Equidistribution of Heegner Points and Ternary Quadratic Forms

Dimitar Jetchev and Ben Kane

Abstract

We prove new equidistribution results for Galois orbits of Heegner points with respect to reduction maps at inert primes. The arguments are based on two different techniques: primitive representations of integers by quadratic forms and distribution relations for Heegner points. Our results generalize one of the equidistribution theorems established by Cornut and Vatsal in the sense that we allow both the fundamental discriminant and the conductor to grow. Moreover, for fixed fundamental discriminant and variable conductor, we deduce an effective surjectivity theorem for the reduction map from Heegner points to supersingular points at a fixed inert prime. Our results are applicable to the setting considered by Kolyvagin in the construction of the Heegner points Euler system.

1. Introduction

Uniform distribution of Galois orbits of Heegner points with respect to reduction maps was the key step in the argument of Cornut and Vatsal for the proof of Mazur's conjecture on the non-triviality of Heegner points over the p-adic anticyclotomic tower (see [Maz83] for the statement; [Cor02], [Vat02], [Vat03] and [CV05] for the proofs). Both Cornut and Vatsal used ergodic theory techniques based on Ratner's theorem for unipotent flows on p-adic Lie groups (see [Rat95]) in order to prove the results for simultaneous reduction maps (i.e., maps that reduce simultaneously n-tuples of Galois conjugates of Heegner points modulo a fixed inert prime ℓ). Due to the p-adic nature of the ergodic techniques, one needs to fix the fundamental discriminant and vary the conductor p-adically.

This paper proves a more general equidistribution result for single reduction maps, in the sense that both the fundamental discriminant and the conductor are allowed to vary and the only assumption on the conductor is that it is prime to the level of the modular curve. We avoid the ergodic theory by using arguments based on equidistribution of primitive representations of integers by quadratic forms in genera, as well as distribution relations of Heegner points and Hecke eigenvalue bounds. Along the way, we obtain a generalization of an equidistribution theorem for Gross points on definite Shimura curves established by Michel. Finally, we prove effective surjectivity results for sufficiently large Galois orbits with respect to reduction maps in the case when the fundamental discriminant is fixed and the conductor varies.

1.1 Notation and hypothesis

Let $N \geqslant 1$ be an integer and let $X_0(N)_{/\mathbb{Q}}$ be the modular curve associated to the congruence subgroup $\Gamma_0(N)$ of $\mathrm{SL}_2(\mathbb{Z})$. Let ℓ be a prime such that $(\ell, N) = 1$ and let $\mathcal{D}_N$ be the set of all fundamental discriminants $D < 0$ such that every prime factor of N is split in $K_D := \mathbb{Q}(\sqrt{D})$ and such that ℓ is inert in K_D. Let Ω_N be the set of all pairs (D, c), where $D \in \mathcal{D}_N$ and $(c, N) = 1$.

2000 Mathematics Subject Classification
Keywords:

Fix an embedding $\iota : \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_\ell$ (i.e., a prime in $\overline{\mathbb{Q}}$ lying above ℓ). Let $(D, c) \in \Omega_N$ and let $\mathcal{O}_{D,c}$ be the order of conductor c in the quadratic imaginary field $K_D = \mathbb{Q}(\sqrt{D})$. Fix an ideal $\mathfrak{n}_D \subset \mathcal{O}_{D,1}$ for which $\mathcal{O}_{D,1}/\mathfrak{n}_D \cong \mathbb{Z}/N\mathbb{Z}$. For $(c, N) = 1$, $\mathfrak{n}_{D,c} := \mathfrak{n}_D \cap \mathcal{O}_{D,c}$ is an invertible ideal of $\mathcal{O}_{D,c}$. Consider the point $x_c = [\mathbb{C}/\mathcal{O}_{D,c} \to \mathbb{C}/\mathfrak{n}_{D,c}^{-1}] \in X_0(N)(\overline{\mathbb{Q}})$. By the theory of complex multiplication, it is defined over the ring class field $K_D[c]$ of conductor c for K_D. We refer to that point as the higher Heegner point of conductor c. Let $\Gamma_{D,c} := \{\sigma x_c : \sigma \in \mathrm{Gal}(K_D[c]/K_D)\}$ be the corresponding Galois orbit. The fixed embedding ι gives us a prime in $K_D[c]$ above ℓ. The choice of the embedding defines a reduction map

$$\mathrm{red}_\ell : X_0(N)(K_D[c]) \hookrightarrow X_0(N)(K_D[c]_\ell) = X_0(N)(\mathcal{O}_{K_D[c]_\ell}) \xrightarrow{\mathrm{mod}\ \ell} X_0(N)(\overline{\mathbb{F}}_\ell)$$

where $\mathcal{O}_{K_D[c]_\ell}$ is the ring of integers of the completion $K_D[c]_\ell$ (the equality in the middle follows from the valuative criterion of properness). Moreover, since ℓ is inert in K_D, then CM points for K_D reduce to supersingular points modulo ℓ (see [Deu41]). Let $X_0(N)^{\mathrm{SS}}_{/\overline{\mathbb{F}}_\ell}$ be the set of supersingular points on $X_0(N)$ modulo ℓ. It is well-known that these points are defined over $\mathbb{F}_{\ell^2}$. We will prove an equidistribution theorem according to which as $d_c := -Dc^2 \to \infty$, every $s \in X_0(N)^{\mathrm{SS}}_{/\mathbb{F}_{\ell^2}}$ will have the same number of preimages in $\Gamma_{D,c}$ under red_ℓ. We will state our result in terms of probability measures on the finite set $X_0(N)^{\mathrm{SS}}_{/\mathbb{F}_{\ell^2}}$.

1.2 A canonical measure on $X_0(N)^{\mathrm{SS}}_{/\overline{\mathbb{F}}_\ell}$

Let $s \in X_0(N)^{\mathrm{SS}}_{/\mathbb{F}_{\ell^2}}$ be a supersingular point. Then s is represented by a pair $(\tilde{E}, \tilde{C})$ of a supersingular elliptic curve $\tilde{E}_{/\overline{\mathbb{F}}_\ell}$ and a cyclic subgroup $\tilde{C}$ of $\tilde{E}$ of order N. Following [Rib90, §3], we refer to the pair $\mathbb{E} = (\tilde{E}, \tilde{C})$ as an *enhanced elliptic curve* over $\mathbb{F}_{\ell^2}$. Homomorphisms of enhanced elliptic curves are defined in the obvious way. In particular, one could talk about endomorphisms and automorphisms of enhanced elliptic curves.

Let $\mathbb{E} = (\tilde{E}, \tilde{C})$ be an enhanced elliptic curve representing the point s. The endomorphism algebra $\mathrm{End}(\tilde{E}) \otimes \mathbb{Q}$ is isomorphic to the unique quaternion algebra $B_{\ell,\infty}$ ramified precisely at ℓ and ∞. The endomorphism ring $\mathrm{End}(\tilde{E})$ is a maximal order in $B_{\ell,\infty}$ and the ring $\mathrm{End}(\mathbb{E})$ is an Eichler order of level N. Indeed, if $\lambda : \tilde{E} \to \tilde{E}/\tilde{C}$ is the quotient map, then $\mathrm{End}(\tilde{E}/\tilde{C})$ can be viewed as a subring of $B_{\ell,\infty}$ via the map $\sigma \in \mathrm{End}(\tilde{E}/\tilde{C}) \mapsto \lambda^{-1}\sigma\lambda$. Then $\mathrm{End}(\mathbb{E})$ is the intersection of the two maximal orders $\mathrm{End}(\tilde{E})$ and $\mathrm{End}(\tilde{E}/\tilde{C})$. Let R_s denote this Eichler order and let $w_s := \#R_s^\times$. We can use w_s to define a canonical measure μ_{can} on $X_0(N)^{\mathrm{SS}}_{/\mathbb{F}_{\ell^2}}$ by

$$\mu_{\mathrm{can}}(s) := \frac{1/w_s}{\sum_{s' \in X_0(N)^{\mathrm{SS}}_{/\mathbb{F}_{\ell^2}}} 1/w_{s'}}.$$

1.3 Main results

1. Equidistribution of Heegner points. We can now state the main result of the paper. For $(D, c) \in \Omega_N$, define a measure $\mu_{D,c}$ on the finite set $X_0(N)^{\mathrm{SS}}_{/\mathbb{F}_{\ell^2}}$ by

$$\mu_{D,c}(s) := \frac{\#\{x \in \Gamma_{D,c} : \mathrm{red}_\ell(x) = s\}}{\#\Gamma_{D,c}}, \quad s \in X_0(N)^{\mathrm{SS}}_{/\mathbb{F}_{\ell^2}}.$$

Theorem 1.1. *The weak-* limit* $\lim\limits_{\substack{-Dc^2 \to \infty, \\ (D,c) \in \Omega_N}} \mu_{D,c}$ *exists and equals* μ_{can}.

Remark 1. To say that the weak-* limit of a sequence of measures $\{\mu_n\}$ on a finite set X exists and converges to a measure μ on X means that for each function $f : X \to \mathbb{R}$, the limit $\lim\limits_{n \to \infty} \int_X f d\mu_n$

exists and equals $\int_X f d\mu$.

2. Equidistribution of Gross points on the definite quaternion algebra $B_{\ell,\infty}$. The curve $X_0(N)_{/\mathbb{Q}}$ can be viewed as a Shimura curve for the quaternion algebra $M_2(\mathbb{Q})$, and thus, Heegner points can be regarded as CM points on the indefinite quaternion algebra $M_2(\mathbb{Q})$. In the case of a totally definite quaternion algebra (e.g., $B_{\ell,\infty}$), the analogues of Heegner points (also known as Gross points) were studied in detail by Gross [Gro87].

Let G' be the algebraic group associated to $B_{\ell,\infty}^\times$ and let $I_1, \dots, I_h$ be left ideals representing the left ideal classes (corresponding to the double quotient $G'(\mathbb{Q})\backslash G'(\mathbb{A}_f)/\widehat{R}^\times$). Let $R_1, \dots, R_h$ be the associated Eichler orders. Given a conductor c, the points of conductor c are simply pairs $(f : \mathcal{O}_c \hookrightarrow R_{i/R_i^\times}, R_i)$ of one of these orders R_i and an $R_i^\times$-conjugacy classes of optimal embeddings $f : \mathcal{O}_c \to R_i$. Recall that $f : \mathcal{O}_c \to R$ is optimal if $f(K) \cap R = \mathcal{O}_c$ (we have extended f to an embedding $f : K \to B_{\ell,\infty}$). Let $\tilde{\mu}_{D,c}([I_i])$ be the number of Gross points (f, R_i) of conductor c divided by the total number of Gross points of conductor c. Then $\tilde{mu}_{D,c}$ is a probability measure on $G'(\mathbb{Q})\backslash G'(\mathbb{A}_f)/\widehat{R}^\times$. There is a canonical measure on $G'(\mathbb{Q})\backslash G'(\mathbb{A}_f)/\widehat{R}^\times$ defined as

$$\tilde{\mu}_{\mathrm{can}}([I_k]) := \frac{1/w_k}{\sum_{i=1}^h 1/w_i}.$$

Theorem 1.2. *The weak-* limit* $\lim_{\substack{-Dc^2\to\infty,\\ (D,c)\in\Omega_N}} \tilde{\mu}_{D,c}$ *exists and equals* $\tilde{\mu}_{\mathrm{can}}$.

Remark 2. A similar statement (for trivial conductor $c = 1$) has already been established by Michel [Mic04, Thm.3] using subconvexity bounds for L-functions and independently by Elkies, Ono, and Yang [EOY05, Theorem 1.2].

Remark 3. Both Theorem 1.1 and Theorem 1.2 hold in greater generality for CM points on indefinite and totally definite quaternion algebras, respectively, with respect to more general reduction maps at several primes. The more general statements will be the subject of a forthcoming paper.

Remark 4. We will see in Section 2.5 that the canonical measures μ_{can} and $\tilde{\mu}_{\mathrm{can}}$ indeed coincide.

3. Congruences for Hilbert class polynomials under the U-operator. Recall that for a function with Fourier expansion $f(z) = \sum_{n\geqslant 0} a(n)q^n$ the operator $U(\ell)$ is defined by $f(z)|U(\ell) := \sum_{n\geqslant 0} a(\ell n)q^n$. Elkies, Ono and Yang were interested in the equidistribution of Heegner points with respect to reduction maps which they used to study a certain congruence for the Hilbert class polynomial under the U-operator. In particular, combining the case $N = 1$ of Theorem 1.1 with [EOY05, Thm 2.3 (1)] gives the following immediate corollary (the case $c = 1$ is [EOY05, Thm. 1.1]):

Corollary 1.3. *Let $H_{D,c} \in \mathbb{Z}[x]$ be the polynomial whose roots are precisely the j-invariants of those elliptic curves with CM by $\mathcal{O}_{D,c}$. Let ℓ be a prime which is nonsplit in $\mathcal{O}_{D,c}$. Then for $d_c = -Dc^2$ sufficiently large (depending on ℓ) there exists a polynomial $P_{D,c,\ell} \in \mathbb{Z}[x]$ such that*

$$H_{D,c}(j(z))|U(\ell) \equiv P_{D,c,\ell}(j(z)) \pmod{\ell}.$$

4. Effective surjectivity of red_ℓ. One consequence of both Theorem 1.1 and Theorem 1.2 is the fact that for sufficiently large discriminant $d_c = -Dc^2$, the reduction map from CM points of conductor c to supersingular points is surjective. It is natural to ask whether this theorem can be made effective. The ineffectiveness of one of the ingredients used in our argument, Siegel's lower bound on the class number, prevents us from establishing an effective result when both D and c vary. Yet, fixing the fundamental discriminant D and varying the conductor c, one can establish effective surjectivity theorems (see Theorem 6.1 and Lemma 6.2).

2. Heegner points and optimal embeddings

Let $s \in X_0(N)^{\mathrm{SS}}_{/\mathbb{F}_{\ell^2}}$ be a supersingular point modulo ℓ. In this section we will establish a one-to-one correspondence between

$$\left\{ \begin{array}{c} \text{Heegner points } x \text{ on } X_0(N) \text{ of conductor } c \\ \text{reducing to } s \in X_0(N)^{\mathrm{SS}}_{/\mathbb{F}_\ell} \end{array} \right\} \iff \left\{ \begin{array}{c} R_s^\times - \text{conjugacy classes of} \\ \text{optimal embeddings } \mathcal{O}_{D,c} \hookrightarrow R_s \end{array} \right\}$$

For $c = 1$, the above correspondence is known as Deuring lifting theorem (see [Deu41]) and has been subsequently refined (as a correspondence) by Gross and Zagier [GZ85, Prop.2.7]. We will deduce the correspondence from a recent result of the first author and Cornut [CJ09].

2.1 Galois orbits of Heegner points

We start by proving that there are exactly $2^{\nu(N)}$ Galois orbits of Heegner points of conductor c, where $\nu(N)$ is the number of distinct prime divisors of N.

Lemma 2.1. *Suppose that $(c, N) = 1$. Then there are exactly $2^{\nu(N)}$ Galois orbits of Heegner points of conductor c on $X_0(N)$ and each of these orbits has size $\#\operatorname{Pic}(\mathcal{O}_{D,c})$.*

Proof. Consider the set of all Heegner points of conductor c on $X_0(N)$. They could be described as pairs $([\mathfrak{a}], \mathfrak{n})$ of an ideal class $[\mathfrak{a}]$ and an ideal $\mathfrak{n} \subset \mathcal{O}_K$ with the property that $\mathcal{O}_K/\mathfrak{n} \cong \mathbb{Z}/N\mathbb{Z}$. The last property is equivalent to the fact that $\mathfrak{n}$ is primitive of norm N ($\mathfrak{n}$ being primitive means that there is no rational prime number dividing $\mathfrak{n}$). Equivalently, if $N = p_1^{e_1} \dots p_t^{e_t}$ are the distinct prime divisors of N, we want $\mathfrak{n} = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_t^{e_t}$, where $\mathfrak{p}_i$ is one of the primes of $\mathcal{O}_K$ above p_i (indeed, if both $\mathfrak{p}_i$ and $\overline{\mathfrak{p}}_i$ occur then $\mathfrak{n}$ would be divisible by p_i and hence, would not be primitive). □

2.2 Modular curves and Shimura curves

Let Γ be a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$ and let $U = U(\Gamma)$ be the closure of Γ in $\mathrm{SL}_2(\mathbb{A}_f)$. The group $\mathrm{SL}_2(\mathbb{Q})$ admits a left action on $\mathfrak{h}$ by linear fractional transformations and a left action on $\mathrm{SL}_2(\mathbb{A}_f)$ by left multiplication. Thus, $\mathrm{SL}_2(\mathbb{Q})$ acts on the left on $\mathfrak{h} \times \mathrm{SL}_2(\mathbb{A}_f)$. Moreover, U has a right action on $\mathfrak{h} \times \mathrm{SL}_2(\mathbb{A}_f)$ by acting trivially on $\mathfrak{h}$ and by right multiplication on $\mathrm{SL}_2(\mathbb{A}_f)$. Strong approximation (see [Vig80, p.81]) gives a homeomorphism

$$Y(\Gamma) := \Gamma\backslash\mathfrak{h} \to \mathrm{SL}_2(\mathbb{Q})\backslash\mathfrak{h} \times \mathrm{SL}_2(\mathbb{A}_f)/U, \ z \mapsto [z, 1].$$

Let H be the compact open subgroup of $\mathrm{GL}_2(\mathbb{A}_f)$ that is the closure (in $\mathrm{GL}_2(\mathbb{A}_f)$) of the image of U under the inclusion $\mathrm{SL}_2(\mathbb{A}_f) \hookrightarrow \mathrm{GL}_2(\mathbb{A}_f)$. We define the Shimura curve corresponding to the compact open subgroup H as

$$\mathrm{Sh}_H = \mathrm{GL}_2(\mathbb{Q})\backslash(\mathbb{C}\backslash\mathbb{R}) \times \mathrm{GL}_2(\mathbb{A}_f)/H.$$

We shall see that Sh_H is a disjoint union of two copies of $Y(\Gamma)$. Indeed, consider the map

$$\phi : \mathrm{Sh}_H \to \mathbb{Q}^\times\backslash\{\pm 1\} \times \mathbb{A}_f^\times/\det(H)$$

given by $[z, g] \mapsto [\mathrm{sgn}(\mathrm{Im}(z)), \det(g)]$. The fiber of this map over the point $[+1, 1]$ is isomorphic to $\mathrm{SL}_2(\mathbb{Q})\backslash\mathrm{SL}_2(\mathbb{A}_f)/U \cong Y(\Gamma)$. Since $\det(H)$ is open, it follows that the quotient $\mathbb{Q}^\times\backslash\mathbb{A}_f^\times/\det(H)$ is discrete. Since $\mathbb{Q}^\times\backslash\mathbb{A}_f^\times \cong \widehat{\mathbb{Z}}^\times$ is compact, the double quotient $\mathbb{Q}^\times\backslash\mathbb{A}_f^\times/\det(H)$ is finite. The quotient $\mathbb{Q}^\times\backslash\{\pm 1\} \times \mathbb{A}_f^\times/\det(H)$ describes the connected components of the Shimura curve Sh_H. For instance, for classical modular curves,

$$\mathrm{GL}_2(\mathbb{Q})\backslash(\mathbb{C}\backslash\mathbb{R}) \times \mathrm{GL}_2(\mathbb{A}_f)/H \cong Y(\Gamma)^+ \sqcup Y(\Gamma)^-.$$

2.3 Adelic description of CM points

1. CM points on the Shimura curve Sh_H. Fix an embedding $K \hookrightarrow M_2(\mathbb{Q})$. This gives us an embedding $T \hookrightarrow \mathrm{GL}_2$, where $T := \mathrm{Res}_{K/\mathbb{Q}} K^\times$. Consider the set CM_H of all points of the form $[g,h] \in \mathrm{Sh}_H$ whose stabilizer is a torus isomorphic to $K^\times$. It is easy to verify that an element $z \in \mathbb{C}\backslash\mathbb{R}$ is in K if and only if $\mathrm{Stab}_{\mathrm{GL}_2(\mathbb{Q})}(z)$ is isomorphic to $\mathrm{Res}_{K/\mathbb{Q}} K^\times = T$. This allows us to conclude that CM_H admits an adelic description as the double quotient $T(\mathbb{Q})\backslash \mathrm{GL}_2(\mathbb{A}_f)/H$. Indeed, a point in CM_H is represented by a pair $[z,g]$, where $z \in \mathbb{C}\backslash\mathbb{R}$ is in K and $g \in \mathrm{GL}_2(\mathbb{A}_f)$. Since all $z \in K$ are $\mathrm{GL}_2(\mathbb{Q})$-conjugates and since the stabilizer of each z in $\mathrm{GL}_2(\mathbb{Q})$ is isomorphic to $T(\mathbb{Q})$, we obtain

$$\mathrm{CM}_H \cong T(\mathbb{Q})\backslash \mathrm{GL}_2(\mathbb{A}_f)/H.$$

3. Conductors of CM points. Here, we assume that $R = (R', R'')$ is an oriented Eichler order of $M_2(\mathbb{Q})$ of level N (i.e., R' and R'' are maximal orders and $R = R' \cap R''$) and consider the Shimura curve Sh_H, where $H = \widehat{R}^\times$. Consider the two degeneracy maps

$$\delta' : \mathrm{CM}_H \to T(\mathbb{Q})\backslash \mathrm{GL}_2(\mathbb{A}_f)/\widehat{R'}^\times$$

and

$$\delta'' : \mathrm{CM}_H \to T(\mathbb{Q})\backslash \mathrm{GL}_2(\mathbb{A}_f)/\widehat{R''}^\times.$$

Given a CM point $x \in T(\mathbb{Q})\backslash G(\mathbb{A}_f)/\widehat{R}^\times$ such that $x = [g]$, let x' and x'' be the images of x in $T(\mathbb{Q})\backslash G(\mathbb{A}_f)/\widehat{R'}^\times$ and $T(\mathbb{Q})\backslash G(\mathbb{A}_f)/\widehat{R''}^\times$, respectively. The stabilizer

$$\mathrm{Stab}_{\widehat{K}^\times}(x') = \widehat{K}^\times \cap g\widehat{R'}^\times g^{-1} = \widehat{\mathcal{O}(x')}^\times$$

for some order $\mathcal{O}(x') \subseteq \mathcal{O}_K$. Let $c(x')$ be the conductor of that order. Similarly, we obtain an integer $c(x'')$ for R''. The conductor $\mathbf{c}(x)$ is then defined as

$$\mathbf{c}(x) := \mathrm{lcm}(c(x'), c(x'')).$$

Remark 5. Note that if q is a prime that divides one of $c(x')$ and $c(x'')$, but not the other one, then q necessarily divides N. This shows that if $(c,N) = 1$, all CM points of conductor c will be in fact Heegner points (i.e, $c(x') = c(x'')$).

Remark 6. For $\Gamma = \Gamma_0(N)$, i.e., for the modular curve $X_0(N)$, these degeneracy maps correspond precisely to the two degeneracy maps $\delta_1, \delta_N : X_0(N) \to X(1)$ that map $[E,C]$ to $[E]$ and $[E/C]$, respectively.

Remark 7. If $X = X_0(N)$, a CM point $[\tau] \in \Gamma_0(N)\backslash\mathfrak{h}$ would correspond to the pair of N-isogenous CM elliptic curves $E' = \mathbb{C}/\langle 1, \tau\rangle$ and $E'' = \mathbb{C}/\langle 1, N\tau\rangle$. Then $\mathcal{O}' = \mathrm{End}(E')$ and $\mathcal{O}'' = \mathrm{End}(E'')$ are both orders in $K = \mathbb{Q}(\sqrt{-D})$. Let c' and c'' be their conductors, respectively. The conductor of the point $[E', E'']$ is then $\mathbf{c}([E', E'']) = \mathrm{lcm}(c', c'')$.

2.4 Optimal embeddings and Gross points

Let $B_{\ell,\infty}$ be the unique quaternion algebra ramified precisely at ℓ and ∞ and let $G' := B_{\ell,\infty}^\times$ be the corresponding algebraic group. Let $R_1, \ldots, R_h$ be the Eichler orders of level N defined in Section 1.3.

Lemma 2.2. *The set of pairs* $(f : \mathcal{O} \hookrightarrow R_i/R_i^\times, [R_i])$ *of an ideal class* $[R_i]$ *of* $G'(\mathbb{Q})\backslash G'(\mathbb{A}_f)/\widehat{R}^\times$ *and a* $R_i^\times$*-conjugacy class of optimal embeddings* $f : \mathcal{O} \hookrightarrow R_i/R_i^\times$ *for some quadratic order* $\mathcal{O}$ *in* K *is in one-to-one correspondence with the double adelic quotient*

$$T(\mathbb{Q})\backslash G'(\mathbb{A}_f)/\widehat{R}^\times.$$

Proof. Given an order R_i representing an ideal class $[R_i]$, the set of $R_i^\times$-conjugacy classes of optimal embeddings $f : \mathcal{O} \hookrightarrow R_i$ is in bijection with $T(\mathbb{Q})\backslash G'(\mathbb{Q})$ (since all the embeddings of K into $B_{\ell,\infty}$ are conjugate). Therefore, the set of the desired pairs is in bijection with

$$T(\mathbb{Q})\backslash G'(\mathbb{Q}) \times G'(\mathbb{Q})\backslash G'(\mathbb{A}_f)/\widehat{R}^\times \cong T(\mathbb{Q})\backslash G'(\mathbb{A}_f)/\widehat{R}^\times.$$

□

2.5 Adelic description of supersingular points

The set $X_0(N)^{\mathrm{SS}}_{/\mathbb{F}_{\ell^2}}$ is in bijection with the double quotient $G'(\mathbb{Q})\backslash G'(\mathbb{A}_f)/\widehat{R'}^\times$ where R' is an Eichler order of level N for $B_{\ell,\infty}$ that is the ring of endomorphisms of a fixed enhanced supersingular elliptic curve $\mathbb{E}_0 = (\tilde{E}_0, \tilde{C}_0)$. We briefly summarize the bijection and refer the reader to [Rib90, Prop.3.3] for the details.

Let $\mathbb{E}$ be any enhanced elliptic curve and take an endomorphism $\lambda \in \mathrm{Hom}(\mathbb{E}, \mathbb{E}_0) \otimes \mathbb{Q}$ (here, we use the fact that there is a single isogeny class of supersingular elliptic curves). One could use λ to identify the adelic Tate module $\widehat{T}(\mathbb{E})$ with a sublattice of $\widehat{V}(\mathbb{E}_0)$. This means that there is a unique element $g \in G'(\mathbb{A}_f)/\widehat{R}^\times$ that sends this sublattice to $\widehat{T}(\mathbb{E}_0)$. Since g is dependent on the choice of λ, it makes sense only in $G'(\mathbb{Q})\backslash G'(\mathbb{A}_f)/\widehat{R}^\times$. This gives us a bijection

$$\varphi : X_0(N)^{\mathrm{SS}}_{/\mathbb{F}_{\ell^2}} \to G'(\mathbb{Q})\backslash G'(\mathbb{A}_f)/\widehat{R}^\times.$$

2.6 Heegner points on definite and indefinite quaternion algebras

The probability measures μ_c are defined in terms of the cardinalities $\left|\mathrm{red}_\ell^{-1}(s) \cap \Gamma_{D,c}\right|$. Let $s \in X_0(N)^{\mathrm{SS}}_{/\mathbb{F}_{\ell^2}}$ be a supersingular point and let $h(\mathcal{O}_{D,c}, R_s)$ be the number of $R_s^\times$-conjugacy classes of optimal embeddings $\mathcal{O}_{D,c} \hookrightarrow R_s$.

We will apply the theorem of Cornut–Jetchev [CJ09, Thm 1.5] together with the above adelic interpretations of CM points, optimal embeddings and supersingular points to deduce the following corollary:

Corollary 2.3. *We have*

$$h(\mathcal{O}_{D,c}, R_s) = 2^{\nu(N)} \left|\{x \in \Gamma_{D,c} \colon \mathrm{red}_\ell(x) = s\}\right|.$$

Proof. By [CJ09, Thm 1.4] and the adelic interpretation of CM points on the definite and the indefinite algebras as well as the adelic desciption of the supersingular points, the subset of CM points on $X_0(N)$ of conductor c reducing to a fixed supersingular point s is in bijection with the $R_s^\times$-conjugacy classes of optimal embeddings $f : \mathcal{O}_c \hookrightarrow R_s$. Since $(c, N) = 1$, all CM points on $X_0(N)$ are Heegner points and by Lemma 2.1 there are exactly $2^{\nu(N)}$ such orbits. □

The corollary shows that

$$\mu_c(s) = \frac{|\{x \in \Gamma_{D,c} \colon \mathrm{red}_\ell(x) = s\}|}{|\Gamma_{D,c}|} = \frac{h(\mathcal{O}_{D,c}, R_s)}{|\mathrm{Pic}(\mathcal{O}_{D,c})|}.$$

In section 4, the number $h(\mathcal{O}_{D,c}, R_s)$ will be related to primitive representations of $d_c = -Dc^2$ by a certain quadratic form associated to R_s.

3. Modular forms of half-integral weight and Shimura correspondence

Let λ be a non-negative integer and consider the space $M_{\lambda+\frac{1}{2}}(\Gamma_0(4M), \chi)$ of modular forms of weight $\lambda + \frac{1}{2}$. Let $S_{\lambda+\frac{1}{2}}(\Gamma_0(4M), \chi)$ be the space of cusp forms. Let $q := e^{2\pi i z}$ and ψ be an odd Dirichlet

character of conductor $r(\psi)$. We will refer to the form

$$h_{\psi,t}(z) := \sum_{m\geqslant 1} \psi(m) m e^{2\pi i t m^2 z} = \sum_{m\geqslant 1} \psi(m) m q^{tm^2} \in S_{3/2}(4r(\psi)^2, \psi\cdot\chi_{-4}) \tag{1}$$

as a *one-dimensional theta series*. Due to the exceptional behaviour of these forms, we will often decompose $S_{3/2}(4M)$ into the subspace spanned by one-dimensional theta series and the orthogonal complement of this space under the Petersson inner product, and then investigate each separately.

3.1 Modular forms of half-integral weight and convolutions with L-series

Suppose that $g(z) \in S_{\lambda+\frac{1}{2}}(\Gamma_0(4M), \chi)$. Let t be a positive square-free integer and let

$$\psi_t(n) := \chi(n) \left(\frac{-1}{n}\right)^{\lambda} \left(\frac{t}{n}\right).$$

Suppose that the complex numbers $A_t(n)$ are defined by

$$\sum_{n=1}^{\infty} \frac{A_t(n)}{n^s} := L(s-\lambda+1, \psi_t) \cdot \sum_{n=1}^{\infty} \frac{b(tn^2)}{n^s}.$$

Shimura then proved that the t-th *Shimura correspondence* $S_{t,\lambda}(g(z)) := \sum_{n=1}^{\infty} A_t(n) q^n$ is a modular form in $M_{2\lambda}(\Gamma_0(2N), \chi^2)$ of weight 2λ.

Kohnen then defined a subspace $S^+_{\lambda+\frac{1}{2}}(\Gamma_0(4M))$, referred to as Kohnen's plus space, consisting of forms $g(z)$ of weight $\lambda+\dfrac{1}{2}$ on $\Gamma_0(4M)$ with Fourier coefficients of the form

$$g(z) = \sum_{(-1)^{\lambda} n \equiv 0,1 \mod 4} b(n) q^n.$$

In this space Kohnen extended the definition of the Shimura correspondence $S_{t,\lambda}$ to $t' := (-1)^{\lambda} D$ where D is a fundamental discriminant. For $D \equiv 1 \pmod 4$ we take $S_{t',\lambda} := S_{t,\lambda}$ as previously defined and for $D \equiv 0 \pmod 4$ we take $S_{t',\lambda} := S_{t,\lambda}|U(4)$. Kohnen's plus space decomposes into new and old subspaces as follows:

$$S^+_{\lambda+\frac{1}{2}}(\Gamma_0(4M)) = S^{\text{new}}_{\lambda+\frac{1}{2}}(\Gamma_0(4M)) \oplus S^{\text{old}}_{\lambda+\frac{1}{2}}(\Gamma_0(4M)).$$

Kohnen used this decomposition and the Shimura correspondences

$$S_{t',\lambda} : S^{\text{new}}_{\lambda+\frac{1}{2}}(\Gamma_0(4M)) \to S_{2\lambda}(\Gamma_0(N))$$

to prove that there exists a finite linear combination of $S_{t',\lambda}$'s which provides an isomorphism

$$S : S^{\text{new}}_{\lambda+\frac{1}{2}}(\Gamma_0(4M)) \to S_{2\lambda}(\Gamma_0(N)) \tag{2}$$

that is Hecke equivariant. The image of a half-integral weight Kohnen newform in $S^{\text{new}}_{\lambda+\frac{1}{2}}(\Gamma_0(4M))$ is a newform in $S^{\text{new}}_{2\lambda}(\Gamma_0(M))$ whose Hecke eigenvalues are the same.

4. Equidistribution and ternary quadratic forms

In order to prove the main theorem, we establish the correspondence between optimal embeddings and primitive representations in Section 4.1 by associating a quadratic form Q_s to the Eichler order R_s. We then compute the discriminant of that quadratic form. We introduce the theta series θ_{Q_s} associated to Q_s, as well as the series $\theta_{\text{gen}(Q_s)}$ and $\theta_{\text{spn}(Q_s)}$ associated to the genus $\text{gen}(Q_s)$ and the

spinor genus $\mathrm{spn}(Q_s)$ of Q_s, respectively. Finally, using that the form $\theta_{\mathrm{gen}(Q_s)} - \theta_{\mathrm{spn}(Q_s)}$ is in the space spanned by one-dimensional theta series, we are able to prove that the coefficients of $\mathrm{gen}(Q_s)$ and $\mathrm{spn}(Q_s)$ coincide away from the primes dividing $N\ell$. We use bounds on Fourier coefficients of modular forms of half-integral weight that lie in the the orthogonal complement (under the Petersson inner product) of the space spanned by one-dimensional theta series (due to Iwaniec and Duke) to conclude the proof of Theorem 1.1 and Theorem 1.2.

4.1 Optimal embeddings and primitive representations by ternary quadratic forms

Let $s \in X_0(N)^{\mathrm{SS}}_{/\mathbb{F}_{\ell^2}}$ and let $R_s := \mathrm{End}(s)$ be the ring of endomorphisms of s. Recall the notation $w_s := \#R_s^\times$ and $u_{D,c} := \#\mathcal{O}_{D,c}$.

1. A ternary quadratic form associated to an Eichler order. Let $V \subset R_s$ be the set of elements of trace zero. Following [Gro87, pp.171–172] define

$$G_s := (2R_s + \mathbb{Z}) \cap V.$$

The $\mathbb{Z}$-module G_s is free of rank 3. Define a quadratic form $Q_s : G_s \to \mathbb{Q}$ by

$$Q_s(b) := \mathrm{nr}(b).$$

2. Correspondence between optimal embeddings and primitive representations.

Let $f : \mathcal{O}_{D,c} \hookrightarrow R_s$ be an embedding (not necessarily optimal) and let $\beta := f(\sqrt{-d_c})$. Notice that $\mathrm{Tr}(\beta) = 0$ and $\mathrm{nr}(\beta) = d_c$. We claim that $\beta \in G_s$. Indeed, since $\mathcal{O}_{D,c} = \mathbb{Z} + \dfrac{d_c + \sqrt{-d_c}}{2}\mathbb{Z}$, it follows that $2f\left(\dfrac{d_c + \sqrt{-d_c}}{2}\right) = d_c + \beta$, i.e.,

$$\beta \equiv -d_c \mod 2R_s.$$

Therefore, $\beta \in (\mathbb{Z} + 2R_s) \cap V = G_s$, i.e., $Q_s(\beta) = d_c$ is a representation.

Conversely, suppose that $\beta \in G_s$ and $Q_s(\beta) = d_c$. We claim that $\beta \equiv -d_c \mod 2R_s$. Indeed, let $\beta = \gamma + 2r$ for some $\gamma \in \mathbb{Z}$ and $r \in R_s$. Then

$$d_c = Q_s(\beta) = \mathrm{nr}(\beta) = \beta\overline{\beta} = -\beta^2 = -(\gamma + 2r)^2 \equiv -\gamma^2 \mod 4R_s. \tag{3}$$

Thus,

$$\beta = \gamma + 2r \equiv (\gamma + \gamma^2) - \gamma^2 \equiv d_c \equiv -d_c \mod 2R_s.$$

Now, we can define an embedding $f : \mathcal{O}_{D,c} \hookrightarrow R_s$ by

$$f\left(\frac{d_c + \sqrt{-d_c}}{2}\right) := \frac{d_c + \beta}{2} \in R_s.$$

We next show under the established correspondence that optimal embeddings correspond to primitive representations.

Lemma 4.1. *The embedding f is optimal if and only if the representation $Q_s(\beta) = d_c$ is primitive.*

Proof. Suppose that the representation $Q_s(\beta) = d_c$ is non-primitive. We will show that f is not an optimal embedding. Indeed, let $\beta = k\alpha$ for some $k \in \mathbb{Z}$ and $\alpha \in G_s$. Then $\mathrm{nr}(\alpha) = \dfrac{d_c}{k^2}$. Let $d = \dfrac{d_c}{k^2}$. Consider the element $\gamma = \dfrac{d + \alpha}{2}$. We claim that $\gamma \in f(K_D) \cap R_s$, but $\gamma \notin f(\mathcal{O}_{D,c})$ which would imply that f is a non-optimal embedding. First, $\gamma = \dfrac{1}{k^2} f\left(\dfrac{d_c + \sqrt{d_c}}{2}\right) \in f(\mathcal{O}_{D,c}) \otimes \mathbb{Q}$. Let $\alpha = a + 2r$ for $a \in \mathbb{Z}$ and $r \in R_s$. Then $d = \mathrm{nr}(\alpha) = -\alpha^2 \equiv -a^2 \mod 2R_s$. Thus, $\alpha =$

$a + 2r \equiv -a^2 \equiv d \equiv -d \mod 2R_s$, i.e., $\gamma \in R_s$. Next, we show that $\gamma \notin f(\mathcal{O}_{D,c})$. If $k \neq 2$ then $\gamma = \dfrac{d+\alpha}{2} = \dfrac{d_c + \beta + dk - dk^2}{2k}$. Since $d_c + \beta = 2f(w) \notin kf(\mathcal{O}_{D,c})$ then $\gamma \notin f(\mathcal{O}_{D,c})$. If $k = 2$ then $\gamma = \dfrac{d_c + \beta - 2d}{4}$. Since $d_c + \beta - 2d = f(2w - 2d) \notin 4f(\mathcal{O}_{D,c})$ we obtain the same statement. Thus, $\gamma \in f(K_D) \cap R_s$, but $\gamma \notin f(\mathcal{O}_{D,c})$, i.e., the embedding is not optimal.

Conversely, suppose that $f : \mathcal{O}_{D,c} \hookrightarrow R_s$ is a non-optimal embedding. Let $\mathcal{O} = (f(\mathcal{O}_{D,c}) \otimes \mathbb{Q}) \cap R_s$. It follows that $\mathcal{O} \cong \mathcal{O}_{D,c'}$, where $c = kc'$ for some $k > 1$. Now, we can choose $\alpha \in (2\mathcal{O} + \mathbb{Z}) \cap V$, such that $Q_s(\alpha) = -Dc'^2$. Since $(\mathbb{Z} + 2\mathcal{O}) \cap V$ is a free $\mathbb{Z}$-module of rank 1, we obtain $\beta = k\alpha$, i.e., the representation $Q_s(\beta) = -Dc^2$ is not primitive. This proves the lemma. □

Thus, we have proved the following:

PROPOSITION 4.2. *There is a* $\dfrac{w_s}{u_{D,c}}$*-to-one correspondence between primitive representations of the integer* $d_c = -Dc^2$ *by* Q_s *and optimal embeddings* $f : \mathcal{O}_{D,c} \hookrightarrow R_s$.

4.2 The discriminant of Q_s

For what follows, we will need the discriminant of the quadratic form Q_s.

LEMMA 4.3. *The discriminant* D_{Q_s} *of the quadratic form* Q_s *is equal to* $4N^2\ell^2$.

Proof. Let $p \neq \ell$ be a prime and let $v_p(N) =: n$. Since R_s is an Eichler order of level N, we know that $R_s \otimes \mathbb{Z}_p$ is an Eichler order of level p^n of two-by-two matrices over $\mathbb{Z}_p$. In particular (up to conjugation) we have

$$R_s \otimes \mathbb{Z}_p = \begin{pmatrix} \mathbb{Z}_p & \mathbb{Z}_p \\ p^n\mathbb{Z}_p & \mathbb{Z}_p \end{pmatrix}.$$

Therefore,

$$G_s \otimes \mathbb{Z}_p = \left[2\begin{pmatrix} \mathbb{Z}_p & \mathbb{Z}_p \\ p^n\mathbb{Z}_p & \mathbb{Z}_p \end{pmatrix} + \mathbb{Z}_p\right] \cap V = \left\{\begin{pmatrix} a & 2b \\ 2p^n c & -a \end{pmatrix} : a, b, c \in \mathbb{Z}_p\right\}.$$

But then the local quadratic form $Q_{s,p} := Q_s \otimes \mathbb{Z}_p$ is given by

$$Q_{s,p}(a, b, c) = \begin{vmatrix} a & 2b \\ 2p^n c & -a \end{vmatrix} = -a^2 - 4p^n bc$$

The corresponding matrix for the quadratic form $Q_{s,p}$ is then

$$\begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & -2p^n \\ 0 & -2p^n & 0 \end{pmatrix}. \tag{4}$$

The determinant of this matrix is $-4p^{2n}$. Therefore, if $p \neq 2$ then 4 is a unit and the contribution to the determinant of Q_s is p^{2n}, while if $p = 2$ the contribution is $4p^{2n}$.

Now consider the case $p = \ell \neq 2$. In this case we have $R_s \otimes \mathbb{Z}_p$ is the unique maximal order of the unique division algebra, with $\mathbb{Z}_p$-basis $(1, \alpha, \beta, \gamma)$ satisfying $\alpha^2 = -p$, $\beta^2 = -1$ and $\gamma = \alpha\beta = -\beta\alpha$. But then $G_s \otimes \mathbb{Z}_p$ has basis $(2\alpha, 2\beta, 2\gamma)$. We obtain the quadratic form

$$Q_{s,p}(2a\alpha + 2b\beta + 2c\gamma) = 4pa^2 + 4b^2 + 4pc^2, \tag{5}$$

which is diagonal with discriminant $64p^2$, contributing p^2 to the discriminant.

For $p = \ell = 2$ we note that since the Eichler order is locally isomorphic to the (unique) maximal order, Gross [Gro87, p. 177] has shown that for $\alpha^2 = \beta^2 = \gamma^2 = -1$ with $\gamma = \alpha\beta = -\beta\alpha$,

$$G_s \otimes Z_p = \{a\alpha + (a + 2b)\beta + (a + 2c)\gamma : a, b, c \in \mathbb{Z}_p\}.$$

Thus the p-adic quadratic form is given by

$$Q_{s,p}(a,b,c) = -(3a^2 + 4ab + 4ac + 4b^2 + 4c^2),$$

with corresponding matrix

$$\begin{pmatrix} 3 & 2 & 2 \\ 2 & 4 & 0 \\ 2 & 0 & 4 \end{pmatrix} \tag{6}$$

The determinant of this matrix is 16, and hence contributes $16 = 4\ell^2$ to the discriminant. □

4.3 The theta series associated to Q_s

Consider the theta series

$$\theta_{Q_s} := \sum_{\beta \in G_s} q^{Q_s(\beta)} = \sum_{d \geqslant 1} a_s(d) q^d.$$

Since $-Q_s(\beta) \equiv 0, 1 \mod 4$, we obtain that $a_s(d) \neq 0$ only if $-d$ is a discriminant, i.e., $-d \equiv 0, 1 \mod 4$. Thus,

$$\theta_{Q_s} = \sum_{\beta \in G_s} q^{Q_s(\beta)} = \sum_{-d \equiv 0,1 \mod 4} a_s(d) q^d.$$

Recall the definition of Kohnen's plus space $M^+_{3/2}(\Gamma_0(4M))$ from section 3.

Lemma 4.4. *We have $\theta_{Q_s} \in M^+_{3/2}(\Gamma_0(4N\ell))$.*

Proof. Let A be the matrix corresponding to Q_s. It is well known that $\theta_{Q_s} \in M^+_{3/2}(\Gamma_0(4M))$, where M is the minimal positive integer, such that $4MA^{-1}$ has coefficients that are even integers (see [Duk05, p. 39]). Since A^{-1} has rational coefficients, it suffices to check that each coefficient of $4MA^{-1}$ has non-negative p-adic valuation for each p. We then explicitly compute the inverse of equations (4), (5) and (6) to check that it has even integral coefficients when we multiply by $4p^{v_p(N\ell)}$. □

4.4 The theta series associated to the genus and the spinor genus of Q_s

Let Q be a ternary quadratic form. Let $\mathrm{gen}(Q)$ be the genus of Q and let $\mathrm{spn}(Q)$ be the spinor genus of Q (see [O'M00, Ch.X] for the definitions). Let $\mathrm{loc}(Q)$ be the set of all integers n that are everywhere locally represented by Q. Let $r_Q(n)$ (resp. $r^*_Q(n)$) be the number of representations (resp. primitive representations) of n by Q. Let w_Q be the number of automorphs of Q (see [Jon50] for the definition).

1. Theta series associated to $\mathrm{gen}(Q)$. Let

$$r(\mathrm{gen}(Q), n) := \frac{\sum_{Q' \in \mathrm{gen}(Q)} r_{Q'}(n)/w_{Q'}}{\sum_{Q' \in \mathrm{gen}(Q)} 1/w_{Q'}}. \tag{7}$$

Similarly, define

$$r^*(\mathrm{gen}(Q), n) := \frac{\sum_{Q' \in \mathrm{gen}(Q)} r^*_{Q'}(n)/w_{Q'}}{\sum_{Q' \in \mathrm{gen}(Q)} 1/w_{Q'}}.$$

We define the theta series associated to $\mathrm{gen}(Q)$ as

$$\theta_{\mathrm{gen}(Q)} := \sum_{n \geqslant 1} r(\mathrm{gen}(Q), n) q^n.$$

By calculating local densities, Jones [Jon50, Thm.86] has shown that for $d_c = -Dc^2$

$$r^*(\mathrm{gen}(Q_s), d_c) = C\frac{h(-\Delta d_c)}{u_{\Delta D,c}}. \tag{8}$$

Here, Δ denotes the discriminant D_{Q_s} of Q_s divided by the square of the greatest common divisor of the determinants of all two-by-two minors of the matrix corresponding to Q_s, and C only depends on the Legendre symbol $\left(\frac{d_c}{D_{Q_s}}\right)$. One can calculate Δ p-adically using equations (4), (5), and (6) to show that the greatest common divisor of the determinants of all two-by-two minors is precisely $\sqrt{D_{Q_s}}$. Thus, $\Delta = 1$.

2. Theta series associated to $\mathrm{spn}(Q)$. We define the theta series associated to the spinor genus in a similar way. First, let

$$r(\mathrm{spn}(Q), n) := \frac{\sum_{Q' \in \mathrm{spn}(Q)} r_{Q'}(n)/w_{Q'}}{\sum_{Q' \in \mathrm{spn}(Q)} 1/w_{Q'}}. \tag{9}$$

Similarly, let

$$r^*(\mathrm{spn}(Q), n) := \frac{\sum_{Q' \in \mathrm{spn}(Q)} r^*_{Q'}(n)/w_{Q'}}{\sum_{Q' \in \mathrm{spn}(Q)} 1/w_{Q'}}.$$

We also define

$$\theta_{\mathrm{spn}(Q)} := \sum_{n \geqslant 1} r(\mathrm{spn}(Q), n) q^n.$$

The theta series $\theta_{\mathrm{gen}(Q)}$ and $\theta_{\mathrm{spn}(Q)}$ are in the same space as θ_Q (by (7) and (9) and the fact that $\theta_{Q'}$ are in the same space as Q for all $Q' \in \mathrm{gen}(Q)$; see also [Han04a, p.366]).

4.5 Equidistribution in terms of quadratic forms

In light of the correspondence obtained in Proposition 4.2, the required equidistribution results (Theorem 1.1 and Theorem 1.2) are equivalent to showing that

$$\lim_{\substack{(D,c) \in \Omega_N \\ d_c \to \infty}} \frac{r^*(Q_s, d_c) u_{D,c}}{2^{\nu(N)} \# \Gamma_{D,c}} = w_s \mu_{\mathrm{can}}(s). \tag{10}$$

This result will be equivalent to showing that the limit

$$f(s) := \lim_{\substack{(D,c) \in \Omega_N \\ d_c \to \infty}} \frac{r^*(Q_s, d_c) u_{D,c}}{\# \Gamma_{D,c}} \tag{11}$$

exists and is independent of the supersingular point s. Here, recall that $d_c := -Dc^2$.

First, note that $\theta_{Q_s} - \theta_{\mathrm{spn}(Q_s)}$ is a modular form of weight $3/2$ that lies in the orthogonal complement of the space of one-dimensional theta series under the Petersson inner product [SP84]. Duke's bound for the Fourier coefficients of such forms [Duk98], extending the work of Iwaniec [Iwa87] to forms of weight $3/2$, combined with Möbius inversion, implies that

$$r^*(\mathrm{spn}(Q_s), d_c) - r^*(Q_s, d_c) = O(d_c^{\frac{13}{28}+\epsilon}).$$

Siegel's lower bound for the class number [Sie35] (see also [Cox89, p. 149]) implies that $\# \Gamma_{D,c} \gg d_c^{\frac{1}{2}-\epsilon}$, so

$$\frac{r^*(Q_s, d_c) u_{D,c}}{\# \Gamma_{D,c}} = \frac{r^*(\mathrm{spn}(Q_s), d_c) u_{D,c}}{\# \Gamma_{D,c}} + O(d_c^{-\frac{1}{28}+\epsilon}) \tag{12}$$

Thus, we only need to show independence and convergence of the limit for each spinor genus.

Since $r^*(\mathrm{gen}(Q_s), n)$ is independent of s by definition, it will be natural to compare $r^*(\mathrm{gen}(Q_s), n)$ with $r^*(\mathrm{spn}(Q_s), n)$ in order to determine the desired independence.

In particular, we have the following.

Lemma 4.5. *The limit*

$$\lim_{k\to\infty} \frac{r^*(\mathrm{gen}(Q_s), -Dp^{2k})u_{D,p^k}}{\#\Gamma_{D,p^k}}$$

exists and is independent of p and s.

Proof. The independence on s is clear from the definition of $\mathrm{gen}(Q_s)$. We will apply (8) to $n = -Dp^{2k}$. First, recall (see [Cox89, Cor.7.28, p.148]) that for any discriminant $D_0 < 0$ and any prime p we have

$$h(-D_0p^{2k}) = Cp^k\left(1 - \frac{1}{p}\left(\frac{-D_0}{p}\right)\right)\cdot\frac{u_{D_0,p^k}}{u_{D_0,1}}h(-D_0) \tag{13}$$

Equation (13) with $D_0 = D$ allows us to express $r^*(\mathrm{gen}(Q_s), -Dp^{2k})$ and $\#\Gamma_{D,p^k}$ as

$$r^*(\mathrm{gen}(Q_s), -Dp^{2k}) = \frac{c_Dh(-Dp^{2k})}{u_{D,p^k}} = c_dCp^k\left(1 - \frac{1}{p}\left(\frac{-D}{p}\right)\right)\frac{h(-D)}{u_{D,1}}, \tag{14}$$

$$\frac{\#\Gamma_{D,p^k}}{u_{D,p^k}} = p^k\left(1 - \frac{1}{p}\left(\frac{-D}{p}\right)\right)\frac{\#\Gamma_{D,1}}{u_{D,1}}. \tag{15}$$

Hence, for $k \geqslant 1$ we obtain

$$\frac{r^*(\mathrm{gen}(Q_s), -Dp^{2k})u_{D,p^k}}{\#\Gamma_{D,p^k}} = c_DC\frac{h(-D)}{\#\Gamma_{D,1}}. \tag{16}$$

The result follows since the right-hand side of (16) is independent of k and p. □

We now define the restricted limit

$$f_{D,p}(s) := \lim_{k\to\infty}\frac{r^*(Q_s, -Dp^{2k})u_{D,p^k}}{\#\Gamma_{D,p^k}} = \lim_{k\to\infty}\frac{r^*(\mathrm{spn}(Q_s), -Dp^{2k})u_{D,p^k}}{\#\Gamma_{D,p^k}}. \tag{17}$$

The equidistribution result of Vatsal [Vat02, Thm.1.5] combined with Proposition 4.2 states the following:

Lemma 4.6. *[Vatsal] For every $s \in X_0(N)^{\mathrm{SS}}_{/\mathbb{F}_{\ell^2}}$, fundamental discriminant $D < 0$ and $p \nmid N\ell$ we have*

$$f_{D,p}(s) = w_s\mu_{\mathrm{can}}(s). \tag{18}$$

We will now use equation (18) to rewrite $r^*(\mathrm{spn}(Q_s), n)$ in terms of $r^*(\mathrm{gen}(Q_s), n)$ and then use equation (12) to show that $f(s)$ exists and is independent of s.

Proposition 4.7. *Let $s \in X_0(N)^{\mathrm{SS}}_{/\mathbb{F}_{\ell^2}}$ and $n = -Dc^2$, where $D < 0$ is a fundamental discriminant. Assume that $(c, N\ell) = 1$. Then*

$$r^*(\mathrm{gen}(Q_s), n) = r^*(\mathrm{spn}(Q_s), n).$$

Let $a_m := r(\mathrm{gen}(Q_s), m) - r(\mathrm{spn}(Q_s), m)$. According to a result of Schulze-Pillot [SP84] as well as Flicker [Fli80], Niwa [Niw74], Cipra and others [Cip83]), $\theta_{\mathrm{gen}(Q_s)} - \theta_{\mathrm{spn}(Q_s)}$ belongs to the subspace of cuspidal forms of weight 3/2 spanned by the one-dimensional theta series (see also [Han04b]). Note that the Fourier coefficients of the one-dimensional theta series $h_{\psi,t}(z)$ defined in equation (1) vanish outside the square class $t\mathbb{Z}^2$. Let

$$\theta_{\mathrm{gen}(Q_s)} - \theta_{\mathrm{spn}(Q_s)} = \sum_{\psi,t} c_{\psi,t}h_{\psi,t}. \tag{19}$$

Let $h_{\psi,t}$ be one of the one-dimensional theta series in (19) and let $4M = 4N\ell$ be the level of $\theta_{\mathrm{gen}(Q_s)} - \theta_{\mathrm{spn}(Q_s)}$. The transformation law for modular forms of level $4M$ with Nebentypus χ implies that $\psi(mn) = \psi(n)\chi_t(m)$ for every $(m, M) = 1$, where $\chi_t(m) = \chi(m)\left(\frac{-t}{m}\right)$ (see [SP84, p.285]). In addition, if $h_{\psi,t} \neq 0$ then $4t \mid M$ (see, e.g., [SP84, Kor.2]).

LEMMA 4.8. *Let $-d > 0$ be the smallest positive integer satisfying the following two conditions:*

i) *If $d = Dc^2$, where $D < 0$ is a fundamental discriminant then c is prime to $N\ell$;*

ii) *$a_{-d} \neq 0$.*

Then $c = 1$ and $d = D$ is a fundamental discriminant.

Proof. It follows from (19) and Lemma 4.4 (since $(m, M) = 1$) that $\psi(m) = \chi_t(m)$. Hence,

$$a_{-d} = \sum_{-d=tm^2,\psi} c_{\psi,t}\psi(m)m = \sum_{-d=tm^2} \chi_t(m)m \sum_{\psi} c_{\psi,t} \neq 0.$$

Hence there exists t satisfying $\sum_{\psi} c_{\psi,t} \neq 0$. Choose the minimal t with this property and observe that $a_t = \sum_{t',t=t'm^2} \sum_{\psi} c_{\psi,t'}\psi(m)m = \sum_{\psi} c_{\psi,t} \neq 0$. Hence, $t = -d$ and

$$a_{-d} = \sum_{-d=tm^2,\psi} c_{\psi,t}h_{\psi,t} = \sum_{\psi} c_{\psi,-d}h_{\psi,-d} \neq 0.$$

Now, if the conductor c of d were not equal to 1, it would have divided M and hence would not have been prime to $N\ell$. Thus, the only possibility is that $c = 1$ and $d = D$ is a fundamental discriminant. □

LEMMA 4.9. *Let $D < 0$ be the fundamental discriminant from Lemma 4.8 and $(c, N\ell) = 1$. If D_{Q_s} is the discriminant of the quadratic form Q_s then*

$$a_{-Dc^2} = c\left(\frac{DD_{Q_s}}{c}\right)a_{-D}.$$

In particular, for $c = p^k$ we have

$$a_{-Dp^{2k}} = p^k\left(\frac{-DD_{Q_s}}{p}\right)^k a_{-D}.$$

Proof. Note that $a_{-Dc^2} = \sum_{-Dc^2=tm^2,\psi} c_{\psi,t}\psi(m)m$. We know that if $t = -D(c')^2$ for some $c' > 1$ then $h_{t,\psi} = 0$ (since $(c', M) = 1$). Hence,

$$a_{-Dc^2} = \sum_{\psi} c_{\psi,D}\psi(c)c = c\chi_D(c)\sum_{\psi} c_{\psi,D} = c\left(\frac{DD_{Q_s}}{c}\right)a_{-D}.$$

□

Proof of Proposition 4.7. We will prove the statement by contradiction. Assume the contrary and let n be the smallest integer whose square part is prime to $N\ell$ and such that $r(\mathrm{gen}(Q_s), n) \neq r(\mathrm{spn}(Q_s), n)$. Lemma 4.8 implies that if $-n = Dc^2$ for a fundamental discriminant D and a conductor c then $c = 1$ and $n = -D$. Let $p \nmid N\ell$ be a prime for which $\left(\frac{DD_{Q_s}}{p}\right) = -1$. We will show that under these assumptions the limit $f_{-D,p}(s)$ does not exist, contradicting Lemma 4.6. Using Lemma

4.9 and equation (15), we have

$$\begin{aligned} f_{-D,p}(s) &= \lim_{k\to\infty}\left(\frac{\left(r^*(\mathrm{spn}(Q_s),-Dp^{2k})-r^*(\mathrm{gen}(Q_s),-Dp^{2k})\right)u_{D,p^k}}{\#\Gamma_{D,p^k}}+\frac{r^*(\mathrm{gen}(Q_s),-Dp^{2k})u_{D,p^k}}{\#\Gamma_{D,p^k}}\right)\\ &= \lim_{k\to\infty}\left(-\frac{a_{-Dp^{2k}}}{\#\Gamma_{D,p^k}/u_{D,p^k}}+\frac{r^*(\mathrm{gen}(Q_s),-Dp^{2k})u_{D,p^k}}{\#\Gamma_{D,p^k}}\right)\\ &= \lim_{k\to\infty}\left(-\frac{a_{-D}p^k\left(\frac{DD_{Q_s}}{p}\right)^k}{p^k\left(1-\frac{1}{p}\left(\frac{D}{p}\right)\right)\#\Gamma_{D,1}/u_{D,1}}+\frac{r^*(\mathrm{gen}(Q_s),-Dp^{2k})u_{D,p^k}}{\#\Gamma_{D,p^k}}\right)\\ &= \lim_{k\to\infty}\left(-\frac{a_{-D}(-1)^k}{\left(1-\frac{1}{p}\left(\frac{D}{p}\right)\right)\#\Gamma_{D,1}/u_{D,1}}+\frac{r^*(\mathrm{gen}(Q_s),-Dp^{2k})u_{D,p^k}}{\#\Gamma_{D,p^k}}\right). \end{aligned}$$

However, the limit

$$\lim_{k\to\infty}\frac{r^*(\mathrm{gen}(Q_s),-Dp^{2k})u_{D,p^k}}{\#\Gamma_{D,p^k}}$$

exists by Lemma 4.5. Therefore, if the limit $f_{-D,p}(s)$ exists, then the limit

$$\lim_{k\to\infty}-\frac{a_{-D}(-1)^k}{\left(1-\frac{1}{p}\left(\frac{D}{p}\right)\right)\#\Gamma_{D,1}/u_{D,1}}$$

must also exist. But $a_{-D}\neq 0$ and the only dependence on k is the term $(-1)^k$, leading to a contradiction. □

4.6 Proof of the main theorem

We are now ready to prove Theorem 1.1 and Theorem 1.2. Let $D<0$ be a fundamental discriminant and let c be an integer with $(c,N\ell)=1$. Define

$$g_{D,c}(s):=\frac{r^*(Q_s,-Dc^2)u_{D,c}}{\#\Gamma_{D,c}}$$

and

$$h_{D,c}:=\frac{r^*(\mathrm{gen}(Q_s),-Dc^2)u_{D,c}}{\#\Gamma_{D,c}}.$$

Note that $h_{D,c}$ is independent of s. Proposition 4.7 combined with equation (12) gives

$$g_{D,c}(s)=h_{D,c}+O_s\left((-Dc^2)^{-\frac{1}{28}+\epsilon}\right).$$

We now divide by w_s and sum over all $s'\in X_0(N)^{\mathrm{SS}}_{/\mathbb{F}_{\ell^2}}$. Recall from Proposition 4.2 that

$$\frac{g_{D,c}(s')\#\Gamma_{D,c}}{w_{s'}}=r^*(Q_{s',-Dc^2})\frac{u_{D,c}}{w_{s'}}$$

is the number of optimal embeddings of $\mathcal{O}_{D,c}$ into $R_{s'}$. Summing over all $s'\in X_0(N)^{\mathrm{SS}}_{/\mathbb{F}_{\ell^2}}$ thus gives $\#\Gamma_{D,c}$. Hence, we have

$$1=\sum_{s'\in X_0(N)^{\mathrm{SS}}_{/\mathbb{F}_{\ell^2}}}\frac{g_{D,c}(s')}{w_{s'}}=h_{D,c}\sum_{s'\in X_0(N)^{\mathrm{SS}}_{/\mathbb{F}_{\ell^2}}}\frac{1}{w_{s'}}+O\left((-Dc^2)^{-\frac{1}{28}+\epsilon}\right). \tag{20}$$

Therefore

$$h_{D,c} = \frac{1}{\sum_{s' \in X_0(N)^{\mathrm{SS}}_{/\mathbb{F}_{\ell^2}}} 1/w_{s'}} + O\left((-Dc^2)^{-\frac{1}{28}+\epsilon}\right).$$

Thus the limit $\lim_{-Dc^2 \to \infty} h_{D,c}$ exists, and we obtain

$$f(s) = \lim_{-Dc^2\to\infty} g_{D,c}(s) = \lim_{-Dc^2\to\infty} \left[h_{D,c}(s) + O\left((Dc^2)^{-\frac{1}{28}+\epsilon}\right)\right] = \frac{1}{\sum_{s' \in X_0(N)^{\mathrm{SS}}_{/\mathbb{F}_{\ell^2}}}} = w_s \mu_{\mathrm{can}}(s).$$

But this is precisely equation (10), and hence we obtain Theorem 1.1.

Remark 8. Due to dependence on Siegel's lower bound for the class number, Theorem 1.1 is ineffective. However, if we fix a fundamental discriminant $D < 0$ and only vary the conductor c, then this result becomes effective due to known growth of the class number in a fixed square class. Moreover, in a fixed square class the $-D$-th Shimura correspondence implies that the difference

$$a_c(s) := g_{D,c}(s) - h_{D,c}$$

are coefficients of a weight 2 cusp form. Using Deligne's optimal bound, the error term can be improved to $O(c^{-1/2+\epsilon})$. Therefore, the error can be written as

$$O((-D)^{-\frac{1}{28}+\epsilon} c^{-\frac{1}{2}+\epsilon}).$$

5. Distribution relations method

In this section, we establish equidistribution when the fundamental discriminant $D < 0$ is fixed and the conductor varies using an alternative argument based on the distribution relations for Heegner points and Hecke eigenvalue bounds.

5.1 An easier equidistribution theorem

Here, we only consider a special infinite set of conductors c and a fixed fundamental discriminant $D < 0$. Let $\mathcal{P}$ be the set of all primes $r \nmid N$, such that r is inert in K. Let $\mathcal{I}$ be the set of all integers that are square-free products of primes in $\mathcal{P}$. Note that $\Lambda \subset \mathcal{I}$. Under the same hypothesis as before, we will prove the following statement:

THEOREM 5.1. *Given a Galois orbit $\Gamma_{D,c}$ let $\mu_{D,c}$ be the measure on $X_0(N)^{\mathrm{SS}}_{/\mathbb{F}_{\ell^2}}$ defined as in Theorem 1.1. Then $\lim_{\substack{c\to\infty,\\ c\in\mathcal{I}}} \mu_{D,c} = \mu_{\mathrm{can}}$.*

Remark 9. The assumption that $c \in \mathcal{I}$ is not necessary and the argument in the more general case is exactly the same, except for the more technical form of the distribution relations. Here, we prove only the less technical statement where the distribution relations are easier to work with (see Section 5.2).

5.2 Distribution relations

Let $X_c \in \mathrm{Div}(X_0(N))$ be defined as $X_c := \sum_{\sigma \in \mathrm{Gal}(K[c]/K)} (x_c^\sigma)$. We will prove the following distribution relation:

LEMMA 5.2. *For any prime number ℓ which is inert in K and any positive integer c coprime to ℓ, the following distribution relation holds:*

$$X_{c\ell} = T_\ell X_c.$$

Proof. Let S be a set of coset representatives for $\mathrm{Gal}(K[c\ell]/K[c])/\mathrm{Gal}(K[c]/K)$. The distribution relation for Heegner points [Gro84, §6] is the following equality of divisors of degree $\ell+1$ on $X_0(N)$:

$$\mathrm{Tr}_{K[\ell c]/K[c]}(x_{c\ell}^{\sigma}) = T_\ell(x_c^{\sigma}),\ \sigma \in \mathrm{Gal}(K[c\ell]/K),$$

i.e.,

$$\sum_{\tau\in\mathrm{Gal}(K[c\ell]/K[c])} (x_{c\ell}^{\sigma\tau}) = T_\ell(x_c^{\sigma}),\ \sigma \in \mathrm{Gal}(K[c\ell]/K).$$

Hence,

$$\sum_{\sigma\in S}\sum_{\tau\in\mathrm{Gal}(K[c\ell]/K[c])} (x_{c\ell}^{\sigma\tau}) = \sum_{\sigma\in S} T_\ell(x_c^{\sigma}),\ \sigma \in \mathrm{Gal}(K[c\ell]/K),$$

which implies

$$X_{c\ell} = T_\ell X_c.$$

□

5.3 Proof of the main theorem

Proof of Theorem 5.1. First, we note that the reduction map $\mathrm{red}_\ell : X_0(N)_{/\mathbb{Q}} \to X_0(N)_{/\mathbb{F}_\ell}$ defined in Section 1 is Hecke equivariant. Thus,

$$\mathrm{red}_\ell(X_{cr}) = T_r\,\mathrm{red}_\ell(X_c).$$

Next, $\mathrm{red}_\ell(X_{cr})$ and $\mathrm{red}_\ell(X_c)$ belong to the subgroup $\mathrm{Div}^{\mathrm{SS}}(X_0(N)_{/\overline{\mathbb{F}}_\ell})$ of divisors supported on the supersingular points of $X_0(N)_{/\overline{\mathbb{F}}_\ell}$. The Hecke algebra $\mathbb{T}_{N\ell}$ acts on the vector space $V_{\mathrm{SS}} = \mathrm{Div}^{\mathrm{SS}}(X_0(N)_{/\overline{\mathbb{F}}_\ell}) \otimes \overline{\mathbb{Q}}$ via its ℓ-new quotient $\mathbb{T}_{N\ell}^{\ell-\mathrm{new}}$ (see [Ser96] or [Par03]). Let

$$V_{\mathrm{SS}} = V_{\mathrm{Eis}} \oplus \left(\bigoplus_f V_f\right)$$

be the eigenspace decomposition of V, where f ranges over all normalized eigenforms $f \in S_2^{\ell-\mathrm{new}}(\Gamma_0(N\ell))$,

$$V_f = \{v \in V_{\mathrm{SS}}\ :\ T_r v = a_r(f)v \text{ for all primes } r\},$$

and

$$V_{\mathrm{Eis}} = \{v \in V_{\mathrm{SS}}\ :\ T_r v = (r+1)v \text{ for all primes } r\}.$$

Here, $a_r(f)$ denotes the r-th Fourier coefficient of the eigenform f.

Let $Y_c = \dfrac{1}{\#\,\mathrm{Pic}(\mathcal{O}_c)}\,\mathrm{red}_\ell(X_c) \in V_{\mathrm{SS}}$. It is easy to see that $Y_c = \displaystyle\sum_{s\in X_0(N)^{\mathrm{SS}}_{/\mathbb{F}_{\ell^2}}} \mu_c(s)\cdot(s)$. We can write the decomposition of Y_c as

$$Y_c = Y_{c,\mathrm{Eis}} + \sum_f Y_{c,f},\ Y_{c,f} \in V_f,\ Y_{c,\mathrm{Eis}} \in V_{\mathrm{Eis}}.$$

The distribution relation from Lemma 5.2 implies that $\#\,\mathrm{Pic}(\mathcal{O}_{cr})Y_{cr} = \#\,\mathrm{Pic}(\mathcal{O}_c)T_rY_c$. Since $\#\,\mathrm{Pic}(\mathcal{O}_{cr}) = (r+1)\#\,\mathrm{Pic}(\mathcal{O}_c)$ then

$$Y_{cr} = \frac{1}{r+1}T_rY_c.$$

We use this equality to obtain $Y_{cr,\mathrm{Eis}} = Y_{c,\mathrm{Eis}}$ and $Y_{cr,f} = \dfrac{a_r(f)}{r+1}Y_{c,f}$ for any normalized eigenform $f \in S_2^{\ell-\mathrm{new}}(\Gamma_0(N\ell))$.

The Ramanujan-Petersson conjecture then implies that

$$\frac{a_r(f)}{r+1} \leqslant \frac{2r^{1/2}}{r+1} \leqslant \frac{2}{r^{1/2}}.$$

Thus, we obtain by induction on the number of prime divisors of c that

$$Y_c = Y_{1,\mathrm{Eis}} + O(c^{-1/2}).$$

This means that $\lim_{\substack{c\to\infty,\\ c\in\mathcal{I}}} Y_c = Y_{1,\mathrm{Eis}}$.

Finally, one uses the result from Section 5.4 to conclude that $Y_{1,\mathrm{Eis}}$ is equal to the divisor associated to the canonical measure μ_{can}. □

5.4 The divisor $Y_{1,\mathrm{Eis}}$

Let

$$D_{\mu_{\mathrm{can}}} := \sum_{s\in X_0(N)^{\mathrm{SS}}_{/\mathbb{F}_{\ell^2}}} \mu_{\mathrm{can}}(s)\cdot(s) \in V_{\mathrm{SS}}.$$

It is well-known (see, e.g., [Vat02, Lem.2.5]) that the divisor $D_{\mu_{\mathrm{can}}}$ is Eisenstein. In other words,

$$T_r D_{\mu_{\mathrm{can}}} = (r+1) D_{\mu_{\mathrm{can}}}$$

for every prime $(r, N) = 1$. Next, we verify that $D_{\mu_{\mathrm{can}}}$ is the same as the Eisenstein part $Y_{1,\mathrm{Eis}}$ of Y_1:

Lemma 5.3. *We have*

$$D_{\mu_{\mathrm{can}}} = Y_{1,\mathrm{Eis}}.$$

Proof. First, note that $\deg(D_{\mu_{\mathrm{can}}}) = 1 = \deg(Y_1)$. Furthermore, a divisor $D \in \mathrm{Div}(X_0(N)^{\mathrm{SS}}_{/\mathbb{F}_{\ell^2}}) \otimes \overline{\mathbb{Q}}$ is cuspidal if and only if it has degree zero (see e.g., [Ser96]). Thus, $\deg(Y_{1,\mathrm{cusp}}) = 0$ and hence, $\deg(Y_{1,\mathrm{Eis}}) = 1$.

Next, consider the exact sequence

$$0 \to \mathrm{Div}^0(X_0(N)^{\mathrm{SS}}) \to \mathrm{Div}(X_0(N)^{\mathrm{SS}}_{/\mathbb{F}_{\ell^2}}) \xrightarrow{\deg} \mathbb{Z} \to 0,$$

and look at the divisor $D = D_{\mu_{\mathrm{can}}} - Y_{1,\mathrm{Eis}}$. We know that $\deg(D) = 0$ and hence, D is cuspidal. At the same time, D is Eisenstein. If $D \neq 0$ then one would obtain a contradiction by using the Hecke eigenvalue bounds for cusp forms. Thus, $D = 0$ and hence, $Y_{1,\mathrm{Eis}} = D_{\mu_{\mathrm{can}}}$. □

6. Effective surjectivity results

We have seen in Theorem 1.1 that $\mu_{D,c} \to \mu_{\mathrm{can}}$ as $d_c := -Dc^2 \to \infty$. In particular, for sufficiently large d_c we have $\mu_{D,c}(s) > 0$ for every $s \in X_0(N)^{\mathrm{SS}}_{/\mathbb{F}_{\ell^2}}$, giving surjectivity of the reduction red_ℓ from $\Gamma_{D,c}$ to $X_0(N)^{\mathrm{SS}}_{/\mathbb{F}_{\ell^2}}$. Here, we discuss effective versions of this surjectivity result.

Recall that the proof of Theorem 1.1 uses Siegel's lower bound on the class number (see (12)). Since Siegel's bound $\#\Gamma_{D,c} \gg_{c,\varepsilon} D^{\frac{1}{2}-\varepsilon}$ is ineffective due to the fact that Siegel proved this result by first assuming the truth of GRH for Dirichlet L-functions and then proved the bound again with a different implied constant depending on the location of a possible Siegel zero [Sie35]. The best known effective results are due to Oesterlé [Oes85], but the growth obtained is only logarithmic in D. Hence, the surjectivity will be ineffective whenever we allow the fundamental discriminant to vary.

Thus, we fix a fundamental discriminant $D < 0$. Given a supersingular point $s \in X_0(N)^{\mathrm{SS}}_{/\mathbb{F}_{\ell^2}}$, decompose θ_{Q_s} as

$$\theta_{Q_s} - \theta_{\mathrm{spn}(Q_s)} = \sum_{i=1}^{r} b_i g_i, \tag{21}$$

where $b_i \in \mathbb{C}$ and $\{g_1, \dots, g_r\}$ is a fixed set of cuspidal Hecke eigenforms in the orthogonal complement (under the Petersson inner product) of the space spanned by one-dimensional theta series of weight $3/2$. We will denote the d-th coefficient of g_i by $a_{g_i}(d)$ and the $-D$-th Shimura correspondence (recall the extended definition in Section 3 given by Kohnen for fundamental discriminants) by $G_i := S_{-D,1}(g_i)$. Denote the number of distinct prime divisors of c by $v(c)$.

The following theorem establishes an effective bound for c (depending on the decomposition (21) and the fundamental discriminant $-D$) beyond which the preimage $\mathrm{red}_\ell^{-1}(s)$ is non-empty. Taking the maximum occurring bound over all $s' \in X_0(N)^{\mathrm{SS}}_{/\mathbb{F}_{\ell^2}}$ gives a bound depending only on N, ℓ and D beyond which surjectivity must hold.

Theorem 6.1. *Let $c > 2$ be an integer prime to $N\ell$ that satisfies the following inequality*

$$\frac{c^{1/2}}{2^{2v(c)+1}\sigma_0(c)\log c} > \frac{1}{\log 2}\frac{u_{D,1}}{\#\Gamma_{D,1}}\left(\sum_{i=1}^{r}|b_i a_{g_i}(-D)|\right)\left(\sum_{s'\in X_0(N)^{\mathrm{SS}}_{/\mathbb{F}_{\ell^2}}} 1/w_{s'}\right)$$

Then the reduction map $\mathrm{red}_\ell : \Gamma_{D,c} \to X_0(N)^{\mathrm{SS}}_{/\mathbb{F}_{\ell^2}}$ satisfies $\mathrm{red}_\ell^{-1}(s) \neq \varnothing$.

Proof. For the θ-series θ_{Q_s} we have the decomposition

$$\theta_{Q_s}(z) = E(z) + H(z) + f(z),$$

where $E(z)$ is an Eisenstein series, $H(z)$ is in the space spanned by one-dimensional theta series of weight $3/2$, and $f(z)$ is a cusp form in the orthogonal complement of the space spanned by one-dimensional theta series (see [Han04b, p.156]). Moreover, from the work of Schulze-Pillot [SP84], we know that $E(z) = \theta_{\mathrm{gen}(Q_s)}(z)$ and $H(z) = \theta_{\mathrm{spn}(Q_s)}(z) - \theta_{\mathrm{gen}(Q_s)}(z)$.

Let $a(n) := r(Q_s, n) - r(\mathrm{spn}(Q_s), n)$ be the nth Fourier coefficient of the form $f(z)$ and let $a^*(n) := r^*(Q_s, n) - r^*(\mathrm{spn}(Q_s), n)$. Let $n > 0$ be an integer satisfying $(n, N\ell) = 1$. We know by Proposition 4.7 that $r(\mathrm{gen}(Q_s), n) = r(\mathrm{spn}(Q_s), n)$. Therefore,

$$r(Q_s, n) = r(\mathrm{gen}(Q_s), n) + (r(Q_s, n) - r(\mathrm{gen}(Q_s), n)) = r(\mathrm{gen}(Q_s), n) + a(n).$$

Next, if $n = tc^2$ where t is square-free, Möbius inversion gives us

$$r^*(Q_s, n) = \sum_{c'|c}\mu(c')r(Q_s, n/c'^2) = r^*(\mathrm{gen}(Q_s), n) + \sum_{c'|c}\mu(c')a(n/c'^2). \tag{22}$$

By Proposition 4.2, we know that $s \in X_0(N)^{\mathrm{SS}}_{/\mathbb{F}_{\ell^2}}$ is in the image of $\mathrm{red}_\ell : \Gamma_{D,c} \to X_0(N)^{\mathrm{SS}}_{/\mathbb{F}_{\ell^2}}$ if and only if Q_s primitively represents $d_c = -Dc^2$. Thus, s is not in the image of the reduction map if and only if $r^*(Q_s, d_c) = 0$, i.e., if and only if

$$r^*(\mathrm{gen}(Q_s), d_c) = -\sum_{c'|c}\mu(c')a(d_c/c'^2). \tag{23}$$

The left-hand side can be computed using Jones' formula and [Cox89, Cor.7.28,p.148] as it was applied previously for (14). We obtain

$$r^*(\mathrm{gen}(Q_s), d_c)\sum_{s'\in X_0(N)^{\mathrm{SS}}_{/\mathbb{F}_{\ell^2}}} 1/w_{s'} = \frac{\#\Gamma_{D,c}}{u_{D,c}} = \left(\sum_{c'|c}\mu(c')\left(\frac{D}{c'}\right)\frac{c}{c'}\right)\frac{\#\Gamma_{D,1}}{u_{D,1}}. \tag{24}$$

For the right-hand side of (23), we would like to express the Fourier coefficient $a(d_c)$ in terms of $a(-D)$. This cannot be done directly for an arbitrary cusp form f in the orthogonal complement of the space of one-dimensional theta series, but could be achieved if f were an eigenform (due to the recurrence relations of the Hecke operators). In order to get such a relation, we write

$$f(z) = \sum_{i=1}^{r} b_i g_i(z),$$

where g_i's are Hecke eigenforms of weight $3/2$ whose images G_i under the $-D$-th Shimura correspondence $S_{-D,1}$ are normalized Hecke eigenforms.

Decomposing $\theta_{Q_s} - \theta_{\mathrm{gen}(Q_s)}$ gives

$$a^*(d_c) = \sum_{i=1}^{r} b_i \sum_{c'|c} \mu(c') a_{g_i}\left(d_{c/c'}\right). \tag{25}$$

If $g := g_i$ is a Hecke eigenform, the $-D$-th Shimura correspondence $G := S_{-D,1}(g) \in S_2(\Gamma_0(N\ell))$ is also a Hecke eigenform. Assume further that G is normalized so that $a_G(1) = 1$. By the multiplicity one theorem for forms of weight 2, there exists a newform $\widetilde{G} \in S_2(\Gamma_0(M))$ for some $M \mid N\ell$ such that $G = \sum_{d|\frac{N\ell}{M}} C_d \widetilde{G}|V(d)$ for some constants C_d (with $C_1 = 1$). Here, the operator $V(d)$ corresponds to one of the degeneracy maps (see e.g., [Ono04, p.28] for the definition). Notice that for $(c, N\ell) = 1$, the cth coefficient of G corresponds to the cth coefficient of the newform $\widetilde{G}$. Since c is relatively prime to the level, the c-th coefficient of $\widetilde{G}$ is determined by the eigenvalues under the Hecke operators.

Using this connection and the definition of the $-D$-th Shimura correspondence to evaluate the coefficients of $\widetilde{G}$ (using the fact that $\widetilde{G}$ is normalized), the second author [Kan09, equation (4.2)] has shown for $c = p^m$ relatively prime to $FN\ell$,

$$a_g(d_{cF}) = a_g(d_F)\left(a_G(p^m) - \left(\frac{-D}{p}\right) a_G(p^{m-1})\right) = a_g(d_F) \sum_{c'|c} \mu(c') \left(\frac{-D}{c'}\right) a_G\left(\frac{c}{c'}\right).$$

Here we have rewritten the right hand side so that extending by multiplicativity, it follows that

$$a_g(d_c) = a_g(d_1) \sum_{c'|c} \mu(c') \left(\frac{D}{c'}\right) a_G\left(\frac{c}{c'}\right).$$

Substituting this in equation (25) gives the identity

$$a^*(d_c) = \sum_{i=1}^{r} b_i a_{g_i}(d_1) \sum_{c'|c} \sum_{c''|\frac{c}{c'}} \mu(c')\mu(c'') \left(\frac{D}{c''}\right) a_{G_i}\left(\frac{c}{c'c''}\right). \tag{26}$$

Thus we have established that the supersingular point $s \in X_0(N)^{\mathrm{SS}}_{/\mathbb{F}_{\ell^2}}$ is not in the image of red_ℓ from $\Gamma_{D,c}$ if and only if

$$\frac{1}{\sum_{s' \in X_0(N)^{\mathrm{SS}}_{/\mathbb{F}_{\ell^2}}} 1/w_{s'}} \left(\sum_{c'|c} \mu(c') \left(\frac{D}{c'}\right) \frac{c}{c'}\right) \frac{\#\Gamma_{D,1}}{u_{D,1}} = -\sum_{i=1}^{r} b_i a_{g_i}(d_1) \sum_{c'|c} \sum_{c''|\frac{c}{c'}} \mu(c')\mu(c'') \left(\frac{D}{c''}\right) a_{G_i}\left(\frac{c}{c'c''}\right). \tag{27}$$

Now consider the Euler φ-function $\varphi(c) := \#\{m < c : (m, c) = 1\}$. Then

$$\sum_{c'|c} \mu(c') \left(\frac{D}{c'}\right) \frac{c}{c'} \geqslant \varphi(c),$$

since the inequality holds for c being a prime power and both functions are multiplicative. We can then use the explicit elementary bound $\varphi(c) \geqslant \dfrac{\log 2}{2}\dfrac{c}{\log c}$ for $c > 2$ (cf. [JMC06, p.9]).

We next pull the absolute value inside the sum on the right hand side of (27) and use Deligne's optimal bound [Del74] for integer weight cusp forms from the proof of the Weil conjectures, namely $|a_{G_i}(n)| \leqslant \sigma_0(n) n^{\frac{1}{2}}$. Since $\#\{c' \mid c : \mu(c') \neq 0\} = 2^{v(c)}$ and $\sigma_0(c') \leqslant \sigma_0(c)$ for $c' \mid c$, we have

$$|a^*(d_c)| \leqslant 2^{2v(c)} \sigma_0(c) c^{\frac{1}{2}} \sum_{i=1}^{r} |b_i a_{g_i}(D)|, \tag{28}$$

giving the assertion. □

2. The case $\#X_0(N)^{\mathrm{SS}}_{/\mathbb{F}_{\ell^2}}$. In the case when $\#X_0(N)^{\mathrm{SS}}_{/\mathbb{F}_{\ell^2}} = 2$ we obtain an explicit bound independent of D beyond which surjectivity holds. Let $m_s = \max\left(1, \dfrac{w_{s'}}{w_s}\right)$.

Lemma 6.2. *If $\#X_0(N)^{\mathrm{SS}}_{/\mathbb{F}_{\ell^2}} = 2$ then the inequality*

$$\varphi(c) > m_s 2^{2v(c)} \sigma_0(c) c^{\frac{1}{2}} \tag{29}$$

implies that the reduction red_ℓ on $\Gamma_{D,c}$ is surjective for any fundamental discriminant $D < 0$.

Proof. Let $X_0(N)^{\mathrm{SS}}_{/\mathbb{F}_{\ell^2}} = \{s, s'\}$. Recall that

$$\theta_{\mathrm{gen}(Q_s)} = \frac{\frac{1}{w_s}\theta_{Q_s} + \frac{1}{w_{s'}}\theta_{Q_{s'}}}{1/w_s + 1/w_{s'}}.$$

By Siegel's theorem (see [DSP90, Thm.2(ii)]) there is a Hecke eigenform g such that $\theta_{Q_s} = \theta_{\mathrm{gen}(Q_s)} + g$ and $\theta_{Q_{s'}} = \theta_{\mathrm{gen}(Q_s)} - \dfrac{w_{s'}}{w_s} g$. Since $r(Q_s, |D|) \geqslant 0$ and $r(Q_{s'}, |D|) \geqslant 0$, we have $|a_g(|D|)| \leqslant \max(1, \dfrac{w_{s'}}{w_s}) r(\mathrm{gen}(Q_s), |D|)$. The lemma then follows immediately by combining equations (24) and (28) with $b_1 g_1 = g$ after canceling $r(\mathrm{gen}(Q_s), |D|)$ on both sides. □

Let $G = S_{-D,1}(g)$ be the $-D$th Shimura correspondence of g as defined in Section 3. Define

$$r_c := \frac{\sum_{c' \mid c} \mu(c') \left(\frac{-D}{c'}\right) \frac{c}{c'}}{\left| \sum_{c' \mid c} \mu(c') \sum_{c'' \mid \frac{c}{c'}} \mu(c'') \left(\frac{-D}{c''}\right) a_G\left(\frac{c}{c'c''}\right) \right|},$$

where we take $r_c = \infty$ by convention if the denominator is zero, and

$$\widetilde{r}_c := \frac{\varphi(c)}{2^{2v(c)} \sigma_0(c) c^{\frac{1}{2}}}.$$

By equations (27) and (28) if $r_c > m_s$ or $\widetilde{r}_c > m_s$ then s is in the image of red_ℓ. Note that both r_c and $\widetilde{r}_c$ are multiplicative and $r_c \geqslant \widetilde{r}_c$. For $c = p^m$ we have

$$\widetilde{r}_c = \frac{p^{\frac{m}{2}-1}(p-1)}{4(m+1)}.$$

For $p \geqslant 5$, $\widetilde{r}_c$ is increasing as a function of m, whereas for $p < 5$ it is increasing for $m > 2$. For a constant a and $m = 1$ the inequality $\widetilde{r}_c > a$ is satisfied for

$$p > P_a := \left(\frac{4a + \sqrt{16a^2 + 4}}{2}\right)^2.$$

For $p \leqslant P_a$ we use the fact that $\widetilde{r}_c$ is increasing exponentially as a function of m to obtain a bound $M_{p,a}$ such that $m > M_{p,a}$ implies that $\widetilde{r}_c > a$. Therefore, there are only finitely many choices for the pair (p, m) with $m \geqslant 1$ for which $r_{p^m} \leqslant a$. Let

$$C_a = \{(p, m) : r_{p^m} \leqslant a\}.$$

Computing r_{p^m} explicitly for $m \leqslant M_{p,a}$ allows us to explicitly calculate C_a.

We first follow the above argument with $a = 1$ to show that

$$r_{\min} := \prod_p \min_{m \geqslant 0} r_{p^m}$$

is well defined and satisfies $r_c \geqslant r_{\min}$ for every c. We will now use the above bounds with $a := \dfrac{m_s}{r_{\min}}$. Let c be an arbitrary integer such that $r_c \leqslant m_s$. Write $c = p^m c'$ with $(p, c') = 1$. By multiplicativity we have

$$m_s \geqslant r_c = r_{c'} r_{p^m} \geqslant r_{\min} r_{p^m}.$$

Therefore $r_{p^m} \leqslant a$, so $(p, m) \in C_a$, and it follows that

$$c \mid \prod_{(p,m) \in C_a} p^m.$$

We can refine this argument by recursively computing

$$S_v := \{c : v(c) = v, r_c \leqslant m_s\}.$$

For $c' \in S_v$, consider

$$a' := a \frac{\prod_{(p,c')=1} \min_{m \geqslant 0} r_{p^m}}{r_{c'}}$$

Then for $c = p^m c'$ with $(p, c) = 1$, $r_c \in S_{v+1}$ if and only if $(p, m) \in C_{a'}$. Constructing the resulting tree in this manner allows us to terminate the depth-first search when $C_{a'}$ is empty.

Proceeding in this manner, we obtain for $\ell = 11$ and $N = 1$ exactly 116 possible values of c in the union of all S_v, the largest of which is 5124. For $\ell = 17$ and $N = 1$ there are 93 possible values of c, the largest of which is 3990, and for $\ell = 19$ and $N = 1$ there are 165 possible values of c, the largest of which is 8502.

Acknowledgements

We are grateful to Christophe Cornut for suggesting the problem and for the numerous discussions. We thank Barry Mazur, Philippe Michel, Steve Miller, Ken Ribet, William Stein and Tonghai Yang for helpful conversations. The first author thanks IHES, France for their kind hospitality and for providing a post-doctoral position during which a significant part of the research was completed. Part of the paper was written while the second author was in residence at IHES in France. He thanks the institute for providing a stimulating research environment.

References

Cip83 B. A. Cipra, *On the Niwa–Shintani theta-kernel lifting of modular forms*, Nagoya Math. J. **91** (1983), 49–117.

CJ09 C. Cornut and D. Jetchev, *Deuring correspondence for quaternion algebras*, in preparation (2009).

Cor02 C. Cornut, *Mazur's conjecture on higher Heegner points*, Invent. Math. **148** (2002), no. 3, 495–523.

Cox89 D. Cox, *Primes of the form $x^2 + ny^2$*, Wiley, New York, NY, 1989.

CV05 C. Cornut and V. Vatsal, *CM points and quaternion algebras*, Doc. Math. **10** (2005), 263–309 (electronic).

Del74 P. Deligne, *La conjecture de Weil I*, Inst. Hautes Études Sci. Publ. Math. **43** (1974), 273–307.

Deu41 M. Deuring, *Die Typen der Multiplikatorenringe elliptischer Funktionenkörpen*, Abh. Math. Sem. Hansischen Univ., vol. 14, 1941, pp. 197–272.

DSP90 W. Duke and R. Schulze-Pillot, *Representation of integers by positive ternary quadratic forms and equidistribution of lattice points on ellipsoids*, Invent. Math. **99** (1990), no. 1, 49–57.

Duk98 W. Duke, *Hyperbolic distribution problems and half-integral weight maass forms*, Invent. Math. **92** (1998), 73–90.

Duk05 ———, *On ternary quadratic forms*, J. Number Theory **110** (2005), no. 1, 37–43.

EOY05 N. Elkies, K. Ono, and T. Yang, *Reduction of cm elliptic curves and modular function congruences*, Int. Math. Res. Not. **44** (2005), 2695–2707.

Fli80 Y. Z. Flicker, *Automorphic forms on covering groups of $GL(2)$*, Invent. Math. **57** (1980), 119–182.

Gro84 B. Gross, *Heegner points on $X_0(N)$*, Modular forms (Durham, 1983), Ellis Horwood Ser. Math. Appl.: Statist. Oper. Res., Horwood, Chichester, 1984, pp. 87–105.

Gro87 B. H. Gross, *Heights and the special values of L-series*, Number theory (Montreal, Que., 1985), CMS Conf. Proc., vol. 7, Amer. Math. Soc., Providence, RI, 1987, pp. 115–187.

GZ85 B. Gross and D. Zagier, *On singular moduli*, J. Reine Angew. Math. **355** (1985), 191–220.

Han04a J. Hanke, *Modular forms of half integral weight and the integral of certain theta functions*, Duke Math. J. **124** (2004), 351–388.

Han04b ———, *Some recent results about (ternary) quadratic forms*, CRM Proceedings and Lecture Notes **36** (2004), 147–164.

Iwa87 H. Iwaniec, *Fourier coefficients of modular forms of half-integral weight*, Invent. Math. **87** (1987), 385–401.

JMC06 S. József, D Mitronović, and B. Crstici, *Handbook of number theory. I*, Springer, Dordrecht, 2006, Reprint of 1996 edition.

Jon50 B. Jones, *The arithmetic theory of quadratic forms*, Carcus Monograph Series, no. 10, The Mathematical Association of America, Buffalo, Buffalo, NY, 1950.

Kan09 B. Kane, *Representations of integers by ternary quadratic forms*, International J. Number Theory (2009), to appear.

Maz83 B. Mazur, *Modular Curves and Arithmetic*, Proceedings of the International Congress of Mathematicians (Warsaw), 1983, pp. 185–211.

Mic04 P. Michel, *The subconvexity problem for Rankin-Selberg L-functions and equidistribution of Heegner points*, Ann. of Math. (2) **160** (2004), no. 1, 185–236.

Niw74 S. Niwa, *Modular forms of half integral weight and the integral of certain theta functions*, Nagoya Math. J. **56** (1974), 147–161.

Oes85 J. Oesterlé, *Nombres de classes des corps quadratiques imaginaires*, Astériques **121-122** (1985), 309–323.

O'M00 O. T. O'Meara, *Introduction to quadratic forms*, Classics in Mathematics, Springer-Verlag, Berlin, 2000, Reprint of the 1973 edition.

Ono04 K. Ono, *The web of modularity: Arithmetic of the coefficients of modular forms and q-series*, CBMS Regional Conference Series in Mathematics, vol. 102, American Mathematical Society, Providence, RI, 2004.

Par03 P. Parent, *Triviality of $X_{\mathrm{split}}(N)(\mathbf{Q})$ for certain congruence classes of N*, C. R. Math. Acad. Sci. Paris **336** (2003), no. 5, 377–380.

Rat95 M. Ratner, *Raghunatan's conjectures for cartesian products of real and p-adic Lie groups*, Duke Math. J. **77** (1995), no. 2, 275–382.

Rib90 K. A. Ribet, *On modular representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ arising from modular forms*, Invent. Math. **100** (1990), no. 2, 431–476.

Ser96 J.-P. Serre, *Two letters on quaternions and modular forms (mod p)*, Israel J. Math. **95** (1996), 281–299, With introduction, appendix and references by R. Livné.

Sie35 C. Siegel, *Über die klassenzahl quadratischer zahlkorper*, Acta Arith. **1** (1935), 83–86.

SP84 R. Schulze-Pillot, *Thetareihen positiv definiter quadratischer Formen*, Invent. Math. **75** (1984), no. 2, 283–299.

Vat02 V. Vatsal, *Uniform distribution of Heegner points*, Invent. Math. **148** (2002), no. 1, 1–46.

Vat03 ———, *Special values of anticyclotomic L-functions*, Duke Math. J. **116** (2003), no. 2, 219–261.

Vig80 M.-F. Vignéras, *Arithmétique des algèbres de quaternions*, Lecture Notes in Mathematics, vol. 800, Springer, Berlin, 1980.

Dimitar Jetchev jetchev@gmail.com
IHES Le Bois-Marie, 35, route de Chartres, Bures-sur-Yvette, France

Ben Kane bkane@science.ru.nl
Department of Mathematics, Radboud Universiteit, Toernooiveld 1, 6525 Nijmegen, Netherlands