use (1) to find for each i a Hecke correspondence containing the packet $\mathscr{P}_i$ and whose volume is small compared to the volume of $\mathscr{P}_i$. In this favorable situation they use an effective version of Linnik's method using an explicit spectral gap for the Hecke operator at the split prime p_1 to deduce that the counting measure on $\mathscr{P}_i$ is approximately equidistributed in the ambient Hecke correspondence. The proof then concludes using the equidistribution of Hecke correspondences in $Y \times Y$.

The analogues questions for function fields in finite characteristic have been studied by Shende and Tsimerman [ST17]. In the finite characteristic setting additional tools are available. Shende and Tsimerman translate the analogues of Duke's theorem and the mixing conjecture to questions about point counting on (singular) varieties. These can be addressed using the Grothendieck-Lefschetz trace formula. They present a proof of Duke's theorem in finite characteristic using this method and a partial result towards the mixing conjecture. For the latter question they succeed in equating the pertinent higher cohomology groups, but the necessary bound on the dimension of the lower cohomology groups is conjectural.

1.4. *Measure rigidity.* Linnik has proved Duke's theorem about equidistribution of a sequence packets of CM points on the complex modular curve assuming that there is a fixed prime p that splits in all the CM fields in the sequence [Lin68]. In this proof Linnik used his "ergodic method" to bootstrap a weak bound on the self-correlation of the periodic measure on a toral packet in intermediate scales to full equidistribution using a dynamical argument. It is this dynamical argument where the assumption of a fixed split prime is used.

Einsiedler, Lindenstrauss, Michel and Venkatesh [ELMV09], [ELMV11], [ELMV12] have introduced a variant of Linnik's "ergodic method," which fits into the framework of homogeneous dynamics. The assumption of a fixed split prime p implies that the adelic, or S-arithmetic, periodic measures corresponding to the packets in the sequence are all invariant under a *split* p-adic torus.

[3] A. Venkatesh has described to me an alternative proof of the mixing conjecture assuming (1) by directly deducing from an appropriate version of Linnik's Basic Lemma that any limit measure must have maximal entropy for the diagonal toral flow at p_1 on $[(\mathbf{G} \times \mathbf{G})(\mathbb{A})]$. This does not rely on a spectral gap and completely circumvents the difficulties arising when $p_1 \mid \mathfrak{N}_i$ in the original argument of [EMV13].

Moreover, the self-correlation bound in the form of Linnik's basic lemma implies that any weak-$*$ limit must have *maximal* entropy with respect to the action of any element in the split p-adic torus. Linnik's theorem now follows from the classification of measures of maximal entropy with respect to the action of a semi-simple p-adic group element that generates an unbounded subgroup. The latter one is straightforward if one uses the relation between entropy and leafwise measures [MT94], [EL10].

The approach of Einsiedler, Lindenstrauss, Michel and Venkatesh has significant ramifications when combined with the modern methods of measure rigidity for toral actions [Lin06], [EKL06], [EL15b], [EL15a]. Although measure rigidity requires further splitting assumptions, it can imply strong equidistribution results based on weaker arithmetic input compared to methods of harmonic analysis. A main example is the analogue of Linnik's theorem for maximal tori in $\mathbf{PGL}_3$ [ELMV11] where equidistribution is deduced by verifying Weyl's equidistribution criterion only for a *small* part of the spectrum.

This strategy is also the starting point for our proof of Theorem 1.3 and its generalizations. The assumption that two primes p_1,p_2 are split in all the CM fields in the sequence is required for the joinings theorem of Einsiedler and Lindenstrauss [EL15a] to apply. This measure rigidity result, concurrently with Linnik's or Duke's theorem for equidistribution of packets in rank 1, implies that any possible weak-$*$ limit measure of periodic measures on joint toral packet must be algebraic; i.e., it is a convex combination of uniform measures and some translates of Hecke correspondences. It is these translates of Hecke correspondence that we need to discard using the genericity assumption $\mathfrak{N}_i \to \infty$ in the conjecture of Michel and Venkatesh, Conjecture 1.1.

1.5. *Cross-correlation.* The main novelty is our method to demonstrate that each limit point of the sequence of measures $\left\{\mu_i^{\text{joint}}\right\}$ in Theorem 1.3 is singular to any convex combination of intermediate measures allowed by the joinings theorem of Einsiedler and Lindenstrauss.

The rudiments of our approach can be described in a general setting. Consider a locally compact G-space X where G is a second countable locally compact topological group. Suppose μ and ν are Borel measures on $X \times X$, and denote by m_G some fixed Haar measure on G. We are interested in the case when ν is a periodic measure for the diagonal subgroup $G^{\Delta} < G \times G$; i.e., there is some $x_0 \in X \times X$ such that $\mathrm{Stab}_{G^{\Delta}}(x_0)$ is a lattice in G^{Δ} and ν is the G^{Δ}-invariant probability measure supported on the closed orbit $G^{\Delta}.x_0$. For any compact subset $C \subset X$, if we take a small enough symmetric identity neighborhood $B \subset G$, then ν-almost every $x \in C \times C$ satisfies

$$\nu\left((B \times B).x\right) \asymp \mathrm{m}_G(B). \tag{2}$$

In order to show that the measures μ and ν are singular we can consider for each compact $C \subset X \times X$ and for a compact symmetric identity neighborhood $B \subset G$ the cross-correlation quantity

$$\widetilde{\mathrm{Cor}}_C[\mu,\nu](B) \coloneqq \mu \times \nu\left(\{(x,y) \in C \times C \mid y \in (B \times B).x\}\right).$$

We call B the *test neighborhood* of the cross-correlation. Assume we are able to establish that

$$\widetilde{\mathrm{Cor}}[\mu,\nu](B) \ll \mathrm{m}_G(B)^{1+\rho} \tag{3}$$

for some $\rho > 0$, for a family of compact subsets C exhausting X and for a family of identity neighborhoods $B \subset G$ with arbitrary small Haar measure. Then the estimates (2) and (3) imply $\nu \perp \mu$.

The first observation when studying the cross-correlation between two algebraic measures on an adelic quotient is that it is bounded above by a relative trace of the automorphic kernel with test function $\mathbb{1}_{B\times B}$. In our setting the relative trace that arises is for the double quotient

$$\mathbf{G}^{\Delta}\backslash^{\mathbf{G}\times\mathbf{G}}/_{\mathbf{T}^{\Delta}},$$

where $\mathbf{T} < \mathbf{G}$ is a maximal torus defined over $\mathbb{Q}$ and anisotropic over $\mathbb{R}$ embedded diagonally $\mathbf{T}^{\Delta} < \mathbf{G} \times \mathbf{G}$. This relative trace has a geometric expansion, and the main difficulty is bounding the sum of the relative orbital integrals. We require an upper bound that is optimal up to a uniform multiplicative constant.

1.6. *Invariants and integral ideals.* Denote by $\Lambda < E$ the order attached to a fixed toral packet. Proposition 8.30 is a fundamental result where we show that a relative orbital integral is bounded in terms of the number of pairs of integral ideals in Λ whose norms satisfy an additive relation. A. Venkatesh has pointed out that this bears a similarity to the calculation of heights in the proof of the Gross-Zagier Theorem [GZ86, §3].

The construction of these integral ideals can be described in an elementary fashion. Assume we are in the setting of the modular curve $Y_0(1)$. Let $\Lambda = \mathcal{O}_E$ be the maximal order in an imaginary quadratic field $E/\mathbb{Q}$ with discriminant $D < 0$. Fix a twist $[\sigma] \in \mathrm{Cl}(E)$. The joint packet in $Y_0(1) \times Y_0(1)$ is the set $\left\{\left(H_{[I]}, H_{[I\sigma]}\right) \mid [I] \in \mathrm{Cl}(E)\right\}$, where $H_{[I]} \in Y_0(1)$ is the CM point attached to the ideal class $[I]$. For simplicity, we only discuss how to show non-accumulation on the diagonal $Y_0(1)^{\Delta} \hookrightarrow Y_0(1) \times Y_0(1)$.

Let $B_\delta \subset \mathbf{PGL}_2(\mathbb{R})$ be the identity neighborhood of radius $\delta > 0$. The cross-correlation between the joint packet and the diagonal with test neighborhood B_δ is a weighted count of the number of points $\left(H_{[I]}, H_{[I\sigma]}\right)$ such that the hyperbolic distance $d(H_{[I]}, H_{[I\sigma]})$ is less then 2δ. The weight is a continuous decreasing function of $d(H_{[I]}, H_{[I\sigma]})$ that vanishes when $d(H_{[I]}, H_{[I\sigma]}) = 2\delta$. For simplicity, consider the unweighted quantity

$$\left|\left\{\left(H_{[I]}, H_{[I\sigma]}\right) \mid d(H_{[I]}, H_{[I\sigma]}) \leq 2\delta,\ [I] \in \mathrm{Cl}(E)\right\}\right|.$$

For each element in the set above, we write an explicit expression for the CM points in the standard fundamental domain in $\mathbb{H} \subset \mathbb{C} \setminus \mathbb{R}$,

$$H_{[I]} = \frac{-b + i\sqrt{|D|}}{2\mathfrak{N}},\ H_{[I\sigma]} = \frac{-b' + i\sqrt{|D|}}{2\mathfrak{N}'},$$

where $I = \left\langle \mathfrak{N}, \frac{-b+i\sqrt{|D|}}{2} \right\rangle, I' = \left\langle \mathfrak{N}', \frac{-b'+i\sqrt{|D|}}{2} \right\rangle \subset E \subset \mathbb{C}$ are the primitive fractional ideals in the classes $[I]$ and $[I\sigma]$ respectively. Consider the elements

$$x = \mathfrak{N}\frac{-b' + i\sqrt{|D|}}{2} - \mathfrak{N}'\frac{-b + i\sqrt{|D|}}{2} \in I \cdot I',$$
$$y = \mathfrak{N}\frac{-b' - i\sqrt{|D|}}{2} - \mathfrak{N}'\frac{-b - i\sqrt{|D|}}{2} \in I \cdot {}^{\sigma}I',$$

and define

$$\mathcal{O}_E \supset \mathfrak{a} = y/(I \cdot {}^{\sigma}I') \in [\sigma] \mod \mathrm{Cl}(E),$$
$$\mathcal{O}_E \supset \mathfrak{b} = x/(I \cdot I') \in [I^{-2}\sigma^{-1}] \mod \mathrm{Cl}(E).$$

A simple calculation shows that

$$\mathrm{Nr}(\mathfrak{a}) = \frac{(\mathfrak{N}b' - \mathfrak{N}'b)^2 + |D|(\mathfrak{N} + \mathfrak{N}')^2}{4\mathfrak{N}\mathfrak{N}'},$$
$$\mathrm{Nr}(\mathfrak{b}) = \frac{(\mathfrak{N}b' - \mathfrak{N}'b)^2 + |D|(\mathfrak{N} - \mathfrak{N}')^2}{4\mathfrak{N}\mathfrak{N}'}$$
$$= \frac{|D|}{4}\left(\cosh(d(H_{[I]}, H_{[I\sigma]})) - 1\right) \ll |D|\mathrm{m}(B_{2\delta}),$$
$$\mathrm{Nr}(\mathfrak{a}) - \mathrm{Nr}(\mathfrak{b}) = \frac{\mathrm{Nr}(y) - \mathrm{Nr}(x)}{\mathfrak{N}\mathfrak{N}'} = |D|.$$

This construction demonstrates the relation between the mass of the joint packet in a neighborhood of the diagonal and counting pairs of *integral* ideals. Specifically, we need to count pairs of integral ideals that satisfy additive norm relations and whose norms are bounded by a multiple of $|D|$. To establish this relation formally we need to check how close the map $\mathrm{inv}\left(H_{[I]}, H_{[I\sigma]}\right) = (\mathfrak{a}, \mathfrak{b})$ is to being injective. The most serious problem with injectivity arises if $\mathfrak{b} = 0$. In our special case it is easy to see that this happens only if $[I] = [I\sigma] \Leftrightarrow [\sigma] = e$. This situation is excluded by the assumption that $\mathfrak{N}_i \to \infty$ in Conjecture 1.1. The full strength of this assumption is needed to establish non-concentration on any translate of a Hecke correspondence.

If $\mathfrak{b} \neq 0$, it turns out that injectivity can fail, in a mild way, only at the ramified primes $p \mid D$. This is the essence of Proposition 8.27. This lack of injectivity is compensated by the fact that $\mathfrak{b}$ is restricted to a fixed class in $\mathrm{Cl}(E)/\mathrm{Cl}(E)^2$. The analysis of the fibers of the map inv and taking into account the restriction modulo $\mathrm{Cl}(E)^2$ produces significant technical complications. These can be avoided if one assumes that $|D|$ is prime.

The full expression for the cross-correlation is a weighted sum over elements in the joint packet that are contained in a δ-neighborhood of the diagonal. The weight is easily seen to be bounded by $\ll \mathrm{m}(B_{2\delta})$.

The author has not arrived at the construction of the invariants $(\mathfrak{a}, \mathfrak{b})$ through this calculation. Rather the ideals $\mathfrak{a}$,$\mathfrak{b}$ arose naturally in a geometric expansion of a relative trace. The classical interpretation above is due to the referee.

1.7. *Shifted-convolution sums.* We now describe how to bound the cross-correlation with test neighborhood $B_\delta \subset \mathbf{G}(\mathbb{R})$ between a joint toral packet and a fixed translate of a Hecke correspondence, e.g., the diagonal.

The final outcome of the arithmetic analysis of the relative orbital integrals in term of pairs of integral invertible Λ-ideals satisfying an additive norm relation is that the cross-correlation is bounded by an expression proportional to a shifted convolution sum that is roughly of the form

$$\mathscr{S} := \sum_{0<x-|D|\leq \kappa \mathrm{m}(B_{2\delta})|D|} g(x) f(x-|D|), \tag{4}$$

where $D = \mathrm{disc}(\Lambda)$, $f(x)$ is the multiplicative function that counts the number of invertible integral Λ-ideals of norm x; and g counts the same ideals as f but with the additional restriction that they belong to the *fixed* Picard class $[\sigma]$. The class $[\sigma] \in \mathrm{Pic}(\Lambda)$ is the Picard class of a single twist in Theorem 1.3. For the sake of simplicity, we consider for now the real number $\kappa > 0$ as a universal constant. We have neglected the non-injectivity of the invariant map as discussed above and the restrictions modulo $\mathrm{Pic}(\Lambda)^2$.

It is not difficult to show that if we extend the range of summation in $\mathscr{S}$, then the asymptotic mean value is $\asymp \frac{\rho}{\sqrt{|D|}}$, where ρ is the residue at 1 of the Dedekind ζ-function of E. In order to complete the proof we need to show a comparable, up to a fixed constant, upper bound in the extremely short range $\kappa \mathrm{m}(B_{2\delta})|D|$. Unfortunately, the various methods from harmonic analysis to estimate shifted convolution sums are of no use in this short range of summation.

We proceed instead using a sieve. Let $q(x, y)$ be the *reduced* primitive integral binary quadratic form corresponding to the class $[\sigma]^{-1} \in \mathrm{Pic}(\Lambda)$. Denote by $\mathscr{E} \subset \mathbb{R}^2$ the elliptical annulus of area $2\pi \mathrm{m}(B_{2\delta})\kappa\sqrt{|D|}$ defined by

$$\mathscr{E} := \left\{(x, y) \in \mathbb{Z}^2 \mid |D| < q(x, y) \leq (1 + \mathrm{m}(B_{2\delta})\kappa)|D|\right\}.$$

The sum $\mathscr{S}$ is tautologically equal to

$$\sum_{(x,y)\in\mathscr{E}\cap\mathbb{Z}^2} f(q(x,y)-|D|).$$

The latter is a sum of a multiplicative function over the values of a polynomial in two variables. We generalize the method of Shiu [Shi80] and Nair [Nai92] to polynomials in two variables on smooth domains in order to deduce a bound of the form

$$S \ll A(\mathscr{E})(\log|D|)^{-1}\sum_{a\ll|D|}\frac{f(a)}{a},$$

where $A(\mathscr{E})$ is the area of the ellipse $\mathscr{E}$. In order to derive an upper bound of the correct order of magnitude for the logarithmic sum above we need to assume the lack of an exceptional zero.

It is important to mention that the sieve method fails when the ellipse $\mathscr{E}$ is distorted too much. Fortunately, this is exactly the case when the proof method of Ellenberg, Michel and Venkatesh [EMV13] applies.

The approach to bounding $\mathscr{S}$ using a sieve is inspired by the work of Bourgain, Sarnak and Rudnick [BSR16]. Sieve methods have been fruitfully applied to shifted convolution sums in other contexts as well. Holowinsky has used a related argument in his work on holomorphic QUE [Hol10], [HS10]. P. Michel has pointed out to the author that in the scenario considered by Holowinsky, the shifted convolutions arise from the L-functions of symmetric squares of holomorphic forms that are known not to have an exceptional zero, in contrast to the case of $\mathscr{S}$ above.

1.8. *Further discussion.*

1.8.1. *Archimedean versus p-adic cross-correlation.* In the exposition above we have presented a method to show that joint packets of CM points do not accumulate on the diagonal diagonal using a cross-correlation quantity that uses an archimedean test neighborhood $B_\delta \subset \mathbf{G}(\mathbb{R})$. In the actual proof we shall use a non-archimedean neighborhood at one of the primes, say p_1, where all the tori in the sequence were assumed to be split.

This modification is necessary because the measure rigidity argument does *not* imply that any weak-$*$ limit of μ_i^{joint} in Theorem 1.3 is a *countable* convex combination of algebraic measures. We may not reduce to a countable collection of possible ergodic components because the normalizer of a diagonally embedded rank 1 torus $\mathbf{T}^{\Delta} < \mathbf{G}\times\mathbf{G}$ contains the subgroup $\mathbf{T}\times\mathbf{T}$ that is much bigger then $\mathbf{T}^{\Delta}$.

Assume for simplicity that Y in Theorem 1.3 is connected. If we restrict to the archimedean setting, then the possible obstructions to equidistribution are all periodic orbits of the form

$$[\delta \mathbf{G}^{\Delta}(\mathbb{R})^{+}\xi_{\mathbb{R}}] \subset {}_{\Gamma}\backslash^{\mathbf{G}(\mathbb{R})} \times {}_{\Gamma}\backslash^{\mathbf{G}(\mathbb{R})},$$

where $\mathbf{G}(\mathbb{R})^{+}$ is the real image of the isogeny from the simply connected cover $\mathbf{G}^{\mathrm{sc}} \to \mathbf{G}$, $\delta \in (\mathbf{G}\times\mathbf{G})(\mathbb{Q})$ and $\xi_{\mathbb{R}} \in (\mathbf{G}\times\mathbf{G})(\mathbb{R})$ is *any* element.

To see how this creates a problem in the argument, notice that the contradiction in Section 1.5 has used the fact (2) that $\nu((B\times B).x) \asymp \mathrm{m}(B)$ for the Haar measure m on $\mathbf{G}(\mathbb{R})$. While this is true if ν is a countable combination of algebraic measures supported on translates of $\mathbf{G}^{\Delta}(\mathbb{R})^{+}$, it can be wrong for uncountable families. In particular, such an uncountable convex combination can even be absolutely continuous with respect to the Haar measure $\mathrm{m}\times\mathrm{m}$ (even if we fix δ above). This phenomenon is analogous to the statement that an uncountable combination of Lebesgue measures on 1-dimensional lines in $\mathbb{R}^2$ can have an arbitrary dimension in the interval $[1,2]$.

To overcome this difficulty we instead use the cross-correlation for a non-archimedean neighborhood $B \subset \mathbf{G}(\mathbb{Q}_{p_1})$. Let $S=\{\infty,p_1\}$. There is a canonical lift of the each measure μ_i^{joint} to a probability measure on a fixed S-arithmetic homogeneous space ${}_{\Gamma_S}\backslash^{\mathbf{G}(\mathbb{Q}_S)}$. Each lift is a finite combination of periodic measures for the diagonal embedding of the torus $K_\infty \times A_{p_1} < \mathbf{G}(\mathbb{Q}_S)$, where $A_{p_1} < \mathbf{G}(\mathbb{Q}_{p_1})$ is a split torus independent of the index i. The measure rigidity argument now implies that the obstruction to equidistribution is a convex combination of algebraic measures supported on $\left[\delta\mathbf{G}^{\Delta}(\mathbb{Q}_S)^{+}(\xi_{\mathbb{R}},\xi_{p_1})\right]$ with $\xi_{\mathbb{R}} \in (\mathbf{G}\times\mathbf{G})(\mathbb{R})$, $\xi_{p_1} \in (\mathbf{G}\times\mathbf{G})(\mathbb{Q}_{p_1})$, and δ is a rational element. In this setting there is an additional restriction[4] on $\xi_{p_1} = (\xi^1_{p_1},\xi^2_{p_1})$ that $(\xi^1_{p_1})^{-1}\xi^2_{p_1} \in A_{p_1}$. This restriction appears in the S-arithmetic setting because each periodic measure in the sequence of packets was invariant under a fixed *split* torus $A^{\Delta}_{p_1}$. This additional piece of information allows us to rule out accumulation on convex combinations of an uncountable family of algebraic measures.

Let ν be any convex combination of algebraic measures supported on closed orbits of the form $\left[\delta\mathbf{G}^{\Delta}(\mathbb{Q}_S)^{+}(\xi_{\mathbb{R}},\xi_{p_1})\right]$, which are all invariant under $A^{\Delta}_{p_1}$. The gist of the argument is that for every $a \in A^{\Delta}_{p_1}$, the metric entropy $\mathrm{h}_\nu(a)$ is a convex combination of the metric entropies on individual periodic measures. There is a relation between metric entropy and self-correlations that implies for a suitable p_1-adic identity neighborhood B that $\nu((B\times B).x)$ cannot *on average* decay as $\mathrm{m}(B)^{1+\rho}$ for any $\rho>0$. This is enough to conclude the necessary contradiction.

[4] A shadow of this condition appears in the archimedean setting as well; the element δ in the archimedean case cannot be an arbitrary rational point and is restricted at the primes $p=p_1,p_2$. It is not clear how to put this information to good use.

1.8.2. *The assumption on the conductor.* In Theorem 1.3 we have assumed the discriminants D_i are all fundamental. The slightly more general version in Theorem 3.2 allows non-trivial conductors $\mathscr{f}_i$ but they should be uniformly bounded. The difficulty with removing this assumption is that if we allow a non-trivial conductor $\mathscr{f}$, then the shifted convolution sum in (4) is $\asymp \kappa \mathrm{m}(B_{2\delta})\rho\sqrt{|D|}\mathscr{f}$. The extra factor of $\mathscr{f}$ appears because the shift $|D|$ is divisible by $\mathscr{f}$, and at primes dividing the shift there is no decoupling between the arithmetic functions f and g in $\mathscr{S}$. The best bound we can expect for $\mathscr{S}/|\operatorname{Pic}(\Lambda)|$ is proportional to $\mathscr{f}$ and tends to ∞ if $\mathscr{f}$ is unbounded. Such a bound is useless for our purposes.

In an upcoming work the author will explain how to overcome this problem by refining the map attaching a pair of integral ideals to orbital integrals. The new map will not be valued just in pairs of integral ideals but will carry additional information.

1.9. *Organization of the paper.* In Section 2 we define the basic notions we work with in the rest of the paper.

In Section 3 we present the main theorems in adelic terms and prove some auxiliary propositions.

In Section 4 we apply the joinings theorem of Einsiedler and Lindenstrauss to the problem at hand.

In Section 5 we review and prove basic facts about explicit representations of quaternion algebras in coordinate form. We also describe representatives "in lowest terms" for elements of the projective group of units of a quaternion algebra over local fields.

In Section 6 we construct the double quotient ${}_{\mathbf{G}^{\Delta}}\backslash^{\mathbf{G}\times\mathbf{G}}/_{\mathbf{T}^{\Delta}}$ using GIT and study its properties over $\mathbb{Q}$. This variety is essential for the geometric expansion of the relative trace appearing later on.

In Section 7 we study basic properties of the intermediate measures arising as obstructions to equidistribution.

Section 8 is a key part of this paper where we study the cross-correlation between a periodic toral measure and a translated Hecke correspondence using a relative trace. Most importantly, we demonstrate the relation between this relative trace and shifted-convolution sums. This requires interpretation of the non-archimedean relative orbital integrals as intersection numbers and explicit parametrization of the relevant intersections using arithmetic invariants.

In Section 9 we generalizes the results of [Shi80], [Nai92] to sums of multiplicative functions along values of polynomials in two variables on smooth domains. This section may be of independent interest.

In Section 10 we combine all of the previously developed tools to a proof of the main theorem.

In Appendix A we review the classical principal genus theory for quadratic orders and provide complete proofs in a form useful to us. These results are necessary in translating the shifted-convolution sums that arise from the relative trace into sums of multiplicative functions over values of polynomials.

In Appendix B we do routine calculations of the number of points on some singular conics over ${}^{\mathbb{Z}}/_{N\mathbb{Z}}$. These are necessary to translate the upper-bound on the cross-correlation we have after applying the sieve method into a sum treatable using analytic number theory.

1.10. *Acknowledgments.* It is a pleasure to thank Peter Sarnak for numerous fruitful and enlightening discussions on this project and for the observation that the results for toral orbits are relevant to the equidistribution of Galois orbits on products of modular curves. I am indebted to Elon Lindenstrauss for his continuous encouragement and his interest in this project. I am grateful to Akshay Venkatesh for valuable conversations and his assistance in clarifying the results of [EMV13]. I thank Manjul Bhargava, Fabian Gundlach and Shou-Wu Zhang for helpful discussions.

I am grateful to Philippe Michel and Wei Zhang for very useful and illuminative comments on a previous version of this manuscript. I am deeply indebted to the referee for pointing out that Lemma 10.11 in the original manuscript was wrong and for bringing forth the description in Section 1.6 of the invariant ideals in a classical language.

The author was supported by a Schmidt Fellowship at the Institute for Advanced Study during 2017-2018.

2. **Preliminaries**

2.1. *Notation and conventions.*

(1) We denote by the letter v a place of $\mathbb{Q}$. For a non-archimedean place v, define q_v to be the size of the residue field of $\mathbb{Q}_v$.

(2) For a linear algebraic group $\mathbf{M}$ defined over $\mathbb{Q}$, we denote

$$[\mathbf{M}(\mathbb{A})] \coloneqq {}_{\mathbf{M}(\mathbb{Q})}\backslash^{\mathbf{M}(\mathbb{A})}.$$

More generally, for any subset $U \subseteq \mathbf{M}(\mathbb{A})$, we denote by $[U]$ its projection to $[\mathbf{M}(\mathbb{A})]$. We also use the notation $[g]$ for the coset of $g \in \mathbf{M}(\mathbb{A})$ in $[\mathbf{M}(\mathbb{A})]$.

(3) If $\mathbf{M}$ is anisotropic over $\mathbb{Q}$, i.e., there are no characters $\mathbf{M} \to \mathbb{G}_{\mathrm{m}}$ defined over $\mathbb{Q}$, then the locally compact space $[\mathbf{M}(\mathbb{A})]$ carries a unique $\mathbf{M}(\mathbb{A})$-invariant probability measure, which we call the Haar measure on $[\mathbf{M}(\mathbb{A})]$ and denote by $m_{\mathbf{M}}$. We use the notation $m_{\mathbf{M}}$ also for the covolume 1 Haar measure on $\mathbf{M}(\mathbb{A})$.

(4) For S a finite set of places of $\mathbb{Q}$, we denote

$$\mathbf{M}(\mathbb{A}^S) \coloneqq \textstyle\prod'_{v\notin S}\mathbf{M}(\mathbb{Q}_v), \qquad \mathbf{M}(\mathbb{Q}_S) \coloneqq \displaystyle\prod_{v\in S}\mathbf{M}(\mathbb{Q}_v).$$

(5) If $\mathbf{L} < \mathbf{M}$ is a closed algebraic subgroup, denote the diagonal embedding of algebraic groups by $\mathbf{L}^{\Delta} < \mathbf{M}\times\mathbf{M}$. We use the similar notation $L^{\Delta} < M\times M$ for the diagonal embedding of a closed subgroup $L < M$ in a locally compact group M.

(6) For any algebraic group $\mathbf{M}$, the morphism $\mathrm{ctr}\colon \mathbf{M}\times\mathbf{M}\to\mathbf{M}$ is defined by $(g_1, g_2)\mapsto g_1^{-1}g_2$.

(7) For a reductive linear algebraic group $\mathbf{M}$, we denote by $\mathbf{M}^{\mathrm{sc}}$ its simply-connected cover. We fix an isogeny $\mathbf{M}^{\mathrm{sc}}\to\mathbf{M}$ and denote for any ring R the image of $\mathbf{M}^{\mathrm{sc}}(R)$ in $\mathbf{M}(R)$ by $\mathbf{M}(R)^{+}$.

(8) If $L < M$ is a unimodular closed subgroup of a unimodular locally compact group M with fixed Haar measures m_L and m_M respectively, then we always normalize the M-invariant Haar measure on ${}_{L}\backslash^{M}$ so that

$$\int_M f\,\mathrm{dm}_M = \int_{L\backslash M}\Big(\int_L f(lg)\,\mathrm{dm}_L(l)\Big)\,\mathrm{dm}_{L\backslash M}(Lg)$$

for any $f\in\mathscr{L}^1(M)$.

(9) For F a global field or a finite product of non-archimedean local fields, we denote by $\mathcal{O}_F$ the ring of integers — the unique maximal order, $F^{(1)}$ the multiplicative subgroup of $F^{\times}$ of norm 1 elements and $\mathcal{O}_F^{(1)}$ the multiplicative group of norm 1 integral elements.

(10) When F as above is a quadratic extension of either $\mathbb{Q}$ or $\mathbb{Q}_v$, it is equipped with an action of the Galois group $\mathfrak{G}\simeq {}^{\mathbb{Z}}/_{2\mathbb{Z}}$. We define the coboundary map

$$\begin{aligned}\mathrm{cbd}\colon F^{\times} &\to F^{(1)},\\ x&\mapsto \frac{x}{{}^{\sigma}x}.\end{aligned}$$

Hilbert's Satz 90 implies that this map surjective.

2.2. *Forms of* $\mathbf{PGL}_2$ *and locally homogeneous spaces.* Let $\mathbf{B}$ be a quaternion algebra defined over $\mathbb{Q}$. Denote $\mathbf{Z}\coloneqq \mathrm{Z}\,\mathbf{B}^{\times}$ — the center of $\mathbf{B}^{\times}$ — and define $\mathbf{G}\coloneqq {}_{\mathbf{Z}}\backslash^{\mathbf{B}^{\times}}$ to be the projective group of units. The linear group $\mathbf{G}$ is a form of $\mathbf{PGL}_2$ defined over $\mathbb{Q}$, and all $\mathbb{Q}$-forms of $\mathbf{PGL}_2$ arise this way. A central object in our discussion is the finite volume adelic locally homogeneous space

$$[\mathbf{G}(\mathbb{A})] = {}_{\mathbf{G}(\mathbb{Q})}\backslash^{\mathbf{G}(\mathbb{A})} \simeq {}_{\mathbf{Z}(\mathbb{A})\mathbf{B}^{\times}(\mathbb{Q})}\backslash^{\mathbf{B}^{\times}(\mathbb{A})}. \tag{5}$$

2.2.1. *Maximal order in* $\mathbf{B}(\mathbb{Q})$. Fix a maximal $\mathbb{Z}$-order $\mathbb{O} \subset \mathbf{B}(\mathbb{Q})$. For any non-archimedean place v, denote the v-adic closure of $\mathbb{O}$ by $\mathbb{O}_v \subset \mathbf{B}(\mathbb{Q}_v)$. The $\mathbb{Z}_v$-order $\mathbb{O}_v$ is maximal in the quaternion algebra $\mathbf{B}(\mathbb{Q}_v)$; cf. [Rei75, (11.2)]. For non-archimedean v, define the compact subgroup $\mathbb{O}_v^\times < \mathbf{B}^\times(\mathbb{Q}_v)$ and let the compact-open subgroup $K_v < \mathbf{G}(\mathbb{Q}_v)$ be its image under the quotient map $\mathbf{B}^\times \to \mathbf{G}$.

We define the adelic points of $\mathbf{B}^\times$ and $\mathbf{G}$ as a restricted product with respect to the compact subgroups $\mathbb{O}_v$ and K_v respectively. Moreover, for any finite set S of places containing ∞, we denote

$$\mathbb{O}^{\times,S} \coloneqq \prod_{v\notin S} \mathbb{O}_v^\times, \qquad K^S \coloneqq \prod_{v\notin S} K_v$$

and

$$\mathbb{O}_f^\times \coloneqq \mathbb{O}^{\times,\{\infty\}} = \prod_{v\neq\infty} \mathbb{O}_v^\times, \qquad K_f \coloneqq K^{\{\infty\}} = \prod_{v\neq\infty} K_v.$$

We need to review some elementary properties of K_v and $\mathbb{O}_v$ for different places v.

Split non-archimedean places. If $\mathbf{B}$ is split over a non-archimedean v, i.e., $\mathbf{B}(\mathbb{Q}_v) \simeq \mathbf{M}_2(\mathbb{Q}_v)$. Then the maximal orders of $\mathbf{B}(\mathbb{Q}_v)$ are in bijection with the vertices of the reduced Bruhat-Tits tree of $\mathbf{B}^\times(\mathbb{Q}_v)$. Explicitly, fix an isomorphism $\mathbf{B}^\times(\mathbb{Q}_v) \simeq \mathrm{End}_{\mathbb{Q}_v}(\mathbb{Q}_v^2)$ then vertices of the Bruhat-Tits tree correspond to homothety classes of full-rank $\mathbb{Z}_v$-lattices $L \subset \mathbb{Q}_v^2$, and all the maximal orders are of the form $\mathrm{End}_{\mathbb{Z}_v}(L)$. In particular, $\mathbb{O}_v^\times$ is a stabilizer of a vertex in the tree and K_v is a special maximal compact-open subgroup.

Ramified non-archimedean places. If $\mathbf{B}$ is ramified over a non-archimedean v, then $\mathbf{B}(\mathbb{Q}_v)$ is a division algebra and $\mathbb{O}_v$ is the unique maximal order — the integral closure of $\mathbb{Z}_v$ in $\mathbf{B}(\mathbb{Q}_v)$; cf. [Rei75, (12.8)]. Because of the uniqueness property of $\mathbb{O}_v$, it is conjugation invariant and $\mathbb{O}_v^\times$ is a *normal* subgroup of $\mathbf{B}^\times(\mathbb{Q}_v)$.

A quaternion division algebra over $\mathbb{Q}_v$ has ramification index 2 (cf. [Rei75, (14.3)]), hence K_v is a normal subgroup of index 2 in the compact group $\mathbf{G}(\mathbb{Q}_v)$.

The archimedean analogue of a maximal order. We will also need an archimedean analogue of a local maximal order. Fix once and for all a maximal compact torus $K_\infty < \mathbf{G}(\mathbb{R})$. We define an isomorphism between $(\mathbf{B}(\mathbb{R}), K_\infty)$ and $(\mathbf{M}_2(\mathbb{R}), \mathbf{PSO}_2(\mathbb{R}))$ to be an isomorphism of algebras $\mathbf{B}(\mathbb{R}) \simeq \mathbf{M}_2(\mathbb{R})$ that induces an isomorphism $\mathbf{G}(\mathbb{R}) \simeq \mathbf{PGL}_2(\mathbb{R})$ mapping K_∞ to $\mathbf{PSO}_2(\mathbb{R})$. Due to the Skolem-Noether theorem and the fact that the normalizer of $\mathbf{PSO}_2(\mathbb{R})$ is $\mathbf{PGO}_2(\mathbb{R})$, such an isomorphism is unique up to composition with the map $\mathrm{Ad}\,\mathbf{PGO}_2(\mathbb{R})$. Assume $\mathbf{B}$ is split over $\mathbb{R}$, and fix such an isomorphism.

Inner-product norms on $\mathbb{R}^2$ are often used analogously to full rank lattices in the non-archimedean settings. Two inner-product norms on $\mathbb{R}^2$ are said to be homothetic if they differ by a positive multiplicative constant. The action of $\mathbf{GL}_2(\mathbb{R})$ on $\mathbb{R}^2$ induces a transitive action on the space of inner-product norms on $\mathbb{R}^2$. This action descends to a transitive action of $\mathbf{PGL}_2(\mathbb{R})$ on homothety classes of inner-product norms. Any inner-product norm $|\bullet|\colon \mathbb{R}^2 \to \mathbb{R}_{>0}$ induces a sub-multiplicative operator norm on $\mathbf{M}_2(\mathbb{R})$ in the standard way:

$$\|g\|_{|\bullet|} = \sup_{0\neq v\in\mathbb{R}^2} \frac{|gv|}{|v|}.$$

This operator norm depends only on the homothety class $\mathbb{R}_{>0}\cdot|\bullet|$. Let $\mathrm{Stab}_{|\bullet|} < \mathbf{PGL}_2(\mathbb{R})$ be the stabilizer of the homothety class of $|\bullet|$. The closed unit-ball in $\mathbf{M}_2(\mathbb{R})$ with respect to $\|\bullet\|_{|\bullet|}$ is an $\mathrm{Ad}\,\mathrm{Stab}_{|\bullet|}$-invariant compact identity neighborhood. Unlike the endomorphism ring of a full-rank lattice, this closed unit-ball is not a ring but only a multiplicative monoid.

Let $|\bullet|_\infty\colon \mathbb{R}^2 \to \mathbb{R}_{>0}$ be the standard Euclidean norm. This is the unique inner-product norm on $\mathbb{R}^2$ stabilized by $\mathbf{O}_2(\mathbb{R})$, and its homothety class $\mathbb{R}^\times|\bullet|_\infty$ is the unique homothety class of inner-product norms stabilized by $\mathbf{PO}_2(\mathbb{R})$. Denote $\|\bullet\|_\infty \coloneqq \|\bullet\|_{|\bullet|_\infty}$ — the operator norm on $\mathbf{B}(\mathbb{R})$ induced by $|\bullet|_\infty$ and the isomorphism above. This norm does not depend on the choice of isomorphism as it is $\mathrm{Ad}\,\mathbf{PGO}_2(\mathbb{R})$-invariant.

If $\mathbf{B}(\mathbb{R})$ is ramified, we fix an isomorphism of $\mathbf{B}(\mathbb{R})$ and the Hamilton quaternions and define $\|\bullet\|_\infty$ to be the the quaternion norm. This definition does not depend on the choice of isomorphism as the quaternion norm is multiplicative and conjugation invariant. Equivalently, in this case $\|\bullet\|_\infty = \sqrt{\mathrm{Nrd}}$.

In both the ramified and unramified cases the norm $\|\bullet\|_\infty$ satisfies the following useful identity:

$$\forall g \in \mathbf{B}^\times(\mathbb{R})\colon \|g^{-1}\|_\infty = \frac{\|g\|_\infty}{|\operatorname{Nrd} g|}. \tag{6}$$

We need the following definitions:

$$\begin{aligned}
\mathbb{O}_\infty &\coloneqq \left\{g \in \mathbf{B}^\times(\mathbb{R}) \mid \|g\|_\infty \leq 1\right\},\\
\mathbb{O}_\infty^\times &\coloneqq \left\{g \in \mathbf{B}^\times(\mathbb{R}) \mid \|g\|_\infty = 1, \operatorname{Nrd} g > 0\right\} \simeq \mathbf{SO}_2(\mathbb{R}),\\
\widetilde{\Omega}_\infty &\coloneqq \left\{g \in \mathbf{B}^\times(\mathbb{R}) \mid \|g^{\pm 1}\|_\infty \leq 2, \operatorname{Nrd} g > 0\right\}.
\end{aligned}$$

The set $\mathbb{O}_\infty$ is the closed unit-ball of $\|\bullet\|_\infty$, $\mathbb{O}_\infty^\times$ is the orientation-preserving isotropy group of the Euclidean norm $|\bullet|_\infty$ and $\widetilde{\Omega}_\infty$ is a connected, symmetric and compact identity neighborhood. Moreover, $\mathbb{O}_\infty^\times\widetilde{\Omega}_\infty = \widetilde{\Omega}_\infty\mathbb{O}_\infty^\times = \widetilde{\Omega}_\infty$. Elements of $\widetilde{\Omega}_\infty$ satisfy the following inequalities that follow from (6) and submultiplicativity of the operator norm:

$$\begin{aligned}\operatorname{Nrd} g &= \frac{\|g\|_\infty \|g^{-1}\|_\infty}{\|g^{-1}\|_\infty^2} \geq \frac{1}{\|g^{-1}\|_\infty^2} \geq 1/4,\\ \operatorname{Nrd} g &= \left(\operatorname{Nrd} g^{-1}\right)^{-1} \leq 4.\end{aligned} \tag{7}$$

2.3. *Simply connected cover.* Let $\mathbf{G}^{\mathrm{sc}} := \mathbf{B}^{(1)}$ be the group of unit quaternions in $\mathbf{B}$. The group $\mathbf{G}^{\mathrm{sc}}$ is the simply connected cover of $\mathbf{G}$. For an algebra $R/\mathbb{Q}$, we denote by $\mathbf{G}(R)^+$ the image of $\mathbf{G}^{\mathrm{sc}}(R)$ in $\mathbf{G}(R)$ under the isogeny map. The subgroup $\mathbf{G}(\mathbb{A})^+ < \mathbf{G}(\mathbb{A})$ is normal, and the reduced norm map $\operatorname{Nrd}\colon \mathbf{B}^\times \to \mathbb{G}_{\mathrm{m}}$ induces a monomorphism of compact abelian groups

$$\operatorname{Nrd}\colon {}^{\mathbf{G}(\mathbb{A})}\big/_{\mathbf{G}(\mathbb{A})^+} \to {}^{\mathbb{A}^\times}\big/_{\mathbb{A}^{\times 2}}.$$

To determine the image of $\operatorname{Nrd}(\mathbf{B}^\times(F))$ for a field $F/\mathbb{Q}$, notice that all the elements with a fixed reduced norm form a torsor of $\mathbf{G}^{\mathrm{sc}}$ defined over F. As such it has an F-point only if it is the trivial torsor. This can be checked using the Galois cohomology of $\mathbf{G}^{\mathrm{sc}}$. The cohomology group is trivial for each p-adic field (cf. [Kne65]), hence each element in $\mathbb{Q}_p^\times$ is a reduced norm; this can also be simply deduced from checking the two possible quaternion algebras over $\mathbb{Q}_p$. For the archimedean field $\mathbb{R}$, there are two possible quaternion algebras. In the split case every element of $\mathbb{R}^\times$ is a reduced norm, and for the Hamilton quaternions, only the positive elements $\mathbb{R}_{>0}$ are reduced norms.

For the global field $\mathbb{Q}$, this question is answered by the Hasse-Schilling-Maass theorem; cf. [Rei75, Th. 33.15]. The following global-to-local map is injective as $\mathbf{G}^{\mathrm{sc}}$ is simple and simply connected:

$$H^1(\mathbb{Q}, \mathbf{G}^{\mathrm{sc}}) \hookrightarrow H^1(\mathbb{R}, \mathbf{G}^{\mathrm{sc}}).$$

Hence if $\mathbf{B}$ is split at ∞, then every element of $\mathbb{Q}^\times$ is a reduced norm, otherwise only elements of $\mathbb{Q}_{>0}$ are reduced norms.

The reduced norm defines a monomorphism of double coset spaces

$$\mathbf{G}(\mathbb{Q})\backslash {}^{\mathbf{G}(\mathbb{A})}\big/_{\mathbf{G}(\mathbb{A})^+} \xrightarrow{\operatorname{Nrd}} \mathbb{Q}^\times \backslash {}^{\mathbb{A}^\times}\big/_{\mathbb{A}^{\times 2}}.$$

Following the discussion above we know that this morphism has full image if $\mathbf{B}$ is split at ∞ and the image is the index-2 subgroup $\mathbb{Q}_{>0}\backslash {}^{\mathbb{R}_{>0} \times \mathbb{A}_f^\times}\big/_{\mathbb{A}^{\times 2}}$ otherwise.

2.4. *Toral periods.* Periodic orbits of tori on Y can be collected into natural arithmetic packets [ELMV09], [ELMV11] that generalize the packets of CM points and closed geodesics on the modular curve.

These are easiest to define in adelic terms. Let $\mathbf{T} < \mathbf{G}$ be a maximal torus defined and anisotropic over $\mathbb{Q}$. We require the torus to be anisotropic so that the space ${}_{\mathbf{T}(\mathbb{Q})}\backslash^{\mathbf{T}(\mathbb{A})}$ has finite volume.

2.4.1. *Homogeneous sets and periodic measures.* Einsiedler, Lindenstrauss, Michel and Venkatesh have defined in [ELMV11] the notion of a homogeneous toral set. For any $g = (g_v)_v \in \mathbf{G}(\mathbb{A})$, the set

$$[\mathbf{T}(\mathbb{A})g] \subset [\mathbf{G}(\mathbb{A})]$$

is a homogeneous toral set. This set is a right translate of $[\mathbf{T}(\mathbb{A})] \simeq {}_{\mathbf{T}(\mathbb{Q})}\backslash^{\mathbf{T}(\mathbb{A})}$ and hence carries a unique probability measure invariant under the locally compact abelian group $H_{\mathbb{A}} \coloneqq g^{-1}\mathbf{T}(\mathbb{A})g$. Denote this measure by μ, and call it the *periodic toral measure*.

Special places. Because the measure rigidity arguments we use require an action by a split torus at two different places, once and for all we fix two finite rational primes p_1, p_2 such that $\mathbf{G}$ is split at p_1 and p_2. We fix two maximal split tori $A_{p_1} < \mathbf{G}(\mathbb{Q}_{p_1})$ and $A_{p_2} < \mathbf{G}(\mathbb{Q}_{p_2})$ and require that the intersection of A_{p_1} and K_{p_1} is maximal compact in A_{p_1}; equivalently, the apartment of A_{p_1} in the Bruhat-Tits buildings contains the vertex stabilized by K_{p_1}. In Section 2.2.1 we have already fixed a maximal compact torus $K_\infty < \mathbf{G}(\mathbb{R})$.

We restrict to the case when $\mathbf{T}$ is split at p_1 and p_2 and anisotropic at ∞. Unless stated otherwise, we shall always assume that

$$(\spadesuit) \qquad g_\infty^{-1}\mathbf{T}(\mathbb{R})g_\infty = K_\infty,\ g_{p_1}^{-1}\mathbf{T}(\mathbb{Q}_{p_1})g_{p_1} = A_{p_1},\ g_{p_2}^{-1}\mathbf{T}(\mathbb{Q}_{p_2})g_{p_2} = A_{p_2}.$$

2.4.2. *Packets.* Let S be a finite set of rational places containing at least ∞, p_1, p_2 and such that the following class number 1 assumption holds:

$$\# {}_{\mathbf{G}(\mathbb{Q})}\backslash^{\mathbf{G}(\mathbb{A})}/_{\mathbf{G}(\mathbb{Q}_S)\cdot K^S} = 1. \tag{8}$$

The $\mathbf{G}(\mathbb{Q}_S)$-equivariant open embedding

$$\begin{aligned} Y &\coloneqq {}_{\Gamma}\backslash^{\mathbf{G}(\mathbb{Q}_S)} \hookrightarrow {}_{\mathbf{G}(\mathbb{Q})}\backslash^{\mathbf{G}(\mathbb{A})}/_{K^S}, \\ \Gamma &\coloneqq \mathbf{G}(\mathbb{Q}) \cap K^S \end{aligned}$$

is an isomorphism due to (8).

Denote the projection of $[\mathbf{T}(\mathbb{A})g]$ to Y by $\mathscr{P}$. The set $\mathscr{P}$ is called a packet of periodic torus orbits. It is a union of periodic orbits[5] for the torus $H = \prod_{v\in S} H_v$ where $H_v = g_v^{-1}\mathbf{T}(\mathbb{Q}_v)g_v$, and our choices ($\spadesuit$) imply $H_\infty = K_\infty$, $H_{p_1} = A_{p_1}$ and $H_{p_2} = A_{p_2}$.

[5] Following [ELMV09] we say that an orbit of a locally compact group H is periodic if it supports a *finite* H-invariant Borel measure.

Action on torus orbits. Denote

$$K_{\mathbf{T}}^{S} \coloneqq gK^{S}g^{-1} \cap \mathbf{T}(\mathbb{A}^{S}) < \mathbf{T}(\mathbb{A}^{S}),$$
$$K_{\mathbf{T},f} \coloneqq K_{\mathbf{T}}^{\{\infty\}} = gK_{f}g^{-1} \cap \mathbf{T}(\mathbb{A}_{f}). < \mathbf{T}(\mathbb{A}_{f}).$$

These are compact-open subgroups of the ambient torus groups. The following finite abelian group acts simply transitively on the set of H-orbits in $\mathscr{P}$:

$$C_{S} \coloneqq {}_{\mathbf{T}(\mathbb{Q})}\backslash^{\mathbf{T}(\mathbb{A})}/_{\mathbf{T}(\mathbb{Q}_{S}) \cdot K_{\mathbf{T}}^{S}}.$$

The finiteness of C_S implies that $\mathscr{P}$ is a *finite* collection of periodic H-orbits.

We can actually incorporate the pointwise action of $H \simeq \mathbf{T}(\mathbb{Q}_S)$ on $\mathscr{P}$ and the action of C_S on the set of H-orbits into a *pointwise* action of the single group ${}^{\mathbf{T}(\mathbb{A})}/_{K_{\mathbf{T}}^{S}}$.

Periodic measure on the packet. The measure μ defines a push-forward measure $\overline{\mu}$ on Y supported on $\mathscr{P}$ and invariant under the action of H. The measure $\overline{\mu}$ is a finite average of periodic H-measures. All the periodic H-measures contribute to $\overline{\mu}$ with the same weight as can be seen using the action of C_S.

2.4.3. *Homogeneous toral sets in* $\mathbf{B}^{\times}$. Any maximal torus $\mathbf{T} < \mathbf{G}$ defined over $\mathbb{Q}$ is the image of a unique maximal torus $\widetilde{\mathbf{T}} < \mathbf{B}^{\times}$ defined over $\mathbb{Q}$.

All maximal rational tori $\widetilde{\mathbf{T}} < \mathbf{B}^{\times}$ are of the form

$$\widetilde{\mathbf{T}} \simeq \operatorname{Res}_{\mathbb{Q}}^{\mathrm{E}} \mathbb{G}_{\mathrm{m}},$$

where $E/\mathbb{Q}$ is a quadratic étale-algebra embeddable into $\mathbf{B}(\mathbb{Q})$. More specifically, let $\iota\colon E \hookrightarrow \mathbf{B}(\mathbb{Q})$ be a ring embedding. Then the image of ι is the $\mathbb{Q}$-points of a maximal commutative algebra subvariety $\mathbf{E}$ with $\mathbf{E}(\mathbb{Q}) = \iota(E)$. The corresponding torus $\widetilde{\mathbf{T}}$ is equal to $\mathbf{E}^{\times}$. Notice that an étale-algebra E does not define the subalgebra $\mathbf{E} < \mathbf{B}$ uniquely as there are many inequivalent ways to embed E in $\mathbf{B}(\mathbb{Q})$. The subalgebra $\mathbf{E}$ is defined by a specific embedding ι, up to an automorphism.

Our requirement that $\mathbf{T} = {}_{\mathbf{Z}}\backslash^{\widetilde{\mathbf{T}}} \simeq {}_{\mathbb{G}_{\mathrm{m}}}\backslash^{\operatorname{Res}_{\mathbb{Q}}^{\mathrm{E}} \mathbb{G}_{\mathrm{m}}}$ is anisotropic over $\mathbb{Q}$ is equivalent to E being a quadratic field. The condition (♠) implies that E is imaginary and split at p_1 and p_2.

Choose any representative of g in $\mathbf{B}^{\times}(\mathbb{A})$, and by abuse of notations denote it by g as well. The isomorphism of adelic quotients (5) induces an identification of homogeneous toral sets

$$[\mathbf{T}(\mathbb{A})g] = [\widetilde{\mathbf{T}}(\mathbb{A})g] \subset {}_{\mathbf{Z}(\mathbb{A})\mathbf{B}^{\times}(\mathbb{Q})}\backslash^{\mathbf{B}^{\times}(\mathbb{A})}.$$

Class group action. Let S be a finite set of rational places as in Section 2.4.2. As before, define

$$K^S_{\widetilde{\mathbf{T}}} \coloneqq g\mathbb{O}^{\times,S}g^{-1} \cap \widetilde{\mathbf{T}}(\mathbb{A}^S) < \widetilde{\mathbf{T}}(\mathbb{A}^S),$$
$$K_{\widetilde{\mathbf{T}},f} \coloneqq K^{\{\infty\}}_{\widetilde{\mathbf{T}}} = g\mathbb{O}_f^{\times}g^{-1} \cap \mathbf{T}(\mathbb{A}_f) < \mathbf{T}(\mathbb{A}_f).$$

Because of our choice of K_v to be the projection of $\mathbb{O}_v^\times$ there is also an surjective homomorphism of finite abelian groups

$$E^\times \backslash {}^{\mathbb{A}_E} \big/ {}_{E_S \cdot K^S_{\widetilde{\mathbf{T}}}} = \widetilde{\mathbf{T}}(\mathbb{Q}) \backslash {}^{\widetilde{\mathbf{T}}(\mathbb{A})} \big/ {}_{\widetilde{\mathbf{T}}(\mathbb{Q}_S) \cdot K^S_{\widetilde{\mathbf{T}}}} \twoheadrightarrow \mathbf{T}(\mathbb{Q}) \backslash {}^{\mathbf{T}(\mathbb{A})} \big/ {}_{\mathbf{T}(\mathbb{Q}_S) \cdot K^S_{\mathbf{T}}} = C_S, \tag{9}$$

where $K^S_{\widetilde{\mathbf{T}}} \coloneqq g\left(\prod_{v \notin S} \mathbb{O}_v^\times\right) g^{-1} \cap \widetilde{\mathbf{T}}(\mathbb{A}^S)$ is a compact-open subgroup in $\widetilde{\mathbf{T}}(\mathbb{A}^S)$.

The kernel of this map is the following quotient:

$$\mathbb{G}_{\mathrm{m}}(\mathbb{Q}) \backslash {}^{\mathbb{G}_{\mathrm{m}}(\mathbb{A})} \big/ {}_{\mathbb{G}_{\mathrm{m}}(\mathbb{Q}_S) \cdot \prod_{v \notin S} \mathbb{Z}_v^\times},$$

which is trivial because $\mathbb{Q}$ has a trivial class group. We see that (9) is actually an isomorphism. We have thus expressed C_S in a natural way as a quotient of the idéle class group of E. It is natural to consider C_S as a generalized S-class group of the field E.

2.4.4. *Quadratic orders and discriminants.*

The local order and local discriminant.

Definition 2.1.

(1) Recall that $\widetilde{\mathbf{T}} = \mathbf{E}^\times$ where $\mathbf{E} < \mathbf{B}$ is a maximal commutative algebra. For each place v, we define

$$\Lambda_v \coloneqq \mathbf{E}(\mathbb{Q}_v) \cap g_v \mathbb{O}_v g_v^{-1}.$$

For v non-archimedean, Λ_v is a commutative ring and an order in the étale-algebra $\mathbf{E}(\mathbb{Q}_v) \simeq E_v$.

(2) For v non-archimedean, denote the maximal order of the étale-algebra E_v by $\mathcal{O}_{E_v}$, i.e., $\mathcal{O}_{E_v} = \prod_{w|v} \mathcal{O}_{E_w}$.

Proposition 2.2. *For almost all v non-archimedean $\Lambda_v = \mathcal{O}_{E_v}$.*

Proof. As $\mathbb{Q} \cdot \mathbb{O} = \mathbf{B}(\mathbb{Q})$, we see that $\Lambda^{\mathrm{naive}} \coloneqq \mathbb{O} \cap \mathbf{E}(\mathbb{Q})$ is a $\mathbb{Z}$-lattice of full rank in the 2-dimensional $\mathbb{Q}$-vector space $\mathbf{E}(\mathbb{Q})$. We can extend any $\mathbb{Z}$-basis b of Λ^{naive} to a $\mathbb{Z}$-basis $b \cup c$ of[6] $\mathbb{O}$.

[6] This can be seen from the fact that ${}^{\mathbb{O}}\big/{}_{\Lambda^{\mathrm{naive}}}$ is a finitely generated torsion-free $\mathbb{Z}$-module and each such module is free.

Fix v non-archimedean, and denote $\Lambda_v^{\mathrm{naive}} \subset \mathbf{E}(\mathbb{Q}_v)$ for the v-adic closure of Λ^{naive}. We can use the basis above and weak approximation to explicitly write $\mathbb{O}_v = \operatorname{Span}_{\mathbb{Z}_v} b \cup c$, $\Lambda_v^{\mathrm{naive}} = \operatorname{Span}_{\mathbb{Z}_v} b$ and $\mathbf{E}(\mathbb{Q}_v) = \operatorname{Span}_{\mathbb{Q}_v} b$. In particular, $\mathbf{E}(\mathbb{Q}_v) \cap \mathbb{O}_v = \Lambda_v^{\mathrm{naive}}$.

For any v such that $g_v \in K_v$, we see that

$$\Lambda_v = \mathbf{E}(\mathbb{Q}_v) \cap \mathbb{O}_v = \Lambda_v^{\mathrm{naive}}.$$

The lattice Λ^{naive} is an order in the number field $\mathbf{E}(\mathbb{Q}) \simeq E$. The p-adic completion of Λ^{naive} is equal to the maximal order for any p relatively prime to the conductor of Λ^{naive}. Hence Λ_v is maximal if $g_v \in K_v$ and q_v is relatively prime to the conductor — which happens for almost all v. □

Lemma 2.3. *For any v non-archmiedean, there exists $\mathfrak{f}_v \in \mathbb{Z}_v$ such that $\Lambda_v = \mathbb{Z}_v + \mathfrak{f}_v \mathcal{O}_{E_v}$. The conductor of Λ_v is $\mathfrak{f}_v \mathcal{O}_{E_v}$, and Λ_v is stable under the Galois action of* $\operatorname{Gal}(E_v/\mathbb{Q}_v)$.

Proof. The argument is the same as for orders in quadratic number fields. □

Definition 2.4. We define the local discriminant D_v of the homogeneous toral set $[\mathbf{T}(\mathbb{A})g]$ in an equivalent way to [ELMV11, §6.1].

(1) For v non-archimedean, D_v is the discriminant of the order Λ_v. In particular, for all places v where E is unramified and Λ_v is maximal, we have D_v=1.

(2) For v archimedean, there is a natural topological ring isomorphism of $\mathbf{E}(\mathbb{R})$ either to $\mathbb{R} \times \mathbb{R}$ or to $\mathbb{C}$ unique up to an automorphism. Consider the standard volume form on $\mathbb{R} \times \mathbb{R}$ or $\mathbb{C}$ induced by the inner-product norm $\alpha \mapsto |\alpha|$ or $(\alpha, \beta) \mapsto \sqrt{|\alpha|^2 + |\beta|^2}$, and pull it back to $\mathbf{E}(\mathbb{R})$.

Let $\Lambda_\infty \subset \mathbf{E}(\mathbb{R})$ be the intersection of the closed unit ball of $\| \bullet \|_\infty$ with $\mathbf{E}(\mathbb{R})$. Define D_∞ to be the square of the volume of Λ_∞ with respect to the latter volume-form.

(3) Finally, the global discriminant is defined to be $D \coloneqq \prod_v D_v$.

Remark 2.5. Conjugating by g_v we have $\Lambda_v \simeq g_v^{-1} \mathbf{E}(\mathbb{Q}_v) g_v \cap \mathbb{O}_v$. Thus the local discriminant D_v for $v = \infty, p_1, p_2$ is the same for all homogeneous toral sets for which $(\spadesuit)$ holds.

Moreover, our choice of $\| \bullet \|_\infty$ to be K_∞-invariant in Section 2.2.1 and the requirement that $g_\infty^{-1} \mathbf{T}(\mathbb{R}) g_\infty = K_\infty$ in $(\spadesuit)$ imply $D_\infty = 1$.

The global order.

Definition 2.6. We define a global order $\Lambda < \mathbf{E}(\mathbb{Q}) \simeq E$ by

$$\Lambda \coloneqq \bigcap_{v \neq \infty} \Lambda_v,$$

where the intersection is taken in the 2-dimensional $\mathbb{Q}$-vector space $\mathbf{E}(\mathbb{Q})$.

Recall that by Proposition 2.2, Λ_v is equal to the v-adic closure of $\mathcal{O}_E$ for almost all v, hence the intersection Λ is a finite index $\mathbb{Z}$-sublattice in $\mathcal{O}_E$. Moreover, it is closed under multiplication, so it is an order in $\mathbf{E}(\mathbb{Q})$. The discriminant of Λ is exactly $\prod_{v\neq\infty} D_v$. Notice that in general $\Lambda \neq \mathbf{E}(\mathbb{Q}) \cap \mathbb{O}$.

Remark 2.7. A consequence of the discussion above is that for all $v \neq \infty$, the compact-open subgroup $\mathbf{K}_{\widetilde{\mathbf{T}},v} := g_v \mathbb{O}_v g_v^{-1} \cap \widetilde{\mathbf{T}}(\mathbb{Q}_v) < \widetilde{\mathbf{T}}(\mathbb{Q}_v)$ is the unit group of the order Λ_v.

In particular, if $K_{\widetilde{\mathbf{T}},f} := \prod_{v\neq\infty} K_{\widetilde{\mathbf{T}},v} < \widetilde{\mathbf{T}}(\mathbb{A}_f)$, then

$$C_{\{\infty\}} \simeq {}_{\widetilde{\mathbf{T}}(\mathbb{Q})}\backslash^{\widetilde{\mathbf{T}}(\mathbb{A})}/_{\widetilde{\mathbf{T}}(\mathbb{Q}_S)\cdot K^S_{\widetilde{\mathbf{T}}}} \simeq \operatorname{Pic}(\Lambda).$$

Idéles and ideals.

Definition 2.8. Let $[\mathbf{T}(\mathbb{A})g]$ be a homogeneous toral set with splitting field $E/\mathbb{Q}$ and global order $\Lambda := \cap_{v\neq\infty}\Lambda_v \subseteq \mathcal{O}_E$.

(1) Denote by $\mathcal{J}(\Lambda)$ the abelian group of invertible proper Λ-fractional ideals. These are exactly the locally principle fractional ideals, and there is a canonical group isomorphism

$$\widetilde{\mathrm{idl}}\colon {}^{\widetilde{\mathbf{T}}(\mathbb{A}_f)}/_{K_{\widetilde{\mathbf{T}},f}} = {}^{\prod_{v\neq\infty} E_v^\times}/_{\prod_{v\neq\infty}\Lambda_v^\times} \to \mathcal{J}(\Lambda)$$

defined by $(\alpha_v\Lambda_v^\times)_{v\neq\infty} \mapsto \bigcap_{v\neq\infty} \alpha_v\Lambda_v \subset E$.

(2) Define $\mathcal{J}(\Lambda)_0 := \mathcal{J}(\Lambda) \cup \{0\cdot\Lambda\}$. This set of ideals does not carry a group structure any more but there is a natural action of $\mathcal{J}(\Lambda)$ on it, and hence also an action of the finite E-idèles. The map above extends naturally to a surjective equivariant map

$$\widetilde{\mathrm{idl}}\colon {}^{\mathbf{E}(\mathbb{A}_f)}/_{K_{\widetilde{\mathbf{T}},f}} = {}^{\prod_{v\neq\infty} E_v}/_{\prod_{v\neq\infty}\Lambda_v^\times} \to \mathcal{J}(\Lambda)_0,$$

which is no longer a bijection. The preimage of the zero ideal contains any non-invertible adèle. The preimage of any invertible fractional ideal still contains only one element.

(3) The map idl above descend to the following function:

$$\begin{aligned}\mathrm{idl}\colon {}^{\mathbf{T}(\mathbb{A}_f)}/_{K_{\mathbf{T},f}} &= {}_{\mathbb{A}_f^\times}\backslash^{\prod_{v\neq\infty} E_v^\times}/_{\prod_{v\neq\infty}\Lambda_v^\times}\\ &= {}_{\mathbb{Q}^\times}\backslash^{\prod_{v\neq\infty} E_v^\times}/_{\prod_{v\neq\infty}\Lambda_v^\times} \xrightarrow{\widetilde{\mathrm{idl}}} {}_{\mathbb{Q}^\times}\backslash^{\mathcal{J}(\Lambda)}.\end{aligned}$$

The second equality above holds because $\mathbb{Q}$ has trivial class group.

2.4.5. *Volume.* The volume of a homogeneous toral set has been defined in [ELMV11]. To motivate the definition, consider a normalization in which the measure of the group under which the homogeneous set is invariant — $H_{\mathbb{A}}$ — is kept fixed while the homogeneous toral set varies in a family. In the adelic setting it is impossible to keep $H_{\mathbb{A}}$ independent of the homogeneous set in the family, yet we can normalize the measures in a uniform way.

To do that fix a compact identity neighborhood $\Omega = \prod_v \Omega_v \subset \mathbf{G}(\mathbb{A})$. Normalize the Haar measure $\mathrm{m}_{H_{\mathbb{A}}}$ on $H_{\mathbb{A}}$ so that $\mathrm{m}_{H_{\mathbb{A}}}(\Omega) = 1$. The measure $\mathrm{m}_{H_{\mathbb{A}}}$ also induces an $H_{\mathbb{A}}$-invariant measure on $[\mathbf{T}(\mathbb{A})g]$ that differs from μ by a constant. The volume of the homogeneous set is defined as the volume of $[\mathbf{T}(\mathbb{A})g]$ with respect to the measure induced by $\mathrm{m}_{H_{\mathbb{A}}}$.

A formula for the volume can be written in terms of the covolume 1 Haar measure $\mathrm{m}_{\mathbf{T}}$ on $\mathbf{T}(\mathbb{A})$,

$$\operatorname{vol}\left([\mathbf{T}(\mathbb{A})g]\right) \coloneqq \mathrm{m}_{\mathbf{T}}\left(g\Omega g^{-1}\right)^{-1}.$$

The definition of the volume depends on the choice of a compact identity neighborhood Ω but in an inessential way. Specifically, for any compact identity neighborhoods Ω and Ω',

$$\operatorname{vol}_{\Omega}\left([\mathbf{T}(\mathbb{A})g]\right) \ll_{\Omega,\Omega'} \operatorname{vol}_{\Omega'}\left([\mathbf{T}(\mathbb{A})g]\right) \ll_{\Omega,\Omega'} \operatorname{vol}_{\Omega}\left([\mathbf{T}(\mathbb{A})g]\right). \tag{10}$$

Most importantly, the constants do not depend on the homogeneous toral set.

Once and for all we fix $\Omega_v = K_v$ for all non-archimedean v and $\Omega_\infty = \mathbf{Z}(\mathbb{R})\widetilde{\Omega}_\infty$, where $\widetilde{\Omega}_\infty$ is as in Section 2.2.1. The set Ω_∞ is a connected, compact, symmetric and $\operatorname{Ad} K_\infty$-invariant identity neighborhood in $\mathbf{G}(\mathbb{R})$. In the ramified case this neighborhood coincides with $\mathbf{G}(\mathbb{R})$. These choices simplify computations later.

2.5. *Joinings of periodic toral measures.* Let $[\mathbf{T}(\mathbb{A})g] \subset [\mathbf{G}(\mathbb{A})]$ be a homogeneous toral set with periodic measure μ as in the previous section. Denote by $\mathbf{T}^{\Delta} < \mathbf{G} \times \mathbf{G}$ the diagonal embedding.

Fix $s \in \mathbf{T}(\mathbb{A})$, and consider the following subset of the cartesian square of $[\mathbf{G}(\mathbb{A})]$:

$$[\mathbf{T}^{\Delta}(\mathbb{A})(g, sg)] \subset [(\mathbf{G} \times \mathbf{G})(\mathbb{A})].$$

This is a homogeneous set for the *non-maximal* rank 1 anisotropic torus $\mathbf{T}^{\Delta}$ in the rank 2 group $\mathbf{G} \times \mathbf{G}$.

By the same arguments as in the previous sections this set carries a probability measure μ^{joint} invariant under the action of[7] $H^{\Delta}_{\mathbb{A}}$.

[7] Notice that s commutes with $\mathbf{T}(\mathbb{A})$.

The measure μ^{joint} projects in each coordinate to the regular periodic toral measure μ supported on $[\mathbf{T}(\mathbb{A})g]$. It is a self-joining of μ that is non-trivial because of the shift by $s \in \mathbf{T}(\mathbb{A})$.

We call s the *twist* of the self-joining. Notice the that whole class of s in ${}_{\mathbf{T}(\mathbb{Q})}\backslash^{\mathbf{T}(\mathbb{A})}$ defines exactly the same self-joining.

2.5.1. *Joining of packets.* Let S and Y be as in Section 2.4.2. Denote by H^{Δ} the diagonal embedding of H into $\mathbf{G}(\mathbb{Q}_S)\times\mathbf{G}(\mathbb{Q}_S)$. The set $[\mathbf{T}^{\Delta}(\mathbb{A})(g,sg)]$ projects to a finite collection of H^{Δ} orbits on $Y \times Y$ denoted by $\mathscr{P}^{\mathrm{joint}}$. The measure μ^{joint} can be pushed forward to an H^{Δ}-invariant probability measure on $\mathscr{P}^{\mathrm{joint}}$, which we denote by $\overline{\mu^{\mathrm{joint}}}$. The measure $\overline{\mu^{\mathrm{joint}}}$ is a self-joining of the H-invariant measure $\overline{\mu}$ on Y.

2.5.2. *Volume and discriminant.* The definitions of volume and discriminant extend trivially from homogeneous set of $\mathbb{Q}$-anisotropic rank 1 tori in $\mathbf{G}$ to anisotropic rank 1 tori in $\mathbf{G}\times\mathbf{G}$. By choosing $\Omega\times\Omega$ as the reference identity neighborhood on $(\mathbf{G}\times\mathbf{G})(\mathbb{A})$ and setting $\mathbb{O}\times\mathbb{O}$ as the reference maximal order in $(\mathbf{B}\times\mathbf{B})(\mathbb{Q})$, we have

$$\operatorname{vol}\left(\left[\mathbf{T}^{\Delta}(\mathbb{A})(g,sg)\right]\right) = \operatorname{vol}\left([\mathbf{T}(\mathbb{A})g]\right).$$
$$\operatorname{disc}\left(\left[\mathbf{T}^{\Delta}(\mathbb{A})(g,sg)\right]\right) = \operatorname{disc}\left([\mathbf{T}(\mathbb{A})g]\right).$$

3. Principal results

In this section we present our main theorem and prove key corollaries, a few reduction steps and complementary propositions. The proof of the main theorem is presented in Section 10 and builds upon the tools developed in the rest of the manuscript.

We will use the following shorthand to simplify our notation.

Definition 3.1. Denote $G_{\mathrm{res}} := {}_{\mathbf{G}(\mathbb{Q})}\backslash^{\mathbf{G}(\mathbb{A})}/_{\mathbf{G}(\mathbb{A})^+}$, and let $\pi^+\colon [\mathbf{G}(\mathbb{A})] \to G_{\mathrm{res}}$ be the quotient map.

The topological space G_{res} is a compact abelian group such that the composition of quotient maps $\mathbf{G}(\mathbb{A}) \to [\mathbf{G}(\mathbb{A})] \xrightarrow{\pi^+} G_{\mathrm{res}}$ is a continuous surjective group homomorphism; cf. Section 2.3. This implies that the push-forward of the probability Haar measure on $[\mathbf{G}(\mathbb{A})]$ to G_{res} is the probability Haar measure of G_{res}.

3.1. *Equidistribution of toral orbits.* The following is the key theorem of this work.

THEOREM 3.2. *Let $\mathbf{G}$ be a form of $\mathbf{PGL}_2$ over $\mathbb{Q}$. Fix a maximal compact torus $K_\infty < \mathbf{G}(\mathbb{R})$ and two finite primes p_1, p_2. Let $\{\mathscr{H}_i\}_i$ be a sequence of joint* *homogeneous toral sets. For each i, write $\mathscr{H}_i = \left[\mathbf{T}^{\Delta}(\mathbb{A})(g, sg)\right]$, where $\mathbf{T}, s, g$ depend on i. Recall that $\mathbf{T} < \mathbf{G}$ is a maximal torus defined and anisotropic over $\mathbb{Q}$, $g \in \mathbf{G}(\mathbb{A})$ and $s \in \mathbf{T}(\mathbb{A})$.*

Let $E_i/\mathbb{Q}$ be the quadratic field splitting $\mathbf{T}$, and let D_i be the discriminant of $\mathscr{H}_i$. Denote by $\mathfrak{f}_i$ the conductor of D_i; i.e., $\mathfrak{f}_i^2 \mid D_i$ is the largest square divisor of D_i.

Denote by μ_i the algebraic probability measure on $[(\mathbf{G} \times \mathbf{G})(\mathbb{A})]$ supported on $\mathscr{H}_i$.

Assume the following for all $i \in \mathbb{N}$:

(1) $g_\infty^{-1}\mathbf{T}(\mathbb{R})g_\infty = K_\infty$,
(2) p_1, p_2 *split in* E_i,
(3) *the Dedekind ζ function of E_i has no exceptional Landau-Siegel zero,*
(4) $\mathfrak{f}_i \ll 1$.

If $|D_i| \to \infty$ and the following holds for any compact subset $B \subset \mathbf{G}(\mathbb{A})$,

$$\forall i \gg_B 1\colon g^{-1}\mathbf{T}(\mathbb{Q})sg \cap B = \emptyset,$$

then any weak-$*$ limit point of $\{\mu_i\}_i$ is a $(\mathbf{G} \times \mathbf{G})(\mathbb{A})^+$-invariant probability measure.

Corollary 3.3. *Denote by*

$$L^2_{00}\left(\left[(\mathbf{G} \times \mathbf{G})(\mathbb{A})\right], \mathrm{m}_{\mathbf{G}\times\mathbf{G}}\}\right) < L^2\left(\left[(\mathbf{G} \times \mathbf{G})(\mathbb{A})\right], \mathrm{m}_{\mathbf{G}\times\mathbf{G}}\right)$$

the subspace orthogonal to the residual spectrum. Then in the setting of Theorem 3.2, for any continuous compactly supported *function*

$$f \in L^2_{00}\left(\left[(\mathbf{G} \times \mathbf{G})(\mathbb{A})\right], \mathrm{m}_{\mathbf{G}\times\mathbf{G}}\right),$$

we have

$$\int f \, \mathrm{d}\mu_i \to_{i\to\infty} 0.$$

Proof. Each fiber of π^+ admits a transitive $\mathbf{G}(\mathbb{A})^+$ action inducing an isomorphism of the fiber with $[\mathbf{G}(\mathbb{A})^+]$. This isomorphism depends on the choice of a base point. The probability Haar measure on $[\mathbf{G}(\mathbb{A})^+]$ defines a probability measure on the fiber which is independent of the choice of base point due to the invariance property of the Haar measure. The conditional measures of $\mathrm{m}_{\mathbf{G}}$ on the fibers of $[\mathbf{G}(\mathbb{A})] \to G_{\mathrm{res}}$ are $\mathbf{G}(\mathbb{A})^+$-invariant probability measures, and hence they can be taken to coincide with the previously described measures on the fibers.

The residual spectrum is by definition the space of function factoring through $\pi^+ \times \pi^+$, and a function is orthogonal to the residual spectrum if its conditional expectation with respect to the pull-back of the Borel σ-algebra under $\pi^+ \times \pi^+$ vanishes. In terms of conditional measures this is equivalent to the function having integral 0 over the conditional measure of $\mathrm{m}_{\mathbf{G}} \times \mathrm{m}_{\mathbf{G}}$ for almost each fiber. For a compactly supported continuous function f orthogonal to the residual spectrum, we deduce that it has integral 0 over each fiber with respect to the $(\mathbf{G}\times\mathbf{G})(\mathbb{A})^{+}$-invariant measure.

Since each $(\mathbf{G}\times\mathbf{G})(\mathbb{A})^{+}$-invariant probability measure on $[(\mathbf{G}\times\mathbf{G})(\mathbb{A})]$ is a convex combination of the measures on the fibers of $\pi^{+}\times\pi^{+}$, we deduce that all the limit points of $\int f\,\mathrm{d}\mu_i$ are 0. □

3.2. *Reduction to a fixed invariance group at p_1, p_2.* In the rest of the manuscript we work with homogeneous toral sets satisfying the conditions of $(\spadesuit)$ that are more restrictive then the conditions in Theorem 3.2. In particular, we require for all homogeneous toral sets $[\mathbf{T}(\mathbb{A})g]$ that $g_{p_j}^{-1}\mathbf{T}(\mathbb{Q}_{p_j})g_{p_j}=A_{p_j}$ for $j\in\{1,2\}$ and some fixed split tori $A_{p_j}<\mathbf{G}(\mathbb{Q}_{p_j})$. In this section we show that Theorem 3.2 can be reduced to the case of joint homogeneous toral sets satisfying these additional conditions.

Proposition 3.4. *Let $\{\mathscr{H}_i\}_i$ and $\{\mu_i\}_i$ be as in Theorem 3.2. Then there is a* bounded *sequence $h_i\in\mathbf{G}(\mathbb{A})$ such that $\mathscr{H}_i(h_i,h_i)\subseteq[(\mathbf{G}\times\mathbf{G})(\mathbb{A})]$ satisfies $(\spadesuit)$ for all $i\in\mathbb{N}$.*

Proof. The main observation is that the local discriminant is a proper continuous map on the variety of tori. Let $p\in\{p_1,p_2\}$. Because all $\mathbb{Q}_p$-split tori in $\mathbf{G}(\mathbb{Q}_p)$ are conjugate, we identify the space of $\mathbb{Q}_p$-split tori with ${}^{\mathbf{G}(\mathbb{Q}_p)}\!/_{\mathrm{N}_{\mathbf{G}(\mathbb{Q}_p)}A_p}$. To each split torus we can associate a discriminant in the manner of Section 2.4.4. Specifically, let $\overline{A}<\mathbf{B}(\mathbb{Q}_p)$ be the split quadratic étale-algebra associated to A_p. If $T=hAh^{-1}$ for some $h\in\mathbf{G}(\mathbb{Q}_p)$ then $\operatorname{disc}(T)$ is the discriminant of the order $h\overline{A}h^{-1}\cap\mathbb{O}$. This function is continuous and proper as follows from [ELMV11, §§4.2, 6.1].

If $\mathscr{H}_i=[\mathbf{T}(\mathbb{A})(g_i,s_ig_i)]$, then assumption (4) in Theorem 3.2 and properness of the local discriminant map imply that $g_{i,p}^{-1}\mathbf{T}_i(\mathbb{Q}_p)g_{i,p}$ is a bounded sequence in the space of tori ${}^{\mathbf{G}(\mathbb{Q}_p)}\!/_{\mathrm{N}_{\mathbf{G}(\mathbb{Q}_p)}A_p}$ for $p\in\{p_1,p_2\}$. Thus we can choose a *bounded* sequence $h_{i,p}\in\mathbf{G}(\mathbb{Q}_p)$ such that $g_{i,p}^{-1}\mathbf{T}_i(\mathbb{Q}_p)g_{i,p}=h_{i,p}A_ph_{i,p}^{-1}$ for all $i\in\mathbb{N}$.

Define $h_i\in\mathbf{G}(\mathbb{A})$ to have coordinate $h_{i,p}$ for $p\in\{p_1,p_2\}$ and have trivial coordinates at all other places. This sequence obviously satisfies the claimed properties. □

Corollary 3.5. *Theorem 3.2 for joint homogeneous toral sets satisfying $(\spadesuit)$ implies the general case of Theorem 3.2.*

Proof. Let $\{\mathscr{H}_i\}_i$ and $\{\mu_i\}_i$ be as in Theorem 3.2. Because this sequence of measures is tight by Duke's theorem, we can pass without loss of generality to a convergent subsequence with limit μ. Let $h_i\in\mathbf{G}(\mathbb{A})$ be the bounded sequence from Proposition 3.4 above. Without loss of generality we pass to a further subsequence such that $h_i \to_{i\to\infty} h \in \mathbf{G}(\mathbb{A})$.

For any $g \in \mathbf{G}(\mathbb{A})$, denote by $R_g\colon [\mathbf{G}(\mathbb{A})] \to [\mathbf{G}(\mathbb{A})]$ the transformation of multiplying by g^{-1} on the right. For each i, the measure $(R_{h_i} \times R_{h_i})_* .\mu_i$ is the algebraic measure supported on $\mathscr{H}_i(h_i, h_i)$ and we have

$$(R_{h_i} \times R_{h_i})_* .\mu_i \to_{i\to\infty} (R_h \times R_h)_* .\mu.$$

Our assumption implies the measure on the right-hand side is a $(\mathbf{G} \times \mathbf{G})(\mathbb{A})^+$ invariant measure. The same statement then holds for μ because $(\mathbf{G} \times \mathbf{G})(\mathbb{A})^+$ is a normal subgroup. □

3.3. *Limit behavior of residual spectrum.* The following, significantly easier, proposition supplements the main theorem as it can be used to understand the asymptotic behavior for the residual spectrum.

Proposition 3.6. *Let $\{\mu_i\}_i$ and $E_i/\mathbb{Q}$ be as in Theorem 3.2, although we do not require that conditions (1)–(4) from the theorem are satisfied.*

Assume one of the following two options holds: either all the fields E_i are distinct, or they are all equal to a fixed quadratic field $E_0/\mathbb{Q}$. In the former case define $H := G_{\mathrm{res}}$, and in the latter case set $H := \ker(\chi_{E_0} \circ \mathrm{Nrd})$, where $\chi_{E_0}\colon {}_{\mathbb{Q}^\times}\backslash^{\mathbb{A}^\times}/_{\mathbb{A}^{\times 2}} \to \{\pm 1\}$ is the real adelic character attached to $E_0/\mathbb{Q}$ by global class field theory.

Then any limit point of $(\pi^+ \times \pi^+)_* .\mu_i$ is an H^Δ-invariant probability measure supported on a single coset of H^Δ.

Remark 3.7. It will be evident from the proof that in general, even under the assumptions of the proposition above $\{(\pi^+ \times \pi^+)_* .\mu_i\}_i$ need not converge.

Proof. Recall from Section 2.3 that the reduced norm map induces a monomorphism

$$\mathrm{Nrd}\colon G_{\mathrm{res}} \to {}_{\mathbb{Q}^\times}\backslash^{\mathbb{A}^\times}/_{\mathbb{A}^{\times 2}}.$$

This map is onto if $\mathbf{B}$ is split at ∞, and otherwise it is the index 2 subgroup ${}_{\mathbb{Q}_{>0}}\backslash^{\mathbb{R}_{>0} \times \mathbb{A}_f^\times}/_{\mathbb{A}^{\times 2}}$.

Assume $\{\mu_i\}_i$ converges weak-$*$, and let $\left[\mathbf{T}_i(\mathbb{A})^\Delta(g_i, s_i g_i)\right]$ be the homogeneous toral set of μ_i. By restricting to a subsequence we can assume without loss of generality that $\pi^+(g_i)$ and $\pi^+(s_i)$ converge in G_{res} to some $\gamma, \sigma \in G_{\mathrm{res}}$.

Fix an index $i \in \mathbb{N}$, and let $\mathbf{T} := \mathbf{T}_i$ and $E := E_i$. Because $\mathbf{T}(\mathbb{A})$ is abelian and $\mathbf{T}$ is isotropic over $\mathbb{Q}$ the homogeneous set, $[\mathbf{T}(\mathbb{A})]$ is a compact abelian group. In particular, $\pi^+([\mathbf{T}(\mathbb{A})])$ is a closed subgroup of G_{res}. To describe this subgroup explicitly recall that the isomorphism $\mathbf{T} \simeq {}_{\mathbb{G}_m}\backslash^{\mathrm{Res}_{\mathbb{Q}}^{E}\mathbb{G}_m}$ intertwines the reduced norm map with the regular field norm map. Thus

$$\mathrm{Nrd} \circ \pi^+([\mathbf{T}(\mathbb{A})]) = \ker \chi_E,$$

where $\chi_E\colon {}_{\mathbb{Q}^\times}\backslash^{\mathbb{A}^\times}/_{\mathbb{A}^{\times 2}} \to \{\pm 1\}$ is the real adelic character attached to $E/\mathbb{Q}$ by global class field theory. Henceforth we shall denote this character by χ_i.

If $\chi_i = \chi_{E_0}$ for all i where $E_0/\mathbb{Q}$ is a fixed imaginary quadratic field, then define $H \coloneqq \ker\left(\chi_{E_0} \circ \mathrm{Nrd}\right) < G_{\mathrm{res}}$. Otherwise, our assumption implies that all the characters χ_i are mutually distinct. Because ${}_{\mathbb{Q}^\times}\backslash^{\mathbb{A}^\times}/_{\mathbb{A}^{\times 2}}$ is compact, its Pontryagin dual is discrete. Hence if the character χ_i are distinct, the sequence $\{\chi_i\}_i$ diverges. If $\{\chi_i\}_i$ diverges, then the sequence of subgroups $\{\langle\chi_i\rangle\}_i$ converge in the Chabauty topology to the trivial group $1 < G_{\mathrm{res}}$. Pontryagin-Chabauty duality [Cor11] then implies that $\ker\chi_i$ converges in the Chabauty topology to the full subgroup ${}_{\mathbb{Q}^\times}\backslash^{\mathbb{A}^\times}/_{\mathbb{A}^{\times 2}}$. In this case set $H \coloneqq G_{\mathrm{res}}$.

For all i, denote $\nu_i \coloneqq (\pi^+ \times \pi^+)_* .\mu_i$, and let ν be the limit measure. From the discussion above it follows that $\mathrm{Nrd}_* .\nu_i$ is the $\ker\chi_i^\Delta$-invariant probability measure on $\ker\chi_i^\Delta(\pi^+(g), \pi^+(gs_i))$. The limit measure $\mathrm{Nrd}_* .\nu$ is invariant under the action of the Chabauty limit of the invariance subgroups $\ker\chi_i^\Delta$, which is $\mathrm{Nrd}(H)^\Delta$. We deduce that ν is invariant under H^Δ.

We are left only with proving that ν is supported on a single coset of H. Using the continuous contraction map $\mathrm{ctr}\colon G_{\mathrm{res}} \times G_{\mathrm{res}} \to G_{\mathrm{res}}$ define the push-forward probability measures $\mathrm{ctr}_* .\nu_i$ on G_{res}. The characterization of $\mathrm{Nrd}_* .\nu_i$ above implies that

$$\mathrm{Nrd}_* .\, \mathrm{ctr}_* .\nu_i = \delta_{\mathrm{Nrd}(\pi^+(s_i))} \to_{i\to\infty} \delta_{\mathrm{Nrd}(\sigma)},$$

hence $\mathrm{ctr}_* .\nu = \delta_\sigma$. This implies that ν is supported on $G_{\mathrm{res}}^\Delta(e,\sigma)$, and the proof is concluded in the case that $H = G_{\mathrm{res}}$.

If $H = \ker\chi_E$, then $\nu_i(\pi^+(g_i), \pi^+(s_i g_i))^{-1}$ is independent of i and is equal to the Haar measure on H^Δ. The claim follows because

$$\nu_i(\pi^+(g_i), \pi^+(s_i g_i))^{-1} \to_{i\to\infty} \nu(\gamma, \sigma\gamma)^{-1}. \qquad \square$$

3.4. *Many-fold toral joinings.* A pleasant consequence of the joining theorem of Einsiedler and Lindenstrauss is that we can understand n-joinings of periodic toral measures using the theorem for 2-joinings. The main observation is that if a reductive subgroup $\mathbf{L} < \underbrace{\mathbf{G} \times \cdots \times \mathbf{G}}_{n}$ projects onto $\mathbf{G} \times \mathbf{G}$ in any of the $\binom{n}{2}$ pairs of coordinates, then it must be equal to the full n-product.

Definition 3.8. Fix $n \in \mathbb{N}$. Let $\mathbf{T} < \mathbf{G}$ be a maximal torus defined and anisotropic $/\mathbb{Q}$. Denote by $\mathbf{T}^\Delta < \mathbf{G}^{\times n}$ the diagonal embedding.

Fix $s_1, \ldots, s_{n-1} \in \mathbf{T}(\mathbb{A})$ and $g \in \mathbf{G}(\mathbb{A})$. The set

$$\left[\mathbf{T}^\Delta(\mathbb{A})(g, s_1 g, \ldots, s_{n-1} g)\right] \subset \left[\mathbf{G}^{\times n}(\mathbb{A})\right]$$

is an n-joint homogeneous toral set. This set supports a unique $\left(g^{-1}\mathbf{T}(\mathbb{A})g\right)^\Delta$-invariant probability measure.

THEOREM 3.9. *Let $\mathbf{G}$ be a form of $\mathbf{PGL}_2$ over $\mathbb{Q}$. Fix a maximal compact torus $K_\infty < \mathbf{G}(\mathbb{R})$ and two finite primes p_1, p_2.*

Let $\{\mathscr{H}_i\}_i$ be a sequence of n-joint homogeneous toral sets. For each i, write $\mathscr{H}_i = \left[\mathbf{T}^\Delta(\mathbb{A})(g, s_1 g, \ldots, s_{n-1}g)\right]$ where $\mathbf{T}, \{s_j\}_{1\leq j<n}, g$ depend on i. Recall that $\mathbf{T} < \mathbf{G}$ is a maximal torus defined and anisotropic over $\mathbb{Q}$, $g \in \mathbf{G}(\mathbb{A})$ and $s_1, \ldots, s_{n-1} \in \mathbf{T}(\mathbb{A})$.

Let $E_i/\mathbb{Q}$ be the quadratic field splitting $\mathbf{T}$, and let D_i be the discriminant of $\mathscr{H}_i$. Denote by f_i the conductor of D_i; i.e., $f_i^2 \mid D_i$ is the largest square divisor of D_i.

Denote by μ_i the algebraic probability measure on $[\mathbf{G}^{\times n}(\mathbb{A})]$ supported on $\mathscr{H}_i$.

Assume the following for all $i \in \mathbb{N}$:

(1) $g_\infty^{-1}\mathbf{T}(\mathbb{R})g_\infty = K_\infty$;
(2) *p_1, p_2 split in E_i;*
(3) *the Dedekind ζ function of E_i has no exceptional Landau-Siegel zero;*
(4) $f_i \ll 1$.

If $|D_i| \to \infty$ and if the following holds for any compact subset $B \subset \mathbf{G}(\mathbb{A})$ and for any pair of distinct elements $s, s' \in \{1, s_1, \ldots, s_{n-1}\}$

$$\forall i \gg_B 1\colon g^{-1}\mathbf{T}(\mathbb{Q})s^{-1}s'g \cap B = \emptyset, \tag{11}$$

then any weak-$*$ limit point of $\{\mu_i\}_i$ is a $\mathbf{G}^{\times n}(\mathbb{A})^+$-invariant probability measure.

Proof. The proof follows from Theorem 9.7 and [EL15a, Cor. 1.5]. □

3.5. *Galois orbits of special points.*

THEOREM 3.10. *Let $\mathbf{G}$ be a form of $\mathbf{PGL}_2$ defined over $\mathbb{Q}$ and split over $\mathbb{R}$. Let X be a product of n quaternionic Shimura varieties relative to $\mathbf{G}$.*

Let $\{x_i\}_i$ be a sequence of special points in X all whose coordinates have CM *by the same quadratic order $\Lambda_i < E_i$ of discriminant $D_i < 0$ and conductor f_i. Fix two primes p_1, p_2, and assume the following for all $i \in \mathbb{N}$:*

(1) *p_1, p_2 split in E_i;*
(2) *the Dedekind ζ-function of E_i has no exceptional Landau-Siegel zero;*
(3) $f_i \ll 1$.

Denote by ν_i the normalized counting measure on the finite Galois orbit of x_i. If the sequence $\{x_i\}_i$ has finite intersection with any proper special subvariety, then any weak-$*$ limit of $\{\nu_i\}_i$ is a convex combination of the uniform probability measures on the connected components of X.

Proof. We will show how this theorem follows from Theorem 3.9 above. The definition of a Shimura variety relative to $\mathbf{G}$ (cf. [Mil05, §5]) implies that there is a surjective projection map

$$\Pi\colon \left[\mathbf{G}^{\times n}(\mathbb{A})\right] \to X$$

defined by dividing the adelic quotient by the compact group $\prod_{j=1}^{n}(K_\infty \times U_j)$ where $K_\infty < \mathbf{G}(\mathbb{R})$ is a compact torus and $U_j < \mathbf{G}(\mathbb{A}_f)$ is a compact-open subgroup for all $1 \leq j \leq n$.

In this case, the reciprocity map of class field theory supplies (cf. [Mil05, §12]) an identification between the Galois orbit of x_i and the image under Π of a homogeneous toral set

$$\mathscr{H}_i = \left[\mathbf{T}^{\Delta}(g_1, \ldots, g_n)\right] \subset \left[\mathbf{G}^{\times n}(\mathbb{A})\right],$$

where $\mathbf{T} < \mathbf{G}$ satisfies the conditions of Theorem 3.9. Moreover, the counting measure on the Galois orbit is the push-forward of the period measure μ_i on $\mathscr{H}_i$.

The homogeneous toral set $\mathscr{H}_i$ is of the form treated in Theorem 3.9 if all the n coordinates of x_i are Galois conjugate. In general, there can be more then one Galois orbit with the same CM order Λ_i, yet they all differ by an element of a maximal compact subgroup in $\mathbf{G}^{\times n}(\mathbb{A})$, i.e., by Atkin-Lehner involutions. Specifically, let $K_{f,j} < \mathbf{G}(\mathbb{A}_f)$ be a maximal compact subgroup containing U_j. Then the homogeneous toral set $\mathscr{H}_i$ can be taken to be

$$\mathscr{H}_i = \left[\mathbf{T}^{\Delta}(g, s_1 g k_1^i, \ldots, s_{n-1} g_n k_{n-1}^i)\right] \subset \left[\mathbf{G}^{\times n}(\mathbb{A})\right],$$

where $g \in \mathbf{G}(\mathbb{A})$, $s_1, \ldots, s_{n-1} \in \mathbf{T}(\mathbb{A})$ and $k^i \coloneqq (1, k_1^i, \ldots, k_{n-1}^i) \in \times K_{1,f} \times \cdots \times K_{n,f}$. Denote by μ_i the period measure supported on $\mathscr{H}_i$ and whose push-forward to X is ν_i.

If the sequence $\{x_i\}_i$ has a finite intersection with any proper special subvariety, then the same property holds for any fixed pair of coordinates of $\{x_i\}_i$ when considered as a sequence of special points on a product of two varieties. This implies the genericity condition (11) in Theorem 3.9 for the homogeneous toral sets $\mathscr{H}_i {k^i}^{-1}$. In particular, all the condition of this theorem hold for the sequence $\{\mathscr{H}_i {k^i}^{-1}\}$ and we deduce the any weak-$*$ limit of $\{\mu_i {k^i}^{-1}\}_i$ is a $\mathbf{G}^{\times n}(\mathbb{A})^+$-invariant probability measures.

Assume without loss of generality that $\mu_i {k^i}^{-1} \to_{i\to\infty} \mu$. By passing to a subsequence we can also assume $k^i \to_{i\to\infty} k^0 \in K_{1,f} \times \cdots \times K_{n,f}$. Then we have that $\mu_i \to_{i\to\infty} \mu k_0$. Because $\mathbf{G}^{\times n}(\mathbb{A})^+$ is a normal subgroup we deduce that μk_0 is also $\mathbf{G}^{\times n}(\mathbb{A})^+$-invariant. The claim follows by pushing-forward μk_0 to X using Π. □

4. Measure rigidity

Here we present a definition of an algebraic probability measure in the S-arithmetic setting and the adelic one. The S-arithmetic definition we use is from [EL15a].

Definition 4.1. Let $\mathbf{M}$ be a linear algebraic group defined over $\mathbb{Q}$.

(1) Fix a finite set of rational places S containing ∞, and let $M < \mathbf{M}(\mathbb{Q}_S)$ be a closed finite index subgroup. Let $\Gamma < M$ be a lattice. A probability measure ν on ${}_{\Gamma}\backslash^{M}$ is *algebraic* if there are a closed unimodular algebraic subgroup $\mathbf{L} < \mathbf{M}$ defined and anisotropic over $\mathbb{Q}$, a finite index subgroup $L < \mathbf{L}(\mathbb{Q}_S)$ and some $g_S \in M$ such that ν is the probability L-Haar measure supported on $[Lg_S] \subseteq {}_{\Gamma}\backslash^{M}$.

(2) A probability measure ν on $[\mathbf{M}(\mathbb{A})]$ is an *algebraic measure* if there are a closed unimodular algebraic subgroup $\mathbf{L} < \mathbf{M}$ defined and anisotropic over $\mathbb{Q}$, an isogeny $\mathbf{L}' \to \mathbf{L}$ over $\mathbb{Q}$ and a closed subgroup of finite index $L < \operatorname{Im}[\mathbf{L}'(\mathbb{A}) \to \mathbf{L}(\mathbb{A})]$ such that ν is the probability L-Haar measure on an orbit $[Lg] \subset [\mathbf{M}(\mathbb{A})]$ for some $g \in \mathbf{G}(\mathbb{A})$.

Remark 4.2. The datum defining a fixed adelic algebraic measure is the $\mathbf{G}(\mathbb{Q})$-orbit of a tuple $(\mathbf{L}, \mathbf{L}' \to \mathbf{L}, L, Lg)$ where $\gamma \in \mathbf{G}(\mathbb{Q})$ acts by

$$\gamma.(\mathbf{L}, \mathbf{L}' \to \mathbf{L}, L, Lg) = (\operatorname{Ad}_\gamma \mathbf{L}, \mathbf{L}' \to \mathbf{L} \xrightarrow{\operatorname{Ad}_\gamma} \operatorname{Ad}_\gamma \mathbf{L}, \operatorname{Ad}_\gamma L, (\operatorname{Ad}_\gamma L)(\gamma g)).$$

Definition 4.3. Write

$$A_{p_i}^{+} \coloneqq A_{p_i} \cap \mathbf{G}(\mathbb{Q}_{p_i})^{+}$$

for $i \in \{1, 2\}$. The subgroup $A_{p_i}^{+}$ is the image in A_{p_i} of a maximal torus in $\mathbf{G}^{\mathrm{sc}}(\mathbb{Q}_{p_i})$ isogenic to A_{p_i}, hence it has finite index in A_{p_i}.

The essential ingredient in the proof of the following theorem is the joinings theorem of Einsiedler and Lindenstrauss [EL15a, Th. 1.4] and Duke's theorem for equidistribution in the absolute rank 1 case. Notice that because we assume a fixed split prime, the equidistribution in the absolute rank 1 case that we use is already covered by Linnik's method [Lin68].

THEOREM 4.4. *Let μ_i^{joint} be a sequence of self-joinings of periodic toral measures on $[(\mathbf{G} \times \mathbf{G})(\mathbb{A})]$ with discriminants $|D_i| \to_{i\to\infty} \infty$ and satisfying (♠). Let the probability measure μ be any limit point of μ_i^{joint}. Then μ is a convex combination of $(A_{p_1}^{+} \times A_{p_2}^{+})^{\Delta}$-invariant algebraic measures. Specifically, there is a Borel probability measure $\mathscr{P}$ on the space of probability measures $\mathscr{M}_1([(\mathbf{G} \times \mathbf{G})(\mathbb{A})])$ supported on the subset of algebraic measures so that*

$$\mu = \int_{\mathscr{M}_1([(\mathbf{G}\times\mathbf{G})(\mathbb{A})])} \lambda \, \mathrm{d}\mathscr{P}(\lambda).$$

Moreover, for almost all the algebraic measures λ in the support of $\mathscr{P}$, the associated $\mathbb{Q}$-group $\mathbf{L} < \mathbf{G} \times \mathbf{G}$ can be taken either to be $\mathbf{G}^{\Delta}$ or $\mathbf{G} \times \mathbf{G}$, and λ is the algebraic measure supported on $[\mathbf{L}(\mathbb{A})^{+}\xi]$ for some $\xi \in (\mathbf{G} \times \mathbf{G})(\mathbb{A})$.

Corollary 4.5. *Let λ be an algebraic measure in the support of $\mathscr{P}$ in Theorem 4.4 above. If λ is supported on $[\mathbf{G}^\Delta(\mathbb{A})^+\xi]$, then $\operatorname{ctr}(\xi)_{p_i} \in A_{p_i}$ for $i \in \{1,2\}$.*

Proof. Fix $i \in \{1,2\}$. The measure λ is $\left(A_{p_i}^+\right)^\Delta$-invariant, and its stabilizer subgroup in $(\mathbf{G}\times\mathbf{G})(\mathbb{Q}_{p_i})$ is contained in $(e,\operatorname{ctr}(\xi)_{p_i})\mathbf{G}^\Delta(\mathbb{Q}_{p_i})(e,\operatorname{ctr}(\xi)_{p_i})^{-1}$. Thus $\operatorname{ctr}(\xi)_{p_i}$ centralizes $A_{p_i}^+$ in $\mathbf{G}(\mathbb{Q}_{p_i})$. This centralizer is A_{p_i}. □

We will use the following standard result.

Lemma 4.6. *For every rational place v that splits $\mathbf{B}$, the action of $\mathbf{G}(\mathbb{Q}_v)^+$ is mixing for the Haar measure on $[\mathbf{G}(\mathbb{A})^+\omega_0]$ for any $\omega_0 \in \mathbf{G}(\mathbb{A})$.*

Proof. The Haar measure on $[\mathbf{G}(\mathbb{A})^+\omega_0]$ is invariant under $\omega_0^{-1}\mathbf{G}(\mathbb{A})^+\omega_0 = \mathbf{G}(\mathbb{A})^+$. Considering the $\mathbf{G}(\mathbb{A})^+$-equivariant isomorphism of measure spaces

$$[\mathbf{G}(\mathbb{A})^+\omega_0] = {}_{\mathbf{G}(\mathbb{Q})}\backslash^{\mathbf{G}(\mathbb{A})^+\omega_0} \simeq {}_{\mathrm{Z}\,\mathbf{G}^{\mathrm{sc}}(\mathbb{A})\cdot\mathbf{G}^{\mathrm{sc}}(\mathbb{Q})}\backslash^{\mathbf{G}^{\mathrm{sc}}(\mathbb{A})},$$

it is enough to show that the action of $\mathbf{G}^{\mathrm{sc}}(\mathbb{Q}_v)$ on $[\mathbf{G}^{\mathrm{sc}}(\mathbb{A})] \coloneqq {}_{\mathbf{G}^{\mathrm{sc}}(\mathbb{Q})}\backslash^{\mathbf{G}^{\mathrm{sc}}(\mathbb{A})}$ is mixing. This result will follow from Howe-Moore [HM79, Th. 5.2] if we show that the only finite dimensional $\mathbf{G}^{\mathrm{sc}}(\mathbb{Q}_v)$-sub-representation in

$$L^2\left([\mathbf{G}^{\mathrm{sc}}(\mathbb{A})], \mathrm{m}_{\mathbf{G}^{\mathrm{sc}}}\right)$$

is the space of constant functions.

By strong approximation for simply-connected absolutely almost simple groups, the group $\mathbf{G}^{\mathrm{sc}}(\mathbb{Q}_v)$ acts minimally on $[\mathbf{G}^{\mathrm{sc}}(\mathbb{A})]$; i.e., all the $\mathbf{G}^{\mathrm{sc}}(\mathbb{Q}_v)$-orbits are topologically dense. Let

$$V < L^2\left([\mathbf{G}^{\mathrm{sc}}(\mathbb{A})], \mathrm{m}_{\mathbf{G}^{\mathrm{sc}}}\right)$$

be a (closed) finite-dimensional sub-$\mathbf{G}^{\mathrm{sc}}(\mathbb{Q}_v)$-representation. The minimality of the $\mathbf{G}^{\mathrm{sc}}(\mathbb{Q}_v)$ action implies that the whole $\mathbf{G}^{\mathrm{sc}}(\mathbb{A})$-orbit of any $\mathbf{G}^{\mathrm{sc}}(\mathbb{Q}_v)$-smooth vector in V is contained in V. The smooth vectors are dense in any closed sub-representation $V < L^2\left([\mathbf{G}^{\mathrm{sc}}(\mathbb{A})], \mathrm{m}_{\mathbf{G}^{\mathrm{sc}}}\right)$, hence V must be $\mathbf{G}^{\mathrm{sc}}(\mathbb{A})$-invariant. Because $\mathbf{G}^{\mathrm{sc}}$ is simply-connected, it has no non-trivial residual spectrum and the only finite dimensional $\mathbf{G}^{\mathrm{sc}}(\mathbb{A})$-sub-representation is $\mathbb{C}\cdot 1$. □

To apply [EL15a, Th. 1.4] to μ we need first to decompose it to ergodic measures on locally homogeneous spaces saturated by unipotents in the sense of [EL15a, Def. 1.1].

The measure μ is $\left(A_{p_1}^+ \times A_{p_2}^+\right)^\Delta$-invariant, and we write

$$\mu = \int_{\mathscr{M}_1([(\mathbf{G}\times\mathbf{G})(\mathbb{A})])} \lambda \, \mathrm{d}\mathscr{P}(\lambda) \tag{12}$$

for the ergodic decomposition of μ with respect to $\left(A_{p_1}^+ \times A_{p_2}^+\right)^\Delta$.

Lemma 4.7. *For $\mathscr{P}$-almost every λ, there is $\omega = (\omega_1, \omega_2) \in \mathbf{G}(\mathbb{A}) \times \mathbf{G}(\mathbb{A})$ such that λ is an $\left(A_{p_1}^+ \times A_{p_2}^+\right)^\Delta$-invariant measure supported on the homogeneous set $[(\mathbf{G} \times \mathbf{G})(\mathbb{A})^+\omega]$. Moreover, its projection to each coordinate is the $\mathbf{G}(\mathbb{A})^+$-Haar measure on $[\mathbf{G}(\mathbb{A})^+\omega_i]$.*

Proof. The $\left(A_{p_1}^+ \times A_{p_2}^+\right)^\Delta$-invariance of λ is built into the definition of an ergodic decomposition. The measures λ in the support of $\mathscr{P}$ are conditional measures of μ on the σ-algebra of $\left(A_{p_1}^+ \times A_{p_2}^+\right)^\Delta$-invariant Borel sets. Denote by $\mathscr{B}^+$ the σ-algebra of Borel $\mathbf{G}(\mathbb{A})^+$-invariant sets in $[\mathbf{G}(\mathbb{A})]$. The σ-algebra of $\left(A_{p_1}^+ \times A_{p_2}^+\right)^\Delta$-invariant sets in $[(\mathbf{G} \times \mathbf{G})(\mathbb{A})]$ contains $\mathscr{B}^+ \times \mathscr{B}^+$ — the σ-algebra of $\mathbf{G}(\mathbb{A})^+ \times \mathbf{G}(\mathbb{A})^+$-invariant Borel sets. Hence $\mathscr{P}$-almost every λ is supported on an atom of $\mathscr{B}^+ \times \mathscr{B}^+$.

The σ-algebra $\mathscr{B}^+$ corresponds to the factor map

$$\mathbf{G}(\mathbb{Q})\backslash^{\mathbf{G}(\mathbb{A})} \to \mathbf{G}(\mathbb{Q})\backslash^{\mathbf{G}(\mathbb{A})}/_{\mathbf{G}(\mathbb{A})^+} \simeq \mathrm{Nrd}(\mathbf{B}^\times(\mathbb{Q}))\backslash^{\mathrm{Nrd}(\mathbf{B}^\times(\mathbb{A}))}/_{\mathbb{A}^{\times 2}},$$

and its atoms are the fibers of this map, which are of the form $[\omega_0\mathbf{G}(\mathbb{A})^+] = [\mathbf{G}(\mathbb{A})^+\omega_0]$ for some $\omega_0 \in \mathbf{G}(\mathbb{A})$. The atoms of $\mathscr{B}^+ \times \mathscr{B}^+$ are then of the form $[(\mathbf{G} \times \mathbf{G})(\mathbb{A})^+\omega]$ for $\omega = (\omega_1, \omega_2) \in \mathbf{G}(\mathbb{A}) \times \mathbf{G}(\mathbb{A})$. This proves the first part of the lemma.

Because of Duke's theorem, proved by Linnik under the assumption of a fixed split prime, μ projects in each coordinate to a $\mathbf{G}(\mathbb{A})^+$-invariant measure on $[\mathbf{G}(\mathbb{A})]$. We deduce that

$$\pi_{i*}\mu = \int \pi_{i*}\lambda \, \mathrm{d}\mathscr{P}(\lambda)$$

is $\mathbf{G}(\mathbb{A})^+$-invariant for $i = 1, 2$. All the $\mathbf{G}(\mathbb{A})^+$-invariant and ergodic measures on $[\mathbf{G}(\mathbb{A})]$ are $\mathbf{G}(\mathbb{A})^+$-Haar measures on $\mathscr{B}^+$ atoms of the form $[\mathbf{G}(\mathbb{A})^+\omega_0]$. By Lemma 4.6 these $\mathbf{G}(\mathbb{A})^+$-Haar measures are $A_{p_1}^+ \times A_{p_2}^+$-ergodic. Hence a $\mathbf{G}(\mathbb{A})^+$-ergodic decomposition of $\pi_{i*}\mu$ is also an $A_{p_1}^+ \times A_{p_2}^+$-ergodic decomposition. By uniqueness of the ergodic decomposition it follows that for $\mathscr{P}$-almost every λ, the projections $\pi_{i*}\lambda$ are $\mathbf{G}(\mathbb{A})^+$-Haar measures on a $\mathscr{B}^+$-atom. □

We now fix a measure λ satisfying the conclusions of Lemma 4.7 and apply [EL15a, Th. 1.4] to it. To do that we need first to pass to an S-arithmetic setting.

Lemma 4.8. *Let λ satisfy the conclusions of Lemma 4.7. In particular, λ is supported on $[\mathbf{G}(\mathbb{A})^+\omega_1 \times \mathbf{G}(\mathbb{A})^+\omega_2]$. Fix S as a finite set of rational places such that*

(1) $\infty, p_1, p_2 \in S$;
(2) $\mathbf{G}$ *has class number* 1 *with respect to* K^S;
(3) $\omega_1, \omega_2 \in \mathbf{G}(\mathbb{Q}_S) \times K^S$.

Denote by $\jmath^S$ the canonical projection

$$\jmath^S\colon\ [(\mathbf{G}\times\mathbf{G})(\mathbb{A})]\to Y_S\times Y_S \coloneqq {}_{\Gamma_S}\backslash^{\mathbf{G}(\mathbb{Q}_S)}\times {}_{\Gamma_S}\backslash^{\mathbf{G}(\mathbb{Q}_S)},$$

where $\Gamma_S \coloneqq \mathbf{G}(\mathbb{Q})\cap K^S$.

Then the measure $\jmath^S_*\lambda$ is an algebraic measure on $Y_S\times Y_S$ supported on $[L_S g_S]$ for some $g_S\in(\mathbf{G}\times\mathbf{G})(\mathbb{Q}_S)$, where $L_S<\mathbf{L}(\mathbb{Q}_S)\cap(\mathbf{G}\times\mathbf{G})(\mathbb{Q}_S)^+$ is a finite index subgroup and $\mathbf{L}<\mathbf{G}$ a closed algebraic subgroup. The group $\mathbf{L}$ is isogenous either to $\mathbf{G}$ or to $\mathbf{G}\times\mathbf{G}$ and projects onto $\mathbf{G}$ in both coordinates.

Proof. Write $\omega_{i,S}\in\mathbf{G}(\mathbb{Q}_S)$ for the S-coordinates of ω_i, $i=1,2$. Denote $\omega_S=(\omega_{1,S},\omega_{2,S})$. Set $\Gamma_S^+\coloneqq\Gamma_S\cap\mathbf{G}(\mathbb{Q}_S)^+$ (this is a lattice in $\mathbf{G}(\mathbb{Q}_S)^+$), and denote $Y_S^+\coloneqq {}_{\Gamma_S^+}\backslash^{\mathbf{G}(\mathbb{Q}_S)^+}$.

Strong approximation for $\mathbf{G}^{\mathrm{sc}}$ implies that $\jmath^S_*\lambda$ is supported on a *single* orbit $[\mathbf{G}(\mathbb{Q}_S)^+\omega_1\times\mathbf{G}(\mathbb{Q}_S)^+\omega_2]$ and its projection to each coordinate is a $\mathbf{G}(\mathbb{Q}_S)^+$-Haar measure. By applying a right translation by ω_S^{-1}, we consider the measure $\jmath^S_*\lambda$ as an $\omega_S^{-1}\left(A^+_{p_1}\times A^+_{p_2}\right)^{\Delta}\omega_S$-invariant and ergodic measure on $Y_S^+\times Y_S^+$ whose projection to each coordinate is the Haar measure on Y_S^+.

The space Y_S^+ is saturated by unipotents because the group

$$\mathbf{G}(\mathbb{Q}_{p_1})^+\simeq\mathbf{PSL}_2(\mathbb{Q}_{p_1})$$

is generated by unipotents and acts ergodically on Y_S^+ by Lemma 4.6. The group $A^+_{p_1}\times A^+_{p_2}$ is a compact extension of a class-$\mathscr{A}'$ group in the sense of [EL15a, Def. 1.3], so $\jmath^S_*\lambda$ is an ergodic invariant measure for a class-$\mathscr{A}'$ group of rank 2. Theorem 1.4 of [EL15a] now applies, and $\jmath^S_*\lambda$ is an algebraic measure on $[L_S g_S]$ for some $g_S\in\mathbf{G}(\mathbb{Q}_S)$ and L_S of finite index in $\mathbf{L}(\mathbb{Q}_S)\cap\mathbf{G}(\mathbb{Q}_S)^+$ for some reductive group $\mathbf{L}<\mathbf{G}$ projecting onto $\mathbf{G}$ in both coordinates. By [EL15a, Lemma 7.4], $\mathbf{L}$ is either isogenous to $\mathbf{G}$ or to $\mathbf{G}\times\mathbf{G}$. □

Lemma 4.9. *In the setting of Lemma 4.8 the group $\mathbf{L}$ is either isomorphic to $\mathbf{G}$ or to $\mathbf{G}\times\mathbf{G}$.*

Proof. Consider the center $\mathrm{Z}\,\mathbf{L}$. It projects in both coordinates to the center of $\mathbf{G}$, which is trivial as $\mathbf{G}$ is of adjoint type. Hence $\mathrm{Z}\,\mathbf{L}$ projects to the trivial group in each coordinate so it is trivial. The group $\mathbf{L}$ is adjoint and the claim follows as both $\mathbf{G}$ and $\mathbf{G}\times\mathbf{G}$ are adjoint. □

If $\mathbf{L}\simeq\mathbf{G}\times\mathbf{G}$, then the inclusion $\mathbf{L}<\mathbf{G}\times\mathbf{G}$ is an equality. The following treats the case that $\mathbf{L}\simeq\mathbf{G}$.

Lemma 4.10. *If $\mathbf{L}<\mathbf{G}\times\mathbf{G}$ is isomorphic to $\mathbf{G}$ and projects onto $\mathbf{G}$ in both coordinates, then $\mathbf{L}$ is conjugate to $\mathbf{G}^{\Delta}$ over $\mathbb{Q}$.*

Proof. Consider the projections $\pi_1, \pi_2 \colon \mathbf{G} \times \mathbf{G} \to \mathbf{G}$ restricted to $\mathbf{L}$. Because $\mathbf{L}$ projects onto $\mathbf{G}$ in both coordinates and $\mathbf{L}$ is simple with trivial center, the kernel of these projections is trivial. In particular, both projections are isomorphism of algebraic groups and $\pi_2\restriction_{\mathbf{L}} \circ \pi_1\restriction_{\mathbf{L}}^{-1}$ is an automorphism of $\mathbf{G}$. As all automorphisms of $\mathbf{G}$ are inner, we see that $\pi_2\restriction_{\mathbf{L}} \circ \pi_1\restriction_{\mathbf{L}}^{-1} = \mathrm{Ad}_g$ for some $g \in \mathbf{G}(\mathbb{Q})$. Thus $(e, g^{-1})\mathbf{L}(e, g) < \mathbf{G}^{\Delta}$, and because $\mathbf{L}$ and $\mathbf{G}^{\Delta}$ have the same dimension and $\mathbf{G}^{\Delta}$ is connected, we conclude $(e, g^{-1})\mathbf{L}(e, g) = \mathbf{G}^{\Delta}$ □

Lemma 4.11. *In Lemma 4.8 we can take $L_S = \mathbf{L}(\mathbb{Q}_S)^+$.*

Proof. Lemmas 4.9 and 4.10 imply that the reduced norm map

$$\mathrm{Nrd} \colon (\mathbf{G} \times \mathbf{G})(\mathbb{Q}_S) \to \mathbb{Q}_S^{\times} / {\mathbb{Q}_S^{\times}}^2$$

restricts to the corresponding reduced norm on $\mathbf{L}(\mathbb{Q}_S)$. In particular, $\mathbf{L}(\mathbb{Q}_S) \cap (\mathbf{G} \times \mathbf{G})(\mathbb{Q}_S)^+ = \mathbf{L}(\mathbb{Q}_S)^+$. The group $\mathbf{L}(\mathbb{Q}_{p_1})^+$ is a product of at most two copies of the abstractly simple [Dic01] group $\mathbf{PSL}_2(\mathbb{Q}_{p_1})$. In particular, $\mathbf{L}(\mathbb{Q}_{p_1})^+$ has no proper subgroups of finite index, hence $L_S \cap \mathbf{L}(\mathbb{Q}_{p_1}) = \mathbf{L}(\mathbb{Q}_{p_1})^+$.

Strong approximation implies that $\mathbf{L}(\mathbb{Q}_{p_1})^+$ acts minimally on the closed set $[\mathbf{L}(\mathbb{Q}_S)^+]$. Because $[L_S]$ is contained in $[\mathbf{L}(\mathbb{Q}_S)^+]$ and it is $\mathbf{L}(\mathbb{Q}_{p_1})^+$-invariant we see that $[L_S] = [\mathbf{L}(\mathbb{Q}_S)^+]$. The $\mathbf{L}(\mathbb{Q}_S)^+$-Haar measure on $[\mathbf{L}(\mathbb{Q}_S)^+]$ is L_S-invariant. Uniqueness of the Haar measure on a homogeneous space implies that the $\mathbf{L}(\mathbb{Q}_S)^+$ and L_S Haar measures on $[L_S] = [\mathbf{L}(\mathbb{Q}_S)^+]$ coincide.

The conclusion of the lemma follows by translating by g_S. □

Proof of Theorem 4.4. We patch the result of the previous lemmata into an adelic statement. Fix a countable well-ordered direct system of finite sets of rational places $\{S\}$ exhausting all the places of $\mathbb{Q}$ and such that all S satisfy the conditions in Lemma 4.8. By excluding a countable union of $\mathscr{P}$-measure zero sets we see that $\mathscr{P}$-almost every λ in (12) projects onto an algebraic measure satisfying the conclusions of Lemma 4.8 for each S in the direct system.

Let $S \subset S'$ be a pair of sets places in the direct system. The algebraic measure $\jmath_*^{S'}\lambda$ supported on $[\mathbf{L}_{S'}(\mathbb{Q}_{S'})g_{S'}]$ projects to the algebraic measure $\jmath_*^{S}\lambda$ supported on $[\mathbf{L}_S(\mathbb{Q}_S)g_S]$. The factor map from $Y_{S'} \times Y_{S'}$ to $Y_S \times Y_S$ is the division by the compact subgroup $\prod_{v \in S' \setminus S} K_v$, thus

$$\Gamma_{S'}\mathbf{L}_S(\mathbb{Q}_S)^+ g_S \prod_{v \in S' \setminus S} K_v = \Gamma_{S'}\mathbf{L}_{S'}(\mathbb{Q}_{S'})^+ g_{S'} \prod_{v \in S' \setminus S} K_v$$

and $\gamma g_{S'} = l g_S k_S$ for some $\gamma \in \Gamma_{S'} = (\mathbf{G} \times \mathbf{G})(\mathbb{Q}) \cap K^{S'} \times K^{S'}$, $l \in \mathbf{L}_S(\mathbb{Q}_S)^+$ and $k_S \in \prod_{v \in S} 1 \times \prod_{v \in S' \setminus S} K_v$. Write $g_{S'} = (g_{S'}^0, g_{S'}^1)$ where $g_{S'}^0$ are the $\mathbb{Q}_S$ coordinates of $g_{S'}$ and $g_{S'}^1$ are the coordinates in $S' \setminus S$. Then $\gamma g_{S'}^0 = l g_S$.

The $g_{S'}^{-1}\mathbf{L}_{S'}(\mathbb{Q}_{S'})^+ g_{S'}$-periodic measure supported on $[\mathbf{L}_{S'}(\mathbb{Q}_{S'})^+ g_{S'}]$ projects to a finite collection of ${g_{S'}^0}^{-1}\mathbf{L}_{S'}(\mathbb{Q}_S)^+ g_{S'}^0$ periodic measures. The

$\left(A^+_{p_1} \times A^+_{p_2}\right)^\Delta$-ergodicity of $\jmath^S_* \lambda$ implies that this collection is a single periodic measure.

The measure $\jmath^S_*\lambda$ is also the $g_S^{-1}\mathbf{L}_S(\mathbb{Q}_S)^+ g_S$-periodic measure with support $[\mathbf{L}_S(\mathbb{Q}_S)^+ g_S]$. The groups stabilizing the measure are equal and so are their normal subgroups of trivial reduced norm. Hence

$$g^0_{S'}{}^{-1}\mathbf{L}_{S'}(\mathbb{Q}_S)^+ g^0_{S'} = g_S^{-1}\mathbf{L}_S(\mathbb{Q}_S)^+ g_S.$$

Because $\gamma g^0_{S'} = l g_S$, this implies that $\mathrm{Ad}_\gamma \mathbf{L}_{S'}(\mathbb{Q}_{S'})^+ = \mathbf{L}_S(\mathbb{Q}_S)^+$.

Because the image of the simply connected cover is Zariski dense over an infinite field, we see that $\mathrm{Ad}_\gamma \mathbf{L}_{S'} = \mathbf{L}_S$. We are free to replace the datum $(\mathbf{L}_{S'}, \mathbf{L}_{S'}(\mathbb{Q}_{S'})^+, g_{S'})$ by the datum $(\mathrm{Ad}_\gamma \mathbf{L}_{S'}, \mathrm{Ad}_\gamma \mathbf{L}_{S'}(\mathbb{Q}_{S'})^+ \gamma g_{S'})$ without changing the corresponding algebraic measure on $Y_{S'} \times Y_{S'}$. Using the new datum the algebraic measure $\jmath^{S'}_* \lambda$ is supported on $[\mathbf{L}_S(\mathbb{Q}_{S'})^+ \gamma g_{S'}] = [\mathbf{L}_S(\mathbb{Q}_{S'})^+ g_S k_S]$ with $k_S \in \prod_{v\in S} 1 \times \prod_{v\in S'\setminus S} K_v$.

Let S_0 be the minimal set of places in the well-ordered direct system. We make the choices of datum for the measures $\jmath^S_*\lambda$ consistently across the ordered system; i.e., for all S, the measure $\jmath^S_*\lambda$ it the algebraic measure supported on $[\mathbf{L}_{S_0}(\mathbb{Q}_S) g_{S_0} k_S]$ and k_S has non-trivial entries only in coordinates not contained in sets of places preceding S. We can then extend k_S trivially to an element of $K < \mathbf{G}(\mathbb{A}_f)$ and define $k = \prod_S k_S \in K$.

The adelic algebraic measure supported on $[\mathbf{L}(\mathbb{A})^+ g_{S_0} k]$ projects under $\jmath^S$ to the measure $\jmath^S_*\lambda$ for all S in the direct system. As the set of compactly supported functions on $[(\mathbf{G}\times\mathbf{G})(\mathbb{A})]$ that are $K^S \times K^S$-smooth for some S is dense in the space of compactly supported continuous functions, we conclude that λ coincides with the algebraic measure supported on $[\mathbf{L}(\mathbb{A})^+ g_{S_0} k]$.

Lemma 4.10 now implies that we can take $\mathbf{L}$ either to be $\mathbf{G}\times\mathbf{G}$ or $\mathbf{G}^\Delta$. □

5. Coordinates for quaternion algebras

The usual representation in coordinates of a split quaternion algebra $\mathbf{B}(\mathbb{Q}_v)$ over a local field $\mathbb{Q}_v$ is the matrix algebra $\mathbf{M}_{2\times 2}(\mathbb{Q}_v)$. When $v \neq \infty$ and we have a fixed maximal order we can choose our coordinates so that this order is $\mathbf{M}_{2\times 2}(\mathbb{Z}_v)$. The downside of this “fixed coordinates” representation is that it is difficult in the general case to write down the intersection of a varying torus $\widetilde{\mathbf{T}}(\mathbb{Q}_v)$ with the maximal order or to describe coordinatewise the action of the torus by conjugation.

Another commonly used coordinate representation of a quaternion algebra, split or not, over $\mathbb{Q}_v$ is a coordinate system adjusted to the varying torus $\widetilde{\mathbf{T}}(\mathbb{Q}_v)$. In this description $\mathbf{B}(\mathbb{Q}_v)$ is identified with the subset of a fixed point of a twisted Galois action on $\mathbf{M}_{2\times 2}(E_v)$, where $E_v/\mathbb{Q}_v$ is a quadratic étale-algebra splitting $\widetilde{\mathbf{T}}$. In this description $\widetilde{\mathbf{T}}(\mathbb{Q}_v)$ corresponds simply to the diagonal torus. The price we pay is that the coordinatewise expression for a fixed maximal order is varying.

In this section, we present the expression for the maximal order in a coordinate system varying with the torus. The results of this section are well known yet because they are of utilitarian nature, it is difficult to point to an exhaustive reference.

Definition 5.1. Define $\mathbf{M}_{2\times 2}=\operatorname{Spec}\mathbb{Q}\left[x_{i,j}\mid 1\leq i,j\leq 2\right]$ to be the 4-dimensional affine space of 2×2 matrices. We define $\mathbf{GL}_2$ as a space of invertible 2×2 matrices using to the closed immersion $\mathbf{GL}_2\hookrightarrow\mathbf{M}_{2\times 2}\times\mathbb{A}_1$

$$\mathbb{Q}[\mathbf{GL}_2]=\mathbb{Q}\left[x_{i,j},\det{}^{-1}\mid 1\leq i,j\leq 2\right]\Big/\left\langle (x_{1,1}x_{2,2}-x_{1,2}x_{2,1})\det{}^{-1}=1\right\rangle .$$

The torus $\widetilde{\mathbf{T}}\simeq\operatorname{Res}_{\mathbb{Q}}^{\mathrm{E}}\mathbb{G}_{\mathrm{m}}$ is split over E, hence $\mathbf{B}_E\simeq\mathbf{M}_{2\times 2,E}$. We now describe the Galois action on $\mathbf{M}_{2\times 2,E}$ corresponding to the $\mathbb{Q}$-form $\mathbf{B}$.

Definition 5.2.

(1) Let $\widetilde{\mathbf{A}}$ be the torus of diagonal matrices in $\mathbf{GL}_2$. We fix an isomorphism of algebras defined over E

$$\mathbf{B}_E\to\mathbf{M}_{2\times 2,E},$$

which sends $\widetilde{\mathbf{T}}_E$ to $\widetilde{\mathbf{A}}_E$. Using this isomorphism we identity henceforth

$$\begin{aligned}&\mathbf{B}_E=\mathbf{M}_{2\times 2,E},\\&\mathbf{B}_E^{\times}=\mathbf{GL}_{2,E},\ \widetilde{\mathbf{T}}_E=\widetilde{\mathbf{A}}_E,\\&\mathbf{G}_E=\mathbf{PGL}_{2,E},\ \mathbf{T}_E=\mathbf{A}_E.\end{aligned}$$

(2) Denote $\mathfrak{G}:-\operatorname{Gal}(E/\mathbb{Q})$ and let σ be the non-trivial element of $\mathfrak{G}$. We consider two actions of $\mathfrak{G}$ on $\mathbf{M}_{2\times 2,E}$ that restrict to actions on $\mathbf{GL}_{2,E}$. The naive action is the one induced by considering $\mathbf{M}_{2\times 2,E}$ as base change of $\mathbf{M}_{2\times 2}$. This action acts on the coordinates by

$$x_{i,j}\mapsto {}^{\sigma}x_{i,j},\qquad\qquad 1\leq i,j\leq 2.$$

(3) The twisted action corresponds to viewing $\mathbf{M}_{2\times 2,E}$ as base change of $\mathbf{B}$. As $\mathbf{B}$ is an inner-form of $\mathbf{M}_{2\times 2}$ this actions differs from the naive one by conjugation by some $\theta\in\mathbf{PGL}_2(E)$, i.e.,

$$x_{i,j}\mapsto\theta\,{}^{\sigma}x_{i,j}\theta^{-1},\qquad\qquad 1\leq i,j\leq 2.$$

The following is very well known.

Proposition 5.3. *The element θ has a representative of the form*

$$\theta = \begin{pmatrix} 0 & \epsilon \\ 1 & 0 \end{pmatrix},$$

where $\epsilon \in \mathbb{Q}^\times$.

Moreover, in this way any $\epsilon \in \mathbb{Q}^\times$ defines an inner-form of $\mathbf{M}_{2\times 2}$ that is split over E. The inner-forms corresponding to ϵ_1, ϵ_2 are isomorphic over $\mathbb{Q}$ if and only if $\epsilon_2 \in \epsilon_1 \operatorname{Nrd} E^\times$. This establishes a bijection between (*inner-*)*forms of $\mathbf{GL}_2$ split over E and ${}^{\mathbb{Q}^\times}/_{\operatorname{Nr} E^\times}$.*

Proof. The torus $\widetilde{\mathbf{A}}_E \simeq \widetilde{\mathbf{T}}_E$ is stable under the twisted Galois action because $\widetilde{\mathbf{T}}$ is defined over $\mathbb{Q}$; thus $\theta \in \mathrm{N}_{\mathbf{PGL}_2}(\widetilde{\mathbf{A}})(E)$. Because $\widetilde{\mathbf{T}}$ is not split, the twisted Galois action is non-trivial on $\widetilde{\mathbf{A}}_E$ and we can write a representative for θ of the required form with $\epsilon \in E^\times$.

Because σ is an involution, we see that ${}^\sigma\theta = \theta^{-1}$, which is equivalent to $\epsilon \in \mathbb{Q}$. Isomorphic forms correspond to coboundarous Galois actions. A coboundary that stabilizes $\widetilde{\mathbf{A}}_E \simeq \widetilde{\mathbf{T}}_E$ is of the form $\theta \mapsto {}^\sigma\upsilon^{-1}\theta\upsilon$, where $\upsilon \in \mathrm{N}_{\mathbf{PGL}_2}(\widetilde{\mathbf{A}})(E)$. This amounts to multiplying ϵ by a norm. □

Remark 5.4. Even for the case $\mathbf{B} = \mathbf{M}_{2\times 2}$ the twisted Galois action differs from the naive one. In this case σ acts by conjugating the matrix elements, interchanging the two diagonal entries and interchanging the two anti-diagonal ones. This differs from the naive one also because it identifies the diagonal torus with $\widetilde{\mathbf{T}}_E$. In particular, the Galois fixed points in $\widetilde{\mathbf{A}}(E)$ are $\widetilde{\mathbf{T}}(\mathbb{Q})$ and *not* $\widetilde{\mathbf{A}}(\mathbb{Q})$.

Proposition 5.5. *The subset $\mathbf{B}(\mathbb{Q}) \subset \mathbf{M}_{2\times 2}(E)$ can be written as*

$$\mathbf{B}(\mathbb{Q}) = \left\{ \begin{pmatrix} a & \epsilon b \\ {}^\sigma b & {}^\sigma a \end{pmatrix} \,\middle|\, a, b \in E \right\}.$$

Proof. By Galois descent for quasi-projective varieties over perfect fields, the fixed points of the Galois actions are exactly the points defined over the base field.

The proposition now follows directly by examining the fixed points of the twisted Galois action. □

5.1. *Coordinates over local fields.* For any place v of $\mathbb{Q}$, let $E_v = \prod_{w|v} E_w$. The group $\mathfrak{G}$ acts on the étale-algebra E_v either as a Galois group of a field extension if v is not split in E or by switching the coordinates if v splits. In both cases the fixed points are $\mathbb{Q}_v$ where in the split case $\mathbb{Q}_v$ is embedded diagonally in E_v. The base change of the isomorphism $\mathbf{B} \to \mathbf{M}_{2\times 2,E}$ to E_v is an isomorphism

$$\mathbf{B}_{E_v} \to \mathbf{M}_{2\times 2,E_v}. \tag{13}$$

The twisted action of $\mathfrak{G}$ extends by the base-change construction to an action on $\mathbf{M}_{2\times 2,E_v}$. This action coincides with the action of $\mathfrak{G}$ on $\mathbf{M}_{2\times 2,E_v}$ induced by the action of the Galois group $\mathrm{Gal}(E_v/\mathbb{Q}_v)$.

Proposition 5.6. *The subset* $\mathbf{B}(\mathbb{Q}_v)$ *can be written as the following set in* $\mathbf{M}_{2\times 2}(E_v)$:

$$\mathbf{B}(\mathbb{Q}_v) = \left\{ \begin{pmatrix} \alpha & \epsilon\beta \\ {}^{\sigma}\beta & {}^{\sigma}\alpha \end{pmatrix} \,\middle|\, \alpha, \beta \in E_v \right\}.$$

Moreover, the elements of $\mathbf{B}(\mathbb{Q}) \subset \mathbf{B}(\mathbb{Q}_v)$ *are exactly the matrices for which* $\alpha, \beta \in E$.

Proof. The matrix θ is a $\mathbb{Q}$-point of $\mathbf{PGL}_2$ and hence also a $\mathbb{Q}_v$-point and a E_v-point. In case v splits in E, the matrix θ sits diagonally in $\mathbf{M}_{2\times 2,E_v} \simeq \mathbf{M}_{2\times 2,\mathbb{Q}_v} \times \mathbf{M}_{2\times 2,\mathbb{Q}_v}$. Because the Galois action of $\mathfrak{G}$ on $\mathbf{M}_{2\times 2,E_v}$ coincides with the base-change action, it is also given by the naive action composed with conjugation by θ.

The first part of the proposition follows once more by computing the fixed points of a Galois action on a quasi-projective varieties.

The statement about points in $\mathbf{B}(\mathbb{Q})$ follows from Proposition 5.5 and the universal property of base change. □

5.2. *The different ideal.* We review some basic properties about the different ideal of a quadratic order.

Definition 5.7. For $v \neq \infty$, define the inverse different ideal of $\Lambda_v \subset \mathbf{E}(\mathbb{Q}_v) = E_v$ by

$$\widehat{\Lambda_v} \coloneqq \{a \in E_v \mid \mathrm{Tr}(a\Lambda_v) \subseteq \mathbb{Z}_v\}.$$

Define the different ideal by

$$\mathfrak{D}(\Lambda_v) \coloneqq \left(\Lambda_v \colon \widehat{\Lambda_v}\right) = \left\{a \in \Lambda_v \mid a\widehat{\Lambda_v} \subseteq \Lambda_v\right\}.$$

Lemma 5.8. *Let* $v \neq \infty$. *The different ideal* $\mathfrak{D}(\Lambda_v)$ *is principal invertible, and its generator* $\mathscr{D}_v \in \Lambda_v$ *satisfies*

$$\mathrm{Nr}\, \mathscr{D}_v = D_v.$$

Remark 5.9. The generator $\mathscr{D}_v$ is well defined only up to multiplication by a unit of Λ_v.

Proof. Notice that the maximal order $\mathbb{O}_{E_v}$ is a product of discrete valuation rings and hence a principal ideal ring. The proof proceeds in the same manner as for an order in a quadratic number field. □

5.3. *Local maximal orders in coordinates.* Fix v as a place of $\mathbb{Q}$. In this section we describe in terms of matrices the elements of the maximal order $g_v \mathbb{O}_v g_v^{-1} < \mathbf{B}(\mathbb{Q}_v)$. The description depends upon whether v splits $\mathbf{B}$ or not.

5.3.1. *Split case.* If $\mathbf{B}(\mathbb{Q}_v)$ is split, then $\mathbf{B}(\mathbb{Q}_v)$ is a matrix algebra and $\epsilon = {}^{\sigma}\!f f$ for some $f \in E_v^\times$.

Because $\mathbf{B}(\mathbb{Q}_v)$ is split, it is isomorphic to a rank-2 matrix algebra. This statement can be strengthened so that the action of the étale-algebra $\mathbf{E}(\mathbb{Q}_v) \subset \mathbf{B}(\mathbb{Q}_v)$ on the vector space coincides with multiplication in the étale-algebra.

Lemma 5.10. *Consider E_v as a 2-dimensional $\mathbb{Q}_v$-vector space. If $\mathbf{B}(\mathbb{Q}_v)$ is split, then there is an isomorphism of $\mathbb{Q}_v$-algebras $\mathbf{B}(\mathbb{Q}_v) \simeq \operatorname{End}_{\mathbb{Q}_v}(E_v)$ such that elements of $\mathbf{E}(\mathbb{Q}_v) \simeq E_v$ act by multiplication on the étale-algebra E_v. Moreover, there is an isomorphism of $\mathbb{Q}_v$ vector space $\mathbf{B}(\mathbb{Q}_v) \simeq E_v \oplus E_v$ so that the action of $\mathbf{B}(\mathbb{Q}_v)$ on E_v satisfies*

$$\forall a \in E_v \colon (\alpha, \beta).a = \alpha \cdot a + \beta \cdot {}^{\sigma}a.$$

Proof. Using Proposition 5.6 we can write $\mathbf{B}(\mathbb{Q}_v) \simeq E_v \oplus E_v$ in the following way:

$$(\alpha, \beta) \mapsto \begin{pmatrix} \alpha & 0 \\ 0 & {}^{\sigma}\alpha \end{pmatrix} + \begin{pmatrix} 0 & \epsilon \cdot \beta / {}^{\sigma}\!f \\ {}^{\sigma}\beta / f & 0 \end{pmatrix} = \begin{pmatrix} \alpha & 0 \\ 0 & {}^{\sigma}\alpha \end{pmatrix} + \begin{pmatrix} 0 & \beta \cdot f \\ {}^{\sigma}\beta / f & 0 \end{pmatrix}. \tag{14}$$

Let $\mathbf{B}(E_v) = \mathbf{M}_{2\times 2}(E_v)$ act on $E_v \times E_v$ in the usual way on the left. We embed $E_v \hookrightarrow E_v \times E_v$ by

$$a \mapsto \begin{pmatrix} f \cdot a \\ {}^{\sigma}a \end{pmatrix},$$

and consider the action of $\mathbf{B}(\mathbb{Q}_v) \subset \mathbf{M}_{2\times 2}(E_v)$ on $\operatorname{Im}(E_v \hookrightarrow E_v \times E_v)$.

The subspace E_v in $\mathbf{B}(\mathbb{Q}_v)$ corresponding to the first coordinate in (14) acts by multiplication $\alpha.a = \alpha a$, and the subspace corresponding to the second coordinate in (14) acts by $\beta.a = \beta \cdot {}^{\sigma}a$.

Thus $\mathbf{B}(\mathbb{Q}_v)$ stabilizes $\operatorname{Im}(E_v \hookrightarrow E_v \times E_v)$ and acts faithfully on it. By comparing dimensions over $\mathbb{Q}_v$ we see that this actions is an isomorphism of algebras $\mathbf{B}(\mathbb{Q}_v) \simeq \operatorname{End}_{\mathbb{Q}_v}(E_v)$. Because the subalgebra $\mathbf{E}(\mathbb{Q}_v)$ is equal to the first coordinate in (14), it acts by ring multiplication as required. □

Lemma 5.11. *Let $v \neq \infty$. If $\mathbf{B}(\mathbb{Q}_v)$ is split, then in terms of the representation in Proposition 5.6,*

$$\operatorname{End}_{\mathbb{Z}_v}(\Lambda_v) \simeq \left\{ \begin{pmatrix} \alpha & \beta f \\ {}^{\sigma}\beta / f & {}^{\sigma}\alpha \end{pmatrix} \,\middle|\, \alpha \in \widehat{\Lambda_v}, \beta - {}^{\sigma}\alpha \in \Lambda_v \right\}. \tag{15}$$

Proof. Because $\mathbf{E}(\mathbb{Q}_v)$ acts on E_v by ring multiplication, any $l \in \Lambda_v \subset \mathbf{E}(\mathbb{Q}_v)$ belongs to $\operatorname{End}_{\mathbb{Z}_v}(\Lambda_v)$. Thus $x \cdot l \in \operatorname{End}_{\mathbb{Z}_v}(\Lambda_v)$ for any $x \in \operatorname{End}_{\mathbb{Z}_v}(\Lambda_v)$ and $l \in \Lambda_v \subset \mathbf{E}(\mathbb{Q}_v)$.

Because the ring $\operatorname{End}_{\mathbb{Z}_v}(\Lambda_v)$ is a maximal order in $\mathbf{B}(\mathbb{Q}_v)$, each element in it is integral. Thus for any $x \in \operatorname{End}_{\mathbb{Z}_v}(\Lambda_v)$,

$$\forall l \in \Lambda_v \subset \mathbf{E}(\mathbb{Q}_v) \colon \operatorname{Trd}(x \cdot l) \in \mathbb{Z}_v. \tag{16}$$

Writing x above as $x = (\alpha, \beta)$ using (14), equation (16) amounts to the statement that $\alpha \in \widehat{\Lambda_v}$.

An element $x = (\alpha, \beta)$ belongs to $\operatorname{End}_{\mathbb{Z}_v}(\Lambda_v)$ if and only if

$$\forall l \in \Lambda_v \colon \Lambda_v \ni \alpha l + \beta {}^{\sigma}l = \operatorname{Tr}(\alpha l) + (\beta - {}^{\sigma}\alpha){}^{\sigma}l,$$

which can be seen by Lemma 2.3 to be equivalent to $\beta - {}^{\sigma}\alpha \in \Lambda_v$. This proves that the endomorphism ring is contained in the right-hand side of (15). The reverse inclusion follows by checking directly that each matrix in the right-hand side of (15) preserves Λ_v. □

Proposition 5.12. *If $v \neq \infty$, then there is some $\tau_v \in E_v^{\times}$ such that*

$$g_v \mathbb{O}_v g_v^{-1} = \left\{ \begin{pmatrix} \alpha & \beta\tau_v \\ {}^{\sigma}\beta/\tau_v & {}^{\sigma}\alpha \end{pmatrix} \middle| \alpha \in \widehat{\Lambda_v}, \beta - {}^{\sigma}\alpha \in \Lambda_v \right\}.$$

Remark 5.13. The condition $\beta - {}^{\sigma}\alpha \in \Lambda_v$ can be rewritten in the equivalent more symmetric form $\alpha + \beta \in \Lambda_v$.

Proof. Maximal $\mathbb{Z}_v$-orders in matrix algebras are endomorphism rings of $\mathbb{Z}_v$-lattices; cf. [Rei75]. Because of the isomorphism from Lemma 5.10, we know that there is a $\mathbb{Z}_v$-lattice $\mathfrak{L} \subset E_v$ of full rank such that $g_v \mathbb{O}_v g_v^{-1} = \operatorname{End}_{\mathbb{Z}_v}(\mathfrak{L})$ and

$$\Lambda_v = \{a \in E_v \mid a\mathfrak{L} \subset \mathfrak{L}\}.$$

In other words, $\mathfrak{L}$ is a proper fractional ideal of Λ_v.

The ring Λ_v is monogenic by the same argument as for orders in quadratic number rings, so [ELMV09, proof of Prop. 2.1] applies and $\mathfrak{L} = l \cdot \Lambda_v$ is an invertible principle fractional ideal with some $l \in E_v^{\times}$. The element $l \in \mathbf{E}(\mathbb{Q}_v) \subset \mathbf{B}(\mathbb{Q}_v)$ sends Λ_v to $\mathfrak{L}$, hence

$$g_v \mathbb{O}_v g_v^{-1} = \operatorname{End}_{\mathbb{Z}_v}(\mathfrak{L}) = l \cdot \operatorname{End}_{\mathbb{Z}_v}(\Lambda_v) \cdot l^{-1}.$$

The proposition follows from Lemma 5.11 by setting $\tau_v = \frac{l}{{}^{\sigma}l} f$. □

Proposition 5.14. *The element $\tau_v \in E_v^{\times}$ from Proposition 5.12 above belongs to $\Lambda_v^{\times}$ for almost all v.*

Proof. The proof follows from the fact that any two $\mathbb{Z}$-lattices of full rank in a $\mathbb{Q}$-vector space are equivalent at almost all v. The order $\mathbb{O}$ is a full rank $\mathbb{Z}$-lattice in the vector space $\mathbf{B}(\mathbb{Q})$. The following subset of $\mathbf{B}(\mathbb{Q})$,

$$\left\{ \begin{pmatrix} a & \epsilon b \\ {}^{\sigma}b & {}^{\sigma}a \end{pmatrix} \middle| a, b \in \mathcal{O}_E \right\},$$

is also a $\mathbb{Z}$-lattice of full rank by Proposition 5.5, and so it is locally equivalent to $\mathbb{O}$ for almost all v. The claim follows by observing that for almost all v, we have $g_v \in \mathbb{O}_v^{\times}$, $\widehat{\Lambda_v} = \Lambda_v = \mathcal{O}_{E_v}$ and $\epsilon \in \mathbb{Z}_v^{\times}$. □

Proposition 5.15. *If $v=\infty$, then*

$$\left\| g_\infty^{-1}\begin{pmatrix}\alpha & \beta f\\ {}^{\sigma}\beta/f & {}^{\sigma}\alpha\end{pmatrix} g_\infty\right\|_\infty = |\alpha|+|\beta|.$$

In particular,

$$g_\infty\widetilde{\Omega}_\infty g_\infty^{-1} = \left\{\begin{pmatrix}\alpha & \beta f\\ {}^{\sigma}\beta/f & {}^{\sigma}\alpha\end{pmatrix} \,\middle|\, \alpha,\beta\in\mathbb{C}, |\alpha|+|\beta|\le 2, |\alpha|-|\beta|\ge 1/2\right\},$$

$$g_\infty\mathbb{O}_\infty g_\infty^{-1} = \left\{\begin{pmatrix}\alpha & \beta f\\ {}^{\sigma}\beta/f & {}^{\sigma}\alpha\end{pmatrix} \,\middle|\, \alpha,\beta\in\mathbb{C}, |\alpha|+|\beta|\le 1\right\}.$$

Proof. From the definition of $\|\bullet\|_\infty$ in Section 2.2.1 we know $\|\operatorname{Ad} g_\infty^{-1}\bullet\|_\infty$ is an operator norm on $\mathbf{B}(\mathbb{R})$ induced from some inner-product norm on $E_\infty \simeq \mathbb{C}\simeq\mathbb{R}^2$ when we let $\mathbf{B}(\mathbb{R})$ act on E_∞ by $\mathbb{R}$-linear endomorphism. This action is explicitly described in Lemma 5.10.

Fix one of the two possible isomorphism $E_\infty\simeq\mathbb{C}$, and identify the two fields. Let $|\bullet|_\infty$ be an inner-product norm on $\mathbb{C}$ corresponding to $\|\bullet\|_\infty$. The inner-product norm corresponding to $\|\operatorname{Ad} g_\infty^{-1}\bullet\|_\infty$ is $g_\infty.|\bullet|_\infty := v\mapsto |g_\infty^{-1}v|_\infty$. Because of the choices made in Section 2.2.1 and (♠), the homothety class $\mathbb{R}_{>0}|\bullet|_\infty$ is invariant under the action of $K_\infty = g_\infty^{-1}\mathbf{T}(\mathbb{R})g_\infty$. Hence the homothety class of $g_\infty.|\bullet|_\infty$ is invariant under $\mathbf{T}(\mathbb{R})$.

We deduce that in the representation of Proposition 5.6 and Lemma 5.10 the homothety class of $g_\infty.|\bullet|_\infty$ is invariant under the action $\mathbf{E}^\times(\mathbb{R})<\mathbf{B}^\times(\mathbb{R})$, which acts on $\mathbb{C}$ by multiplication. This implies that $g_\infty.|\bullet|_\infty$ is in the homothety class of the standard norm on $\mathbb{C}$ defined by $|x|^2 = x\cdot{}^{\sigma}x$.

Using this explicit description of $g_\infty.|\bullet|_\infty$ it is simple to compute the associated operator norm in the coordinates of Lemma 5.10, which turns out to be the norm

$$\|(\alpha,\beta)\| = |\alpha|+|\beta| = \sqrt{(\Re\alpha)^2+(\Im\alpha)^2}+\sqrt{(\Re\beta)^2+(\Im\beta)^2}.$$

The description of $g_\infty\Omega_\infty g_\infty^{-1}$ is now a simple calculation using the definition in Section 2.4.5. □

5.3.2. *Ramified case.* Assume now that $\mathbf{B}(\mathbb{Q}_v)$ is ramified. There is a unique maximal order that includes all integral elements. In particular, we have $\mathbb{O}_v = g_v^{-1}\mathbb{O}_v g_v$ and $\Lambda_v = \mathcal{O}_{E_v}$. Moreover, there is an easy criterion to check whether an element is integral using its norm (cf. [Rei75, Chapter 3]):

$$\begin{aligned}\mathbb{O}_v &= \{x\in\mathbf{B}(\mathbb{Q}_v)\mid \operatorname{Nrd}(x)\in\mathbb{Z}_v\}\\ &= \left\{\begin{pmatrix}\alpha & \epsilon\beta\\ {}^{\sigma}\beta & {}^{\sigma}\alpha\end{pmatrix},\ \alpha,\beta\in E_v \,\middle|\, |\operatorname{Nr}(\alpha)-\epsilon\operatorname{Nr}(\beta)|_v\le 1\right\},\end{aligned}$$

where the second equality uses Proposition 5.6. The following is a simple statement about p-adic numbers

Lemma 5.16. *Let π be a uniformizer of the maximal ideal in $\mathbb{Z}_v$. Two numbers $a, b \in \mathbb{Q}_v$ satisfy $|a-b|_v \leq 1$ if and only if one of the following two options happens*:

(1) $a, b \in \mathbb{Z}_v$,

(2) $|a|_v = |b|_v = |\pi|_v^{-n}$ *for some* $n \in \mathbb{Z}$ *and* $a/b \equiv 1 \mod \pi^n \mathbb{Z}_v$.

Proof. The proof follows from elementary properties of p-adic fields. □

Proposition 5.17. *Assume that v is inert in E and $\mathbf{B}(\mathbb{Q}_v)$ is ramified. Let π be a uniformizer of the maximal ideal in $\mathbb{Z}_v$, and write* $\operatorname{ord}_v \epsilon = 2k+1$ *for $k \in \mathbb{Z}$. Then*

$$g_v \mathbb{O}_v g_v^{-1} = \left\{ \begin{pmatrix} \alpha & \pi^{k+1}\beta \\ \pi^{-k}\, {}^{\sigma}\beta & {}^{\sigma}\alpha \end{pmatrix} \middle| \alpha, \beta \in \Lambda_v, \right\}.$$

Notice that in this case $\widehat{\Lambda_v} = \Lambda_v$ because Λ_v is the maximal order and $E_v/\mathbb{Q}_v$ is unramified.

Proof. If v is inert in E, then $E_v/\mathbb{Q}_v$ is an unramified quadratic extension. Hence $\operatorname{ord}_v \operatorname{Nr}(\alpha)$ is even for any $\alpha \in E_v^\times$. Moreover, as the norm map of an unramified extension of local fields is surjective when restricted to the unit groups, we deduce that $\operatorname{Nr}(E_v^\times) = \pi^{2\mathbb{Z}} \cdot \mathbb{Z}_v^\times$. Because B is ramified, ϵ is not an $E_v^\times$-norm in $\mathbb{Q}_v^\times$ and $\operatorname{ord}_v \epsilon = 2k+1$ for $k \in \mathbb{Z}$.

Let $\alpha, \beta' \in E_v$ such that $|\operatorname{Nr}(\alpha) - \epsilon \operatorname{Nr}(\beta')|_v \leq 1$. The second option in Lemma 5.16 can never happen for $a = \operatorname{Nr}(\alpha), b = \epsilon \operatorname{Nr}(\beta')$ because $\operatorname{ord}_v \operatorname{Nr}(\alpha)$ is even and $\operatorname{ord}_v (\epsilon \operatorname{Nr}(\beta'))$ is odd.

We conclude that necessarily $\operatorname{Nr}(\alpha') \in \mathbb{Z}_v$ and $\epsilon \operatorname{Nr}(\beta') \in \mathbb{Z}_v$. This implies that $\alpha \in \mathcal{O}_{E_v} = \Lambda_v$ and $\beta' \in \pi^{-k}\Lambda_v$. □

Proposition 5.18. *Assume both $E_v/\mathbb{Q}_v$ and $\mathbf{B}(\mathbb{Q}_v)$ are ramified. Let $\Pi \in \mathcal{O}_{E_v}$ be a uniformizer. Then there exists $u \in \mathbb{Z}_v^\times$ and $k \in \mathbb{Z}$ such that*

$$g_v \mathbb{O}_v g_v^{-1} \subseteq \left\{ \begin{pmatrix} \alpha & \Pi^k u \beta \\ \Pi^{-k}\, {}^{\sigma}\beta & {}^{\sigma}\alpha \end{pmatrix} \middle| \alpha, \beta \in \widehat{\Lambda_v} \right\}.$$

Proof. Let $\pi = \operatorname{Nr} \Pi$ be a uniformizer for $\mathbb{Z}_v$. Because $E_v/\mathbb{Q}_v$ is totally ramified, by local class field theory there exists an index 2 subgroup $U_{E_v} < \mathbb{Z}_v^\times$ such that $\operatorname{Nr}(E_v^\times) = \pi^{\mathbb{Z}} U_{E_v}$. Hence $\epsilon = \pi^k u$ for some $k \in \mathbb{Z}$ and $u \in \mathbb{Z}_v^\times \setminus U_{E_v}$.

Let $x \in g_v \mathbb{O}_v g_v^{-1}$, and write $x = \left(\begin{smallmatrix} \alpha & \epsilon\beta' \\ {}^{\sigma}\beta' & {}^{\sigma}\alpha \end{smallmatrix}\right)$ for some $\alpha, \beta' \in E_v$. Set also $\beta' = {}^{\sigma}\Pi^{-k}\beta$ where $\beta \in E_v$. Then $\epsilon\beta' = \Pi^k u \beta$.

Any element $l \in \Lambda_v$ belongs to $g_v \mathbb{O}_v g_v^{-1}$, so $x \cdot l \in g_v \mathbb{O}_v g_v^{-1}$ and $x \cdot l$ is integral. This implies

$$\forall l \in \Lambda_v \colon \operatorname{Tr}(\alpha \cdot l) = \operatorname{Trd}(x \cdot l) \in \mathbb{Z}_v,$$

and thus $\alpha \in \widehat{\Lambda_v}$.

If the first option in Lemma 5.16 holds, then $\epsilon\,\mathrm{Nr}(\beta') = u\,\mathrm{Nr}(\beta) \in \mathbb{Z}_v$ and necessarily $\beta \in \mathcal{O}_{E_v} = \Lambda_v \subseteq \widehat{\Lambda_v}$. The second case is relevant only when $\alpha \in \widehat{\Lambda_v} \setminus \Lambda_v$ and then $|\epsilon\,\mathrm{Nr}(\beta')|_v = |\,\mathrm{Nr}(\beta)|_v = |\,\mathrm{Nr}(\alpha)|_v$. As $\widehat{\Lambda_v}$ is a principal ideal we deduce that β must also belong to $\widehat{\Lambda_v}$. □

5.3.3. *General case.* We summarize the results of this section in a form useful to us.

Proposition 5.19. *For any finite rational place v, there is some $\tau_v \in E_v^\times$ such that*

$$g_v \mathbb{O}_v g_v^{-1} \subseteq \left\{ \begin{pmatrix} \alpha & \beta\upsilon_v\tau_v \\ {}^\sigma\beta/\tau_v & {}^\sigma\alpha \end{pmatrix} \,\middle|\, \alpha, \beta \in \widehat{\Lambda_v} \right\}.$$

If $\mathbf{B}$ is split at v, then $\upsilon_v = 1$. If $\mathbf{B}$ is ramified and E is inert at v, then υ_v is a uniformizer in $\mathbb{Z}_v$, and if both $\mathbf{B}$ and E are ramified at v, then υ_v is a unit that is not an $E_v^\times$ norm. Moreover, $\tau_v \in \Lambda_v^\times$ for almost all v and $\tau_v = 1$ if B is ramified at v.

Proof. Propostiion 5.19 is an immediate corollary of Propositions 5.12, 5.17, 5.18 and 5.14. □

5.4. *Good integral representatives.* In this section we will discuss how to find good representatives in $\mathbb{O}_v \subset \mathbf{B}(\mathbb{Q}_v)$ of elements in $\mathbf{G}(\mathbb{Q}_v)$ using the Cartan decomposition. The notion of a good representative generalizes the idea of writing a rational number as an integer fraction in lowest terms.

Definition 5.20.

(1) For a finite rational place v where $\mathbf{G}$ splits, let $\mathscr{B}_v$ be the the Bruhat-Tits building of $\mathbf{G}(\mathbb{Q}_v)$. If $\mathbf{G}$ is ramified at $v \neq \infty$, let $\mathscr{B}_v$ the connected graph with two vertices corresponding to ${}^{\mathbf{G}(\mathbb{Q}_v)}/_{K_v}$. Denote by d the geodesic distance function on the graph $\mathscr{B}_v$ normalized so that the length of each edge is 1.

(2) If $\mathbf{B}(\mathbb{R})$ is split, set $\mathscr{B}_\infty = {}^{\mathbf{G}(\mathbb{R})}/_{\mathrm{N}_{\mathbf{G}(\mathbb{R})}(K_\infty)}$. This manifold is the upper half-plane that we equip with the standard hyperbolic distance function d. If $\mathbf{B}(\mathbb{R})$ is ramified let $\mathscr{B}_\infty$ be a single point with the trivial metric.

(3) For each place v, let x_0 be the point in $\mathscr{B}_v$ stabilized by K_v. Let q be the residue characteristic for $v \neq \infty$ and $q = e$ for $v = \infty$. Define a continuous function $\mathfrak{d}_v \colon \mathbf{G}(\mathbb{Q}_v) \to \mathbb{R}_{>0}$ by

$$\mathfrak{d}_v(x_v) \coloneqq q^{d(x_0, x_v . x_0)}.$$

(4) Define the continuous function $\mathfrak{d}_f \colon \mathbf{G}(\mathbb{A}_f) \to \mathbb{N}$ by

$$\mathfrak{d}_f\left((x_v)_{v\neq\infty}\right) = \prod_{v\neq\infty} \mathfrak{d}_v(x_v).$$

Proposition 5.21. *Let v be a rational place and $x_v \in \mathbf{G}(\mathbb{Q}_v)$. For any $h \in \Omega_v x_v \Omega_v \subset \mathbf{G}(\mathbb{Q}_v)$, there is $r \in \mathbb{O}_v \subset \mathbf{B}(\mathbb{Q}_v)$ such that $h = \mathbf{Z}(\mathbb{Q}_v) r$ and*

$$|\operatorname{Nrd}(r)|_v \, \mathfrak{d}_v(x_v) = 1 \text{ if } v \neq \infty,$$
$$2^{-8} \leq |\operatorname{Nrd}(r)|_\infty \, \mathfrak{d}_v(x_v) \leq 1 \text{ if } v = \infty.$$

Moreover, for $v \neq \infty$, this representative is optimal in the following way. If $h \in \Omega_v x_v \Omega_v$, then it has no representative in $\mathbb{O}_v$ whose reduced norm has smaller valuation than r above.

Proof. In the split case this follows from the Cartan decomposition, the equality $K_v \Omega_v = \Omega_v K_v = \Omega_v$ and (7) for $v = \infty$. In the finite ramified case this is a consequence of the fact that the ramification index of $\mathbf{B}(\mathbb{Q}_v)$ is 2; i.e., the value group of $\mathbb{Q}_v$ is an index 2 subgroup of the value group of the division algebra $\mathbf{B}(\mathbb{Q}_v)$. In the infinite ramified case, $\Omega_v = \mathbf{G}(\mathbb{Q}_v)$ and the statement is trivial.

The last statement about the optimality of the representative for $v \neq \infty$ follows from the mutual disjointness of the K_v double cosets in the Cartan decomposition. □

Definition 5.22. Let $B \subseteq G(\mathbb{Q}_{p_1})$ be an identity neighborhood and $n \in \mathbb{N} \cup \{0\}$. Let $\lambda \colon \mathbb{Q}_{p_1}^\times \to A_{p_1}$ be a cocharacter spanning $X_\bullet(A_{p_1})$. Set $a = \lambda(p_1) \in A_{p_1}$. We use the following notation for the symmetric homogeneous B-Bowen ball for the a-action:

$$B^{(-n,n)} \coloneqq \bigcap_{k=-n}^{n} a^k B a^{-k}.$$

Notice that the definition of $B^{(-n,n)}$ does not depends on the choice of λ.

We similarly define

$$\mathbb{O}_{p_1}^{(-n,n)} \coloneqq \bigcap_{k=-n}^{n} a^k \mathbb{O}_{p_1} a^{-k} \subset \mathbf{B}(\mathbb{Q}_{p_1}).$$

Proposition 5.23. *Fix $\xi_{p_1} \in A_{p_1}$ and $n \geq 0$. For any*

$$h \in K_{p_1}^{(-n,n)} \xi_{p_1} K_{p_1}^{(-n,n)},$$

there is $r \in \mathbb{O}_{p_1}^{(-n,n)}$ with $h = \mathbf{Z}(\mathbb{Q}_{p_1}) r$ and $|\operatorname{Nrd}(r)|_{p_1} \mathfrak{d}_{p_1}(\xi_{p_1}) = 1$.

Proof. Because ξ_{p_1} centralizes A_{p_1},

$$h \in K_{p_1}^{(-n,n)} \xi_{p_1} K_{p_1}^{(-n,n)} \subseteq \bigcap_{k=-n}^{n} a^k K_{p_1} \xi_{p_1} K_{p_1} a^{-k}.$$

Applying Lemma 5.21 for each set in the intersection above we conclude that for every $-n \leq k \leq n$, there is a representative $r_k \in a^k \mathbb{O}_{p_1} a^{-k}$ of h such that $|\operatorname{Nrd} r_k|_v \, \mathfrak{d}_{p_1}(\xi_{p_1}) = 1$.

All the representatives r_k for different values of k are in the same $\mathbf{Z}(\mathbb{Q}_{p_1})$-orbit and their reduced norms have the same absolute value. Thus they are all in the same orbit of $\mathbb{Z}_{p_1}^{\times} < \mathbb{Q}_{p_1}^{\times} = \mathbf{Z}(\mathbb{Q}_{p_1})$. Multiplying each r_k by an appropriate element of $\mathbb{Z}_{p_1}^{\times} < a^k\mathbb{O}_{p_1}a^{-k}$, for all k, we can make all the representatives r_k equal to each other without affecting the valuation of their reduced norm and so that they still satisfy $r_k \in a^k\mathbb{O}_{p_1}a^{-k}$. This common representative satisfies the conditions of the claim. □

6. The double quotient $\mathbf{G}^{\Delta}\backslash\mathbf{G}\times\mathbf{G}/\mathbf{T}^{\Delta}$

When studying the relative position of a homogeneous Hecke set and a joint homogeneous toral set we need to understand the double quotient ${}_{\mathbf{G}^{\Delta}}\backslash^{\mathbf{G}\times\mathbf{G}}/_{\mathbf{T}^{\Delta}}$. This can be achieved using GIT and Galois descent.

6.1. *The* GIT *double quotient.*

Definition 6.1.

(1) Denote $\mathbf{M} \coloneqq \mathbf{G}\times\mathbf{T}$. The linear algebraic $\mathbf{M}$ group is defined over $\mathbb{Q}$. We consider an action of the group $\mathbf{M}$ on the affine variety $\mathbf{G}\times\mathbf{G}$ by letting the $\mathbf{G}$ coordinate act by diagonal multiplication on the left and by letting the $\mathbf{T}$ coordinate to act by diagonal multiplication by the inverse on the right. For geometric points, the action is
$$(l,t).(g_1,g_2) = (lg_1t^{-1}, lg_2t^{-1}).$$

(2) The universal categorical quotient for the action of the linear reductive group $\mathbf{M}$ on the affine variety $\mathbf{G}\times\mathbf{G}$ is representable by the following affine variety defined over $\mathbb{Q}$ [MFK94, Th. 1.1]:
$$\mathbf{W} \coloneqq {}_{\mathbf{G}^{\Delta}}\backslash^{\mathbf{G}\times\mathbf{G}}/_{\mathbf{T}^{\Delta}} \coloneqq \operatorname{Spec}{}^{\mathbf{G}^{\Delta}}\mathbb{Q}\left[\mathbf{G}\times\mathbf{G}\right]^{\mathbf{T}^{\Delta}},$$
where ${}^{\mathbf{G}^{\Delta}}\mathbb{Q}[\mathbf{G}\times\mathbf{G}]^{\mathbf{T}^{\Delta}}$ is the ring of regular functions of $\mathbf{G}\times\mathbf{G}$ invariant under the $\mathbf{M}$ action.

(3) For any $\gamma\in(\mathbf{G}\times\mathbf{G})(\mathbb{Q})$, define $\mathbf{M}_\gamma$ to be the stabilizer of γ. It is a linear algebraic group defined over $\mathbb{Q}$.

(4) Denote by $\pi_{\mathbf{W}}\colon \mathbf{G}\times\mathbf{G}\to\mathbf{W}$ the $\mathbf{M}$-equivariant projection map.

Definition 6.2. Let $w_{\mathbf{T}}\in \mathrm{N}_{\mathbf{G}}\,\mathbf{T}(\mathbb{Q})$ be a rational representative of the non-trivial class of the Weyl group of $\mathbf{T}$, i.e., $w_{\mathbf{T}}\not\in\mathbf{T}(\mathbb{Q})$. Such a representative always exists, for example because of Proposition 5.5. Although, the element $w_{\mathbf{T}}$ is not uniquely defined, the variety $w_{\mathbf{T}}\mathbf{T}$ is a well-defined closed sub-variety of $\mathbf{G}$ defined over $\mathbb{Q}$.

PROPOSITION 6.3. *Let $\gamma=(\gamma_1,\gamma_2)\in(\mathbf{G}\times\mathbf{G})(\mathbb{Q})$ be a rational point.*

(1) *The $\mathbf{M}$-orbit of γ is Zariski closed.*

(2) *Recall that* $\mathrm{ctr}(\gamma)=\gamma_1^{-1}\gamma_2$. *The stabilizer* $\mathbf{M}_\gamma$ *is trivial if* $\mathrm{ctr}(\gamma)\notin \mathrm{N}_{\mathbf{G}}\,\mathbf{T}(\mathbb{Q})$. *If* $\mathrm{ctr}(\gamma)\in \mathrm{N}_{\mathbf{G}}\,\mathbf{T}(\mathbb{Q})$, *then*

$$\mathbf{M}_\gamma \simeq \mathrm{Z}_{\mathbf{T}}(\mathrm{ctr}(\gamma)) = \begin{cases}\mathbf{T} & \mathrm{ctr}(\gamma)\equiv 1 \mod \mathbf{T}(\mathbb{Q}),\\ \mathbf{T}[2] & \mathrm{ctr}(\gamma)\not\equiv 1 \mod \mathbf{T}(\mathbb{Q}).\end{cases}$$

The isomorphism above is $t\mapsto(\gamma_1 t\gamma_1^{-1},t)$. *Moreover, the diagonalizable abelian affine group* $\mathbf{T}[2]$ *is isomorphic to* μ_2 *over* $\mathbb{Q}$.

(3) *If* $\mathrm{ctr}(\gamma)\notin\ w_{\mathbf{T}}\mathbf{T}(\mathbb{Q})$, *then the following set is a singleton*:

$$\ker\left[H^1(\mathbb{Q},\mathbf{M}_\gamma)\to H^1(\mathbb{Q},\mathbf{M})\right].$$

(4) *If* $\mathrm{ctr}(\gamma)\notin w_{\mathbf{T}}\mathbf{T}(\mathbb{Q})$, *then* $\pi_{\mathbf{W}}^{-1}(\gamma)(\mathbb{Q})$ *is a single* $\mathbf{M}(\mathbb{Q})$*-orbit.*

Proof. Part (1). Assume the orbit of γ is not Zariski closed. By [MFK94, Cor. 1.2] the map $\pi_{\mathbf{W}}$ separates $\mathbf{M}$-invariant closed subsets. Because $\mathbf{G}\times\mathbf{G}$ is Noetherian, we deduce that the fiber $\pi_{\mathbf{W}}^{-1}(\pi_{\mathbf{W}}(\gamma))$ contains a unique minimal non-empty Zariski closed $\mathbf{M}$-invariant subset. Let $\mathbf{S}$ be the closed subvariety supported on this set. Because the map $\pi_{\mathbf{W}}$ separates invariant closed subsets, the support of $\mathbf{S}$ is contained in any non-empty invariant closed subset in the fiber.

The orbit $\mathbf{M}.\gamma$ is open in its closure, so $\overline{\mathbf{M}.\gamma}^{\mathrm{Zar}}\backslash\mathbf{M}.\gamma$ is an invariant Zariski closed subset that by our assumption is non-empty, hence $\mathbf{S}$ is contained in it. In particular, $\gamma\notin\mathbf{S}(\mathbb{Q})$.

The Zariski closure of the orbit of γ contains $\mathbf{S}$, and hence by [Kem78, Cor. 4.3] there is a one-parameter subgroup $\lambda\colon\mathbb{G}_{\mathrm{m}}\to\mathbf{M}=\mathbf{G}\times\mathbf{T}$ defined over $\mathbb{Q}$ such that $\delta=\lim_{s\to0}\lambda(s).\gamma\in\mathbf{S}(\mathbb{Q})$.

The torus $\mathbf{T}$ is anisotropic over $\mathbb{Q}$ so the image of λ lies in $\mathbf{G}$ and $\delta\in\overline{\mathbf{G}.\gamma}^{\mathrm{Zar}}(\mathbb{Q})$. But $\mathbf{G}.\gamma\simeq\mathbf{G}.e=\mathbf{G}^\Delta$, which is Zariski closed, so

$$\delta\in(\mathbf{G}.\gamma\cap\mathbf{S})(\mathbb{Q}).$$

As $\mathbf{S}$ is $\mathbf{M}$-invariant, we deduce a contradiction that $\gamma\in S(\mathbb{Q})$.

Part (2) Let $e\neq(g,t)\in\mathbf{M}_\gamma(\bar{\mathbb{Q}})<\mathbf{G}(\bar{\mathbb{Q}})\times\mathbf{T}(\bar{\mathbb{Q}})$. Then

$$\begin{aligned}(g\gamma_1 t^{-1},g\gamma_2 t^{-1})=(\gamma_1,\gamma_2)&\Longrightarrow t\,\mathrm{ctr}(\gamma)t^{-1}=\mathrm{ctr}(\gamma)\\ &\Longrightarrow \mathrm{ctr}(\gamma)\in\mathrm{N}_{\mathbf{G}(\bar{\mathbb{Q}})}(t)=\mathbf{T}(\bar{\mathbb{Q}}).\end{aligned}$$

Moreover, in this case $g=\gamma_1 t\gamma_1^{-1}$. We deduce that the stabilizer is trivial unless $\mathrm{ctr}(\gamma)\in\mathrm{N}_{\mathbf{G}}\,\mathbf{T}(\mathbb{Q})$ and it is isomorphic to $\mathrm{Z}_{\mathbf{T}}(\mathrm{ctr}(\gamma))$ otherwise with the isomorphism exactly as stated in claim (2).

If $\mathrm{ctr}(\gamma)\in\mathbf{T}(\mathbb{Q})$, then the entire torus $\mathbf{T}$ centralizers it. If $\mathrm{ctr}(\gamma)\in\mathrm{N}_{\mathbf{G}}\,\mathbf{T}(\mathbb{Q})$, then only elements of order 2 centralize it. This finishes the computation of the stabilizers.

To see that $\mathbf{T}[2]\simeq\mu_2$, we consider the dual group $\widehat{\mathbf{T}[2]}\simeq\widehat{\mathbf{T}}/\widehat{\mathbf{T}}^2$, which has two geometric points. As the Galois group $\mathrm{Gal}(E/\mathbb{Q})$ acts by inversion on $\mathbf{T}$, its action on $\widehat{\mathbf{T}}/\widehat{\mathbf{T}}^2$ is trivial. Hence this dual group is the constant $\mathbb{Z}/2\mathbb{Z}$-group scheme and its dual is μ_2.

Part (3) If the stabilizer is trivial, then the statement is obvious. Otherwise, we use the projection on the second coordinate $\mathbf{M} = \mathbf{G} \times \mathbf{T} \to \mathbf{T}$ to construct a sequence of maps

$$H^1(\mathbb{Q}, \mathbf{M}_\gamma) \to H^1(\mathbb{Q}, \mathbf{M}) \to H^1(\mathbb{Q}, \mathbf{T}). \tag{17}$$

In order to prove that $\ker\left[H^1(\mathbb{Q}, \mathbf{M}_\gamma) \to H^1(\mathbb{Q}, \mathbf{M})\right] = 1$ it is enough to show that the kernel of the composite map of (17) is trivial.

The isomorphism $\mathbf{M}_\gamma \simeq \mathrm{Z}_{\mathbf{T}}(\mathrm{ctr}(\gamma))$ is given by the inclusion map in the second coordinate, hence the composite map of (17) is exactly the map of cohomology sets $H^1(\mathbb{Q}, \mathrm{Z}_{\mathbf{T}}(\mathrm{ctr}(\gamma))) \to H^1(\mathbb{Q}, \mathbf{T})$ induced by the inclusion $\mathrm{Z}_{\mathbf{T}}(\mathrm{ctr}(\gamma)) \hookrightarrow \mathbf{T}$. This map is the identity if $\mathrm{Z}_{\mathbf{T}}(\mathrm{ctr}(\gamma)) = \mathbf{T}$ and obviously has a trivial kernel.

Part (4). Because the $\pi_{\mathbf{W}}$-fiber of any rational point contains a unique Zariski closed orbit of a rational point, we conclude that $\pi_{\mathbf{W}}$ separates $\mathbf{M}(\bar{\mathbb{Q}})$-orbits of rational points. We are left with proving that for any $\gamma \notin w_{\mathbf{T}}\mathbf{T}(\mathbb{Q})$ the orbit $\mathbf{M}(\bar{\mathbb{Q}})$ contains a unique $\mathbf{M}(\mathbb{Q})$-orbit.

The collection of $\mathbf{M}(\mathbb{Q})$-orbits in $\mathbf{M}(\bar{\mathbb{Q}}).\gamma$ is in bijection with

$$\ker\left[H^1(\mathbb{Q}, \mathbf{M}_\gamma) \to H^1(\mathbb{Q}, \mathbf{M})\right], \tag{18}$$

which is trivial by part (3) if $\mathrm{ctr}(\gamma) \notin w_{\mathbf{T}}\mathbf{T}(\mathbb{Q})$. □

The proposition above implies that the set theoretic double cosets

$$\mathbf{G}^{\Delta}(\mathbb{Q})\backslash(\mathbf{G}\times\mathbf{G})(\mathbb{Q})/\mathbf{T}^{\Delta}(\mathbb{Q})$$

are almost parametrized by the associated points in $\mathbf{W}(\mathbb{Q})$. Not all the points in $\mathbf{W}(\mathbb{Q})$ actually correspond to set theoretic double cosets of rational points of $\mathbf{G}$.

6.2. *The quotient of* $\mathbf{G}$ *by the adjoint action of* $\mathbf{T}$. Because the left action of $\mathbf{G}^\Delta$ and right action of $\mathbf{T}^\Delta$ on $\mathbf{G} \times \mathbf{G}$ commute, we have the following commutative diagram:

$$\begin{tikzcd}
\mathbf{G}\times\mathbf{G} \arrow[r, two heads] \arrow[d] & \mathbf{W} \arrow[dd] \\
\mathbf{G}^{\Delta}\backslash\mathbf{G}\times\mathbf{G} \arrow[d, "\wr"] & \\
\mathbf{G} \arrow[r, two heads] & \mathrm{Ad}\,\mathbf{T}\backslash\mathbf{G},
\end{tikzcd}$$

where ${}_{\operatorname{Ad}\mathbf{T}}\backslash^{\mathbf{G}}$ is the GIT quotient of the affine variety $\mathbf{G}$ by the adjoint action of the reductive group $\mathbf{T}$. The existence of the morphism $\mathbf{W} \to {}_{\operatorname{Ad}\mathbf{T}}\backslash^{\mathbf{G}}$ follows from the universal property of the categorical quotient $\mathbf{W}$. The composite $\mathbf{G}^{\Delta}$-invariant map $\mathbf{G} \times \mathbf{G} \to \mathbf{G}$ in the left column of the diagram is exactly the contraction map ctr.

Proposition 6.4. *The morphism* $\mathbf{W} \to {}_{\operatorname{Ad}\mathbf{T}}\backslash^{\mathbf{G}}$ *is an isomorphism.*

Proof. The morphism ${}_{\mathbf{G}^{\Delta}}\backslash^{\mathbf{G} \times \mathbf{G}} \to \mathbf{G}$ is an isomorphism. Hence the ring of regular functions on ${}_{\operatorname{Ad}\mathbf{T}}\backslash^{\mathbf{G}}$ is identified with the regular functions on ${}_{\mathbf{G}^{\Delta}}\backslash^{\mathbf{G} \times \mathbf{G}}$ that are invariant under the right action of $\mathbf{T}^{\Delta}$. This is the same as the ring of $\mathbf{M}$-invariant regular functions on $\mathbf{G} \times \mathbf{G}$ because the left action of $\mathbf{G}^{\Delta}$ commutes with the right action of $\mathbf{T}^{\Delta}$. □

Corollary 6.5. *Let* $\pi^0_{\mathbf{W}} \colon \mathbf{G} \to {}_{\operatorname{Ad}\mathbf{T}}\backslash^{\mathbf{G}} \simeq \mathbf{W}$ *be the* $\operatorname{Ad}\mathbf{T}$*-equivariant projection map. For any* $\gamma_0 \in \mathbf{G}(\mathbb{Q})$*, if* $\gamma_0 \notin w_{\mathbf{T}}\mathbf{T}(\mathbb{Q})$*, then* ${\pi^0_{\mathbf{W}}}^{-1}(\gamma_0)(\mathbb{Q})$ *is a single* $\operatorname{Ad}\mathbf{T}(\mathbb{Q})$*-orbit.*

Proof. The proof follows immediately from Proposition 6.4 and part (4) of Proposition 6.3. □

Definition 6.6. Recall that $\mathbf{G}^{\mathrm{sc}}$ is identified with the group of unit quaternions in $\mathbf{B}$. Define $\mathbf{T}^{(1)}$ to be the maximal torus defined over $\mathbb{Q}$ in $\mathbf{G}^{\mathrm{sc}}$ that maps under the isogeny $\mathbf{G}^{\mathrm{sc}} \to \mathbf{G}$ to $\mathbf{T}$. The identity $\mathbf{G}^{\mathrm{sc}} = \mathbf{B}^{(1)}$ implies that the torus $\mathbf{T}^{(1)}$ is the subgroup of unit quaternions in $\widetilde{\mathbf{T}}$.

Using the isogeny $\mathbf{T}^{(1)} \to \mathbf{T}$ we let $\mathbf{T}^{(1)}$ act on $\mathbf{G}$ through the adjoint action of $\mathbf{T}$. As $\mathbf{T}^{(1)} \to \mathbf{T}$ is surjective, we have

$${}_{\operatorname{Ad}\mathbf{T}}\backslash^{\mathbf{G}} = {}_{\operatorname{Ad}\mathbf{T}^{(1)}}\backslash^{\mathbf{G}}.$$

We let $\mathbf{T}^{(1)}$ act on $\mathbf{B}^{\times}$ by the adjoint action. Because the actions of $\operatorname{Ad}\mathbf{T}^{(1)}$ and $\mathbf{Z}$ on $\mathbf{B}^{\times}$ commute, the reductive group $\mathbf{Z}$ acts on the affine variety ${}_{\operatorname{Ad}\mathbf{T}^{(1)}}\backslash^{\mathbf{B}^{\times}}$ and the GIT quotient for this action is canonically isomorphic to ${}_{\operatorname{Ad}\mathbf{T}}\backslash^{\mathbf{G}}$. In particular, the morphism of Noetherian schemes

$${}_{\operatorname{Ad}\mathbf{T}^{(1)}}\backslash^{\mathbf{B}^{\times}} \to {}_{\operatorname{Ad}\mathbf{T}}\backslash^{\mathbf{G}} \simeq \mathbf{W}$$

is universally submersive.

6.3. *The quotient of* $\mathbf{GL}_2$ *by the adjoint action of the diagonal torus.* To describe the ring of regular function of ${}_{\operatorname{Ad}\mathbf{T}^{(1)}}\backslash^{\mathbf{B}^{\times}}$ we begin with a simpler case when $\mathbf{B} = \mathbf{M}_{2\times 2}$ is split over $\mathbb{Q}$ and $\mathbf{T}^{(1)}$ is replaced by the torus of diagonal matrices with determinant 1.

Definition 6.7. Let $\mathbf{A}^{(1)} < \mathbf{GL}_2$ be the rank-1 torus of diagonal matrices with determinant 1. Denote by $\mathbf{A}$ the maximal torus of split diagonal matrices in $\mathbf{PGL}_2$. The map $\mathbf{A}^{(1)} \to \mathbf{A}$ is surjective in terms of schemes.

Definition 6.8.

(1) We let $\mathbf{A}^{(1)}$ act on $\mathbf{M}_{2\times 2} \times \mathbb{A}_1$ by conjugating the 2×2 matrix and leaving the $\det^{-1}$ coordinate invariant. We denote this action by $\operatorname{Ad}\mathbf{A}^{(1)}$. This action is clearly equivariant with respect to the map $\mathbf{GL}_2 \hookrightarrow \mathbf{M}_{2\times 2} \times \mathbb{A}_1$.

(2) Define $\vartheta_1, \vartheta_2, \psi \in \mathbb{Q}[\mathbf{M}_{2\times 2}]$ by

$$\vartheta_1 \coloneqq x_{1,1}, \qquad \vartheta_2 \coloneqq x_{2,2}, \qquad \psi \coloneqq x_{1,2}x_{2,1}.$$

Lemma 6.9. *There is an equality of* $\mathbb{Q}$*-algebras*

$$\mathbb{Q}[\mathbf{M}_{2\times 2} \times \mathbb{A}_1]^{\operatorname{Ad}\mathbf{A}^{(1)}} = \mathbb{Q}[\vartheta_1, \vartheta_2, \psi, \det^{-1}].$$

The left-hand side is the ring of regular functions of $\mathbf{M}_{2\times 2}\times\mathbb{A}_1$ *invariant under* $\operatorname{Ad}\mathbf{A}^{(1)}$, *and the right-hand side is a polynomial algebra over* $\mathbb{Q}$.

Proof. It is easy the check that $\vartheta_1, \vartheta_2, \psi, \det^{-1}$ are $\operatorname{Ad}\mathbf{A}^{(1)}$-invariant. We need to show that these functions generate the ring of invariants and that there are no non-trivial syzygies.

Because $\mathbb{Q}[\mathbf{M}_{2\times 2} \times \mathbb{A}_1]$ is a polynomial ring and the action of $\operatorname{Ad}\mathbf{A}^{(1)}$ preserves monomials, the invariant ring is generated by monomials. Let $f \in \mathbb{Q}[\mathbf{M}_{2\times 2} \times \mathbb{A}_1]^{\operatorname{Ad}\mathbf{A}^{(1)}}$ be a monomial, and write

$$f = \left(\det^{-1}\right)^d \prod_{1\le i,j\le 2} x_{i,j}^{a_{i,j}} = \left(\det^{-1}\right)^d \vartheta_1^{a_{1,1}} \vartheta_2^{a_{2,2}} x_{1,2}^{a_{1,2}} x_{2,1}^{a_{2,1}}.$$

For f to be $\operatorname{Ad}\mathbf{A}^{(1)}$-invariant, we must have $a_{1,2} = a_{2,1}$, which implies that $f \in \mathbb{Q}[\vartheta_1, \vartheta_2, \psi, \det^{-1}]$.

A syzygy Q is a formal polynomial in the variables $\vartheta_1, \vartheta_2, \psi, \det^{-1}$ with coefficients in $\mathbb{Q}$ that vanishes as an element of $\mathbb{Q}[\mathbf{M}_{2\times 2} \times \mathbb{A}_1]^{\operatorname{Ad}\mathbf{A}^{(1)}}$. Because each variable $x_{i,j}, \det^{-1}$, $1 \le i,j \le 2$ appears in only one of the monomials ϑ_1, ϑ_2, ψ, $\det^{-1}$, we conclude that if Q vanishes as an element of $\mathbb{Q}[\vartheta_1, \vartheta_2, \psi, \det^{-1}]$, it also vanishes as an element of the free polynomial algebra $\mathbb{Q}[\mathbf{M}_{2\times 2} \times \mathbb{A}_1]$. Thus all the relations between $\vartheta_1, \vartheta_2, \psi, \det^{-1}$ are trivial. □

Proposition 6.10. *The ring of* $\operatorname{Ad}\mathbf{A}^{(1)}$*-invariant regular functions on* $\mathbf{GL}_2$ *is*

$$\mathbb{Q}[\mathbf{GL}_2]^{\operatorname{Ad}\mathbf{A}^{(1)}} = \mathbb{Q}\left[\vartheta_1, \vartheta_2, \psi, \det^{-1}\right] \Big/ \left\langle (\vartheta_1\vartheta_2 - \psi)\det^{-1} = 1 \right\rangle .$$

Proof. If a *linearly* reductive group $\mathbf{H}$ acts on two affine schemes $\mathbf{X}, \mathbf{Y}$ of finite type over a field k, then a lemma of Nagata [Nag64, Lemma 5.1.A] implies that an $\mathbf{H}$-equivariant closed immersion $\mathbf{X} \hookrightarrow \mathbf{Y}$ over k descends to a *closed immersion* of GIT quotients ${}_{\mathbf{H}}\backslash^{\mathbf{X}} \hookrightarrow {}_{\mathbf{H}}\backslash^{\mathbf{Y}}$.

The proposition follows by applying this result to the closed immersion $\mathbf{GL}_2 \hookrightarrow \mathbf{M}_{2\times 2} \times \mathbb{A}_1$ and using Lemma 6.9. □

Definition 6.11.

(1) Define the the degree of ϑ_1 and ϑ_2 to be 1, the degree of ψ to be 2 and the degree of $\det^{-1}$ to be -2. Define the degree of a monomial in $\vartheta_1, \vartheta_2, \psi, \det^{-1}$ as the sum of the degrees of the individual variables appearing in the product. The degree of a constant is 0.

(2) A polynomial in $\mathbb{Q}\left[\vartheta_1, \vartheta_2, \psi, \det^{-1}\right]$ is of zero degree if it is the sum of zero degree monomials. Denote the $\mathbb{Q}$-algebra of zero-degree elements by $\mathbb{Q}\left[\vartheta_1, \vartheta_2, \psi, \det^{-1}\right]^0$.

Corollary 6.12. *The ring of* $\operatorname{Ad}\mathbf{A}$*-invariant regular functions on* $\mathbf{PGL}_2$ *is the ring*

$$\mathbb{Q}[\mathbf{PGL}_2]^{\operatorname{Ad}\mathbf{A}} = \mathbb{Q}\left[\vartheta_1, \vartheta_2, \psi, \det^{-1}\right]^0 \Big/ \left\langle (\vartheta_1\vartheta_2 - \psi)\det^{-1} = 1 \right\rangle .$$

Moreover, this ring is generated by the functions

$$\psi\det^{-1}, \qquad \vartheta_1^2\det^{-1}, \qquad \vartheta_2^2\det^{-1}.$$

Proof. Because the actions of $\mathbf{Z}$ and $\operatorname{Ad}\mathbf{A}^{(1)}$ on $\mathbf{GL}_2$ commute, there is an isomorphism

$$\mathbf{Z}\backslash\left(\operatorname{Ad}\mathbf{A}^{(1)}\backslash\mathbf{GL}_2\right) \to \operatorname{Ad}\mathbf{A}^{(1)}\backslash\mathbf{PGL}_2 = \operatorname{Ad}\mathbf{A}\backslash\mathbf{PGL}_2.$$

The equality on the right follows from the surjectivity of $\mathbf{A}^{(1)} \to \mathbf{A}$.

This implies that the ring $\mathbb{Q}[\mathbf{PGL}_2]^{\operatorname{Ad}\mathbf{A}}$ is a the subring of elements in $\mathbb{Q}[\mathbf{GL}_2]^{\operatorname{Ad}\mathbf{A}^{(1)}}$ that are $\mathbf{Z}$-invariant. It is a direct computation to see that these are exactly the degree 0 elements and that the given functions generate this ring. □

Remark 6.13. A slightly more delicate analysis shows that

$$\mathbb{Q}[\mathbf{PGL}_2]^{\operatorname{Ad}\mathbf{A}} \simeq \mathbb{Q}[x,y,z]/\left\langle x^2 = yz \right\rangle,$$

where $x = 1+\psi\det^{-1}$, $y = \vartheta_1^2\det^{-1}$, $z = \vartheta_1^2\det^{-1}$. Geometrically, $\operatorname{Ad}\mathbf{A}\backslash\mathbf{PGL}_2$ is a circular conical surface. The singular point $x, y, z = 0$ corresponds to the $\operatorname{Ad}\mathbf{A}$ orbit of $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$.

6.4. *Descent from* $\mathbf{GL}_{2,E}$ *to* $\mathbf{B}^\times$. Recall from Section 5 that we have fixed an isomorphism of algebraic groups over E,

$$\mathbf{B}_E^\times \simeq \mathbf{GL}_{2,E},$$

such that $\widetilde{\mathbf{T}}$ is identified with $\widetilde{\mathbf{A}}$. As this isomorphism identifies the reduced norm map with the determinant map, the torus $\mathbf{T}_E^{(1)}$ is identified with $\mathbf{A}_E^{(1)}$.

Lemma 6.14. *Let $g \in \mathbf{B}^{\times}(\mathbb{Q}) \subset \mathbf{GL}_2(E)$ or $g \in \mathbf{B}^{\times}(\mathbb{Q}_v) \subset \mathbf{GL}_2(E_v)$ for some rational place v. Then*

$$ {}^{\sigma}\vartheta_1(g) = \vartheta_2(g), \qquad {}^{\sigma}\psi(g) = \psi(g), \qquad {}^{\sigma}\det{}^{-1}(g) = \det{}^{-1}(g). $$

Proof. This follows from Definition 6.8 and Propositions 5.5 and 5.6. □

Proposition 6.15. *The image of $g \in \mathbf{G}(\mathbb{Q})$ in $\mathbf{W}(\mathbb{Q})$ is determined by the values of*

$$ \vartheta_1^2 \det{}^{-1}(g), \psi \det{}^{-1}(g) \in E. $$

Proof. The universality of the GIT quotients for affine schemes implies that

$$ \left({}_{\mathrm{Ad}\,\mathbf{T}}\backslash^{\mathbf{G}}\right)_E = {}_{\mathrm{Ad}\,\mathbf{T}_E}\backslash^{\mathbf{G}_E} \simeq {}_{\mathrm{Ad}\,\mathbf{A}_E}\backslash^{\mathbf{PGL}_{2,E}} = \left({}_{\mathrm{Ad}\,\mathbf{A}}\backslash^{\mathbf{PGL}}\right)_E, \tag{19} $$

where we have the induced isomorphism $\mathbf{G}_E \simeq \mathbf{PGL}_{2,E}$ sending $\mathbf{T}_E$ to the diagonal torus $\mathbf{A}_E$.

The claim follows from (19), Lemma 6.14 and Corollary 6.12. □

7. Homogeneous Hecke sets

In this section we study elementary properties of the possible counterexamples to equidistribution arising in Section 4.

Definition 7.1. For any $\xi \in (\mathbf{G} \times \mathbf{G})(\mathbb{A})$, we define $\left[\mathbf{G}^{\Delta}(\mathbb{A})\xi\right]$ to be a homogeneous Hecke set. This set carries a $\xi^{-1}\mathbf{G}^{\Delta}(\mathbb{A})\xi$-invariant algebraic probability measure.

We also define $\left[\mathbf{G}^{\Delta}(\mathbb{A})^{+}\xi\right]$ to be a simply connected homogeneous Hecke set. This set carries a $\xi\mathbf{G}^{\Delta}(\mathbb{A})^{+}\xi$-invariant algebraic probability measure.

Remark 7.2. Fixing the subgroup $\mathbf{G}^{\Delta} < \mathbf{G} \times \mathbf{G}$, the datum defining a homogeneous Hecke set $\left[\mathbf{G}^{\Delta}(\mathbb{A})\xi\right]$ is $[\xi] \in {}_{\mathbf{G}^{\Delta}(\mathbb{A})}\backslash^{(\mathbf{G}\times\mathbf{G})(\mathbb{A})}$. Using the contraction map this can be identified with $\mathrm{ctr}(\xi) \in \mathbf{G}(\mathbb{A})$.

The datum defining a simply connected homogeneous Hecke set $\left[\mathbf{G}^{\Delta}(\mathbb{A})^{+}\xi\right]$ for $\xi = (\xi_1, \xi_2)$ is $[\xi] \in {}_{\mathbf{G}^{\Delta}(\mathbb{A})^{+}}\backslash^{(\mathbf{G}\times\mathbf{G})(\mathbb{A})}$. Using the contraction map this can be identified with $[\xi_1] \in {}^{\mathbf{G}(\mathbb{A})}/_{\mathbf{G}(\mathbb{A})^{+}}$ and $\mathrm{ctr}(\xi) \in \mathbf{G}(\mathbb{A})$.

Homogeneous Hecke sets generalize the notion of a classical Hecke correspondence. An obvious necessary condition for equidistribution is that the joint homogeneous toral sets are not trapped in a sequence of homogeneous Hecke sets with periodic measure converging to a periodic measure on some other fixed homogeneous Hecke set. The goal of this manuscript is to show that this condition is not only necessary but also sufficient, at least under the hypothesis described in the introduction. In this section we translate this condition to a condition on the twist $s \in \mathbf{T}(\mathbb{A})$.

Because these sets are somewhat more general than the classical Hecke correspondences, we need to extend some well-known results about Hecke correspondences and present them in a language adapted to the applications discussed in this manuscript.

In this section we fix a joint homogeneous toral set $\left[\mathbf{T}^{\Delta}(g, sg)\right]$ satisfying ($\spadesuit$).

7.1. *Homogeneous Hecke sets containing a joint homogeneous toral set.*

LEMMA 7.3. *All the homogeneous Hecke sets containing* $\left[\mathbf{T}^{\Delta}(\mathbb{A})(g, sg)\right]$ *are of the form* $\left[\mathbf{G}^{\Delta}(\mathbb{A})(g, t_{\mathbb{Q}}sg)\right]$ *for some* $t_{\mathbb{Q}} \in \mathbf{T}(\mathbb{Q})$.

Remark 7.4. If $\left[\mathbf{T}^{\Delta}(\mathbb{A})(g, sg)\right]$ satisfies ($\spadesuit$) and

$$\left[\mathbf{T}^{\Delta}(\mathbb{A})(g, sg)\right] \subset \left[\mathbf{G}^{\Delta}(\mathbb{A})\xi\right],$$

then

$$\operatorname{ctr}(\xi_\infty) \in K_\infty,\ \operatorname{ctr}(\xi_{p_1}) \in A_{p_1},\ \operatorname{ctr}(\xi_{p_2}) \in A_{p_2}.$$

Proof. Because $\mathrm{Z}_{(\mathbf{G}\times\mathbf{G})(\mathbb{A})}\left(\mathbf{T}^{\Delta}(\mathbb{A})\right) = \left(\mathbf{T} \times \mathbf{T}\right)(\mathbb{A})$, we have for any $t_{\mathbb{Q}} \in \mathbf{T}(\mathbb{Q})$,

$$\left[\mathbf{T}^{\Delta}(\mathbb{A})(g, sg)\right] = \left[\mathbf{T}^{\Delta}(\mathbb{A})(g, t_{\mathbb{Q}}sg)\right] \subset \left[\mathbf{G}^{\Delta}(\mathbb{A})(g, t_{\mathbb{Q}}sg)\right].$$

On the other hand, if $\left[\mathbf{T}^{\Delta}(\mathbb{A})(g, sg)\right] \subset \left[\mathbf{G}^{\Delta}(\mathbb{A})(g, \xi_0 g)\right]$ for some $\xi_0 \in \mathbf{G}(\mathbb{A})$, then a simple calculation shows that

$$\forall t \in \mathbf{T}(\mathbb{A})\colon t\xi_0 s^{-1} t^{-1} \in \mathbf{G}(\mathbb{Q}). \tag{20}$$

In particular, $\xi_0 s^{-1} \in \mathbf{G}(\mathbb{Q})$. If $\xi_0 s^{-1} \in w_{\mathbf{T}}\mathbf{T}(\mathbb{Q})$, that is, it belongs to the non-trivial class of the normalizer of $\mathbf{T}$, then we deduce that $t^2\xi_0 s^{-1} \in \mathbf{G}(\mathbb{Q})$ for all $t \in \mathbf{T}(\mathbb{A})$, which is a contradiction. Otherwise, Corollary 6.5 implies

$$\mathbf{T}(\mathbb{A}) = \mathbf{T}(\mathbb{Q}) \operatorname{Stab}_{\operatorname{Ad}\mathbf{T}(\mathbb{A})}(\xi_0 s^{-1}).$$

Considering all the options for the stabilizer in Proposition 6.3 we deduce that $\operatorname{Stab}_{\operatorname{Ad}\mathbf{T}(\mathbb{A})}(\xi_0 s^{-1}) = \mathbf{T}(\mathbb{A})$ and $\xi_0 s^{-1} \in \mathbf{T}(\mathbb{Q})$. □

7.2. *Volume of a homogeneous Hecke set.* The volume of a homogeneous Hecke set is defined similarly to the volume of a homogeneous toral set

$$\begin{aligned}\operatorname{vol}\left(\left[\mathbf{G}^{\Delta}(\mathbb{A})\xi\right]\right) &\coloneqq \mathrm{m}_{\mathbf{G}^{\Delta}}\left(\xi\Omega \times \Omega\xi^{-1}\right)^{-1} \\ &= \mathrm{m}_{\mathbf{G}}\left(\Omega \cap \operatorname{ctr}(\xi)\Omega\operatorname{ctr}(\xi)^{-1}\right)^{-1},\end{aligned}$$

where $\mathrm{m}_{\mathbf{G}} = \mathrm{m}_{\mathbf{G}^{\Delta}}$ is a covolume 1 Haar measure. The volume of a simply connected Hecke correspondence is defined analogously.

The map $\xi \mapsto \operatorname{vol}\left(\left[\mathbf{G}^{\Delta}(\mathbb{A})\xi\right]\right)$ is a continuous map from $(\mathbf{G}\times\mathbf{G})(\mathbb{A})$ to $\mathbb{R}_{>0}$ that factors through the map $\operatorname{ctr}\colon (\mathbf{G}\times\mathbf{G})(\mathbb{A}) \to \mathbf{G}(\mathbb{A})$.

7.2.1. *Volume computation using the Bruhat-Tits tree.*

Definition 7.5. Define the proper continuous function $\mathfrak{d}_{sf}\colon \mathbf{G}(\mathbb{A}_f) \to \mathbb{N}$ by

$$\mathfrak{d}_{sf}(h_f) = \prod_{\infty\neq v \text{ splits } \mathbf{B}} \mathfrak{d}_v(h_v).$$

Because $1 \leq \mathfrak{d}_v(\xi_v) \leq q_v$ for any finite v where $\mathbf{B}$ ramifies, we see that for all $h_f \in \mathbf{G}(\mathbb{A}_f)$,

$$\mathfrak{d}_{sf}(h_f) \asymp_{\mathbf{G}} \mathfrak{d}_f(h_f).$$

LEMMA 7.6. *Let* $\xi \in (\mathbf{G}\times\mathbf{G})(\mathbb{A})$ *with* $\operatorname{ctr}(\xi)_\infty \in K_\infty$. *Then*

$$\operatorname{vol}\left(\left[\mathbf{G}^{\Delta}(\mathbb{A})\xi\right]\right) \mathrm{m}_{\mathbf{G}}(\Omega) = \mathfrak{d}_{sf}(\operatorname{ctr}(\xi)_f) \prod_{p\mid \mathfrak{d}_{sf}(\operatorname{ctr}(\xi)_f)} \left(1+\frac{1}{p}\right).$$

Proof. By definition,

$$\operatorname{vol}\left(\left[\mathbf{G}^{\Delta}(\mathbb{A})\xi\right]\right) \mathrm{m}_{\mathbf{G}}(\Omega) = \frac{\mathrm{m}_{\mathbf{G}}(\Omega)}{\mathrm{m}_{\mathbf{G}}\left(\Omega\cap\operatorname{ctr}(\xi)\Omega\operatorname{ctr}(\xi)^{-1}\right)}.$$

Because Ω_∞ is $\operatorname{Ad} K_\infty$-invariant and $\operatorname{ctr}(\xi)_\infty \in K_\infty$, we can rewrite the quotient of measures as

$$\frac{\mathrm{m}_{\mathbf{G}}(\Omega)}{\mathrm{m}_{\mathbf{G}}\left(\Omega\cap\operatorname{ctr}(\xi)\Omega\operatorname{ctr}(\xi)^{-1}\right)} = \prod_{v\neq\infty}\left[K_v\colon K_v\cap\xi_v K_v {\xi_v}^{-1}\right]. \tag{21}$$

The group K_v is for almost all v the maximal compact subgroup in the restricted product definition of $\mathbf{G}(\mathbb{A})$, hence $\xi_v \in K_v$ for almost all v. If $\mathbf{B}$ is ramified over $\mathbb{Q}_v$, then $K_v < \mathbf{G}(\mathbb{Q}_v)$ is a normal subgroup Section 2.2.1. Hence $\left[K_v\colon K_v\cap\xi_v K_v {\xi_v}^{-1}\right] \neq 1$ only if $\xi_v \notin K_v$ and $\mathbf{B}(\mathbb{Q}_v)$ is split. In particular, the product (21) is finite.

When $\mathbf{G}(\mathbb{Q}_v)$ is split, i.e., $\mathbf{G}(\mathbb{Q}_v) \simeq \mathbf{PGL}_2(\mathbb{Q}_v)$, the index

$$\left[K_v\colon K_v\cap\xi_v K_v {\xi_v}^{-1}\right]$$

can be calculated using the Bruhat-Tits building $\mathscr{B}_v$ of $\mathbf{G}(\mathbb{Q}_v)$.

Our conditions in Section 2.2.1 imply that K_v is actually the whole stabilizer of x_0; in particular, it preserves types of vertices. The subgroup $\xi_v K_v {\xi_v}^{-1}$ is the stabilizer of the vertex $\xi_v.x_0$, thus $K_v\cap\xi_v K_v {\xi_v}^{-1}$ stabilizes the whole geodesic segment connecting x_0 to $\xi_v.x_0$. The cosets of $K_v\cap\xi_v K_v {\xi_v}^{-1}$ in K_v are in bijection with the vertices in the K_v-orbit of $\xi_v.x_0$. We claim that this orbit is exactly the vertices y such that $d(x_0,y)=d(x_0,\xi_v.x_0)$. It is clear that the orbit is contained in this set as the action of the group on the building is by isometries.

Fix y such that $d(x_0,y)=d(x_0,\xi_v.x_0)$. Let z_1 be the vertex adjacent to $\xi_v.x_0$ on the geodesic segment connecting x_0 and $\xi_v.x_0$, and set z_2 to be the vertex adjacent to y on the geodesic segment connecting x_0 and y. The edges $(z_1,\xi_v.x_0)$ and (z_2,y) define alcoves in the tree. Let $\mathscr{A}_1$, $\mathscr{A}_2$ be two apartments containing these alcoves and x_0.

Because the action of the type-preserving subgroup of $\mathbf{G}(\mathbb{Q}_v)$ on the building is strongly transitive,[8] there is an element of $\mathbf{G}(\mathbb{Q}_v)$ sending $\mathscr{A}_1$ to $\mathscr{A}_2$ and $(z_1,\xi_v.x_0)$ to (z_2,y). Such an element must stabilize x_0 and send $\xi_v.x_0$ to y, hence y is in the K_v-orbit of $\xi_v.x_0$ as required.

By counting vertices of distance $d(x_0,\xi_v.x_0)$ from x_0 in a q_v+1 regular tree we see that if $d(x_0,\xi_v.x_0)>0$, then

$$\left[K_v\colon K_v\cap \xi_v K_v {\xi_v}^{-1}\right]=(q_v+1)q_v^{d(x_0,\xi_v.x_0)-1}=q_v^{d(x_0,\xi_v.x_0)}\left(1+\frac{1}{q_v}\right). \qquad \square$$

7.3. *Equivalence of necessary conditions for equidistribution.*

Lemma 7.7. *Let $\tau\in\mathbf{T}(\mathbb{A})$. Then $\mathfrak{d}_f(g_f^{-1}\tau_f g_f)$ is the minimal norm of an* integral *fraction ideal in the homothety class* $\operatorname{idl}(\tau)\in {}_{\mathbb{Q}^\times}\backslash^{\mathscr{J}(\Lambda)}$.

Proof. To show the equality between these two positive integers we show that their p-parts are equal for all primes p. The representatives of τ in $\mathbf{B}(\mathbb{A})$ can be written in coordinates as

$$\tau=\left(\mathbb{Q}_v^\times\begin{pmatrix}\alpha_v & 0\\ 0 & {}^\sigma\alpha_v\end{pmatrix}\right)_v .$$

Fix $v\neq\infty$. A representative r_v of $g_v^{-1}\tau_v g_v$ is contained in Ω_v if and only if $g_v r_v g_v^{-1}$ is contained in $g_v\mathbb{O}_v g_v^{-1}$. Hence by Proposition 5.21, $\mathfrak{d}_v(g_v^{-1}\tau_v g_v)$ has the same valuation as the minimal reduced norm of a representative of τ_v contained in $g_v\mathbb{O}_v g_v^{-1}\cap\mathbf{E}(\mathbb{Q}_v)$. The latter set is by the definition of the local order equal to

$$g_v\mathbb{O}_v g_v^{-1}\cap\mathbf{E}(\mathbb{Q}_v)=\left\{\begin{pmatrix}\lambda_v & 0\\ 0 & {}^\sigma\lambda_v\end{pmatrix}\mid \lambda_v\in\Lambda_v\right\}.$$

We deduce that $\operatorname{ord}_v\mathfrak{d}_v(g_v^{-1}\tau_v g_v)=\operatorname{ord}_v\operatorname{Nr}(q_v\alpha_v)$, where $q_v\in\mathbb{Q}_v^\times$ is an element of minimal valuation satisfying $q_v\alpha_v\in\Lambda_v$.

Set $q\in\mathbb{Q}^\times$ so that $q\mathbb{Q}=\bigcap_{v\neq\infty}q_v\mathbb{Q}_v$. Then by definition, $q\widetilde{\operatorname{idl}}\left((\alpha_v)_{v\neq\infty}\right)$ is the minimal integral element in the homothety class $\operatorname{idl}(\tau)$ and its norm has the same valuation for all primes p as $\mathfrak{d}_f(g_f^{-1}\tau_f g_f)$. $\square$

[8] The action is transitive on pairs $(\mathscr{C},\mathscr{A})$ of an apartment $\mathscr{A}$ and an alcove $\mathscr{C}\subset\mathscr{A}$.

Proposition 7.8. *Let $\left\{\left[\mathbf{T}_i^{\Delta}(\mathbb{A})(g_i, s_i g_i)\right]\right\}_i$ be a sequence of joint homogeneous toral sets with associated global orders Λ_i. Denote $\mathfrak{s}_i = \operatorname{idl}(s_{i,f}) \in \mathbb{Q}^{\times}\backslash^{\mathcal{J}(\Lambda_i)}$, and let $[\mathfrak{s}_i]$ be the class of $\mathfrak{s}_i$ in $\operatorname{Pic}(\Lambda_i)$.*

The following are equivalent:

(1)
$$\min_{\left[\mathbf{T}_i^{\Delta}(\mathbb{A})(g_i,s_ig_i)\right]\subset[\mathbf{G}^{\Delta}(\mathbb{A})\xi]} \operatorname{vol}\left(\left[\mathbf{G}^{\Delta}(\mathbb{A})\xi\right]\right) \to_{i\to\infty} \infty;$$

(2)
$$\min_{\substack{\mathfrak{a}\subseteq\Lambda\\ [\mathfrak{a}]=[\mathfrak{s}_i]}} \operatorname{Nr}\mathfrak{a} \to_{i\to\infty} \infty;$$

(3) *for every compact set $B \subset \mathbf{G}(\mathbb{A})$, there is $N \in \mathbb{N}$ such that for all $i > N$,*

$$g_i^{-1}\mathbf{T}_i(\mathbb{Q})s_i g_i \cap B = \emptyset.$$

Proof. The equivalence of (2) and (3) is a consequence of Lemma 7.7 above and the fact that the function $h \mapsto \mathfrak{d}_f(h_f)$ is a continuous *proper* function from $K_\infty \times \mathbf{G}(\mathbb{A}_f)$ to $\mathbb{N}$.

The equivalence of (1) and (2) follows from Lemmata 7.3, 7.6, 7.7, the remark in Definition 7.5 and the fact that for all $N \in \mathbb{N}$,

$$1 \leq \prod_{p|N}\left(1+\frac{1}{p}\right) \ll \log\log N,$$

which follows from the prime number theorem. □

8. Geometric expansion of the pair cross-correlation

Throughout this section we fix a joint homogeneous toral set $[\mathbf{T}^{\Delta}(\mathbb{A})(g, sg)]$ with periodic measure μ, and we set a simply connected homogeneous Hecke set $[\mathbf{G}^{\Delta}(\mathbb{A})^{+}\xi]$ with periodic measure ν. We also write $\xi = (\xi_1, \xi_2)$.

8.1. *Pair cross-correlation.* We define the pair cross-correlation between the periodic measure μ and the periodic measure ν.

Definition 8.1. Let $V \subseteq [(\mathbf{G}\times\mathbf{G})(\mathbb{A})]$ be a compact identity neighborhood. Define the automorphic kernel $K_V\colon [(\mathbf{G}\times\mathbf{G})(\mathbb{A})]^{\times 2} \to \mathbb{R}$:

$$K_V(x,y) = \sum_{\gamma\in(\mathbf{G}\times\mathbf{G})(\mathbb{Q})} \mathbb{1}_V(x^{-1}\gamma y).$$

As V is compact, the sum on the right is finite for every x and y. Moreover, the number of non-trivial summands is uniformly bounded when x and y are restricted to fixed compact subsets. In particular, the convergence is uniform on compact sets.

Definition 8.2. Let $B = \prod_v B_v \subseteq \mathbf{G}(\mathbb{A})$ be a compact identity neighborhood with $B_v = K_v$ for almost all v, and let B_v be a compact-open subgroup for all v non-archimedean. Let λ_1, λ_2 be probability measures on $[(\mathbf{G}\times\mathbf{G})(\mathbb{A})]$, and let $K_{B\times B}$ be as in Definition 8.1.

For a fixed closed subset $C\subseteq[\mathbf{G}(\mathbb{A})]$, we define

$$\mathrm{Cor}_C[\lambda_1,\lambda_2](B) := \int_{C\times C}\int_{C\times C} K_{B\times B}(x,y)\,\mathrm{d}\lambda_1(x)\,\mathrm{d}\lambda_2(y).$$

We also write $\mathrm{Cor}[\lambda_1,\lambda_2](B)=\mathrm{Cor}_{Y_{\mathbb{A}}}[\lambda_1,\lambda_2](B)$.

We say that B is injective on C if the quotient map $\mathbf{G}(\mathbb{A})\to[\mathbf{G}(\mathbb{A})]$ is injective when restricted to gB for any $g\in\mathbf{G}(\mathbb{A})$ such that $[g]\in C$. When C is compact there is always an identity neighborhood injective on C.

Lemma 8.3. *In the setting of Definition 8.2, we always have*

$$\lambda_1\times\lambda_2\,(x,y\in C\times C\mid y\in xB)\leq\mathrm{Cor}_C[\lambda_1\times\lambda_2](B)$$

with equality if B is injective on C.

Proof. The proof follows directly from the definitions. □

8.2. *Main theorem about cross-correlation.* The main result in this section and the main structural result in this manuscript is Theorem 8.7 below to be proved in Section 8.8. First we need a few definitions.

Definition 8.4. We introduce the following notation for a fixed joint homogeneous toral set $\left[\mathbf{T}^{\Delta}(\mathbb{A})(g,sg)\right]$:

(1) The twist $s\in\mathbf{T}(\mathbb{A})$ defines a homothety class of invertible fractional Λ-ideals

$$\mathbb{Q}^{\times}\mathfrak{s}:=\mathrm{idl}(s)\in{}_{\mathbb{Q}^{\times}}\backslash^{\mathcal{J}(\Lambda)}.$$

(2) Define the following invertible fractional Λ-ideal, which encapsulates the splitting behavior of $\mathbf{B}$ outside of ∞:

$$\mathfrak{e}:=\widetilde{\mathrm{idl}}\left((\upsilon_v\tau_v)_v\right),$$

where υ_v,τ_v are as in Proposition 5.19.

(3) We also need the following integer, which is also closely related to the splitting of $\mathbf{B}$:

$$\upsilon:=\mathrm{sign}(\epsilon)\prod_{\substack{\mathbf{B}\text{ is ramified and}\\ E\text{ is inert at }p}}p.$$

Remark 8.5. In the simplest case, when $\mathbf{G}\simeq\mathbf{PGL}_2$ is split we can choose $\epsilon=1$ and then $\upsilon=1$ and $\mathfrak{e}=\Lambda$.

Definition 8.6. Define the arithmetic functions $f_{[\mathfrak{g}]}, g_{[\mathfrak{g}]} \colon \mathbb{Z} \to \mathbb{Z}$ for any $[\mathfrak{g}] \in \operatorname{Pic}(\Lambda)$ as follows:

$$\begin{aligned} g_{[\mathfrak{g}]}(x) &= \#\left\{\mathfrak{a} \in \mathcal{J}(\Lambda)_0 \mid \operatorname{Nr}(\mathfrak{a}) = x,\ \mathfrak{a} \subseteq \Lambda,\ [\mathfrak{a}] = [\mathfrak{g}] \text{ or } \mathfrak{a} = 0\right\}, \\ f_{[\mathfrak{g}]}(x) &= \#\left\{\mathfrak{b} \in \mathcal{J}(\Lambda) \mid \operatorname{Nr}(\mathfrak{b}) = x,\ \mathfrak{b} \subseteq \Lambda,\ [\mathfrak{b}] \in [\mathfrak{g}] \operatorname{Pic}(\Lambda)^2\right\}. \end{aligned}$$

Define also the multiplicative function $r \colon \mathbb{N} \to \mathbb{N}$ by requiring that for any *odd* prime $p \mid D$, if $\mathbf{B}$ splits at p, then

$$r(p^k) = \begin{cases} 1 & k < \operatorname{ord}_p D, \\ 2 & k \geq \operatorname{ord}_p D. \end{cases}$$

If $2 \mid D$, we set $r(2^k) = 2^{\mu_{\text{wild}}}$, where $\mu_{\text{wild}} \in \{0,1,2,3\}$ is defined in Corollary A.7. If $p \mid D$ and $\mathbf{B}$ ramifies at p, we define $r(p^k) = 2$. For all primes $p \nmid D$, we set $r(p^k) = 1$.

THEOREM 8.7. *Fix a joint homogeneous toral set* $\left[\mathbf{T}^{\Delta}(\mathbb{A})(g, sg)\right]$ *with splitting field* $E/\mathbb{Q}$ *and quadratic order* $\Lambda \leq \mathcal{O}_E$ *of discriminant* D. *Assume that* $(\spadesuit)$ *is satisfied.*

Let $B = \prod_v B_v \subset \mathbf{G}(\mathbb{A})$ *with* $B_v = \Omega_v$ *for all* $v \neq p_1$ *and* $B_{p_1} = K_{p_1}^{(-n,n)}$ *for some* $n \in \mathbb{N}$. *Fix also a simply connected homogeneous Hecke set* $\left[\mathbf{G}^{\Delta}(\mathbb{A})^{+}\xi\right]$ *with* $\operatorname{ctr}(\xi)_{p_1} \in A_{p_1}$, *and assume*

$$g^{-1}\mathbf{T}(\mathbb{Q})sg \cap B \operatorname{ctr}(\xi) B = \emptyset.$$

Let μ *be the algebraic probability measure supported on* $\left[\mathbf{T}^{\Delta}(\mathbb{A})(g, sg)\right]$ *and let* ν *be the algebraic probability measure supported on* $\left[\mathbf{G}^{\Delta}(\mathbb{A})^{+}\xi\right]$. *Denote* $\kappa = 2^8\, \mathfrak{d}_\infty(\operatorname{ctr}(\xi)_\infty)\, \mathfrak{d}_f(\operatorname{ctr}(\xi)_f)$ *and* $\omega = -\operatorname{sign}(\operatorname{Nrd}(\operatorname{ctr}(\xi)_\infty))\, \mathfrak{d}_f(\operatorname{ctr}(\xi)_f)$. *Then*

$$\begin{aligned} \operatorname{Cor}[\mu,\nu](B) \ll{} & \operatorname{vol}\left([\mathbf{T}(\mathbb{A})g]\right)^{-1} \operatorname{vol}\left(\left[\mathbf{G}^{\Delta}(\mathbb{A})^{+}\xi\right]\right)^{-1} p_1^{-2n} \\ & \cdot \sum_{\substack{0 \leq x \leq \kappa|D| \\ x \equiv \omega D \mod \upsilon p_1^{2n}}} g_{[\mathfrak{s}]}(x) f_{[p_1^n \mathfrak{s}\mathfrak{e}]^{-1}}\left(\frac{x - \omega D}{\upsilon p_1^{2n}}\right) r\left(\frac{x - \omega D}{\upsilon p_1^{2n}}\right). \end{aligned}$$

Remark 8.8. Notice that υ is supported on primes that are inert in $E/\mathbb{Q}$ while p_1 splits; thus $\gcd(\upsilon, p_1^{2n}) = 1$.

8.3. *Geometric expansion.*

Definition 8.9. Set

$$W_{\mathbb{Q}} = {}_{\mathbf{G}^{\Delta}(\mathbb{Q})}\backslash^{(\mathbf{G} \times \mathbf{G})(\mathbb{Q})}/_{\mathbf{T}^{\Delta}(\mathbb{Q})}.$$

We denote by $[\gamma] \in W_{\mathbb{Q}})$ the double coset corresponding to $\gamma \in (\mathbf{G} \times \mathbf{G})(\mathbb{Q})$.

We have a natural map $W_{\mathbb{Q}} \to \mathbf{W}(\mathbb{Q})$, where $\mathbf{W}$ is the GIT quotient defined in Section 6. Recall from Proposition 6.3 that this map is injective outside of $\{[(\gamma_0, \gamma_0 w_{\mathbf{T}} t_{\mathbb{Q}})] \mid \gamma_0 \in \mathbf{G}(\mathbb{Q}),\ t_{\mathbb{Q}} \in \mathbf{T}(\mathbb{Q})\}$.

Definition 8.10. For any closed subgroup $N < \mathbf{M}(\mathbb{A})$, denote

$$N^\dagger \coloneqq N \cap \left(\mathbf{G}(\mathbb{A})^+ \times \mathbf{T}(\mathbb{A})\right).$$

The subgroup $N^\dagger$ is always normal in N.

The following proposition is the geometric expansion of the relative trace corresponding to the subgroups $\mathbf{G}^\Delta$ and $\mathbf{T}^\Delta$ of $\mathbf{G} \times \mathbf{G}$. The situation is relatively simple as the stabilizers have finite volume adelic quotients.

Proposition 8.11. *Let μ be the periodic measure on a joint homogeneous toral set $[\mathbf{T}^\Delta(\mathbb{A})(g, sg)]$ and ν the periodic measure on a simply-connected Hecke correspondence $[\mathbf{G}^\Delta(\mathbb{A})^+\xi]$, $\xi = (\xi_1, \xi_2)$. Set $B' = \xi_1 B g^{-1} \times \xi_2 B g^{-1} s^{-1}$. Then*

$$\begin{aligned}
\operatorname{Cor}[\mu,\nu](B) &= \int_{[\mathbf{G}(\mathbb{A})^+]} \int_{[\mathbf{T}(\mathbb{A})]} K_{B'}(l,t)\,\mathrm{d}l\,\mathrm{d}t \\
&= \sum_{[\gamma]\in W_{\mathbb{Q}}} \sum_{\varkappa\in\pi_{\mathbf{G}}(\mathbf{M}_\gamma(\mathbb{Q}))\backslash\mathbf{G}(\mathbb{Q})/\mathbf{G}(\mathbb{Q})^+} \operatorname{vol}(\mathbf{M}_\gamma)\cdot \operatorname{RO}_{\gamma,\varkappa}(B), \\
\operatorname{RO}_{\gamma,\varkappa}(B) &\coloneqq \int_{\mathbf{M}_\gamma(\mathbb{A})^\dagger\backslash\mathbf{M}(\mathbb{A})^\dagger} \mathbb{1}_{B'}\left((\varkappa l)^{-1}\gamma t\right)\,\mathrm{d}(l,t), \\
\operatorname{vol}(\mathbf{M}_\gamma) &\coloneqq \mathrm{m}_{\mathbf{M}_\gamma(\mathbb{A})^\dagger}\left({\mathbf{M}_\gamma(\mathbb{Q})^\dagger}\backslash{\mathbf{M}_\gamma(\mathbb{A})^\dagger}\right),
\end{aligned}$$

where the Haar measures on ${\mathbf{M}_\gamma(\mathbb{A})^\dagger}\backslash{\mathbf{M}(\mathbb{A})^\dagger}$ and $\mathbf{M}_\gamma(\mathbb{A})^\dagger$ are mutually normalized.

Following the relative trace formula terminology, we call $\operatorname{RO}_{\gamma,\varkappa}(B)$ a relative orbital integral.

We will use the following lemma in the proof of the proposition.

Lemma 8.12. *For any $a \in \mathbf{M}(\mathbb{A})$, let $\operatorname{Ad}_a \colon \mathbf{M}(\mathbb{A})^\dagger \to \mathbf{M}(\mathbb{A})^\dagger$ be the conjugation automorphism of the normal subgroup $\mathbf{M}(\mathbb{A})^\dagger$. Then the map Ad_a fixes any Haar measure on $\mathbf{M}(\mathbb{A})^\dagger$.*

Proof. Let $\mathrm{m}_{\mathbf{M}(\mathbb{A})^\dagger}$ be a Haar measure on $\mathbf{M}(\mathbb{A})^\dagger$. Then $(\operatorname{Ad}_a)_* \mathrm{m}_{\mathbf{M}(\mathbb{A})^\dagger}$ is a Haar measure as well and proportional to the original one $(\operatorname{Ad}_a)_* \mathrm{m}_{\mathbf{M}(\mathbb{A})^\dagger} = \alpha(a)\mathrm{m}_{\mathbf{M}(\mathbb{A})^\dagger}$. The map $\alpha \colon \mathbf{M}(\mathbb{A}) \to \mathbb{R}_{>0}$ is a character that is trivial on $\mathbf{M}(\mathbb{A})^\dagger$, hence it factors through the 2-torsion group ${\mathbf{M}(\mathbb{A})^\dagger}\backslash{\mathbf{M}(\mathbb{A})}$. Because $\mathbb{R}_{>0}$ has no non-trivial torsion elements, α is trivial. □

Proof of Proposition 8.11. Let $[\gamma]\in W_{\mathbb{Q}}$ be a double coset with representative $\gamma\in(\mathbf{G}\times\mathbf{G})(\mathbb{Q})$. Denote $f\coloneqq \mathbb{1}_{B'}$. We unfold the definition of the cross-correlation and exchange summation and integration using the uniform convergence of the kernel on compact subsets

$$\begin{aligned}\operatorname{Cor}[\mu,\nu](B)&=\int_{[\mathbf{M}(\mathbb{A})^\dagger]}\sum_{\gamma\in(\mathbf{G}\times\mathbf{G})(\mathbb{Q})} f(l^{-1}\gamma t)\,\mathrm{d}(l,t)\\ &=\sum_{[\gamma]\in W_{\mathbb{Q}}}\sum_{\gamma'\in[\gamma]}\int_{[\mathbf{M}(\mathbb{A})^\dagger]} f(l^{-1}\gamma' t)\,\mathrm{d}(l,t) \qquad (22)\\ &=\sum_{[\gamma]\in W_{\mathbb{Q}}}\sum_{\gamma'\in[\gamma]}\int_{[\mathbf{M}(\mathbb{A})^\dagger]} f(m^{-1}.\gamma')\,\mathrm{d}m.\end{aligned}$$

We now deal individually with each internal sum for $[\gamma]$ fixed. Let $\mathscr{F}\subset\mathbf{M}(\mathbb{A})^\dagger$ be a fundamental domain for the left action of $\mathbf{M}(\mathbb{Q})^\dagger$ on $\mathbf{M}(\mathbb{A})^\dagger$. We write the internal sum in (22) as a sum of integrals on $\mathscr{F}$. To do this we choose some fixed representatives for each set of cosets appearing in the following:
(23)

$$\begin{aligned}\sum_{\gamma'\in[\gamma]}\int_{[\mathbf{M}(\mathbb{A})^\dagger]} f(m^{-1}.\gamma')\,\mathrm{d}m&=\sum_{m_{\mathbb{Q}}\in\mathbf{M}_\gamma(\mathbb{Q})\backslash\mathbf{M}(\mathbb{Q})}\int_{\mathscr{F}} f\left(m^{-1}m_{\mathbb{Q}}^{-1}.\gamma\right)\,\mathrm{d}m\\ &=\sum_{\bar{\varkappa}\in\mathbf{M}_\gamma(\mathbb{Q})\backslash\mathbf{M}(\mathbb{Q})/\mathbf{M}(\mathbb{Q})^\dagger}\ \sum_{m_{\mathbb{Q}}\in\bar{\varkappa}^{-1}\mathbf{M}_\gamma(\mathbb{Q})^\dagger\bar{\varkappa}\backslash\mathbf{M}(\mathbb{Q})^\dagger}\int_{\mathscr{F}} f\left((m^{-1}m_{\mathbb{Q}}^{-1}\bar{\varkappa}^{-1}).\gamma\right)\,\mathrm{d}m\\ &=\sum_{\bar{\varkappa}\in\mathbf{M}_\gamma(\mathbb{Q})\backslash\mathbf{M}(\mathbb{Q})/\mathbf{M}(\mathbb{Q})^\dagger}\ \sum_{m_{\mathbb{Q}}\in\bar{\varkappa}^{-1}\mathbf{M}_\gamma(\mathbb{Q})^\dagger\bar{\varkappa}\backslash\mathbf{M}(\mathbb{Q})^\dagger}\int_{m_{\mathbb{Q}}\mathscr{F}} f\left((m^{-1}\bar{\varkappa}^{-1}).\gamma\right)\,\mathrm{d}m.\end{aligned}$$

Now fix a representative

$$\bar{\varkappa}\in {}_{\mathbf{M}_\gamma(\mathbb{Q})}\backslash^{\mathbf{M}(\mathbb{Q})}/_{\mathbf{M}(\mathbb{Q})^\dagger}.$$

The function $f\left((m^{-1}\bar{\varkappa}^{-1}).\gamma\right)$ is a well-defined compactly supported integrable function on ${}_{\bar{\varkappa}^{-1}\mathbf{M}_\gamma(\mathbb{A})^\dagger\bar{\varkappa}}\backslash^{\mathbf{M}(\mathbb{A})^\dagger}$.

Using the mutual normalization of Haar measures we can rewrite the inner sum in (23) as

$$\begin{aligned}&\int_{\bar{\varkappa}^{-1}\mathbf{M}_\gamma(\mathbb{A})^\dagger\bar{\varkappa}\backslash\mathbf{M}(\mathbb{A})^\dagger} f\left((m^{-1}\bar{\varkappa}^{-1}).\gamma\right)\,\mathrm{d}m \qquad (24)\\ &\cdot\sum_{m_{\mathbb{Q}}\in\bar{\varkappa}^{-1}\mathbf{M}_\gamma(\mathbb{Q})^\dagger\bar{\varkappa}\backslash\mathbf{M}(\mathbb{Q})^\dagger}\mathrm{m}_{\bar{\varkappa}^{-1}\mathbf{M}_\gamma(\mathbb{A})^\dagger\bar{\varkappa}}\left(m_{\mathbb{Q}}\mathscr{F}\right).\end{aligned}$$

For a fixed Haar measure $\mathrm{m}_{\mathbf{M}_\gamma(\mathbb{A})^\dagger}$ on $\mathbf{M}_\gamma(\mathbb{A})^\dagger$, define a Haar measure on $\bar{\varkappa}^{-1}\mathbf{M}_\gamma(\mathbb{A})^\dagger\bar{\varkappa}$ by $\left(\operatorname{Ad}_{\bar{\varkappa}^{-1}}\right)_*\mathrm{m}_{\mathbf{M}_\gamma(\mathbb{A})^\dagger}$. Using this normalization we have
(25)

$$\sum_{m_{\mathbb{Q}}\in\bar{\varkappa}^{-1}\mathbf{M}_\gamma(\mathbb{Q})^\dagger\bar{\varkappa}\backslash\mathbf{M}(\mathbb{Q})^\dagger}\mathrm{m}_{\bar{\varkappa}^{-1}\mathbf{M}_\gamma(\mathbb{A})^\dagger\bar{\varkappa}}\left(m_{\mathbb{Q}}\mathscr{F}\right)=\sum_{m_{\mathbb{Q}}\in\mathbf{M}_\gamma(\mathbb{Q})^\dagger\backslash\mathbf{M}(\mathbb{Q})^\dagger}\mathrm{m}_{\mathbf{M}_\gamma(\mathbb{A})^\dagger}\left(m_{\mathbb{Q}}\mathscr{F}\right).$$

The set $\bigsqcup_{m_{\mathbb{Q}}\in\mathbf{M}_\gamma(\mathbb{Q})^\dagger\backslash\mathbf{M}(\mathbb{Q})^\dagger} m_{\mathbb{Q}}\mathscr{F}$ is a fundamental domain for the left action of $\mathbf{M}_\gamma(\mathbb{Q})^\dagger$ on $\mathbf{M}(\mathbb{A})^\dagger$; hence the sum (25) is equal to $\mathrm{m}_{\mathbf{M}_\gamma(\mathbb{A})^\dagger}\left({}_{\mathbf{M}_\gamma(\mathbb{Q})^\dagger}\backslash^{\mathbf{M}_\gamma(\mathbb{A})^\dagger}\right)$.

Under the normalization of Haar measures as above there is an isomorphism of the following measure spaces equipped with their respective Haar measures:

$$\bar{\varkappa}^{-1}\mathbf{M}_\gamma(\mathbb{A})^\dagger\bar{\varkappa}\backslash^{\mathbf{M}(\mathbb{A})^\dagger} \simeq {}_{\mathbf{M}_\gamma(\mathbb{A})^\dagger}\backslash^{\mathbf{M}(\mathbb{A})^\dagger},$$
$$\left(\bar{\varkappa}^{-1}\mathbf{M}_\gamma(\mathbb{A})^\dagger\bar{\varkappa}\right)m \mapsto \left(\mathbf{M}_\gamma(\mathbb{A})^\dagger\right)\bar{\varkappa}m\bar{\varkappa}^{-1}.$$

This implies

$$\int_{\bar{\varkappa}^{-1}\mathbf{M}_\gamma(\mathbb{A})^\dagger\bar{\varkappa}\backslash\mathbf{M}(\mathbb{A})^\dagger} f\left((m^{-1}\bar{\varkappa}^{-1}).\gamma\right)\,\mathrm{d}m = \int_{\mathbf{M}_\gamma(\mathbb{A})^\dagger\backslash\mathbf{M}(\mathbb{A})^\dagger} f\left((\bar{\varkappa}^{-1}m^{-1}).\gamma\right)\mathrm{d}m$$
$$= \int_{\mathbf{M}_\gamma(\mathbb{A})^\dagger\backslash\mathbf{M}(\mathbb{A})^\dagger} f\left((m^{-1}\bar{\varkappa}^{-1}).\gamma\right)\mathrm{d}m,$$

where the last equality follows from Lemma 8.12.

Combining all of the above and using the following bijection induced by the projection map $\pi_{\mathbf{G}}\colon \mathbf{M}=\mathbf{G}\times\mathbf{T}\to\mathbf{G}$,

$${}_{\mathbf{M}_\gamma(\mathbb{Q})}\backslash^{\mathbf{M}(\mathbb{Q})}/_{\mathbf{M}(\mathbb{Q})^\dagger} \simeq {}_{\pi_{\mathbf{G}}\left(\mathbf{M}_\gamma(\mathbb{Q})\right)}\backslash^{\mathbf{G}(\mathbb{Q})}/_{\mathbf{G}(\mathbb{Q})^+},$$

we arrive to the required final form. □

Lemma 8.13. *Fix $\gamma\in(\mathbf{G}\times\mathbf{G})(\mathbb{Q})$ with $\mathbf{M}_\gamma(\mathbb{A})$ compact. Then under a suitable normalization of measures,*

$$\mathrm{RO}_{\gamma,\varkappa}(B) := \int_{\mathbf{M}(\mathbb{A})^\dagger} \mathbb{1}_{B'}\left((\varkappa l)^{-1}\gamma t\right)\,\mathrm{d}(l,t)$$

and

$$\sum_{\varkappa\in\pi_{\mathbf{G}}(\mathbf{M}_\gamma(\mathbb{Q}))\backslash\mathbf{G}(\mathbb{Q})/\mathbf{G}(\mathbb{Q})^+} \mathrm{vol}(\mathbf{M}_\gamma)\cdot\mathrm{RO}_{\gamma,\varkappa}(B) = \frac{1}{\#\mathbf{M}_\gamma(\mathbb{Q})} \sum_{\varkappa\in\mathbf{G}(\mathbb{Q})/\mathbf{G}(\mathbb{Q})^+} \mathrm{RO}_{\gamma,\varkappa}(B).$$

Notice that the group $\mathbf{M}_\gamma(\mathbb{Q})$ is a discrete subgroup of a compact group, hence it is finite.

This proposition shows that the case of a compact stabilizer is very similar to that of a trivial one, the only difference being the easy to compute factor.

Proof. The group $\mathbf{M}_\gamma(\mathbb{A})^\dagger$ is a closed subgroup of a compact group, hence it is compact. We normalize the Haar measure on $\mathbf{M}_\gamma(\mathbb{A})^\dagger$ so that it is equal to 1. This normalization results in $\mathrm{RO}_{\gamma,\varkappa}(B)$ being equal to the integral above over $\mathbf{M}(\mathbb{A})^\dagger$. In this normalization we also have $\mathrm{vol}(\mathbf{M}_\gamma) = \left(\#\mathbf{M}_\gamma(\mathbb{Q})^\dagger\right)^{-1}$.

When summing over $\varkappa\in\mathbf{G}(\mathbb{Q})/\mathbf{G}(\mathbb{Q})^+$ instead of $\varkappa\in\pi_{\mathbf{G}}\left(\mathbf{M}_\gamma(\mathbb{Q})\right)\backslash\mathbf{G}(\mathbb{Q})/\mathbf{G}(\mathbb{Q})^+$, the same summand appear multiple times and needs to be accounted for. The multiplicity of a summand is the size of the corresponding fiber in

$\mathbf{G}(\mathbb{Q})/\mathbf{G}(\mathbb{Q})^+ \to \pi_{\mathbf{G}}\left(\mathbf{M}_\gamma(\mathbb{Q})\right)\backslash\mathbf{G}(\mathbb{Q})/\mathbf{G}(\mathbb{Q})^+$. As $\mathbf{M}(\mathbb{A})^\dagger < \mathbf{M}(\mathbb{A})$ is normal, all the fibers have the same size, which is

$$\left[\mathbf{M}_\gamma(\mathbb{Q}) : \mathbf{M}_\gamma(\mathbb{Q})^\dagger\right].$$

Finally, the correct proportionality factor between the two sums in the claim is

$$\operatorname{vol}(\mathbf{M}_\gamma)\left[\mathbf{M}_\gamma(\mathbb{Q}) : \mathbf{M}_\gamma(\mathbb{Q})^\dagger\right]^{-1} = \left(\#\mathbf{M}_\gamma(\mathbb{Q})\right)^{-1}. \qquad \square$$

8.4. *Reduction to compact stabilizers.* Recall from Proposition 7.8 that the minimal volume of a homogeneous Hecke set containing a joint homogeneous toral set depends on the distance of the discrete orbit $g^{-1}\mathbf{T}(\mathbb{Q})sg$ from the identity. In particular, for a sequence of joint homogeneous toral sets, we need to assume that for every compact subset $B_0 \subset \mathbf{G}(\mathbb{A})$, the orbit $g^{-1}\mathbf{T}(\mathbb{Q})sg$ does not intersect B_0 for all joint homogeneous toral sets with discriminant large enough.

In this section we show that for a fixed simply connected homogeneous Hecke set, the assumption above implies that the contribution to the cross correlation from terms with a non-compact stabilizer vanishes. This is the fundamental application of this assumption.

Once more we will use the fact that the shift $g^{-1}\mathbf{T}(\mathbb{Q})sg$ is large when bounding the pertinent shifted convolution sum.

Whenever the shift has a small representative, the cross-correlation with some Hecke correspondence will have terms with non-compact stabilizers and these will be the dominant contribution to the cross-correlation. The simplest bad case is the cross-correlation between a periodic joint toral measure and a Hecke correspondence containing its support.

LEMMA 8.14. *Assume that*

$$g^{-1}\mathbf{T}(\mathbb{Q})sg \cap B^{-1}\operatorname{ctr}(\xi)B = \emptyset. \tag{26}$$

Then for all $\gamma \in (\mathbf{G}\times\mathbf{G})(\mathbb{Q})$, *if* $\mathbf{M}_\gamma(\mathbb{A})^\dagger$ *is not compact, then* $\mathrm{RO}_{\gamma,\varkappa}(B) = 0$ *for all*

$$\varkappa \in \pi_{\mathbf{G}}(\mathbf{M}_\gamma(\mathbb{Q}))\backslash{}^{\mathbf{G}(\mathbb{Q})}/_{\mathbf{G}(\mathbb{Q})^+}.$$

Proof. Write $\xi = (\xi_1, \xi_2)$. Assume $\mathbf{M}_\gamma(\mathbb{A})^\dagger$ is not compact. Then according to Proposition 6.3, $\gamma = (\gamma_1, \gamma_1 t_{\mathbb{Q}})$ for some $t_{\mathbb{Q}} \in \mathbf{T}(\mathbb{Q})$. If $\mathrm{RO}_{\gamma,\varkappa}(B) \neq 0$ for some $\varkappa$, then

$$\begin{gathered}\exists l \in \mathbf{G}(\mathbb{A})^+, t \in \mathbf{T}(\mathbb{A})\colon \left((\varkappa l)^{-1}\gamma_1 t, l^{-1}\varkappa^{-1}\gamma_1 t_{\mathbb{Q}} t\right) \in B' = \xi_1 B g^{-1} \times \xi_2 B g^{-1} s^{-1} \\ \Longrightarrow t_{\mathbb{Q}} \in g B^{-1}\xi_1^{-1}\xi_2 B g^{-1} s^{-1} \Longrightarrow g^{-1} t_{\mathbb{Q}} s g \in B^{-1}\xi_1^{-1}\xi_2 B,\end{gathered}$$

which contradicts the assumption (26). $\square$

Remark 8.15. Notice that if condition (26) holds, then $\mathrm{Cor}[\mu,\nu](B_0)$ will have no contribution from terms with a non-compact stabilizer for any $B_0 \subset B$. This will be useful, as in the endgame we would like to bound the cross-correlation between a limit measure and a simply connected Hecke correspondence for an arbitrarily small identity neighborhood.

Corollary 8.16. *Assume*

$$g^{-1}\mathbf{T}(\mathbb{Q})sg \cap B^{-1}\,\mathrm{ctr}(\xi)B = \emptyset.$$

Then

$$\mathrm{Cor}[\mu,\nu](B) = \sum_{\substack{[\gamma]\in W_{\mathbb{Q}} \\ \psi\det^{-1}(\gamma)\neq 0}} \frac{1}{\#\mathbf{M}_\gamma(\mathbb{Q})} \sum_{\varkappa\in\mathbf{G}(\mathbb{Q})/\mathbf{G}(\mathbb{Q})^+} \mathrm{RO}_{\gamma,\varkappa}(B)$$

and

$$\#\mathbf{M}_\gamma(\mathbb{Q}) = \begin{cases} 1 & \mathrm{ctr}(\gamma)\notin \mathrm{N}_{\mathbf{G}}\,\mathbf{T}(\mathbb{Q}), \\ 2 & \textit{otherwise.} \end{cases}$$

Proof. Lemma 8.14 implies that the geometric expansion of $\mathrm{Cor}[\mu,\nu](B)$ has no contributions from $[\gamma]$ such that $\mathrm{ctr}(\gamma)\in\mathbf{T}(\mathbb{Q})$. The condition $\psi\det^{-1}(\gamma) \neq 0$ is exactly equivalent to $\mathrm{ctr}(\gamma)\notin\mathbf{T}(\mathbb{Q})$.

The claimed expression for $\mathrm{Cor}[\mu,\nu](B)$ now holds due to Proposition 8.11 and Lemma 8.13. To calculate $\mathbf{M}_\gamma(\mathbb{Q})$ in the relevant cases we use Proposition 6.3. This proposition implies that $\mathbf{M}_\gamma$ is trivial if $\mathrm{ctr}(\gamma)\notin\mathrm{N}_{\mathbf{G}}(\mathbf{T})(\mathbb{Q})$ and $\mathbf{M}_\gamma\simeq\mu_2$ otherwise. The final part of the claim holds because $\mu_2(\mathbb{Q})\simeq {}^{\mathbb{Z}}/_{2\mathbb{Z}}$. □

8.5. *Decomposition of the relative orbital integral.*

Definition 8.17. Fix $\gamma\in(\mathbf{G}\times\mathbf{G})(\mathbb{Q})$ with $\mathbf{M}_\gamma(\mathbb{A})$ compact, and let $\varkappa\in\mathbf{G}(\mathbb{Q})$. We split the relative orbital integral into an archimedean and non-archimedean parts

$$\mathrm{RO}_{\gamma,\varkappa}(B) = \mathrm{RO}^\infty_\gamma(B)\cdot\mathrm{RO}^f_\gamma(B),$$
$$\mathrm{RO}^\infty_{\gamma,\varkappa}(B) := \int_{\mathbf{M}(\mathbb{R})^\dagger} \mathbb{1}_{B'_\infty}\left((\varkappa l)^{-1}\gamma t\right)\,\mathrm{d}(l,t),$$
$$\mathrm{RO}^f_{\gamma,\varkappa}(B) := \int_{\mathbf{M}(\mathbb{A}_f)^\dagger} \mathbb{1}_{B'_f}\left((\varkappa l)^{-1}\gamma t\right)\,\mathrm{d}(l,t).$$

The complicated expression to handle is the non-archimedean part. We will see that the archimedean part is rather simple due to the fact that we have restricted to the case $H_\infty = K_\infty$ in $(\spadesuit)$.

In the next section we interpret the non-archimedean relative orbital integral as counting the number of intersections between the $\mathbf{M}(\mathbb{A}_f)$-orbit of γ and

B' modulo a compact-open subgroup of $\mathbf{M}(\mathbb{A}_f)$. The main result is a finite-to-one map between intersections and pairs of integral Λ-ideals satisfying a list of arithmetic conditions.

Unlike Linnik's argument for the equidistribution of CM points on a modular curve, we do not calculate the relative orbital integrals at each place separately. Instead, we match them globally with a different global object.

8.6. *Archimedean relative orbital integral.*

Lemma 8.18. *Let* $\gamma = (\gamma_1, \gamma_2) \in (\mathbf{G} \times \mathbf{G})(\mathbb{Q})$ *and* $\varkappa \in \mathbf{G}(\mathbb{Q})$. *Assume* $B_\infty = \Omega_\infty$. *Then* $\mathrm{RO}^\infty_{\gamma,\varkappa}(B) = 0$ *if* $\operatorname{ctr}(\gamma) \notin g_\infty \Omega_\infty \operatorname{ctr}(\xi)_\infty \Omega_\infty g_\infty^{-1}$, *and*

$$\mathrm{RO}^\infty_{\gamma,\varkappa}(B) \le \mathrm{m}_{\mathbf{T}(\mathbb{R})}\left(\mathbf{T}(\mathbb{R})\right) \mathrm{m}_{\mathbf{G}(\mathbb{R})^+}\left(\xi_{1,\infty}\Omega_\infty^2 \xi_{1,\infty}^{-1} \cap \xi_{2,\infty}\Omega_\infty^2 \xi_{2,\infty}^{-1}\right)$$

otherwise.

Proof. From $\Omega_\infty K_\infty = \Omega_\infty$ and $g_\infty^{-1}\mathbf{T}(\mathbb{R})g_\infty = K_\infty$ we deduce $B'_\infty \cdot \mathbf{T}(\mathbb{R})^\Delta = \xi_1\Omega_\infty g_\infty^{-1} \times \xi_2 \Omega_\infty g_\infty^{-1}$. Hence $\mathbb{1}_{B'_\infty}\left((\varkappa l)^{-1}\gamma t\right) = 1$ if and only if

$$(\varkappa l)^{-1} \in \xi_{1,\infty}\Omega_\infty g_\infty^{-1}\gamma_1^{-1} \cap \xi_{2,\infty}\Omega_\infty g_\infty^{-1}\gamma_2^{-1}.$$

If the intersection on the right-hand side is non-empty, then there are some $\omega_1, \omega_2 \in \Omega_\infty$ such that

$$\operatorname{ctr}(\gamma) = g_\infty \omega_1 \operatorname{ctr}(\xi)_\infty \omega_2 g_\infty^{-1} \in g_\infty \Omega_\infty \operatorname{ctr}(\xi)_\infty \Omega_\infty g_\infty^{-1}. \tag{27}$$

This proves the first claim.

Moreover, the infinite part of the relative orbital integral is

$$\begin{aligned}\mathrm{RO}^\infty_{\gamma,\varkappa}(B) &:= \int_{\mathbf{M}(\mathbb{R})^\dagger} \mathbb{1}_{B'_\infty}\left((\varkappa l)^{-1}\gamma t\right) \mathrm{d}(l,t) \\ &= \mathrm{m}_{\mathbf{T}(\mathbb{R})}\left(\mathbf{T}(\mathbb{R})\right) \int_{\mathbf{G}(\mathbb{R})^+} \mathbb{1}_{\xi_{1,\infty}\Omega_\infty g_\infty^{-1}\gamma_1^{-1} \cap \xi_{2,\infty}\Omega_\infty g_\infty^{-1}\gamma_2^{-1}}\left((\varkappa l)^{-1}\right) \mathrm{d}l \\ &= \mathrm{m}_{\mathbf{T}(\mathbb{R})}\left(\mathbf{T}(\mathbb{R})\right) \mathrm{m}_{\mathbf{G}(\mathbb{R})^+}\left(\xi_{1,\infty}\Omega_\infty g_\infty^{-1}\gamma_1^{-1}\varkappa \cap \xi_{2,\infty}\Omega_\infty g_\infty^{-1}\gamma_2^{-1}\varkappa\right).\end{aligned}$$

The right-hand side above is trivially zero unless $\operatorname{Nrd} \varkappa^{-1}\gamma_1 g_\infty \xi_{1,\infty}^{-1} > 0$ so we may assume it is the case. Using the right invariance of a Haar measure on $\mathbf{G}(\mathbb{R})^+$ and (27), we have

$$\begin{aligned}&\mathrm{m}_{\mathbf{G}(\mathbb{R})^+}\left(\xi_{1,\infty}\Omega_\infty g_\infty^{-1}\gamma_1^{-1}\varkappa \cap \xi_{2,\infty}\Omega_\infty g_\infty^{-1}\gamma_2^{-1}\varkappa\right) \\ &\qquad = \mathrm{m}_{\mathbf{G}(\mathbb{R})^+}\left(\xi_{1,\infty}\Omega_\infty \xi_{1,\infty}^{-1} \cap \xi_{2,\infty}\Omega_\infty g_\infty^{-1}\gamma_2^{-1}\gamma_1 g_\infty \xi_{1,\infty}^{-1}\right) \\ &\qquad = \mathrm{m}_{\mathbf{G}(\mathbb{R})^+}\left(\xi_{1,\infty}\Omega_\infty \omega_1^{-1}\xi_{1,\infty}^{-1} \cap \xi_{2,\infty}\Omega_\infty \omega_2^{-1}\xi_{2,\infty}^{-1}\right) \\ &\qquad \le \mathrm{m}_{\mathbf{G}(\mathbb{R})^+}\left(\xi_{1,\infty}\Omega_\infty^2 \xi_{1,\infty}^{-1} \cap \xi_{2,\infty}\Omega_\infty^2 \xi_{2,\infty}^{-1}\right)\end{aligned}$$

as claimed. □

8.7. *Non-archimedean relative orbital integrals.*

Definition 8.19. Let $B_f < \mathbf{G}(\mathbb{A}_f)$ be a compact-open subgroup and fix a homogeneous Hecke set $\left[\mathbf{G}^{\Delta}(\mathbb{A})^{+}(\xi_1,\xi_2)\right]$ and a homogeneous toral set $[\mathbf{T}(\mathbb{A})g]$. We fix the following notation:

$$\begin{aligned}
B_{\mathbf{G},f} &\coloneqq \xi_{1,f} B_f \xi_{1,f}^{-1} \cap \xi_{2,f} B_f \xi_{2,f}^{-1} < \mathbf{G}(\mathbb{A}_f),\\
B_{\mathbf{G},f}^{+} &\coloneqq B_{\mathbf{G},f} \cap \mathbf{G}(\mathbb{A}_f)^{+} < \mathbf{G}(\mathbb{A}_f)^{+},\\
B_{\mathbf{T},f} &\coloneqq g_f B_f g_f^{-1} \cap \mathbf{T}(\mathbb{A}_f) < \mathbf{T}(\mathbb{A}_f),\\
B_{\mathbf{M},f} &\coloneqq B_{\mathbf{G},f} \times B_{\mathbf{T},f} < \mathbf{M}(\mathbb{A}_f),\\
B_{\mathbf{M},f}^{\dagger} &\coloneqq B_{\mathbf{G},f}^{+} \times B_{\mathbf{T},f} < \mathbf{M}(\mathbb{A}_f)^{\dagger}.
\end{aligned}$$

Each of these is a compact-open subgroup of the appropriate group.

Definition 8.20. Let $\gamma \in (\mathbf{G} \times \mathbf{G})(\mathbb{Q})$ and $\varkappa \in \mathbf{G}(\mathbb{Q})$. Define the following functions:

$$\begin{aligned}
f_{\gamma,\varkappa}(l,t) &\coloneqq \mathbb{1}_{B'_f}\left((\varkappa l)^{-1}\gamma t\right),\\
f_{\gamma}(l,t) &\coloneqq \mathbb{1}_{B'_f}\left(l^{-1}\gamma t\right).
\end{aligned}$$

The former is a $B_{\mathbf{M},f}^{\dagger}$-invariant function on $\mathbf{M}(\mathbb{A}_f)^{\dagger}$, and the latter is a $B_{\mathbf{M},f}$-invariant function on $\mathbf{M}(\mathbb{A}_f)$.

8.7.1. *Intersection numbers.*

Lemma 8.21. *Let $B = B_\infty \times B_f \subset \mathbf{G}(\mathbb{A})$ be an identity neighborhood such that $B_f \subseteq \mathbf{G}(\mathbb{A}_f)$ is contained in the union of all compact-open subgroups. Then each coset from ${\mathbf{M}(\mathbb{A}_f)}/{B_{\mathbf{M},f}}$ contains at most two cosets from ${\mathbf{G}(\mathbb{Q})\mathbf{M}(\mathbb{A}_f)^{\dagger}}/{B_{\mathbf{M},f}^{\dagger}}$, where we consider $\mathbf{G}$ as a subgroup of $\mathbf{M} = \mathbf{G} \times \mathbf{T}$ in the usual way.*

Proof. Let $\varkappa_{-1} \in \mathbf{B}^{\times}(\mathbb{Q})$ be an element with reduced norm -1 if it exists, i.e., if $\mathbf{B}$ is split at ∞; see Section 2.3. By abuse of notation we use the notation $\varkappa_{-1}$ also for the corresponding element in $\mathbf{G}(\mathbb{Q})$.

Fix $m \in \mathbf{M}(\mathbb{A}_f)$. Assume $\varkappa_i m_i^{\dagger} B_{\mathbf{M},f}^{\dagger} \subseteq m B_{\mathbf{M},f}$, where $\varkappa_i \in \mathbf{G}(\mathbb{Q})$, $m_i^{\dagger} \in \mathbf{M}(\mathbb{A}_f)^{\dagger}$ for $i \in \{1,2\}$. We show that either $\varkappa_1 \in \varkappa_2 \mathbf{G}(\mathbb{Q})^{+}$ or $\varkappa_1 \in \varkappa_2 \varkappa_{-1} \mathbf{G}(\mathbb{Q})^{+}$ if $\varkappa_{-1}$ exists.

Our assumption implies that there is some $b \in B_{\mathbf{M},f}$ such that $\varkappa_1 m_1^{\dagger} = \varkappa_2 m_2^{\dagger} b$. We apply the injective map

$$\operatorname{Nrd}\colon \mathbf{G}(\mathbb{A}_f) \to {\mathbb{A}_f^{\times}}/{\mathbb{A}_f^{\times 2}}.$$

We deduce $\mathrm{Nrd}(\varkappa_2^{-1}\varkappa_1) = \mathrm{Nrd}(b)$. The condition satisfied by B_f implies that $\mathrm{Nrd}\, b \in \widehat{\mathbb{Z}}^\times \mod \left(\mathbb{A}_f^\times\right)^2$. Thus the valuation of $\mathrm{Nrd}(\varkappa_2^{-1}\varkappa_1)$ is even at each finite place. As $\mathrm{Nrd}(\varkappa_2^{-1}\varkappa_1)$ is rational, it must belong to $\pm\mathbb{Q}^{\times 2}$, i.e., it is either trivial in ${}^{\mathbb{A}_f^\times}/_{\mathbb{A}_f^{\times 2}}$ or has the same class as $\varkappa_{-1}$. Because Nrd has kernel $\mathbf{G}(\mathbb{A}_f)^+$, we conclude that $\varkappa_2^{-1}\varkappa_1$ either belongs to $\mathbf{G}(\mathbb{Q})^+$ or to $\varkappa_{-1}\mathbf{G}(\mathbb{Q})^+$. The claim follows immediately. □

Remark 8.22. It is not difficult to analyze for a specific B exactly how many cosets from ${}^{\mathbf{G}(\mathbb{Q})\mathbf{M}(\mathbb{A}_f)^\dagger}/_{B^\dagger_{\mathbf{M},f}}$ are contained in a fixed coset from ${}^{\mathbf{M}(\mathbb{A}_f)}/_{B_{\mathbf{M},f}}$. This would allow converting several of the inequalities in what follows to equalities. As this of no practical use to us we do not pursue it here.

Proposition 8.23. *Let $[\gamma] \in W_\mathbb{Q}$. Then*

$$\sum_{\varkappa\in\mathbf{G}(\mathbb{Q})/\mathbf{G}(\mathbb{Q})^+} \mathrm{RO}^f_{\gamma,\varkappa}(B) \leq 2\mathrm{m}_{\mathbf{G}(\mathbb{A}_f)}(B_{\mathbf{G},f})\mathrm{m}_{\mathbf{T}(\mathbb{A}_f)}(B_{\mathbf{T},f})N_{[\gamma]},$$

where $N_{[\gamma]}$ is the number of times the $\mathbf{M}(\mathbb{A}_f)$ orbit of γ intersects B'_f modulo $B_{\mathbf{M},f}$.

Proof. For any $\varkappa \in {}^{\mathbf{G}(\mathbb{Q})}/_{\mathbf{G}(\mathbb{Q})^+}$, we can write

$$\mathrm{RO}^f_{\gamma,\varkappa}(B) = \mathrm{m}_{\mathbf{G}(\mathbb{A}_f)}(B_{\mathbf{G},f})\mathrm{m}_{\mathbf{T}(\mathbb{A}_f)}(B_{\mathbf{T},f})N_{\gamma,\varkappa},$$

where $N_{\gamma,\varkappa}$ is the number of times the $\mathbf{M}(\mathbb{A}_f)^\dagger$ orbit of $\varkappa^{-1}.\gamma$ intersect B'_f modulo $B^\dagger_{\mathbf{M},f}$. This follows from the $B^\dagger_{\mathbf{M},f}$-invariance of $f_{\gamma,\varkappa}$. The proof is finished by applying Lemma 8.21. □

Lemma 8.24. *Consider the action of the algebraic group $\mathbf{M} = \mathbf{G}\times\mathbf{T}$ on the affine variety $\mathbf{G}$ where the $\mathbf{G}$-coordinate acts trivially and the $\mathbf{T}$-coordinate acts by conjugation. The contraction morphism* ctr: $\mathbf{G}\times\mathbf{G}\to\mathbf{G}$ *defined by $(g_1, g_2) \mapsto g_1^{-1}g_2$ is an $\mathbf{M}$-equivariant morphism of affine varieties.*

The set

$$B'_f = \xi_{1,f}B_f g_f^{-1} \times \xi_{2,f}B_f g_f^{-1}s_f^{-1} \subset (\mathbf{G}\times\mathbf{G})(\mathbb{A}_f)$$

is $B_{\mathbf{M},f}$-invariant and the contraction map is a bijection between ${}_{B_{\mathbf{M},f}}\backslash^{B'_f}$ and its image ${}_{\mathrm{Ad}\,B_{\mathbf{T},f}}\backslash^{\mathrm{ctr}(B'_f)}$. In particular, for any $\gamma = (\gamma_1,\gamma_2) \in (\mathbf{G}\times\mathbf{G})(\mathbb{Q})$,

$$N_{[\gamma]} = \#\left({}_{\mathrm{Ad}\,B_{\mathbf{T},f}}\backslash^{\mathrm{Ad}\,\mathbf{T}(\mathbb{A}_f)\,\mathrm{ctr}(\gamma)\cap\mathrm{ctr}(B'_f)}\right).$$

Proof. The map ctr: ${}_{B_{\mathbf{M},f}}\backslash^{B'_f} \to {}_{\mathrm{Ad}\,B_{\mathbf{T},f}}\backslash^{\mathrm{ctr}(B'_f)}$ is obviously surjective and we need only prove injectivity. Assume

$$th_1^{-1}h_2t^{-1} = h_1'^{-1}h_2' \tag{28}$$

for some $(h_1, h_2), (h'_1, h'_2) \in (\mathbf{G} \times \mathbf{G})(\mathbb{A}_f)$ and $t \in \operatorname{Ad} B_{\mathbf{T},f}$. We need to prove that there is some $l \in B_{\mathbf{G},f}$ so that $l h_i t^{-1} = h'_i$ for $i \in \{1, 2\}$.

Set $l = h'_1 t h_1^{-1} \in \mathbf{G}(\mathbb{A}_f)$. Then (28) implies that $l h_i t^{-1} = h'_i$ for $i \in \{1, 2\}$. To see that $l \in B_{\mathbf{G},f}$, notice that for $i \in \{1, 2\}$,

$$l = h'_i t h_i^{-1} \in \xi_{i,f} B_f B_{\mathbf{T},f} B_f^{-1} \xi_{i,f}^{-1} = \xi_{i,f} B_f \xi_{i,f}^{-1}$$

and $B_{\mathbf{G},f} = \bigcap_{i \in \{1,2\}} \xi_{i,f} B_f \xi_{i,f}^{-1}$. □

8.7.2. *Matching intersections to pairs of integral ideals.* The last lemma indicates that $N_{[\gamma]}$ can be computed by understanding intersections of $\operatorname{Ad} B_{\mathbf{T},f}$-orbits on $\operatorname{Ad} \mathbf{T}(\mathbb{A}_f)\mathbf{G}(\mathbb{Q}) \subset \mathbf{G}(\mathbb{A}_f)$ with $\operatorname{ctr}(B'_f)$. We restrict to the case $B_{\mathbf{T},f} = K_{\mathbf{T},f}$ and develop arithmetic invariants, refining results of GIT, to detect these intersections.

Definition 8.25. Recall that $K_{\mathbf{T},f} \coloneqq \mathbf{T}(\mathbb{A}_f) \cap g_f K_f g_f^{-1}$. We construct a function

$$\operatorname{inv}_f \colon {}_{\operatorname{Ad} K_{\mathbf{T},f}}\backslash^{\mathbf{G}(\mathbb{A}_f)} \to {}_{\mathbb{Q}^{\times\Delta}}\backslash^{\mathscr{J}(\Lambda)_0 \times \mathscr{J}(\Lambda)_0}$$

in the following manner.

Let $[h_f] = [(h_v)_{v \neq \infty}] \in {}_{\operatorname{Ad} K_{\mathbf{T},f}}\backslash^{\mathbf{G}(\mathbb{A}_f)}$. For all $v \neq \infty$, choose a representative of h_v in $\mathbf{B}^\times(\mathbb{Q}_v)$ and write it in coordinates using Proposition 5.19:

$$h_v = \mathbb{Q}_v^\times \begin{pmatrix} \alpha_v & \beta_v \upsilon_v \tau_v \\ {}^\sigma\beta_v / \tau_v & {}^\sigma\alpha_v \end{pmatrix},$$

where $\alpha_v, \beta_v \in E_v$ and υ_v, τ_v are as in the proposition. Now define $\operatorname{inv}_f([h_f])$ as

$$\operatorname{inv}_f\left([h_f]\right) = \left(\widetilde{\operatorname{idl}}(\alpha_v), \widetilde{\operatorname{idl}}(\beta_v)\right) = \left(\bigcap_{v \neq \infty} \alpha_v \Lambda_v, \bigcap_{v \neq \infty} \beta_v \Lambda_v\right).$$

This pair of ideals is obviously well defined up to multiplication by a common ideal of the form $\bigcap_{v \neq \infty} q_v \Lambda_v$, where $q_v \in \mathbb{Q}_v^\times$ for all $v \neq \infty$. Because $\mathbb{Q}$ has class number one, this is equivalent to multiplying the ideals by the same element of $\mathbb{Q}^\times$.

The map inv_f is also invariant under conjugation by $K_{\mathbf{T},f}$. Recall that $\operatorname{cbd}(x) = x / {}^\sigma x$ for all $x \in E_v^\times$. Conjugating by an element of $K_{\mathbf{T},f}$ is equivalent to multiplying β_v by an element of $\operatorname{cbd}(\Lambda_v^\times) \subset \Lambda_v^\times$ and hence defines the same fractional ideals.

Definition 8.26.

(1) Set $\mathbf{G}(\mathbb{A})_{\text{accessible}} \coloneqq \operatorname{Ad} \mathbf{T}(\mathbb{A})\mathbf{G}(\mathbb{Q})$. This is an $\operatorname{Ad} \mathbf{T}(\mathbb{A})$-invariant subset of $\mathbf{G}(\mathbb{A})$.

(2) Define the map

$$\mathrm{inv}\colon {}_{\operatorname{Ad}\mathbf{T}(\mathbb{R})\operatorname{Ad}K_{\mathbf{T},f}}\backslash^{\mathbf{G}(\mathbb{A})_{\text{accessible}}} \to {}_{\mathbb{Q}^\times}\backslash^{\mathscr{J}(\Lambda)_0\times\mathscr{J}(\Lambda)_0}$$

by evaluating inv_f from Definition 8.25 on the finite part.

(3) For each v, we have defined a map $\pi_{\mathbf{W}}\colon {}_{\operatorname{Ad}\mathbf{T}(\mathbb{Q}_v)}\backslash^{\mathbf{G}(\mathbb{Q}_v)} \to \mathbf{W}(\mathbb{Q}_v)$. For an element of $\mathbf{G}(\mathbb{A})_{\text{accessible}}$, the map $\pi_{\mathbf{W}}$ maps each place to the *same* value in $\mathbf{W}(\mathbb{Q})$. We thus have a well-defined map

$$\pi_{\mathbf{W}}\colon {}_{\operatorname{Ad}\mathbf{T}(\mathbb{A})}\backslash^{\mathbf{G}(\mathbb{A})_{\text{accessible}}} \to \mathbf{W}(\mathbb{Q}),$$

which send an element to the common value of $\pi_{\mathbf{W}}$ evaluated at any place.

The next proposition is a central observation relating cross-correlation to shifted convolution sums of ideal counting functions.

Proposition 8.27. *Let $[\mathbf{T}(\mathbb{A})g]$ be a homogeneous toral set. Let*

$$[h] \in {}_{\operatorname{Ad}\mathbf{T}(\mathbb{R})\operatorname{Ad}K_{\mathbf{T},f}}\backslash^{\mathbf{G}(\mathbb{A})_{\text{accessible}}}$$

such that $\mathrm{inv}(h) \in {}_{\mathbb{Q}^\times}\backslash^{\mathscr{J}(\Lambda)_0\times\mathscr{J}(\Lambda)}$, *i.e.,* $h \notin \mathbf{T}(\mathbb{Q})$. *Then there is a faithful action of* $\prod_{v\neq\infty} H^1(\mathfrak{G},\Lambda_v^\times)$ *on* $\mathrm{inv}^{-1}([h])$, *and the number of orbits is* ≤ 8.

Proof. Our strategy is to show that $(\mathrm{inv}\times\pi_{\mathbf{W}})^{-1}([h])$ is a principal homogeneous space for $\prod_{v\neq\infty} H^1(\mathfrak{G},\Lambda_v^\times)$ and to prove that $\pi_{\mathbf{W}}\left(\mathrm{inv}^{-1}(\mathrm{inv}([h]))\right)$ contains at most eight elements.

Denote $\mathbb{Q}^\times(\mathfrak{a},\mathfrak{b}) := \mathrm{inv}([h])$. We first show there are at most eight possible elements in $\pi_{\mathbf{W}}\left(\mathrm{inv}^{-1}\left(\mathbb{Q}^\times(\mathfrak{a},\mathfrak{b})\right)\right)$. Proposition 6.15 implies that an element of $\mathbf{W}(\mathbb{Q})$ is uniquely determined by the values in E of the regular functions $\vartheta_1^2\det^{-1}, \vartheta_1\vartheta_2\det^{-1}, \psi\det^{-1}$. We define a map $\mathbf{W}(\mathbb{Q})\to\mathbb{P}^2(E)$ by

$$w \mapsto [\vartheta_1^2\det^{-1}(w) : \vartheta_1\vartheta_2\det^{-1}(w) : \psi\det^{-1}(w)].$$

We claim that this map is injective on $\mathbf{W}(\mathbb{Q})$. A priori it defines the values of the necessary functions only up to a common multiplicative constant. But the value of this constant is uniquely determined by the syzygy

$$\vartheta_1\vartheta_2\det^{-1} - \psi\det^{-1} = 1.$$

Let $t\gamma t^{-1} \in \mathbf{G}(\mathbb{A})_{\text{accessible}}$, $\gamma\in\mathbf{G}(\mathbb{Q})$, $t\in\mathbf{T}(\mathbb{A})$ represent an element in $\mathrm{inv}^{-1}\left(\mathbb{Q}^\times(\mathfrak{a},\mathfrak{b})\right)$. For any $v\neq\infty$, the pair of fractional ideal $(\mathfrak{a},\mathfrak{b})$ corresponds to some local ideals $(\alpha_v\Lambda_v, \beta_v\Lambda_v)$ such that

$$\begin{pmatrix} \alpha_v & \beta_v\upsilon_v\tau_v \\ {}^\sigma\beta_v/\tau_v & {}^\sigma\alpha_v \end{pmatrix}$$

is in the $\operatorname{Ad}\mathbf{T}(\mathbb{Q}_v)$-orbit of γ. We can calculate the coordinate functions of $[\gamma]\in\mathbf{W}(\mathbb{Q})$ using this matrix, but their values depend on the specific representative in $\alpha_v\Lambda_v^\times$, $\beta_v\Lambda_v^\times$. Nevertheless, the local principle ideals $(\alpha_v\Lambda_v, \beta_v\Lambda_v)$ uniquely determine, for any $w \mid v$, the w-part of

$$[\vartheta_1^2 \det{}^{-1}(\gamma) : \vartheta_1\vartheta_2 \det{}^{-1}(\gamma) : \psi \det{}^{-1}(\gamma)],$$

and this hold for all finite E-places w. As all the entries are in E they are uniquely defined up to an element of $\mathcal{O}_E^\times$. Moreover, the last two entries are in $\mathbb{Q}$ so they are defined up to an element in $\mathbb{Z}^\times$. In total we are left with $4 \cdot 2 = 8$ possibilities at most for the homogeneous vector above. Hence there are at most eight possible corresponding points in $\mathbf{W}(\mathbb{Q})$.

Next we need to study the fiber of $\mathrm{inv} \times \pi_{\mathbf{W}}$. Let

$$\left(\mathbb{Q}^\times(\mathfrak{a}, \mathfrak{b}), [\gamma]\right) \in \operatorname{Im} \mathrm{inv} \times \pi_{\mathbf{W}},$$

where $\mathfrak{a} \in \mathcal{J}_0(\Lambda)$, $\mathfrak{b} \in \mathcal{J}(\Lambda)$ and $\gamma \in \mathbf{G}(\mathbb{Q})$.

First assume that $\gamma \notin w_{\mathbf{T}}\mathbf{T}(\mathbb{Q})$. Due to Proposition 6.3, the fiber in $\mathbf{G}(\mathbb{A})_{\text{accessible}}$ of $\pi_{\mathbf{W}}$ over this point is $\operatorname{Ad}\mathbf{T}(\mathbb{A})\gamma$. In coordinates we can write

$$\operatorname{Ad}\mathbf{T}(\mathbb{A})\gamma = \left\{ \mathbb{Q}_v^\times \begin{pmatrix} a & \epsilon b \operatorname{cbd}(x_v) \\ {}^\sigma b \, {}^\sigma\operatorname{cbd}(x_v) & {}^\sigma a \end{pmatrix}_v \;\middle|\; x = (x_v)_v \in \prod_v E_v^\times \right\}, \tag{29}$$

where $a \in E$ and $b \in E^\times$. The pertinent fiber of $\mathrm{inv} \times \pi_{\mathbf{W}}$ in $\mathbf{G}(\mathbb{A})_{\text{accessible}}$ is $\operatorname{Ad}\mathbf{T}(\mathbb{A})\gamma \cap \mathrm{inv}^{-1}\left(\mathbb{Q}^\times(\mathfrak{a}, \mathfrak{b})\right)$.

Otherwise, if $\gamma \in w_{\mathbf{T}}\mathbf{T}(\mathbb{Q})$, then $\mathfrak{a} = 0$. For any

$$h' = t'\gamma' t'^{-1} \in \mathrm{inv}^{-1}\left(\mathbb{Q}^\times(0, \mathfrak{b})\right),$$

we have $\gamma' = \gamma t_{\mathbb{Q}}$ with $t_{\mathbb{Q}} \in \mathbf{T}(\mathbb{Q})$. Moreover, because γ and γ' have the same invariants, we see that $t_{\mathbb{Q}} \in \mathbf{T}(\mathbb{Q}) \cap K_{\mathbf{T},f} = \mathbf{T}(\mathbb{Z}) \simeq {}_{\mathbb{Z}^\times}\backslash\Lambda^\times$. In particular, using Hilbert's Satz 90 for E we see that $\gamma' \in \operatorname{Ad}\mathbf{T}(\mathbb{Q})\gamma$.

In both cases we conclude the fiber is equal to $\operatorname{Ad}\mathbf{T}(\mathbb{A})\gamma \cap \mathrm{inv}^{-1}\left(\mathbb{Q}^\times(\mathfrak{a}, \mathfrak{b})\right)$. These are all the elements of (29) satisfying

$$\left(\widetilde{\mathrm{idl}}(a), \widetilde{\mathrm{idl}}\left(\frac{\epsilon}{\upsilon_v\tau_v} b \operatorname{cbd}(x)\right)\right) \in \mathbb{Q}^\times(\mathfrak{a}, \mathfrak{b}). \tag{30}$$

Denote $\mathfrak{b}' \coloneqq \widetilde{\mathrm{idl}}\left(\frac{\epsilon}{\upsilon_v\tau_v} b\right) \in \mathcal{J}(\Lambda)$. Then there is some $q \in \mathbb{Q}^\times$ such that

$$\widetilde{\mathrm{idl}}(\operatorname{cbd}(x)) = q\frac{\mathfrak{b}}{\mathfrak{b}'}.$$

The left-hand side is a fractional Λ-ideal of norm 1, hence $q = \pm q_0$ where $q_0 = \sqrt{\operatorname{Nr}\mathfrak{b}' / \operatorname{Nr}\mathfrak{b}}$. In particular, $\widetilde{\mathrm{idl}}(\operatorname{cbd}(x)) = q_0\frac{\mathfrak{b}}{\mathfrak{b}'}$.

Fix $c_v \in E_v^\times$ for all $v \neq \infty$ such that $\widetilde{\mathrm{idl}}((c_v)_v) = q_0\frac{\mathfrak{b}}{\mathfrak{b}'}$. For each $v \neq \infty$, the element c_v has norm 1, so by Hilbert's Satz 90 there is some $y_v \in E_v^\times$ satisfying $c_v = \operatorname{cbd}(y_v)$. The condition (30) is equivalent to

$$\forall v \neq \infty\colon\ \operatorname{cbd}(x_v) \in \operatorname{cbd}(y_v)\Lambda_v^\times \Leftrightarrow \operatorname{cbd}(x_v y_v^{-1}) \in \Lambda_v^{(1)}.$$

Thus the fiber in $\mathbf{G}(\mathbb{A})_{\text{accessible}}$ is a principal homogeneous space for $\operatorname{Ad}\mathbf{T}(\mathbb{R}) \times \prod_{v\neq\infty} \Lambda_v^{(1)}$. Writing these in coordinates we see that the fiber in $\mathbf{G}(\mathbb{A})_{\text{accessible}}$ is a principal homogeneous space for $\operatorname{Ad}\mathbf{T}(\mathbb{R}) \times \prod_{v\neq\infty} \Lambda_v^{(1)}$.

The quotient of the fiber by the action of $\operatorname{Ad}\mathbf{T}(\mathbb{R}) \operatorname{Ad} K_{\mathbf{T},f}$ is a principle homogeneous space for $\prod_{v\neq\infty} \operatorname{cbd}(\Lambda_v^\times)\backslash^{\Lambda_v^{(1)}} \simeq \prod_{v\neq\infty} H^1(\mathfrak{G}, \Lambda_v^\times)$ as claimed. □

Corollary 8.28. *Let* $[h] \in {}_{\operatorname{Ad}\mathbf{T}(\mathbb{R}) \operatorname{Ad} K_{\mathbf{T},f}}\backslash^{\mathbf{G}(\mathbb{A})_{\text{accessible}}}$ *such that* $\operatorname{inv}(h) \in {}_{\mathbb{Q}^\times}\backslash^{\mathcal{J}(\Lambda)_0 \times \mathcal{J}(\Lambda)}$, *i.e.,* $h \notin \mathbf{T}(\mathbb{Q})$. *Then*

$$\#\operatorname{inv}^{-1}([h]) \ll \operatorname{Pic}(\Lambda)[2].$$

Proof. The proof follows from Proposition 8.27 above and Corollary A.12. □

Lemma 8.29. *Let* $h = t\gamma t^{-1} \in \mathbf{G}(\mathbb{A})_{\text{accessible}}$, $t \in \mathbf{T}(\mathbb{A})$, $\gamma \in \mathbf{G}(\mathbb{Q})$. *If* $\operatorname{inv}(h) = \mathbb{Q}^\times(\mathfrak{a}, \mathfrak{b})$, *then*

(1) $[\mathfrak{a}] = 1$ *in* $\operatorname{Pic}(\Lambda)$ *if* $\mathfrak{a} \neq 0$,
(2) $[\mathfrak{b}\mathfrak{e}] \in \operatorname{Pic}(\Lambda)^2$ *if* $\mathfrak{b} \neq 0$.

Proof. Fixing representatives for γ and h_v for all places $v \neq \infty$, we have

$$\begin{pmatrix} \alpha_v & \beta_v \upsilon_v \tau_v \\ {}^\sigma\beta_v/\tau_v & {}^\sigma\alpha_v \end{pmatrix} = q_v \begin{pmatrix} a & \epsilon b \frac{\lambda_v}{{}^\sigma\lambda_v} \\ {}^\sigma b \frac{{}^\sigma\lambda_v}{\lambda_v} & {}^\sigma a \end{pmatrix},$$

where $\alpha_v, \beta_v \in E_v$, $\lambda_v \in E_v^\times$, $q_v \in \mathbb{Q}_v^\times$ and $a, b \in E^\times$. The ideals $\mathfrak{a}$ and $\mathfrak{e}\mathfrak{b}$ either vanish or their classes in $\operatorname{Pic}(\Lambda)$ satisfy

$$\begin{aligned} [\mathfrak{a}] &= (\alpha_v)_{v\neq\infty} \mod \mathbb{Q}^\times \prod_{v\neq\infty} \Lambda_v^\times = (a)_{v\neq\infty} \mod \mathbb{Q}^\times \prod_{v\neq\infty} \Lambda_v^\times = 1, \\ [\mathfrak{b}\mathfrak{e}] &= (\beta_v \upsilon_v \tau_v)_{v\neq\infty} \mod \mathbb{Q}^\times \prod_{v\neq\infty} \Lambda_v^\times \\ &= (\epsilon b \frac{\lambda_v}{{}^\sigma\lambda_v})_{v\neq\infty} \mod \mathbb{Q}^\times \prod_{v\neq\infty} \Lambda_v^\times \in \operatorname{Pic}(\Lambda)^2. \end{aligned}$$ □

Proposition 8.30. *Fix* $(x_v)_v \in \mathbf{G}(\mathbb{A}_f)$. *Let* $B_v = \Omega_v$ *for* $v \neq p_1$ *and* $B_{p_1} = K_{p_1}^{(-n,n)} \subset \Omega_{p_1}$ *for some* $n \in \mathbb{N}$. *If* $h \in \mathbf{G}(\mathbb{A})_{\text{accessible}}$ *is contained in* $\prod_v g_v B_v^{-1} x_v B_v g_v^{-1} s_v^{-1}$, *then*

$$\operatorname{inv}(h) = \mathbb{Q}^\times \widehat{\Lambda}(\mathfrak{a} \cdot \mathfrak{s}^{-1}, \mathfrak{b} \cdot {}^\sigma\mathfrak{s}^{-1})$$

for some $\mathfrak{a}, \mathfrak{b} \in \mathcal{J}_0(\Lambda)$ *satisfying*

(1) $\mathfrak{a}, \mathfrak{b} \subseteq \Lambda$,
(2) $p_1^n \mid \mathfrak{b}$,
(3) $\operatorname{Nr}(\mathfrak{a}) - \upsilon \operatorname{Nr}(\mathfrak{b}) = \operatorname{sign}(\operatorname{Nrd}(x_\infty))\, \mathfrak{d}_f(x_f)|D|$,

(4) $\operatorname{Nr}(\mathfrak{a}) \leq 2^8\, \mathfrak{d}_\infty(x_\infty)\, \mathfrak{d}_f(x_f)|D|$,
(5) $[\mathfrak{a}] = [\mathfrak{s}]$ *in* $\operatorname{Pic}(\Lambda)$ *if* $\mathfrak{a} \neq 0$,
(6) $[\mathfrak{b}] \in [\mathfrak{s}\mathfrak{e}]^{-1}\operatorname{Pic}(\Lambda)^2$ *if* $\mathfrak{b} \neq 0$.

Proof. For each place v, choose a representative $r_v \in \mathbf{B}^\times(\mathbb{Q}_v) \cap \mathbb{O}_v$ of $g_v^{-1} h_v s_v g_v \in \Omega_v x_v \Omega_v$ satisfying the conclusion of Proposition 5.21. For $v = p_1$, let r_v satisfy the stronger conclusions of Proposition 5.23. The element $g_v r_v g_v^{-1}$ belongs to $g_v \mathbb{O}_v g_v^{-1}$ and has same reduced norm as r_v, i.e., $|\operatorname{Nrd} g_v r_v g_v^{-1}|_v = \mathfrak{d}_v(x_v)^{-1}$ for $v \neq \infty$ and $|\operatorname{Nrd} g_\infty r_\infty g_\infty^{-1}| \geq 2^{-8}\mathfrak{d}_\infty(x_\infty)^{-1}$. We can use this to represent h_v in $\mathbf{B}^\times(\mathbb{Q}_v)$ as

$$h_v = \mathbf{Z}(\mathbb{Q}_v)\begin{pmatrix} \alpha_v s_v^{-1} & \beta_v {}^\sigma s_v{}^{-1} \upsilon_v \tau_v \\ {}^\sigma\beta_v s_v^{-1}/\tau_v & {}^\sigma\alpha_v {}^\sigma s_v{}^{-1} \end{pmatrix}, \tag{31}$$

where $\alpha_v, \beta_v \in \widehat{\Lambda}_v$ due to Proposition 5.19. The definition of inv implies that $\operatorname{inv}(h) = \mathbb{Q}^\times(\mathfrak{a}_0, \mathfrak{b}_0)$, where $\mathfrak{a}_0 = \bigcap_{v\neq\infty} \alpha_v s_v^{-1}\Lambda_v$ and $\mathfrak{b}_0 = \bigcap_{v\neq\infty} \beta_v {}^\sigma s_v{}^{-1}\Lambda_v$. Define $\widehat{\mathfrak{a}} := \bigcap_{v\neq\infty} \alpha_v \Lambda_v$ and $\widehat{\mathfrak{b}} := \bigcap_{v\neq\infty} \beta_v \Lambda_v$. Then $\widehat{\mathfrak{a}}, \widehat{\mathfrak{b}} \subseteq \widehat{\Lambda}$. Finally, set $\mathfrak{a} := \widehat{\Lambda}^{-1}\widehat{\mathfrak{a}}$ and $\mathfrak{b} := \widehat{\Lambda}^{-1}\widehat{\mathfrak{b}}$. Then $\mathfrak{a}, \mathfrak{b} \subseteq \Lambda$ and $\mathfrak{a}_0 = \widehat{\Lambda}\mathfrak{a}\mathfrak{s}^{-1}$, $\mathfrak{b}_0 = \widehat{\Lambda}\mathfrak{b}{}^\sigma\mathfrak{s}^{-1}$.

We conclude that $\operatorname{inv}(h) = \mathbb{Q}^\times\widehat{\Lambda}(\mathfrak{a}\mathfrak{s}^{-1}, \mathfrak{b}{}^\sigma\mathfrak{s}^{-1})$. Obviously (1) is satisfied and (5), (6) are simply a restatement of Lemma 8.29.

We claim that

$$\begin{aligned} \operatorname{Nr}(\widehat{a}) &= \operatorname{sign}(\operatorname{Nrd}(x_\infty))\, \mathfrak{d}_f(x_f)\vartheta_1\vartheta_2 \det{}^{-1}(h), \\ \upsilon \operatorname{Nr}(\widehat{b}) &= \operatorname{sign}(\operatorname{Nrd}(x_\infty))\, \mathfrak{d}_f(x_f)\psi \det{}^{-1}(h). \end{aligned} \tag{32}$$

For any prime p, the p-part of (32) follows by calculating $\vartheta_1\vartheta_2\det^{-1}$ and $\psi\det^{-1}$ using the representative in (31) for the corresponding non-archimedean v. To establish (32) with the correct signs, calculate $\vartheta_1\vartheta_2\det^{-1}$ and $\psi\det^{-1}$ using the representative in (31) for $v = \infty$.

Recall that $\operatorname{Nrd}(\mathfrak{a}) = \operatorname{Nrd}(\widehat{\Lambda}^{-1}\widehat{\mathfrak{a}}) = |D|\operatorname{Nrd}(\widehat{\mathfrak{a}})$ and similarly for $\mathfrak{b}$. Claim (3) follows from (32) and the syzygy $\vartheta_1\vartheta_2\det^{-1} - \psi\det^{-1} = 1$. The archimedean bound $|\vartheta_1\vartheta_2\det^{-1}(h)| \leq 2^8\,\mathfrak{d}_\infty(x_\infty)$ follows from using (31) for $v = \infty$, Proposition 5.15 and the inequality $|\operatorname{Nrd} g_v r_v g_v^{-1}| \geq 2^{-8}\,\mathfrak{d}_\infty(x_\infty)^{-1}$. Claim (4) follows from this bound and (32).

To prove (2) we use the conclusions of Proposition 5.23. Rewrite

$$g_{p_1}\mathbb{O}_{p_1}^{(-n,n)}g_{p_1}^{-1} = \bigcap_{k=-n}^{n} t^k g_{p_1}\mathbb{O}_{p_1}^{(-n,n)}g_{p_1}^{-1}t^{-k},$$

where $t = g_{p_1}\lambda(p_1)g_{p_1}^{-1} \in \mathbf{T}(\mathbb{Q}_{p_1})$. Using the freedom in the choice of λ we can assume

$$t \in \mathbb{Q}_{p_1}^\times \begin{pmatrix} \pi & 0 \\ 0 & {}^\sigma\pi \end{pmatrix},$$

where $\pi \in E_{p_1}$ is a uniformizer for one of the two maximal ideals of $\mathcal{O}_{p_1}$ and ${}^\sigma\pi$ is a uniformizer for the second one. Because $r_{p_1} \in t^k g_{p_1}\mathbb{O}_{p_1}^{(-n,n)}g_{p_1}^{-1}t^{-k}$ for all $-n \leq k \leq n$, using Proposition 5.19 we conclude that

$$\mathscr{D}_{p_1}\beta_{p_1} \in \bigcap_{k=-n}^{n} \frac{{}^{\sigma}\pi^k}{\pi^k}\Lambda_{p_1} = p_1^n \Lambda_{p_1}. \tag{33}$$

Because $\mathfrak{b} = \widehat{\Lambda}^{-1}\widehat{\mathfrak{b}} = \bigcap_v \mathscr{D}_{p_1}\beta_v\Lambda_v$, Claim (1) follows from (33). □

Remark 8.31. Elements h with $\mathrm{inv}(h) = \mathbb{Q}^\times\widehat{\Lambda}(\mathfrak{a}\cdot\mathfrak{s}^{-1}, 0)$ in the Proposition above corresponds to $\mathbf{M}(\mathbb{A}_f)$-orbits of elements $\gamma \in (\mathbf{G}\times\mathbf{G})(\mathbb{Q})$ with stabilizer $\mathbf{M}_\gamma \simeq \mathbf{T}$.

We know from Lemma 8.14 and Proposition 7.8 that the contribution of these elements to the cross-correlation should vanish if the minimal norm of an integral ideal in the Picard class $[\mathfrak{s}]$ is $\geq C$ for some constant C depending only on ξ. If $\mathrm{sign}(\mathrm{Nrd}(\mathrm{ctr}(\xi)_\infty)) = 1$, this seems to contradict the proposition above, which states that such γ correspond to integral ideals $\mathfrak{a}$ with $\mathrm{Nr}(\mathfrak{a}) = \mathrm{sign}(\mathrm{Nrd}(\mathrm{ctr}(\xi)_\infty))\,\mathfrak{d}_f(\mathrm{ctr}(\xi)_f)|D|$, which for $|D|$ large enough is bigger then C.

The contradiction is resolved by observing that in this case $\mathrm{ctr}(\gamma) \in \mathbf{T}(\mathbb{Q})$, and in the language of the proof above we know that not only $\widehat{\mathfrak{a}} \subseteq \widehat{\Lambda}$ but also $\widehat{\mathfrak{a}} \subseteq \Lambda$. This implies that $\mathfrak{a} \subset \widehat{\Lambda}^{-1} \subsetneq \Lambda$, and if

$$\mathrm{Nr}(\mathfrak{a}) = \mathrm{sign}(\mathrm{Nrd}(\mathrm{ctr}(\xi)_\infty))\,\mathfrak{d}_f(\mathrm{ctr}(\xi)_f)|D|,$$

then $\widehat{\Lambda}\mathfrak{a}$ is an integral ideal in the class $[\mathfrak{s}]$ of norm

$$\mathrm{sign}(\mathrm{Nrd}(\mathrm{ctr}(\xi)_\infty))\,\mathfrak{d}_f(\mathrm{ctr}(\xi)_f),$$

which does not grow to infinity with $|D|$.

This reasoning can also be used to exclude the situation

$$\mathrm{inv}(h) = \mathbb{Q}^\times(0, \mathfrak{b}\cdot{}^{\sigma}\mathfrak{s}^{-1}),$$

i.e., $\mathbf{M}_\gamma \simeq \mu_2$. These unnecessary terms will have negligible contribution to the shifted convolution sum, and we do not take the extra effort to write them off. The essential part is that the contribution of a non-compact stabilizer to the geometric expansion is eliminated in Lemma 8.14.

Proposition 8.32. *Let* $h \in \mathbf{G}(\mathbb{A})_{\mathrm{accessible}}$ *and* $\mathrm{inv}(h) = \mathbb{Q}^\times\widehat{\Lambda}(\mathfrak{a}\mathfrak{s}^{-1}, \mathfrak{b}^{\sigma}\mathfrak{s}^{-1})$ *be as in Proposition 8.30 above. Let $p \mid D$ be an odd prime where* $\mathbf{B}$ *splits. Denote by v the place associated to p, and recall from Proposition 8.27 that* $H^1(\mathfrak{G}, \Lambda_v^\times)$ *acts faithfully on* $\mathrm{inv}^{-1}(\mathrm{inv}(h))$.

Let $-1 \in H^1(\mathfrak{G}, \Lambda_v^\times)$ *be the unique non-trivial element; cf. Lemmata A.13 and A.14. If* $\mathrm{ord}_p \mathrm{Nr}(\mathfrak{b}) < \mathrm{ord}_p D$, *then* $-1.h_v \notin g_v B_v^{-1} x_v B_v g_v^{-1} s_v^{-1}$.

Proof. Assume in contradiction that both h_v and $-1.h_v$ belong to

$$g_v B_v^{-1} x_v B_v g_v^{-1} s_v^{-1}.$$

We write $(\pm 1.h_v)s_v$ in coordinates as in (31) in the proof of Proposition 8.30 above (notice that $\upsilon_v = 1$ in the split case):

$$(\pm 1.h_v)s_v = \mathbf{Z}(\mathbb{Q}_v)\begin{pmatrix} \alpha_v & \pm\beta_v\tau_v \\ \pm{}^{\sigma}\beta_v/\tau_v & {}^{\sigma}\alpha_v \end{pmatrix}.$$

Above we have used the fact from Lemmata A.13 and A.14 that for odd residue characteristic, the unique non-trivial cohomology class is represented by $-1 \in \Lambda_v^{(1)}$. The explicit form of the action of $H^1(\mathfrak{G}, \Lambda_v^\times)$ is evident from the proof of Proposition 8.27.

Because the matrix on the right-hand side above belongs to $g_v\mathbb{O}_v g_v^{-1}$ for both $(\pm 1.h_v)s_v$, Proposition 5.12 implies that

$$\pm\beta_v - {}^{\sigma}\alpha_v \in \Lambda_v \implies 2\beta_v \in \Lambda_v \implies \beta_v \in \Lambda_v.$$

In the last implication we have used once more that the residue characteristic is odd.

Following the definition of $\mathfrak{b}$ in the proof of Proposition 8.30 above, we see that the completion of $\mathfrak{b}$ at v is $\mathscr{D}_v\beta_v\Lambda_v \subseteq \mathscr{D}_v\Lambda_v$. Hence $\operatorname{ord}_p \operatorname{Nr}\mathfrak{b} \geq \operatorname{ord}_p D$ in contradiction to the assumption. □

8.8. *Proof of Theorem* 8.7. We need one last lemma before we can proceed to the proof the theorem.

Lemma 8.33. *For any $n \in \mathbb{N}$ and any $a \in A_{p_1}$,*

$$\frac{\mathrm{m}_{\mathbf{G}(\mathbb{Q}_{p_1})}\left(K_{p_1} \cap aK_{p_1}a^{-1}\right)}{\mathrm{m}_{\mathbf{G}(\mathbb{Q}_{p_1})}\left(K_{p_1}^{(-n,n)} \cap aK_{p_1}^{(-n,n)}a^{-1}\right)} = p_1^{2n}.$$

Proof. Let $\mathscr{A}$ be the apartment in $\mathscr{B}_{p_1}$ stabilized by A_{p_1}. We fix an orientation on $\mathscr{A}$ and enumerate all vertices in $\mathscr{A}$ consecutively according to the adjacency $\ldots, x_{-1}, x_0, x_1, \ldots$ in such a way that x_0 is the vertex stabilized by K_{p_1} and $a.x_0 = x_k$ for some $k \geq 0$.

Because $\mathbf{G}(\mathbb{Q}_p)$ acts by simplicial automorphism, we have that $K_{p_1} \cap aK_{p_1}a^{-1}$ is the stabilizer in $\mathbf{G}(\mathbb{Q}_p)$ of the finite path $[x_0, \ldots, x_k]$ in $\mathscr{A}$ and $K_{p_1}^{(-n,n)} \cap aK_{p_1}^{(-n,n)}a^{-1}$ is the stabilizer in $\mathbf{G}(\mathbb{Q}_p)$ of the finite path

$$[x_{-n}, \ldots, x_0, \ldots x_k, \ldots, x_{n+k}].$$

In particular,

$$\begin{aligned}
&\frac{\mathrm{m}_{\mathbf{G}(\mathbb{Q}_{p_1})}\left(K_{p_1} \cap aK_{p_1}a^{-1}\right)}{\mathrm{m}_{\mathbf{G}(\mathbb{Q}_{p_1})}\left(K_{p_1}^{(-n,n)} \cap aK_{p_1}^{(-n,n)}a^{-1}\right)} \\
&= \left[\operatorname{Stab}_{\mathbf{G}(\mathbb{Q}_p)}\left([x_0, \ldots, x_k]\right) : \operatorname{Stab}_{\mathbf{G}(\mathbb{Q}_p)}\left([x_{-n}, \ldots, x_0, \ldots x_k, \ldots, x_{n+k}]\right)\right] \\
&= \#\left(\operatorname{Stab}_{\mathbf{G}(\mathbb{Q}_p)}\left([x_0, \ldots, x_k]\right).\left([x_{-n}, \ldots, x_0] \cup [x_k, \ldots, x_{k+n}]\right)\right).
\end{aligned}$$

Because the action is by simplicial automorphism and $\mathscr{B}_{v_1}$ is a tree for any $h \in \mathrm{Stab}_{\mathbf{G}(\mathbb{Q}_p)}([x_0, \ldots, x_k])$, the position of $h.([x_{-n}, \ldots, x_0] \cup [x_k, \ldots, x_{k+n}])$ is completely determined by the position of $h.x_{-n}$ and $h.x_{k+n}$.

Let y_1 be a vertex so that $d(x_0, y_1) = d(x_0, x_{-n})$ and the geodesic connecting x_0 and y_1 does not pass through x_1. Similarly, let y_2 be a vertex so that $d(x_k, y_2) = d(x_k, x_{k+n})$ and the geodesic connecting x_k and y_2 does not pass through x_{k-1}. We can use the strong transitivity of the action to show the existence of an element $h \in \mathbf{G}(\mathbb{Q}_p)$ so that $h.[x_0, \ldots, x_k] = [x_0, \ldots, x_k]$ and $h.x_{-n} = y_1$ and $h.x_{k+n} = y_2$. Counting pairs of vertices y_1, y_2 as above we deduce

$$\#\left(\mathrm{Stab}_{\mathbf{G}(\mathbb{Q}_p)}([x_0, \ldots, x_k]) . ([x_{-n}, \ldots, x_0] \cup [x_k, \ldots, x_{k+n}])\right) = p_1^{2n}. \qquad \square$$

Proof of Theorem 8.7. We begin with some necessary measure computations. For the torus $\mathbf{T}$, we have $g_\infty^{-1}\mathbf{T}(\mathbb{R})g_\infty = K_\infty$ and hence $\mathbf{T}(\mathbb{R}) \subset g_\infty \Omega_\infty g_\infty^{-1}$. Denote $a = \lambda(p_1)$ as in Definition 5.22. Then for every $m \in \mathbb{Z}$,

$$g_{p_1}^{-1}\mathbf{T}(\mathbb{Q}_{p_1})g_{p_1} \cap a^m K_{p_1} a^{-m} = A_{p_1} \cap a^m K_{p_1} a^{-m} = A_{p_1} \cap K_{p_1}.$$

Hence $\mathbf{T}(\mathbb{Q}_{p_1}) \cap g_{p_1} K_{p_1}^{(-n,n)} g_{p_1}^{-1} = \mathbf{T}(\mathbb{Q}_{p_1}) \cap g_{p_1} K_{p_1} g_{p_1}^{-1}$. $\square$

We conclude that

$$\begin{aligned}&\mathrm{vol}\left([\mathbf{T}(\mathbb{A})g]\right)^{-1}\\ &\quad = \mathrm{m}_{\mathbf{T}(\mathbb{R})}\left(\mathbf{T}(\mathbb{R})\right) \mathrm{m}_{\mathbf{T}(\mathbb{Q}_{p_1})}\left(g_{p_1} K_{p_1}^{(-n,n)} g_{p_1}^{-1}\right) \prod_{v \neq \infty, p_1} \mathrm{m}_{\mathbf{T}(\mathbb{Q}_v)}\left(g_v K_v g_v^{-1}\right).\end{aligned}$$

For $\mathbf{G}^\Delta$, we use Lemma 8.33 and the condition $\mathrm{ctr}(\xi)_{p_1} \in A_{p_1}$ to deduce that

$$\begin{aligned}\mathrm{vol}\left(\left[\mathbf{G}^\Delta(\mathbb{A})^+\xi\right]\right)^{-1} p_1^{-2n} \geq\ & \mathrm{m}_{\mathbf{G}(\mathbb{R})^+}\left(\xi_{1,\infty}\Omega_\infty^2\xi_{1,\infty}^{-1} \cap \xi_{2,\infty}\Omega_\infty^2\xi_{2,\infty}^{-1}\right)\\ &\cdot \mathrm{m}_{\mathbf{G}(\mathbb{Q}_{p_1})}\left(K_{p_1}^{(-n,n)} \cap \mathrm{ctr}(\xi)_{p_1} K_{p_1}^{(-n,n)} \mathrm{ctr}(\xi)_{p_1}^{-1}\right)\\ &\cdot \prod_{v \neq \infty, p_1} \mathrm{m}_{\mathbf{G}(\mathbb{Q}_v)^+}\left(g_v K_v g_v^{-1}\right).\end{aligned}$$

The inequality above can be replaced by $\asymp_{\Omega_\infty}$ because of (10) from Section 2.4.5.

Using Corollary 8.16, Lemma 8.18, Proposition 8.23 and the volume computations above, we can write

$$\begin{aligned}\mathrm{Cor}[\mu, \nu](B) \ll\ & \mathrm{vol}\left([\mathbf{T}(\mathbb{A})g]\right)^{-1} \mathrm{vol}\left(\left[\mathbf{G}^\Delta(\mathbb{A})^+\xi\right]\right)^{-1} p_1^{-2n}\\ &\cdot \sum_{\substack{[\gamma] \in W_\mathbb{Q}\\ \psi \det^{-1}(\gamma) \neq 0}} N_{[\gamma]} \cdot \mathbb{1}_{g_\infty \Omega_\infty \mathrm{ctr}(\xi)_\infty \Omega_\infty g_\infty^{-1}}(\mathrm{ctr}(\gamma)_\infty).\end{aligned}$$

We now need to bound the bottom sum over $[\gamma] \in W_\mathbb{Q}$. Using Lemma 8.24, we know that the last sum is equal to the number of $\mathrm{Ad}\,\mathbf{T}(\mathbb{R})\,\mathrm{Ad}\,K_{\mathbf{T},f}$-orbits intersecting $\mathrm{ctr}(B')$ in the set $\mathbf{G}(\mathbb{A})_{\mathrm{accessible}}$. To each such intersection we can associate a pair of integral ideals satisfying the conclusions of Proposition 8.30.

Due to Propositions 8.27 and 8.32 we know that the map *intersection* $\mapsto$ $(\mathfrak{a},\mathfrak{b})$ where $\mathfrak{a},\mathfrak{b}$ are the integral ideals of Proposition 8.30 is at most $8r(\mathrm{Nr}(\mathfrak{b}))$ to 1.

For each pertinent pair of ideals $(\mathfrak{a},\mathfrak{b})$, set $\mathfrak{b}=p_1^n\mathfrak{b}'$, where $0\neq\mathfrak{b}'\subseteq\Lambda$ is an integral invertible Λ-ideal satisfying $[\mathfrak{b}']\in[p_1^n\mathfrak{s}\mathfrak{c}]^{-1}\,\mathrm{Pic}(\Lambda)^2$. The claim follows when we notice that $g_{[\mathfrak{s}]}(x)f_{[p_1^n\mathfrak{s}\mathfrak{c}]^{-1}}\left(\frac{x-\omega D}{\upsilon p_1^{2n}}\right)$ with $x\leq\kappa|D|$ is exactly the number of pairs of ideals $(\mathfrak{a},p_1^n\mathfrak{b}')$ satisfying the conclusions of Proposition 8.30 and $\mathrm{Nr}(\mathfrak{a})=x$.

9. Sums of multiplicative functions over polynomials in two variables

In this section we generalize the results of Shiu and Nair [Shi80], [Nai92] to sums of the form

$$\sum_{(x,y)\in\mathscr{E}\cap\mathbb{Z}^2} f(Q(x,y)),$$

where f is a slowly growing non-negative multiplicative function, $Q\in\mathbb{Z}[x,y]$ and $\mathscr{E}\subsetneq\mathbb{R}^2$ is a closed smooth convex domain. Similar sums for homogeneous polynomials in two variables over axis-aligned boxes have been studied in [dlBB06], [dlBT12].

Most of the proof in [Shi80], [Nai92] follows through in higher dimensions even for the case of more general domains as long as good estimates are available for the lattice counting problem.

Nevertheless, the following presentation contains two ideas that seem to be novel even in the 1-variable case. They are essential when we need to apply the sieved upper bound to a family of polynomials Q in a uniform manner. Both of them have to do with the behavior of Q at primes of bad reduction.

The first one is a simple yet crucial observation that the function counting $\mathbb{Z}/_{p^k\mathbb{Z}}$-points on X_Q — the plane curve cutout by Q — can be replaced by a function counting only the points that do not have the maximal possible amount of lifts to $X_Q\left(\mathbb{Z}/_{p^{k+1}\mathbb{Z}}\right)$.

The second one is directly related to the dependence of the upper bound on the singularities of the reduction of X_Q modulo p. The structure of singularities for a 1-variable polynomial modulo p, i.e., 0-dimensional affine scheme of finite type, is simple and can be summarized by the discriminant of the polynomial. The possible singularities of a reduction of a curve, although rather well-understood through resolution of singularities, are significantly more diverse. The most general expression replacing the dependence on the discriminant for polynomials in two variables seems to be a product of values of local Igusa zeta-functions. We chose not to pursue this path here as it does not lends itself easily to applications. Instead, we observe that as long as there is an a priori bound $\#X_Q\left(\mathbb{Z}/_{p^k\mathbb{Z}}\right) \leq Cp^{k(2-r)}$ with $C>0$ and $1\geq r>0$ independent of p^k, our upper bound can be shown to depend only on C and r. Such bounds seem to be easy to establish explicitly, at least for the application at hand. Moreover, this approach generalizes verbatim to polynomials with arbitrary many variables.

Definition 9.1.

(1) For any polynomial in two variables $Q\in\mathbb{Z}[x,y]$ and $a\in\mathbb{N}$, denote by $\rho_Q(a)$ the number of solution in $\mathbb{Z}^2/_{a\mathbb{Z}^2}$ to the equation
$$Q(x,y)\equiv 0 \mod a.$$

(2) Let X_Q be the affine plane curve cutout by Q, i.e.,
$$X_Q\coloneqq \operatorname{Spec}\mathbb{Z}[x,y]/\left\langle Q(x,y)\right\rangle.$$
By definition, $\rho_Q(a)=\left|X_Q\left(\mathbb{Z}/_{a\mathbb{Z}}\right)\right|$.

(3) Fix a prime power p^k. A lift of a point $x\in X_Q\left(\mathbb{Z}/_{p^k\mathbb{Z}}\right)$ is a $\mathbb{Z}/_{p^{k+1}\mathbb{Z}}$-point of X_Q that reduces to x mod p^k.

We split $X_Q\left(\mathbb{Z}/_{p^k\mathbb{Z}}\right)$ into three types of points:
- smooth points — by Hensel's lemma each such point has exactly p lifts;
- singular points with a lift, by the Taylor polynomial formula each such point has exactly p^2 lifts;
- singular points without a lift.

(4) We denote by $\widetilde{\rho}_Q(p^k)$ the number of $\mathbb{Z}/_{p^k\mathbb{Z}}$-points on X_Q that are either smooth or have no lift. We extend $\widetilde{\rho}_Q$ to a multiplicative function on $\mathbb{N}$ in the regular fashion. Obviously, $\widetilde{\rho}_Q(a)\leq\rho_Q(a)$ for all a.

(5) Denote by $\rho_Q^{\text{sing}}(p^k)$ the number of $\mathbb{Z}/_{p^k\mathbb{Z}}$-points on X_Q that are not smooth, i.e., either having 0 or p^2 lifts.

The following lemmata are elementary properties of points on curves over congruence classes of integers.

Lemma 9.2 (DeMillo-Lipton-Schwartz-Zippel Lemma). *Let $0\neq Q\in\mathbb{Z}[x,y]$. Then the inequality $\rho_Q(p)\leq\deg(Q)p$ holds for any prime $p\nmid Q$.*

Proof. This has been proven in [Sch80], and a slightly weaker bound has been shown in [DJL78], [Zip79]. See [Tao14, Lemma 1.2] for a streamlined proof. □

Lemma 9.3. *Let $0\neq Q\in\mathbb{Z}[x,y]$. Then*
$$\widetilde{\rho}_Q(p^k)=\rho_Q(p^k)-\frac{\rho^{\text{sing}}(p^{k+1})}{p^2}.$$

Proof. This follows immediately from the observation that the points in $X_Q\left(\mathbb{Z}/_{p^{k+1}}\mathbb{Z}\right)$ that reduce to smooth points modulo p^n are exactly the smooth points modulo p^{n+1}. □

In the following two definitions we describe the objects appearing in our main sieving theorem.

Definition 9.4.

- We say that a convex domain $\mathscr{E} \subset \mathbb{R}^2$ is C^2 if its boundary is a twice continuously differentiable curve. We then denote by $R_{\max}(\mathscr{E})$ the maximum of the radius of curvature of the boundary of $\mathscr{E}$ and by $A(\mathscr{E})$ the area of $\mathscr{E}$. If no confusion arises, we shall use the shorthand $R_{\max}$ for $R_{\max}(\mathscr{E})$.
- Let $C_l, \theta_l > 0$. We denote by $\mathscr{L}(C_l, \theta_l)$ the collection of C^2 convex planar domains $\mathscr{E}$ such that for any $a \in \mathbb{N}$ and $(x_0, y_0) \in \mathbb{Z}^2$, if $A(\mathscr{E}) \geq a^2$, then

$$\left|\#\left(a^{-1}(\mathscr{E} - (x_0, y_0)) \cap \mathbb{Z}^2\right) - a^{-2}A(\mathscr{E})\right| \leq C_l \left(R_{\max}(\mathscr{E})/a\right)^{\theta_l}.$$

Remark 9.5. The Van der Corput bound [vdC20] implies that for any $\varepsilon > 0$, there is $C_l > 0$ depending on ε such that any C^2 convex domain belongs to $\mathscr{L}(C_l, 2/3 + \varepsilon)$.

The bound of Huxley [Hux03, Prop. 5 and Th. 5] for lattice points in C^3 planar domains implies that for any $\varepsilon > 0$, there is $C_l > 0$ depending on ε such that all ellipses belong to $\mathscr{L}(C_l, 131/208 + \varepsilon)$. A suitable generalization of the Gauss circle problem conjecture should imply that the constant 131/208 can be replaced by 1/2, at least for ellipses defined by integral binary quadratic forms.

Definition 9.6. Let $A \geq 1$ and $B, \varepsilon > 0$. We say that a multiplicative function $f\colon \mathbb{N} \to \mathbb{R}$ is of class $\mathscr{M}(A, B, \varepsilon)$ if it is non-negative, and for any integer $n > 0$,

$$f(n) \leq \min\left(A^{\Omega(n)}, Bn^{\varepsilon}\right).$$

THEOREM 9.7. *Let $\mathscr{E} \subset \mathbb{R}^2$ be planar domain of class $\mathscr{L}(C_l, \theta_l)$ for $C_l, \theta_l > 0$. Denote by $A(\mathscr{E})$ the area of $\mathscr{E}$, let $R_{\max}$ be the maximal radius of curvature of the boundary, and assume $R_{\max}^{\theta_l} \leq A(\mathscr{E})^{1-3\eta}$ for some $1/2 > \eta > 0$.*

Let $Q \in \mathbb{Z}[x, y]$ such that there are $C > 0, 1 \geq r > 0$ satisfying $\widetilde{\rho}_Q(p^k) \leq Cp^{k(2-r)}$ for all prime powers p^k. Let $X \geq 1$ be a constant satisfying

$$\max\left\{|Q(x,y)| \mid (x,y) \in \mathscr{E} \cap \mathbb{Z}^2\right\} \leq X \leq A(\mathscr{E})^{\delta}$$

for some $\delta > 0$.

Let f be a non-negative multiplicative function of class $\mathscr{M}(A,B,\varepsilon)$ for some $A\geq 1$, $B>0$ and $0<\varepsilon<\min\{r,\eta r/(4\delta)\}$. Then

$$\sum_{(x,y)\in\mathscr{E}\cap\mathbb{Z}^2} f\left(Q(x,y)\right)\ll A(\mathscr{E})\prod_{\substack{\deg(Q)<p\leq X\\ p\nmid Q}}\left(1-\frac{\rho_Q(p)}{p^2}\right)\sum_{a\leq X}\frac{f(a)\widetilde{\rho}_Q(a)}{a^2}, \tag{34}$$

where the implicit constant depends only on $C_l, A, B, \varepsilon, \deg(Q), C, r, \eta, \delta$.

9.1. *Notation.* We introduce several notation to be used in the section. For an integer $n>1$, denote by $\omega(n)$ the number of distinct prime factors of n, and let $\Omega(n)$ be the number of prime factors counted with multiplicity. Denote also by $P^+(n), P^-(n)$ the largest and the smallest prime divisor of n respectively. It shall also be useful to define $P^+(1)=1, P^-(1)=\infty$.

For any two integers a,b, we write $a\mid b^\infty$ if the prime support of a is contained in the prime support of b. Lastly, we denote by $\gcd(a,b^\infty)$ the product of all primes powers dividing a for primes appearing in the support of b.

9.2. *Sieving.* The following lemma is a straightforward generalization of the lower bound in [GKM15, Lemma 2.1].

Lemma 9.8. *Let $g\colon\mathbb{N}\to\mathbb{R}$ be a multiplicative function such that there is some $d>0$ so that $0\leq g(p)\leq d$ for all primes p. Then for any $z>1$,*

$$\sum_{n\leq z}\mu(n)^2\frac{g(n)}{n}\gg_d\prod_{d<p\leq z}\left(1-\frac{g(p)}{p}\right)^{-1}. \tag{35}$$

Proof. As the left-hand side of (35) is supported on the square-free numbers, we can assume without loss of generality that g is completely multiplicative. Define a new completely multiplicative function h by $h(p)=d-g(p)$. The Dirichlet convolution $g*h$ is a multiplicative function that satisfies $g*h(p)=g(1)h(p)+g(p)h(1)=d$ for any prime p. Hence for any square-free integer n, we have $g*h(n)=d^{\omega(n)}$. This implies

$$\sum_{n\leq z}\mu(n)^2\frac{g(n)}{n}\cdot\sum_{n\leq z}\mu(n)^2\frac{h(n)}{n}\geq\sum_{n\leq z}\mu(n)^2\frac{d^{\omega(n)}}{n}\gg_d(\log z)^d. \tag{36}$$

On the other hand,

$$\sum_{n\leq z}\mu(n)^2\frac{h(n)}{n}\leq\prod_{p\leq z}\left(1+\frac{h(p)}{p}\right)\ll_d\prod_{d<p\leq z}\left(1-\frac{h(p)}{p}\right)^{-1}.$$

Hence

$$\begin{aligned}
&\left(\sum_{n\le z}\mu(n)^2\frac{h(n)}{n}\right)^{-1}\cdot\prod_{d<p\le z}\left(1-\frac{g(p)}{p}\right)\\
&\gg_d \prod_{d<p\le z}\left(1-\frac{d-g(p)}{p}\right)\left(1-\frac{g(p)}{p}\right) \qquad (37)\\
&=\prod_{d<p\le z}\left(1-\frac{d}{p}+\frac{dg(p)-g(p)^2}{p^2}\right)\ge\prod_{d<p\le z}\left(1-\frac{d}{p}\right)\gg_d(\log z)^{-d}.
\end{aligned}$$

The claim now follows by multiplying inequality (36) by (37). □

The following result is where we apply a sieve. As we require only upper bounds, we use the large sieve due to its great generality.

Lemma 9.9. *Let $Q\in\mathbb{Z}[x,y]$ be a polynomial. Let $\mathscr{E}\subset\mathbb{R}^2$ be a domain of class $\mathscr{L}(C_l,\theta_l)$. If*

$$1\le z\le\min\left\{\left(\frac{A(\mathscr{E})}{R_{\max}^{\theta_l}}\right)^{1/5},A(\mathscr{E})^{1/2}\right\},$$

then

$$\begin{aligned}
S&:=\left|\left\{(x,y)\in\mathscr{E}\cap\mathbb{Z}^2\mid P^-(Q(x,y))\ge z\right\}\right|\\
&\ll_{\deg(Q),C_l}A(\mathscr{E})\prod_{\deg(Q)<p\le z}\left(1-\frac{\rho_Q(p)}{p^2}\right).
\end{aligned}$$

Remark 9.10. The exponent 1/5 in the level of distribution is certainly far from optimal, yet for our application any positive exponent suffices.

Proof. The inequality is trivially true if there is $p\mid Q$ such that $p\le z$; hence we assume this is not the case.

We use the large sieve in the setup of Kowalski [Kow08]. Our sieve setting is

$$\left(\mathbb{Z}^2,\text{primes},\mathbb{Z}^2\to{\mathbb{Z}^2}/{p\mathbb{Z}^2}\right),$$

and the siftable set is $\mathscr{E}_{\mathbb{Z}}:=\mathscr{E}\cap\mathbb{Z}^2\subset\mathbb{Z}^2$ with the counting measure.

We choose our sieve support to be the set of square-free positive integers $\le z$. The large sieve inequality as presented in [Kow08, Prop. 2.3] implies that

$$\begin{aligned}
&S\le\Delta H^{-1},\\
&H:=\sum_{n\le z}\mu(n)^2\prod_{p\mid n}\frac{\rho_Q(p)}{p^2-\rho_Q(p)}, \qquad (38)
\end{aligned}$$

where Δ is the large sieve constant that we bound from above using the equidistribution method as in [Kow08, §2.13]. For any integer $n\le A(\mathscr{E})^{1/2}$ and any

$y \in {}^{\mathbb{Z}^2}/_{n\mathbb{Z}^2}$, define the discrepancy

$$r_n(y) := \left|\mathscr{E} \cap \left(n\mathbb{Z}^2 + y\right)\right| - n^{-2}|\mathscr{E}_{\mathbb{Z}}|.$$

The assumption $\mathscr{E} \in \mathscr{L}(C_l, \theta_l)$ implies for $\mathscr{E}$ and $n^{-1}(\mathscr{E} - y)$, whose areas are ≥ 1, that

$$|r_n(y)| \leq C_l \left(\frac{R_{\max}}{n}\right)^{\theta_l}.$$

We use the orthonormal base of characters for finite abelian groups and bound Δ using [Kow08, Cor. 2.13]

$$\begin{aligned}\Delta - |\mathscr{E}_{\mathbb{Z}}| &\leq \max_{m \leq z} \sum_{n \leq z} \sum_{y \in {}^{\mathbb{Z}^2}/_{[m,n]\mathbb{Z}^2}} n \left|r_{[m,n]}(y)\right| \\ &\leq C_l \max_{m \leq z} \sum_{n \leq z} n[m,n]^2 \left(\frac{R_{\max}}{[m,n]}\right)^{\theta_l} \\ &\leq C_l R_{\max}^{\theta_l} z^2 \sum_{n \leq z} n^2 \ll C_l R_{\max}^{\theta_l} z^5 \leq C_l A(\mathscr{E}),\end{aligned}$$

where in the last inequality we have used the upper bound assumption on z. Applying the lattice count bound to $|\mathscr{E}_{\mathbb{Z}}|$ we deduce that $\Delta \ll_{C_l} A(\mathscr{E})$.

We bound H below by

$$H \geq \sum_{n \leq z} \mu(n)^2 \prod_{p|n} \frac{\rho_Q(p)}{p^2}.$$

Next we apply Lemma 9.8 to the multiplicative function $\rho_Q(n)/n$ that is bounded by Lemma 9.2 to deduce

$$H \gg_{\deg(Q)} \prod_{\deg(Q) < p \leq z} \left(1 - \frac{\rho_Q(p)}{p^2}\right)^{-1}.$$

The claim follows by combining the bounds on H and Δ with (38). □

9.3. *Extending the level of distribution.* The range of z where the lemma above is applicable is very restricted. The following results show that we can actually take this range to be any power of $A(\mathscr{E})$ if we are willing to pay a price in the constant depending only on the exponent.

LEMMA 9.11. *Let $Q \in \mathbb{Z}[x,y]$ be a polynomial. Then for any $z \geq 1$, $s > 0$,*

$$\prod_{\deg(Q) < p \leq z^{1/s}} \left(1 - \frac{\rho_Q(p)}{p^2}\right) \ll_{\deg(Q)} s^{\deg(Q)} \prod_{\substack{\deg(Q) < p \leq z \\ p \nmid Q}} \left(1 - \frac{\rho_Q(p)}{p^2}\right).$$

Proof. The proof of [Nai92, Lemma 2(i)] applies when combined with Lemma 9.2. □

LEMMA 9.12. *Let $5 \geq \eta > 0$ and $\varsigma_0 > 0$. In the setting of Lemma 9.9 above, if $R_{\max}^{\theta_l} \leq A(\mathscr{E})^{1-\eta}$ and $1 \leq z \leq A(\mathscr{E})^{\varsigma_0}$, then*

$$S \ll_{\deg(Q),C_l,\eta,\varsigma_0} A(\mathscr{E}) \prod_{\deg(Q)<p\leq z} \left(1 - \frac{\rho_Q(p)}{p^2}\right).$$

Proof. The statement is trivial $\exists p \leq z$ such that $p \mid Q$, hence assume the contrary. Assume $z > A(\mathscr{E})^{\eta/5}$, as otherwise Lemma 9.9 applies directly. Applying Lemma 9.9 for $z_0 = A(\mathscr{E})^{\eta/5} \leq \min\left\{\left(\frac{A(\mathscr{E})}{R_{\max}^{\theta_l}}\right)^{1/5}, A(\mathscr{E})^{1/2}\right\}$, we deduce that

$$S \ll_{\deg(Q),C_l} A(\mathscr{E}) \prod_{\deg(Q)<p\leq A(\mathscr{E})^{\eta/5}} \left(1 - \frac{\rho_Q(p)}{p^2}\right),$$

and the claim follows from Lemma 9.11 with $s = 5\varsigma_0/\eta$. □

9.4. *The sieve bound for values in a homogeneous arithmetic progressions.* We now generalize these results to subsets of points where the polynomial value is divisible by a fixed integer.

LEMMA 9.13. *Let $Q \in \mathbb{Z}[x,y]$ be a polynomial. Let $\mathscr{E} \subset \mathbb{R}^2$ be a domain of class $\mathscr{L}(C_l,\theta_l)$. Fix $1/2 > \eta > 0$, $\varsigma > 0$, and assume $R_{\max}^{\theta_l} \leq A(\mathscr{E})^{1-3\eta}$. Then for any $a, z \in \mathbb{N}$ such that $a \leq A(\mathscr{E})^{\eta}$ and $1 \leq z \leq A(\mathscr{E})^{\varsigma}$,*

$$\begin{aligned} S :=& \Big|\Big\{(x,y) \in \mathscr{E} \cap \mathbb{Z}^2 \mid a|Q(x,y),\ \gcd(a, Q(x,y)/a) = 1 \\ &\qquad\qquad\qquad \text{and } P^-(Q(x,y)/a) \geq z\Big\}\Big| \\ &\ll_{\deg(Q),C_l,\eta,\varsigma} \frac{A(\mathscr{E})\widetilde{\rho}_Q(a)}{a^2} \prod_{\substack{\deg(Q)<p\leq z\\ p\nmid a}} \left(1 - \frac{\rho_Q(p)}{p^2}\right).\end{aligned}$$

Proof. The statement is trivial if there is $p \leq z$ such that $p \nmid a$ and $p \mid Q$, so we assume the contrary. Let $(x_0, y_0) \in {\mathbb{Z}^2}/{a\mathbb{Z}^2}$ be one of the $\rho_Q(a)$ classes where Q vanishes modulo a. Define $Q_0 \in \mathbb{Z}[x,y]$ by

$$Q(ax + x_0, ay + y_0) = a \cdot Q_0(x,y).$$

Then for any $p \nmid a$, we have $\rho_{Q_0}(p) = \rho_Q(p)$. Notice that if $p^k \parallel a$ and the point $(x_0, y_0) \in X_Q\left(\mathbb{Z}/p^k\mathbb{Z}\right)$ has p^2 lifts, then $p \mid Q_0$. By the assumption $\gcd(a, Q(x,y)/a) = 1$ no point in the sieved set reduces to such (x_0, y_0). Hence it is sufficient to consider only the $\widetilde{\rho}_Q(a)$ classes of points that at all primes are either smooth or have no lift.

We apply Lemma 9.12 to Q_0 and the convex C^2 domain $a^{-1}(\mathscr{E} - (x_0, y_0))$ with area $A(\mathscr{E})/a^2$ and maximal curvature radius $R_{\max}/a$. We take $\varsigma_0 = \frac{\varsigma}{1-2\eta} > 0$.

The first condition of Lemma 9.12 reads

$$(R_{\max}/a)^{\theta_l} \leq A(\mathscr{E})^{1-\eta}/a^{2-2\eta} \Leftrightarrow R_{\max}^{\theta_l} \leq A(\mathscr{E})^{1-\eta}/a^{2-2\eta-\theta_l}. \tag{39}$$

Using the assumption $a \leq A(\mathscr{E})^{\eta}$, we deduce that

$$A(\mathscr{E})^{1-\eta}/a^{2-2\eta-\theta_l} \geq A(\mathscr{E})^{1-\eta-\eta(2-2\eta-\theta_l)} = A(\mathscr{E})^{1-\eta(3-2\eta-\theta_l)} \geq A(\mathscr{E})^{1-3\eta}.$$

Thus (39) is satisfied because of the assumption $R_{\max}^{\theta_l} \leq A(\mathscr{E})^{1-3\eta}$. The second condition of Lemma 9.12 reads

$$1 \leq z \leq \left(\frac{A(\mathscr{E})}{a^2}\right)^{\varsigma_0}. \tag{40}$$

Using the assumption $a \leq A(\mathscr{E})^{\eta}$ we see that

$$\left(\frac{A(\mathscr{E})}{a^2}\right)^{\varsigma_0} \geq A(\mathscr{E})^{(1-2\eta)\varsigma_0} = A(\mathscr{E})^{\varsigma}.$$

Hence condition (40) is satisfied as well.

Summing the bounds we obtain from applying Lemma 9.12 to each of the relevant $\widetilde{\rho}_Q(a)$ residue class and using the fact $\rho_{Q_0}(p) = \rho_Q(p)$ for each $p \nmid a$, we obtain the claimed inequality. □

Corollary to Proof of 9.14. *In the setting of Lemma 9.13 above the following holds*:

$$\left|\left\{(x,y) \in \mathscr{E} \cap \mathbb{Z}^2 \mid a|Q(x,y) \text{ and } P^-(Q(x,y)/a) \geq z\right\}\right| \ll_{\deg(Q),C_l,\eta,\varsigma} \frac{A(\mathscr{E})\rho_Q(a)}{a^2} \prod_{\substack{\deg(Q)<p\leq z \\ p\nmid a}} \left(1 - \frac{\rho_Q(p)}{p^2}\right).$$

Proof. The only place where the condition $\gcd(a, Q(x,y)/a) = 1$ was used was to dispose of the residue classes that do not lift. Hence the proof follows in the same manner except that $\widetilde{\rho}_Q(a)$ is replaced by $\rho_Q(a)$. □

Definition 9.15. For any $Q \in \mathbb{Z}[x,y]$, define the multiplicative function θ_Q by

$$\theta_Q(p^k) = \begin{cases} 1 + 2\frac{\rho_Q(p)}{p^2} & p \nmid Q, \\ 1 & p \mid Q \end{cases}$$

for all primes p and all integers $k \geq 1$.

Write $\theta_Q = 1 * \lambda_Q$. Then by Möbius inversion,

$$\lambda_Q(n) = \begin{cases} \mu(n)^2 \frac{2^{\omega(n)}\rho_Q(n)}{n^2} & \gcd(n,Q) = 1, \\ 0 & \gcd(n,Q) \neq 1. \end{cases}$$

Remark 9.16. If $f \in \mathscr{M}(A, B, \varepsilon)$, then an easy computation shows that for any $\varepsilon' > 0$,

$$f\theta_Q \in \mathscr{M}\left(A', B', \varepsilon + \varepsilon'\right),$$

with $A' \ll_{\deg(Q)} A$ and $B' \ll_{\varepsilon',\deg(Q)} B$.

Corollary 9.17. *The next inequality holds in the setting of Lemma 9.13 above*:

$$S \ll_{\deg(Q),C_l,\eta,\varsigma} \frac{A(\mathscr{E})\widetilde{\rho}_Q(a)}{a^2}\theta_Q(a) \prod_{\substack{\deg(Q)<p\leq z\\ p\nmid\gcd(Q,a)}} \left(1 - \frac{\rho_Q(p)}{p^2}\right).$$

Proof. The proof follows immediately from Lemma 9.13 and the fact that $0 \leq \frac{\rho_Q(p)}{p^2} \leq \frac{1}{2}$ for any $p \geq 2\deg(Q)$, $p \nmid Q$. □

9.5. *Decoupling multiplicative functions.* The following lemma is standard — if not in form, then in function. Although it is not singled as such, this is a main technical tool in [NT98].

Lemma 9.18. *Let g and ψ be non-negative multiplicative functions, and denote $h = 1 * \psi$. Then for any $z \geq 1$,*

$$\sum_{a\leq z} g(a)h(a) \leq \mathfrak{M}_z(g,\psi) \cdot \sum_{a\leq z} g(a)$$

$$\mathfrak{M}_z(g,\psi) := \prod_{p\leq z}\left[1 + \sum_{v=1}^{\log z/\log p} \psi(p^v)\sum_{j=v}^{\infty} g(p^j)\right].$$

Remark 9.19. We can write an upper bound for $\mathfrak{M}_z(g,\psi)$ using h:

$$\mathfrak{M}_z(g,\psi) \leq \prod_{p\leq z}\sum_{j=0}^{\infty} g(p^j)\sum_{v=0}^{j}\psi(p^v) = \prod_{p\leq z}\sum_{j=0}^{\infty} g(p^j)h(p^j).$$

Proof. First we expend h in terms of ψ:

$$\sum_{a\leq z} g(a)h(a) = \sum_{a\leq z}\sum_{k|a}\psi(k)g(a) = \sum_{k\leq z}\sum_{t\leq z/k}\psi(k)g(kt).$$

We decompose each t in the sum above as $t = ln$, where $l = \gcd(t, k^\infty)$. Then the expression above is equal to

$$\sum_{k\leq z}\sum_{t\leq z/k}\psi(k)g(kl)g(n) \leq \left(\sum_{k\leq z}\psi(k)\sum_{l|k^\infty} g(kl)\right)\sum_{n\leq z} g(n).$$

To complete the proof we bound the double sum in the scopes

$$\sum_{k\leq z}\psi(k)\sum_{l|k^\infty} g(kl) \leq \prod_{p\leq z}\left[1 + \sum_{v=1}^{\log z/\log p}\psi(p^v)\sum_{j=v}^{\infty} g(p^j)\right].$$ □

We use the decoupling lemma above to prove the two key results to be used in the proof of Theorem 9.7. The first one shows that on average the product over primes in Lemma 9.13 can be extended to include primes dividing a.

Lemma 9.20. *Let $Q \in \mathbb{Z}[x,y]$ such that there are $C > 0, 1 \geq r > 0$ satisfying $\widetilde{\rho}_Q(p^k) \leq Cp^{k(2-r)}$ for all prime powers p^k. Let f be a non-negative multiplicative function such that $f(n) < Bn^{\varepsilon}$ for some $B > 0$, $r > \varepsilon > 0$ and all n. Then for any $z \geq 1$,*

$$\sum_{a \leq z} \frac{\widetilde{\rho}_Q(a) f(a)}{a^2} \theta_Q(a) \ll_{\deg(Q),B,C,r,\varepsilon} \sum_{a\leq z} \frac{\widetilde{\rho}_Q(a) f(a)}{a^2}.$$

Proof. Apply Lemma 9.18 to $g(a) := f(a)\widetilde{\rho}_Q(a)/a^2 \geq 0$ and $\psi = \lambda_Q$. To complete the proof we need bound $\mathfrak{M}_z(g, \lambda_Q)$.

Using the assumptions we bound

$$f(p^k)\widetilde{\rho}_Q(p^k) \leq BCp^{k(2-r+\varepsilon)}$$

and

$$f(p^2)\rho_Q(p^2) \leq f(p^2)\rho_Q(p)p^2 \leq A^2 \deg(Q) p^3.$$

Because λ_Q is supported on the square-free integers, we see that

$$\begin{aligned}\mathfrak{M}(g,\lambda_Q) &\leq \prod_{p\leq z}\left[1+\sum_{v\geq 1}\lambda_Q(p^v)\sum_{j=v}^{\infty} g(p^j)\right] \leq \prod_{\substack{p\leq z\\ p\nmid Q}}\left(1+2\frac{\rho_Q(p)}{p^2}\sum_{j=1}^{\infty}\frac{BC}{p^{j(r-\varepsilon)}}\right)\\ &\leq \prod_{p<\infty}\left(1+2\deg(Q)BC\frac{1}{p^{1+r-\varepsilon}}\frac{1}{1-p^{-(r-\varepsilon)}}\right) \ll_{\deg(Q),B,C,r-\varepsilon} 1. \qquad \square\end{aligned}$$

We also use Lemma 9.18 to establish a saving for the pertinent sums over smooth integers satisfying $P^+(a) \leq z^{1/s}$ for a fixed $s > 0$. The crux of the following lemma is that it saves an exponent in s, and it will be applied to control a term that grows geometrically in the parameter s.

Lemma 9.21. *Let $Q \in \mathbb{Z}[x,y]$ such that there are $C > 0, 1 \geq r > 0$ satisfying $\widetilde{\rho}_Q(p^k) \leq Cp^{k(2-r)}$ for all prime powers p^k. Let f be a non-negative multiplicative function of class $\mathscr{M}(A,B,\varepsilon)$ with $0 < \varepsilon < r$. Then for any $\alpha, s > 0$, $z > 1$ and $(r-\varepsilon)\log(z)/(2s) \geq \kappa > 0$,*

$$\sum_{\substack{z^{\alpha}\leq a\leq z\\ P^+(a)\leq z^{1/s}}} \frac{\widetilde{\rho}_Q(a)f(a)}{a^2} \ll_{\kappa,A,B,\varepsilon,C,r,\deg(Q)} \exp(-s\alpha\kappa)\sum_{a\leq z}\frac{\widetilde{\rho}_Q(a)f(a)}{a^2}. \tag{41}$$

Remark 9.22. If the curve cutout by Q is smooth over $\mathbb{Q}$, then by Hensel's lemma we have $\rho_Q(p^k) \leq \rho_Q(p)p^{k-1} \leq \deg(Q)p^{k(2-1)}$ for all primes p of good reduction. In this case the constants C, r only depend on the number of points on the curve modulo powers of primes of bad reduction.

Proof. Let $(r-\varepsilon)/2 \geq \beta := \frac{\kappa s}{\log z} > 0$. Then the left-hand side of (41) is bounded above by

$$z^{-\alpha\beta} \sum_{\substack{z^{\alpha} \leq a \leq z \\ P^{+}(a) \leq z^{1/s}}} \frac{\widetilde{\rho}_Q(a) f(a)}{a^2} a^{\beta} \leq z^{-\alpha\beta} \sum_{\substack{a \leq z \\ P^{+}(a) \leq z^{1/s}}} \frac{\widetilde{\rho}_Q(a) f(a)}{a^2} a^{\beta}. \tag{42}$$

Define the non-negative multiplicative function g by $g(a) = f(a)\widetilde{\rho}_Q(a)/a^2$ if $P^{+}(a) \leq z^{1/s}$ and $g(a) = 0$ otherwise. Let ψ be the Möbius inversion of the multiplicative function $a \mapsto a^{\beta}$. An explicit formula for ψ is

$$\psi(p^k) = p^{\beta k} - p^{\beta(k-1)}$$

for all primes p and all $k \geq 0$.

Applying Lemma 9.18 with g and ψ as above we can bound the right-hand side of (42) above by

$$z^{-\alpha\beta} \cdot \mathfrak{M}_z(g, \psi) \sum_{\substack{a \leq z \\ P^{+}(a) \leq z^{1/s}}} \frac{\widetilde{\rho}_Q(a) f(a)}{a^2}.$$

We now wish to estimate $\mathfrak{M}_z(g,\psi)$. Using the fact that g is supported on integers without prime factors bigger than $z^{1/s}$ and Remark 9.19, we deduce

$$\mathfrak{M}_z(g,\psi) \leq \prod_{p \leq z^{1/s}} \left(1 + \sum_{j=1}^{\infty} g(p^j) p^{j\beta}\right). \tag{43}$$

Let $K_0 := \lceil 4/(r-\varepsilon) \rceil > 0$. For any $k \leq K_0$, we estimate $\widetilde{\rho}_Q(p^k) \leq \rho_Q(p) p^{2k-2} \leq \deg(Q) p^{2k-1}$. For $k > K_0$, we use the assumption $\widetilde{\rho}_Q(p^k) \leq C p^{k(2-r)}$. Combined with inequality (43) this implies

$$\log \mathfrak{M}_z(g,\psi) \leq K_0 A^{K_0} \deg(Q) \sum_{p \leq z^{1/s}} \frac{p^{K_0 \beta}}{p} + BC \sum_{p \leq z^{1/s}} \sum_{j=K_0+1}^{\infty} p^{-j(r-\beta-\varepsilon)}. \tag{44}$$

We bound the second summand above using the inequality $r - \beta - \varepsilon \geq (r-\varepsilon)/2 > 0$:

$$\begin{aligned} \sum_{p \leq z^{1/s}} \sum_{j=K_0+1}^{\infty} p^{-j(r-\beta-\varepsilon)} &\leq \sum_{p \leq z^{1/s}} p^{-(K_0+1)(r-\varepsilon)/2} \frac{1}{1 - p^{-(r-\varepsilon)/2}} \\ &\ll_{K_0} \sum_{p \leq z^{1/s}} p^{-K_0(r-\varepsilon)/2} \leq \sum_{p \leq \infty} p^{-2} \ll 1. \end{aligned}$$

We bound the main term in (44) above using the prime number theorem

$$\sum_{p \leq z^{1/s}} \frac{p^{K_0\beta}}{p} = \mathrm{Li}(z^{K_0\beta/s}) + z^{K_0\beta/s} \cdot o_{\log(z)/s}(1) \ll_{K_0} 1.$$

We can now conclude that

$$\mathfrak{M}_z(g,\psi) \ll_{\kappa,A,B,\varepsilon,C,r,\deg(Q)} 1. \qquad \square$$

Finally, the following lemma shows that the sums over extremely smooth integers are completely negligible.

Lemma 9.23. *Let $Q \in \mathbb{Z}[x,y]$ such that there are $C > 0$, $1 \geq r > 0$ satisfying $\widetilde{\rho}_Q(p^k) \leq Cp^{k(2-r)}$ for all prime powers p^k. Then for any $\beta > 0$ and $1 \geq \alpha \geq 0$,*

$$\sum_{\substack{z^\alpha \leq a \leq z \\ P^+(a) \leq \log z \log\log z}} \frac{\widetilde{\rho}_Q(a)}{a^2} \ll_{C,\alpha,\beta} z^{-r\alpha+\beta}. \tag{45}$$

Proof. The assumed upper bound on $\widetilde{\rho}_Q$ implies $\widetilde{\rho_Q}(a)/a^2 \leq C^{\omega(a)}/a^r$ for all $a \in \mathbb{N}$. This can be used to bound the left-hand side of (45) by

$$\sum_{\substack{z^\alpha \leq a \leq z \\ P^+(a) \leq \log z \log\log z}} \frac{C^{\omega(a)}}{a^r}. \tag{46}$$

We apply the standard bound $\omega(a) \leq K \log a / \log\log a$ for some fixed $K > 0$ to deduce that for any $z^\alpha \leq a \leq z$,

$$C^{\omega(a)} \leq z^{K \log C/(\log\log z + \log \alpha)}.$$

We split our calculation into two cases.

(1) If $\log\log z \geq K \log C \cdot 2/\beta - \log \alpha$, then $C^{\omega(a)} \leq z^{\beta/2}$ and we bound (46) by

$$z^{-r\alpha+\beta/2} \sum_{\substack{a \leq z \\ P^+(a) \leq \log z \log\log z}} 1 = z^{-r\alpha+\beta/2} \Psi(z, \log z \log\log z).$$

This case is settled because of the inequality $\Psi(z, \log z \log\log z) \ll_\beta z^{\beta/2}$ which follows from [Shi80, Lemma 1].

(2) On the other hand, if $\log\log z < K \log C \cdot 2/\beta - \log\alpha$, then using the trivial bound $\widetilde{\rho}_Q(a) \leq a^2 \leq z^2 \ll_{C,\alpha,\beta} 1$ we estimate (45) by

$$\sum_{\substack{z^\alpha \leq a \leq z \\ P^+(a) \leq \log z \log\log z}} \frac{\widetilde{\rho}_Q(a)}{a^2} \ll_{C,\alpha,\beta} \sum_{z^\alpha \leq a \leq z} \frac{1}{a^2} \ll z^{-\alpha}. \qquad \square$$

9.6. *Proof of Theorem* 9.7. In this section only all the implicit constants in the $\ll$ notation are allowed to depend on $\eta, A, B, \varepsilon, C, r, \deg(Q), \delta, C_l$ without further notation. Denote $\mathscr{E}_{\mathbb{Z}} := \mathscr{E} \cap \mathbb{Z}^2$. We introduce notation similar to that in [Nai92]. Let $Z := A(\mathscr{E})^\eta$. For any fixed $(x,y) \in \mathscr{E}_{\mathbb{Z}}$, we write a decomposition into prime powers

$$Q(x,y) = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_l^{e_l},$$

where $p_1 < p_2 < \cdots < p_l$. Define $a \coloneqq p_1^{e_1} \cdot \ldots p_j^{e_j}$ so that $a \leq Z$ but $a \cdot p_{j+1}^{e_j+1} > Z$, in particular $a = 1$ if all $p_1^{e_1} > Z$. Let $b \coloneqq Q(x,y)/a$, and set $q \coloneqq p_{j+1}$, $e \coloneqq e_{j+1}$. Because f is multiplicative, we always have $f\left(Q(x,y)\right) = f(a)f(b)$.

Following [Shi80] we split the sum on the left-hand side of (34) into four ranges:

(1) R_1 is the set of all $(x,y) \in \mathscr{E}_{\mathbb{Z}}$ such that $q \geq Z^{1/2}$;
(2) R_2 is the set of all $(x,y) \in \mathscr{E}_{\mathbb{Z}}$ such that $q < Z^{1/2}, a \leq Z^{1/2}$;
(3) R_3 is the set of all $(x,y) \in \mathscr{E}_{\mathbb{Z}}$ such that $q < \log Z \log\log Z, a > Z^{1/2}$;
(4) R_4 is the set of all $(x,y) \in \mathscr{E}_{\mathbb{Z}}$ such that $\log Z \log\log Z \leq q < Z^{1/2}, a > Z^{1/2}$.

Moreover, for any fixed integers a, z, we denote

$$S(a,z) \coloneqq \Big\{(x,y) \in \mathscr{E}_{\mathbb{Z}} \mid a | Q(x,y),\ \gcd(a, Q(x,y)/a) = 1 \\ \text{and } P^-(Q(x,y)/a) \geq z\Big\}.$$

Recall that $\Omega(b)$ is the number of prime factors of b counted with multiplicity. For any $(x,y) \in R_1$, we have

$$Z^{1/2\cdot\Omega(b)} \leq b \leq X \leq A(\mathscr{E})^{\delta},$$

hence $\Omega(b) \ll 1$ and $f(b) \ll 1$. This implies that we have a bound

$$\sum_{(x,y)\in R_1} f\left(Q(x,y)\right) \ll \sum_{a \leq Z} f(a)|S(a, Z^{1/2})|.$$

We can apply Lemma 9.13 with $\varsigma = \delta$ to bound $|S(a, Z^{1/2})|$ from above. Combining this with Corollary 9.17 and Lemma 9.20, we deduce

$$\sum_{(x,y)\in R_1} f\left(Q(x,y)\right) \ll A(\mathscr{E}) \prod_{\deg(Q) < p \leq Z^{1/2}} \left(1 - \frac{\rho_Q(p)}{p^2}\right) \sum_{a \leq Z} \frac{f(a)\widetilde{\rho}_Q(a)}{a^2},$$

which is consistent with the claimed bound due to Lemma 9.11.

Next we make an observation necessary to treat the sums over R_2 and R_3 and that also indicates the natural limit of the theorem. The following lower bound for the right-hand side of (34) holds:

$$\begin{aligned} A(\mathscr{E}) &\prod_{\substack{\deg(Q) < p \leq X \\ p \nmid Q}} \left(1 - \frac{\rho_Q(p)}{p^2}\right) \sum_{a \leq X} \frac{f(a)\widetilde{\rho}_Q(a)}{a^2} \\ &\geq A(\mathscr{E}) \prod_{\substack{\deg(Q) < p \leq X \\ p \nmid Q}} \left(1 - \frac{\deg(Q)}{p}\right) \\ &\gg A(\mathscr{E})/(\log X)^{\deg(Q)} \gg A(\mathscr{E})/(\log A(\mathscr{E}))^{\deg(Q)}. \end{aligned}$$

Thus any bound of the form $\ll A(\mathscr{E})^{1-\varepsilon_0}$ for $\varepsilon_0 > 0$ is consistent with the claim.

For any $(x,y)\in R_2$,

$$Z<aq^e\le Z^{1/2}q^e \implies Z^{1/2}<q^e,$$

but $q<Z^{1/2}$ hence $e\ge 2$. For each prime $p\le Z^{1/2}$, let $e_p\ge 2$ be the minimal integer satisfying $p^{e_p}>Z^{1/2}$. Notice that $p^{e_p}=p^{e_p-1}p\le Z^{1/2}p\le Z=A(\mathscr{E})^{\eta}$, so we can apply Corollary 9.14 with $a=p^{e_p}$. This implies the following bound:

$$\begin{aligned}\sum_{(x,y)\in R_2} f\left(Q(x,y)\right) &\ll X^{\varepsilon}\sum_{p\le Z^{1/2}}\left|\{(x,y)\in\mathscr{E}_{\mathbb{Z}}\mid p^{e_p}|Q(x,y)\}\right| \\ &\ll X^{\varepsilon}A(\mathscr{E})\sum_{p\le Z^{1/2}}\frac{\rho_Q(p^{e_p})}{p^{2e_p}}\ll X^{\varepsilon}A(\mathscr{E})\sum_{p\le Z^{1/2}}\frac{1}{p^{e_p}}.\end{aligned}\tag{47}$$

The latter sum is bounded by

$$\sum_{p\le Z^{1/2}}\frac{1}{p^{e_p}}\le\sum_{p\le Z^{1/4}}\frac{1}{Z^{1/2}}+\sum_{Z^{1/4}<p\le Z^{1/2}}\frac{1}{p^2}\ll Z^{1/4-1/2}+Z^{-1/4}\ll Z^{-1/4}.$$

We conclude from (47) that

$$\sum_{(x,y)\in R_2} f\left(Q(x,y)\right)\ll X^{\varepsilon}A(\mathscr{E})Z^{-1/4}\ll A(\mathscr{E})^{1+\varepsilon\delta-\eta/4}.$$

Because $\varepsilon\delta-\eta/4<0$, this bound saves a power of $A(\mathscr{E})$ and is compatible with the claim.

We proceed to estimate the sums over R_3 using Lemma 9.13:

$$\begin{aligned}\sum_{(x,y)\in R_3} f\left(Q(x,y)\right) &\ll X^{\varepsilon}\sum_{\substack{Z^{1/2}\le a\le Z\\ P^+(a)\le\log Z\log\log Z}}|S(a,1)| \\ &\ll X^{\varepsilon}A(\mathscr{E})\sum_{\substack{Z^{1/2}\le a\le Z\\ P^+(a)\le\log Z\log\log Z}}\frac{\widetilde{\rho}_Q(a)}{a^2}.\end{aligned}$$

Next apply Lemma 9.23 with $\beta=r/4$ to deduce

$$\sum_{(x,y)\in R_3} f\left(Q(x,y)\right)\ll X^{\varepsilon}A(\mathscr{E})Z^{-r/4}\ll A(\mathscr{E})^{1+\delta\varepsilon-\eta r/4},$$

which is consistent with the claim because we have assumed $\delta\varepsilon-\eta r/4<0$.

We split R_4 further according to the value of q. For any integer

$$s_0\coloneqq 2\le s\le s_1\coloneqq\frac{\log Z}{\log\left(\log Z\log\log Z\right)},$$

let R_4^s be the set of $(x,y)\in R_4$ such that $Z^{1/(s+1)}\le q\le Z^{1/s}$. Recalling that q is the smallest prime divisor of b, we see that for $(x,y)\in R_4^s$,

$$Z^{\Omega(b)/(s+1)}\le b\le X\le A(\mathscr{E})^{\delta},$$

hence $\Omega(b) \leq (s+1)\delta/\eta$ and $f(b) \ll A_0^s$, where $A_0 := A^{\delta/\eta}$. We can now write

$$\sum_{(x,y)\in R_4} f\left(Q(x,y)\right) \leq \sum_{s_0\leq s\leq s_1} A_0^s \sum_{\substack{Z^{1/2}\leq a\leq Z\\ P^+(a)\leq Z^{1/s}}} f(a)|S(a,Z^{1/(s+1)})|. \tag{48}$$

Similarly to the case of R_1, we apply Lemma 9.13 with $\varsigma = \delta$ and Corollary 9.17 to bound the right-hand side of (48) from above by

$$\begin{aligned}
&A(\mathscr{E}) \sum_{s_0\leq s\leq s_1} A_0^s \sum_{\substack{Z^{1/2}\leq a\leq Z\\ P^+(a)\leq Z^{1/s}}} \prod_{\deg(Q)<p\leq Z^{1/(s+1)}} \left(1-\frac{\rho_Q(p)}{p^2}\right) \frac{f(a)\theta_Q(a)\widetilde{\rho}_Q(a)}{a^2}\\
&\quad\ll A(\mathscr{E}) \prod_{\substack{\deg(Q)<p\leq X\\ p\nmid Q}} \left(1-\frac{\rho_Q(p)}{p^2}\right)\\
&\qquad\cdot \sum_{s_0\leq s\leq s_1} A_0^s(s+1)^{\deg(Q)} \sum_{\substack{Z^{1/2}\leq a\leq Z\\ P^+(a)\leq Z^{1/s}}} \frac{f(a)\theta_Q(a)\widetilde{\rho}_Q(a)}{a^2},
\end{aligned} \tag{49}$$

where we have applied Lemma 9.11.

Let $\kappa := 4\ln(A_0)$. If $\kappa > \frac{3r+\varepsilon}{4}\log\left(\log Z \log\log Z\right)$, then $Z \ll 1$, hence $s_1 \ll 1$ and

$$\sum_{s_0\leq s\leq s_1} A_0^s(s+1)^{\deg(Q)} \ll 1.$$

Otherwise, $\kappa \leq \frac{3r+\varepsilon}{4}\log\left(\log Z \log\log Z\right)$, and we can estimate each of the innermost sums in (49) using Lemma 9.21 with κ as above and f replaced by $f\theta_Q$. The conditions of the lemma are satisfied due to Remark 9.16 with $\varepsilon' = (r-\varepsilon)/2$. Then

$$\begin{aligned}
&\sum_{s_0\leq s\leq s_1} A_0^s(s+1)^{\deg(Q)} \sum_{\substack{Z^{1/2}\leq a\leq Z\\ P^+(a)\leq Z^{1/s}}} \frac{f(a)\theta_Q(a)\widetilde{\rho}_Q(a)}{a^2}\\
&\quad\ll \sum_{a\leq Z} \frac{\widetilde{\rho}_Q(a)f(a)\theta_Q(a)}{a^2} \cdot \sum_{s_0\leq s\leq s_1} A_0^s(s+1)^{\deg(Q)}\exp(-s\kappa/2)\\
&\quad\ll \sum_{a\leq Z} \frac{\widetilde{\rho}_Q(a)f(a)\theta_Q(a)}{a^2}.
\end{aligned}$$

In both cases we deduce

$$\begin{aligned}\sum_{(x,y)\in R_4} &\ll A(\mathscr{E}) \prod_{\substack{\deg(Q)<p\leq X\\ p\nmid Q}} \left(1-\frac{\rho_Q(p)}{p^2}\right) \sum_{a\leq Z} \frac{\widetilde{\rho}_Q(a)f(a)\theta_Q(a)}{a^2}\\ &\ll A(\mathscr{E}) \prod_{\substack{\deg(Q)<p\leq X\\ p\nmid Q}} \left(1-\frac{\rho_Q(p)}{p^2}\right) \sum_{a\leq Z} \frac{\widetilde{\rho}_Q(a)f(a)}{a^2},\end{aligned}$$

where in the last line we have applied Lemma 9.20. This is again consistent with the claim.

9.7. *Sums restricted by congruence conditions.* In this section we extend Theorem 9.7 to sums with congruence restrictions.

Definition 9.24. Let $Q\in\mathbb{Z}[x,y]$. For any $k\in\mathbb{N}$ and $0\leq l<k$, define $\rho_Q(l;k)$ to be the number of solutions modulo k to the equation $Q(x,y)\equiv l$. In particular, $\rho_Q(0;k)=\rho_Q(k)$ and $\rho_Q(l;k)=\rho_{Q-l}(k)$.

PROPOSITION 9.25. *Fix $k_0\in\mathbb{N}$. Consider the setting of Theorem 9.7 but assume the stronger assumptions $(R_{\max}/k_0)^{\theta_l}\leq A(\mathscr{E})/k_0^2$ and $X\leq A(\mathscr{E})^\delta k_0^{1-2\delta}$. Then*

$$\begin{aligned}&\sum_{\substack{(x,y)\in\mathscr{E}\cap\mathbb{Z}^2\\ k_0\mid Q(x,y)}} f\left(\frac{Q(x,y)}{k_0}\right)\\ &\qquad\ll A(\mathscr{E}) \prod_{\substack{\deg(Q)<p\leq X/k_0\\ p\nmid k_0,\ p\nmid Q}} \left(1-\frac{\rho_Q(p)}{p^2}\right) \sum_{a\leq X/k_0} \frac{f(a)\widetilde{\rho}_Q(k_0a)}{(k_0a)^2}.\end{aligned}$$

The implicit constant is the same as in Theorem 9.7.

Proof. Let $r=(r_1,r_2)$ be a representative of one of the congruence classes modulo k_0 solving the equation $Q(x,y)\equiv 0 \mod k_0$. Define $Q_1^r, Q_0^r\in\mathbb{Z}[x,y]$ by

$$Q_1^r(x,y):=Q(k_0x+r_1,k_0y+r_2)=k_0Q_0^r(x,y).$$

Notice that $\deg(Q_i^r)=\deg(Q)$ for $i=0,1$. Moreover, $\rho_Q(p^k)=\rho_{Q_0^r}(p^k)$ for any $p\nmid k_0$ and $k\geq 0$, and the same holds for $\widetilde{\rho}$. Now we can apply Theorem 9.7

to the sum over a single congruence class as follows:

$$\begin{aligned}\sum_{\substack{(x,y)\in\mathscr{E}\cap\mathbb{Z}^2\\(x,y)\equiv r \bmod k_0}} f\left(\frac{Q(x,y)}{k_0}\right) &= \sum_{(x,y)\in k_0^{-1}(\mathscr{E}-r)\cap\mathbb{Z}^2} f\left(Q_0^r(x,y)\right)\\ &\ll \frac{A(\mathscr{E})}{k_0^2}\prod_{\substack{\deg(Q)<p\leq X/k_0\\ p\nmid k_0,\, p\nmid Q}}\left(1-\frac{\rho_Q(p)}{p^2}\right)\sum_{a\leq X/k_0}\frac{f(a)\widetilde{\rho}_{Q_0^r}(a)}{a^2}\\ &= A(\mathscr{E})\prod_{\substack{\deg(Q)<p\leq X/k_0\\ p\nmid k_0,\, p\nmid Q}}\left(1-\frac{\rho_Q(p)}{p^2}\right)\\ &\quad\cdot\sum_{a\leq X/k_0}\frac{f(a)\widetilde{\rho}_Q\left(\frac{a}{\gcd(a,k_0^\infty)}\right)\widetilde{\rho}_{Q_0^r}\left(\gcd(a,k_0^\infty)\right)}{(k_0a)^2}.\end{aligned}$$

A direct calculation shows that the conditions of Theorem 9.7 are satisfied when applied to the sum above. Summing over all the pertinent conjugacy classes we deduce

(50)

$$\begin{aligned}\sum_{\substack{(x,y)\in\mathscr{E}\cap\mathbb{Z}^2\\ k_0\mid Q(x,y)}} f\left(\frac{Q(x,y)}{k_0}\right) \ll A(\mathscr{E})&\prod_{\substack{\deg(Q)<p\leq X\\ p\nmid k_0,\, p\nmid Q}}\left(1-\frac{\rho_Q(p)}{p^2}\right)\\ &\cdot\sum_{a\leq X}\frac{f(a)\widetilde{\rho}_Q\left(\frac{a}{\gcd(a,k_0^\infty)}\right)}{(k_0a)^2}\left(\sum_r\widetilde{\rho}_{Q_0^r}\left(\gcd(a,k_0^\infty)\right)\right).\end{aligned}$$

For any $b\mid k_0^\infty$, we can see from the definitions in 9.1 that

$$\sum_r\widetilde{\rho}_{Q_0^r}(b)=\widetilde{\rho}_Q(k_0b).$$

The claim follows from combining this observation with (50). □

Proposition 9.26. *Consider the setting of Theorem 9.7 but assume the stronger assumptions $R_{\max}^{\theta_l}\leq A(\mathscr{E})^{1-4\eta}$ and $X\leq A(\mathscr{E})^{\delta/2}$. Fix $k_0,k_1,k_2\in\mathbb{N}$ such that all primes dividing k_1 also divide k_2, $\gcd(k_0,k_2)=1$ and $k:=k_0k_1k_2\leq A(\mathscr{E})^{\eta/2}$. Let $l\in\left(\mathbb{Z}/_{k_2\mathbb{Z}}\right)^\times$. Then*

$$\begin{aligned}\sum_{\substack{(x,y)\in\mathscr{E}\cap\mathbb{Z}^2\\ Q(x,y)\equiv k_0k_1l \bmod k}} f\left(\frac{Q(x,y)}{k_0}\right)&\ll A(\mathscr{E})\frac{f(k_1)\rho_Q\left(k_1l;k_1k_2\right)}{(k_1k_2)^2}\\ &\cdot\prod_{\substack{\deg(Q)<p\leq X/(k_0k_1)\\ p\nmid k_0k_2,\, p\nmid Q}}\left(1-\frac{\rho_Q(p)}{p^2}\right)\sum_{\substack{a\leq X/(k_0k_1)\\ \gcd(a,k_2)=1}}\frac{f(a)\widetilde{\rho}_Q(k_0a)}{(k_0a)^2}.\end{aligned}$$

The implicit constant is the same as in Theorem 9.7.

Proof. Let $r = (r_1, r_2)$ be a representative of one of the $\rho_Q(k_1l; k_1k_2)$ congruence classes modulo k_1k_2 solving the equation $Q(x, y) \equiv k_1 l \mod k_1k_2$. Define $Q_2, Q_1, Q_0 \in \mathbb{Z}[x, y]$ by

$$Q_2(x, y) := Q(kx + r_1, ky + r_2) = k_1 Q_1(x, y) = k_1(l + k_2 Q_0(x, y)).$$

Notice that $\deg(Q_i) = \deg(Q)$ for $i = 0, 1, 2$. Moreover, $\rho_Q(p^m) = \rho_{Q_2}(p^m) = \rho_{Q_1}(p^m)$ for any $p \nmid k_1k_2$ and $m \geq 0$. The same holds for $\widetilde{\rho}$. Because l is a unit modulo k_2, we conclude that $\rho_{Q_1}(p^m) = 0$ for $p \mid k_2$, $m \geq 1$. Finally, notice that because the prime support of k_1 is contained in that of k_2, the condition $p \mid k_1k_2$ is equivalent to $p \mid k_2$.

Because $\gcd(k_0, k_2) = 1$, we know that $k_0 \mid Q_2(x, y)$ if and only if $k_0 \mid Q_1(x, y)$. Write the pertinent sum over the fixed congruence class represented by r:

$$\sum_{\substack{(x,y)\in(k_1k_2)^{-1}(\mathscr{E}-r)\cap\mathbb{Z}^2\\ k_0\mid Q_2(x,y)}} f\left(\frac{Q_2(x,y)}{k_0}\right)$$
$$= f(k_1) \sum_{\substack{(x,y)\in(k_1k_2)^{-1}(\mathscr{E}-r)\cap\mathbb{Z}^2\\ k_0\mid Q_1(x,y)}} f\left(\frac{Q_1(x,y)}{k_0}\right).$$

A direct calculation shows that the conditions of Proposition 9.25 are satisfied when applied to the sum on the right-hand side. (The restriction on X holds because $k \leq A(\mathscr{E})^{1/4}$ as we have assumed $\eta < 1/2$.) The claim follows by summing over all the relevant conjugacy classes modulo k_1k_2. □

10. Proof of main theorem

In this section we use the following notation for all integers $n \geq 0$:

$$B^{(-n,n)} := \prod_{v \neq p_1} \Omega_v \times K_{p_1}^{(-n,n)} \subset \mathbf{G}(\mathbb{A}).$$

For the sake of brevity, we shall denote $B := B^{(-0,0)}$.

Moreover, for any $\xi \in (\mathbf{G} \times \mathbf{G})(\mathbb{A})$, we denote by ν_ξ the algebraic measure supported on $\left[\mathbf{G}^\Delta(\mathbb{A})^+ \xi\right]$.

10.1. *Reduction to a bound on cross-correlation.* We begin by showing that Theorem 3.2 follows from an appropriate bound on the cross-correlation.

Lemma 10.1. *Let $\mathscr{H}_i = \left[\mathbf{T}^\Delta(\mathbb{A})(g, sg)\right]$ be a sequence of homogeneous toral sets where $\mathbf{T}$, g and s depend on the index $i \in \mathbb{N}$. Assume that the splitting conditions (♠) are satisfied for all i. Denote by μ_i the algebraic measure supported on $\mathscr{H}_i$, and assume $\mu_i \to_{i\to\infty} \mu$.*

Assume that there is some $F\colon \mathbf{G}(\mathbb{A}) \to \mathbb{R}_{>0}$ continuous such that for all $n \in \mathbb{N}$, for all $\xi \in (\mathbf{G}\times\mathbf{G})(\mathbb{A})$ and for all $i \gg_{n,\xi} 1$,

$$\operatorname{Cor}[\mu_i, \nu_\xi]\left(B^{(-n,n)}\right) \ll F(\operatorname{ctr}(\xi)) p_1^{-2(1+\rho)n}$$

for some $\rho > 0$ fixed. Then μ is a $(\mathbf{G}\times\mathbf{G})(\mathbb{A})^+$-invariant probability measure.

Proof. From Duke's theorem we know that μ is a probability measure. Theorem 4.4 and Corollary 4.5 imply that μ is a convex combination of a $(\mathbf{G}\times\mathbf{G})(\mathbb{A})^+$-invariant probability measure and algebraic measures supported on homogeneous Hecke sets of the form $\left[\mathbf{G}^\Delta(\mathbb{A})^+\xi\right]$ such that

$$\operatorname{ctr}(\xi)_{p_j} \in A_{p_j}$$

for $j \in \{1, 2\}$.

Assume in contradiction that μ is not $(\mathbf{G}\times\mathbf{G})(\mathbb{A})^+$-invariant. Then there is a finite non-vanishing measure λ_0 on ${}_{\mathbf{G}^\Delta(\mathbb{A})^+}\backslash^{(\mathbf{G}\times\mathbf{G})(\mathbb{A})}$ so that

$$\mu \geq \int_{\mathbf{G}^\Delta(\mathbb{A})^+\backslash(\mathbf{G}\times\mathbf{G})(\mathbb{A})} \nu_\xi \,\mathrm{d}\lambda_0(\xi)$$

and the following set has full λ_0-measure:

$$\Xi_1 \coloneqq \left\{\xi \in {}_{\mathbf{G}^\Delta(\mathbb{A})^+}\backslash^{(\mathbf{G}\times\mathbf{G})(\mathbb{A})} \middle| \operatorname{ctr}(\xi)_{p_1} \in A_{p_1}, \operatorname{ctr}(\xi)_{p_2} \in A_{p_2}\right\}.$$

Moreover, because λ_0 is a finite measure, it is regular so there is a compact subset $\Xi_0 \subset \Xi_1$ of positive measure. We now have

$$\mu \geq \lambda_0(\Xi_0)\cdot\bar{\nu},$$
$$\bar{\nu} \coloneqq \frac{1}{\lambda_0(\Xi_0)} \int_{\Xi_0} \nu_\xi \,\mathrm{d}\lambda_0(\xi),$$

and $\bar{\nu}$ is a probability measure on $[(\mathbf{G}\times\mathbf{G})(\mathbb{A})]$.

Let $a = \lambda(p_1) \in A_{p_1}$, where $\lambda \in X_\bullet(A_{p_1})$ generates the cocharacter group. The element $a^\Delta \in A_{p_1}^\Delta$ acts on $[(\mathbf{G}\times\mathbf{G})(\mathbb{A})]$ on the right. For all $\xi \in \Xi_0$, the action of a^Δ on the space $[(\mathbf{G}\times\mathbf{G})(\mathbb{A})]$ keeps ν_ξ invariant because $\operatorname{ctr}(\xi) \in A_{p_1}$. Additivity of entropy implies

$$\mathrm{h}_{a^\Delta}(\bar{\nu}) = \frac{1}{\lambda_0(\Xi_0)} \int_{\Xi_0} h_{a^\Delta}(\nu_\xi)\,\mathrm{d}\lambda_0(\xi).$$

The measurable dynamical system $\left([(\mathbf{G}\times\mathbf{G})(\mathbb{A})], \nu_\xi, a^\Delta\right)$ is measure theoretically isomorphic to a acting on the space

$$Z_{\mathbf{G}^{\mathrm{sc}}}(\mathbb{A})\mathbf{G}^{\mathrm{sc}}(\mathbb{Q})\backslash^{\mathbf{G}^{\mathrm{sc}}(\mathbb{A})}$$

equipped with the probability Haar measure. This entropy can be computed using the leaf-wise measure [EL10], [MT94] on the horospherical subgroup of a. As the Haar measure is invariant under the full group action, the leaf-wise measure will be the Haar measure on the horospherical subgroup and

$$\mathrm{h}_{a^\Delta}(\bar{\nu}) = \log p_1.$$

We will show next that the assumed cross-correlation estimate implies that the entropy of $\bar{\nu}$ must be at least $(1+\rho)\log p_1$, which contradicts the equality above.

Weak-$*$ convergence of measures implies that for any bounded open subset $C^\circ \subset [\mathbf{G}(\mathbb{A})]$,

$$\begin{aligned}\mathrm{Cor}_{C^\circ}[\mu,\nu_\xi]\left(B^{(-n,n)^\circ}\right) &\leq \liminf_{i\to\infty}\mathrm{Cor}_{C^\circ}[\mu_i,\nu_\xi]\left(B^{(-n,n)^\circ}\right)\\ &\leq \liminf_{i\to\infty}\mathrm{Cor}[\mu_i,\nu_\xi]\left(B^{(-n,n)}\right).\end{aligned}$$

Fix a closed identity neighborhood $\Omega_{\infty,0}\subset\Omega_\infty^\circ$, and set $B_0^{(-n,n)}=\Omega_{\infty,0}\times\prod_{v\neq p_1,\infty}\Omega_v\times K_{p_1}^{(-n,n)}$. Taking a monotone sequence of bounded open subsets that exhausts $[\mathbf{G}(\mathbb{A})]$, we deduce that

$$\mathrm{Cor}[\mu,\nu_\xi]\left(B_0^{(-n,n)}\right)\leq\liminf_{i\to\infty}\mathrm{Cor}[\mu_i,\nu_\xi]\left(B^{(-n,n)}\right)\ll F(\mathrm{ctr}(\xi))p_1^{-2(1+\rho)n}.$$

Monotonicity of integration and Fubini imply that

$$\begin{aligned}\mathrm{Cor}[\bar{\nu},\bar{\nu}]\left(B_0^{(-n,n)}\right) &\leq \frac{1}{\lambda_0(\Xi_0)}\mathrm{Cor}[\mu,\bar{\nu}]\left(B_0^{(-n,n)}\right)\\ &= \frac{1}{\lambda_0(\Xi_0)^2}\int_{\Xi_0}\mathrm{Cor}[\mu,\nu_\xi]\left(B_0^{(-n,n)}\right)\mathrm{d}\lambda_0(\xi)\\ &\ll \frac{p_1^{-2(1+\rho)n}}{\lambda_0(\Xi_0)^2}\int_{\Xi_0}F(\mathrm{ctr}(\xi))\,\mathrm{d}\lambda_0(\xi).\end{aligned}$$

Notice that $\int_{\Xi_0}F(\mathrm{ctr}(\xi))\,\mathrm{d}\lambda_0(\xi)$ is finite because Ξ_0 is compact and F is continuous.

An upper bound on the self-correlation of a measure for Bowen balls implies a lower bound for the metric entropy. The self-correlation bound for the adelic quotient implies an identical bound for any S-arithmetic quotient, as long as we take the set of places S to include ∞, p_1. On the other hand, a lower bound for the entropy for S-arithmetic quotients for arbitrary large S implies the same bound for the adelic quotient.

Using [ELMV09, Prop. 3.2], which generalizes, *mutatis mutandis*, to the S-arithmetic setting, we deduce from the last inequality that $\mathrm{h}_{a^\Delta}(\bar{\nu})\geq(1+\rho)\log p_1$ as required. □

10.2. *From a shifted convolution to sums over a polynomial.* The first step in producing an upper bound on the cross-correlation as required in Lemma 10.1 is translation of the shifted-convolution sum in Theorem 8.7 to sums of a *multiplicative* function over values of a polynomial in two variables.

In this section we work in the setting of Theorem 8.7, which we now review. Fix a joint homogeneous toral set $\left[\mathbf{T}^\Delta(\mathbb{A})(g,sg)\right]$ satisfying (♠) with a splitting field $E/\mathbb{Q}$ and quadratic order $\Lambda\leq\mathcal{O}_E$ of discriminant D.

Fix also a simply connected homogeneous Hecke set $\left[\mathbf{G}^{\Delta}(\mathbb{A})^{+}\xi\right]$ with $\mathrm{ctr}(\xi)_{p_1} \in A_{p_1}$, and assume

$$g^{-1}\mathbf{T}(\mathbb{Q})sg \cap B\,\mathrm{ctr}(\xi)B = \emptyset.$$

Notice that this condition implies the same for $B^{(-n,n)}$ for all n.

Let μ be the algebraic probability measure supported on $\left[\mathbf{T}^{\Delta}(\mathbb{A})(g,sg)\right]$, and let ν_ξ be the algebraic probability measure supported on $\left[\mathbf{G}^{\Delta}(\mathbb{A})^{+}\xi\right]$. Denote $\kappa = 2^8\,\mathfrak{d}_\infty(\mathrm{ctr}(\xi)_\infty)\,\mathfrak{d}_f(\mathrm{ctr}(\xi)_f)$ and $\omega = \mathrm{sign}(\mathrm{Nrd}(\mathrm{ctr}(\xi)_\infty))\,\mathfrak{d}_f(\mathrm{ctr}(\xi)_f)$.

Initially, we transform the shifted-convolution sum to a sum of a non-multiplicative function over polynomial values. Afterwards we shall use principal genus theory to split the sum in the following lemma into sums that can be effectively bounded by multiplicative functions.

Lemma 10.2. *Fix an arbitrary $\mathbb{Z}$-basis $A, B \in E^\times$ for the fractional Λ-ideal $\mathfrak{s}^{-1}$, and let $q(x,y) \in \mathbb{Z}[x,y]$ be the associated norm form*

$$q(x,y) \coloneqq \frac{\mathrm{Nr}(Ax+By)}{\mathrm{Nr}(\mathfrak{s}^{-1})}.$$

This is a primitive integral binary quadratic form of discriminant D.

The shifted convolution sum of Theorem 8.7 satisfies

$$\sum_{\substack{0\le x\le \kappa|D| \\ x\equiv \omega|D| \mod \upsilon p_1^{2n}}} g_{[\mathfrak{s}]}(x) f_{[p_1^n\mathfrak{s}\mathfrak{c}]^{-1}}\left(\frac{x-\omega D}{\upsilon p_1^{2n}}\right) r\left(\frac{x-\omega D}{\upsilon p_1^{2n}}\right)$$
$$= \frac{1}{\#\Lambda^\times} \sum_{\substack{(x,y)\in\mathbb{Z}^2\colon\, q(x,y)\le\kappa|D| \\ \upsilon p_1^{2n}|Q(x,y)}} \left(f_{[p_1^n\mathfrak{s}\mathfrak{c}]^{-1}}\cdot r\right)\left(\frac{Q(x,y)}{\upsilon p_1^{2n}}\right),$$

where

$$Q(x,y) \coloneqq q(x,y) - \omega D.$$

Proof. This follows immediately from the correspondence between invertible integral ideals in the class $[\mathfrak{s}] \in \mathrm{Pic}(\Lambda)$ and points in $\mathfrak{s}^{-1}$. Explicitly, if $\mathfrak{a} \in [\mathfrak{s}]$, then there is some $a \in E^\times$ so that $\mathfrak{a} = a\mathfrak{s}$ and $a\mathfrak{s} \subseteq \mathfrak{f}$, i.e., $a \in \mathfrak{s}^{-1}$. Moreover, two different values of a corresponding to $\mathfrak{a}$ must differ by a unit of Λ. □

Definition 10.3. We now fix $q(x,y) \in \mathbb{Z}$ to be the unique *reduced*[9] norm form for $\mathfrak{s}^{-1}$ and denote

$$\mathscr{E} \coloneqq \left\{(x,y)\in\mathbb{R}^2 \mid q(x,y) \le \kappa|D|\right\}.$$

[9] That is, it is reduced with respect to the usual fundamental domain for the $\mathbf{SL}_2(\mathbb{Z})$-action on the upper half plain.

In the current section we shall always denote by $R_{\max}$ and $A(\mathscr{E})$ the maximal radius of curvature and area of $\mathscr{E}$.

Lemma 10.4. *The set $\mathscr{E}$ is an ellipse centered at the origin. Its area is $A(\mathscr{E}) = 2\pi\kappa\sqrt{|D|}$, and the maximal radius of curvature satisfies*

$$R_{\max} \leq \sqrt{A(\mathscr{E})}\left(\frac{\sqrt{|D|}}{\mathfrak{N}}\right)^{3/2},$$

where $\mathfrak{N} \coloneqq \min_{\substack{\mathfrak{a}\subseteq\Lambda\\ [\mathfrak{a}]=[\mathfrak{s}]}} \operatorname{Nr}\mathfrak{a}$.

Proof. The domain $\mathscr{E}$ is an ellipse because q is positive-definite. The formula for the area follows from the fact that $\operatorname{disc}(q) = D$. To estimate $R_{\max}$ consider the ellipse $\mathscr{E}_0$ of area π homothetic to $\mathscr{E}$ and let $a \geq a^{-1} > 0$ be the lengths of its semi-major axes. The maximal radius of curvature satisfies

$$R_{\max} = \sqrt{A(\mathscr{E})}R_{\max}(\mathscr{E}_0) = \sqrt{A(\mathscr{E})}\frac{a^2}{a^{-1}} = \sqrt{A(\mathscr{E})}a^3. \tag{51}$$

The group $\mathbf{SL}_2(\mathbb{R})$ acts transitively on the space of ellipses of area π and centered at the origin. The stabilizer of the unit circle S^1 is $\mathbf{SO}_2(\mathbb{R})$. We identify this space of ellipses with the upper half-plane $\mathbb{H}$ by sending S^1 to $i \in \mathbb{H}$. The point in $\mathbb{H}$ corresponding to $\mathscr{E}_0$ coincides with the point corresponding to q in the fundamental domain. Denote this point by $x_0 \in \mathbb{H}$. This point can be written down explicitly as[10]

$$x_0 = \frac{-b + i\sqrt{|D|}}{2\mathfrak{N}},$$

where $\left\langle \mathfrak{N}, \frac{-b+i\sqrt{|D|}}{2} \right\rangle \subset E$ is the primitive integral ideal in the class $[\mathfrak{s}^{-1}]$. In particular,

$$\Im(x_0) = \frac{\sqrt{|D|}}{2\mathfrak{N}}.$$

If $\mathscr{E}_0 = g.S^1$, then the lengths of the semi-major axes are exactly the element of the diagonal matrix in the Cartan decomposition of g, i.e. $g \in \mathbf{SO}_2(\mathbb{R})\left(\begin{smallmatrix} a & 0 \\ 0 & a^{-1}\end{smallmatrix}\right)\mathbf{SO}_2(\mathbb{R})$. In particular, $a^2 + a^{-2} = \operatorname{Tr}(g^t g)$.

We would like to find the relation of between a and $\Im(x_0)$. Using the Iwasawa decomposition of $\mathbf{SL}_2(\mathbb{R})$ we can write

$$g \in \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}\begin{pmatrix} \sqrt{\Im(x_0)} & 0 \\ 0 & \sqrt{\Im(x_0)}^{-1} \end{pmatrix}\mathbf{SO}_2(\mathbb{R})$$

[10] Notice that because an ideal class and its inverse are Galois conjugate, $\min_{\substack{\mathfrak{a}\subseteq\Lambda\\ [\mathfrak{a}]=[\mathfrak{s}]}} \operatorname{Nr}\mathfrak{a} = \min_{\substack{\mathfrak{a}\subseteq\Lambda\\ [\mathfrak{a}]=[\mathfrak{s}^{-1}]}} \operatorname{Nr}\mathfrak{a}$.

for some $-1/2 \leq t \leq 1/2$. We deduce that

$$a^2 + a^{-2} = \operatorname{Tr}(g^t g) = \Im(x_0) + \Im(x_0)^{-1}(1 + t^2).$$

Solving the above quadratic equation for a^2 and using standard calculus with the inequalities $t^2 \leq 1/4$ and $\Im(x_0) \geq \sqrt{3}/2$ we deduce that

$$a^2 \leq 2\Im(x_0) = \frac{\sqrt{|D|}}{\mathfrak{N}}.$$

The claim follows by combining this inequality with (51). □

The next step is to split the sum from Lemma 10.2 according to further congruence conditions to take into account the restrictions modulo $\operatorname{Pic}(\Lambda)^2$. We shall do that only for small odd primes dividing $D_E = \operatorname{disc}(E)$. Our sieve method will not be able to take into account large prime divisor. Fortunately, we will see later that not taking into account the genus congruence conditions for larger primes only changes the final upper bound by an absolute constant.

Let $C_\theta \geq 1$ be a constant such that for all $X \in \mathbb{N}$,

$$C_\theta^{-1} X \leq \sum_{p \leq X} \log p \leq C_\theta X. \tag{52}$$

Such a C_θ exists due to the Chebyshev bounds on the prime counting function. We fix $1/2 > \eta > 0$ to be determined later. Write $D = D_{\text{small}} D_{\text{large}}$, where

$$D_{\text{small}} \coloneqq \prod_{\substack{p \| D,\, p \nmid \omega \\ 2 < p \leq \eta/(4C_\theta) \log |D|}} p.$$

Because of (52) we know that $D_{\text{small}} \leq |D|^{\eta/4}$. We are going to split the sum in Lemma 10.2 according to congruence classes modulo υp_1^{2n} and p^2 for any $p \mid D_{\text{small}}$. It is exactly these congruence conditions that our sieve bound can take into account. Because we only seek upper bounds, we can simply ignore any restrictions that the condition modulo $\operatorname{Pic}(\Lambda^2)$ implies for primes $p \mid D_{\text{large}}$. Fortunately, ignoring the congruence conditions modulo large primes only changes the upper-bound by a fixed constant independent of D.

Thus our goal is to replace in each congruence class the functions $f_{[p_1^n \mathfrak{s}\mathfrak{e}]^{-1}}$ and r by the simpler functions f and r_0 from the following definition.

Definition 10.5. Let $f \colon \mathbb{N} \to \mathbb{N}$ be the multiplicative function counting integral invertible Λ-ideals, i.e.,

$$f(n) \coloneqq \#\left\{\mathfrak{a} \in \mathcal{J}(\Lambda) \mid \mathfrak{a} \subseteq \Lambda,\ \operatorname{Nr} \mathfrak{a} = n\right\}.$$

Define also the multiplicative function $r_0 \colon \mathbb{N} \to \mathbb{Z}$ by requiring that $r_0(p^k) = 2$ if $p \mid D_{\text{large}}$ and $k \geq \operatorname{ord}_p D$, and $r_0(p^k) = 1$ otherwise.

To take into account the condition modulo $\mathrm{Pic}(\Lambda^2)$, we need to add weights to the sums over different congruence classes for $p \mid D_{\mathrm{small}}$. We now define the correct weights as follows from principal genus theory. Define $k \coloneqq \upsilon p_1^{2n} D_{\mathrm{small}}^2$, and write

$$\mathbb{Z}/k\mathbb{Z} = \mathbb{Z}/\upsilon\mathbb{Z} \times \mathbb{Z}/p_1^{2n}\mathbb{Z} \times \prod_{p \mid D_{\mathrm{small}}} \mathbb{Z}/p^2\mathbb{Z}.$$

For each prime $p \mid D_{\mathrm{small}}$, we partition $\mathbb{Z}/p^2\mathbb{Z}$ in the following way:

$$\begin{aligned}
\mathbb{Z}/p^2\mathbb{Z} &= C_{+0}^{p^2} \sqcup C_{-0}^{p^2} \sqcup C_{+1}^{p^2} \sqcup C_{-1}^{p^2} \sqcup C_{2}^{p^2},\\
C_{\pm 0}^{p^2} &\coloneqq \left\{ u \in \left(\mathbb{Z}/p^2\mathbb{Z}\right)^{\times} \,\middle|\, \left(\frac{u}{p}\right) = \pm 1 \right\},\\
C_{\pm 1}^{p^2} &\coloneqq \left\{ pu \,\middle|\, u \in \left(\mathbb{Z}/p\mathbb{Z}\right)^{\times},\ \left(\frac{u}{p}\right) = \pm 1 \right\},\\
C_{2}^{p^2} &\coloneqq \{0\}.
\end{aligned}$$

We define a measure w_p on $\mathbb{Z}/p^2\mathbb{Z}$. The measure w_p is uniform on each atom of the partition above and assigns the following weights for each atom:

$$\begin{aligned}
w_p(C_{\pm 0}^{p^2}) &= \# C_{\pm 0}^{p^2} = \frac{p^2}{2}\left(1 - \frac{1}{p}\right),\\
w_p(C_{2}^{p^2}) &= 2 \cdot \# C_{2}^{p^2} = 2,\\
w_p(C_{\epsilon}^{p^2}) &= \# C_{\epsilon}^{p^2} \cdot \begin{cases} 2 & \chi_p\left(\mathrm{Nr}(p_1^n \mathfrak{se})\right) = -\epsilon,\\ 0 & \chi_p\left(\mathrm{Nr}(p_1^n \mathfrak{se})\right) \neq -\epsilon \end{cases}\\
&= p\left(1 - \frac{1}{p}\right)\delta_{\chi_p\left(\mathrm{Nr}(p_1^n \mathfrak{se})\right) = -\epsilon},
\end{aligned}$$

where $\epsilon \in \{\pm 1\}$ and we denote by χ_p both the unique primitive real Dirichlet character of conductor $p > 2$ and its adelic lift. See Definition A.9 in the appendix for details.

Each weight takes into account both the difference between r_0 and r and the information from principal genus theory about the condition modulo $\mathrm{Pic}(\Lambda^2)$; cf. Proposition A.10. In particular, the factor of 2 in the weights of all congruence classes modulo p outside of $C_{\pm 0}^{p^2}$ is due to the contribution of r. The fact that one of the two sets $C_{\pm 1}^{p^2}$ has weight 0 is due to the genus restriction.

These measures for $p \mid D_{\mathrm{small}}$ define a product measure w_k on $\mathbb{Z}/k\mathbb{Z}$ by

$$w_k \coloneqq \delta_{0 \bmod \upsilon} \times \delta_{0 \bmod p_1^{2n}} \times \prod_{p \mid D_{\mathrm{small}}} w_p.$$

Lemma 10.6. *The following holds*:

$$\frac{1}{\#\Lambda^\times}\sum_{\substack{(x,y)\in\mathscr{E}\cap\mathbb{Z}^2\\ \upsilon p_1^{2n}|Q(x,y)}}\left(f_{[p_1^n\mathfrak{s}\mathfrak{e}]^{-1}}\cdot r\right)\left(\frac{Q(x,y)}{\upsilon p_1^{2n}}\right)$$
$$\ll_{\mathbf{G}}\int\sum_{\substack{(x,y)\in\mathscr{E}\cap\mathbb{Z}^2\\ Q(x,y)\equiv m \bmod k}}(f\cdot r_0)\left(\frac{Q(x,y)}{\upsilon p_1^{2n}}\right)\mathrm{d}w_k(m).$$

Remark 10.7. Unlike r, the mean value of the multiplicative function r_0 is bounded above only in terms of η independently of D. This is why its contribution is of no significant effect. The contribution of r that is not covered by r_0 is negated by the restriction to a fixed genus class whenever $p\mid D_{\mathrm{small}}$ and $p\parallel Q(x,y)$.

Proof. Notice that $\#\Lambda^\times\geq 1$ hence the factor $\frac{1}{\#\Lambda^\times}$ is uniformly bounded. Moreover, using Proposition A.10 we deduce that

$$\frac{1}{\#\Lambda^\times}\sum_{\substack{(x,y)\in\mathscr{E}\cap\mathbb{Z}^2\\ \upsilon p_1^{2n}|Q(x,y)}}\left(f_{[p_1^n\mathfrak{s}\mathfrak{e}]^{-1}}\cdot r\right)\left(\frac{Q(x,y)}{\upsilon p_1^{2n}}\right)$$
$$\leq\sum_{\substack{m\in{}^{\mathbb{Z}}/{}_{k\mathbb{Z}}\\ m\equiv 0 \mod \upsilon p_1^{2n}\\ \forall p|D_{\mathrm{small}}:\, m \bmod p^2\notin C^{p^2}_{\chi_p\left(\mathrm{Nr}(p_1^n\mathfrak{s}\mathfrak{e})\right)}}}\ \sum_{\substack{(x,y)\in\mathscr{E}\cap\mathbb{Z}^2\\ Q(x,y)\equiv m \bmod k}}(f\cdot r)\left(\frac{Q(x,y)}{\upsilon p_1^{2n}}\right).$$

Notice that Proposition A.10 has only been applied to primes $p\mid D_{\mathrm{small}}$ and only in the case that $p\parallel Q(x,y)$. If $Q(x,y)$ is a unit modulo p, then $\frac{Q(x,y)}{\upsilon p_1^{2n}}\equiv\frac{q(x,y)}{\upsilon p_1^{2n}}\mod p$, where $q(x,y)$ is a norm of an ideal in the class $[\mathfrak{s}]$. Unwinding the definitions of υ and $\mathfrak{e}$, we see that the genus congruence class of $\frac{Q(x,y)}{\upsilon p_1^{2n}}$ modulo p is equal to the genus congruence class modulo p of $[\mathfrak{s}\mathfrak{e}^{-1}\mathfrak{p}_1^{-n}]\equiv[\mathfrak{p}_1^n\mathfrak{s}\mathfrak{e}]^{-1}\mod\mathrm{Pic}(\Lambda)^2$. This implies that principal genus theory in the form of Proposition A.10 provides no extra information in this case. We also neglect any information from principal genus theory if $\mathrm{ord}_p\,Q(x,y)\geq 2$, but this will only affects our final bound by multiplying it by a constant independent of all parameters.

Finally notice that if $Q(x,y) \equiv m \mod k$, then

$$r\left(\frac{Q(x,y)}{\upsilon p_1^{2n}}\right) = w_k(m) r_0 \left(\frac{Q(x,y)}{\upsilon p_1^{2n}}\right) 2^{\mu_{\mathrm{wild}}\delta_{2|D}} \prod_{\substack{p \| Q(x,y) \\ \mathbf{G} \text{ ramifies at } p}} 2$$

$$\ll_{\mathbf{G}} w_k(m) r_0 \left(\frac{Q(x,y)}{\upsilon p_1^{2n}}\right). \qquad \square$$

10.3. *The sieved upper bound.* We are finally ready to apply Theorem 9.7 in the form of Proposition 9.26 to bound the cross-correlation.

Definition 10.8. We say that an exponent $\theta_l > 0$ is admissible if there is some $C_l > 0$ depending on θ_l such that all ellipses defined by definite integral binary quadratic forms belong to $\mathscr{L}(C_l, \theta_l)$.

Van Der Corput's [vdC20] bound implies that any $\theta_l > 2/3$ is admissible, while the bound of Huxley [Hux03] implies that any $\theta_l > 131/208 > 0.6298$ is admissible.

Definition 10.9. For any $m \in \mathbb{Z}/_{k\mathbb{Z}}$, define

$$D_i(m) = \prod_{\substack{p | D_{\mathrm{small}} \\ \mathrm{ord}_p\, m = i}} p$$

for $i \in \{0, 1, 2\}$. Then $D_{\mathrm{small}} = D_0(m) D_1(m) D_2(m)$.

Proposition 10.10. *Let* $m \in \mathbb{Z}/_{k\mathbb{Z}}$ *with* $w_k(m) > 0$. *Let* $\theta_l > 0$ *be admissible, fix* $0 < \eta < 1/2$, *and assume* $R_{\max}^{\theta_l} \le A(\mathscr{E})^{1-4\eta}$. *If* $\upsilon p_1^{2n} \le |D|^{\eta/2}$, *then*

$$\sum_{\substack{(x,y) \in \mathscr{E} \cap \mathbb{Z}^2 \\ Q(x,y) \equiv m \bmod k}} (f \cdot r_0)\left(\frac{Q(x,y)}{\upsilon p_1^{2n}}\right) \ll_{f,\eta} A(\mathscr{E}) \frac{\rho_Q\left(m; (D_0(m) D_1(m))^2\right)}{(D_0(m) D_1(m))^4}$$

$$\cdot \prod_{\substack{2 < p \le 2\kappa |D|^{1-\eta} \\ p \nmid \upsilon p_1 D_{\mathrm{small}}}} \left(1 - \frac{\rho_Q(p)}{p^2}\right) \sum_{\substack{a \le 2\kappa |D| \\ \gcd(a, D_0(m) D_1(m)) = 1}} \frac{f(a) r_0(a) \widetilde{\rho}_Q(\upsilon p_1^{2n} D_2(m)^2 a)}{(\upsilon p_1^{2n} D_2(m)^2 a)^2}.$$

Proof. Write

$$m \equiv D_1(m) l \mod D_0(m)^2 D_1(m)^2,$$

where $l \in \left(\mathbb{Z}/_{D_0(m)^2 D_1(m)\mathbb{Z}}\right)^\times$.

Notice that if $p \parallel D$, then $f(pn) = f(n)$ for all $n \in \mathbb{N}$. Using this we write

$$\sum_{\substack{(x,y) \in \mathscr{E} \cap \mathbb{Z}^2 \\ Q(x,y) \equiv m \bmod k}} (f \cdot r_0)\left(\frac{Q(x,y)}{\upsilon p_1^{2n}}\right) = \sum_{\substack{(x,y) \in \mathscr{E} \cap \mathbb{Z}^2 \\ Q(x,y) \equiv m \bmod k}} (f \cdot r_0)\left(\frac{Q(x,y)}{\upsilon p_1^{2n} D_2(m)^2}\right).$$

We wish to apply Proposition 9.26. We now define k_0, k_1, k_2, X and δ and verify that the conditions of the proposition hold.

Set $k_0 = \upsilon p_1^{2n} D_2(m)^2$, $k_1 = D_1(m)$ and $k_2 = D_0(m)^2 D_1(m)$. Notice that $k_0 k_1 k_2 = \upsilon p_1^{2n} D_2(m)^2 D_0(m)^2 D_1(m)^2 = \upsilon p_1^{2n} D_{\mathrm{small}} = k$. Because $D_{\mathrm{small}} \leq |D|^{\eta/2}$ and using Lemma 10.4, we deduce that $k \leq |D|^\eta \leq A(\mathscr{E})^{\eta/2}$.

For any $(x, y) \in \mathscr{E} \cap \mathbb{Z}^2$, we know from the definition of $Q(x, y)$ that $Q(x, y) = \upsilon \operatorname{Nr}(\mathfrak{b})$, where $(\mathfrak{a}, \mathfrak{b})$ is a pair of integral ideals satisfying the conclusions of Proposition 8.30 with $x = \operatorname{ctr}(\xi)$. We deduce the following, using the explicit formulae for κ and ω from Theorem 8.7:

$$\begin{aligned}\max\left\{|Q(x,y)| \;\middle|\; (x,y) \in \mathscr{E} \cap \mathbb{Z}^2\right\} &= \max_{\substack{\mathscr{J}_0(\Lambda) \ni \mathfrak{a} \subseteq \Lambda \\ \operatorname{Nr}\mathfrak{a} \leq \kappa |D|}} |\operatorname{Nr}\mathfrak{a} - \omega D| \\ &\leq (\kappa + |\omega|)|D| \leq 2\kappa|D| \leq A(\mathscr{E}).\end{aligned}$$

Hence we can take $X = 2\kappa|D|$ and $\delta = 2$ in the conditions of Proposition 9.26.

Moreover, using the standard Euler product for the Dedekind ζ-function of E with the necessary modifications at primes dividing the conductor, we see that for every $\varepsilon > 0$, there are some $1 \leq A \ll_{\mathfrak{f}} 1$ and $0 < B \ll_{\varepsilon, \mathfrak{f}} 1$ so that $f \in \mathscr{M}(A, B, \varepsilon)$. Finally, to apply Proposition 9.26 we need a bound of the form $\widetilde{\rho}_Q(p^k) \leq C p^{k(2-r)}$ for some $C \geq 1$, $0 < r < 1$. Such a bound holds with $C = 16$ and $r = 1/2$ due to Corollary B.6.

Notice that $f(k_1) = 1$ because k_1 is supported on ramified primes and it is coprime to $\mathfrak{f}$. After applying Proposition 9.26, we arrive at the necessary sum with product and summation up to $X/(k_0 k_1)$. The final result follows because $2\kappa|D| = X \geq X/(k_0 k_1) \geq X/k \geq 2\kappa|D|^{1-\eta}$. □

Lemma 10.11. *Let $m \in {}^{\mathbb{Z}}/_{k\mathbb{Z}}$ with $w_k(m) > 0$. For any $a \in \mathbb{N}$ such that* $\gcd(a, D_0(m) D_1(m)) = 1$, *the following inequality holds:*

$$\frac{\widetilde{\rho}_Q(\upsilon p_1^{2n} D_2(m)^2 a)}{(\upsilon p_1^{2n} D_2(m)^2 a)^2} \ll_{\mathfrak{f}, \mathbf{G}} \frac{|\omega|^2}{p_1^{2n} D_2(m)^2 a} \left[\prod_{p \mid a}\left(1 + \frac{1}{p}\right)\right] \left[\prod_{p \mid D_2(m)} 2\left(1 - \frac{1}{p}\right)\right] r_1(a),$$

where r_1 is a multiplicative function defined by $r_1(p^k) = 2$ for any $p \mid D_{\mathrm{large}}$ and $k > \operatorname{ord}_p D_{\mathrm{large}}$ and $r_1(p^k) = 1$ otherwise.

Remark 10.12. Notice that by definition, $r_1 \leq r_0$.

Proof. Recall that υ and $D_2(m)$ are square-free. To prove the lemma we use the multiplicativity of $\widetilde{\rho}_Q$ to write

$$\begin{aligned}\widetilde{\rho}_Q(\upsilon p_1^{2n} D_2(m)^2 a) = &\left[\prod_{p \mid \upsilon} \widetilde{\rho}_Q\left(p^{\operatorname{ord}_p a + 1}\right)\right] \widetilde{\rho}_Q\left(p_1^{\operatorname{ord}_{p_1} a + 2n}\right) \\ &\cdot \left[\prod_{p \mid D_2(m)} \widetilde{\rho}_Q\left(p^{\operatorname{ord}_p a + 2}\right)\right] \prod_{\substack{p \mid a \\ p \nmid \upsilon p_1 D_2(m)}} \widetilde{\rho}_Q\left(p^{\operatorname{ord}_p a}\right).\end{aligned}$$

We treat each term above separately.

Any prime dividing υ necessarily is coprime to the conductor (cf. Section 5.3.2) and is inert in $E/\mathbb{Q}$; thus according to Proposition B.3,

$$\prod_{p\mid\upsilon}\widetilde{\rho}_Q\left(p^{\operatorname{ord}_p a+1}\right)=\prod_{p\mid\upsilon}(p+1)p^{\operatorname{ord}_p a}=\upsilon\gcd(a,\upsilon^\infty)\prod_{p\mid\upsilon}\left(1+\frac{1}{p}\right)\ll_{\mathbf{G}}\gcd(a,\upsilon^\infty).$$

The last inequality holds because υ is bounded above by the product of all primes where $\mathbf{B}$ ramifies.

The prime p_1 is split in $E/\mathbb{Q}$ and coprime to $\mathscr{f}$, hence by Proposition B.3,

$$\widetilde{\rho}_Q\left(p_1^{\operatorname{ord}_{p_1} a+2n}\right)=(p_1-1)p_1^{\operatorname{ord}_{p_1} a+2n-1}<p_1^{2n}\gcd(a,p_1^\infty).$$

Next we consider all primes p dividing $D_2(m)$. These are ramified in $E/\mathbb{Q}$ and coprime to $4\mathscr{f}\omega$. Hence due to Corollary B.7, we know that

$$\begin{aligned}\prod_{p\mid D_2(m)}\widetilde{\rho}_Q(p^{\operatorname{ord}_p a+2})&=\prod_{p\mid D_2(m)}\frac{\rho_Q^0(p)}{p}p^{\operatorname{ord}_p a+2}\left(1-\frac{1}{p}\right)\\&\le D_2(m)^2\gcd(a,D_2(m)^\infty)\prod_{p\mid D_2(m)}2\left(1-\frac{1}{p}\right).\end{aligned}$$

We are left dealing with primes $p\mid a$ that are coprime to $\upsilon p_1 D_2(m)$. Because we have assumed $\gcd(a,D_0(m)D_1(m))=1$, we know that $p\nmid D_{\mathrm{small}}$. If $2<p\mid\omega$, then because of Proposition B.5,

$$\widetilde{\rho}_Q(p^{\operatorname{ord}_p a})\le 2\operatorname{ord}_p\omega p^{\operatorname{ord}_p\mathscr{f}}p^{\operatorname{ord}_p a}r_1(p^{\operatorname{ord}_p a}).$$

Applying Proposition B.5 for $p=2$, we deduce

$$\begin{aligned}\prod_{p\mid\gcd(4\omega,a)}\widetilde{\rho}_Q(p^{\operatorname{ord}_p a})&\ll_{\mathscr{f}}\gcd(a,\omega^\infty)r_1(\gcd(a,\omega^\infty))\prod_{p\mid\omega}2\operatorname{ord}_p\omega\\&\le\gcd(a,\omega^\infty)r_1(\gcd(a,\omega^\infty))|\omega|^2.\end{aligned}$$

In the last inequality we have used the facts $\prod_{p\mid\omega}2\le|\omega|$ and $\prod_{p\mid\omega}\operatorname{ord}_p\omega\le|\omega|\le d(|\omega|)\le|\omega|$, where $d(|\omega|)$ is the number of divisors of ω.

For any prime $p\mid a$ coprime to $4D_{\mathrm{small}}\omega$, we can apply Proposition B.3 and Corollary B.7 to deduce

$$\prod_{\substack{p\mid a\\ p\nmid 4D_{\mathrm{small}}\omega}}\widetilde{\rho}_Q(p^{\operatorname{ord}_p a})\ll_{\mathscr{f}}\prod_{\substack{p\mid a\\ p\nmid 4D_{\mathrm{small}}\omega}}p^{\operatorname{ord}_p a}r_1(p^{\operatorname{ord}_p a})\left(1+\frac{1}{p}\right).$$

The claim follows by combining all the inequalities above for the different cases of p. □

Proposition 10.13. *Let $m\in{}^{\mathbb{Z}}/_{k\mathbb{Z}}$ with $w_k(m)>0$. Let $\theta_l>0$ be admissible, fix $0<\eta<1/2$ and assume $R_{\max}^{\theta_l}\le A(\mathscr{E})^{1-4\eta}$. If $\upsilon p_1^{2n}\le|D|^{\eta/2}$,* *then*

$$\sum_{\substack{(x,y)\in\mathscr{E}\cap\mathbb{Z}^2\\ Q(x,y)\equiv m \bmod k}} (f\cdot r_0)\left(\frac{Q(x,y)}{\upsilon p_1^{2n}}\right)$$
$$\ll_{f,\eta,\mathbf{G}} A(\mathscr{E})p_1^{-2n}\frac{\rho_Q\left(m;(D_0(m)D_1(m))^2\right)}{(D_0(m)D_1(m))^4}\frac{2^{\omega(D_2(m))}}{D_2(m)^2}$$
$$\cdot\,|\omega|^2(\log\log(2|\omega|))^8 \prod_{\substack{2<p\leq 2\kappa|D|^{1-\eta}\\ p\nmid D_0(m)D_1(m)}}\left(1-\frac{\rho_Q(p)}{p^2}\right)\sum_{\substack{a\leq 2\kappa|D|\\ \gcd(a,D_0(m)D_1(m))=1}}\frac{f(a)}{a}.$$

Proof. We begin by substituting the result of Lemma 10.11 into Proposition 10.10 to see that

$$\sum_{\substack{(x,y)\in\mathscr{E}\cap\mathbb{Z}^2\\ Q(x,y)\equiv m \bmod k}} (f\cdot r_0)\left(\frac{Q(x,y)}{\upsilon p_1^{2n}}\right)$$
$$\ll_{f,\eta} A(\mathscr{E})p_1^{-2n}\frac{\rho_Q\left(m;(D_0(m)D_1(m))^2\right)}{(D_0(m)D_1(m))^4}\frac{2^{\omega(D_2(m))}}{D_2(m)^2}$$
$$\cdot\,\omega\log\omega \prod_{\substack{2<p\leq 2\kappa|D|^{1-\eta}\\ p\nmid \upsilon p_1 D_0(m)D_1(m)}}\left(1-\frac{\rho_Q(p)}{p^2}\right)$$
$$\cdot \sum_{\substack{a\leq 2\kappa|D|\\ \gcd(a,D_0(m)D_1(m))=1}}\frac{f(a)r_0(a)r_1(a)}{a}\left[\prod_{p|a}\left(1+\frac{1}{p}\right)\right].$$

Using Lemma 9.2 we deduce

$$\prod_{\substack{2<p\leq 2\kappa|D|^{1-\eta}\\ p\nmid \upsilon p_1 D_0(m)D_1(m)}}\left(1-\frac{\rho_Q(p)}{p^2}\right)\ll_{\mathbf{G}}\prod_{\substack{2<p\leq 2\kappa|D|^{1-\eta}\\ p\nmid D_0(m)D_1(m)}}\left(1-\frac{\rho_Q(p)}{p^2}\right).$$

Because $r_1(a)\leq r_0(a)$, to prove the claim we need only to show that

$$\sum_{\substack{a\leq 2\kappa|D|\\ \gcd(a,D_0(m)D_1(m))=1}}\frac{f(a)r_0(a)^2}{a}\left[\prod_{p|a}\left(1+\frac{1}{p}\right)\right]$$
$$\ll_{f,\eta}(\log\log(2|\omega|))^8\sum_{\substack{a\leq 2\kappa|D|\\ \gcd(a,D_0(m)D_1(m))=1}}\frac{f(a)}{a}.$$

We prove this by applying the decoupling lemma 9.18 twice. In the first application let $g(p^l) = f(p^l)r_0(p^l)^2/p^l$ if $p \nmid D_0(m)D_1(m)$ and $g(p^l) = 1$ otherwise, and let $h(p^l) = \left(1 + \frac{1}{p}\right)$ for $l \geq 1$. We can write $h = 1 * \psi$, where $\psi(p^l) = 0$ for $l \geq 2$ and $\psi(p) = 1/p$.

We need to estimate $\mathfrak{M}_z(g, \psi)$ as follows:

$$\begin{aligned}\mathfrak{M}_z(g,\psi) &\leq \prod_{p \leq \infty} \left[1 + \psi(p) \sum_{j=1}^{\infty} \frac{f(p^l)r_0(p^l)^2}{p^l}\right] \ll_{\ell} \prod_{p \leq \infty} \left[1 + \frac{1}{p} \sum_{j=1}^{\infty} \frac{2(k+1)}{p^l}\right] \\ &= \prod_{p \leq \infty} \left[1 + \frac{2}{p} \frac{2p-1}{(p-1)^2}\right] \leq \prod_{p \leq \infty} \left[1 + \frac{4}{(p-1)^2}\right] \ll 1,\end{aligned}$$

where we have used the trivial bound $f(p^l) \leq (k+1)/2$ for every $p \nmid \ell$. We have thus proved that

$$\sum_{\substack{a \leq 2\kappa|D| \\ \gcd(a, D_0(m)D_1(m))=1}} \frac{f(a)r_0(a)^2}{a} \left[\prod_{p|a} \left(1 + \frac{1}{p}\right)\right] \ll_{\ell} \sum_{\substack{a \leq 2\kappa|D| \\ \gcd(a, D_0(m)D_1(m))=1}} \frac{f(a)r_0(a)^2}{a}.$$

We continue by applying Lemma 9.18 again, this time with $g(p^l) = f(p^l)/p^l$ whenever $p \nmid D_0(m)D_1(m)$ and $g(p^l) = 1$ otherwise, and with $h(p^l) = r_0(p^l)^2$. We have $h = 1 * \psi$, where $\psi(p^{\operatorname{ord}_p D}) = 4$ for $p \mid D_{\text{high}}$ and $\psi(p^l) = 0$ for all other prime powers with $l \geq 1$. We estimate $\mathfrak{M}_z(g, \psi)$ in the following way:

$$\begin{aligned}\mathfrak{M}_z(g,\psi) &\leq \prod_{p|D_{\text{high}}} \left(1 + 4 \sum_{j=\operatorname{ord}_p D}^{\infty} \frac{f(p^l)}{p^l}\right) \ll_{\ell} \prod_{p|D_{\text{high}}} \left(1 + 4 \sum_{j=1}^{\infty} \frac{1}{p^l}\right) \\ &= \prod_{p|D_{\text{high}}} \left(1 + \frac{4}{p-1}\right) \leq \prod_{p|D_{\text{high}}} \left(1 + \frac{8}{p}\right) \leq \prod_{p|D_{\text{high}}} \left(1 + \frac{1}{p}\right)^8 \\ &\leq \prod_{p|\omega} \left(1 + \frac{1}{p}\right)^8 \prod_{\substack{p|D \\ p > \eta/(4C_\theta)\log|D|}} \left(1 + \frac{1}{p}\right)^8.\end{aligned}$$

We bound the two factors above separately. The first one can be bounded because

$$\prod_{p|\omega} \left(1 + \frac{1}{p}\right) \ll \log\log(2|\omega|).$$

For the second factor, we have the following upper bound due to (52):

$$\prod_{\substack{p|D \\ p > \eta/(4C_\theta)\log|D|}} \left(1 + \frac{1}{p}\right) \leq \prod_{\eta/(4C_\theta)\log|D| < p \leq C_\theta \log|D|} \left(1 + \frac{1}{p}\right) \ll_{\eta} 1. \qquad \square$$

The second inequality holds due to Mertens' theorem.

Proposition 10.14. *Let* $m \in {}^{\mathbb{Z}}/_{k\mathbb{Z}}$ *with* $w_k(m) > 0$. *Fix* $1/2 > \eta > 0$. *If* $C > 0$ *satisfies*

$$\frac{L'(1,\chi_E)}{L(1,\chi_E)} \leq C \log |D_E|,$$

then

$$\prod_{\substack{2<p\leq 2\kappa|D|^{1-\eta} \\ p\nmid D_0(m)D_1(m)}} \left(1 - \frac{\rho_Q(p)}{p^2}\right) \sum_{\substack{a\leq 2\kappa|D| \\ \gcd(a,D_0(m)D_1(m))=1}} \frac{f(a)}{a}$$

$$\ll_{C,\eta} L(1,\chi_E) \prod_{p|f} \left(1 - \left(\frac{D_E}{p}\right)\frac{1}{p}\right) + |D|^{-2/3+o(1)}.$$

Proof. We first estimate the product over primes appearing above. From Propositions B.3 and B.5 we deduce that $\rho_Q(p) \geq p-1$ for all primes p. Thus

(53)

$$\begin{aligned}
\prod_{\substack{2<p\leq 2\kappa|D|^{1-\eta} \\ p\nmid D_0(m)D_1(m)}} \left(1 - \frac{\rho_Q(p)}{p^2}\right) &\leq \prod_{\substack{2<p\leq 2\kappa|D|^{1-\eta} \\ p\nmid D_0(m)D_1(m)}} \left(1 - \frac{1}{p} + \frac{1}{p^2}\right) \\
&\leq \prod_{\substack{2<p\leq 2\kappa|D|^{1-\eta} \\ p\nmid D_0(m)D_1(m)}} \left(1 - \frac{1}{p}\right) \prod_{p<\infty} \left(1 + \frac{1}{p^2 - p}\right) \\
&\leq \prod_{\substack{2<p\leq 2\kappa|D|^{1-\eta} \\ p\nmid D_0(m)D_1(m)}} \left(1 - \frac{1}{p}\right) \prod_{p<\infty} \left(1 + \frac{2}{p^2}\right) \ll \prod_{\substack{2<p\leq 2\kappa|D|^{1-\eta} \\ p\nmid D_0(m)D_1(m)}} \left(1 - \frac{1}{p}\right) \\
&\ll \log(2\kappa|D|^{1-\eta})^{-1} \prod_{p|D_0(m)D_1(m)} \left(1 - \frac{1}{p}\right)^{-1}.
\end{aligned}$$

The last inequality above follows from Mertens' theorem.

The logarithmic mean

$$\sum_{\substack{a\leq 2\kappa|D| \\ \gcd(a,D_0(m)D_1(m))=1}} \frac{f(a)}{a}$$

can be estimated using standard tools from multiplicative number theory. Consider the multiplicative function g defined by $g(p^l) = f(p^l)$ if $p \nmid D_0(m)D_1(m)$ and $g(p^l) = 1$ if $g \mid D_0(m)D_1(m)$. Then because of the decomposition $\zeta_E(s) = \zeta(s)L(s,\chi_E)$ with $L(s,\chi_E)$ holomorphic, the Dirichlet series of g can be written as $L_g(s) = \zeta(s)\widetilde{L_g}(s)$ with $\widetilde{L_g}(s)$ holomorphic.

Let $\varphi\colon [0,\infty) \to [0,\infty)$ be a compactly-supported smooth non-increasing function satisfying $\mathbb{1}_{[0,1]} \leq \varphi \leq \mathbb{1}_{[0,2]}$; i.e., φ is a smooth approximation of the characteristic function of $[0,1]$. Notice that the Mellin transform satisfies

$s\mathscr{M}(\varphi)(s) = \mathscr{M}(\Theta\varphi)(s)$, where $\Theta(\varphi)(x) = -x\varphi'(x) \geq 0$ is a smooth compactly-supported function vanishing outside of $[1, 2]$. Hence $s\mathscr{M}(\varphi)(s)$ decays faster than any polynomial in the vertical direction. The decay is uniform in any strip of the form $\sigma_0 \leq \Re(s) \leq \sigma_1$. The same property holds for $\mathscr{M}(\varphi)(s)$ outside a small neighborhood of $s = 0$. Moreover, the the Laurent expansion of $\mathscr{M}(\varphi)(s)$ around $s = 0$ is $\frac{1}{s} + \int_1^\infty \frac{\varphi(x)}{x}\,\mathrm{d}x + O(|s|)$. Using contour integration, the Perron formula and the decay of Dirichlet L-functions in the vertical direction, we see that

(54)

$$\sum_{\substack{a \leq 2\kappa|D| \\ \gcd(a, D_0(m)D_1(m))=1}} \frac{f(a)}{a} \leq \widetilde{L_g}(1)\left(\log(2\kappa|D|) + \gamma + \frac{\widetilde{L_g}'(1)}{\widetilde{L_g}(1)} + \int_1^\infty \frac{\varphi(x)}{x}\,\mathrm{d}x\right)$$
$$+ \frac{1}{2\pi}\int_{-\infty}^{\infty} \frac{|L_g(1/2+it)|}{(2\kappa|D|)^{1/2}} |\mathscr{M}\varphi(-1/2+it)|\,\mathrm{d}t,$$

where γ is the Euler-Mascheroni constant.

Because all the primes $p \mid D_0(m)D_1(m)$ are ramified in $E/\mathbb{Q}$ and coprime to $\mathscr{f}$, the following properties of $\widetilde{L_g}(s)$ are an immediate consequence of comparing the Euler product of $L_g(s)$ with that of $\zeta_E(s)$:

$$\widetilde{L_g}(1) = L(1, \chi_E)\prod_{p|\mathscr{f}}\left(1 - \left(\frac{D_E}{p}\right)\frac{1}{p}\right)\prod_{p|D_0(m)D_1(m)}\left(1 - \frac{1}{p}\right),$$
$$\left|\frac{\widetilde{L_g}'(1)}{\widetilde{L_g}(1)} - C\log|D_E|\right| \ll 1,$$
$$|\widetilde{L_g}(1/2+it)| \ll_{\mathscr{f}} |L(1/2+it, \chi_E)| \ll_{\mathscr{f}} |D|^{1/6+o(1)}|1/2+it|^A.$$

The constant $A > 0$ is absolute. The last inequality for $|L(1/2, \chi_E)|$ is due to Conrey and Iwaniec [CI00, Cor. 1.5] strengthening the convexity breaking result of Burgess [Bur62] for real characters. Substituting these and (53) into (54) and using the super-polynomial decay of $|\mathscr{M}(\varphi)(1/2+it)|$, we deduce

$$\prod_{\substack{2<p\leq 2\kappa|D|^{1-\eta} \\ p\nmid D_0(m)D_1(m)}}\left(1 - \frac{\rho_Q(p)}{p^2}\right) \leq \log(2\kappa|D|^{1-\eta})^{-1} L(1, \chi_E)\prod_{p|\mathscr{f}}\left(1 - \left(\frac{D_E}{p}\right)\frac{1}{p}\right)$$
$$\cdot\left(\log(2\kappa|D|) + C\log|D| + O(1)\right) + O(1)\cdot\frac{|D|^{1/6+o(1)}}{(2\kappa|D|)^{1/2}}$$
$$\ll_{\eta,C} L(1, \chi_E)\prod_{p|\mathscr{f}}\left(1 - \left(\frac{D_E}{p}\right)\frac{1}{p}\right) + |D|^{-2/3+o(1)}. \qquad \square$$

We can now combine all the results of this section to deduce a final bound on the shifted convolution sum.

Proposition 10.15. *Let $\theta_l > 0$ be admissible, fix $0 < \eta < 1/2$ and assume $R_{\max}^{\theta_l} \leq A(\mathscr{E})^{1-4\eta}$. Suppose $\upsilon p_1^{2n} \leq |D|^{\eta/2}$. If $C > 0$ satisfies*

$$\frac{L'(1,\chi_E)}{L(1,\chi_E)} \leq C \log |D_E|,$$

then

$$\sum_{\substack{0\leq x\leq \kappa|D| \\ x\equiv w|D| \mod \upsilon p_1^{2n}}} g_{[\mathfrak{s}]}(x) f_{[p_1^n \mathfrak{s}\mathfrak{e}]^{-1}}\left(\frac{x-\omega D}{\upsilon p_1^{2n}}\right) r\left(\frac{x-\omega D}{\upsilon p_1^{2n}}\right)$$
$$\ll_{\mathbf{G},\ell,\eta,C} \kappa|\omega| \log(2|\omega|)(\log\log(2|\omega|))^8 \frac{\sqrt{|D|}\left(L(1,\chi_E)+|D|^{-2/3+o(1)}\right)}{p_1^{2n}}.$$

Proof. In this proof only we allow all implicit constants to depend on $C, \eta, \ell, \mathbf{G}$ without specifying that further.

From Lemmata 10.2, 10.6 and Propositions 10.13 and 10.14 we deduce that the shifted convolution sums is bounded above by

$$A(\mathscr{E}) p_1^{-2n}\left(L(1,\chi_E)+|D|^{-2/3+o(1)}\right)|\omega|^2(\log\log(2|\omega|))^8$$
$$\cdot \int_{m\equiv 0 \bmod \upsilon p_1^{2n}} \frac{\rho_Q\left(m;(D_0(m)D_1(m))^2\right)}{(D_0(m)D_1(m))^4}\frac{2^{\omega(D_2(m))}}{D_2(m)^2}\,\mathrm{d}w_k(m).$$

The claim would follow immediately from the formula for $A(\mathscr{E})$ in Lemma 10.4 if we prove that

$$\int_{m\equiv 0 \bmod \upsilon p_1^{2n}} \frac{\rho_Q\left(m;(D_0(m)D_1(m))^2\right)}{(D_0(m)D_1(m))^4}\frac{2^{\omega(D_2(m))}}{D_2(m)^2}\,\mathrm{d}w_k(m) \ll 1.$$

The integrand decomposes as a product of functions on $\mathbb{Z}/_{p^2\mathbb{Z}}$ for $p \mid D_{\mathrm{small}}$, and the measure is a product measure. Thus we can use Fubini to write

$$\int_{m\equiv 0 \bmod \upsilon p_1^{2n}} \frac{\rho_Q\left(m;(D_0(m)D_1(m))^2\right)}{(D_0(m)D_1(m))^4}\frac{2^{\omega(D_2(m))}}{D_2(m)^2}\,\mathrm{d}w_k(m)$$
$$= \prod_{p\mid D_{\mathrm{small}}}\left[\frac{2}{p^2}w_p(0) + \sum_{0\neq a\in \mathbb{Z}/_{p^2\mathbb{Z}}} \frac{\rho_Q(a;p^2)}{p^4} w_p(a)\right].$$

We bound the term for each $p \mid D_{\mathrm{small}}$ using the definition of w_p and Proposition B.8:

$$\frac{2}{p^2}w_p(0) + \sum_{0\neq a\in \mathbb{Z}/_{p^2\mathbb{Z}}} \frac{\rho_Q(a;p^2)}{p^4}w_p(a) = \frac{4}{p^2} + \left(1-\frac{1}{p}\right) + \frac{1}{p}\left(1-\frac{f}{p}\right)$$
$$= 1 + \frac{4-f}{p^2} \leq 1 + \frac{5}{p^2},$$

where

$$f = 1 + \epsilon\left(\frac{-D/p}{p}\right)\chi_p(\mathrm{Nr}\,\mathfrak{s}^{-1}) + \left(\frac{\omega}{p}\right)\chi_p(\mathrm{Nr}\,\mathfrak{s}^{-1}) \in \{-1,1,3\}.$$

We conclude that the integral in question is bounded above by

$$\prod_{p<\infty}\left(1+\frac{5}{p^2}\right) \ll 1. \qquad \square$$

10.4. *Conclusion of the proof.* Let $\theta_l > 0$ be an admissible exponent for lattice counting in ellipses. If there is some $\eta_0 > 0$ such that for all $i \gg 1$

$$\mathfrak{N}_i \geq |D_i|^{(2-\theta_l^{-1})/3+\eta_0}, \tag{55}$$

then using Lemma 10.4 we can deduce that the condition $R_{\max}^{\theta_l} \leq A(\mathscr{E})^{1-4\eta}$ holds for all $\mathscr{H}_i$ in the sequence where $1/2 > \eta > 0$ depends only on η_0 and θ_l. Assume first that such $\eta_0 > 0$ exists. The condition that all fields $E_i/\mathbb{Q}$ have no exceptional zero implies that there is $C > 0$ independent of i such that

$$\frac{L'(1,\chi_{E_i})}{L(1,\chi_{E_i})} \leq C\log|D_{E_i}|.$$

This result has been attributed to Hecke by Landau [Lan18].

Let $\xi \in (\mathbf{G}\times\mathbf{G})(\mathbb{A})$. Fix $n \in \mathbb{N}$. Then for any $i \gg_{p_1,n,\varepsilon,\mathbf{G}} 1$, we have $\upsilon p_1^{2n} \leq |D_i|^{\eta/2}$. Moreover, the assumptions of Theorem 3.2 imply that

$$g_i^{-1}\mathbf{T}_i(\mathbb{Q})s_i g_i \cap B^{(-n,n)}\operatorname{ctr}(\xi)B^{(-n,n)} = \emptyset$$

for all $i \gg_\xi 1$.

Thus for i large enough, we can use Proposition 10.15 and Theorem 8.7 to deduce that for any $n \in \mathbb{N}$,

$$\begin{aligned}\mathrm{Cor}[\mu_i,\nu_\xi](B^{(-n,n)}) &\ll_{\mathbf{G},\varepsilon,\mathfrak{f}} \mathrm{vol}\left([\mathbf{T}(\mathbb{A})g]\right)^{-1}\mathrm{vol}\left(\left[\mathbf{G}^{\Delta}(\mathbb{A})^+\xi\right]\right)^{-1}p_1^{-2n}\\ &\qquad\cdot\kappa|\omega|^2(\log\log(2|\omega|))^8\frac{\sqrt{|D|}\left(L(1,\chi_E)+|D|^{-2/3+o(1)}\right)}{p_1^{2n}}\\ &\ll_{\mathfrak{f}} \mathrm{vol}\left(\left[\mathbf{G}^{\Delta}(\mathbb{A})^+\xi\right]\right)^{-1}\kappa|\omega|^2(\log\log(2|\omega|))^8 p_1^{-4n}.\end{aligned}$$

The last inequality follows from the computation of the volume of a homogeneous toral set using the analytic class number formula; cf. [ELMV11]. The expression $\kappa|\omega|^2(\log\log(2|\omega|))^8$ is a continuous function of $\operatorname{ctr}(\xi)$ as can be seen from the definition of κ and ω in Theorem 8.7. Moreover, the definition of the volume implies immediately that $\operatorname{vol}\left(\left[\mathbf{G}^{\Delta}(\mathbb{A})^{+}\xi\right]\right)$ is a non-vanishing continuous function of $\xi \in {}_{\mathbf{G}^{\Delta}(\mathbb{A})^{+}}\backslash^{(\mathbf{G}\times\mathbf{G})(\mathbb{A})}$. Because the fiber of the continuous map $\operatorname{ctr}\colon {}_{\mathbf{G}^{\Delta}(\mathbb{A})^{+}}\backslash^{(\mathbf{G}\times\mathbf{G})(\mathbb{A})} \to \mathbf{G}(\mathbb{A})$ is compact,[11] the function $\xi \mapsto \operatorname{vol}\left(\left[\mathbf{G}^{\Delta}(\mathbb{A})^{+}\xi\right]\right)$ is bounded below by a non-vanishing continuous function of $\operatorname{ctr}(\xi)$.

We deduce that if condition (55) holds, then the proof is concluded by Lemma 10.1. If condition (55) fails, then the theorem follows from the methods of Ellenberg, Michel and Venkatesh [EMV13, §3], which are based on Linnik's method for equidistribution of CM points. Although the argument of [EMV13, §3] applies verbatim only to the case of $\mathbf{G}$ ramified at ∞ and functions invariant under an Iwahori at the place p_1, these restrictions are relaxed using the technical improvements presented in [Kha17, §5].

The following discussion is a recap of [EMV13] with an emphasis on the required adaptation when removing the restriction $\gcd(\mathfrak{N}_i, p_1) = 1$. Let $m \in \mathbb{N}$ to be determined later. Because we have assumed a splitting condition for two primes we can use the flow either at p_1 or at p_2. The input required by [EMV13] and [Kha17] is a norm gap for the Hecke operator

$$T_{p_j^m}\colon {}_{\mathbf{G}^{\mathrm{sc}}(\mathbb{Q})}\backslash^{\mathbf{G}^{\mathrm{sc}}(\mathbb{A})}/_{U} \to {}_{\mathbf{G}^{\mathrm{sc}}(\mathbb{Q})}\backslash^{\mathbf{G}^{\mathrm{sc}}(\mathbb{A})}/_{U},$$

where $j \in \{1,2\}$ and $U = \prod_p U_p < \mathbf{G}^{\mathrm{sc}}(\mathbb{A}_f)$ is a compact-open subgroup such that U_{p_j} is the intersection of two Iwahori in the apartment corresponding to A_{p_j}. Fix $K_{p_j} < \mathbf{G}^{\mathrm{sc}}(\mathbb{Q}_{p_j})$ as a maximal compact subgroup containing U_{p_j}. The following norm gap for $T_{p_j^m}$ follows for any $\varepsilon > 0$ from the decay of matrix coefficients of automorphic representations of $\mathbf{SL}_2$ [Sar91], [BS91], [CU04], [COU01] and the Jacquet-Langlands correspondence [JL70]:

$$\|T_{p_j^m}\|_0 \ll_{U^{p_j},p_j,\epsilon} [K_{p_j} : U_{p_j}] p_j^{-m(1-\theta+\epsilon)/2}, \tag{56}$$

where $\|T_{p_j^m}\|_0$ is the norm of $T_{p_j^m}$ restricted to the subspace of $L^2\left([\mathbf{G}^{\mathrm{sc}}(\mathbb{A})]\right)^U$ orthogonal to the constant function, $U^{p_j} = \prod_{p\neq p_j} U_p$ and θ is the best bound towards the Generalized Ramanujan Conjecture for $\mathbf{SL}_2$ in the sense of [CU04]. The dependence of the constant on the parameters U^{p^j}, p_j and ϵ is effective and can be made explicit.

In the Ellenberg-Michel-Venkatesh argument we restrict a joint homogeneous toral set to an ambient Hecke correspondence of volume $\mathfrak{N}_i \prod_{p|\mathfrak{N}_i}\left(1+\frac{1}{p}\right)$

[11] The fiber is isomorphic to $^{\mathbf{G}(\mathbb{A})}/_{\mathbf{G}(\mathbb{A})^{+}}$.

and apply an effective equidistribution argument in conjunction with Linnik's Basic Lemma to show that the joint period toral measure is close to the Haar measure on the ambient Hecke correspondence.

Let $a_j \in A_{p_j}$ be as in Definition 5.22. We can use the effective equidistribution theorem from [Kha17], which builds upon the work of [Lin68], [EMV13], to deduce the necessary equidistribution result for the argument of Ellenberg-Michel-Venkatesh as long as for each i there is some m such that $\|T_{p_j^m}\|_0 < 1/2$ and that Linnik's Basic Lemma is valid for $p_1^{m(1+\epsilon')}$ for some $\epsilon' > 0$.

If $p_j \mid \mathfrak{N}_i$, we know that $[K_{p_j} \colon U_{p_j}] = p_j^{\operatorname{ord}_{p_j} \mathfrak{N}_i}\left(1+\frac{1}{p_j}\right)$; cf. Section 7. Because of the freedom to use either p_1 or p_2, we can assume without loss of generality that

$$p_1^{\operatorname{ord}_{p_1} \mathfrak{N}_i} \leq \sqrt{\mathfrak{N}_i}.$$

For a fixed U^{p_1}, the bound $\|T_{p_1^m}\|_0 < 1/2$ would follow from (56) for any $m \in \mathbb{N}$ satisfying

$$p_1^m \gg_{U^{p_1}, p_1, \epsilon} \mathfrak{N}_i^{1/(1-\theta+\epsilon)}. \tag{57}$$

On the other hand, Linnik's Basic Lemma for *one-sided* Bowen balls in this setting (cf. [EMV13]) applies only for $m \in \mathbb{N}$ in the range

$$\mathfrak{N}_i p_1^m \leq |D|^{1/2+o(1)}, \tag{58}$$

where the $o(1)$ is ineffective as it is derived from Siegel's bound. There exists an $m \in \mathbb{N}$ satisfying both (57) and (58) if

$$\mathfrak{N}_i^{1+1/(1-\theta+\epsilon)} \ll_{U^{p_1}, p_1, \epsilon} |D|^{1/2+o(1)}.$$

This condition is satisfied if we know that there is $\epsilon_1 > 0$ such that for all $i \gg 1$,

$$\mathfrak{N}_i \leq |D|^{\frac{1}{2+2/(1-\theta)}-\epsilon_1}. \tag{59}$$

In the range (59) the conclusion of the Ellenberg-Michel-Venkatesh argument is that for any limit measure μ, one has $\int f \, \mathrm{d}\mu = 0$ for any smooth compactly supported $f \in L^2_{00}\left(\left[(\mathbf{G}\times\mathbf{G})(\mathbb{Q})\right], m_{\mathbf{G}\times\mathbf{G}}\right)$ that is invariant in the place p_1 under an intersection of two Iwahori subgroups stabilizing edges in the apartment of A_{p_1}.

We can now bootstrap this to deduce the conclusion of the theorem. Let $A^0_{p_1} < A_{p_1}$ be the maximal compact subgroup of the torus. Using a decreasing sequence of intersections of two Iwahori, we conclude that the push forward of the limit measure μ to

$$(\mathbf{G}\times\mathbf{G})(\mathbb{Q}) \backslash (\mathbf{G}\times\mathbf{G})(\mathbb{A}) / A^0_{p_1} \times A^0_{p_1}$$

is a measure of maximal entropy for the action of a^{Δ} for any element of $a \in A_{p_1}^{+}$ that is not contained in a compact subgroup. As this factor and the space $[(\mathbf{G} \times \mathbf{G})(\mathbb{A})]$ have the same maximal entropy for a^{Δ}, we deduce that any limit measure μ has maximal entropy for a on $[(\mathbf{G} \times \mathbf{G})(\mathbb{A})]$, which implies it is $(\mathbf{G} \times \mathbf{G})(\mathbb{A})^{+}$-invariant.

To conclude the proof we need to verify that the range of (55) overlaps with the range of (59). Taking $\theta_l > 2/3$ from Van der Corput's bound [vdC20] and $\theta = 1/2$ from Gelbart-Jacquet, we see that any improvement to either bound would imply the necessary overlap in ranges. This can be achieved either by taking a smaller admissible value of θ_l such as provided by [Hux03] or using any improvement towards Ramanujan beyond $\theta \leq 1/2$ as in [Sha88], [LRS99].

Appendix A. Principal genus theory

In this appendix we collect results related to the principal genus theory of quadratic orders. The results we discuss are classical when presented in an elementary form, going back to Gauss in the case of maximal orders.[12] Unfortunately, the author is unfamiliar with a modern concise presentation treating the case of non-maximal orders. This appendix contains all the statements that are of use in this manuscript with complete proofs.

As is usually the case with topics in algebraic number theory the treatment is significantly streamlined by the use of adéles. Noticeable features of the presentation below are that it uses class field theory only for quadratic extension and does not resort to the properties of ring class fields and genus fields. The main tools are Hilbert's Satz 90 for quadratic global and local fields, and the Hasse norm theorem, which for quadratic fields was proven by Hilbert and elementary Galois cohomology. Except for treatment of the wild prime 2, I have tried to circumvent explicit computations wherever possible.

Notation. Let Λ be an order in an imaginary quadratic extension $E < \mathbb{Q}$. As usual we denote by D the discriminant of Λ and define Λ_v to be the closure of Λ in $E_v \coloneqq \prod_{w|v} E_w$ for any rational place $v \neq \infty$.

A.1. *Adelic form of* $\operatorname{Pic}(\Lambda)/\operatorname{Pic}(\Lambda)^2$. The adelic interpretation below is used both for computing the structure of the group ${}^{\operatorname{Pic}(\Lambda)}\!/_{\operatorname{Pic}(\Lambda)^2}$ and in describing the characters in the dual group $\widehat{\operatorname{Pic}(\Lambda)}$ vanishing on $\operatorname{Pic}(\Lambda)^2$ using Kronecker symbols of ideal norms.

[12] The reader interested in the history of the development of principal genus theory can consult the review [Lem07] by Lemmermeyer.

Proposition A.1. *The adelic norm map* $\mathrm{Nr}\colon \mathbb{A}_E^\times \to \mathbb{A}^\times$ *and the real adelic character* $\chi_E\colon {}_{\mathbb{Q}^\times}\backslash^{\mathbb{A}^\times} \to \{\pm 1\}$ *attached to the quadratic extension* $E/\mathbb{Q}$ *by global class field theory descend to a short exact sequence*

$$1 \to {}^{\operatorname{Pic}(\Lambda)}/_{\operatorname{Pic}(\Lambda)^2} \xrightarrow{\mathrm{Nr}} {}_{\mathbb{Q}^\times}\backslash^{\mathbb{A}^\times}/_{\mathbb{R}_{>0}\prod_{v\neq\infty}\mathrm{Nr}\,\Lambda^\times} \xrightarrow{\chi_E} \{\pm 1\} \to 1.$$

Proof. Recall that $\operatorname{Pic}(\Lambda) \simeq {}_{E^\times}\backslash^{\mathbb{A}_E^\times}/_{\mathbb{C}^\times \prod_{v\neq\infty}\Lambda_v^\times}$. Because σ acts by inversion on $\operatorname{Pic}(\Lambda)$, the group $\operatorname{Pic}(\Lambda)^2$ is equal to the group of coboundaries $\operatorname{cbd}(\operatorname{Pic}(\Lambda))$. Hence $\operatorname{Pic}(\Lambda)^2$ is the image of $\prod_v \operatorname{cbd}(E_v) < \mathbb{A}_E^\times$ in ${}_{E^\times}\backslash^{\mathbb{A}_E^\times}/_{\mathbb{C}^\times \prod_{v\neq\infty}\Lambda_v^\times}$. Hilbert's Satz 90 implies $\operatorname{cbd}(E_v) = E_v^{(1)}$ for each v, hence $\prod_v \operatorname{cbd}(E_v)$ is the kernel of the norm map $\mathbb{A}_E^\times \to \mathbb{A}^\times$.

The norm map descends to a map

$$\mathrm{Nr}\colon {}_{E^\times}\backslash^{\mathbb{A}_E^\times} \to {}_{\mathbb{Q}^\times}\backslash^{\mathbb{A}^\times}.$$

The Hasse norm theorem implies that the kernel of this map is the projection of $\prod_v \operatorname{cbd}(E_v)$. Global class field theory states that the image is the kernel of χ_E. It follows that there is a norm map

$$\mathrm{Nr}\colon \operatorname{Pic}(\Lambda) \to {}_{\mathbb{Q}^\times}\backslash^{\mathbb{A}^\times}/_{\mathbb{R}_{>0}\prod_{v\neq\infty}\mathrm{Nr}\,\Lambda_v^\times}$$

with kernel $\operatorname{Pic}(\Lambda)^2$. Moreover, the conductor of the quadratic character χ_E contains $\mathrm{Nr}\,E_\infty^\times \prod_{v\neq\infty}\mathrm{Nr}\,\mathcal{O}_{E_v}^\times$, thus χ_E factors through the right-hand side above and its kernel is the image of Nr. □

Corollary A.2. *The index* $\left[\operatorname{Pic}(\Lambda)\colon \operatorname{Pic}(\Lambda)^2\right]$ *can be computed by*

$$2\left[\operatorname{Pic}(\Lambda)\colon \operatorname{Pic}(\Lambda)^2\right] = \prod_{v\neq\infty}\left[\mathbb{Z}_v^\times\colon \mathrm{Nr}\,\Lambda_v^\times\right].$$

Proof. By Proposition A.1 above, the group ${}_{\mathbb{Q}^\times}\backslash^{\mathbb{A}^\times}/_{\mathbb{R}_{>0}\prod_{v\neq\infty}\mathrm{Nr}\,\Lambda^\times}$ is a 2-cover of ${}^{\operatorname{Pic}(\Lambda)}/_{\operatorname{Pic}(\Lambda)^2}$. Thus we need only to compute the size of this adelic quotient.

We use the fact that $\mathbb{Q}$ has class number 1 to conclude that the following sequence is exact:

$$1 \to \mathbb{Z}^\times \cdot \mathbb{R}_{>0}\prod_{v\neq\infty}\mathrm{Nr}\,\Lambda_v^\times \to \mathbb{R}^\times \prod_{v\neq\infty}\mathbb{Z}_v^\times \to {}_{\mathbb{Q}^\times}\backslash^{\mathbb{A}^\times}/_{\mathbb{R}_{>0}\prod_{v\neq\infty}\mathrm{Nr}\,\Lambda_v^\times} \to 1.$$

Moreover, the inclusion map descends to an isomorphism

$$\prod_{v\neq\infty} {}^{\mathbb{Z}_v^\times}/_{\mathrm{Nr}\,\Lambda_v^\times} \to {}_{\mathbb{Z}^\times}\backslash^{\mathbb{R}^\times\prod_{v\neq\infty}\mathbb{Z}_v^\times}/_{\mathbb{R}_{>0}\prod_{v\neq\infty}\mathrm{Nr}\,\Lambda_v^\times}.$$

□

The following two lemmata are necessary in order to understand non-maximal orders in terms of their reduction modulo the conductor.

Lemma A.3. *Assume $\Lambda_v < \mathcal{O}_{E_v}$ is a* non-*maximal order. Let $\mathfrak{f}_v\mathcal{O}_{E_v}$ be the conductor of Λ_v. Then $1+\mathfrak{f}_v\mathcal{O}_{E_v} \subseteq \Lambda_v^\times$.*

Proof. Because Λ_v is non-maximal, $\operatorname{ord}_v \mathfrak{f}_v \geq 1$ for $\mathfrak{f}_v \in \mathbb{Z}_v$ as above. This implies that the Taylor series for $\frac{1}{1+x}$ converges for any $x \in \mathfrak{f}_v\mathcal{O}_{E_v}$. As Λ_v is a closed subset, we deduce $(1+x)^{-1} \in \Lambda_v$. □

Lemma A.4. *Assume $\Lambda_v < \mathcal{O}_{E_v}$ is a non-maximal order. Consider the reduction map $\operatorname{red}_{\mathfrak{f}_v} \colon \mathcal{O}_{E_v} \to {}^{\mathcal{O}_{E_v}}\!/\!_{\mathfrak{f}_v\mathcal{O}_{E_v}}$. Then*

$$\Lambda_v^\times = \operatorname{red}_{\mathfrak{f}_v}^{-1}(\operatorname{red}_{\mathfrak{f}_v}(\mathbb{Z})^\times) = \mathbb{Z}_v^\times + \mathfrak{f}_v\mathcal{O}_{E_v}$$

Proof. Notice that $\Lambda_v = \operatorname{red}_{\mathfrak{f}_v}^{-1}(\operatorname{red}_{\mathfrak{f}_v}(\mathbb{Z}_v)) = \operatorname{red}_{\mathfrak{f}_v}^{-1}(\operatorname{red}_{\mathfrak{f}_v}(\mathbb{Z}))$. The first equality follows from Lemma 2.3, and the second equality holds because $\mathbb{Z}$ is dense in $\mathbb{Z}_v$. It follows immediately that $\Lambda_v^\times \subseteq \operatorname{red}_{\mathfrak{f}_v}^{-1}(\operatorname{red}_{\mathfrak{f}_v}(\mathbb{Z})^\times)$. The reverse inclusion is a consequence of Lemma A.3. □

We now compute the groups $\operatorname{Nr}\Lambda_v^\times$ appearing in Proposition A.1.

Lemma A.5. *Fix $v \neq \infty$, and denote by p the residue characteristic of $\mathbb{Q}_v$. Then*

$$\operatorname{Nr}\mathcal{O}_{E_v}^\times = \begin{cases} \mathbb{Z}_v^\times & E_v/\mathbb{Q}_v \text{ is unramified,} \\ \mathbb{Z}_v^{\times 2} & E_v/\mathbb{Q}_v \text{ is ramified and } p > 2. \end{cases}$$

If $p = 2$ ramifies in $E/\mathbb{Q}$, then $\operatorname{Nr}\mathcal{O}_{E_v}^\times$ is one of the three possible index 2 subgroups of $\mathbb{Z}_2^\times$ containing the index 4 subgroup $\mathbb{Z}_2^{\times 2}$, i.e., one of the index 2 subgroups of

$$\mathbb{Z}_v^\times/_{\mathbb{Z}_v^{\times 2}} \simeq \left(\mathbb{Z}/_{8\mathbb{Z}}\right)^\times \simeq \mathbb{Z}/_{2\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}}.$$

Proof. Notice that $\mathbb{Z}_v^\times < \mathcal{O}_{E_v}^\times$ hence $\mathbb{Z}_v^{\times 2} < \operatorname{Nr}\mathcal{O}_{E_v}^\times$ for all $v \neq \infty$. The claim now follows immediately from the local class field correspondence between degree 2 extensions of $\mathbb{Q}_v$ and index 2 subgroups of $\mathbb{Q}_v^\times$. □

Lemma A.6. *Assume $\Lambda_v \lneq \mathcal{O}_{E_v}$ is a* non-*maximal order. If $p > 2$, then*

$$\operatorname{Nr}\Lambda_v^\times = \mathbb{Z}_v^{\times 2}.$$

If $p = 2$, *then*

$$\operatorname{Nr}\Lambda_v^\times = \begin{cases} \operatorname{Nr}\mathcal{O}_{E_v}^\times & 2 \parallel \mathfrak{f}_v, \\ 1 + 4\mathbb{Z}_2 & \begin{matrix} 4 \parallel \mathfrak{f}_v \textit{ and } E_v/\mathbb{Q}_v \textit{ is unramified} \\ \textit{or } \operatorname{Nr}\mathcal{O}_{E_v}^\times = 1 + 4\mathbb{Z}_2, \end{matrix} \\ 1 + 8\mathbb{Z}_2 = \mathbb{Z}_v^{\times 2} & \textit{otherwise.} \end{cases}$$

Proof. For any $v \neq \infty$, we have $\mathbb{Z}_v^\times < \Lambda_v^\times$ and $\mathbb{Z}_v^{\times 2} < \operatorname{Nr}\Lambda_v^\times$. Also for all v, we know $\operatorname{Nr}\Lambda_v^\times < \operatorname{Nr}\mathcal{O}_{E_v}^\times$. Hence if $E_v/\mathbb{Q}_v$ is ramified and $p > 2$, then Lemma A.5 implies that $\operatorname{Nr}\Lambda_v^\times = \mathbb{Z}_v^{\times 2}$.

Assume now that $E_v/\mathbb{Q}_v$ is unramified or $p = 2$. We compute $\operatorname{Nr}\mathcal{O}_{E_v}^\times/\operatorname{Nr}\Lambda_v^\times$ in the following way:

$$\begin{aligned} \operatorname{Nr}\mathcal{O}_{E_v}^\times/\operatorname{Nr}\Lambda_v^\times &\simeq \mathcal{O}_{E_v}^\times\backslash\Lambda_v^\times/\mathcal{O}_{E_v}^{(1)} \simeq \operatorname{red}_{\mathfrak{f}_v}(\mathcal{O}_{E_v})^\times\backslash\operatorname{red}_{\mathfrak{f}_v}(\Lambda_v)^\times/\mathcal{O}_{E_v}^{(1)} \\ &\simeq \operatorname{Nr}\operatorname{red}_{\mathfrak{f}_v}(\mathcal{O}_{E_v})^\times/\operatorname{Nr}\operatorname{red}_{\mathfrak{f}_v}(\Lambda_v)^\times \\ &= \operatorname{red}_{\mathfrak{f}_v}\operatorname{Nr}(\mathcal{O}_{E_v})^\times/\operatorname{red}_{\mathfrak{f}_v}\operatorname{Nr}(\Lambda_v)^\times. \end{aligned}$$

The first and the third equalities above hold because the kernels of the norm maps are the corresponding norm 1 elements; the second equality follows from Lemma A.4, and the fourth equality holds because the reduction map is equivariant for the Galois action. As all the isomorphisms above are canonical their composite is exactly the reduction map $\operatorname{red}_{\mathfrak{f}_v}$. We use Lemma A.4 once more to deduce $\operatorname{red}_{\mathfrak{f}_v}\operatorname{Nr}(\Lambda_v)^\times \simeq \left(\mathbb{Z}/\mathfrak{f}_v\mathbb{Z}\right)^{\times 2}$. We continue case by case.

If $E_v/\mathbb{Q}_v$ is unramified, then we use Lemma A.5 to deduce

$$\begin{aligned} \mathbb{Z}_v^\times/\operatorname{Nr}\Lambda_v^\times = \operatorname{Nr}\mathcal{O}_{E_v}^\times/\operatorname{Nr}\Lambda_v^\times &\simeq \left(\mathbb{Z}/\mathfrak{f}_v\mathbb{Z}\right)^\times/\left(\mathbb{Z}/\mathfrak{f}_v\mathbb{Z}\right)^{\times 2} \\ &\simeq \begin{cases} \mathbb{Z}/2\mathbb{Z} & p > 2, \\ 1 & p = 2, 2 \parallel \mathfrak{f}_v, \\ \mathbb{Z}/2\mathbb{Z} & p = 2, 4 \parallel \mathfrak{f}_v, \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & p = 2, 8 \mid \mathfrak{f}_v. \end{cases} \end{aligned}$$

This settles all the cases when $p > 2$ and the unramified case when $p = 2$.

Assume $p = 2$ and $E_v/\mathbb{Q}_v$ is ramified. If $2 \parallel \mathfrak{f}_v$, then $\operatorname{Nr}\mathcal{O}_{E_v}^\times = \operatorname{Nr}\Lambda_v^\times$ because $\mathbb{F}_2^\times = 1$. If $4 \parallel \mathfrak{f}_v$, then $\operatorname{red}_{\mathfrak{f}_v}\operatorname{Nr}\Lambda_v^\times \equiv \{1\}$, and hence $\operatorname{Nr}\Lambda_v^\times = \operatorname{Nr}\mathcal{O}_{E_v}^\times \cap 1 + 4\mathbb{Z}_2$. If $\operatorname{Nr}\mathcal{O}_{E_v}^\times = 1 + 4\mathbb{Z}_2 = \{1, -3\} + 8\mathbb{Z}_2$, then we deduce $\operatorname{Nr}\Lambda_v^\times = \operatorname{Nr}\mathcal{O}_{E_v}^\times$, otherwise $\operatorname{Nr}\Lambda_v^\times = 1 + 8\mathbb{Z}_2$.

If $8 \mid \mathfrak{f}_v$, then $\operatorname{red}_{\mathfrak{f}_v} \operatorname{Nr}\Lambda_v^\times = \{1\}$ and ${\mathbb{Z}_v^\times}^2 < \operatorname{Nr}\Lambda_v^\times$ and hence $\operatorname{Nr}\Lambda_v^\times = {\mathbb{Z}_v^\times}^2 = 1 + 8\mathbb{Z}_2$. □

Corollary A.7. *Let μ_{tame} be the number of* odd *primes dividing D. Set*

$$\mu_{\mathrm{wild}} \coloneqq \operatorname{ord}_2\left[\mathbb{Z}_2^\times \colon \operatorname{Nr}\Lambda_2^\times\right] \in \{0,1,2\}.$$

Notice that μ_{wild} depends only on $\mathfrak{f}_2$ and the ramification of 2 in $E/\mathbb{Q}$.

The following equalities holds for any imaginary quadratic order Λ:

$$\#\operatorname{Pic}(\Lambda)[2] = \left[\operatorname{Pic}(\Lambda) \colon \operatorname{Pic}(\Lambda)^2\right] = 2^{\mu_{\mathrm{tame}}+\mu_{\mathrm{wild}}-1} \asymp 2^{\omega(D)}.$$

Corollary A.8. *The first equality holds because the squaring homomorphism fits in a short exact sequence*

$$1 \to \operatorname{Pic}(\Lambda)[2] \to \operatorname{Pic}(\Lambda) \xrightarrow{x \mapsto x^2} \operatorname{Pic}(\Lambda)^2 \to 1.$$

The second equality follows from Corollary A.2 and Lemma A.6.

A.2. *Characters orthogonal to* $\operatorname{Pic}(\Lambda)^2$.

Definition A.9. For any prime $p > 2$, define $p^* \coloneqq (-1)^{\frac{p-1}{2}} p \equiv 1 \mod 4$, and for $n \in \mathbb{N}$, set

$$\chi_p(n) = \left(\frac{p^*}{n}\right).$$

This is the unique non-trivial primitive real Dirichlet character of modulus p.

Also define

$$\chi_4(n) = \left(\frac{-4}{n}\right),\ \chi_8(n) = \left(\frac{8}{n}\right).$$

The unique non-trivial primitive real Dirichlet character of modulus 4 is χ_4, and the non-trivial primitive real Dirichlet characters of modulus 8 are χ_8 and $\chi_4\,\chi_8$.

We multiplicatively extend every Dirichlet character of modulus q to the multiplicative group of rationals that are coprime to all prime divisors of q.

Moreover, we abuse the notation and denote by $\chi_q \colon {}_{\mathbb{Q}^\times}\backslash^{\mathbb{A}^\times} \to \{\pm 1\}$ the adelic lift of the corresponding Dirichlet character.

Proposition A.10. *Let $\mathfrak{a} \in \mathscr{J}(\Lambda)$. Then $[\mathfrak{a}] \in \operatorname{Pic}(\Lambda)^2$ if and only if*

$$\chi\left(\frac{\operatorname{Nr}(\mathfrak{a})}{\gcd(\operatorname{Nr}(\mathfrak{a}), \operatorname{modulus}(\chi)^\infty)}\right) = 1$$

for all the following real Dirichlet characters χ:

1. *χ_p for all* odd *primes $p \mid D$;*
2. *one of*[13] *$\chi_4, \chi_8, \chi_4\,\chi_8$ if $\left[\mathbb{Z}_2^\times \colon \operatorname{Nr}\Lambda_2^\times\right] = 2$;*
3. *χ_4 and χ_8 if $\operatorname{Nr}\Lambda_2^\times = 1 + 8\mathbb{Z}_2$.*

[13] The specific character depends on the subgroup $\operatorname{Nr}\Lambda_2^\times < \mathbb{Z}_2^\times$.

Proof. Our goal is to compute all the characters orthogonal to $\mathrm{Pic}(\Lambda)^2$. Because $(\mathrm{Pic}(\Lambda)^2)^\perp = \widehat{\mathrm{Pic}(\Lambda)}[2]$, all these characters are real.

Consider the short exact sequence of character groups dual to the short exact sequence of Proposition A.1:

$$1 \leftarrow \left(\mathrm{Pic}(\Lambda)^2\right)^\perp \xleftarrow{\widehat{\mathrm{Nr}}} \left(\widehat{{}_{\mathbb{Q}^\times}\backslash^{\mathbb{A}^\times}/_{\mathbb{R}_{>0}\prod_{v\neq\infty}\mathrm{Nr}\,\Lambda^\times}}\right) \xleftarrow{\widehat{\chi_E}} \{\pm 1\} \leftarrow 1.$$

Exactness implies that every character in $\left(\mathrm{Pic}(\Lambda)^2\right)^\perp$ can be expressed as a composition with the norm map of a real rational Hecke grossencharacter ${}_{\mathbb{Q}^\times}\backslash^{\mathbb{A}^\times} \to \{\pm 1\}$ that vanishes on $\mathbb{R}_{>0}\prod_{v\neq\infty}\mathrm{Nr}\,\Lambda_v^\times$. Moreover, the only non-trivial relation is that χ_E is trivial in $\left(\mathrm{Pic}(\Lambda)^2\right)^\perp$.

The translation between finite rational Hecke grossencharacters and Dirichlet characters implies that the relevant characters are adelic lifts of real Dirichlet characters with conductor containing $\mathbb{R}_{>0}\prod_{v\neq\infty}\mathrm{Nr}\,\Lambda_v^\times$. Using Lemma A.6 and the fact that all primitive real Dirichlet characters are the Kronecker symbols described in Definition A.9, we deduce that $\left(\widehat{{}_{\mathbb{Q}^\times}\backslash^{\mathbb{A}^\times}/_{\mathbb{R}_{>0}\prod_{v\neq\infty}\mathrm{Nr}\,\Lambda^\times}}\right)$ is generated by the adelic lifts of the characters listed in the claim. The explicit expressions for the evaluation of a character at the norm of an ideal follows by unwinding the adelic lifting procedure. □

A.3. *2-torsion in the Picard group.* The cohomological interpretation of the 2-torsion in the Picard group is used in the description of the fiber of the invariant map attaching pairs of fractional ideals to intersections.

Proposition A.11. *The diagonal restriction map*

$$H^1(\mathfrak{G}, \Lambda^\times) \to \prod_{v\neq\infty} H^1(\mathfrak{G}, \Lambda_v^\times)$$

is injective, and there is a canonical isomorphism

$${}_{H^1(\mathfrak{G},\Lambda^\times)}\backslash^{\prod_{v\neq\infty} H^1(\mathfrak{G},\Lambda_v^\times)} \simeq \mathrm{Pic}(\Lambda)[2].$$

Proof. We construct the necessary isomorphism in several steps. On the way we also prove the claimed injectivity. For any order $\mathcal{O} < \mathcal{O}_F$ in a global field F, denote by $\mathscr{P}(\mathcal{O}) \coloneqq {}_{\mathcal{O}^\times}\backslash^{F^\times}$ the group of invertible principle fractional $\mathcal{O}$-ideals.

We begin by examining the following commuting diagram with exact rows:

$$\begin{tikzcd}
1 \arrow[r] & \Lambda^\times \arrow[r] \arrow[d] & E^\times \arrow[r] \arrow[d] & \mathscr{P}(\Lambda) \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & \prod_{v\neq\infty} \Lambda_v^\times \arrow[r] & \prod'_{v\neq\infty} E_v^\times \arrow[r] & \mathscr{J}(\Lambda) \arrow[r] & 1.
\end{tikzcd}$$

This diagram induces a commuting diagram of $\mathfrak{G}$-cohomology with exact rows:

$$\begin{tikzcd}
1 \arrow[r] & \mathbb{Z}^\times \arrow[r] \arrow[d] & \mathbb{Q}^\times \arrow[r] \arrow[d] & \mathscr{P}(\Lambda)^{\mathfrak{G}} \arrow[r] \arrow[d] & H^1(\mathfrak{G},\Lambda^\times) \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & \prod_{v\neq\infty}\mathbb{Z}_v^\times \arrow[r] & \prod'_{v\neq\infty}\mathbb{Q}_v^\times \arrow[r] & \mathscr{J}(\Lambda)^{\mathfrak{G}} \arrow[r] & \prod_{v\neq\infty} H^1(\mathbb{Q}_v,\Lambda_v^\times) \arrow[r] & 1.
\end{tikzcd} \tag{60}$$

The last terms are trivial due to Hilbert's Satz 90. We can truncate the diagram above to the following commuting diagram with exact rows:

$$\begin{tikzcd}
1 \arrow[r] & \mathscr{P}(\mathbb{Z}) \arrow[r] \arrow[d] & \mathscr{P}(\Lambda)^{\mathfrak{G}} \arrow[r] \arrow[d] & H^1(\mathfrak{G},\Lambda^\times) \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & \mathscr{J}(\mathbb{Z}) \arrow[r] & \mathscr{J}(\Lambda)^{\mathfrak{G}} \arrow[r] & \prod_{v\neq\infty} H^1(\mathbb{Q}_v,\Lambda_v^\times) \arrow[r] & 1.
\end{tikzcd} \tag{61}$$

Because $\mathscr{P}(\Lambda)^{\mathfrak{G}} \to \mathscr{J}(\Lambda)^{\mathfrak{G}}$ is injective, the four-lemma implies that

$$\ker\left[H^1(\mathfrak{G},\Lambda^\times) \to \prod_{v\neq\infty} H^1(\mathbb{Q}_v,\Lambda_v^\times)\right] \simeq {}_{\mathscr{P}(\mathbb{Z})}\backslash^{\mathscr{J}(\mathbb{Z})} = \operatorname{Pic}(\mathbb{Z}) = 1.$$

This proves the first claim. Next we deduce from (61) that

$$ {}_{\mathscr{P}(\Lambda)^{\mathfrak{G}}}\backslash^{\mathscr{J}(\Lambda)^{\mathfrak{G}}} \simeq {}_{H^1(\mathfrak{G},\Lambda^\times)}\backslash^{\prod_{v\neq\infty} H^1(\mathbb{Q}_v,\Lambda_v^\times)}. \tag{62}$$

We can also continue the long exact sequence in the first row of (60),

$$H^1(\mathfrak{G},\Lambda^\times) \to 1 \to H^1(\mathfrak{G},\mathscr{P}(\Lambda)) \to {}^{\mathbb{Z}^\times}/_{\operatorname{Nr}\Lambda^\times} \to {}^{\mathbb{Q}^\times}/_{\operatorname{Nr}E^\times}, \tag{63}$$

where we have computed the second cohomology groups using the formula $H^2(C,M) \simeq {}^{M^C}/_{\operatorname{Nr}M}$ valid for any finite cyclic group C acting on an abelian group M. Because E is an imaginary quadratic field, $\mathbb{Z}^\times \cap \operatorname{Nr}E^\times = 1$, and thus the last map in (63) is injective. By exactness we deduce $H^1(\mathfrak{G},\mathscr{P}(\Lambda)) = 1$.

We finally consider the long exact sequence associated to the short exact sequence

$$1 \to \mathscr{P}(\Lambda) \to \mathscr{J}(\Lambda) \to \operatorname{Pic}(\Lambda) \to 1.$$

The equality $H^1(\mathfrak{G},\mathscr{P}(\Lambda)) = 1$ implies

$$\operatorname{Pic}(\Lambda)[2] = \operatorname{Pic}(\Lambda)^{\mathfrak{G}} \simeq {}_{\mathscr{P}(\Lambda)^{\mathfrak{G}}}\backslash\cdot\mathscr{J}(\Lambda)^{\mathfrak{G}}. \tag{64}$$

The claimed isomorphism is a composition of (64) and (62). □

Corollary A.12. *Recall the definition* $\operatorname{cbd}(x) = x/{}^{\sigma}x$ *for* $x \in E_v^\times$ *for any* v. *The proposition above implies*

$$\prod_{v\neq\infty}\left[\Lambda_v^{(1)}\colon \operatorname{cbd}(\Lambda_v^\times)\right] = \prod_{v\neq\infty}\#H^1(\mathfrak{G},\Lambda_v^\times) = 2\#\operatorname{Pic}(\Lambda)[2].$$

Proof. The definition of H^1 using cocycles and coboundaries implies that $H^1(\mathfrak{G}, L) \simeq {}^{L^{(1)}}\!/_{\operatorname{cbd}(L^\times)}$ for $L = \Lambda$ and $L = \Lambda_v$ for all $v \neq \infty$. Hence by Proposition A.11 the factor of proportionality between $\prod_{v\neq\infty}\left[\Lambda_v^{(1)} \colon \operatorname{cbd}(\Lambda_v^\times)\right]$ and $\#\operatorname{Pic}(\Lambda)[2]$ is $\left[\Lambda^{(1)} \colon \operatorname{cbd}(\Lambda^\times)\right] = 2$. □

Lemma A.13. *Let $v \neq \infty$. The first Galois cohomology group of the unit group of a maximal order is*

$$\begin{cases} H^1(\mathbb{Q}_v, \mathcal{O}_{E_v}^\times) = 1 & \textit{if } E_v/\mathbb{Q}_v \textit{ is unramified,} \\ H^1(\mathbb{Q}_v, \mathcal{O}_{E_v}^\times) = {}^{\mathbb{Z}}\!/_{2\mathbb{Z}} & \textit{if } E_v/\mathbb{Q}_v \textit{ is ramified.} \end{cases}$$

If $E_v/\mathbb{Q}_v$ is tamely totally ramified, i.e., the residue characteristic is odd, then the non-trivial class of $H^1(\mathbb{Q}_v, \mathcal{O}_{E_v}^\times)$ is represented by the cocycle corresponding to $-1 \in \mathcal{O}_{E_v}^{(1)}$.

Proof. Denote by g the number of places above v in $E/\mathbb{Q}$, and let e be the ramification index of v in $E/\mathbb{Q}$. Consider the short exact sequence

$$1 \to \mathcal{O}_{E_v}^\times \to E_v^\times \to \mathbb{Z}^g \to 1.$$

The third map is the valuation map, and if $g = 2$, then the Galois group acts on the value group $\mathbb{Z}^g$ by switching the coordinates. The associated long exact cohomology sequence is

$$1 \to \mathbb{Z}_v^\times \to \mathbb{Q}_v^\times \to \mathbb{Z} \to H^1(\mathfrak{G}, \mathcal{O}_{E_v}^\times) \to 1,$$

where the last group is trivial by Hilbert's Satz 90 and the third map is the valuation map of $E_v^\times$ restricted to $\mathbb{Q}_v^\times$. The image of $\mathbb{Q}_v^\times \to \mathbb{Z}$ is $e\mathbb{Z}$, and we deduce that

$$H^1(\mathfrak{G}, \mathcal{O}_{E_v}^\times) \simeq {}^{\mathbb{Z}}\!/_{e\mathbb{Z}}.$$

Assume $E_v/\mathbb{Q}_v$ is ramified. If Π is a uniformizer of $\mathcal{O}_{E_v}$, then the map $\mathbb{Z} \to H^1(\mathfrak{G}, \mathcal{O}_{E_v}^\times)$ can be written explicitly as $n \mapsto \operatorname{cbd}(\Pi^n)$. If the ramification is tame, we can choose a uniformizer so that ${}^\sigma\Pi = -\Pi$ and $H^1(\mathfrak{G}, \mathcal{O}_{E_v}^\times)$ is generated by -1. □

Lemma A.14. *Assume $\Lambda_v < \mathcal{O}_{E_v}$ is a non-maximal order, and denote the residue characteristic by p. Then*

$$\#H^1(\mathfrak{G}, \Lambda_v^\times) = \begin{cases} 2 & p > 2, \\ 2^{\mu_{\mathrm{wild}}} & p = 2. \end{cases}$$

Moreover, when $p > 2$, the non-trivial cocycle of $H^1(\mathfrak{G}, \Lambda_v^\times)$ is represented by $-1 \in \Lambda_v^{(1)}$.

Proof. The short exact sequence of abelian $\mathfrak{G}$-modules

$$1 \to \Lambda_v^\times \to \mathbb{O}_{E_v}^\times \to {}^{\mathbb{O}_{E_v}^\times}\!/_{\Lambda_v^\times} \to 1$$

induces a long exact sequence of cohomology

$$\begin{aligned}
&1 \to \mathbb{Z}_v^\times \to \mathbb{Z}_v^\times \to \left({}^{\mathbb{O}_{E_v}^\times}\!/_{\Lambda_v^\times}\right)^{\mathfrak{G}} \\
&\to H^1(\mathbb{Q}_v, \Lambda_v^\times) \to H^1(\mathbb{Q}_v, \mathbb{O}_{E_v}^\times) \to H^1\left(\mathbb{Q}_v, {}^{\mathbb{O}_{E_v}^\times}\!/_{\Lambda_v^\times}\right) \\
&\to {}^{\mathbb{Z}_v^\times}\!/_{\operatorname{Nr}\Lambda_v^\times} \to {}^{\mathbb{Z}_v^\times}\!/_{\operatorname{Nr}\mathbb{O}_{E_v}^\times}.
\end{aligned} \tag{65}$$

□

Because $\mathfrak{G}$ acts on ${}^{\mathbb{O}_{E_v}^\times}\!/_{\Lambda_v^\times}$ by inversion we see that

$$\begin{aligned}
\left({}^{\mathbb{O}_{E_v}^\times}\!/_{\Lambda_v^\times}\right)^{\mathfrak{G}} &\simeq \left({}^{\mathbb{O}_{E_v}^\times}\!/_{\Lambda_v^\times}\right)[2], \\
H^1\left(\mathbb{Q}_v, {}^{\mathbb{O}_{E_v}^\times}\!/_{\Lambda_v^\times}\right) &\simeq \left({}^{\mathbb{O}_{E_v}^\times}\!/_{\Lambda_v^\times}\right) \Big/ \left({}^{\mathbb{O}_{E_v}^\times}\!/_{\Lambda_v^\times}\right)^2.
\end{aligned}$$

The second map in (65) is simply the identity, and we can truncate the sequence (65) to an exact sequence

$$\begin{aligned}
&1 \to \left({}^{\mathbb{O}_{E_v}^\times}\!/_{\Lambda_v^\times}\right)[2] \\
&\to H^1(\mathbb{Q}_v, \Lambda_v^\times) \to H^1(\mathbb{Q}_v, \mathbb{O}_{E_v}^\times) \to \left({}^{\mathbb{O}_{E_v}^\times}\!/_{\Lambda_v^\times}\right) \Big/ \left({}^{\mathbb{O}_{E_v}^\times}\!/_{\Lambda_v^\times}\right)^2 \\
&\to {}^{\operatorname{Nr}\mathbb{O}_{E_v}^\times}\!/_{\operatorname{Nr}\Lambda_v^\times} \to 1.
\end{aligned}$$

The second and the fifth groups above are non-canonically isomorphic, and exactness implies

$$\#H^1(\mathbb{Q}_v, \Lambda_v^\times) = \#H^1(\mathbb{Q}_v, \mathbb{O}_{E_v}^\times) \cdot \#{}^{\operatorname{Nr}\mathbb{O}_{E_v}^\times}\!/_{\operatorname{Nr}\Lambda_v^\times} = \begin{cases} 2 & p > 2, \\ 2^{\mu_{\mathrm{wild}}} & p = 2. \end{cases}$$

The second equality above follows from Lemmata A.13, A.5 and A.6.

We need only show that the cocycle of $-1 \in \Lambda_v^{(1)}$ is not a coboundary if $p > 2$. Assume in the contrary the $-1 = x/{}^\sigma x$ for some $x \in \Lambda_v^\times$. Then by Lemma A.4 we know that

$$-1 = \frac{x}{{}^\sigma x} \equiv \frac{x}{x} \mod f_v \mathbb{O}_{E_v} \equiv 1 \mod f_v \mathbb{O}_{E_v},$$

which is a contradiction because the residue characteristic is odd.

Appendix B. Points on conics

B.1. *Notation.* In this section we denote by $q(x,y)$ a primitive binary integral quadratic form of discriminant $D<0$ and define $Q(x,y)=q(x,y)-\omega D$ for some $\omega\in\mathbb{Z}$. We denote by $X_Q\coloneqq \operatorname{Spec}\mathbb{Z}[x,y]/\left\langle Q(x,y)\right\rangle$ the affine plane curve cutout by Q.

We shall also need the homogenized polynomial $\overline{Q}(x,y,z)=q(x,y)-\omega Dz^2$. Denote by $\overline{X_Q}\coloneqq \operatorname{Proj}\mathbb{Z}[x,y,z]/\left\langle\overline{Q}(x,y,z)\right\rangle$ the projective completion of the curve X_Q. The plane curve X_Q is an affine conic and $\overline{X_Q}$ is a projective conic.

B.2. *Local diagonlization of binary quadratic forms.*

Lemma B.1. *For any prime p, the form $q(x,y)$ is equivalent over $\mathbb{Z}_p$ to a form $q'(x,y)$ with $\mathbb{Z}_p$ coefficients and satisfying the following.*

If $p>2$ or $p=2$ and $D\equiv 0 \mod 4$, then $q'(x,y)=ux^2+Ay^2$ is diagonal. Moreover, we can assume $u\in\mathbb{Z}_p^\times$. If $p^l\parallel A$, then we write $A=u_Ap^l$ for $u_A\in\mathbb{Z}_p^\times$.

For $p=2$ and $D\equiv 1 \mod 4$,

$$q'(x,y)=\begin{cases}xy & D\equiv +1 \mod 8 \iff \left(\frac{D}{2}\right)=+1,\\ x^2+xy+y^2 & D\equiv -3 \mod 8 \iff \left(\frac{D}{2}\right)=-1.\end{cases}$$

Proof. This is classical; cf. [Cas78, Ch. 8]. □

Remark B.2. Assume q corresponds to the ideal class $[\mathfrak{s}]\in\operatorname{Pic}(\Lambda)$ where Λ is a quadratic order of discriminant D. If $p>2$ and $q'(x,y)=ux^2+Ay^2$ as above, then $\left(\frac{u}{p}\right)=\chi_p(\mathrm{Nr}[\mathfrak{s}])$, where χ_p is the genus class group character from Proposition A.10. In particular, the class of u in $\mathbb{Z}_p^\times/\mathbb{Z}_p^{\times 2}$ depends only on $[\mathfrak{s}] \mod \operatorname{Pic}(\Lambda)^2$. By abuse of notation, for odd $p\mid D$ we shall denote

$$\chi_p(q)\coloneqq\chi_p(\mathrm{Nr}[s])=\left(\frac{u}{p}\right).$$

Moreover, because $D=-4uA$, for $p>2$ we have $\left(\frac{u_A}{p}\right)=\left(\frac{-D/p^l}{p}\right)\chi_p(q)$ where $p^l\parallel D$.

B.3. *Regular primes.*

Proposition B.3. *If $p\nmid\omega D$, then $\widetilde{\rho}_Q(p^k)=\rho_Q(p^k)=\rho_Q(p)p^{k-1}$ and*

$$\rho_Q(p)=p-\left(\frac{D}{p}\right).$$

Proof. If $p\nmid D$, then $\overline{X_Q}$ and X_Q have a smooth reduction modulo p. The first claim is an application of Hensel's lemma.

The reduction of $\overline{X_Q}$ is a smooth conic over a finite field and it is isomorphic to the projective line. In particular, $\left|\overline{X_Q}\left({}^{\mathbb{Z}}/_{p\mathbb{Z}}\right)\right| = p+1$.

To calculate $\rho_Q(p) = \left|X_Q\left({}^{\mathbb{Z}}/_{p\mathbb{Z}}\right)\right|$ we need to subtract the points of $\overline{X_Q}$ on the line at infinity $z=0$. These are exactly the points on the projective variety cutout by $q(x,y)$, equivalently $q'(x,y)$ from Lemma B.1. There are either two or zero such points depending on the Kronecker symbol $\left(\frac{D}{p}\right)$. □

B.4. *Singular primes.*

Lemma B.4. *Let $q_0(x,y) \in \mathbb{Z}_p[x,y]$ be a homogeneous binary quadratic form such that either $q_0(x,y) = u_1x^2 + u_2y^2$ with $u_1, u_2 \in \mathbb{Z}_p^\times$ or $p=2$ and $q_0(x,y) = xy$ or $q_0(x,y) = x^2+xy+y^2$.*

Fix $u_3 \in \mathbb{Z}_p^\times$. For any integer $m \geq 0$, define

$$Q_m(x,y) \coloneqq q_0(x,y) - u_3p^m.$$

If $p>2$ or $p=2$ and q_0 is not diagonal, then

$$\rho_{Q_m}(p^n)$$
$$= \begin{cases} \lceil\frac{n}{2}\rceil p^{n-1}\left(1-\left(\frac{\operatorname{disc}(q_0)}{p}\right)\right) + p^n\delta_{n\equiv 0 \bmod 2} + p^{n-1}\delta_{n\equiv 1 \bmod 2} & n\leq m, \\ \left(1+\lfloor\frac{m}{2}\rfloor\right)p^{n-1}\left(1-\left(\frac{\operatorname{disc}(q_0)}{p}\right)\right) + p^n\left(1-\frac{1}{p}\right)\delta_{m\equiv 0 \bmod 2} & n>m. \end{cases}$$

Otherwise if $p=2$ and q_0 is diagonal, then

$$\rho_{Q_m}(2^n) \leq \min\left(\left\lceil\frac{n}{2}\right\rceil, 1+\left\lfloor\frac{m}{2}\right\rfloor\right)2^{n+3} + 2^n.$$

Proof. Denote by $\rho(p^n\colon p^m)$ the number of solutions to

$$Q_m(x,y) \equiv 0 \mod p^n. \tag{66}$$

Similarly, denote by $\rho^0(p^n\colon p^m)$ the number of solutions modulo p^n reducing to $(0,0)$ modulo p, and let $\rho^1(p^n\colon p^m)$ be the number of solutions not reducing to zero modulo p.

Case I: $m=0$. If $p>2$ or $p=2$ and $q_0(x,y)$ is *not* diagonal, then $Q_0(x,y)$ defines a smooth affine conic modulo p. Subtracting the points on the line at infinity from the projective conic we deduce

$$\rho(p\colon p^0) = \rho^1(p\colon p^0) = p - \left(\frac{\operatorname{disc}(q_0)}{p}\right).$$

Moreover, all these solutions are smooth, and in this case

$$\begin{aligned}\rho(p^n\colon p^0) = \rho^1(p^n\colon p^0) &= p^{n-1}\left(p-\left(\frac{\operatorname{disc}(q_0)}{p}\right)\right) \\ &= p^{n-1}\left(1-\left(\frac{\operatorname{disc}(q_0)}{p}\right)\right) + p^n\left(1-\frac{1}{p}\right).\end{aligned}$$

If $p = 2$ and q_0 is diagonal, then $\rho^0(2^n\colon 2^0) = 0$ and for $n \leq 3$, we use the trivial bound $\rho(2^n\colon 2^0) \leq 2^{2n} \leq 2^{n+3}$. Hensel's lemma in the strong form implies for $n \geq 3$ that $\rho(2^n\colon 2^0) = 2^{n-3}\rho(2^3\colon p^0) \leq 2^{n+3}$. We deduce that for all $n \geq 1$,

$$\rho(2^n\colon 2^0) = \rho^1(2^n\colon 2^0) \leq 2^{n+3}.$$

Case II: $n = 1$, $m \geq 1$ *and* ρ^1 *for* $n \geq 1$. If $p > 2$ or $p = 2$ and q_0 is not diagonal, then $Q \equiv q_0 \mod p$ and q_0 is a non-degenerate quadratic form modulo p. We see that

$$\rho^0(p\colon p^m) = 1$$
$$\rho^1(p\colon p^m) = 1 - \left(\frac{\mathrm{disc}(q_0)}{p}\right).$$

Moreover, in this case all the solutions except $(0, 0)$ are smooth, thus if $m \geq 1$ and $p > 2$ or $p = 2$ and q_0 is not diagonal, then

$$\rho^1(p^n\colon p^m) = p^{n-1}\left(1 - \left(\frac{\mathrm{disc}(q_0)}{p}\right)\right).$$

If $m \geq 1$, $p = 2$ and q_0 is diagonal, then the same arguments as in Case I imply that

$$\rho^0(2\colon 2^m) = 1,$$
$$\rho^1(2^n\colon 2^m) \leq 2^{n+3}.$$

Case III: ρ^0 *for* $n \geq 2$, $m \geq 1$. We proceed to compute $\rho^0(p^n\colon p^m)$ for $n \geq 2$, $m \geq 1$. We need to count solutions to (66) of the form $(x, y) = (px_0, py_0)$ for $(x_0, y_0) \in {}^{\mathbb{Z}}/_{p^{n-1}\mathbb{Z}} \times {}^{\mathbb{Z}}/_{p^{n-1}\mathbb{Z}}$. The pertinent (px_0, py_0) solve (66) if and only if

$$p^2 q_0(x_0, y_0) - u_3 p^m \equiv 0 \mod p^n. \tag{67}$$

The first case to consider is $n = 2$, $m \geq 1$. Then obviously

$$\rho^0(p^2\colon p^m) = \begin{cases} 0 & m = 1, \\ p^2 & m > 1. \end{cases}$$

If $n \geq 3$ and $m = 1$, then (67) implies that

$$\rho^0(p^n\colon p^1) = 0.$$

If $n \geq 3$ and $m \geq 2$, then (67) is equivalent to

$$q_0(x_0, y_0) - u_3 p^{m-2} \equiv 0 \mod p^{n-2}$$

and we have a recursion formula

$$\rho^0(p^n\colon p^m) = p^2\rho(p^{n-2}\colon p^{m-2}).$$

Finally we can use the recursion formula and the all the cases computed above to deduce the claim. □

Proposition B.5. *Fix a prime $p \mid \omega D$, and set $l \coloneqq \operatorname{ord}_p D$, $m \coloneqq \operatorname{ord}_p(4\omega)$. For $p > 2$, define*

$$\rho_Q^0(p) \coloneqq \begin{cases} p - \left(\frac{D/p^l}{p}\right) & l \equiv 0 \mod 2, \\ 2p & l \equiv 1 \mod 2 \text{ and } \left(\frac{\omega}{p}\right) = +\chi_p(q), \\ 0 & l \equiv 1 \mod 2 \text{ and } \left(\frac{\omega}{p}\right) = -\chi_p(q). \end{cases}$$

If $n \leq l$, then for all primes p,

$$\rho_Q(p^n) = p^{n+\lfloor n/2 \rfloor}.$$

If $p > 2$, $n > l$ and $p \nmid \omega$, then

$$\rho_Q(p^l) = p^{n+\lfloor l/2 \rfloor} \frac{\rho_Q^0(p)}{p}.$$

If $p > 2$, $n > l$ and $p \mid \omega$, then set $m = \operatorname{ord}_p(4\omega)$:

$$\rho_Q(p^n) = p^{n+\lceil l/2 \rceil}$$
$$\cdot \begin{cases} \left(\left\lceil \frac{n-l}{2} \right\rceil - (l \bmod 2)\right) \frac{1}{p} \left(1 - \left(\frac{D/p^l}{p}\right)\right) + \delta_{n \equiv l \mod 2} + \frac{1}{p} \delta_{n \not\equiv l \mod p} & n - l \leq m, \\ \left(1 + \left\lfloor \frac{m}{2} \right\rfloor - (l \bmod 2)\right) \frac{1}{p} \left(1 - \left(\frac{D/p^l}{p}\right)\right) + \left(1 - \frac{1}{p}\right) \delta_{m \equiv 0 \bmod 2} & n - l > m. \end{cases}$$

If $p = 2$ and $n > l$, then

$$\rho_Q(2^n) \leq 2^{n+\lceil l/2 \rceil} \left[\min\left(\left\lceil \frac{n-l}{2} \right\rceil, 1 + \left\lfloor \frac{m}{2} \right\rfloor\right) 2^3 + 1\right].$$

Proof. Let $q'(x, y) \coloneqq ux^2 + Ay^2$ as in Lemma B.1. We solve the equivalent equation $Q'(x, y) \coloneqq q'(x, y) - \omega D \equiv 0 \mod p^n$.

Case I: $n \leq \operatorname{ord}_p D$. Because $n \leq \operatorname{ord}_p D$, the equation $Q'(x, y) \equiv 0 \mod p^n$ is equivalent to

$$ux^2 \equiv 0 \mod p^n \iff x \equiv 0 \mod p^{\lceil n/2 \rceil}.$$

Equivalently, $(x, y) \in \left(\mathbb{Z}/p^n\mathbb{Z}\right)$ is a solution to $Q(x, y) = 0$ if and only if $x \equiv 0 \mod p^{\lceil n/2 \rceil}$. The formula for $\rho_Q(p^n)$, $n \leq l$, follows immediately.

Case II: $n > \operatorname{ord}_p D$. Any solution modulo p^n must reduce to a solution modulo p^l; i.e., it must satisfy $x \equiv 0 \mod p^{\lceil l/2 \rceil}$. Write $x = p^{\lceil l/2 \rceil} x_0$, where $x_0 \in \mathbb{Z}/p^{n - \lceil l/2 \rceil}\mathbb{Z}$, and denote $\varpi \coloneqq l \bmod 2 \in \{0, 1\}$. Then the equation $Q'(x, y) \equiv 0 \mod p^n$ is equivalent to

$$\begin{aligned} & up^{l+2\varpi} x_0^2 + Ay^2 - \omega D \equiv 0 \mod p^n \\ & \qquad \iff up^{2\varpi} x_0^2 + u_A y^2 - 4\omega u u_A \equiv 0 \mod p^{n-l}, \end{aligned} \tag{68}$$

where $A = u_A p^l$ and $D = -4uA$.

Denote

$$q_0(x_0, y) := up^{2\varpi}x_0^2 + u_A y^2 - 4\omega u u_A \in \mathbb{Z}_p[x, y].$$

We have shown that the solutions of $Q'(x, y) \equiv 0 \mod p^n$ are exactly the residue classes of the form $(p^{\lceil l/2 \rceil}x_0, y)$ where $(x_0, y) \in {}^{\mathbb{Z}}/_{p^{n-\lceil l/2 \rceil}\mathbb{Z}} \times {}^{\mathbb{Z}}/_{p^n\mathbb{Z}}$ reduces to a root of $q_0(x_0, y)$ modulo p^{n-l}. In particular,

$$\rho_Q(p^n) = p^{l-\lceil l/2 \rceil}p^l \rho_{q_0}(p^{n-l}) = p^{l+\lfloor l/2 \rfloor}\rho_{q_0}(p^{n-l}).$$

If $\varpi \equiv 0 \mod 2$, then we can apply Lemma B.4 directly to q_0 with $m = \operatorname{ord}_p(4\omega)$.

If $\varpi \equiv 1 \mod 2$, then we have two options. If $p \nmid 4\omega$, then q_0 defines a smooth affine conic modulo p. Computing explicitly and using Hensel's lemma, then we deduce

$$\rho_{q_0}(p) = \begin{cases} 2p & \left(\frac{\omega}{p}\right) = +\chi_p(q), \\ 0 & \left(\frac{\omega}{p}\right) = -\chi_p(q), \end{cases}$$

$$\rho_{q_0}(p^{n-l}) = p^{n-l}\frac{\rho_{q_0}(p)}{p}.$$

Otherwise, if $p \mid 4\omega$, then reducing (68) modulo p we conclude that necessarily $y \equiv 0 \mod p$. Moreover, if $n - l = 1$, then $\rho_{q_0}(p) = p$. Otherwise, if $n \geq l + 2$, we write $y = py_0$ for $y_0 \in {}^{\mathbb{Z}}/_{p^{n-l-1}\mathbb{Z}}$.

Equation (68) is then equivalent to

$$up^2x_0^2 + u_A p^2 y_0^2 - 4\omega u u_A \equiv 0 \mod p^{n-l}.$$

If $m = \operatorname{ord}_p(4\omega) = 1$, then this equation has no solutions, i.e., $\rho_{q_0}(p) = 0$. If $m \geq 2$, then define $q_1 := ux_0^2 + u_A y_0^2 - (4\omega/p^2)uu_A$. Then $\rho_{q_0}(p^{n-l}) = p^3\rho_{q_1}(p^{n-l-2})$, and apply Lemma B.4 to q_1. □

COROLLARY B.6. *The following bound holds for any prime power p^n:*

$$\rho_Q(p^n) \leq 16p^{n(2-1/2)}.$$

COROLLARY B.7. *Let $p \mid D$, and set $l = \operatorname{ord}_p D$. Then if $n \leq l$,*

$$\widetilde{\rho}_Q(p^n) = \begin{cases} p^{n+\lfloor n/2 \rfloor}\left(1 - \frac{1}{p}\right) & n \equiv 0 \mod 2, \\ 0 & n \equiv 1 \mod 2. \end{cases}$$

Assume next that $p \nmid 4\omega$. Then

$$\widetilde{\rho}_Q(p^l) = p^{l+\lfloor l/2 \rfloor}\left(1 - \frac{\rho_Q^0(p)}{p^2}\right)$$

and for $n > l$,

$$\widetilde{\rho}_Q(p^n) = p^{n+\lfloor l/2 \rfloor}\frac{\rho_Q^0(p)}{p}\left(1 - \frac{1}{p}\right).$$

Proof. Notice that if $p \mid D$, then $X_Q\left(\mathbb{Z}/_{p\mathbb{Z}}\right)$ has no smooth points. The claim follows from Proposition B.5 and Lemma 9.3. □

Proposition B.8. *Fix a prime $p \parallel D$ and $k \in \{0, 1\}$. Assume $p \nmid 4\omega$. If $\epsilon \in \{\pm 1\}$, then*

$$\sum_{a \in \left(\mathbb{Z}/_{p^{2-k}\mathbb{Z}}\right)^\times;\ \left(\frac{a}{p}\right)=\epsilon} \rho_Q(p^k a; p^2) = \begin{cases} p^4\left(1 - \frac{1}{p}\right) & k = 0,\ \chi_p(q) = +\epsilon, \\ 0 & k = 0,\ \chi_p(q) = -\epsilon, \\ \frac{p^3}{2}\left(1 - \frac{f}{p}\right) & k = 1, \end{cases} \tag{69}$$

where

$$f := 1 + \epsilon\left(\frac{-D/p}{p}\right)\chi_p(q) + \left(\frac{\omega}{p}\right)\chi_p(q).$$

Proof. Let $q'(x, y) := ux^2 + Ay^2$ as in Lemma B.1 and write $A = u_A p$ where $u_A \in \mathbb{Z}_p^\times$. Let $u_\epsilon \in \mathbb{Z}_p^\times$ such that $\left(\frac{u_\epsilon}{p}\right) = \epsilon$. Define

$$V(x, y, w) := ux^2 - u_A p y^2 - 4\omega u u_A p - p^k u_\epsilon w^2 \in \mathbb{Z}_p[x, y, w].$$

Consider the equation

$$V(x, y, w) \equiv 0 \mod p^2. \tag{70}$$

The left-hand side of (69) is proportional to the number of solutions to (70) satisfying $w \not\equiv 0 \mod p$. The proportionality constant is exactly the number of solutions to $p^k u_\epsilon w^2 \equiv p^k u_\varepsilon w_0^2 \mod p^2$ for any fixed unit w_0. The latter equation has $2p^k$ solutions. In conclusion,

$$\sum_{a \in \left(\mathbb{Z}/_{p^2\mathbb{Z}}\right)^\times;\ \left(\frac{a}{p}\right)=\epsilon} \rho_Q(a; p^2)$$
$$= \frac{1}{2p^k} \# \left\{(x, y, w) \in \mathbb{Z}/_{p^2\mathbb{Z}} \times \mathbb{Z}/_{p^2\mathbb{Z}} \times \left(\mathbb{Z}/_{p^2\mathbb{Z}}\right)^\times \mid V(x, y, w) = 0\right\}.$$

Equation (70) reduces modulo p to

$$ux^2 - p^k u_\varepsilon w^2 \equiv 0 \mod p. \tag{71}$$

Case I: $k = 0$. All the solutions to equation (71) with $w \not\equiv 0 \mod p$ are smooth. There 0 such solutions if $\left(\frac{uu_\epsilon}{p}\right) = -1$ and $2p(p-1)$ solutions otherwise. Using Hensel's lemma we conclude that the number of solutions to (70) with $w \not\equiv 0 \mod p$ is $2p^4\left(1 - \frac{1}{p}\right)$ if $\chi_p(q) = +\epsilon$ and 0 otherwise.

Case II: $k = 1$. Equation (71) implies that necessarily $x \equiv 0 \mod p$. Hence equation (70) is equivalent to

$$u_A y^2 - u_\epsilon w^2 - 4\omega u u_A \equiv 0 \mod p. \tag{72}$$

This is an equation of a smooth conic with $p+1$ projective solutions. The are either two or zero solutions on the line at infinity depending on the sign of $\epsilon\left(\frac{u_A}{p}\right)=\left(\frac{u_\epsilon u_A^{-1}}{p}\right)$. Hence the number of solutions to (72) is $p-\epsilon\left(\frac{u_A}{p}\right)$.

We also need to subtract from the solutions of (72) the cases where $w\equiv 0 \mod p$. Substituting 0 for w in (72) we see that there are either two or zero such solution depending on the sign of $\left(\frac{\omega u}{p}\right)$.

We conclude that the number of relevant solutions to (70) is

$$p^4\left(1-\frac{f}{p}\right),$$

where $f:=1+\epsilon\left(\frac{u_A}{p}\right)+\left(\frac{\omega u}{p}\right)$. □

References

[And98] Y. André, Finitude des couples d'invariants modulaires singuliers sur une courbe algébrique plane non modulaire, *J. Reine Angew. Math.* **505** (1998), 203–208. MR 1662256. Zbl 0918.14010. https://doi.org/10.1515/crll.1998.118.

[BSR16] J. Bourgain, P. Sarnak, and Z. Rudnick, Local statistics of lattice points on the sphere, in *Modern Trends in Constructive Function Theory*, *Contemp. Math.* **661**, Amer. Math. Soc., Providence, RI, 2016, pp. 269–282. MR 3489563. Zbl 1394.11059. https://doi.org/10.1090/conm/661/13287.

[dlBB06] R. de la Bretèche and T. D. Browning, Sums of arithmetic functions over values of binary forms, *Acta Arith.* **125** no. 3 (2006), 291–304. MR 2276196. Zbl 1159.11035. https://doi.org/10.4064/aa125-3-6.

[dlBT12] R. de la Bretèche and G. Tenenbaum, Moyennes de fonctions arithmétiques de formes binaires, *Mathematika* **58** no. 2 (2012), 290–304. MR 2965973. Zbl 1284.11126. https://doi.org/10.1112/S0025579311002154.

[BS91] M. Burger and P. Sarnak, Ramanujan duals. II, *Invent. Math.* **106** no. 1 (1991), 1–11. MR 1123369. Zbl 0774.11021. https://doi.org/10.1007/BF01243900.

[Bur62] D. A. Burgess, On character sums and L-series, *Proc. London Math. Soc.* (3) **12** (1962), 193–206. MR 0132733. Zbl 0106.04004. https://doi.org/10.1112/plms/s3-12.1.193.

[Cas78] J. W. S. Cassels, *Rational Quadratic Forms*, *London Math. Soc. Monogr.* **13**, Academic Press, Inc. [Harcourt Brace Jovanovich, Publishers], London-New York, 1978. MR 0522835. Zbl 0395.10029.

[Che04] T. Chelluri, *Equidistribution of Roots of Quadratic Congruences*, ProQuest LLC, Ann Arbor, MI, 2004, Thesis (Ph.D.)–Rutgers The State University of New Jersey - New Brunswick. MR 2717231. Available at http://gateway.proquest.com/openurl?url_ver=Z39.88-2004&rft_val_fmt=

info:ofi/fmt:kev:mtx:dissertation&res_dat=xri:pqdiss&rft_dat=xri:pqdiss:3153552.

[COU01] L. Clozel, H. Oh, and E. Ullmo, Hecke operators and equidistribution of Hecke points, *Invent. Math.* **144** no. 2 (2001), 327–351. MR 1827734. Zbl 1144.11301. https://doi.org/10.1007/s002220100126.

[CU04] L. Clozel and E. Ullmo, Équidistribution des points de Hecke, in *Contributions to Automorphic Forms, Geometry, and Number Theory*, Johns Hopkins Univ. Press, Baltimore, MD, 2004, pp. 193–254. MR 2058609. Zbl 1068.11042.

[CI00] J. B. Conrey and H. Iwaniec, The cubic moment of central values of automorphic L-functions, *Ann. of Math.* (2) **151** no. 3 (2000), 1175–1216. MR 1779567. Zbl 0973.11056. https://doi.org/10.2307/121132.

[Cor11] Y. Cornulier, On the Chabauty space of locally compact abelian groups, *Algebr. Geom. Topol.* **11** no. 4 (2011), 2007–2035. MR 2826931. Zbl 1221.22008. https://doi.org/10.2140/agt.2011.11.2007.

[vdC20] J. G. van der Corput, Über Gitterpunkte in der Ebene, *Math. Ann.* **81** no. 1 (1920), 1–20. MR 1511951. JFM 47.0159.01. https://doi.org/10.1007/BF01563613.

[DJL78] R. A. Demillo and R. J. Lipton, A probabilistic remark on algebraic program testing, *Information Processing Letters* **7** no. 4 (1978), 193 – 195. Zbl 0397.68011. https://doi.org/10.1016/0020-0190(78)90067-4.

[Dic01] L. E. Dickson, Theory of linear groups in an arbitrary field, *Trans. Amer. Math. Soc.* **2** no. 4 (1901), 363–394. MR 1500573. Zbl 32.0131.03. https://doi.org/10.2307/1986251.

[Duk88] W. Duke, Hyperbolic distribution problems and half-integral weight Maass forms, *Invent. Math.* **92** no. 1 (1988), 73–90. MR 0931205. Zbl 0628.10029. https://doi.org/10.1007/BF01393993.

[Edi98] B. Edixhoven, Special points on the product of two modular curves, *Compositio Math.* **114** no. 3 (1998), 315–328. MR 1665772. Zbl 0928.14019. https://doi.org/10.1023/A:1000539721162.

[Edi05] B. Edixhoven, Special points on products of modular curves, *Duke Math. J.* **126** no. 2 (2005), 325–348. MR 2115260. Zbl 1072.14027. https://doi.org/10.1215/S0012-7094-04-12624-7.

[EKL06] M. Einsiedler, A. Katok, and E. Lindenstrauss, Invariant measures and the set of exceptions to Littlewood's conjecture, *Ann. of Math.* (2) **164** no. 2 (2006), 513–560. MR 2247967. Zbl 1109.22004. https://doi.org/10.4007/annals.2006.164.513.

[EL10] M. Einsiedler and E. Lindenstrauss, Diagonal actions on locally homogeneous spaces, in *Homogeneous Flows, Moduli Spaces and Arithmetic*, *Clay Math. Proc.* **10**, Amer. Math. Soc., Providence, RI, 2010, pp. 155–241. MR 2648695. Zbl 1225.37005.

[EL15a] M. Einsiedler and E. Lindenstrauss, Joinings of higher rank torus actions on homogeneous spaces, 2015, to appear, *Publ. Math. Inst. Hautes Études Sci.*, 2017. arXiv 1502.05133.

[EL15b] M. Einsiedler and E. Lindenstrauss, On measures invariant under tori on quotients of semisimple groups, *Ann. of Math.* (2) **181** no. 3 (2015), 993–1031. MR 3296819. Zbl 1316.22009. https://doi.org/10.4007/annals.2015.181.3.3.

[ELMV09] M. Einsiedler, E. Lindenstrauss, P. Michel, and A. Venkatesh, Distribution of periodic torus orbits on homogeneous spaces, *Duke Math. J.* **148** no. 1 (2009), 119–174. MR 2515103. Zbl 1172.37003. https://doi.org/10.1215/00127094-2009-023.

[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** no. 2 (2011), 815–885. MR 2776363. Zbl 1248.37009. https://doi.org/10.4007/annals.2011.173.2.5.

[ELMV12] M. Einsiedler, E. Lindenstrauss, P. Michel, and A. Venkatesh, The distribution of closed geodesics on the modular surface, and Duke's theorem, *Enseign. Math.* (2) **58** no. 3-4 (2012), 249–313. MR 3058601. Zbl 1312.37032. https://doi.org/10.4171/LEM/58-3-2.

[EMV13] J. S. Ellenberg, P. Michel, and A. Venkatesh, Linnik's ergodic method and the distribution of integer points on spheres, in *Automorphic Representations and L-Functions*, *Tata Inst. Fundam. Res. Stud. Math.* **22**, Tata Inst. Fund. Res., Mumbai, 2013, pp. 119–185. MR 3156852. Zbl 1371.11071.

[GKM15] A. Granville, D. Koukoulopoulos, and K. Matomäki, When the sieve works, *Duke Math. J.* **164** no. 10 (2015), 1935–1969. MR 3369306. Zbl 1326.11055. https://doi.org/10.1215/00127094-3120891.

[GZ86] B. H. Gross and D. B. Zagier, Heegner points and derivatives of L-series, *Invent. Math.* **84** no. 2 (1986), 225–320. MR 0833192. Zbl 0608.14019. https://doi.org/10.1007/BF01388809.

[Hol10] R. Holowinsky, Sieving for mass equidistribution, *Ann. of Math.* (2) **172** no. 2 (2010), 1499–1516. MR 2680498. Zbl 1214.11054.

[HS10] R. Holowinsky and K. Soundararajan, Mass equidistribution for Hecke eigenforms, *Ann. of Math.* (2) **172** no. 2 (2010), 1517–1528. MR 2680499. Zbl 1211.11050. https://doi.org/10.4007/annals.2010/172.1517.

[HM79] R. E. Howe and C. C. Moore, Asymptotic properties of unitary representations, *J. Funct. Anal.* **32** no. 1 (1979), 72–96. MR 0533220. Zbl 0404.22015. https://doi.org/10.1016/0022-1236(79)90078-8.

[Hux03] M. N. Huxley, Exponential sums and lattice points. III, *Proc. London Math. Soc.* (3) **87** no. 3 (2003), 591–609. MR 2005876. Zbl 1065.11079. https://doi.org/10.1112/S0024611503014485.

[Iwa87] H. Iwaniec, Fourier coefficients of modular forms of half-integral weight, *Invent. Math.* **87** no. 2 (1987), 385–401. MR 0870736. Zbl 0606.10017. https://doi.org/10.1007/BF01389423.

[JL70] H. Jacquet and R. P. Langlands, *Automorphic Forms on* GL(2), *Lecture Notes in Math.* **114**, Springer-Verlag, Berlin-New York, 1970. MR 0401654. Zbl 0236.12010. https://doi.org/10.1007/BFb0058988.

[Kem78] G. R. Kempf, Instability in invariant theory, *Ann. of Math.* (2) **108** no. 2 (1978), 299–316. MR 0506989. Zbl 0406.14031. https://doi.org/10.2307/1971168.

[Kha17] I. Khayutin, Large deviations and effective equidistribution, *Int. Math. Res. Not. IMRN* no. 10 (2017), 3050–3106. MR 3658132. https://doi.org/10.1093/imrn/rnw099.

[Kne65] M. Kneser, Galois-Kohomologie halbeinfacher algebraischer Gruppen über $\mathfrak{p}$-adischen Körpern. I, *Math. Z.* **88** (1965), 40–47. MR 0174559. Zbl 0143.04702. https://doi.org/10.1007/BF01112691.

[Kow08] E. Kowalski, *The Large Sieve and its Applications*, Arithmetic Geometry, Random Walks and Discrete Groups, *Cambridge Tracts in Math.* **175**, Cambridge University Press, Cambridge, 2008. MR 2426239. Zbl 1177.11080. https://doi.org/10.1017/CBO9780511542947.

[Lan18] E. Landau, Über imaginär- quadratischer zahlkörper, *Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen, Mathematisch-Physikalische Klasse* **1918** (1918), 285–295. Zbl 46.0258.04. Available at http://eudml.org/doc/59028.

[Lem07] F. Lemmermeyer, The development of the principal genus theorem, in *The Shaping of Arithmetic after C. F. Gauss's Disquisitiones Arithmeticae*, Springer, Berlin, 2007, pp. 529–561. MR 2308295. https://doi.org/10.1007/978-3-540-34720-0_20.

[Lin06] E. Lindenstrauss, Invariant measures and arithmetic quantum unique ergodicity, *Ann. of Math.* (2) **163** no. 1 (2006), 165–219. MR 2195133. Zbl 1104.22015. https://doi.org/10.4007/annals.2006.163.165.

[Lin68] Y. V. Linnik, *Ergodic Properties of Algebraic Fields, translated from the Russian by M. S. Keane*, Ergeb. Math. Grenzgeb. **45**, Springer-Verlag New York Inc., New York, 1968. MR 0238801. Zbl 0162.06801.

[LRS99] W. Luo, Z. Rudnick, and P. Sarnak, On the generalized Ramanujan conjecture for GL(n), in *Automorphic Forms, Automorphic Representations, and Arithmetic* (Fort Worth, TX, 1996), *Proc. Sympos. Pure Math.* **66**, Amer. Math. Soc., Providence, RI, 1999, pp. 301–310. MR 1703764. Zbl 0965.11023.

[MT94] G. A. Margulis and G. M. Tomanov, Invariant measures for actions of unipotent groups over local fields on homogeneous spaces, *Invent. Math.* **116** no. 1-3 (1994), 347–392. MR 1253197. Zbl 0816.22004. https://doi.org/10.1007/BF01231565.

[Mic04] P. Michel, The subconvexity problem for Rankin-Selberg L-functions and equidistribution of Heegner points, *Ann. of Math.* (2) **160** no. 1 (2004), 185–236. MR 2119720. Zbl 1068.11033. https://doi.org/10.4007/annals.2004.160.185.

[MV06] P. Michel and A. Venkatesh, Equidistribution, L-functions and ergodic theory: on some problems of Yu. Linnik, in *International Congress of Mathematicians. Vol. II*, Eur. Math. Soc., Zürich, 2006, pp. 421–457. MR 2275604. Zbl 1157.11019.

[Mil05] J. S. Milne, Introduction to Shimura varieties, in *Harmonic Analysis*, *the Trace Formula*, *and Shimura Varieties*, *Clay Math. Proc.* **4**, Amer. Math. Soc., Providence, RI, 2005, pp. 265–378. MR 2192012. Zbl 1148.14011. Available at http://www.claymath.org/library/proceedings/cmip04.pdf.

[MFK94] D. Mumford, J. Fogarty, and F. Kirwan, *Geometric Invariant Theory*, third ed., *Ergeb. Math. Grenzgeb.* **34**, Springer-Verlag, Berlin, 1994. MR 1304906. Zbl 0797.14004.

[Nag64] M. Nagata, Invariants of a group in an affine ring, *J. Math. Kyoto Univ.* **3** (1963/1964), 369–377. MR 0179268. Zbl 0146.04501. https://doi.org/10.1215/kjm/1250524787.

[Nai92] M. Nair, Multiplicative functions of polynomial values in short intervals, *Acta Arith.* **62** no. 3 (1992), 257–269. MR 1197420. Zbl 0768.11038. https://doi.org/10.4064/aa-62-3-257-269.

[NT98] M. Nair and G. Tenenbaum, Short sums of certain arithmetic functions, *Acta Math.* **180** no. 1 (1998), 119–144. MR 1618321. Zbl 0917.11048. https://doi.org/10.1007/BF02392880.

[Pil11] J. Pila, O-minimality and the André-Oort conjecture for $\mathbb{C}^n$, *Ann. of Math.* (2) **173** no. 3 (2011), 1779–1840. MR 2800724. Zbl 1243.14022. https://doi.org/10.4007/annals.2011.173.3.11.

[PT13] J. Pila and J. Tsimerman, The André-Oort conjecture for the moduli space of abelian surfaces, *Compos. Math.* **149** no. 2 (2013), 204–216. MR 3020307. Zbl 1304.11055. https://doi.org/10.1112/S0010437X12000589.

[Rei75] I. Reiner, *Maximal Orders*, *London Math. Soc. Monogr.* **5**, Academic Press [A subsidiary of Harcourt Brace Jovanovich, Publishers], London-New York, 1975. MR 0393100. Zbl 1024.16008.

[Sar91] P. C. Sarnak, Diophantine problems and linear groups, in *Proceedings of the International Congress of Mathematicians*, *Vol. I*, *II* (Kyoto, 1990), Math. Soc. Japan, Tokyo, 1991, pp. 459–471. MR 1159234. Zbl 0743.11018.

[Sch80] J. T. Schwartz, Fast probabilistic algorithms for verification of polynomial identities, *J. Assoc. Comput. Mach.* **27** no. 4 (1980), 701–717. MR 0594695. Zbl 0452.68050. https://doi.org/10.1145/322217.322225.

[Sha88] F. Shahidi, On the Ramanujan conjecture and finiteness of poles for certain L-functions, *Ann. of Math.* (2) **127** no. 3 (1988), 547–584. MR 0942520. Zbl 0654.10029. https://doi.org/10.2307/2007005.

[ST17] V. Shende and J. Tsimerman, Equidistribution in $\mathrm{Bun}_2(\mathbb{P}^1)$, *Duke Math. J.* **166** no. 18 (2017), 3461–3504. MR 3732881. Zbl 06837465. https://doi.org/10.1215/00127094-2017-0025.

[Shi80] P. Shiu, A Brun-Titchmarsh theorem for multiplicative functions, *J. Reine Angew. Math.* **313** (1980), 161–170. MR 0552470. Zbl 0412.10030. https://doi.org/10.1515/crll.1980.313.161.

[Tao14] T. Tao, Algebraic combinatorial geometry: the polynomial method in arithmetic combinatorics, incidence combinatorics, and number theory, *EMS Surv. Math. Sci.* **1** no. 1 (2014), 1–46. MR 3200226. Zbl 1294.05044. https://doi.org/10.4171/EMSS/1.

[Tsi18] J. Tsimerman, The André-Oort conjecture for $\mathscr{A}_g$, *Ann. of Math.* (2) **187** no. 2 (2018), 379–390. MR 3744855. Zbl 06841543. https://doi.org/10.4007/annals.2018.187.2.2.

[Zha05] S.-W. Zhang, Equidistribution of CM-points on quaternion Shimura varieties, *Int. Math. Res. Not.* no. 59 (2005), 3657–3689. MR 2200081. Zbl 1096.14016. https://doi.org/10.1155/IMRN.2005.3657.

[Zip79] R. Zippel, Probabilistic algorithms for sparse polynomials, in *Symbolic and Algebraic Computation* (EUROSAM '79, Internat. Sympos., Marseille, 1979), *Lecture Notes in Comput. Sci.* **72**, Springer, Berlin-New York, 1979, pp. 216–226. MR 0575692. Zbl 0418.68040. https://doi.org/10.1007/3-540-09519-5_73.

(Received: October 18, 2017)
(Revised: October 15, 2018)

Princeton University, Princeton, NJ
and Institute for Advanced Study, Princeton, NJ
E-mail: khayutin@princeton.edu