Simultaneous supersingular reductions of CM elliptic curves

Originally published in:
Journal für die reine und angewandte Mathematik 2022(786), https://doi.org/10.1515/crelle-2021-0086

Funding acknowledgement:
- Dynamics on homogeneous spaces and number theory ()
- Geometric and Analytic Number Theory ()

J. reine angew. Math. **786** (2022), 1–43
DOI 10.1515/crelle-2021-0086

Journal für die reine und angewandte Mathematik

Simultaneous supersingular reductions of CM elliptic curves

By *Menny Aka* at Zurich, *Manuel Luethi* at Lausanne, *Philippe Michel* at Lausanne and *Andreas Wieser* at Jerusalem

Abstract. We study the simultaneous reductions at several supersingular primes of elliptic curves with complex multiplication. We show – under additional congruence assumptions on the CM order – that the reductions are surjective (and even become equidistributed) on the product of supersingular loci when the discriminant of the order becomes large. This variant of the equidistribution theorems of Duke and Cornut–Vatsal is an(other) application of the recent work of Einsiedler and Lindenstrauss on the classification of joinings of higher-rank diagonalizable actions.

1. Introduction

1.1. Simultaneous reduction of CM elliptic curves. Let $\mathbf{K} = \mathbb{Q}(\sqrt{D})$ be an imaginary quadratic number field with ring of integers $\mathscr{O}_{\mathbf{K}}$ and discriminant $D = D_{\mathbf{K}} < 0$.

An elliptic curve over $\mathbb{C}$ is a smooth projective variety in $\mathbb{P}^2_{\mathbb{C}}$ defined by an equation of the shape

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

and equipped with the structure of an abelian group via the usual chord-tangent construction and the point $[0, 1, 0]$ as neutral element. We say that $E/\mathbb{C}$ has complex multiplication (CM) by $\mathscr{O}_{\mathbf{K}}$ if its ring of endomorphisms is isomorphic to $\mathscr{O}_{\mathbf{K}}$. Denote by $\mathrm{Ell}^{\mathrm{cm}}_{\mathscr{O}_{\mathbf{K}}}$ the finite set of $\mathbb{C}$-isomorphism classes of such elliptic curves.

Given $E \in \mathrm{Ell}^{\mathrm{cm}}_{\mathscr{O}_{\mathbf{K}}}$, its j-invariant $j(E)$ is an algebraic integer, cf. [45, Chapter II, Theorem 6.1], and $\mathbf{K}(j(E)) \subset \bar{\mathbb{Q}} \subset \mathbb{C}$ is the Hilbert class field $\mathbf{H}_{\mathbf{K}}$ of $\mathbf{K}$, cf. [45, Chapter II, Theorem 4.3]. Consequently, E is defined over $\mathbf{H}_{\mathbf{K}}$.

The corresponding author is Menny Aka.

Manuel Luethi acknowledges the support of the SNF (grants 200021_178958, P1EZP2_181725 and 200021_197045) and of the ISF (grant 1483/16). Philippe Michel is partially supported by a DFG-SNF lead agency program grant 200021L_175755 and by the SNF grant 200021_197045. Andreas Wieser was partially supported by SNF grant 20021_178958, SNF Doc. Mobility grant 195737, and ERC 2020 grant no. 833423.

Given p a fixed odd prime, we also fix throughout an embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}_p}$; in particular this embedding uniquely determines, for any field $\mathbf{K}$ as above, a prime ideal $\mathfrak{p} = \mathfrak{p}_{\mathbf{H_K}} \subset \mathscr{O}_{\mathbf{H_K}}$ above p.

Assume that p is inert in $\mathbf{K}$. The curve E (or rather an $\mathbf{H_K}$-form of it) has good reduction $E \bmod \mathfrak{p}$ at $\mathfrak{p}$, cf. Section 5.3, and its j-invariant is

$$j(E \bmod \mathfrak{p}) = j(E) \bmod \mathfrak{p} \in \mathbb{F}_{p^2},$$

and the curve $E \bmod \mathfrak{p}$ is supersingular, i.e. its endomorphism ring is a maximal order in a quaternion algebra over $\mathbb{Q}$, namely in the unique quaternion algebra $\mathbf{B}_{p,\infty}$ ramified at p and ∞.

We denote by $\mathrm{Ell}_p^{\mathrm{ss}}$ the set of isomorphism classes of supersingular elliptic curves defined over $\overline{\mathbb{F}_p}$. This is a finite set of cardinality $\frac{p}{12} + O(1)$ (see [46, Chapter V, Theorem 4.1]). We will be interested in studying the reduction map

$$\mathrm{red}_p : \mathrm{Ell}^{\mathrm{cm}}_{\mathscr{O}_{\mathbf{K}}} \to \mathrm{Ell}_p^{\mathrm{ss}}, \quad E \mapsto E \bmod \mathfrak{p}$$

for various values of p.

By Deuring's lifting theorem [13] every supersingular curve can be obtained as the reduction of some elliptic curve (with complex multiplication by some order of some imaginary quadratic field). A natural question then is whether the CM order can be taken to be maximal and if so, which are the possible orders. In [35], the third named author remarked that by combining the works of Gross, Duke and Iwaniec [14,25,27], any $E_0 \in \mathrm{Ell}_p^{\mathrm{ss}}$ may be lifted to some $E \in \mathrm{Ell}^{\mathrm{cm}}_{\mathscr{O}_{\mathbf{K}}}$ as soon as p is inert in $\mathbf{K}$ and D is sufficiently large (depending on p). In other terms, for D large enough, the reduction map red_p is surjective. This result was subsequently reinterpreted and refined by several authors – see for example [21,28,54].

In the present paper we are interested in a further refinement of this question: namely whether given several supersingular elliptic curves at several distinct primes there exists a *single* elliptic curve with CM by $\mathscr{O}_{\mathbf{K}}$ which is a lifting of all of them. More precisely, let $\mathbf{p} = \{p_1, \dots, p_s\}$ be a finite set of distinct odd primes and for each i a fixed embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}_{p_i}}$. Let $\mathbf{K}$ be an imaginary quadratic field in which the primes $p_1, \dots, p_s$ are all inert. For each $i \in \{1, \dots, s\}$ let $\mathfrak{p}_i = \mathfrak{p}_{i,\mathbf{H_K}}$ be the prime ideal in $\mathbf{H_K}$ determined by $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}_{p_i}}$. We now have a simultaneous reduction map

$$\mathrm{red}_{\mathbf{p}} : \mathrm{Ell}^{\mathrm{cm}}_{\mathscr{O}_{\mathbf{K}}} \to \prod_{i \le s} \mathrm{Ell}_{p_i}^{\mathrm{ss}}, \quad E \mapsto (E \bmod \mathfrak{p}_i)_{i \le s}.$$

The question is whether this map is surjective or not. We expect that this is the case as long as D is large enough (depending on $\mathbf{p}$). A consequence of our main Theorem 1.3 stated below is that this is the case at least under some additional congruence assumptions on D:

Theorem 1.1 (Simultaneous lifting). *Let q_1, q_2 be two distinct, odd primes, and let $p_1, \dots, p_s$ be distinct odd primes also distinct from q_1 and q_2. There is some $D_0 \ge 1$ (depending on $\mathbf{p} = \{p_1, \dots, p_s\}$ and q_1, q_2) with the following property: for any imaginary quadratic field $\mathbf{K}$ of discriminant D such that*

(1) $|D| \ge D_0$,

(2) *each p_i for $1 \le i \le s$ is inert in $\mathbf{K}$, and*

(3) *q_1 and q_2 are split in $\mathbf{K}$,*

the map $\mathrm{red}_{\mathfrak{p}}$ *is surjective. In other terms, for all* $E_i \in \mathrm{Ell}^{\mathrm{ss}}_{p_i}$, $i = 1, \dots, s$, *there exists an elliptic curve* $E \in \mathrm{Ell}^{\mathrm{cm}}_{\mathscr{O}_{\mathbf{K}}}$ *satisfying*

$$E \bmod \mathfrak{p}_i = E_i \quad (i = 1, \dots, s).$$

In fact, this surjectivity result admits a more precise formulation in the form of an equidistribution statement on the product of $\prod_{1 \le i \le s} \mathrm{Ell}^{\mathrm{ss}}_{p_i}$.

Given $E_0 \in \mathrm{Ell}^{\mathrm{ss}}_p$, we define

$$w_{E_0} = |\mathrm{End}^{\times}(E_0)/\{\pm 1\}|.$$

Eichler's mass formula states that

$$\sum_{E_0 \in \mathrm{Ell}^{\mathrm{ss}}_p} \frac{1}{w_{E_0}} = \frac{p-1}{12}, \tag{1.1}$$

see e.g. [25, equation (1.2)]. We then introduce the probability measure

$$\nu_p = \frac{12}{p-1} \sum_{E_0 \in \mathrm{Ell}^{\mathrm{ss}}_p} \frac{1}{w_{E_0}} \delta_{E_0}.$$

Remark 1.2. It is known that the product of the w_{E_0} over the distinct isomorphism classes is a divisor of 12, cf. [25, equation (1.1)], and hence asymptotically most weights are equal to 1 so the above measure is almost uniform.

Using the observation in [35] referred to previously, the third author established that for every $E_0 \in \mathrm{Ell}^{\mathrm{ss}}_p$ we have

$$\frac{|\{E \in \mathrm{Ell}^{\mathrm{cm}}_{\mathscr{O}_{\mathbf{K}}} : E \bmod \mathfrak{p} \cong E_0\}|}{|\mathrm{Ell}^{\mathrm{cm}}_{\mathscr{O}_{\mathbf{K}}}|} \to \nu_p(E_0)$$

as $D \to -\infty$ along the set of fundamental discriminants. In other terms, the push-forward of the uniform probability measure on $\mathrm{Ell}^{\mathrm{cm}}_{\mathscr{O}_{\mathbf{K}}}$ by the map red_p converges to the measure ν_p.

We establish a similar equidistribution statement towards the product measure $\bigotimes_{i \le s} \nu_{p_i}$; in fact, we include an additional archimedean equidistribution result.

Let Ell_{∞} be the moduli space of all complex elliptic curves up to $\mathbb{C}$-isomorphism. This space is identified with the space of lattices in $\mathbb{C}$ up to $\mathbb{C}^{\times}$-homothety, i.e. the complex modular curve

$$Y_0(1) = \mathrm{SL}_2(\mathbb{Z}) \backslash \mathbb{H},$$

via the map

$$[z] = \mathrm{SL}_2(\mathbb{Z}).z \mapsto [\Lambda_z] := [\mathbb{Z} + \mathbb{Z}.z] \mapsto [\mathbb{C}/\Lambda_z].$$

In this representation an elliptic curve E with CM by $\mathscr{O}_{\mathbf{K}}$ is one for which the corresponding lattice Λ_{z_E} satisfies

$$\mathrm{End}(\Lambda_{z_E}) := \{z \in \mathbb{C} : z.\Lambda_{z_E} \subset \Lambda_{z_E}\} = \mathscr{O}_{\mathbf{K}} \subset \mathbf{K} \subset \mathbb{C}.$$

By this identification Ell_{∞} is equipped with a probability measure ν_{∞} corresponding to the normalized hyperbolic measure $\frac{3}{\pi} \frac{dxdy}{y^2}$.

Let red_∞ denote the obvious injection

$$\mathrm{red}_\infty : \mathrm{Ell}^{\mathrm{cm}}_{\mathscr{O}_{\mathbf{K}}} \to \mathrm{Ell}_\infty, \quad E \mapsto E(\mathbb{C}).$$

It was proven by Duke in [14] that the push-forward of the uniform probability measure on $\mathrm{Ell}^{\mathrm{cm}}_{\mathscr{O}_{\mathbf{K}}}$ converges to ν_∞ as $D \to -\infty$.

Setting now

$$\mathbf{p} = \{p_0 = \infty\} \cup \{p_i : 1 \leq i \leq s\}$$

we consider the map $\mathrm{red}_{\mathbf{p}} = (\mathrm{red}_{p_i})_{0 \leq i \leq s}$ and its image

$$\mathrm{red}_{\mathbf{p}}(\mathrm{Ell}^{\mathrm{cm}}_{\mathscr{O}_{\mathbf{K}}}) = \{(\mathrm{red}_{p_i}(E))_{0 \leq i \leq s} : E \in \mathrm{Ell}^{\mathrm{cm}}_{\mathscr{O}_{\mathbf{K}}}\} \subset \mathrm{Ell}_\infty \times \prod_{i=1}^{s} \mathrm{Ell}^{\mathrm{ss}}_{p_i}.$$

We prove:

Theorem 1.3. *Let q_1, q_2 be distinct, odd primes which are distinct from $p_1, \ldots, p_s$. As $D \to -\infty$ along the set of fundamental negative discriminants such that*

(1) *each p_i for $1 \leq i \leq s$, is inert in $\mathbf{K} = \mathbb{Q}(\sqrt{D})$, and*

(2) *q_1, q_2 are split in $\mathbf{K}$,*

the push-forward of the counting probability measure on $\mathrm{Ell}^{\mathrm{cm}}_{\mathscr{O}_{\mathbf{K}}}$ by $\mathrm{red}_{\mathbf{p}}$ equidistributes towards $\nu_\infty \otimes \nu_{p_1} \otimes \cdots \otimes \nu_{p_s}$.

This equidistribution result is true more generally if instead of a sequence of maximal orders $\mathscr{O}_{\mathbf{K}}$ we consider sequences of quadratic orders $\mathscr{O} \subset \mathscr{O}_{\mathbf{K}} \subset \mathbf{K}$ and the sets $\mathrm{Ell}^{\mathrm{cm}}_{\mathscr{O}}$ of elliptic curves with complex multiplication by $\mathscr{O}$ (again with suitable congruence condition); we refer to Theorem 7.1 for the precise statement.

Remark 1.4. In this extended setting, a version of this equidistribution result was proven by Cornut [8] using ideas of Vatsal [48] for non-maximal orders whose discriminants are of the form Dp^{2n} for $D < 0$ a fixed fundamental discriminant, p a fixed prime coprime to D and $n \to +\infty$. As in the present paper, these works make crucial use of dynamics and ergodic theory on locally homogeneous spaces. A chief difference is that the above mentioned works use unipotent dynamics (i.e. Ratner's theorems such as [41]) while we also need to rely on the recent work of Einsiedler and Lindenstrauss on rigidity of joinings of higher rank diagonalizable actions [16].

An especially interesting case is that of orders whose discriminants are of the form Dp^n for $D < 0$ a fixed fundamental discriminant, $n \geq 1$ a fixed exponent, and $p \to +\infty$ along the primes coprime to D (see Theorem 7.1). Although the quadratic field $\mathbf{K} = \mathbb{Q}(\sqrt{D})$ is fixed, the fact that p is varying also seems to require the use of rigidity of higher rank diagonalizable actions. As explained to us by Henri Darmon such a case could be interesting for the study of certain Euler systems. We will pursue other variants along this direction in future joint work with D. Ramakrishnan.

Remark 1.5. Theorem 1.3 can be upgraded in several directions:

- The most immediate is by incorporating additional level structures; for instance by considering for $N \geq 1$, the space $Y_0(N)$ of isomorphism classes of pairs of elliptic curves $\varphi : E_1 \mapsto E_2$, where φ has a cyclic kernel of order N. Suppose that every prime divisor

of N splits in $\mathbf{K}$. If $(\varphi : E_1 \mapsto E_2) \in Y_0(N)(\mathbb{C})$ is such that $E_1 \in \mathrm{Ell}^{\mathrm{cm}}_{\mathscr{O}_\mathbf{K}}$, then $E_2 \in \mathrm{Ell}^{\mathrm{cm}}_{\mathscr{O}_\mathbf{K}}$ as well; the set, $Y_0(N)^{\mathrm{cm}}_{\mathbf{K}}$ say, of such "CM" points is then called the set of *Heegner points* ([24, Section I.3.]). Note that if, in addition, N has two distinct prime factors q_1, q_2, the splitting condition is automatic.

- In [26], S. Herrero, R. Menares, and J. Rivera-Letelier have established a refined version of the equidistribution of CM elliptic curves modulo an inert prime p (more generally for any kind of prime) by describing how the CM curves equidistribute on $\mathrm{Ell}^{\mathrm{ss}}(\mathbb{C}_p)$, the moduli space of elliptic curves over $\mathbb{C}_p$ with supersingular reduction. Their proof relies among other things on Duke's approach to prove equidistribution (i.e. by bounding Fourier coefficient of an adequate theta series). In a forthcoming project with the authors of [26] we will combine both their and our methods to prove the joint equidistribution of $\mathrm{Ell}^{\mathrm{cm}}_{\mathscr{O}}$ on the product of the moduli spaces $\mathrm{Ell}^{\mathrm{ss}}(\mathbb{C}_{p_i})$ for $i = 1, \dots, s$.
- These equidistribution theorems also generalize to equidistribution for CM points in the space of abelian varieties of dimension $2[F : \mathbb{Q}]$, admitting complex multiplication by a quaternion algebra defined over a fixed totally real number field F. We refer to [8–11, 48] for examples of work in this direction.

Remark 1.6. Though seemingly artificial, the splitting assumption on q_1, q_2 in Theorem 1.3 allows the use of diagonalizable dynamics alluded to in Remark 1.4 (see the discussion after Theorem 1.8). One may generalize Theorem 1.3 to treat for instance all imaginary quadratic fields $\mathbf{K}$ for which there are two split primes $q_1, q_2 \notin \{2, p_1, \dots, p_s\}$ below a fixed threshold $C > 0$. Furthermore, even assuming GRH one cannot remove the splitting assumption using the arguments in the present paper as the dynamical argument uses two fixed split primes that are not allowed to vary with the field.

1.2. Reduction to an equidistribution statement. As hinted at above, Theorem 1.3 is a consequence of a dynamical statement in the context of locally homogeneous spaces. The first step is to realize $\mathrm{red}_{\mathbf{p}}(\mathrm{Ell}^{\mathrm{cm}}_{\mathscr{O}_\mathbf{K}})$ as (the projection of) an orbit of the adelic points of the torus

$$\mathbf{T}_\mathbf{K} = \mathrm{Res}_{\mathbf{K}/\mathbb{Q}}\mathbb{G}_m/\mathbb{G}_m$$

on a product of adelic locally homogeneous spaces. We describe this realization here. Using this realization, Theorem 1.3 is then obtained from an equidistribution result for such orbits, more specifically Theorem 1.8 which will be discussed in the next section.

We use several $\mathbb{Q}$-forms of PGL_2, namely the projective unit groups $\mathbf{G}_i = \mathbf{PB}_i^\times$ for $i = 0, \dots, s$ of the quaternion algebras $\mathbf{B}_0, \mathbf{B}_1, \dots, \mathbf{B}_s$ defined over $\mathbb{Q}$, where $\mathbf{B}_0 = \mathrm{Mat}_2$ is the split quaternion algebra and where $\mathbf{B}_i$ for $1 \leq i \leq s$ is the quaternion algebra ramified exactly at ∞ and p_i.

As explained in Section 5 there is for each p_i an identification

$$\psi_i : \mathrm{Ell}^{\mathrm{ss}}_{p_i} \xrightarrow{\sim} \mathbf{G}_i(\mathbb{Q})\backslash\mathbf{G}_i(\mathbb{A})/\mathbf{G}_i(\mathbb{R})\mathrm{P}\widehat{\mathcal{O}_i}^\times,$$

where $\mathcal{O}_i \subset \mathbf{B}_i(\mathbb{Q})$ is some fixed maximal order and $\widehat{O_i} = \mathcal{O}_i \otimes \widehat{\mathbb{Z}}$. There is also an identification for the archimedean place

$$\psi_0 : \mathrm{Ell}_\infty \xrightarrow{\sim} \mathrm{PGL}_2(\mathbb{Q})\backslash\mathrm{PGL}_2(\mathbb{A})/\mathrm{PSO}_2(\mathbb{R})\mathrm{PGL}_2(\widehat{\mathbb{Z}}).$$

Let $E \in \mathrm{Ell}^{\mathrm{cm}}_{\mathscr{O}_{\mathbf{K}}}$. To E is associated for each $i = 0, \dots, s$ a class $[g_{E,i}] = \psi_i(\mathrm{red}_{p_i}(E))$ and an embedding of $\mathbb{Q}$-algebras $\iota_i : \mathbf{K} \hookrightarrow \mathbf{B}_i$, and consequently a morphism of $\mathbb{Q}$-algebraic groups

$$\iota_i : \mathbf{T}_{\mathbf{K}} \hookrightarrow \mathbf{G}_i .$$

Let us recall that the ideal class group $\mathrm{Pic}(\mathscr{O}_{\mathbf{K}})$ acts simply transitively on $\mathrm{Ell}^{\mathrm{cm}}_{\mathscr{O}_{\mathbf{K}}}$; we denote this action by

$$([\mathfrak{a}], E) \mapsto [\mathfrak{a}] \star E,$$

where $[\mathfrak{a}]$ is the class of an ideal $\mathfrak{a} \subset \mathscr{O}_{\mathbf{K}}$. We also have a natural identification

$$\mathrm{Pic}(\mathscr{O}_{\mathbf{K}}) \simeq \mathbf{T}_{\mathbf{K}}(\mathbb{Q}) \backslash \mathbf{T}_{\mathbf{K}}(\mathbb{A}) / \mathbf{T}_{\mathbf{K}}(\mathbb{R}) \mathbf{T}_{\mathbf{K}}(\widehat{\mathbb{Z}}),$$

where $\mathbf{T}_{\mathbf{K}}(\widehat{\mathbb{Z}})$ corresponds to the projectivized group of units in the completion $\widehat{\mathscr{O}_{\mathbf{K}}}$, where the integral structure defining $\mathbf{T}_{\mathbf{K}}(\widehat{\mathbb{Z}})$ is the one induced by the choice of maximal orders $\mathcal{O}_1, \dots, \mathcal{O}_s$. We show in Section 4.3 and Section 5.4 that for $i = 0, \dots, s$, if $t_{\mathrm{f}} \in \mathbf{T}_{\mathbf{K}}(\mathbb{A}_{\mathrm{f}})$ is such that $[t_{\mathrm{f}}] \simeq [\mathfrak{a}]$, then

$$\psi_i(\mathrm{red}_{p_i}([\mathfrak{a}] \star E)) = [\iota_i(t_{\mathrm{f}}^{-1}) g_{E,i}].$$

We now collect these identities for all $0 \leq i \leq s$. Let us set

$$\iota = (\iota_i)_{0 \leq i \leq s} : \mathbf{T}_{\mathbf{K}} \to \mathbf{G} = \prod_{i=0}^{s} \mathbf{G}_i$$

and define $\mathrm{g}_E = (g_{E,i})_{0 \leq i \leq s}$ as well as the compact groups

$$K_\infty = \mathrm{PSO}_2(\mathbb{R}) \times \prod_{i=1}^{s} \mathbf{G}_i(\mathbb{R}) \quad \text{and} \quad K_{\mathrm{f}} = \mathrm{PGL}_2(\widehat{\mathbb{Z}}) \times \prod_{i=1}^{s} \mathrm{P}\widehat{\mathcal{O}}_i^{\times}.$$

We obtain that the componentwise identification

$$\psi : \mathrm{Ell}_\infty \times \prod_i \mathrm{Ell}^{\mathrm{ss}}_{p_i} \xrightarrow{\sim} \mathbf{G}(\mathbb{Q}) \backslash \mathbf{G}(\mathbb{A}) / K_\infty K_{\mathrm{f}}$$

satisfies for any $[t_{\mathrm{f}}]$ and $[\mathfrak{a}]$ as above

$$\psi(\mathrm{red}_{\mathbf{p}}([\mathfrak{a}] \star E)) = [\iota(t_{\mathrm{f}}^{-1}) \mathrm{g}_E].$$

Therefore $\mathrm{red}_{\mathbf{p}}(\mathrm{Ell}^{\mathrm{cm}}_{\mathscr{O}_{\mathbf{K}}})$ is identified with the projection of the orbit of the torus $\mathbf{T}_{\mathbf{K}}(\mathbb{A})$ embedded diagonally into the product group $\mathbf{G}$ by ι:

$$[\iota(\mathbf{T}_{\mathbf{K}}(\mathbb{A})) \mathrm{g}_E] \subset \mathbf{G}(\mathbb{Q}) \backslash \mathbf{G}(\mathbb{A}) / K_\infty K_{\mathrm{f}}.$$

Let $\mathbf{T}_\iota$ denote the image $\iota(\mathbf{T}_{\mathbf{K}})$. The situation can be summarized in the following commutative diagram:

$$\begin{array}{ccc} [\mathfrak{a}] \star E \in \mathrm{Pic}(\mathscr{O}_{\mathbf{K}}).E = \mathrm{Ell}^{\mathrm{cm}}_{\mathscr{O}_{\mathbf{K}}} & \xrightarrow{\mathrm{red}_{\mathbf{p}}} & \mathrm{Ell}_\infty \times \prod_{i=1}^{s} \mathrm{Ell}^{\mathrm{ss}}_{p_i} \\ \Big\downarrow \iota & & \Big\downarrow \psi \\ [\iota(t_{\mathrm{f}}^{-1})] \in \mathbf{T}_\iota(\mathbb{Q}) \backslash \mathbf{T}_\iota(\mathbb{A}) / \mathbf{T}_\iota(\mathbb{R}) \mathbf{T}_\iota(\widehat{\mathbb{Z}}) & \longrightarrow & \mathbf{G}(\mathbb{Q}) \backslash \mathbf{G}(\mathbb{A}) / K_\infty K_{\mathrm{f}}. \end{array}$$

Here, the bottom arrow is given by mapping $[\iota(t)]$ to $[\iota(t)\mathrm{g}_E]$ seen as an element in the double quotient on the right. This discussion reduces Theorem 1.3 to considering the behavior of sets of the form $[\iota(\mathbf{T}_{\mathbf{K}}(\mathbb{A}))\mathrm{g}_E]$ as the discriminant of $\mathbf{K}$ goes to negative infinity.

1.3. Equidistribution of diagonal torus orbits. By the reduction step in the previous section, the proof of Theorem 1.3 is a direct consequence of a general equidistribution theorem. To state it in full, we (re-)introduce some notation.

Let $\mathbf{B}_i$ for $0 \leq i \leq s$ be finitely many distinct rational quaternion algebras. We denote by $\mathbf{G}_i = \mathbf{PB}_i^\times$ the associated projective group of units and set

$$\mathbf{G} = \prod_{i=0}^{s} \mathbf{G}_i \quad \text{and} \quad [\mathbf{G}] = \mathbf{G}(\mathbb{Q})\backslash\mathbf{G}(\mathbb{A}).$$

Furthermore, we fix for each $i \in \{0, \dots, s\}$ a compact open subgroup $K_{\mathrm{f},i} < \mathbf{G}_i(\mathbb{A}_\mathrm{f})$ and define

$$K_\mathrm{f} = \prod_i K_{\mathrm{f},i} \text{ and } [\mathbf{G}]_{K_\mathrm{f}} = [\mathbf{G}]/K_\mathrm{f}. \tag{1.2}$$

By a theorem of Borel and Harish-Chandra [4], the homogeneous space $[\mathbf{G}]$ comes with a Haar probability measure which we denote by dg. It induces a probability measure on $[\mathbf{G}]_{K_\mathrm{f}}$ (by restriction to the continuous right K_f-invariant functions on $[\mathbf{G}]$) which we also denote by dg for simplicity.

1.3.1. Toral packets and discriminants. For each index $i \in \{0, \dots, s\}$ we let ι_i be an embedding of a quadratic field $\mathbf{K}$ (possibly a real quadratic field) into the quaternion algebra $\mathbf{B}_i(\mathbb{Q})$. We thus obtain an induced morphism of $\mathbb{Q}$-algebraic groups

$$\iota_i : \mathbf{T}_\mathbf{K} \to \mathbf{G}_i$$

and a diagonal morphism

$$\iota : \mathbf{T}_\mathbf{K} \to \mathbf{G}.$$

We denote its image by

$$\mathbf{T}_\iota = \{(\iota_0(t), \dots, \iota_s(t)) : t \in \mathrm{Res}_{\mathbf{K}/\mathbb{Q}}(\mathbb{G}_m)/\mathbb{G}_m\}. \tag{1.3}$$

For $\mathrm{g} = (g_0, \dots, g_s)$ in $\mathbf{G}(\mathbb{A})$ and a tuple $\iota = (\iota_0, \dots, \iota_s)$ of embeddings as above, we denote by

$$[\mathbf{T}_\iota \mathrm{g}] = \mathbf{G}(\mathbb{Q})\backslash\mathbf{G}(\mathbb{Q})\mathbf{T}_\iota(\mathbb{A})\mathrm{g} \subset [\mathbf{G}]$$

the associated (compact) toral packet and by $[\mathbf{T}_\iota \mathrm{g}]_{K_\mathrm{f}}$ its projection to $[\mathbf{G}]_{K_\mathrm{f}}$.

The arithmetic complexity of the toral packet $[\mathbf{T}_\iota \mathrm{g}]$ is measured using the notion of *discriminant*; in the present case we define the discriminant as

$$\mathrm{disc}([\mathbf{T}_\iota \mathrm{g}]) = \min_{i=0,\dots,s} \mathrm{disc}([\mathbf{T}_{\iota_i} g_i]), \tag{1.4}$$

where $[\mathbf{T}_{\iota_i} g_i]$ is the projection of $[\mathbf{T}_\iota \mathrm{g}]$ to the i-th factor $[\mathbf{G}_i]$ and the discriminant $\mathrm{disc}([\mathbf{T}_{\iota_i} g_i])$ is defined in [18, Section 4].

Remark 1.7. In the context of Theorem 1.3 and in view of Section 1.2, the above discriminant of a toral packet $[\mathbf{T}_\iota \mathrm{g}]$ with associated field $\mathbf{K}$ is comparable to $|\mathrm{disc}(\mathbf{K})|$ and the terms on the right-hand side of (1.4) are roughly the same size.

1.3.2. The main theorem. We are now able to formulate the dynamical input for Theorem 1.3, which is of independent interest.

Theorem 1.8 (Equidistribution of diagonal torus orbits). *Let q_1, q_2 be two distinct odd primes. Let $\mathbf{T}_n = \mathbf{T}_{\iota_n} < \mathbf{G}$ for $n \geq 1$ be a sequence of tori as in* (1.3) *with underlying fields $\mathbf{K}_n$ such that q_1 and q_2 both split in $\mathbf{K}_n$ for every n. For any $n \geq 1$ let $\mathrm{g}_n \in \mathbf{G}(\mathbb{A})$. Let $K_\mathrm{f} < \mathbf{G}(\mathbb{A}_\mathrm{f})$ be a compact open subgroup as in* (1.2)*. We assume that for every $i = 0, \dots, s$ the reduced norm $\mathrm{Nr}_{\mathbf{B}_i}$ induces a surjective map*

$$\mathrm{Nr}_{\mathbf{B}_i} : K_{\mathrm{f},i} \twoheadrightarrow \widehat{\mathbb{Z}}^\times \big/ (\widehat{\mathbb{Z}}^\times)^2. \tag{1.5}$$

If $\mathrm{disc}([\mathbf{T}_n \mathrm{g}_n]) \to \infty$ as $n \to \infty$ the sequence of packets $[\mathbf{T}_n \mathrm{g}_n]_{K_\mathrm{f}}$ equidistributes on $[\mathbf{G}]_{K_\mathrm{f}}$. That is, for any K_f-invariant function $f \in \mathcal{C}_c([\mathbf{G}])$ we have

$$\int_{[\mathbf{T}_n]} f(t\,\mathrm{g}_n)\ \mathrm{d}t \to \int_{[\mathbf{G}]} f(\mathrm{g})\,\mathrm{d}\mathrm{g}$$

as $n \to \infty$, where the left-hand side denotes the integral with respect to the Haar probability measure.

Remark 1.9. If $\mathbf{K}_n$ is a real quadratic field for every n, the condition that q_2 splits in $\mathbf{K}_n$ can be omitted as the "infinite place" already splits in $\mathbf{K}_n$.

Remark 1.10. Condition (1.5) is in particular satisfied if $K_{\mathrm{f},i} = \mathrm{P}\widehat{\mathcal{O}_i}^\times$ for an Eichler order $\mathcal{O}_i$ in $\mathbf{B}_i(\mathbb{Q})$ – see also Section 9.3 for this well-known fact.

The proof of Theorem 1.8 is a consequence of the classification of joinings of higher rank diagonalizable actions by Einsiedler and Lindenstrauss [16] as formulated in Theorem 8.4. For this, the splitting assumption is crucial. Such an assumption is commonly called a *Linnik-type condition* and imposing two such splitting conditions gives rise to higher-rank diagonalizable acting groups. It is reasonable to expect that Theorems 8.4, 1.8 and 1.3 remain true without this assumption (as is the case for a single factor). However, a proof without this assumption would require a completely different argument.

Remark 1.11. In the case of two factors ($s = 2$ in our notations), Valentin Blomer and Farrell Brumley have recently developed a proof of Theorem 1.3 which is conditional on the Generalized Riemann Hypothesis but does not require any splitting assumption. As expected, the methods are entirely different from ours and build on the evaluation of fractional moments of L-functions in the spirit of [33, 40].

The joinings classification [16] allows us to show that any weak*-limit of the measures on the packets $[\mathbf{T}_n \mathrm{g}_n]$ is invariant under the image of the simply connected cover of $\mathbf{G}$ in $\mathbf{G}(\mathbb{A})$. Thus, Theorem 1.8 is reduced to the verification of equidistribution for functions in the character spectrum. Under assumption (1.5), the character spectrum on $[\mathbf{G}]_{K_\mathrm{f}}$ is trivial and hence equidistribution holds. In Corollary 10.4, we provide an equivalent condition to equidistribution for a general compact open subgroup K_f under the assumption that the underlying quadratic fields $\mathbf{K}_n$ for $n \geq 1$ do not belong to a finite set of exceptional fields determined by K_f.

Remark 1.12. As already pointed out above, Theorem 1.8 is a rather direct application of the classification of joinings of higher rank diagonalizable actions due to Einsiedler and Lindenstrauss [16]. There is by now a number of works building on this deep and powerful result, for instance [1–3, 30]. As far as we know, the deepest of these applications is the work of Khayutin [29] who made striking progress on the mixing conjecture by Venkatesh and the third named author (see [22]).

1.4. Structure of the paper. As this article brings together two different areas of research from dynamics and number theory, the authors have put an effort into making it accessible to both of these communities. In particular, most of the material discussed in Sections 3, 4 and 5 will probably be considered standard by many number theorists but we hope this will be helpful to dynamicists. As explained above, the main theorem (Theorem 1.3) follows from Theorem 1.8 which is an equidistribution result of adelic toral orbits. Therefore, we first need to describe the objects above in adelic terms. In Section 3 we give an adelic description of the set of complex elliptic curves. In Section 4 we describe adelically the complex multiplication curves, the action of the Picard group on them, and the reduction map red_∞. In Section 5 we describe adelically the set of the supersingular elliptic curves together with a natural measure on them, the associated reduction map and its compatibility with the Picard group action. Then, in Section 6 we combine the result of the previous sections to show compatibility between the reductions maps at different primes. This enables us to derive Theorem 1.3 from Theorem 1.8 in Section 7. The proof of Theorem 1.8 is then done in two steps: In Section 8 we show that the limiting measure of the toral orbits is invariant under the image of the simply-connected cover and in Section 9 we show that equidistribution holds for K_{f}-invariant functions. Finally, in Section 10 we discuss further possible strengthenings of our main results.

2. Notations and background

If E/k is an elliptic curve defined over a field k, we will in general see it as defined over an algebraic closure $\overline{k}$. In particular, its ring of endomorphism $\mathrm{End}(E)$ is the ring for $E/\overline{k}$ and likewise for the set of isogenies $\mathrm{Hom}(E, E')$ (plus the constant zero map) between two elliptic curves E/k and E'/k and similarly for the set of isomorphisms. Also we will usually use the same notation E for an elliptic curve and its isomorphism class.

By $\mathbb{A}$ (resp. $\mathbb{A}_{\mathrm{f}}$) we mean the ring of adeles (resp. finite adeles) over $\mathbb{Q}$ and more generally given a subset S of the set $\mathcal{V}$ of places of $\mathbb{Q}$ we let $\mathbb{Q}_S$ be the restricted product of $\mathbb{Q}_v$ for $v \in S$ with respect to the sequence $(\mathbb{Z}_p)_{p\in S}$. We also write $\mathcal{V}_{\mathrm{f}}$ for the set of finite places (i.e. for the set of rational primes).

For any affine algebraic group G defined over $\mathbb{Q}$, we denote by $\mathrm{G}(\mathbb{A})$ (resp. $\mathrm{G}(\mathbb{A}_{\mathrm{f}})$) the group of its adelic (resp. finite adelic) points and more generally by

$$\mathrm{G}(\mathbb{Q}_S) = \prod_{v\in S}{}' \mathrm{G}(\mathbb{Q}_v)$$

the group of its $\mathbb{Q}_S$-points. In particular, if V is a finite dimensional $\mathbb{Q}$-vector space, we denote the sets of its v-adic points, $\mathbb{Q}_S$-points, finite adelic, and adelic points by

$$V(\mathbb{Q}_v) = V_v = V \otimes_{\mathbb{Q}} \mathbb{Q}_v,$$

$V(\mathbb{Q}_S)$, $V(\mathbb{A}_{\mathrm{f}})$, and $V(\mathbb{A})$, respectively.

We will use this notation also for a number field $\mathbf{K}$ or more generally a finite dimensional $\mathbb{Q}$-algebra. That is, the rings of v-adic, $\mathbb{Q}_S$-, finite adelic, and adelic points of $\mathbf{K}$ will be denoted by $\mathbf{K}_v = \mathbf{K}(\mathbb{Q}_v)$, $\mathbf{K}(\mathbb{Q}_S)$, $\mathbf{K}(\mathbb{A}_\mathrm{f})$, and $\mathbf{K}(\mathbb{A})$, respectively. Furthermore, viewing the multiplicative group $\mathbf{K}^\times$ of $\mathbf{K}$ as a $\mathbb{Q}$-algebraic group (which we also denote by $\mathrm{Res}_{\mathbf{K}/\mathbb{Q}}(\mathbb{G}_m)$), we write $\mathbf{K}_v^\times = \mathbf{K}^\times(\mathbb{Q}_v)$, $\mathbf{K}^\times(\mathbb{Q}_S)$, $\mathbf{K}^\times(\mathbb{A}_\mathrm{f})$, and $\mathbf{K}^\times(\mathbb{A})$, respectively.

2.1. Homogeneous spaces. Equipped with the respective natural topologies, the groups $\mathrm{G}(\mathbb{Q}_v)$,$\mathrm{G}(\mathbb{Q}_S)$, $\mathrm{G}(\mathbb{A}_\mathrm{f})$, and $\mathrm{G}(\mathbb{A})$ are locally compact groups. The group of rational points $\mathrm{G}(\mathbb{Q})$ then embeds discretely in $\mathrm{G}(\mathbb{A})$ via the diagonal embedding. We denote by $[\mathrm{G}]$ the quotient

$$[\mathrm{G}] = \mathrm{G}(\mathbb{Q})\backslash\mathrm{G}(\mathbb{A})$$

and if $K < \mathrm{G}(\mathbb{A})$ is a subgroup, we denote the associated double quotient by

$$[\mathrm{G}]_K = [\mathrm{G}]/K = \mathrm{G}(\mathbb{Q})\backslash\mathrm{G}(\mathbb{A})/K.$$

For $g \in \mathbf{G}(\mathbb{A})$ an element and $A \subset \mathbf{G}(\mathbb{A})$ a subset we denote their images in $[\mathbf{G}]$ or $[\mathbf{G}]/K$ by $[g]$, $[g]_K$ and $[A]$, $[A]_K$, respectively. If the subgroup K is understood, we will sometimes drop the index K from the notation above and just write $[g]$ for the class $[g]_K$.

If G has no non-trivial $\mathbb{Q}$-characters (which will always be the case in this paper), $\mathrm{G}(\mathbb{Q})$ is a lattice in $\mathrm{G}(\mathbb{A})$ [39, Theorem 5.5] and the groups $\mathrm{G}(\mathbb{Q}_v)$, $\mathrm{G}(\mathbb{Q}_S)$, $\mathrm{G}(\mathbb{A}_\mathrm{f})$, and $\mathrm{G}(\mathbb{A})$ are unimodular. In general, we denote by $m_{[\mathrm{G}]}$ (or sometimes simply dg) a $\mathrm{G}(\mathbb{A})$-invariant measure on the quotient $[\mathrm{G}]$ (which is unique up to scaling). If $\mathrm{G}(\mathbb{Q})$ is a lattice in $\mathrm{G}(\mathbb{A})$, we always normalize $m_{[\mathrm{G}]}$ to be a probability measure.

For $K < \mathrm{G}(\mathbb{A})$ a compact subgroup, we write $m_{[\mathrm{G}]_K}$ for the induced measure on $[\mathrm{G}]_K$ which is the restriction of $m_{[\mathrm{G}]}$ to the space of K-invariant continuous functions on $[\mathrm{G}]$ of compact support. This measure on $[\mathrm{G}]_K$ is a probability measure whenever $m_{[\mathrm{G}]}$ is.

Whenever $K_\mathrm{f} < \mathrm{G}(\mathbb{A})$ is a compact open subgroup, we will call

$$\mathrm{G}(\mathbb{Q})\backslash\mathrm{G}(\mathbb{A})/\mathrm{G}(\mathbb{R}) \times K_\mathrm{f}$$

the class set of K_f. This is always a finite set [39, Theorem 5.1].

2.2. Lattices. A lattice L in a finite-dimensional $\mathbb{Q}$-vector space V is a finitely generated $\mathbb{Z}$-module containing a $\mathbb{Q}$-basis of V. We denote by $\mathcal{L}(V)$ the space of all lattices in V. In the following, q will always denote a (finite) prime. A lattice $L_q \subset V_q$ is a finitely generated $\mathbb{Z}_q$-module containing a $\mathbb{Q}_q$-basis of V_q and we denote by $\mathcal{L}(V_q)$ the space of all lattices in V_q. Given $L \in \mathcal{L}(V)$, we write $L_q = L \otimes_\mathbb{Z} \mathbb{Z}_q \in \mathcal{L}(V_q)$ for the closure of L in V_q and moreover $L_S = \prod_{q\in S} L_q$ whenever $S \subset \mathcal{V}_\mathrm{f}$ as well as $\widehat{L} = \prod_q L_q$.

2.2.1. The local-global principle. Let $L_0 \subset V$ by a fixed lattice. The local-global principle for lattices states that the map

$$L \mapsto \widehat{L} = (L_q)_q$$

is a bijection

$$\mathcal{L}(V) \simeq \mathcal{L}(\widehat{V}) := \prod_q{}' \mathcal{L}(V_q).$$

Here, we denote by

$$\prod_q{}' \mathcal{L}(V_q)$$

the set of sequences $(L_q)_q$ of local lattices $L_q \subset V_q$ such that for all but finitely q we have $L_q = (L_0)_q$. Equivalently, $\mathcal{L}(\widehat{V})$ is the set of $\widehat{\mathbb{Z}}$-modules in $\widehat{V}$ commensurable with $\widehat{L_0}$. We remark that the definition of $\mathcal{L}(\widehat{V})$ is independent of the choice of lattice $L_0 \subset V$. The inverse map is given by

$$\widehat{L} = (L_q)_q \mapsto V \cap \widehat{L} := \bigcap_q V \cap L_q \subset V.$$

2.2.2. Interpretation in terms of adelic quotients. Let GL_V denote the general linear group of V. If $V = \mathbb{Q}^n$, we denote this group by GL_n. The group $\mathrm{GL}_V(\mathbb{Q})$ acts transitively on $\mathcal{L}(V)$ and each of the local groups $\mathrm{GL}_V(\mathbb{Q}_q)$ acts transitively on the local space $\mathcal{L}(V_q)$. These local actions induce a transitive action

$$\mathrm{GL}_V(\mathbb{A}_\mathrm{f}) \curvearrowright \mathcal{L}(\widehat{V})$$

and therefore a transitive action $\mathrm{GL}_V(\mathbb{A}_\mathrm{f}) \curvearrowright \mathcal{L}(V)$ by the local-global principle: given an element $g_\mathrm{f} \in \mathrm{GL}_V(\mathbb{A}_\mathrm{f})$ and L a lattice in V, we have

$$g_\mathrm{f}.L = V \cap (g_\mathrm{f}.\widehat{L}).$$

This action is compatible with the classical action $\mathrm{GL}_V(\mathbb{Q}) \curvearrowright \mathcal{L}(V)$: if

$$\delta_\mathrm{f} : \mathrm{GL}_V(\mathbb{Q}) \hookrightarrow \mathrm{GL}_V(\mathbb{A}_\mathrm{f})$$

denotes the diagonal embedding, one has for any lattice L in V and any $g_\mathbb{Q} \in \mathrm{GL}_V(\mathbb{Q})$

$$g_\mathbb{Q}.L = \delta_\mathrm{f}(g_\mathbb{Q}).L.$$

Let $\mathrm{GL}_V(\mathbb{Z})$, $\mathrm{GL}_V(\widehat{\mathbb{Z}})$ be the stabilizers of L_0 under the corresponding actions. It follows that

$$\begin{aligned}\mathcal{L}(V) &\simeq \mathrm{GL}_V(\mathbb{Q})\big/\mathrm{GL}_V(\mathbb{Z}) \simeq \mathrm{GL}_V(\mathbb{A}_\mathrm{f})\big/\mathrm{GL}_V(\widehat{\mathbb{Z}}) \\ &\simeq \mathrm{GL}_V(\mathbb{Q})\backslash\mathrm{GL}_V(\mathbb{Q}) \times \mathrm{GL}_V(\mathbb{A}_\mathrm{f})\big/\mathrm{GL}_V(\widehat{\mathbb{Z}}).\end{aligned}$$

For the last bijection the group $\mathrm{GL}_V(\mathbb{Q})$ is embedded diagonally in $\mathrm{GL}_V(\mathbb{Q}) \times \mathrm{GL}_V(\mathbb{A}_\mathrm{f})$ and the bijection is induced by the map

$$g_\mathbb{Q} g_\mathrm{f} \in \mathrm{GL}_V(\mathbb{Q}) \times \mathrm{GL}_V(\mathbb{A}_\mathrm{f}) \mapsto g_\mathbb{Q}^{-1} g_\mathrm{f}.L_0 \in \mathcal{L}(V).$$

Let $\mathcal{L}(V_\infty)$ be the space of 'real' lattices in $V_\infty = V \otimes_\mathbb{Q} \mathbb{R}$ (i.e. discrete subgroups of maximal rank). We have the identification

$$\mathcal{L}(V_\infty) \simeq \mathrm{GL}_V(\mathbb{R})/\mathrm{GL}_V(\mathbb{Z})$$

and the following identification in terms of adelic groups:

$$\mathcal{L}(V_\infty) \simeq \mathrm{GL}_V(\mathbb{Q})\backslash\mathrm{GL}_V(\mathbb{A})/\mathrm{GL}_V(\widehat{\mathbb{Z}}). \tag{2.1}$$

In the latter, $\mathrm{GL}_V(\mathbb{Q})$ is embedded diagonally in $\mathrm{GL}_V(\mathbb{A})$ and the bijection is induced by the map

$$g_\infty g_\mathrm{f} \in \mathrm{GL}_V(\mathbb{A}) \mapsto g_\infty^{-1} g_\mathrm{f}.L_0 \in \mathcal{L}(V_\infty). \tag{2.2}$$

2.2.3. Commensurability. We recall the following definition.

Definition 2.1. Two lattices $L, L' \in \mathcal{L}(V_\infty)$ are commensurable if there is an integer $n \neq 0$ such that $nL' \subset L$.

For any $L \in \mathcal{L}(V_\infty)$ we denote by

$$L^0 := L \otimes_{\mathbb{Z}} \mathbb{Q}$$

the $\mathbb{Q}$-subspace of V_∞ spanned by L. Then two lattices $L, L' \in \mathcal{L}(V_\infty)$ are commensurable if and only if $L^0 = (L')^0$. Hence, the commensurability class of L is simply the set of lattices in L^0, that is,

$$\mathcal{L}(L^0) = \mathrm{GL}_V(\mathbb{Q}).L.$$

Here, $\mathrm{GL}_V(\mathbb{Q})$ is viewed as a subgroup of $\mathrm{GL}_V(\mathbb{R})$. Alternatively, if $g_\infty \in \mathrm{GL}_V(\mathbb{R})$ is such that $g_\infty^{-1} L_0 = L$, then

$$\mathcal{L}(L^0) = g_\infty^{-1}\mathrm{GL}_V(\mathbb{Q}).L_0 = g_\infty^{-1}\mathrm{GL}_V(\mathbb{A}_{\mathrm{f}}).L_0.$$

In other terms the map (2.2) provides the following identification for the commensurability class of L:

$$\mathcal{L}(L^0) \simeq \mathrm{GL}_V(\mathbb{Q})\backslash\mathrm{GL}_V(\mathbb{Q})g_\infty\mathrm{GL}_V(\mathbb{A}_{\mathrm{f}})/\mathrm{GL}_V(\widehat{\mathbb{Z}}). \tag{2.3}$$

By the set on the right-hand side we mean the image under the quotient map to (2.1) of the set $\mathrm{GL}_V(\mathbb{Q})\backslash\mathrm{GL}_V(\mathbb{Q})g_\infty\mathrm{GL}_V(\mathbb{A}_{\mathrm{f}})$. Note that the copies of $\mathrm{GL}_V(\mathbb{Q})$ in (2.3) are embedded differently in $\mathrm{GL}_V(\mathbb{A})$, the left copy is embedded diagonally while the right copy is a priori embedded in $\mathrm{GL}_V(\mathbb{R})$. However, the presence of $\mathrm{GL}_V(\mathbb{A}_{\mathrm{f}})$ allows us to take $\mathrm{GL}_V(\mathbb{Q})$ diagonally embedded in either case.

Remark 2.2. This is only interesting for the place $v = \infty$; the lattices in $\mathcal{L}(V)$ or $\mathcal{L}(V_p)$ are all commensurable.

2.3. Quadratic fields and tori. In this paper, $\mathbf{K}$ will usually denote a quadratic extension of $\mathbb{Q}$ (in Sections 4–7 always imaginary). We denote by $\mathrm{Tr}_{\mathbf{K}}$ and $\mathrm{Nr}_{\mathbf{K}}$ the trace and norm on $\mathbf{K}$ and denote in the same way the natural extensions to $\mathbf{K}_v$, $\mathbf{K}(\mathbb{Q}_S)$, $\mathbf{K}(\mathbb{A}_{\mathrm{f}})$ and $\mathbf{K}(\mathbb{A})$. Recall that we view the multiplicative group $\mathbf{K}^\times$ of $\mathbf{K}$ as a $\mathbb{Q}$-algebraic group (which is $\mathrm{res}_{\mathbf{K}/\mathbb{Q}}\mathbb{G}_m$). We will usually denote the projective group by

$$\mathbf{T}_{\mathbf{K}} = \mathrm{Res}_{\mathbf{K}/\mathbb{Q}}(\mathbb{G}_m)/\mathbb{G}_m.$$

2.3.1. Quadratic orders. We write $\mathscr{O}_{\mathbf{K}}$ for the ring of integer of $\mathbf{K}$. Recall that a subring $\mathscr{O} \subset \mathbf{K}$ is an order if $\mathscr{O}$ is a $\mathbb{Z}$-lattice in $\mathbf{K}$. It follows that $\mathscr{O} \subset \mathscr{O}_K$ and that there is a unique integer $c = c(\mathscr{O}) > 0$ (the *conductor of* $\mathscr{O}$) such that

$$\mathscr{O} = \mathbb{Z} + c\mathscr{O}_{\mathbf{K}}.$$

The discriminant of $\mathscr{O}$ is $\mathrm{disc}(\mathscr{O}) = \det(\mathrm{Tr}_{\mathbf{K}}(e_i e_j))_{i,j=1,2}$, where (e_1, e_2) is any $\mathbb{Z}$-basis of $\mathscr{O}$. One has

$$\mathrm{disc}(\mathscr{O}) = \mathrm{disc}(\mathscr{O}_{\mathbf{K}})c^2.$$

2.4. Quaternion algebras. In this paper $\mathbf{B}$ will usually denote a quaternion algebra over $\mathbb{Q}$ (possibly the *split* quaternion algebra Mat_2 of 2×2 matrices over $\mathbb{Q}$). Given a (possibly empty) finite set of places S of $\mathbb{Q}$ with $|S|$ even, there is up to $\mathbb{Q}$-isomorphism a unique quaternion algebra $\mathbf{B}_S$ ramified exactly at the places in S (see e.g. [50, Theorem 14.6.1]). Any quaternion algebra over $\mathbb{Q}$ is of this form. We say that $\mathbf{B}$ is *definite* if $\mathbf{B}(\mathbb{R})$ is isomorphic to the algebra of Hamiltonian quaternions and otherwise we say that it is indefinite.

Denote by $\mathrm{Tr}_{\mathbf{B}}$ and $\mathrm{Nr}_{\mathbf{B}}$ the (reduced) trace and (reduced) norm on $\mathbf{B}$. Let $\mathbf{B}^0 \subset \mathbf{B}$ be the subspace the quaternions of trace 0 and let $\mathbf{B}^1$ be the group the quaternions of norm 1.

The $\mathbb{Q}$-algebraic group of units $\mathbf{B}^\times$ acts on the $\mathbb{Q}$-space $\mathbf{B}^0$ by conjugation. The image of $\mathbf{B}^\times$ in $\mathrm{GL}_{\mathbf{B}^0}$ is isomorphic to the quotient of $\mathbf{B}^\times$ by its center and is called the projective group of units of $\mathbf{B}$. We denote it by

$$\mathbb{G}_m \backslash \mathbf{B}^\times = \mathbf{PB}^\times.$$

The group $\mathbf{PB}^\times$ is $\mathbb{Q}$-almost simple with trivial center and its simply connected cover is the group of norm one units $\mathbf{B}^1$. These two connected groups are anisotropic over $\mathbb{Q}$ if and only if $\mathbf{B} \neq \mathrm{Mat}_2$.

Notice that the conjugation action preserves the norm form $\mathrm{Nr}_{\mathbf{B}}$ restricted to $\mathbf{B}^0$, therefore $\mathbf{PB}^\times \subset \mathrm{SO}_{\mathrm{Nr}_{\mathbf{B}}|_{\mathbf{B}^0}}$, and since these two groups are connected, we have an isomorphism of $\mathbb{Q}$-groups

$$\mathbf{PB}^\times \cong \mathrm{SO}_{\mathrm{Nr}_{\mathbf{B}}|_{\mathbf{B}^0}},$$

see [49, Chapter I, Theorem 3.3].

Write $\mathbf{G} = \mathbf{PB}^\times$ for simplicity. By the above, the homogeneous space $[\mathbf{G}]$ for the group $\mathbf{G}$ has finite volume (i.e. $\mathbf{G}(\mathbb{Q})$ is a lattice in $\mathbf{G}(\mathbb{A})$). We note that if $\mathbf{B} \neq \mathrm{Mat}_2$, $[\mathbf{G}]$ is in fact compact.

2.4.1. Integral structures. The choice of an order $\mathcal{O} \subset \mathbf{B}(\mathbb{Q})$ defines an integral structure on $\mathbf{G} = \mathbf{PB}^\times$ by setting

$$\mathbf{G}(\mathbb{Z}) = \{g \in \mathbf{G}(\mathbb{Q}) : g\mathcal{O}g^{-1} = \mathcal{O}\}.$$

The integral structure also provides distinguished local and global compact open subgroups, namely, for any prime p the subgroups

$$\mathbf{G}(\mathbb{Z}_p) = \{g \in \mathbf{G}(\mathbb{Q}_p) : g\mathcal{O}_p g^{-1} = \mathcal{O}_p\}$$

and the product

$$\mathbf{G}(\widehat{\mathbb{Z}}) = \prod_p \mathbf{G}(\mathbb{Z}_p) < \mathbf{G}(\mathbb{A}_{\mathrm{f}}).$$

If $\mathbf{B} = \mathrm{Mat}_2$, we will always choose the integral structure defined by $\mathcal{O} = \mathrm{Mat}_2(\mathbb{Z})$. In this case, $\mathbf{G}(\mathbb{Z})$ equals $\mathrm{PGL}_2(\mathbb{Z})$, i.e. the image of $\mathrm{GL}_2(\mathbb{Z})$ in $\mathrm{PGL}_2(\mathbb{Q})$.

2.4.2. Quadratic fields and quaternions. Let us recall that a quadratic number field $\mathbf{K}$ embeds in a quaternion algebra $\mathbf{B}$ if and only if the following local conditions are satisfied:

(i) If $\mathbf{B}$ is definite, then $\mathbf{K}$ is imaginary.

(ii) If p is a ramified prime of $\mathbf{B}$, then p is non-split in $\mathbf{K}$.

This is a consequence of the Hasse-Minkowski theorem applied to the quadratic form $\mathrm{Nr}_{\mathbf{B}}|_{\mathbf{B}^0}$.

Suppose we have such an embedding

$$\iota : \mathbf{K} \hookrightarrow \mathbf{B}.$$

Then we have for any $z \in \mathbf{K}$,

$$\mathrm{Tr}_{\mathbf{B}}(\iota(z)) = \mathrm{Tr}_{\mathbf{K}}(z), \quad \mathrm{Nr}_{\mathbf{B}}(\iota(z)) = \mathrm{Nr}_{\mathbf{K}}(z).$$

The embedding ι also induces an embedding for the multiplicative and projective $\mathbb{Q}$-groups which we denote in the same way by

$$\iota : \mathbf{K}^\times \hookrightarrow \mathbf{B}^\times, \quad \mathbf{T}_{\mathbf{K}} \hookrightarrow \mathbf{G} = \mathbf{PB}^\times.$$

In fact, $\iota(\mathbf{K}^\times) \subset \mathbf{B}^\times$ and $\iota(\mathbf{T}_{\mathbf{K}}) \subset \mathbf{PB}^\times$ are the stabilizers in $\mathbf{B}^\times$ or $\mathbf{PB}^\times$ of the line

$$\mathbb{Q}.\iota(z_0) \subset \mathbf{B}^0(\mathbb{Q}),$$

where $z_0 \in \mathbf{K}$ is any non-zero element with trace 0.

3. Complex elliptic curves

Let Ell_∞ be the set of elliptic curves over $\mathbb{C}$ up to isomorphism. Any elliptic curve E admits a complex uniformization, that is, it is isomorphic as a Riemann surface to a quotient

$$E \simeq \mathbb{C}/\Lambda,$$

where $\Lambda \subset \mathbb{C}$ is a $\mathbb{Z}$-lattice. Conversely, any lattice gives rise to an elliptic curve over $\mathbb{C}$; cf. [43, Chapter 7, Section 2].

Given two elliptic curves $E \simeq \mathbb{C}/\Lambda$, $E' \simeq \mathbb{C}/\Lambda'$, the set of isogenies from E to E' is given by

$$\mathrm{Hom}(E, E') \simeq \{z \in \mathbb{C} : z\Lambda \subset \Lambda'\}.$$

In particular, two curves are isomorphic if and only if $\Lambda' = z\Lambda$ for some $z \in \mathbb{C}^\times$ (i.e. the lattices Λ and Λ' are $\mathbb{C}^\times$-homothetic). Taking $E' = E$ one has

$$\mathrm{End}(E) = \{z \in \mathbb{C} : z\Lambda \subset \Lambda\} \quad \text{and} \quad \mathrm{Aut}(E) = \mathrm{End}(E)^\times.$$

The endomorphism ring $\mathrm{End}(E)$ is either $\mathbb{Z}$ (the generic case) or an order $\mathscr{O}$ in an imaginary quadratic field $\mathbf{K}$. In this last case, one says that E has (exact) complex multiplication by $\mathscr{O}$ and we discuss this further in the next section. In any case we set

$$\mathrm{End}^0(E) = \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q} \subset \mathbb{C}, \quad \mathrm{Aut}^0(E) = \mathrm{End}^0(E)^\times = \mathrm{End}^0(E) \setminus \{0\} \subset \mathbb{C}^\times.$$

Let $\mathscr{L}(\mathbb{C})$ be the space of $\mathbb{Z}$-lattices in $\mathbb{C}$. The map

$$\Lambda \in \mathscr{L}(\mathbb{C}) \mapsto E_\Lambda = \mathbb{C}/\Lambda \tag{3.1}$$

induces a bijection

$$\mathbb{C}^\times \backslash \mathscr{L}(\mathbb{C}) \simeq \mathrm{Ell}_\infty.$$

Furthermore, any $\mathbb{Z}$-lattice in $\mathbb{C}$ is $\mathbb{C}^\times$-homothetic to a lattice of the form

$$\Lambda_z = \mathbb{Z} + \mathbb{Z}\, z$$

for some $z \in \mathbb{H}$, where $\mathbb{H} = \{z \in \mathbb{C} : \Im z > 0\}$ is the upper-half plane. Moreover, two such lattices $\Lambda_z, \Lambda_{z'}$ are homothetic if and only if z, z' are in the same $\mathrm{SL}_2(\mathbb{Z})$-orbit.

From this we obtain the usual identification

$$\mathrm{Ell}_\infty \simeq \mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H} = Y_0(1)$$

of Ell_∞ with the complex points of the modular curve.

In the sequel, we identify $\mathbb{C}$ with the Euclidean plane $\mathbb{R}^2$ by matching the $\mathbb{R}$-basis $(1, \mathrm{i})$ of $\mathbb{C}$ with the canonical basis $((1,0),(0,1))$ of $\mathbb{R}^2$. We denote this identification by

$$\theta_{\mathrm{i}} : \mathbb{C} \simeq \mathbb{R}^2. \tag{3.2}$$

Under this identification, the action of the group $\mathbb{C}^\times \simeq \mathbb{R}_{>0} \times \mathbb{S}^1$ on $\mathbb{C}$ by multiplication corresponds to the standard action of $\mathbb{R}_{>0} \times \mathrm{SO}_2(\mathbb{R})$ on $\mathbb{R}^2$. By (2.1) we have the adelic description

$$\begin{aligned} \mathbb{C}^\times\backslash\mathscr{L}(\mathbb{C}) &\simeq \mathbb{R}_{>0}\mathrm{SO}_2(\mathbb{R})\backslash\mathscr{L}(\mathbb{R}^2) \\ &\simeq \mathrm{GL}_2(\mathbb{Q})\backslash\mathrm{GL}_2(\mathbb{A})/\mathbb{R}_{>0}\mathrm{SO}_2(\mathbb{R})\mathrm{GL}_2(\widehat{\mathbb{Z}}). \end{aligned} \tag{3.3}$$

Since $\mathbb{A}^\times = \mathbb{Q}^\times\mathbb{R}_{>0}\widehat{\mathbb{Z}}^\times$, it follows that $\mathbb{C}^\times\backslash\mathscr{L}(\mathbb{C})$ is expressed as an adelic quotient of the projective group

$$\begin{aligned} \mathbb{C}^\times\backslash\mathscr{L}(\mathbb{C}) &\simeq \mathrm{PSO}_2(\mathbb{R})\backslash\mathrm{PGL}_2(\mathbb{R})/\mathrm{PGL}_2(\mathbb{Z}) \\ &\simeq \mathrm{PGL}_2(\mathbb{Q})\backslash\mathrm{PGL}_2(\mathbb{A})/\mathrm{PSO}_2(\mathbb{R})\mathrm{PGL}_2(\widehat{\mathbb{Z}}). \end{aligned}$$

Recall here from Section 2.4.1 that $\mathrm{PGL}_2(\widehat{\mathbb{Z}})$ denotes the image of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ in $\mathrm{PGL}_2(\mathbb{A}_{\mathrm{f}})$ under the natural projection. We denote the resulting identification

$$\psi_\infty : \mathrm{Ell}_\infty \simeq \mathrm{PGL}_2(\mathbb{Q})\backslash\mathrm{PGL}_2(\mathbb{A})/\mathrm{PSO}_2(\mathbb{R})\mathrm{PGL}_2(\widehat{\mathbb{Z}}) \tag{3.4}$$

3.1. Isogenies. Given $E = \mathbb{C}/\Lambda$ a complex elliptic curve, let

$$Y(E) = \{[E'] : \mathrm{Hom}(E', E) \neq 0\} \subset \mathrm{Ell}_\infty$$

be the set of isomorphism classes of complex elliptic curves E' isogenous to E (recall that being isogenous is an equivalence relation).

Given $E' \simeq \mathbb{C}/\Lambda'$ isogenous to E, there is $z \in \mathbb{C}^\times$ such that $z\Lambda' \subset \Lambda$. In other terms, $z\Lambda'$ is commensurable with Λ; cf. Section 2.2.3. Conversely, if Λ' is commensurable with Λ, then $E' \simeq \mathbb{C}/\Lambda'$ is isogenous to E: given $n \neq 0$ such that $n\Lambda' \subset \Lambda$ the map

$$[\times n] : z + \Lambda' \in \mathbb{C}/\Lambda' \mapsto nz + n\Lambda' + \Lambda \in \mathbb{C}/\Lambda$$

gives an isogeny. Therefore, the map (3.1) gives an identification between $Y(E)$ and $\mathbb{C}^\times$-homothety classes of lattices commensurable to Λ. In other words, it induces a bijection

$$Y(E) \simeq \mathbb{C}^\times\backslash\mathbb{C}^\times\mathscr{L}(\Lambda^0).$$

Here, $\Lambda^0 = \Lambda \otimes_{\mathbb{Z}} \mathbb{Q}$, see Section 2.2.3 for the notation. Let $g_\infty \in \mathrm{GL}_2(\mathbb{R})$ be such that $\Lambda = g_\infty^{-1}.\mathbb{Z}^2$. In terms of the identifications (3.3) and (3.4) we have (cf. (2.3))

$$Y(E) \simeq \mathrm{GL}_2(\mathbb{Q})\backslash \mathrm{GL}_2(\mathbb{Q}) g_\infty \mathrm{GL}_2(\mathbb{A}_{\mathrm{f}})/\mathbb{R}_{>0}\mathrm{SO}_2(\mathbb{R})\mathrm{GL}_2(\widehat{\mathbb{Z}}), \tag{3.5}$$

and letting $\overline{g}_\infty$ denote the projection of g_∞ to $\mathrm{PGL}_2(\mathbb{R})$) we obtain

$$\psi_\infty|_{Y(E)} : Y(E) \simeq \mathrm{PGL}_2(\mathbb{Q})\backslash \mathrm{PGL}_2(\mathbb{Q}) \overline{g}_\infty \mathrm{PGL}_2(\mathbb{A}_{\mathrm{f}})/\mathrm{PSO}_2(\mathbb{R})\mathrm{PGL}_2(\widehat{\mathbb{Z}}).$$

Remark 3.1. Since the stabilizer of Λ^0 in $\mathbb{C}^\times$ is $\mathrm{Aut}^0(E)$, we also have

$$Y(E) \simeq \mathrm{Aut}^0(E)\backslash \mathscr{L}(\Lambda^0).$$

4. CM elliptic curves

4.1. Curves with complex multiplication. Recall that given an imaginary quadratic field $\mathbf{K} \subset \mathbb{C}$, a complex elliptic curve $E \simeq \mathbb{C}/\Lambda$ has complex multiplication (CM) by $\mathbf{K}$ if

$$\mathrm{End}^0(E) := \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q} = \mathbf{K} \subset \mathbb{C}.$$

In that case the ring of endomorphisms $\mathrm{End}(E)$ is isomorphic to an order $\mathscr{O}$ in $\mathbf{K}$:

$$\mathrm{End}(E) \simeq \mathscr{O}$$

and one then says that E has CM by $\mathscr{O}$.

We denote by $\mathrm{Ell}^{\mathrm{cm}}_{\mathbf{K}}$ the set of $\mathbb{C}$-isomorphism classes of elliptic curves E with complex multiplication by $\mathbf{K}$ and by $\mathrm{Ell}^{\mathrm{cm}}_D$ or $\mathrm{Ell}^{\mathrm{cm}}_{\mathscr{O}} \subset \mathrm{Ell}^{\mathrm{cm}}_{\mathbf{K}}$ the subset consisting of elliptic curves E with CM by $\mathscr{O}$, where $D = \mathrm{disc}(\mathscr{O})$. We have a decomposition as a disjoint union

$$\mathrm{Ell}^{\mathrm{cm}}_{\mathbf{K}} = \bigsqcup_{\mathscr{O} \subset \mathbf{K}} \mathrm{Ell}^{\mathrm{cm}}_{\mathscr{O}},$$

where $\mathscr{O}$ ranges over all the orders of $\mathbf{K}$.

4.1.1. Explicit description in terms of the complex uniformization. As a general remark, an elliptic curve E given by its complex uniformization $E(\mathbb{C}) = \mathbb{C}/\Lambda$ has CM by an order $\mathscr{O} \subset \mathbf{K}$ if and only if

$$\mathrm{End}(\Lambda) = \{z \in \mathbb{C} : z\Lambda \subset \Lambda\} = \mathscr{O}.$$

An example of such an elliptic curve is given by $E_{\mathscr{O}}(\mathbb{C}) = \mathbb{C}/\mathscr{O}$.

Proposition 4.1. *The map* (3.1) *induces a bijection*

$$\mathrm{Ell}^{\mathrm{cm}}_{\mathbf{K}} \simeq \mathbf{K}^\times\backslash \mathscr{L}(\mathbf{K}),$$

where $\mathscr{L}(\mathbf{K})$ *denotes the set of* $\mathbb{Z}$*-lattices in the* $\mathbb{Q}$*-vector space* $\mathbf{K}$ *as in Section* 2.2*. In particular, all elliptic curves with CM by* $\mathbf{K}$ *are isogenous and for any* $E \in \mathrm{Ell}^{\mathrm{cm}}_{\mathbf{K}}$ *we have*

$$\mathrm{Ell}^{\mathrm{cm}}_{\mathbf{K}} = Y(E).$$

Proof. For any elliptic curve $E \in \mathrm{Ell}^{\mathrm{cm}}_{\mathbf{K}}$ with $E = \mathbb{C}/\Lambda$ the lattice Λ is homothetic to a lattice containing an order $\mathscr{O}$ in $\mathbf{K}$. In particular, the latter is commensurable to $\mathscr{O}$. It follows from Section 3.1 that E is isogenous to $E_{\mathscr{O}}$. Conversely, if a lattice Λ is homothetic to a lattice in $\mathbf{K}$, it has complex multiplication by an order in $\mathbf{K}$. □

4.1.2. The Picard group and its action. We recall the structure of $\mathrm{Ell}^{\mathrm{cm}}_{\mathscr{O}}$ for $\mathscr{O} \subset \mathbf{K}$ an order.

Definition 4.2. A (fractional) proper $\mathscr{O}$-ideal is a lattice $\mathfrak{a} \subset \mathbf{K}$ such that

$$\mathrm{End}(\mathfrak{a}) = \{z \in \mathbf{K} : z\mathfrak{a} \subset \mathfrak{a}\} = \mathscr{O}.$$

We denote the set of proper $\mathscr{O}$-ideals by $\mathscr{I}(\mathscr{O}) \subset \mathscr{L}(\mathbf{K})$.

The group $\mathbf{K}^\times$ acts on $\mathscr{I}(\mathscr{O})$ by multiplication and from Definition 4.2 and the proof of Proposition 4.1, the restriction of the map (3.1) to $\mathscr{I}(\mathscr{O})$ yields the bijection

$$\mathrm{Ell}^{\mathrm{cm}}_{\mathscr{O}} \simeq \mathbf{K}^\times \backslash \mathscr{I}(\mathscr{O}). \tag{4.1}$$

Let us recall that $\mathscr{O}$ is a Gorenstein ring, so the set of proper $\mathscr{O}$-ideals $\mathscr{I}(\mathscr{O})$ is exactly the set of $\mathscr{O}$-modules in $\mathbf{K}$ which are locally free of rank 1 and so invertible [19, Section 2.3]. The set $\mathscr{I}(\mathscr{O})$ is therefore stable under multiplication of $\mathscr{O}$-ideals and forms a commutative group whose neutral element is $\mathscr{O}$.

Definition 4.3. The quotient $\mathrm{Pic}(\mathscr{O}) = \mathbf{K}^\times \backslash \mathscr{I}(\mathscr{O})$ is called the *Picard group* of $\mathscr{O}$.

It is a very classical result that $\mathrm{Pic}(\mathscr{O})$ is a finite group, see for example [12, Theorems 2.13 and 7.7]. The set $\mathrm{Ell}^{\mathrm{cm}}_{\mathscr{O}}$ is in bijection with $\mathrm{Pic}(\mathscr{O})$; it is not a group a priori but comes very close being one.

Proposition 4.4. *The set* $\mathrm{Ell}^{\mathrm{cm}}_{\mathscr{O}}$ *is endowed with a simply transitive action of the Picard group* $\mathrm{Pic}(\mathscr{O})$.

Proof. The action of the Picard group is defined as follows. Let $E \in \mathrm{Ell}^{\mathrm{cm}}_{\mathscr{O}}$ and by (4.1) let $\Lambda \in \mathscr{I}(\mathscr{O})$ such that $E(\mathbb{C}) \simeq \mathbb{C}/\Lambda$. Furthermore, let $\mathfrak{a}$ be a proper $\mathscr{O}$-ideal and write $\mathfrak{a}^{-1} \in \mathscr{I}(\mathscr{O})$ for its inverse. The set $\mathfrak{a}^{-1}\Lambda$ is in $\mathscr{I}(\mathscr{O})$ and hence is a lattice in $\mathbb{C}$ satisfying $\mathrm{End}(\mathfrak{a}^{-1}\Lambda) = \mathscr{O}$. It follows that

$$\mathfrak{a} \star E := \mathbb{C}/\mathfrak{a}^{-1}\Lambda$$

has CM by $\mathscr{O}$ and it is easy to check that its isomorphism class depends only on the classes of $\mathfrak{a}$ and E. This action is transitive since $\mathfrak{a} \star E_{\mathscr{O}} = \mathbb{C}/\mathfrak{a}^{-1}$ and simply transitive by (4.1). □

Remark 4.5. For the sequel it will be useful to take note of the isomorphism of $\mathscr{O}$-modules

$$\mathrm{Hom}(\mathfrak{a} \star E, E) = \{z \in \mathbb{C} : z\mathfrak{a}^{-1}\Lambda \subset \Lambda\} = \mathfrak{a},$$

where $\mathscr{O}$ acts on the left on $\mathrm{Hom}(\mathfrak{a} \star E, E)$ via postcomposition by isogenies of E. Conversely, one verifies that the map $u + \mathfrak{a}^{-1}\Lambda \mapsto [z \in \mathfrak{a} \to zu + \Lambda]$ induces a bijection

$$\mathrm{Hom}_{\mathscr{O}}(\mathfrak{a}, E) \simeq \mathfrak{a} \star E(\mathbb{C}),$$

where $\mathrm{Hom}_{\mathscr{O}}$ denotes the $\mathscr{O}$-module homomorphisms.

4.1.3. The Galois action. Any elliptic curve E with CM by $\mathscr{O}$ has a model defined over the ring class field $\mathbf{H}_{\mathscr{O}}$ and the j-invariant satisfies $\mathbf{K}(j(E)) = \mathbf{H}_{\mathscr{O}}$. In addition, the Galois and

the Picard actions are compatible in the sense that

$$[\mathfrak{a} \star E] = [E^\sigma],$$

where $[\mathfrak{a}] \in \mathrm{Pic}(\mathscr{O}_{\mathbf{K}})$ and

$$\sigma = \left(\frac{\mathbf{H}_{\mathscr{O}}/\mathbf{K}}{[\mathfrak{a}]}\right)$$

is the Artin symbol from class field theory. See [42, p. 293] for a proof when $\mathscr{O} = \mathscr{O}_{\mathbf{K}}$ is the full ring of integers and [47, Section 22] in general.

4.2. The set of CM elliptic curves as an adelic quotient. We now give an adelic description of the action

$$\mathrm{Pic}(\mathscr{O}) \curvearrowright \mathrm{Ell}^{\mathrm{cm}}_{\mathscr{O}} \subset \mathrm{Ell}^{\mathrm{cm}}_{\mathbf{K}} \subset \mathrm{Ell}_{\infty}.$$

Let $\mathrm{GL}_{\mathbf{K}} = \mathrm{End}_{\mathbb{Q}}(\mathbf{K})^\times$ be the linear group of the $\mathbb{Q}$-vector space $\mathbf{K}$. We have an injection $\mathbf{K}^\times \hookrightarrow \mathrm{GL}_{\mathbf{K}}(\mathbb{Q})$ via the multiplicative action of $\mathbf{K}^\times$ on $\mathbf{K}$. By Proposition 4.1 and the local-global principle for lattices, we have

$$\begin{aligned}\mathrm{Ell}^{\mathrm{cm}}_{\mathbf{K}} &\simeq \mathbf{K}^\times\backslash\mathscr{L}(\mathbf{K}) \simeq \mathbf{K}^\times\backslash\mathrm{GL}_{\mathbf{K}}(\mathbb{A}_{\mathrm{f}}).\widehat{\mathscr{O}} \\ &\simeq \mathbf{K}^\times\backslash\mathrm{GL}_{\mathbf{K}}(\mathbb{A}_{\mathrm{f}})/\mathrm{GL}_{\mathbf{K}}(\widehat{\mathbb{Z}}).\end{aligned}$$

Here $\mathrm{GL}_{\mathbf{K}}(\widehat{\mathbb{Z}})$ is the stabilizer of $\widehat{\mathscr{O}}$ under the action of $\mathrm{GL}_{\mathbf{K}}(\mathbb{A}_{\mathrm{f}})$ on $\mathbf{K}(\mathbb{A}_{\mathrm{f}})$.

By Proposition 4.4 we have that the inclusion

$$\mathrm{Ell}^{\mathrm{cm}}_{\mathscr{O}} \subset \mathrm{Ell}^{\mathrm{cm}}_{\mathbf{K}}$$

corresponds to the homothety classes of lattices which are proper $\mathscr{O}$-ideals:

$$\mathbf{K}^\times\backslash\mathscr{I}(\mathscr{O}) \subset \mathbf{K}^\times\backslash\mathscr{L}(\mathbf{K}).$$

As already discussed the proper $\mathscr{O}$-ideals are precisely the locally free ones: for any $\mathfrak{a} \in \mathscr{I}(\mathscr{O})$ there is $t_{\mathrm{f}} \in \mathbf{K}^\times(\mathbb{A}_{\mathrm{f}})$ such that

$$\mathfrak{a} = \mathbf{K} \cap \widehat{\mathfrak{a}}, \quad \text{where } \widehat{\mathfrak{a}} = t_{\mathrm{f}}\widehat{\mathscr{O}}. \tag{4.2}$$

Conversely, for any $\widehat{\mathfrak{a}} = t_{\mathrm{f}}\widehat{\mathscr{O}}$ formula (4.2) defines a proper $\mathscr{O}$-ideal. Moreover, t_{f} is uniquely defined modulo $\widehat{\mathscr{O}}^\times$ and therefore

$$\mathbf{K}^\times\backslash\mathscr{I}(\mathscr{O}) = \mathrm{Pic}(\mathscr{O}) \simeq \mathbf{K}^\times\backslash\mathbf{K}^\times(\mathbb{A}_{\mathrm{f}})/\widehat{\mathscr{O}}^\times,$$

which gives an adelic description of the group $\mathrm{Pic}(\mathscr{O})$.

If one prefers to think in terms of homothety classes of lattices, one has

$$\mathbf{K}^\times\backslash\mathscr{I}(\mathscr{O}) \simeq \mathbf{K}^\times\backslash\mathbf{K}^\times(\mathbb{A}_{\mathrm{f}}).\widehat{\mathscr{O}} \simeq \mathbf{K}^\times\backslash\mathbf{K}^\times(\mathbb{A}_{\mathrm{f}}).\mathrm{GL}_{\mathbf{K}}(\widehat{\mathbb{Z}})/\mathrm{GL}_{\mathbf{K}}(\widehat{\mathbb{Z}}).$$

Indeed, note that by definition of $\mathrm{GL}_{\mathbf{K}}(\widehat{\mathbb{Z}})$ the stabilizer of $\widehat{\mathscr{O}}$ is the stabilizer of the identity coset in $\mathrm{GL}_{\mathbf{K}}(\mathbb{A}_{\mathrm{f}}) \,/\, \mathrm{GL}_{\mathbf{K}}(\widehat{\mathbb{Z}})$. It is equal to $\mathbf{K}^\times(\mathbb{A}_{\mathrm{f}}) \cap \mathrm{GL}_{\mathbf{K}}(\widehat{\mathbb{Z}}) = \widehat{\mathscr{O}}^\times$. Thus, the two descriptions are compatible:

$$\mathbf{K}^\times\backslash\mathbf{K}^\times(\mathbb{A}_{\mathrm{f}}).\mathrm{GL}_{\mathbf{K}}(\widehat{\mathbb{Z}})/\mathrm{GL}_{\mathbf{K}}(\widehat{\mathbb{Z}}) \simeq \mathbf{K}^\times\backslash\mathbf{K}^\times(\mathbb{A}_{\mathrm{f}})/\widehat{\mathscr{O}}^\times.$$

To summarize, we have the identifications

$$\mathrm{Ell}_{\mathscr{O}}^{\mathrm{cm}} \simeq \mathbf{K}^\times\backslash\mathbf{K}^\times(\mathbb{A}_\mathrm{f})/\widehat{\mathscr{O}}^\times \simeq \mathrm{Pic}(\mathscr{O}) \tag{4.3}$$

$$\simeq \mathbf{K}^\times\backslash\mathbf{K}^\times(\mathbb{A}_\mathrm{f}).\mathrm{GL}_{\mathbf{K}}(\widehat{\mathbb{Z}})/\mathrm{GL}_{\mathbf{K}}(\widehat{\mathbb{Z}}) \tag{4.4}$$

and the action of $\mathrm{Pic}(\mathscr{O})$ on $\mathrm{Ell}_{\mathscr{O}}^{\mathrm{cm}}$ is realized as follows:

Proposition 4.6. *If $\mathfrak{a} \in \mathscr{I}(\mathscr{O})$ and $t_\mathrm{f} \in \mathbf{K}^\times(\mathbb{A}_\mathrm{f})$ are related by* (4.2)*, the isomorphism class of $\mathfrak{a} \star E_{\mathscr{O}}$ is represented in* (4.3) *resp.* (4.4) *by the class*

$$[t_\mathrm{f}^{-1}] = \mathbf{K}^\times t_\mathrm{f}^{-1}\widehat{\mathscr{O}}^\times \quad \textit{resp.} \quad \mathbf{K}^\times t_\mathrm{f}^{-1}.\mathrm{GL}_{\mathbf{K}}(\widehat{\mathbb{Z}}).$$

Proof. From the proof of Proposition 4.4 it follows that the homothety class of lattices corresponding to $\mathfrak{a} \star E_{\mathscr{O}}$ under the identification $\mathbb{C}^\times\backslash\mathscr{L}(\mathbb{C}) \simeq \mathrm{Ell}_\infty$ is given by the lattice $\mathfrak{a}^{-1} \in \mathscr{I}(\mathscr{O}) \subset \mathscr{L}(\mathbf{K})$. The statement is thus a direct consequence of (4.2). □

4.3. The map red_∞. In this subsection we describe the map red_∞ adelically. Let us recall that

$$\begin{aligned}\mathrm{Ell}_\infty &\simeq \mathrm{GL}_2(\mathbb{Q})\backslash\mathrm{GL}_2(\mathbb{A})/\mathbb{R}_{>0}\mathrm{SO}_2(\mathbb{R})\mathrm{GL}_2(\widehat{\mathbb{Z}})\\ &\simeq \mathrm{PGL}_2(\mathbb{Q})\backslash\mathrm{PGL}_2(\mathbb{A})/\mathrm{PSO}_2(\mathbb{R})\mathrm{PGL}_2(\widehat{\mathbb{Z}}).\end{aligned}$$

As we have seen, the elliptic curves with CM by $\mathbf{K}$ correspond to the isogeny class of $E_{\mathscr{O}}$ and to the sublattices of $\mathbf{K}$

$$\mathrm{Ell}_{\mathbf{K}}^{\mathrm{cm}} = Y(E_{\mathscr{O}}) \simeq \mathbb{C}^\times\backslash\mathbb{C}^\times\mathscr{L}(\mathbf{K}), \tag{4.5}$$

where $\mathbf{K}$ is viewed as a $\mathbb{Q}$-vector space of dimension 2 inside the $\mathbb{R}$-vector space $\mathbb{C} = \mathbb{R}^2$ and the sublattices of $\mathbf{K}$ are the images of one of them (say $\mathscr{O}$) under all the invertible $\mathbb{Q}$-linear maps on that space (see Section 2.2.3). Concretely, we choose a $\mathbb{Z}$-basis $\mathscr{O} = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$. This choice gives isomorphisms

$$\theta : \mathscr{O} \to \mathbb{Z}^2, \quad \theta : \mathbf{K} \to \mathbb{Q}^2$$

as well as $\mathbb{Z}$ and $\mathbb{Q}$-algebra embeddings

$$\iota : \mathscr{O} = \mathrm{End}(\mathscr{O}) \hookrightarrow \mathcal{O} := \mathrm{Mat}_2(\mathbb{Z}), \quad \iota : \mathbf{K} = \mathrm{End}(\mathscr{O})^0 \hookrightarrow \mathbf{B} := \mathrm{Mat}_2(\mathbb{Q})$$

satisfying:

- Compatibility: for all $z \in \mathbf{K}^\times$ and $w \in \mathbf{K}$

$$\theta(z.w) = \iota(z)(\theta(w)).$$

- Optimality: one has

$$\iota(\mathbf{K}) \cap \mathcal{O} = \iota(\mathscr{O}). \tag{4.6}$$

Restricting ι to $\mathbf{K}^\times$, we obtain an embedding of $\mathbb{Q}$-algebraic groups

$$\iota : \mathrm{Res}_{\mathbf{K}/\mathbb{Q}}(\mathbb{G}_m) \hookrightarrow \mathrm{GL}_2,$$

where we recall that we view $\mathbf{K}^\times = \mathrm{Res}_{\mathbf{K}/\mathbb{Q}}(\mathbb{G}_m)$. We denote the image by $\iota(\mathbf{K}^\times)$ for which (4.6) translates into

$$\iota(\mathbf{K}^\times)(\mathbb{A}_\mathrm{f}) \cap \mathrm{GL}_2(\widehat{\mathbb{Z}}) = \iota(\widehat{\mathscr{O}}^\times).$$

Remark 4.7. Note that if one chooses another basis, then the induced embedding ι' will be $\mathrm{GL}_2(\mathbb{Q})$-conjugate to ι and in particular the corresponding torus $\iota'(\mathrm{Res}_{\mathbf{K}/\mathbb{Q}}(\mathbb{G}_m))$ will be $\mathrm{GL}_2(\mathbb{Q})$-conjugate to $\iota(\mathrm{Res}_{\mathbf{K}/\mathbb{Q}}(\mathbb{G}_m))$.

Let $g_\infty \in \mathrm{GL}_2(\mathbb{R})$ be the $\mathbb{R}$-linear extension of θ, where we have $\mathbf{K} \otimes_\mathbb{Q} \mathbb{R} = \mathbb{C} = \mathbb{R}^2$ under (3.2). We have

$$\iota(\mathbf{K}^\times)(\mathbb{R}) = g_\infty \mathbb{R}_{>0} \mathrm{SO}_2(\mathbb{R}) g_\infty^{-1} \tag{4.7}$$

as well as $\mathbf{K} = g_\infty \mathbb{Q}^2$. As of (4.5) we obtain by applying the characterization of commensurability classes in (2.3) (see also (3.5))

$$\mathrm{Ell}^{\mathrm{cm}}_{\mathbf{K}} \simeq \mathrm{GL}_2(\mathbb{Q}) \backslash \mathrm{GL}_2(\mathbb{Q}) g_\infty \mathrm{GL}_2(\mathbb{A}_\mathrm{f}) / \mathbb{R}_{>0} \mathrm{SO}_2(\mathbb{R}) \mathrm{GL}_2(\widehat{\mathbb{Z}}) \tag{4.8}$$

by identifying elliptic curves over $\mathbb{C}$ with homothety classes of lattices $\mathbb{C}$. The set $\mathrm{Ell}^{\mathrm{cm}}_{\mathscr{O}}$ correspond under this identification to the homothety classes of the lattices

$$g_\infty^{-1}.\iota(\mathbf{K}^\times)(\mathbb{A}_\mathrm{f}).\mathbb{Z}^2$$

by the adelic description in Section 4.2. As a subset of (4.8), $\mathrm{Ell}^{\mathrm{cm}}_{\mathscr{O}}$ corresponds to

$$\mathrm{GL}_2(\mathbb{Q}) g_\infty \iota(\mathbf{K}^\times)(\mathbb{A}_\mathrm{f}) \mathbb{R}_{>0} \mathrm{SO}_2(\mathbb{R}) \mathrm{GL}_2(\widehat{\mathbb{Z}}) = \mathrm{GL}_2(\mathbb{Q}) \iota(\mathbf{K}^\times)(\mathbb{A}) g_\infty \mathbb{R}_{>0} \mathrm{SO}_2(\mathbb{R}) \mathrm{GL}_2(\widehat{\mathbb{Z}})$$

by (4.7). More precisely if $\mathfrak{a} \in \mathscr{I}(\mathscr{O})$ and $t_\mathrm{f} \in \mathbf{K}^\times(\mathbb{A}_\mathrm{f})$ are related by (4.2), the homothety class of the lattice $\mathfrak{a}$ is given by

$$[\iota(t_\mathrm{f}) g_\infty] = \mathrm{GL}_2(\mathbb{Q}) \iota(t_\mathrm{f}) g_\infty \mathbb{R}_{>0} \mathrm{SO}_2(\mathbb{R}) \mathrm{GL}_2(\widehat{\mathbb{Z}}).$$

Passing to the projective group, let

$$\iota : \mathbf{T}_\mathbf{K} = \mathrm{Res}_{\mathbf{K}/\mathbb{Q}}(\mathbb{G}_m)/\mathbb{G}_m \hookrightarrow \mathrm{PGL}_2$$

be the induced embedding. For $t \in \mathbf{K}^\times$ we denote by $\overline{t} \in \mathbf{T}_\mathbf{K}$ the image.

From (3.4) recall that we denote by ψ_∞ the identification of Ell_∞ with an adelic double quotient of PGL_2. Summarizing the above, we get the following proposition.

Proposition 4.8. *Let $\overline{g}_\infty \in \mathrm{PGL}_2(\mathbb{R})$ be the image of g_∞ under the natural projection. Under ψ_∞ the set $\mathrm{Ell}^{\mathrm{cm}}_{\mathscr{O}}$ is mapped to*

$$\psi_\infty(\mathrm{Ell}^{\mathrm{cm}}_{\mathscr{O}}) = [\iota(\mathbf{T}_\mathbf{K})(\mathbb{A}).\overline{g}_\infty] = \mathrm{PGL}_2(\mathbb{Q}) \iota(\mathbf{T}_\mathbf{K})(\mathbb{A}) \overline{g}_\infty \mathrm{PSO}_2(\mathbb{R}) \mathrm{PGL}_2(\widehat{\mathbb{Z}})$$

which is the image of the adelic torus orbit $\mathrm{PGL}_2(\mathbb{Q}) \iota(\mathbf{T}_\mathbf{K})(\mathbb{A}) \overline{g}_\infty$. Moreover, if $\mathfrak{a} \in \mathscr{I}(\mathscr{O})$ and $t_\mathrm{f} \in \mathbf{K}^\times(\mathbb{A}_\mathrm{f})$ are related by (4.2)*, i.e. $\widehat{\mathfrak{a}} = t_\mathrm{f}.\widehat{\mathscr{O}}$, then $\mathrm{red}_\infty(\mathfrak{a} \star E_\mathscr{O})$ is represented by the class*

$$\psi_\infty(\mathrm{red}_\infty(\mathfrak{a} \star E_\mathscr{O})) = [\iota(\overline{t_\mathrm{f}}^{-1}) \overline{g}_\infty] = \mathrm{PGL}_2(\mathbb{Q}) \iota(\overline{t_\mathrm{f}}^{-1}) \overline{g}_\infty \mathrm{PSO}_2(\mathbb{R}) \mathrm{PGL}_2(\widehat{\mathbb{Z}}).$$

5. Supersingular elliptic curves

Recall that an elliptic curve $E_0/\overline{k}$ defined over an algebraically closed field is *supersingular* if its endomorphism ring $\mathrm{End}(E_0)$ is an order in a quaternion algebra. In that case, the characteristic of $\overline{k}$ is a prime, say p and the quaternion algebra

$$\mathbf{B} = \mathrm{End}(E_0) \otimes \mathbb{Q}$$

is (isomorphic to) the quaternion algebra $\mathbf{B}_{\infty,p}$ defined over $\mathbb{Q}$ ramified exactly at ∞ and p. Moreover,

$$\mathcal{O} := \mathrm{End}(E_0) \subset \mathbf{B}$$

is a *maximal* order; cf. [13] or [50, Theorem 42.1.9]. In addition E_0 has a model defined over $\mathbb{F}_{p^2}$. In particular, the set of j-invariants of such supersingular curves over $\overline{k}$ is finite and so there are only finitely many isomorphism classes. We denote by $\mathrm{Ell}_p^{\mathrm{ss}}$ the (finite) set of isomorphism classes of supersingular elliptic curves over $\overline{\mathbb{F}_p}$.

The first aim of this section is to recall how $\mathrm{Ell}_p^{\mathrm{ss}}$ is realized as an adelic quotient. We will show the following.

Proposition 5.1. *Let $\mathbf{G} = \mathbf{PB}^\times = \mathbf{B}^\times/\mathbb{G}_m$ be the projective group of units of $\mathbf{B}$ and let $\mathbf{G}(\widehat{\mathbb{Z}})$ be the image in $\mathbf{G}(\mathbb{A}_{\mathrm{f}})$ of the open compact subgroup $\widehat{\mathcal{O}}^\times \subset \mathbf{B}^\times(\mathbb{A}_{\mathrm{f}})$. There is a natural identification*

$$\psi_p : \mathrm{Ell}_p^{\mathrm{ss}} \simeq \mathbf{G}(\mathbb{Q})\backslash\mathbf{G}(\mathbb{A}_{\mathrm{f}})/\mathbf{G}(\widehat{\mathbb{Z}}) \simeq \mathbf{G}(\mathbb{Q})\backslash\mathbf{G}(\mathbb{A})/\mathbf{G}(\mathbb{R})\mathbf{G}(\widehat{\mathbb{Z}}). \tag{5.1}$$

Proposition 5.2 (cf. [50, Lemma 42.1.11]). *The set $\mathrm{Ell}_p^{\mathrm{ss}}$ forms a single isogeny class.*

5.1. Supersingular curves and ideal classes.

Definition 5.3. A (fractional) left-$\mathcal{O}$-ideal $I \subset \mathbf{B}(\mathbb{Q})$ is a lattice, invariant under multiplication on the left by $\mathcal{O}$. We denote by $\mathcal{I}(\mathcal{O})$ the set of left-$\mathcal{O}$-ideals.

Two such ideals I, J are $\mathbf{B}^\times$-homothetic if and only if there is some $z \in \mathbf{B}^\times(\mathbb{Q})$ such that $J = Iz$. We denote by

$$\mathrm{Cl}(\mathcal{O}) = \mathcal{I}(\mathcal{O})/\mathbf{B}(\mathbb{Q})^\times$$

the set of $\mathbf{B}^\times$-homothety classes of left-$\mathcal{O}$-ideals and by $h(\mathcal{O}) = |\mathrm{Cl}(\mathcal{O})|$ its cardinality.

Let E_0 be a supersingular curve over $\overline{\mathbb{F}_p}$ and let $\mathcal{O}$ and $\mathbf{B}$ as defined above.

Proposition 5.4. *There is a one-to-one correspondence*

$$\mathrm{Ell}_p^{\mathrm{ss}} \simeq \mathcal{I}(\mathcal{O})/\mathbf{B}(\mathbb{Q})^\times = \mathrm{Cl}(\mathcal{O}).$$

Sketch of Proof. We briefly recall the principle of the proof and refer to [52, Section 3] and [50, Chapter 42] for details.

In one direction, the map is given as follows: given $E/\overline{\mathbb{F}_p}$ a supersingular elliptic curve and $\varphi : E \to E_0$ an isogeny the set $\mathrm{Hom}(E, E_0)$ is a left $\mathcal{O}$-module (via post-composition by isogenies of E_0) and embeds into $\mathcal{O}$ via

$$\psi \in \mathrm{Hom}(E, E_0) \hookrightarrow \psi\hat{\varphi} \in \mathcal{O},$$

where $\hat{\varphi} : E_0 \mapsto E$ is the dual of φ. Moreover, its image $I_{E,\varphi} = \mathrm{Hom}(E, E_0)\hat{\varphi}$ contains

$$\mathcal{O}\varphi\hat{\varphi} = \deg(\varphi)\mathcal{O}$$

so $I_{E,\varphi}$ is a left-$\mathcal{O}$-ideal. One then checks that its homothety class is independent of the choice of φ.

In the reverse direction, given a left-$\mathcal{O}$-ideal $I \subset \mathbf{B}(\mathbb{Q})$, up to multiplying I by some integer $n \neq 0$, we may assume that $I \subset \mathcal{O}$. Let

$$H(I) = \bigcap_{\phi \in I} \ker \phi \subset E_0.$$

Then $H(I)$ is a finite subgroup scheme and the quotient

$$E_I = E_0/H(I) \tag{5.2}$$

is an elliptic curve satisfying $\mathrm{Hom}(E_I, E_0) \simeq I$. This isomorphism and the fact that these two maps are well-defined and inverses of one another (upon taking isomorphism and homothety classes) follow from [52, Theorem 3.11]; the key point is that, since $\mathcal{O}$ is a maximal order, the $\mathcal{O}$-ideals above are *kernel ideals* ([52, Theorem 3.15]). □

Proof of Proposition 5.1. Since $\mathcal{O}$ is maximal, any left $\mathcal{O}$-ideal I is locally principal (see [50, Theorem 16.1.3]): for any prime ℓ

$$I_\ell := I \otimes \mathbb{Z}_\ell = \mathcal{O}_\ell \beta_\ell$$

for some $\beta_\ell \in \mathbf{B}(\mathbb{Q}_\ell)^\times$ uniquely defined modulo (left multiplications by) $\mathcal{O}_\ell^\times$, where

$$\mathcal{O}_\ell = \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_\ell.$$

By the local-global principle for lattices, the map

$$\beta_{\mathrm{f}} = (\beta_\ell)_\ell \in \mathbf{B}^\times(\mathbb{A}_{\mathrm{f}}) \mapsto (\mathcal{O}_\ell \beta_\ell^{-1})_\ell = (I_\ell)_\ell \mapsto I$$

yields a bijection

$$\mathcal{I}(\mathcal{O}) \simeq \mathbf{B}^\times(\mathbb{A}_{\mathrm{f}})/\widehat{\mathcal{O}}^\times. \tag{5.3}$$

Thus, we obtain

$$\mathrm{Cl}(\mathcal{O}) \simeq \mathbf{B}^\times(\mathbb{Q}) \backslash \mathbf{B}^\times(\mathbb{A}_{\mathrm{f}})/\widehat{\mathcal{O}}^\times.$$

It follows from $\mathbb{A}_{\mathrm{f}}^\times = \mathbb{Q}^\times \widehat{\mathbb{Z}}^\times$ that the projection $\mathbf{B}^\times \to \mathbf{G}$ induces a bijection

$$\mathrm{Cl}(\mathcal{O}) \simeq \mathbf{G}(\mathbb{Q}) \backslash \mathbf{G}(\mathbb{A}_{\mathrm{f}}) / \mathbf{G}(\widehat{\mathbb{Z}}) \simeq \mathbf{G}(\mathbb{Q}) \backslash \mathbf{G}(\mathbb{A}) / \mathbf{G}(\mathbb{R})\mathbf{G}(\widehat{\mathbb{Z}}), \tag{5.4}$$

where the class of $I = \widehat{\mathcal{O}}\beta \cap \mathbf{B}(\mathbb{Q}) \subset \mathcal{O}$ is mapped to the class of β^{-1}. Proposition 5.4 concludes the proof. □

5.2. A natural measure on $\mathrm{Cl}(\mathcal{O})$. Identification (5.1) provides the finite set $\mathrm{Cl}(\mathcal{O})$ with a natural probability measure $m_{\mathrm{Cl}(\mathcal{O})}$ deduced from the Haar measure $m_{[\mathbf{G}]}$ on $[\mathbf{G}]$. In this subsection we compute the mass of the various ideal classes $[I] \in \mathrm{Cl}(\mathcal{O})$.

To describe the measure we will need the following notion.

Definition 5.5. For any left-$\mathcal{O}$-ideal I we define its right-order by

$$\mathcal{O}_R(I) = \{\beta \in \mathbf{B}(\mathbb{Q}) : I\beta \subseteq I\}.$$

If I, J are two left-$\mathcal{O}$-ideals in the same homothety class, their right-orders are clearly $\mathbf{B}^\times(\mathbb{Q})$-conjugate. More generally, if

$$I = \alpha_\mathrm{f} \star \mathcal{O} := \widehat{\mathcal{O}}\alpha_\mathrm{f}^{-1} \cap \mathbf{B}(\mathbb{Q})$$

as in (5.3) for some $\alpha_\mathrm{f} = (\alpha_q)_q \in \mathbf{B}^\times(\mathbb{A}_\mathrm{f})$, then

$$\mathcal{O}_R(I) = \alpha_\mathrm{f}\widehat{\mathcal{O}}\alpha_\mathrm{f}^{-1} \cap \mathbf{B}(\mathbb{Q}). \tag{5.5}$$

In particular, right-orders are locally maximal hence maximal.

Notice also that the action by conjugation of $\mathbf{B}^\times(\mathbb{A}_\mathrm{f})$ as in (5.5) is transitive on the set of maximal orders (for every prime ℓ, $\mathrm{GL}_2(\mathbb{Q}_\ell)$ acts transitively on the maximal orders of $\mathrm{Mat}_2(\mathbb{Q}_\ell)$ and a division algebra over the local field $\mathbb{Q}_\ell$ has only one maximal order). This implies that any maximal order of $\mathbf{B}(\mathbb{Q})$ is the right-order of some (possibly non-unique) left-$\mathcal{O}$-ideal.

Lemma 5.6 (Mass distribution). *For any* $[I] \in \mathrm{Cl}(\mathcal{O})$ *we have*

$$m_{\mathrm{Cl}(\mathcal{O})}([I]) = \frac{|\mathcal{O}_R(I)^\times/\{\pm 1\}|^{-1}}{\sum_{[J]\in\mathrm{Cl}(\mathcal{O})} |\mathcal{O}_R(J)^\times/\{\pm 1\}|^{-1}} = \frac{|\mathcal{O}_R(I)^\times|^{-1}}{\sum_{[J]\in\mathrm{Cl}(\mathcal{O})} |\mathcal{O}_R(J)^\times|^{-1}}.$$

As noted in the introduction, Eichler's mass formula (1.1) states that

$$\sum_{[J]\in\mathrm{Cl}(\mathcal{O})} \frac{1}{|\mathcal{O}_R(J)^\times/\{\pm 1\}|} = \frac{p-1}{12}.$$

Proof. Recall that $\mathbf{B}$ is definite and therefore $\mathbf{G}(\mathbb{R})$ is compact. Write $I = \alpha_\mathrm{f} \star \mathcal{O}$ for some $\alpha_\mathrm{f} \in \mathbf{B}^\times(\mathbb{A}_\mathrm{f})$. By definition, $m_{\mathrm{Cl}(\mathcal{O})}([I])$ is the $m_{[\mathbf{G}]}$-measure of the coset

$$[\alpha_\mathrm{f}\mathbf{G}(\mathbb{R})\mathbf{G}(\widehat{\mathbb{Z}})] = \mathbf{G}(\mathbb{Q})\backslash\mathbf{G}(\mathbb{Q})\alpha_\mathrm{f}\mathbf{G}(\mathbb{R})\mathbf{G}(\widehat{\mathbb{Z}}) \subset [\mathbf{G}]$$

or, by invariance of $m_{[\mathbf{G}]}$, equal to $m_{[\mathbf{G}]}([\mathbf{G}(\mathbb{R})\alpha_\mathrm{f}\mathbf{G}(\widehat{\mathbb{Z}})\alpha_\mathrm{f}^{-1}])$. Observe that

$$\widehat{\mathcal{O}_R(I)} = \alpha_\mathrm{f}\widehat{\mathcal{O}}\alpha_\mathrm{f}^{-1} \quad \text{and} \quad \alpha_\mathrm{f}\mathbf{G}(\widehat{\mathbb{Z}})\alpha_\mathrm{f}^{-1} = \mathrm{P}\widehat{\mathcal{O}_R(I)}^\times.$$

Now notice that the stabilizer of the identity coset under the right-action of $\alpha_\mathrm{f}\mathbf{G}(\widehat{\mathbb{Z}})\alpha_\mathrm{f}^{-1}$ is

$$\mathbf{G}(\mathbb{Q}) \cap \alpha_\mathrm{f}\mathbf{G}(\widehat{\mathbb{Z}})\alpha_\mathrm{f}^{-1} = \mathrm{P}\mathcal{O}_R(I)^\times := \mathcal{O}_R(I)^\times/\{\pm 1\}$$

Therefore, using unimodularity of $\mathbf{G}(\mathbb{A})$, we have

$$m_{\mathrm{Cl}(\mathcal{O})}([I]) = \frac{m_{\mathbf{G}(\mathbb{A})}(\mathbf{G}(\mathbb{R})\alpha_\mathrm{f}\mathbf{G}(\widehat{\mathbb{Z}})\alpha_\mathrm{f}^{-1})}{|\mathrm{P}\mathcal{O}_R(I)^\times|} = \frac{m_{\mathbf{G}(\mathbb{A})}(\mathbf{G}(\mathbb{R})\mathbf{G}(\widehat{\mathbb{Z}}))}{|\mathrm{P}\mathcal{O}_R(I)^\times|}.$$

Summing over all $[I] \in \mathrm{Cl}(\mathcal{O})$ (see (5.4)) and using that $m_{[\mathbf{G}]}$ is a probability measure, we see that

$$m_{\mathbf{G}(\mathbb{A})}(\mathbf{G}(\mathbb{R})\mathbf{G}(\widehat{\mathbb{Z}}))^{-1} = \sum_{[I]\in\mathrm{Cl}(\mathcal{O})} \frac{1}{|\mathrm{P}\mathcal{O}_R(I)^\times|}.$$

Thus, $m_{\mathrm{Cl}(\mathcal{O})}([I])$ is the expression claimed. □

5.2.1. Interpretation in terms of elliptic curves. By Proposition 5.4, we have an identification

$$\mathrm{Cl}(\mathcal{O}) \simeq \mathrm{Ell}_p^{\mathrm{ss}}.$$

Let us look at what Lemma 5.6 means in terms of elliptic curves. Let $\{I_0 = \mathcal{O}, \dots, I_{h(\mathcal{O})-1}\}$ be representatives of the various ideal classes in $\mathrm{Cl}(\mathcal{O})$ with $I_i \subset \mathcal{O}$. For every $i = 0, \dots, h(\mathcal{O})-1$ let E_i be the elliptic curve corresponding to I_i constructed in the proof of Proposition 5.4. By [52, Proposition 3.9] we have $\mathrm{End}(E_i) \simeq \mathcal{O}_R(I_i)$. Hence, for any $E \in \mathrm{Ell}_p^{\mathrm{ss}}$,

$$m_{\mathrm{Ell}_p^{\mathrm{ss}}}(E) = \frac{|\mathrm{Aut}(E)|^{-1}}{\sum_{E' \in \mathrm{Ell}_p^{\mathrm{ss}}} |\mathrm{Aut}(E')|^{-1}} = \nu_p(E),$$

where ν_p is defined in the introduction.

5.3. Supersingular reduction of CM elliptic curves. Let $\mathbf{K}$ be an imaginary quadratic field and $\mathcal{O} \subset \mathbf{K}$ an order. As in the introduction, we fix for any p an embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}_p}$. This choice determines a place of $\overline{\mathbb{Q}}$ above p which we denote by $\mathfrak{p}$. For any subextension $k \subset \overline{\mathbb{Q}}$ we denote by $\mathcal{O}_{k,\mathfrak{p}}$ the completion of $\mathcal{O}_k$ at $\mathfrak{p}$ and write $\overline{\mathcal{O}}_{\mathfrak{p}}$ for $\mathcal{O}_{\overline{\mathbb{Q}},\mathfrak{p}}$.

Given E an elliptic curve with CM by $\mathcal{O}$, we may assume that E is defined over the ring class field $\mathbf{H}_{\mathcal{O}}$ of $\mathcal{O}$ and in particular over $\overline{\mathbb{Q}}$. By the work of Serre–Tate [44, pp. 506–507], E has potential good reduction everywhere. In particular, there is an elliptic curve E' defined over $\mathbf{H}_{\mathcal{O}}$ with good reduction at $\mathfrak{p}$ and isomorphic to E over $\overline{\mathbb{Q}}$ (i.e. an $\mathbf{H}_{\mathcal{O}}$-form of E): there exists a smooth model $\mathcal{E}'$ defined over $\mathcal{O}_{\mathbf{H}_{\mathcal{O}},\mathfrak{p}}$ whose generic fiber is E' and whose special fiber at $\mathfrak{p}$ is a certain elliptic curve denoted by $\mathcal{E}' \bmod \mathfrak{p}$ and defined over the residue field of $\mathcal{O}_{\mathbf{H}_{\mathcal{O}},\mathfrak{p}}$. Its j-invariant $j(E)$ is an algebraic integer [45, Chapter II, Section 6] (this is a consequence of the everywhere potential good reduction of E) and we have

$$j(\mathcal{E}' \bmod \mathfrak{p}) = j(E) \bmod \mathfrak{p}.$$

In particular, the isomorphism class of the reduction does not depend on the choice of the form E'. We will thus simply speak of *the reduction modulo* $\mathfrak{p}$ of the isomorphism class $E \in \mathrm{Ell}_{\mathcal{O}}^{\mathrm{cm}}$ and will sometimes denote the class of $\mathcal{E}' \bmod \mathfrak{p}$ by $E \bmod \mathfrak{p}$.

Remark 5.7. In fact, given s distinct primes $p_1, \dots, p_s$, $\mathfrak{p}_1, \dots, \mathfrak{p}_s$ a choice of places above these primes as before, and an elliptic curve E with CM by $\mathcal{O}$, there exists E' isomorphic to E over $\overline{\mathbb{Q}}$ such that E' has good reduction at every $\mathfrak{p}_i$ ([44, Corollary 1, p. 507]).

From now on we assume that E has good reduction at $\mathfrak{p}$ and we denote by $\mathcal{E}$ its Néron model (which we take over the larger ring $\overline{\mathcal{O}}_{\mathfrak{p}}$ to avoid any rationality issues).

Lemma 5.8. *Let $E \in \mathrm{Ell}_{\mathcal{O}}^{\mathrm{cm}}$. For p inert in $\mathbf{K}$, the elliptic curve $E \bmod \mathfrak{p}$ is supersingular.*

Proof. This is a result of Deuring [13, p. 203] and a modern reference is [31, Chapter 13, Theorem 12]. □

We assume now that p is inert in $\mathbf{K}$. Denote the maximal order and the quaternion algebra attached to $E \bmod \mathfrak{p} = \mathcal{E} \bmod \mathfrak{p}$ by

$$\mathcal{O}_E = \mathrm{End}(\mathcal{E} \bmod \mathfrak{p}) \subset \mathbf{B}_E = \mathrm{End}(\mathcal{E} \bmod \mathfrak{p}) \otimes_{\mathbb{Z}} \mathbb{Q} \simeq \mathbf{B}_{\infty,p}. \tag{5.6}$$

We therefore have an identification

$$\mathrm{Ell}_p^{\mathrm{ss}} \simeq \mathrm{Cl}(\mathcal{O}_E) = \mathcal{I}(\mathcal{O}_E)/\mathbf{B}_E^\times(\mathbb{Q}) \tag{5.7}$$

under which the class of $\mathcal{E} \bmod \mathfrak{p}$ corresponds to the ideal class $[\mathcal{O}_E]$.

5.4. Compatibility with the Picard group action. As in the previous section, let E have CM by $\mathscr{O}$ and let $\mathcal{E}$ be its Néron model. By general properties of the Néron model, the reduction modulo $\mathfrak{p}$ induces an embedding

$$\iota_E : \mathrm{End}_{\overline{\mathbb{Q}}}(E) \simeq \mathrm{End}_{\overline{\mathscr{O}}_\mathfrak{p}}(\mathcal{E}) = \mathscr{O} \hookrightarrow \mathrm{End}_{\overline{\mathbb{F}}_p}(E \bmod \mathfrak{p}) = \mathcal{O}_E,$$

and by extension (tensoring with $\mathbb{Q}$) a $\mathbb{Q}$-algebra embedding

$$\iota_E : \mathbf{K} \hookrightarrow \mathbf{B}_E. \tag{5.8}$$

Proposition 5.9. *Assume that p does not divide the conductor of $\mathscr{O}$. The embedding ι_E of $\mathscr{O}$ is optimal, that is, one has*

$$\iota_E(\mathbf{K}) \cap \mathcal{O}_E = \iota_E(\mathscr{O}).$$

Proof. See [32, Proposition 2.2]. It is proven that the embedding is locally optimal at every prime $\neq p$ and it is optimal at p if and only if $\mathscr{O}_p$ is the maximal order of $\mathbf{K}_p$. The latter is equivalent to our assumption. □

We have seen that all elliptic curves with CM by $\mathscr{O}$ are of the form (up to isomorphism) $\mathfrak{a} \star E$, where $\mathfrak{a} \subset \mathscr{O}$ is a proper $\mathscr{O}$-ideal. The next proposition states that this presentation is compatible with reduction modulo $\mathfrak{p}$.

Proposition 5.10. *In the identification* (5.7) *the isomorphism class of* $\mathfrak{a} \star E \bmod \mathfrak{p}$ *corresponds to the class of the left-$\mathcal{O}_E$ module $\mathcal{O}_E\, \iota_E(\mathfrak{a})$.*

The proof of this proposition, which one can find[1)] in [7, Theorem 7.12], is discussed in the section below. The main ingredient is a construction due to Serre [42]: the $\mathfrak{a}$-*transform*. We briefly recall its definition and refer to [7, Section 7], [23] and [38, Chapter 7] for more details.

5.5. The $\mathfrak{a}$-transform. Let A be a (not necessarily commutative) associative ring with unit, M be a projective left A-module of finite type and constant rank r, S a scheme and E/S a (smooth) elliptic scheme over S on which A acts (on the left) by S-isogenies. The functor

$$M \star E : T \rightsquigarrow \mathrm{Hom}_A(M, E(T))$$

on the category of schemes over S is representable by an abelian group scheme over S of relative dimension r and equipped with an A-action.

Example 5.11. For $A = \mathscr{O}$, $M = \mathfrak{a} \in \mathcal{I}(\mathscr{O})$ a proper ideal, $S = \mathrm{Spec}(\overline{\mathscr{O}}_\mathfrak{p})$, $\mathcal{E}/S$ the Néron model of an elliptic curve $E \in \mathrm{Ell}_{\mathscr{O}}^{\mathrm{cm}}$ with good reduction at $\mathfrak{p}$, we have ([7, Theorem 7.6])

$$\mathfrak{a} \star \mathcal{E}(\mathbb{C}) = \mathfrak{a} \star E(\mathbb{C}) \simeq \mathbb{C}/\Lambda\mathfrak{a}^{-1}.$$

[1)] The proof is given for $\mathscr{O} = \mathscr{O}_\mathbf{K}$ the maximal order but it carries over to general orders of $\mathbf{K}$ since quadratic orders are Gorenstein rings.

Example 5.12. Given $E_0 \in \mathrm{Ell}_p^{\mathrm{ss}}$,

$$A = \mathrm{End}_{\overline{\mathbb{F}_p}}(E_0) = \mathcal{O}_{E_0} \subset \mathrm{End}^0_{\overline{\mathbb{F}_p}}(E_0) = \mathbf{B}_{E_0}$$

a maximal order and $I \subset \mathcal{O}_{E_0}$ a left $\mathcal{O}_{E_0}$-module and $S = \mathrm{Spec}(\overline{\mathbb{F}_p})$, we have (see (5.2))

$$I \star E_0 = E_I = E_0/H(I).$$

In the case of Example 5.11, after translating the notations of [7] into ours, the formula in [7, Theorem 7.12] is the isomorphism of $\mathcal{O}_E$-modules

$$\mathrm{Hom}_{\overline{\mathbb{F}_p}}(\mathfrak{a} \star \mathcal{E} \bmod \mathfrak{p}, \mathcal{E} \bmod \mathfrak{p}) \simeq \mathcal{O}_E\, \iota_E(\mathfrak{a}).$$

This is the claim in Proposition 5.10.

5.6. Compatibility with the Picard group action in adelic terms. In this subsection we interpret Proposition 5.10 and therefore the map

$$\mathrm{red}_p : \mathrm{Ell}_{\mathscr{O}}^{\mathrm{cm}} \to \mathrm{Ell}_p^{\mathrm{ss}},\ E \mapsto E \bmod \mathfrak{p}$$

(see Section 5.3) in adelic terms. Here, $\mathscr{O} \subset \mathbf{K}$ is a quadratic order, p is inert in $\mathbf{K}$ (see Lemma 5.8). We assume that p does not divide the conductor of $\mathscr{O}$ as in Proposition 5.9.

Given $E \in \mathrm{Ell}_{\mathscr{O}}^{\mathrm{cm}}$, we let $\mathcal{O}_E$ and $\mathbf{B}_E$ be the maximal order and the quaternion algebra associated to E as in (5.6) and let $\mathbf{G}_E = \mathbf{PB}_E^\times = \mathbf{B}_E^\times/\mathbb{G}_m$ be the projective group. Thus, we have an identification

$$\psi_{E,p} : \mathrm{Ell}_p^{\mathrm{ss}} \simeq \mathbf{B}_E^\times(\mathbb{Q})\backslash\mathbf{B}^\times(\mathbb{A}_{\mathrm{f}})/\widehat{\mathcal{O}}_E^\times \simeq \mathbf{G}_E(\mathbb{Q})\backslash\mathbf{G}_E(\mathbb{A}_{\mathrm{f}})/\mathbf{G}_E(\widehat{\mathbb{Z}}) \tag{5.9}$$

by Proposition 5.1, where the isomorphism class of $E \bmod \mathfrak{p}$ corresponds to the class of the identity element and where $\mathbf{G}_E(\widehat{\mathbb{Z}}) = \mathrm{P}\widehat{\mathcal{O}_E}^\times$.

The embedding ι_E in (5.8) induces an embedding of $\mathbb{Q}$-algebraic groups

$$\iota_E : \mathrm{Res}_{\mathbf{K}/\mathbb{Q}}(\mathbb{G}_m) \hookrightarrow \mathbf{B}_E^\times$$

and by optimality (Proposition 5.9) we have

$$\iota_E(\widehat{\mathscr{O}}^\times) = \iota_E(\mathbf{K}(\mathbb{A}_{\mathrm{f}}))^\times \cap \widehat{\mathcal{O}}_E^\times.$$

Projecting to $\mathbf{G}_E$, we obtain a torus embedding

$$\iota_E : \mathbf{T}_{\mathbf{K}} = \mathrm{Res}_{\mathbf{K}/\mathbb{Q}}(\mathbb{G}_m)/\mathbb{G}_m \to \mathbf{G}_E$$

whose image we denote by $\mathbf{T}_E$. By Section 4.2 we have

$$\begin{aligned}\mathrm{Pic}(\mathscr{O}) &\simeq \mathbf{K}^\times\backslash\mathbf{K}^\times(\mathbb{A}_{\mathrm{f}})/\widehat{\mathscr{O}}^\times \simeq \mathbf{T}_{\mathbf{K}}(\mathbb{Q})\backslash\mathbf{T}_{\mathbf{K}}(\mathbb{A}_{\mathrm{f}})/\mathrm{P}\widehat{\mathscr{O}}^\times \\ &\simeq \mathbf{T}_E(\mathbb{Q})\backslash\mathbf{T}_E(\mathbb{A}_{\mathrm{f}})/\mathbf{T}_E(\widehat{\mathbb{Z}}),\end{aligned} \tag{5.10}$$

where $\mathbf{T}_E(\widehat{\mathbb{Z}}) := \mathbf{T}_E(\mathbb{A}_{\mathrm{f}}) \cap \mathbf{G}_E(\widehat{\mathbb{Z}})$.

Let $\mathfrak{a} \in \mathcal{I}(\mathscr{O})$ and $t_{\mathrm{f}} \in \mathbf{K}^\times(\mathbb{A}_{\mathrm{f}})$ be related by (4.2) (i.e. such that $\widehat{\mathfrak{a}} = t_{\mathrm{f}}\widehat{\mathscr{O}}$) and let $\bar{t}_{\mathrm{f}}$ be the image of t_{f} in $\mathbf{T}_{\mathbf{K}}(\mathbb{A}_{\mathrm{f}})$. By Proposition 5.10 the class of $\mathfrak{a} \star E \bmod \mathfrak{p}$ corresponds to the left $\mathcal{O}_E$-module

$$\mathcal{O}_E\, \iota_E(\mathfrak{a}) = \mathbf{B}_E(\mathbb{Q}) \cap \widehat{\mathcal{O}}_E\, \iota_E(t_{\mathrm{f}})$$

and therefore to the classes $[\iota_E(t_{\mathrm{f}})^{-1}]$ and $[\iota_E(\bar{t}_{\mathrm{f}})^{-1}]$, respectively under the identifications in (5.9). To summarize, we have shown that

$$\psi_{E,p}(\mathfrak{a} \star E \bmod \mathfrak{p}) = [\iota_E(\overline{t_{\mathrm{f}}^{-1}})]. \tag{5.11}$$

5.6.1. Changing the reference curve. A minor point is that the identification (5.9) is made with respect to the reference curve $E \bmod \mathfrak{p}$ which is a priori varying with $\mathscr{O}$. Since p is fixed and the space $\mathrm{Ell}_p^{\mathrm{ss}}$ is finite, we could resolve the issue by passing to subsequences of orders $\mathscr{O}$ such that all the curves $E_{\mathscr{O}}$ have a given reduction modulo $\mathfrak{p}$. However, it is more natural to keep track of (5.9) when we use (5.1) with a fixed reference curve $E_0 \in \mathrm{Ell}_p^{\mathrm{ss}}$.

Let $E_0 \in \mathrm{Ell}_p^{\mathrm{ss}}$ with associated quaternion algebra, maximal order and projective group denoted by $\mathbf{B}$, $\mathcal{O}$ and $\mathbf{G}$, respectively.

Let $E \in \mathrm{Ell}_{\mathscr{O}}^{\mathrm{cm}}$ and

$$\varphi : E \bmod \mathfrak{p} \to E_0$$

an isogeny between the two curves. We have an embedding

$$f_\varphi : \psi \in \mathrm{End}(E \bmod \mathfrak{p}) = \mathcal{O}_E \hookrightarrow \frac{1}{\deg(\varphi)} \varphi \psi \hat{\varphi} \in \mathbf{B}(\mathbb{Q}),$$

which extends to an isomorphism of $\mathbb{Q}$-algebras

$$f_\varphi : \mathbf{B}_E \simeq \mathbf{B}.$$

This also gives a bijection

$$f_\varphi : \mathbf{G}_E(\mathbb{Q}) \backslash \mathbf{G}_E(\mathbb{A}_{\mathrm{f}}) / \mathbf{G}_E(\widehat{\mathbb{Z}}) \simeq \mathbf{G}(\mathbb{Q}) \backslash \mathbf{G}(\mathbb{A}_{\mathrm{f}}) / f_\varphi(\mathbf{G}_E(\widehat{\mathbb{Z}})).$$

The right order of the left $\mathcal{O}$-ideal

$$I_{E,\varphi} := \mathrm{Hom}(E \bmod \mathfrak{p}, E_0)\hat{\varphi} \subset \mathcal{O} = \mathrm{End}(E_0)$$

is the maximal order $f_\varphi(\mathcal{O}_E)$. One can check (see Remark 5.13) that its (right) $\mathbf{B}^\times(\mathbb{Q})$-homothety class does not depend on φ and represents (the isomorphism class of) $E \bmod \mathfrak{p}$ under Proposition 5.4.

Let $\beta_{E,\mathrm{f}} \in \mathbf{B}^\times(\mathbb{A}_{\mathrm{f}})$ such that

$$\widehat{I}_{E,\varphi} = \widehat{\mathcal{O}} \beta_{E,\mathrm{f}}^{-1}. \tag{5.12}$$

Since the right order of $I_{E,\varphi}$ is $f_\varphi(\mathcal{O}_E)$ have

$$f_\varphi(\widehat{\mathcal{O}}_E) = \beta_{E,\mathrm{f}} \widehat{\mathcal{O}} \beta_{E,\mathrm{f}}^{-1}$$

and hence

$$f_\varphi(\mathbf{G}_E(\widehat{\mathbb{Z}})) = \beta_{E,\mathrm{f}} \mathbf{G}(\widehat{\mathbb{Z}}) \beta_{E,\mathrm{f}}^{-1}.$$

From this we deduce that the map

$$\mathbf{G}(\mathbb{Q}) \alpha_{\mathrm{f}} f_\varphi(\mathbf{G}_E(\widehat{\mathbb{Z}})) \mapsto \mathbf{G}(\mathbb{Q}) \alpha_{\mathrm{f}} \beta_{E,\mathrm{f}} \mathbf{G}(\widehat{\mathbb{Z}})$$

is a bijection

$$\mathbf{G}(\mathbb{Q}) \backslash \mathbf{G}(\mathbb{A}_{\mathrm{f}}) / f_\varphi(\mathbf{G}_E(\widehat{\mathbb{Z}})) \simeq \mathbf{G}(\mathbb{Q}) \backslash \mathbf{G}(\mathbb{A}_{\mathrm{f}}) / \mathbf{G}(\widehat{\mathbb{Z}}). \tag{5.13}$$

Remark 5.13. If we choose a different isogeny φ', then the Skolem–Noether theorem implies that the images of $\mathcal{O}_E$ by f_φ and $f_{\varphi'}$ are conjugate and the modules I_E and I'_E vary accordingly.

Let $\iota : \mathbf{K} \to \mathbf{B}$ be the composition of the embedding $\iota_E : \mathbf{K} \to \mathbf{B}_E$ with f_φ. This defines an embedding

$$\iota : \mathbf{T}_\mathbf{K} \hookrightarrow \mathbf{G}. \tag{5.14}$$

The optimality property of ι_E translates into

$$\iota(\widehat{\mathscr{O}}^\times) = \iota(\mathbf{K}(\mathbb{A}_\mathrm{f}))^\times \cap \beta_{E,\mathrm{f}} \widehat{\mathcal{O}}^\times \beta_{E,\mathrm{f}}^{-1}. \tag{5.15}$$

Combining (5.11) with the bijection (5.13), we obtain the analogue of Proposition 4.8 at the place p.

Proposition 5.14. *Let $E = E_\mathscr{O} \in \mathrm{Ell}^{\mathrm{cm}}_\mathscr{O}$ and ι the embedding constructed above. In the identification* (5.1) *the set* $\mathrm{red}_p(\mathrm{Ell}^{\mathrm{cm}}_\mathscr{O})$ *is represented by the projection of the adelic torus orbit* $\mathbf{G}(\mathbb{Q})\iota(\mathbf{T}_\mathbf{K})(\mathbb{A})\beta_{E,\mathrm{f}}$. *That is,*

$$\psi_p(\mathrm{red}_p(\mathrm{Ell}^{\mathrm{cm}}_\mathscr{O})) = [\iota(\mathbf{T}_\mathbf{K})(\mathbb{A})\beta_{E,\mathrm{f}}] = \mathbf{G}(\mathbb{Q})\iota(\mathbf{T}_\mathbf{K})(\mathbb{A})\beta_{E,\mathrm{f}}\mathbf{G}(\mathbb{R})\mathbf{G}(\widehat{\mathbb{Z}}).$$

More precisely, if $\mathfrak{a} \in \mathscr{I}(\mathscr{O})$ *and* $t_\mathrm{f} \in \mathbf{K}^\times(\mathbb{A}_\mathrm{f})$ *are related by* (4.2)*, then*

$$\mathrm{red}_p(\mathfrak{a} \star E) = \mathfrak{a} \star E \bmod \mathfrak{p}$$

is represented by the class

$$\psi_p(\mathrm{red}_p(\mathfrak{a} \star E)) = [\iota(\overline{t_\mathrm{f}}^{-1})\beta_{E,\mathrm{f}}] = \mathbf{G}(\mathbb{Q})\iota(\overline{t_\mathrm{f}}^{-1})\beta_{E,\mathrm{f}}\mathbf{G}(\mathbb{R})\mathbf{G}(\widehat{\mathbb{Z}}).$$

6. Diagonal compatibility

In this section we combine Propositions 4.8 and 5.14 as already outlined in Section 1.2. This continues the reduction of Theorem 1.3 to Theorem 1.8.

We fix $p_1, \dots, p_s$ distinct odd primes and for each $i = 1, \dots, s$ we fix a supersingular elliptic curve $E_{0,i} \in \mathrm{Ell}^{\mathrm{ss}}_{p_i}$ in characteristic p_i. Each $E_{0,i}$ determines a quaternion algebra $\mathbf{B}_i \simeq \mathbf{B}_{p_i,\infty}$ and a maximal order $\mathcal{O}_i$ in it. We denote by $\mathbf{G}_i = \mathbf{PB}_i^\times$ the corresponding projective group of units. Furthermore, let $\mathbf{B}_0 = \mathrm{Mat}_2$ be the split quaternion algebra, $\mathcal{O}_0 = \mathrm{Mat}_2(\mathbb{Z})$ and $\mathbf{G}_0 = \mathrm{PGL}_2$. We also define for $i = 0, \dots, s$ the compact subgroups

$$K_i = K_{\infty,i} K_{\mathrm{f},i} \subset \mathbf{G}_i(\mathbb{A}),$$

where $K_{\infty,i} = \mathbf{G}_i(\mathbb{R})$ for $i \geq 1$, $K_{\infty,0} = \mathrm{PSO}_2(\mathbb{R})$ and where

$$K_{\mathrm{f},i} = \mathbf{G}_i(\widehat{\mathbb{Z}}) := \mathrm{P}\widehat{\mathcal{O}}_i^\times = \widehat{\mathcal{O}}_i^\times / \widehat{\mathbb{Z}}^\times$$

for all i. For the product group

$$\mathbf{G} := \prod_{i=0}^{s} \mathbf{G}_i$$

we define the compact subgroups

$$K = K_\infty K_\mathrm{f} = \prod_{i=0}^{s} K_i \subset \mathbf{G}(\mathbb{A}), \quad K_\infty = \prod_i K_{\infty,i}, \quad K_\mathrm{f} = \prod_i K_{\mathrm{f},i}.$$

The identifications (3.4) for $i = 0$ and (5.1) for $i = 1, \dots, s$ combine into an identification

$$\psi : \mathrm{Ell}_\infty \times \prod_{i=1}^{s} \mathrm{Ell}^{\mathrm{ss}}_{p_i} \simeq \mathbf{G}(\mathbb{Q})\backslash\mathbf{G}(\mathbb{A})/K. \tag{6.1}$$

Let $\mathbf{K}$ be an imaginary quadratic field in which for each $i = 1, \dots, s$ the prime p_i is inert. Let $\mathscr{O} \subset \mathbf{K}$ be an order and assume that the primes $p_1, \dots, p_s$ do not divide the conductor of $\mathscr{O}$. The various reduction maps red_{p_i} for $i = 0, \dots, s$ combine into a multi-reduction map

$$\mathrm{red}_{\mathbf{p}} : E \in \mathrm{Ell}^{\mathrm{cm}}_{\mathscr{O}} \mapsto (\mathrm{red}_{p_i} E)_{i=0,\dots,s} \in \mathrm{Ell}_\infty \times \prod_{i=1}^{s} \mathrm{Ell}^{\mathrm{ss}}_{p_i}.$$

The choice of the CM curve $E_{\mathscr{O}} \simeq \mathbb{C}/\mathscr{O}$ provides a parametrization of $\mathrm{Ell}^{\mathrm{cm}}_{\mathscr{O}}$ by $\mathrm{Pic}(\mathscr{O})$ via

$$[\mathfrak{a}] \mapsto \mathfrak{a} \star E_{\mathscr{O}} = E_{\mathfrak{a}^{-1}}$$

and a map

$$[\mathfrak{a}] \in \mathrm{Pic}(\mathscr{O}) \mapsto \mathrm{red}_{\mathbf{p}}(\mathfrak{a} \star E_{\mathscr{O}}) = \mathrm{red}_{\mathbf{p}}(E_{\mathfrak{a}^{-1}}). \tag{6.2}$$

In addition, the choice of $E = E_{\mathscr{O}}$ determines embeddings $\iota_i : \mathbf{T}_{\mathbf{K}} \hookrightarrow \mathbf{G}_i$ (see (5.14)) which combine into a diagonal embedding

$$\iota = (\iota_i)_{i=0,\dots,s} : \mathbf{T}_{\mathbf{K}} \hookrightarrow \mathbf{G} = \prod_{i=0}^{s} \mathbf{G}_i$$

whose image we denote by

$$\mathbf{T}_\iota := \iota(\mathbf{T}_{\mathbf{K}}).$$

We let $\mathrm{g} = \mathrm{g}_\infty \mathrm{g}_{\mathrm{f}} \in \mathbf{G}(\mathbb{A})$ be given by

$$\mathrm{g}_\infty = (\overline{g}_\infty, \mathrm{Id}, \dots, \mathrm{Id}) \in \mathbf{G}(\mathbb{R}), \tag{6.3}$$

$$\mathrm{g}_{\mathrm{f}} = (\mathrm{Id}, \beta_{\mathrm{f},1}, \dots, \beta_{\mathrm{f},s}) \in \mathbf{G}(\mathbb{A}_{\mathrm{f}}), \tag{6.4}$$

where $g_\infty \in \mathrm{GL}_2(\mathbb{R})$ is defined above (4.7) and where $\beta_{\mathrm{f},i}$ for $i \geq 1$ is defined in (5.12) given the curve $E = E_{\mathscr{O}}$. By definition of $\overline{g}_\infty$ and of K_∞ we have

$$\mathbf{T}_\iota(\mathbb{R}) < \mathrm{g}_\infty K_\infty \mathrm{g}_\infty^{-1}.$$

By (4.6) and (5.15), the embedding ι is *optimal* in the sense that

$$\iota(\mathrm{P}\widehat{\mathscr{O}}^\times) = \mathbf{T}_\iota(\mathbb{A}_{\mathrm{f}}) \cap \mathrm{g}_{\mathrm{f}} K_{\mathrm{f}} \mathrm{g}_{\mathrm{f}}^{-1}.$$

Combining Proposition 4.8 and Proposition 5.14, we obtain that the map (6.2) admits the following adelic description:

Proposition 6.1. *In the identification* (6.1)*, the set* $\mathrm{red}_{\mathbf{p}}(\mathrm{Ell}^{\mathrm{cm}}_{\mathscr{O}})$ *is represented by the projection of the adelic torus orbit* $\mathbf{G}(\mathbb{Q})\mathbf{T}_\iota(\mathbb{A})\mathrm{g}$*. That is,*

$$\psi(\mathrm{red}_{\mathbf{p}}(\mathrm{Ell}^{\mathrm{cm}}_{\mathscr{O}})) = [\mathbf{T}_\iota(\mathbb{A})\mathrm{g}] = \mathbf{G}(\mathbb{Q})\mathbf{T}_\iota(\mathbb{A})\mathrm{g}K.$$

More precisely, if $\mathfrak{a} \in \mathscr{I}(\mathscr{O})$ *and* $t_{\mathrm{f}} \in \mathbf{K}^\times(\mathbb{A}_{\mathrm{f}})$ *are related by* (4.2)*, then* $\mathrm{red}_{\mathbf{p}}(\mathfrak{a} \star E)$ *is represented by the class*

$$\psi(\mathrm{red}_{\mathbf{p}}(\mathfrak{a} \star E)) = [\iota(\overline{t}_{\mathrm{f}}^{-1})\mathrm{g}] = \mathbf{G}(\mathbb{Q})\iota(\overline{t}_{\mathrm{f}}^{-1})\mathrm{g}K.$$

7. Joint equidistribution for CM elliptic curves

In this section we prove Theorem 1.3 from the introduction assuming Theorem 1.8. In fact, we prove the following generalization.

Theorem 7.1. *Let $p_1, \dots, p_s, q_1, q_2$ be distinct odd primes. As $D \to -\infty$ along the set of discriminants of imaginary quadratic orders $\mathscr{O}$ such that*

(1) *every p_i for $i \leq s$, is inert in $\mathbf{K} = \mathbb{Q}(\sqrt{D})$,*

(2) *D is coprime to p_i for all $i \leq s$, and*

(3) *q_1 and q_2 are split in $\mathbf{K}$,*

the push-forward of the counting probability measure on $\mathrm{Ell}^{\mathrm{cm}}_{\mathscr{O}}$ by $\mathrm{red}_{\mathfrak{p}}$ equidistributes towards the product measure $\nu_\infty \otimes \nu_{p_1} \otimes \cdots \otimes \nu_{p_s}$.

Given Proposition 6.1, the proof is essentially an exercise in translating between the classical and the adelic language.

7.1. Some notations. Let $p_1, \dots, p_s, q_1, q_2$ be as above. We consider a sequence of imaginary quadratic orders

$$\mathscr{O}_n \subset \mathbf{K}_n, \quad n \geq 1,$$

of discriminant $D_n \to -\infty$ such that D_n satisfies (1)–(3) in Theorem 7.1 for every n. Let

$$E_n := E_{\mathscr{O}_n} \simeq \mathbb{C}/\mathscr{O}_n.$$

In the notation of the previous section, each curve E_n gives rise to a diagonal embedding of $\mathbf{T}_{\mathbf{K}_n}$

$$\iota_n = (\iota_{0,n}, \dots, \iota_{s,n}) : \mathbf{T}_{\mathbf{K}_n} \hookrightarrow \mathbf{G}$$

whose image we denote by $\mathbf{T}_{\iota_n}$. Define $\mathrm{g}_n = \mathrm{g}_{\infty,n}\mathrm{g}_{\mathrm{f},n}$ as in (6.3) and (6.4) so that in particular

$$\mathbf{T}_{\iota_n}(\mathbb{R}) < \mathrm{g}_{\infty,n} K_\infty \mathrm{g}_{\infty,n}^{-1}. \tag{7.1}$$

We have the following optimality property:

$$T_{\iota_n,\mathrm{f}} := \iota(\mathrm{P}\widehat{\mathscr{O}}_n^\times) = \mathbf{T}_{\iota_n}(\mathbb{A}_{\mathrm{f}}) \cap \mathrm{g}_{\mathrm{f},n} K_{\mathrm{f}} \mathrm{g}_{\mathrm{f},n}^{-1}. \tag{7.2}$$

Finally, we define the compact subgroup

$$T_{\iota_n} := \mathbf{T}_{\iota_n}(\mathbb{R}) \times T_{\iota_n,\mathrm{f}} \subset \mathbf{T}_{\iota_n}(\mathbb{A}).$$

Remark 7.2. Our assumption (3) on q_1 and q_2 implies that $\mathbf{T}_{\iota_n}$ is split at q_1 and q_2.

7.2. Proof of Theorem 1.3. It is sufficient to show that for any function $f_0 \in \mathscr{C}_c(\mathrm{Ell}_\infty)$ and any tuple of super-singular elliptic curves $(\overline{E}_i)_{1 \leq i \leq s} \in \prod_i \mathrm{Ell}^{\mathrm{ss}}_{p_i}$ one has

$$\frac{1}{|\mathrm{Pic}(\mathscr{O}_n)|} \sum_{[\mathfrak{a}] \in \mathrm{Pic}(\mathscr{O}_n)} f_0(\mathbb{C}/\mathfrak{a}^{-1}) \prod_{i \geq 1} \delta_{\overline{E}_i}(\mathfrak{a} \star E_n \bmod \mathfrak{p}_i) \to \nu_\infty(f_0) \prod_{i \geq 1} \nu_{p_i}(\overline{E}_i) \tag{7.3}$$

as $n \to \infty$, where $\delta_{\overline{E}_i}$ denotes the Dirac function at the point $\overline{E}_i \in \mathrm{Ell}^{\mathrm{ss}}_{p_i}$. To prove this convergence, we will interpret the left- and the right-hand sides of (7.3) as adelic integrals.

7.2.1. The right-hand side of (7.3). Under the identification (3.4) the function f_0 correspond to a continuous compactly supported function on $[\mathbf{G}_0]_{K_0}$ or equivalently to a continuous compactly supported function $\tilde{f_0}$ (say) on $[\mathbf{G}_0]$ which is K_0-invariant. In particular,

$$\int_{[\mathbf{G}_0]} \tilde{f_0}(g_0)\,\mathrm{d}g_0 = \nu_\infty(f_0).$$

Similarly, for $i \geq 1$ the Dirac function $\delta_{\overline{E}_i}$ corresponds to a $K_i = \mathbf{G}_i(\mathbb{R})K_{\mathrm{f},i}$-invariant continuous function on $[\mathbf{G}_i]$ under (5.1), namely the characteristic function of the class

$$[g_{\mathrm{f},\overline{E}_i}\mathbf{G}_i(\mathbb{R})K_{\mathrm{f},i}] = [g_{\mathrm{f},\overline{E}_i}K_i] \subset [\mathbf{G}_i]$$

where the class of $g_{\mathrm{f},\overline{E}_i}$ corresponds to $\overline{E}_i$ under (5.1). By Lemma 5.6 and the discussion in Section 5.2.1, we have

$$\int_{[\mathbf{G}_i]} 1_{[g_{\mathrm{f},\overline{E}_i}K_i]}(g_i)\,\mathrm{d}g_i = \nu_{p_i}(\overline{E}_i).$$

The product function

$$f = f_0 \times \prod_{i=1}^{s} \delta_{\overline{E}_i} : \mathrm{Ell}_\infty \times \prod_{i\geq 1} \mathrm{Ell}_{p_i}^{\mathrm{ss}} \to \mathbb{C}$$

corresponds to the K-invariant function

$$\tilde{f} := \tilde{f_0} \times \prod_{i\geq 1} 1_{[g_{\mathrm{f},\overline{E}_i}K_i]} : [\mathbf{G}] \to \mathbb{C}$$

which satisfies

$$\int_{[\mathbf{G}]} \tilde{f}(\mathrm{g})\,\mathrm{d}\mathrm{g} = \nu_\infty(f_0)\prod_{i\geq 1}\nu_{p_i}(\overline{E}_i).$$

7.2.2. The left-hand side of (7.3). To ease notation, we will not display the index n here.

Because of the obvious bijection

$$\mathbf{T}_\iota(\mathbb{Q})\backslash\mathbf{T}_\iota(\mathbb{A}) \simeq \mathbf{G}(\mathbb{Q})\backslash\mathbf{G}(\mathbb{Q})\mathbf{T}_\iota(\mathbb{A}) = [\mathbf{T}_\iota],$$

we view (by restriction) the shifted function on $[\mathbf{G}]$

$$\mathrm{g}.\tilde{f}(\cdot) : t \mapsto \tilde{f}(t\mathrm{g})$$

as a (continuous) function on $[\mathbf{T}_\iota]$. By (7.2) and (7.1) this function is T_ι-invariant, that is, it is constant along any set of the shape

$$[t_\mathrm{f}T_\iota] = \mathbf{T}_\iota(\mathbb{Q})\backslash\mathbf{T}_\iota(\mathbb{Q})t_\mathrm{f}T_\iota \text{ for } t_\mathrm{f} \in \mathbf{T}_\iota(\mathbb{A}_\mathrm{f}).$$

Moreover, by invariance of the Haar measure we have

$$\mathrm{vol}_{[\mathbf{T}_\iota]}([t_\mathrm{f}T_\iota]) = \mathrm{vol}_{[\mathbf{T}_\iota]}([T_\iota t_\mathrm{f}]) = \mathrm{vol}_{[\mathbf{T}_\iota]}([T_\iota])$$

as $\mathbf{T}_\iota$ is abelian. Thus, all T_ι-cosets have the same volume. Hence,

$$\mathrm{vol}_{[\mathbf{T}_\iota]}([t_\mathrm{f}T_\iota]) = \frac{1}{|[\mathbf{T}_\iota]_{T_\iota}|} = \frac{1}{|\mathrm{Pic}(\mathscr{O})|}$$

where in the second equality we used (5.10) and (7.1). It follows that

$$\begin{aligned}\int_{[\mathbf{T}_\iota]} \tilde{f}(t\mathrm{g})\,\mathrm{d}t &= \frac{1}{|[\mathbf{T}_\iota]_{T_\iota}|} \sum_{[t_\mathrm{f}]\in[\mathbf{T}_\iota]_{T_\iota}} \tilde{f}(t_\mathrm{f}\mathrm{g}) \\ &= \frac{1}{|\mathrm{Pic}(\mathscr{O})|} \sum_{[\mathfrak{a}]\in\mathrm{Pic}(\mathscr{O})} f(\mathrm{red}_\mathbf{p}(\mathfrak{a}^{-1}\star E)),\end{aligned}$$

where the last equality follows from Proposition 6.1. This is equal to the left-hand side of (7.3).

Therefore, we have for any n,

$$\frac{1}{|\mathrm{Pic}(\mathscr{O}_n)|} \sum_{[\mathfrak{a}]\in\mathrm{Pic}(\mathscr{O}_n)} f_0(\mathbb{C}/\mathfrak{a}^{-1}) \prod_{i\geq 1} \delta_{\overline{E}_i}(\mathfrak{a}\star E_n \bmod \mathfrak{p}_i) = \int_{[\mathbf{T}_{\iota_n}]} \tilde{f}(t\mathrm{g}_n)\,\mathrm{d}t,$$

which realizes the left-hand side of (7.3) as an adelic integral.

7.2.3. The convergence claim in (7.3). By Section 7.2.1 and Section 7.2.2 it remains to show that as $n\to\infty$,

$$\int_{[\mathbf{T}_{\iota_n}]} \tilde{f}(t\mathrm{g}_n)\,\mathrm{d}t \to \int_{[\mathbf{G}]} \tilde{f}(\mathrm{g})\,\mathrm{d}\mathrm{g}.$$

Therefore, Theorem 1.3 will follow from the equidistribution statement in Theorem 1.8 once we have verified all its assumptions.

Condition (1.5) is satisfied since $\mathcal{O}_i$ is a maximal order in $\mathbf{B}_i$ for any i (see the more general Lemma 9.5). It remains to see that the discriminant fulfills

$$\mathrm{disc}([\mathbf{T}_{\iota_n}\mathrm{g}_n]) = \min_i \mathrm{disc}([\mathbf{T}_{\iota_{i,n}} g_{i,n}]) \to \infty$$

as $n\to\infty$. Here, $g_{i,n}$ is the projection of g_n to the i-th factor. The *discriminant* of the torus orbit $\mathrm{disc}([\mathbf{T}_{\iota_{i,n}} g_{i,n}])$ is defined in [18, Section 4], and one can show that there exists a constant $C>1$ independent of n with

$$C^{-1}|D_n| \leq \mathrm{disc}([\mathbf{T}_{\iota_{i,n}} g_{i,n}]) \leq C|D_n|$$

using [17, Proposition 4.1] and [18, Theorem 5.2 (1)] and the fact that D_n is coprime to p_i. Therefore

$$\mathrm{disc}([\mathbf{T}_{\iota_n}\mathrm{g}_n]) \to \infty.$$

Thus, Theorem 1.8 applies and concludes the proof of Theorem 1.3. □

Remark 7.3. Theorem 1.3 can be refined further to provide more precise information by reducing the size of the compact subgroup

$$K = \mathrm{PSO}_2(\mathbb{R})\mathrm{PGL}_2(\widehat{\mathbb{Z}}) \times \prod_{i=1}^{s} \mathbf{G}_i(\mathbb{R})\mathbf{G}_i(\widehat{\mathbb{Z}}).$$

For instance, we could replace for each index $i=1,\dots,s$ the full group $K_{\infty,i}=\mathbf{G}_i(\mathbb{R})$ by $K_{\infty,i}=\mathbf{G}_i(\mathbb{R})_{z_i}$, the stabilizer of a line

$$\mathbb{R}z_i \subset \mathbf{B}_i^0(\mathbb{R})$$

in the quadratic space of real trace-zero quaternions on which $\mathbf{G}_i$ act by conjugation.

In that case $\mathbf{G}_i(\mathbb{R})/K_{\infty,i}$ identifies with the ellipsoid of traceless quaternions of norm 1

$$\mathbf{B}_i^{0,1}(\mathbb{R}) = \{z \in \mathbf{B}_i(\mathbb{R}) : \mathrm{Tr}_{\mathbf{B}_i}(z) = 0,\ \mathrm{Nr}_{\mathbf{B}_i}(z) = 1\}.$$

Theorem 1.8 restricted to the $\prod_{i=0}^{s} K_{\infty,i}\, K_{\mathrm{f}}$-invariant functions and applied to sequences of torus orbits $[\mathbf{T}_n \mathrm{g}_n]$ for suitable g_n may be interpreted as a joint equidistribution statement as $n \to \infty$ for primitive representations of $|D_n|$ by the genus classes of the ternary quadratic spaces $(\mathbf{B}_i^0, \mathrm{Nr}_{\mathbf{B}_i})_{i=0,\dots,s}$. We leave it to the interested reader to work out this interpretation.

8. Invariance under the simply connected cover

In this section we discuss the main step towards the proof of Theorem 1.8, namely Theorem 8.4; we briefly review the standard approach. Let $[\mathbf{T}_{\iota_n} \mathrm{g}_n]$ be a sequence of toral packets and denote by μ_n the Haar probability measure on $[\mathbf{T}_{\iota_n} \mathrm{g}_n]$. We analyze possible limits of the measures μ_n. To this end, recall that the space of (Borel) measures ν on $[\mathbf{G}]$ with $\nu([\mathbf{G}]) \leq 1$ is compact (and metrizable) in the weak*-topology by a theorem of Banach and Alaoglu. Let $(\mu_{n_k})_k$ be an arbitrary convergent subsequence of the sequence $(\mu_n)_n$. This means that there is a measure μ on $[\mathbf{G}]$ with $\mu([\mathbf{G}]) \leq 1$ and with

$$\int_{[\mathbf{G}]} f \,\mathrm{d}\mu_{n_k} \to \int_{[\mathbf{G}]} f \,\mathrm{d}\mu$$

for all $f \in \mathcal{C}_c([\mathbf{G}])$. Such a measure μ is called a weak*-limit of the sequence $(\mu_n)_n$. To prove Theorem 1.8, we need to show that any such weak*-limit μ projects to the Haar measure $m_{[\mathbf{G}]_{K_{\mathrm{f}}}}$ on $[\mathbf{G}]_{K_{\mathrm{f}}}$, or equivalently, that for any K_{f}-invariant function $f \in \mathcal{C}_c([\mathbf{G}])$ we have

$$\int_{[\mathbf{G}]} f \,\mathrm{d}\mu = \int_{[\mathbf{G}]} f \,\mathrm{d}m_{[\mathbf{G}]}.$$

Theorem 8.4 establishes that any μ as above, that is, any weak*-limit of the measures $m_{[\mathbf{T}_{\iota_n} \mathrm{g}_n]}$ is a probability measure[2] and is invariant under the group of adelic points of the simply connected cover of $\mathbf{G}$.

In Section 9 we explain how the surjectivity assumption (1.5) allows us to deduce Theorem 1.8 from Theorem 8.4. A key ingredient in the proof of the latter is a generalization of Duke's result [14], cf. Theorem 8.1, which roughly speaking addresses Theorem 8.4 in the case when $\mathbf{G}$ has one simple factor. We then apply the joinings classification theorem of Einsiedler and Lindenstrauss [16] to deduce Theorem 8.4.

8.1. Invariance for one factor. Let $\mathbf{B}$ be a quaternion algebra defined over $\mathbb{Q}$ (possibly the split algebra Mat_2). Let $\mathbf{G} = \mathbf{P}\mathbf{B}^\times$ be the associated projective group and $\mathbf{G}(\mathbb{A})^+ < \mathbf{G}(\mathbb{A})$ the image of $\mathbf{B}^1(\mathbb{A})$ under the canonical projection of the subgroup $\mathbf{B}^1 < \mathbf{B}^\times$ of quaternions of norm 1. In the context of ergodic theory, $\mathbf{B}^1$ has a special role as it is generated by unipotents over the algebraic closure. The following theorem was stated (without proof)[3] in [18, Theorem 4.6].

[2] In other words, there is "no escape of mass". If $[\mathbf{G}]$ were compact, this would be automatic.

[3] A proof will be given in the forthcoming book [36].

Theorem 8.1 (Invariance in single factors). *Let* $\mathbf{B}$ *be a quaternion algebra over* $\mathbb{Q}$ *and let* $\mathbf{G} = \mathbf{PB}^\times$. *Let* $[\mathbf{T}_{\iota_n} g_n]$ *be a sequence of toral packets where* $\iota_n : \mathbf{K}_n \to \mathbf{B}(\mathbb{Q})$ *are embeddings of quadratic fields and where* $g_n \in \mathbf{G}(\mathbb{A})$. *Assume that*

$$\operatorname{disc}\big([\mathbf{T}_{\iota_n} g_n]\big) \to \infty \quad (n \to \infty).$$

Then any weak-limit of the normalized Haar measures on the packets* $[\mathbf{T}_{\iota_n} g_n]$ *is a probability measure invariant under* $\mathbf{G}(\mathbb{A})^+$.

Remark 8.2. Theorem 8.1 is a broad generalization of Duke's equidistribution theorems [14] and a consequence of deep results by many authors [6, 15, 37, 51]. It builds on the theory of automorphic forms and associated L-functions, in particular on Waldspurger's formula and on subconvexity bounds. We invite the reader to look at the discussion surrounding [18, Theorem 4.6] for more details.

Remark 8.3. For the purpose of proving Theorem 8.4, one can also assume that a fixed prime q_1 splits in all the quadratic fields $\mathbf{K}_n$. Under this splitting assumption, one can then use (for certain natural sequences of toral packets) the modern presentations of the *ergodic method* of Linnik [34] (for instance [22]) to prove Theorem 8.1. This has been carried out by the last named author in [53].

8.2. Joint invariance. We now upgrade Theorem 8.1 to multiple factors. Let us briefly recall the notation used in Theorem 1.8. Let $\mathbf{B}_i$ for $i = 0, \dots, s$ be a finite set of distinct quaternion algebras and let $\mathbf{G}_i$ be their of projective groups of units. Set

$$\mathbf{G} = \mathbf{G}_0 \times \cdots \times \mathbf{G}_s$$

and denote by $\mathbf{G}(\mathbb{A})^+ \subset \mathbf{G}(\mathbb{A})$ the product of the groups $\mathbf{G}_i(\mathbb{A})^+$ for $i = 0, \dots, s$. Without loss of generality we may and will assume that $\mathbf{G}_0 = \mathrm{PGL}_2$. Given a tuple $\iota = (\iota_0, \dots, \iota_s)$ of embeddings $\iota_i : \mathbf{K} \to \mathbf{B}_i$ of a given quadratic field $\mathbf{K}$, we obtain a tuple of morphisms of $\mathbb{Q}$-groups

$$\iota_i : \mathbf{T}_\mathbf{K} = \mathrm{Res}_{\mathbf{K}/\mathbb{Q}}(\mathbb{G}_m)/\mathbb{G}_m \to \mathbf{G}_i\,.$$

We denote by

$$\mathbf{T}_\iota = \{(\iota_0(t), \dots, \iota_s(t)) : t \in \mathbf{T}_\mathbf{K}\}$$

the diagonally embedded image.

Theorem 8.4 (Invariance in the product). *Let* $p_1, \dots, p_s$ *and* q_1, q_2 *be distinct odd primes. Let* $\mathbf{K}_n$ *for* $n \geq 1$ *be a sequence of quadratic fields such that for every* n,

(1) $p_1, \dots, p_s$ *are inert in* $\mathbf{K}_n$, *and*

(2) q_1 *and* q_2 *are split in* $\mathbf{K}_n$.

Let $\iota_n = (\iota_{i,n})_{i=0,\dots,s}$ *be a tuple of embeddings* $\iota_{i,n} : \mathbf{K}_n \to \mathbf{B}_i$ *and let* $\mathrm{g}_n \in \mathbf{G}(\mathbb{A})$. *If one has* $\operatorname{disc}([\mathbf{T}_{\iota_n} \mathrm{g}_n]) \to \infty$ *as* $n \to \infty$, *then any weak*-limit of the sequence of normalized Haar measures on the packets* $[\mathbf{T}_{\iota_n} \mathrm{g}_n]$ *is a probability measure invariant under* $\mathbf{G}(\mathbb{A})^+$.

Proof. As the groups $\mathbf{G}_i$ are not isogenous over $\mathbb{Q}$, Theorem 8.1 and [16, Theorem 1.8] imply the theorem. □

9. Proof of Theorem 1.8

In this section we upgrade Theorem 8.4 using the norm surjectivity assumption in (1.5) to obtain Theorem 1.8. We will also comment on stronger versions of Theorem 1.8 in Section 10.

9.1. Conditioning on $\mathbf{G}(\mathbb{A})^+$-orbits. We denote by m the Haar probability measure on $[\mathbf{G}]$. Let $\mathcal{A}$ be the preimage of the Borel σ-algebra on $[\mathbf{G}]/\mathbf{G}(\mathbb{A})^+$. In particular, $\mathcal{A}$ is countably generated and its atoms are the $\mathbf{G}(\mathbb{A})^+$-orbits in $[\mathbf{G}]$. As $\mathbf{G}(\mathbb{A})^+$ is normal in $\mathbf{G}(\mathbb{A})$, $\mathcal{A}$ is invariant under $\mathbf{G}(\mathbb{A})$. Also, each $\mathbf{G}(\mathbb{A})^+$-orbit is closed since it is of the form

$$\mathbf{G}(\mathbb{Q})\mathrm{g}\mathbf{G}(\mathbb{A})^+ = \mathbf{G}(\mathbb{Q})\mathbf{G}(\mathbb{A})^+\mathrm{g}$$

and $\mathbf{G}(\mathbb{Q})\mathbf{G}(\mathbb{A})^+$ is closed (this follows from a theorem of Borel and Harish-Chandra [4] applied to $\prod_i \mathbf{B}_i^1$).

For m-almost every element $x \in [\mathbf{G}]$ we may let $m_x^{\mathcal{A}}$ be the conditional measure of m on the atom of x. As the atoms of $\mathcal{A}$ are closed subsets, these measures are supported on the $\mathbf{G}(\mathbb{A})^+$-orbits (see [20, Chapter 5] for the definition and basic properties of conditional measures). By $\mathbf{G}(\mathbb{A})^+$-invariance of m, it follows that $m_x^{\mathcal{A}}$ is the $\mathbf{G}(\mathbb{A})^+$-invariant probability measure on the closed orbit $x\mathbf{G}(\mathbb{A})^+$ m-almost everywhere. Using that, we may as well define $m_x^{\mathcal{A}}$ to be the unique $\mathbf{G}(\mathbb{A})^+$-invariant probability measure on $x\mathbf{G}(\mathbb{A})^+$ *everywhere*, preserving the defining property of conditional measures.

9.1.1. The space of bounded uniformly continuous functions. For what follows, it will be convenient to work with a certain class of test functions. A function $f : [\mathbf{G}] \to \mathbb{C}$ is *uniformly continuous* if for all $\varepsilon > 0$ there is a neighborhood $U \subseteq \mathbf{G}(\mathbb{A})$ of the identity such that

$$\sup_{\mathrm{g}\in U,\, x\in[\mathbf{G}]} |f(x\mathrm{g}) - f(x)| < \varepsilon.$$

We note that the bounded uniformly continuous functions form a subspace $\mathcal{C}_u([\mathbf{G}])$ of the continuous functions that contains the space $\mathcal{C}_c([\mathbf{G}])$ of compactly supported continuous functions on $[\mathbf{G}]$. Equipped with the uniform norm $\mathcal{C}_u([\mathbf{G}])$ is a Banach algebra.

The natural action of $\mathbf{G}(\mathbb{A})$ on the space of bounded measurable functions given by $g \cdot f(x) = f(xg)$ preserves $\mathcal{C}_u([\mathbf{G}])$ and the resulting representation is strongly continuous. In fact, the space $\mathcal{C}_u([\mathbf{G}])$ can be identified with the space of continuous vectors for the representation of $\mathbf{G}(\mathbb{A})$ on $L^\infty_m([\mathbf{G}])$.

9.1.2. Decomposing $\mathcal{C}_u([\mathbf{G}])$. We use the conditional measures for $\mathcal{A}$ to decompose functions on $[\mathbf{G}]$. For f a bounded measurable function on $[\mathbf{G}]$ define

$$f_{\mathrm{char}} : x \mapsto \int_{[\mathbf{G}]} f \, \mathrm{d}m_x^{\mathcal{A}}.$$

Note that f_{char} is $\mathbf{G}(\mathbb{A})^+$-invariant and $\mathcal{A}$-measurable. Moreover, the two functions f_{char} and $f - f_{\mathrm{char}}$ are bounded. The function $f - f_{\mathrm{char}}$ satisfies that

$$\int_{[\mathbf{G}]} (f - f_{\mathrm{char}}) \, \mathrm{d}m_x^{\mathcal{A}} = 0$$

since f_{char} is constant on $\mathbf{G}(\mathbb{A})^+$-orbits.

Remark 9.1. The map $f \mapsto f_{\mathrm{char}}$ is introduced in [29] as a projection operator from $L^2_m([\mathbf{G}])$ onto the *character spectrum* of $L^2_m([\mathbf{G}])$, i.e. the subspace of $\mathbf{G}(\mathbb{A})^+$-invariant functions. Note that for functions in the orthogonal complement of the character spectrum Theorem 1.8 follows directly from Theorem 8.4 without assuming K_{f}-invariance of the function – see [29, Corollary 3.3] as well as Lemma 9.3 below.

Lemma 9.2. *For any $f \in \mathcal{C}_u([\mathbf{G}])$ we have $f_{\mathrm{char}} \in \mathcal{C}_u([\mathbf{G}])$. Furthermore, if f is invariant under a subgroup $H < \mathbf{G}(\mathbb{A})$, then so is f_{char}.*

We have thus obtained for any function $f \in \mathcal{C}_u([\mathbf{G}])$ the decomposition

$$f = f_{\mathrm{char}} + (f - f_{\mathrm{char}})$$

into a $\mathbf{G}(\mathbb{A})^+$-invariant function and a function with zero integral over all $\mathbf{G}(\mathbb{A})^+$-orbits (which respects additional invariance of f).

Proof of Lemma 9.2. We first prove that f_{char} is uniformly continuous. Let $\varepsilon > 0$ be given and choose a symmetric neighborhood U of the identity in $\mathbf{G}(\mathbb{A})$ for f and ε as in the definition of uniform continuity. Let $x \in [\mathbf{G}]$ and $\mathrm{g} \in U$ be arbitrary. Invariance of $\mathcal{A}$ under the action of $\mathbf{G}(\mathbb{A})$, uniform continuity of f, and the triangle inequality imply that f_{char} is uniformly continuous. If f is H-invariant, we see that

$$f_{\mathrm{char}}(xh) = \int_{[\mathbf{G}]} f \,\mathrm{d}m^{\mathcal{A}}_{xh} = \int_{[\mathbf{G}]} h.f \,\mathrm{d}m^{\mathcal{A}}_{x} = \int_{[\mathbf{G}]} f \,\mathrm{d}m^{\mathcal{A}}_{x} = f_{\mathrm{char}}(x)$$

as claimed. □

9.2. Concluding the proof of Theorem 1.8. We recall that our final goal is to prove that any weak*-limit of the Haar measures on the toral packets in Theorem 1.8 is equal to $m_{[\mathbf{G}]_{K_{\mathrm{f}}}}$. This amounts to showing that $\int_{[\mathbf{G}]} f \,\mathrm{d}\mu = \int_{[\mathbf{G}]} f \,\mathrm{d}m$ for a large class of K_{f}-invariant functions f and any such weak*-limit μ.

Lemma 9.3. *Let μ be any measure on $[\mathbf{G}]$ invariant under $\mathbf{G}(\mathbb{A})^+$. Then for any function $f \in \mathcal{C}_u([\mathbf{G}])$ with $f_{\mathrm{char}} = 0$ we have*

$$\int_{[\mathbf{G}]} f \,\mathrm{d}\mu = \int_{[\mathbf{G}]} f \,\mathrm{d}m = 0.$$

In the context of Theorem 1.8, the measure μ is $\mathbf{G}(\mathbb{A})^+$-invariant by Theorem 8.4.

Proof. Let $\{\mu^{\mathcal{A}}_x : x \in [\mathbf{G}]\}$ be a family of conditional measures for μ with respect to $\mathcal{A}$. As μ is $\mathbf{G}(\mathbb{A})^+$-invariant, it follows that the measure $\mu^{\mathcal{A}}_x$, which is supported on the orbit $x\mathbf{G}(\mathbb{A})^+$, is $\mathbf{G}(\mathbb{A})^+$-invariant for μ-almost all $x \in [\mathbf{G}]$. By uniqueness of the invariant measure, it follows that $\mu^{\mathcal{A}}_x = m^{\mathcal{A}}_x$ for μ-almost all $x \in [\mathbf{G}]$. Thus we have shown that

$$\int_{[\mathbf{G}]} f \,\mathrm{d}\mu^{\mathcal{A}}_x = \int_{[\mathbf{G}]} f \,\mathrm{d}m^{\mathcal{A}}_x = f_{\mathrm{char}}(x) = 0$$

for μ-almost every $x \in [\mathbf{G}]$. In particular, we obtain the statement of the lemma by the characterizing properties of conditional measures. □

Proof of Theorem 1.8. Recall that we have $K_{\mathrm{f}} = \prod_i K_{\mathrm{f},i}$, where for any i the compact open subgroup $K_{\mathrm{f},i} < \mathbf{G}_i(\mathbb{A}_{\mathrm{f}})$ satisfies (1.5), i.e. that

$$\mathrm{Nr}_{\mathbf{B}_i} : K_{\mathrm{f},i} \to \widehat{\mathbb{Z}}^\times \big/ (\widehat{\mathbb{Z}}^\times)^2$$

is surjective.

Let μ be a weak*-limit of the Haar measures in Theorem 1.8. We need to show that for any K_{f}-invariant compactly supported f on $[\mathbf{G}]$ we have

$$\int_{[\mathbf{G}]} f \,\mathrm{d}\mu = \int_{[\mathbf{G}]} f \,\mathrm{d}m. \tag{9.1}$$

By Theorem 8.4 the measure μ is $\mathbf{G}(\mathbb{A})^+$-invariant and hence Lemma 9.3 applies to show (9.1) for $f - f_{\mathrm{char}}$ as $(f - f_{\mathrm{char}})_{\mathrm{char}} = 0$. It thus remains to check (9.1) for f_{char} which is $K_{\mathrm{f}}\,\mathbf{G}(\mathbb{A})^+$-invariant by Lemma 9.2. Note that $K_{\mathrm{f}}\,\mathbf{G}(\mathbb{A})^+$ is a subgroup of $\mathbf{G}(\mathbb{A})$ as $\mathbf{G}(\mathbb{A})^+$ is normal.

We claim that such a function f_{char} is constant in which case (9.1) is obvious. This follows from the fact that the double quotient

$$\mathbf{G}(\mathbb{Q}) \backslash \mathbf{G}(\mathbb{A}) \big/ K_{\mathrm{f}}\,\mathbf{G}(\mathbb{A})^+$$

is a singleton under our assumptions on K_{f}. To this end, it suffices to prove that for any $i \in \{0, \dots, s\}$ the double quotient

$$\mathbf{G}_i(\mathbb{Q}) \backslash \mathbf{G}_i(\mathbb{A}) \big/ K_{\mathrm{f},i}\,\mathbf{G}_i(\mathbb{A})^+ \tag{9.2}$$

is a singleton. For this we consider the group homomorphism induced by the reduced norm $\mathrm{Nr}_i = \mathrm{Nr}_{\mathbf{B}_i}$

$$\mathrm{Nr}_i : \mathbf{G}_i(\mathbb{Q}) \backslash \mathbf{G}_i(\mathbb{A}) / K_{\mathrm{f},i}\,\mathbf{G}_i(\mathbb{A})^+ \to \mathbb{Q}^\times \backslash \mathbb{A}^\times / \mathbb{A}^{\times 2} \mathrm{Nr}_i(K_{\mathrm{f},i}).$$

We note first that it is injective hence an isomorphism onto its image.

Let us compute the image: for any prime q the norm $\mathrm{Nr}_i : \mathbf{B}_i^\times(\mathbb{Q}_q) \to \mathbb{Q}_q^\times$ is surjective since any non-degenerate quadratic form in five variables over $\mathbb{Q}_q$ is isotropic [5, Chapter 4]. Over the real numbers, the norm $\mathrm{Nr}_i : \mathbf{B}_i(\mathbb{R})^\times \to \mathbb{R}^\times$ is surjective if $\mathbf{B}_i$ is indefinite and otherwise it has image $\mathbb{R}_{>0}$. It follows that

$$\mathrm{Nr}_i(\mathbf{B}_i^\times(\mathbb{A})) = \begin{cases} \mathbb{A}^\times & \text{if } \mathbf{B}_i \text{ is indefinite,} \\ \mathbb{R}_{>0}\mathbb{A}_{\mathrm{f}}^\times & \text{if } \mathbf{B}_i \text{ is definite} \end{cases}.$$

In addition, by the Hasse-Minkowski Theorem [5, Chapter 6] this also implies that

$$\mathrm{Nr}_i(\mathbf{B}_i^\times(\mathbb{Q})) = \begin{cases} \mathbb{Q}^\times & \text{if } \mathbf{B}_i \text{ is indefinite,} \\ \mathbb{Q}_{>0} & \text{if } \mathbf{B}_i \text{ is definite} \end{cases}.$$

From this we conclude that (9.2) is isomorphic to

$$\begin{cases} \mathbb{Q}^\times \backslash \mathbb{A}^\times / \mathbb{A}^{\times 2} \mathrm{Nr}_i(K_{\mathrm{f},i}) & \text{if } \mathbf{B}_i \text{ is indefinite,} \\ \mathbb{Q}_{>0} \backslash \mathbb{R}_{>0} \times \mathbb{A}_{\mathrm{f}}^\times / \mathbb{A}^{\times 2} \mathrm{Nr}_i(K_{\mathrm{f},i}) & \text{if } \mathbf{B}_i \text{ is definite.} \end{cases}$$

Under the assumption (1.5) (i.e. $\mathrm{Nr}_i(K_{\mathrm{f},i}) = \widehat{\mathbb{Z}}^\times/(\widehat{\mathbb{Z}}^\times)^2$) this is either

$$\mathbb{A}^\times / \mathbb{Q}^\times \widehat{\mathbb{Z}}^\times \mathbb{A}^{\times 2} \text{ or } \mathbb{R}_{>0}\mathbb{A}_{\mathrm{f}}^\times / \mathbb{Q}_{>0} \widehat{\mathbb{Z}}^\times \mathbb{A}^{\times 2}$$

and both are trivial since $\mathbb{A}_{\mathrm{f}}^\times = \mathbb{Q}_{>0}\widehat{\mathbb{Z}}^\times$. This concludes the proof of the above claim and thus also of the theorem. □

9.3. The case of Eichler orders. In this subsection we remark that assumption (1.5) holds more generally for open-compact subgroups associated to Eichler orders (such as maximal orders). This extension is important as it allows to prove joint equidistributions results similar to Theorem 7.1 for *Heegner points*.

Definition 9.4. An Eichler order in a quaternion algebra $\mathbf{B}$ is an intersection of two maximal orders.

Being an Eichler order is a local property. Indeed, an order $\mathcal{O} \subset \mathbf{B}(\mathbb{Q})$ is Eichler if and only if it is everywhere locally Eichler: for every prime q, $\mathcal{O}_q = \mathcal{O} \otimes \mathbb{Z}_q$ is the intersection of two maximal orders in $\mathbf{B}(\mathbb{Q}_q)$.

Moreover, one has the following classification of local Eichler orders in the quaternion algebra $\mathbf{B}(\mathbb{Q}_q)$ (see [50, Proposition 13.3.4, Proposition 23.4.3]):

- If $\mathbf{B}$ is ramified at q, then $\mathcal{O}_q$ is the unique maximal order of $\mathbf{B}(\mathbb{Q}_q)$ given by
$$\mathcal{O}_q = \{x \in \mathbf{B}(\mathbb{Q}_q) : \mathrm{Nr}(x) \in \mathbb{Z}_q\}.$$
- If $\mathbf{B}$ is non-ramified at q, one has $\mathbf{B}(\mathbb{Q}_q) \simeq \mathrm{Mat}_2(\mathbb{Q}_q)$ and under this identification, there is some $e \geq 0$ such that $\mathcal{O}_q$ is conjugate to the order
$$\left\{ \begin{pmatrix} a & b \\ q^e c & d \end{pmatrix} : a, b, c, d \in \mathbb{Z}_q \right\}.$$

The classification implies the following lemma verifying condition (1.5) for the open-compact subgroup $\widehat{\mathcal{O}}^\times$ when $\mathcal{O}$ is an Eichler order.

Lemma 9.5. *For $\mathcal{O} \subset \mathbf{B}(\mathbb{Q})$ an Eichler order we have*
$$\mathrm{Nr}(\widehat{\mathcal{O}}^\times) = \widehat{\mathbb{Z}}^\times.$$

10. Further refinements

In this section we will analyze under which assumptions on sequences of toral packets $[\mathbf{T}_n g_n]_{K_\mathrm{f}}$ Theorem 1.8 holds for a general compact open subgroup $K_\mathrm{f} = \prod_i K_{\mathrm{f},i} \subset \mathbf{G}(\mathbb{A}_\mathrm{f})$.

By Lemma 9.3 it is sufficient to check whether condition (9.1) holds for functions invariant under $K_\mathrm{f}\mathbf{G}(\mathbb{A})^+$, i.e. functions on the quotient $\mathbf{G}_{\mathrm{char}}/K_\mathrm{f}$, where $\mathbf{G}_{\mathrm{char}}$ denotes the abelian group
$$\mathbf{G}_{\mathrm{char}} = \mathbf{G}(\mathbb{Q})\backslash\mathbf{G}(\mathbb{A})/\mathbf{G}(\mathbb{A})^+.$$
Furthermore, we only have to check (9.1) for K_f-invariant characters on $\mathbf{G}_{\mathrm{char}}$. We start by spelling out what they are.

10.1. Characters on $\mathbf{G}_{\mathrm{char}}$. We have $\mathbf{G}_{\mathrm{char}} = \prod_i \mathbf{G}_{i,\mathrm{char}}$, where
$$\mathbf{G}_{i,\mathrm{char}} = \mathbf{G}_i(\mathbb{Q})\backslash\mathbf{G}_i(\mathbb{A})/\mathbf{G}_i(\mathbb{A})^+.$$
Recall that in the course of proving Theorem 1.8 we have also established the following lemma.

Lemma 10.1. *For any $i \in \{0, \dots, s\}$ the reduced norm induces isomorphisms*

$$\mathrm{Nr}_i : \mathbf{G}_{i,\mathrm{char}} \simeq \mathbb{Q}_{>0}\backslash \mathbb{R}_{>0} \times \mathbb{A}_{\mathrm{f}}^{\times} / \mathbb{A}^{\times 2}$$

if $\mathbf{B}_i$ is definite and

$$\mathrm{Nr}_i : \mathbf{G}_{i,\mathrm{char}} \simeq \mathbb{Q}^{\times}\backslash \mathbb{A}^{\times} / \mathbb{A}^{\times 2}.$$

if $\mathbf{B}_i$ is indefinite.

Note that the natural homomorphism

$$\mathbb{Q}_{>0}\backslash \mathbb{R}_{>0} \times \mathbb{A}_{\mathrm{f}}^{\times} / \mathbb{A}^{\times 2} \to \mathbb{Q}^{\times}\backslash \mathbb{A}^{\times} / \mathbb{A}^{\times 2}$$

is an isomorphism as any element of $\mathbb{A}^{\times}$ can be multiplied by $-1 \in \mathbb{Q}^{\times}$ if necessary to have a positive real component. Lemma 10.1 thus gives an isomorphism (independent of the ramification at the archimedean place)

$$\mathrm{Nr}_i : \mathbf{G}_{i,\mathrm{char}} \simeq \mathbb{Q}^{\times}\backslash \mathbb{A}^{\times} / \mathbb{A}^{\times 2}. \tag{10.1}$$

In particular, $\mathbf{G}_{\mathrm{char}}$ is a compact abelian group, every continuous function on $\mathbf{G}_{\mathrm{char}}$ is uniformly continuous, and $\mathcal{C}(\mathbf{G}_{\mathrm{char}})$ is densely generated by its group of characters $\widehat{\mathbf{G}_{\mathrm{char}}}$.

By the previous lemma, any character of $\mathbf{G}_{i,\mathrm{char}}$ is of the shape $\chi_i \circ \mathrm{Nr}_i$ for a quadratic Hecke character χ_i of $\mathbb{Q}$, i.e. a character

$$\chi_i : \mathbb{Q}^{\times}\backslash \mathbb{A}^{\times} / \mathbb{A}^{\times 2} \to \{\pm 1\}.$$

Thus, any character $\chi \in \widehat{\mathbf{G}_{\mathrm{char}}}$ is of the shape

$$\mathrm{g} = (g_i)_i \in \mathbf{G}_{\mathrm{char}} \mapsto \chi(\mathrm{g}) = \prod_{i=0}^{s} \chi_i(\mathrm{Nr}_i(g_i)) \tag{10.2}$$

for a uniquely defined tuple $(\chi_i)_i$ of quadratic Hecke characters as above. The K_{f}-invariant characters correspond to the tuples of characters $(\chi_i)_i$, where χ_i is $\mathrm{Nr}_i(K_{\mathrm{f},i})$-invariant for all i.

10.2. The torus integral for a character. Let χ be a character of $\mathbf{G}_{\mathrm{char}}$ given by a tuple $(\chi_i)_i$ of quadratic Hecke characters as in (10.2). We view χ as a $\mathbf{G}(\mathbb{A})^+$-invariant function in $\mathcal{C}_u([\mathbf{G}])$. Let $[\mathbf{T}_\iota \mathrm{g}] \subset [\mathbf{G}]$ be a toral packet with associated quadratic field $\mathbf{K}$. As of Weyl's equidistribution theorem, we consider the torus integral

$$\int_{[\mathbf{T}_\iota \mathrm{g}]} \chi = \int_{[\mathbf{T}_\iota]} \chi(t\,\mathrm{g})\,\mathrm{d}t.$$

Since χ is a character, we have

$$\int_{[\mathbf{T}_\iota]} \chi(t\,\mathrm{g})\,\mathrm{d}t = \chi(\mathrm{g}) \int_{[\mathbf{T}_\iota]} \chi(t)\,\mathrm{d}t.$$

Let Π be the product map

$$\Pi : (\chi_i)_i \mapsto \prod_i \chi_i$$

on quadratic Hecke characters.

Proposition 10.2. *Let $(\chi_i)_i$ be a tuple of quadratic Hecke characters and let χ be the associated character on $\mathbf{G}_{\mathrm{char}}$ as in* (10.2)*.*

- *If $\Pi(\chi_i)_i \equiv 1$, then for any torus orbit $\mathbf{T}_\iota$ we have*
$$\int_{[\mathbf{T}_\iota]} \chi(t)\,\mathrm{d}t = 1.$$
- *If $\Pi(\chi_i)_i \not\equiv 1$, let $\mathbf{K}_{\Pi(\chi_i)_i}$ be the quadratic field corresponding to the Legendre symbol corresponding to the Hecke character $\Pi(\chi_i)_i$. For any torus $\mathbf{T}_\iota$ with associated quadratic field $\mathbf{K}$, we have*
$$\int_{[\mathbf{T}_\iota]} \chi(t)\,\mathrm{d}t = \begin{cases} 0 & \text{if } \mathbf{K} \neq \mathbf{K}_{\Pi(\chi_i)_i}, \\ 1 & \text{else.} \end{cases}$$

Proof. Note that for any $x \in \mathbf{K}$ and any i we have $\mathrm{Nr}_i(\iota_i(x)) = \mathrm{Nr}_{\mathbf{K}}(x)$, where $\mathrm{Nr}_{\mathbf{K}}$ denotes the norm form of $\mathbf{K}/\mathbb{Q}$. Hence, we have

$$\int_{[\mathbf{T}_\iota]} \chi(t)\,\mathrm{d}t = \int_{[\mathbf{T}_{\mathbf{K}}]} \prod_i \chi_i(\mathrm{Nr}_i(\iota_i(t)))\,\mathrm{d}t = \int_{[\mathbf{T}_{\mathbf{K}}]} \Pi(\chi_i)_i(\mathrm{Nr}_{\mathbf{K}}(t))\,\mathrm{d}t.$$

This shows the first part, so we assume that $\Pi(\chi_i)_i$ is non-trivial.

The character $\Pi(\chi_i)_i$ corresponds to a classical Legendre symbol character and is associated with some uniquely defined quadratic field $\mathbf{K}_{\Pi(\chi_i)_i}$. If $\mathbf{K} = \mathbf{K}_{\Pi(\chi_i)_i}$, then we have by definition of the Legendre symbol

$$\Pi(\chi_i)_i \circ \mathrm{Nr}_{\mathbf{K}} = 1 \implies \int_{[\mathbf{T}_{\mathbf{K}}]} \Pi(\chi_i)_i(\mathrm{Nr}_{\mathbf{K}}(t))\,\mathrm{d}t = 1.$$

If $\mathbf{K} \neq \mathbf{K}_{\Pi(\chi_i)_i}$, there exists a prime p split in $\mathbf{K}$ and inert in $\mathbf{K}_{\Pi(\chi_i)_i}$ so that for t_p in the corresponding idele class one has

$$\Pi(\chi_i)_i\big(\mathrm{Nr}_{\mathbf{K}}(t_p)\big) = -1 \implies \int_{[\mathbf{T}_{\mathbf{K}}]} \Pi(\chi_i)_i(\mathrm{Nr}_{\mathbf{K}}(t))\,\mathrm{d}t = 0$$

as follows from the substitution $t \mapsto t t_p$, where t_p is as above. □

Definition 10.3. Let $K_{\mathrm{f}} = \prod_i K_{\mathrm{f},i} \subset \mathbf{G}(\mathbb{A}_{\mathrm{f}})$ be a compact open subgroup. The set of *exceptional fields* attached to K_{f} is defined as the set of quadratic fields attached to the non-trivial products $\Pi(\chi_i)_i$ for which the corresponding character χ of $\mathbf{G}_{\mathrm{char}}$ is K_{f} invariant:

$$\mathscr{K}(K_{\mathrm{f}}) = \left\{ \mathbf{K}_{\Pi(\chi_i)_i} : \Pi(\chi_i)_i \neq 1,\ \chi = \prod_i \chi_i \circ \mathrm{Nr}_{\mathbf{B}_i}\ K_{\mathrm{f}}\text{-invariant} \right\}.$$

In particular, given a limit measure μ of a sequence of toral packets $[\mathbf{T}_{\iota_n} \mathrm{g}_n]$ for which the underlying quadratic field is constant equal to $\mathbf{K}_{\Pi(\chi_i)_i}$, the measure μ cannot satisfy (9.1) for the test function $\chi = \prod_i \chi_i \circ \mathrm{Nr}_{\mathbf{B}_i}$ if the latter is K_{f}-invariant. Indeed, all torus integrals in that case have modulus 1 as

$$\left| \int_{[\mathbf{T}_{\iota_n} \mathrm{g}_n]} \chi \right| = |\chi(\mathrm{g}_n)| = 1$$

by Proposition 10.2. On the other hand, since χ is non-trivial

$$\int_{[\mathbf{G}]} \chi = \prod_i \int_{[\mathbf{G}_i]} \chi_i(\mathrm{Nr}_{\mathbf{B}_i}(g_i))\,\mathrm{d}g_i = 0.$$

Thus, these finitely many exceptional fields are natural obstructions to equidistribution on $[\mathbf{G}]_{K_\mathrm{f}}$. Therefore, one only has to consider sequences of toral packets $[\mathbf{T}_{\iota_n}\mathrm{g}_n]$ whose associated quadratic fields $\mathbf{K}_n$ are not exceptional.

We remark that $\mathscr{K}(K_\mathrm{f})$ is a finite set as $\mathbf{G}_{\mathrm{char}}/K_\mathrm{f}$ is finite.

10.3. A refined equidistribution criterion. We denote by

$$\pi_i : \mathbf{G}_i(\mathbb{A}) \to \mathbf{G}_{i,\mathrm{char}}, \quad \pi : \mathbf{G}(\mathbb{A}) \to \mathbf{G}_{\mathrm{char}}$$

the natural projections. We also define the closed diagonal subgroup

$$\Delta\mathbf{G}_{\mathrm{char}} = \{h \in \mathbf{G}_{\mathrm{char}} : \mathrm{Nr}_i(h_i) = \mathrm{Nr}_j(h_j) \text{ for all } i, j\}.$$

Here, the condition $\mathrm{Nr}_i(h_i) = \mathrm{Nr}_j(h_j)$ is understood in the sense of (10.1).

Corollary 10.4. *Let $K_\mathrm{f} = \prod_i K_{\mathrm{f},i} < \mathbf{G}(\mathbb{A}_\mathrm{f})$ be a compact open subgroup. Let $\mathscr{K}(K_\mathrm{f})$ be the set of exceptional quadratic fields attached to it. Let q_1, q_2 be distinct odd primes. For any sequence $\mathrm{g}_n \in \mathbf{G}(\mathbb{A})$ and any sequence of diagonally embedded tori $\mathbf{T}_n \subset \mathbf{G}$ attached to quadratic fields $\mathbf{K}_n$ such that*

- *for any n, $\mathbf{K}_n \notin \mathscr{K}(K_\mathrm{f})$,*
- *$\mathrm{disc}([\mathbf{T}_n\mathrm{g}_n]) \to \infty$ for $n \to \infty$, and*
- *q_1 and q_2 are split in $\mathbf{K}_n$ for every n,*

the following are equivalent:

(1) *The packets $[\mathbf{T}_n\mathrm{g}_n]_{K_\mathrm{f}}$ equidistribute in $[\mathbf{G}]_{K_\mathrm{f}}$.*

(2) $\Delta\mathbf{G}_{\mathrm{char}}\,\pi(K_\mathrm{f}) = \mathbf{G}_{\mathrm{char}}$.

Proof. By Theorem 8.4, Lemma 9.3, Proposition 10.2 and our assumption that the fields $\mathbf{K}_n$ are never exceptional, equidistribution in $[\mathbf{G}]_{K_\mathrm{f}}$ is equivalent to the non-existence of a character χ of $\mathbf{G}_{\mathrm{char}}$ which is non-trivial, K_f-invariant and such that $\Pi(\chi_i)_i$ is trivial. But $\Pi(\chi_i)_i$ being trivial is equivalent to the tuple $(\chi_i \circ \mathrm{Nr}_i)_i$ being constant equal to 1 along the diagonal subgroup $\Delta\mathbf{G}_{\mathrm{char}}$ and χ being K_f-invariant is equivalent to $(\chi_i)_i$ being $\pi(K_\mathrm{f})$-invariant (hence constant equal to 1 along $\pi(K_\mathrm{f})$). □

Acknowledgement. We want to express our gratitude towards the referee, whose careful reading of the manuscript improved the exposition and helped us remove an inaccuracy present in a preliminary version of this article. We also thank Valentin Blomer, Farrell Brumley, Brian Conrad, Henri Darmon, Dick Gross, Jennifer-Jayne Jakob, Ilya Khayutin, Bjorn Poonen, Dinakar Ramakrishnan and Tomer Schlank for helpful discussions. Part of this work was carried out while Philippe Michel was visiting the Department of Mathematics at Caltech, while Manuel Luethi was visiting the Einstein institute of Mathematics at the Hebrew University of Jerusalem, and while the authors were visiting the Hausdorff Research Institute during the program "Dynamics: Topology and Numbers".

References

[1] *M. Aka*, *M. Einsiedler* and *U. Shapira*, Integer points on spheres and their orthogonal grids, J. Lond. Math. Soc. (2) **93** (2016), no. 1, 143–158.

[2] *M. Aka*, *M. Einsiedler* and *U. Shapira*, Integer points on spheres and their orthogonal lattices, Invent. Math. **206** (2016), no. 2, 379–396.

[3] *M. Aka*, *M. Einsiedler*, and *A. Wieser*, Planes in four space and four associated CM points, preprint 2019, `https://arxiv.org/abs/1901.05833`; to appear in Duke Math. J.

[4] *A. Borel* and *Harish-Chandra*, Arithmetic subgroups of algebraic groups, Ann. of Math. (2) **75** (1962), 485–535.

[5] *J. W. S. Cassels*, Rational quadratic forms, London Math. Soc. Monogr. **13**, Academic Press, London 1978.

[6] *L. Clozel* and *E. Ullmo*, Équidistribution de mesures algébriques, Compos. Math. **141** (2005), no. 5, 1255–1309.

[7] *B. Conrad*, Gross–Zagier revisited, in: Heegner points and Rankin L-series. With an appendix by W. R. Mann, Math. Sci. Res. Inst. Publ. **49**, Cambridge University Press, Cambridge (2004), 67–163.

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

[9] *C. Cornut* and *D. Jetchev*, Liftings of reduction maps for quaternion algebras, Bull. Lond. Math. Soc. **45** (2013), no. 2, 370–386.

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

[11] *C. Cornut* and *V. Vatsal*, Nontriviality of Rankin-Selberg L-functions and CM points, in: L-functions and Galois representations, London Math. Soc. Lecture Note Ser. **320**, Cambridge University Press, Cambridge (2007), 121–186.

[12] *D. A. Cox*, Primes of the form $x^2 + ny^2$: Fermat, class field theory and complex multiplication, John Wiley & Sons, New York 1989.

[13] *M. Deuring*, Die Typen der Multiplikatorenringe elliptischer Funktionenkörper, Abh. Math. Sem. Hansischen Univ. **14** (1941), 197–272.

[14] *W. Duke*, Hyperbolic distribution problems and half-integral weight Maass forms, Invent. Math. **92** (1988), no. 1, 73–90.

[15] *W. Duke*, *J. Friedlander* and *H. Iwaniec*, Bounds for automorphic L-functions, Invent. Math. **112** (1993), no. 1, 1–8.

[16] *M. Einsiedler* and *E. Lindenstrauss*, Joinings of higher rank torus actions on homogeneous spaces, Publ. Math. Inst. Hautes Études Sci. **129** (2019), 83–127.

[17] *M. Einsiedler*, *E. Lindenstrauss*, *P. Michel* and *A. Venkatesh*, Distribution of periodic torus orbits on homogeneous spaces, Duke Math. J. **148** (2009), no. 1, 119–174.

[18] *M. Einsiedler*, *E. Lindenstrauss*, *P. Michel* and *A. Venkatesh*, Distribution of periodic torus orbits and Duke's theorem for cubic fields, Ann. of Math. (2) **173** (2011), no. 2, 815–885.

[19] *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** (2012), no. 3–4, 249–313.

[20] *M. Einsiedler* and *T. Ward*, Ergodic theory with a view towards number theory, Grad. Texts in Math. **259**, Springer, London 2011.

[21] *N. Elkies*, *K. Ono* and *T. Yang*, Reduction of CM elliptic curves and modular function congruences, Int. Math. Res. Not. IMRN **2005** (2005), no. 44, 2695–2707.

[22] *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 Institute of Fundamental Research, Mumbai (2013), 119–185.

[23] *J. Giraud*, Remarque sur une formule de Shimura-Taniyama, Invent. Math. **5** (1968), 231–236.

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

[25] *B. H. Gross*, Heights and the special values of L-series, in: Number theory (Montreal 1985), CMS Conf. Proc. **7**, American Mathematical Society, Providence (1987), 115–187.

[26] *S. Herrero*, *R. Menares*, and *J. Rivera-Letelier*, p-adic distribution of cm points and Hecke orbits II: Linnik equidistribution on the supersingular locus, preprint 2021.

[27] *H. Iwaniec*, Fourier coefficients of modular forms of half-integral weight, Invent. Math. **87** (1987), no. 2, 385–401.

[28] *B. Kane*, CM liftings of supersingular elliptic curves, J. Théor. Nombres Bordeaux **21** (2009), no. 3, 635–663.

[29] *I. Khayutin*, Joint equidistribution of CM points, Ann. of Math. (2) **189** (2019), no. 1, 145–276.

[30] *I. Khayutin*, Equidistribution on Kuga-Sato varieties of torsion points on CM elliptic curves, J. Eur. Math. Soc. (JEMS) **23** (2021), no. 9, 2949–3016.

[31] *S. Lang*, Elliptic functions. With an appendix by J. Tate, 2nd ed., Grad. Texts in Math. **112**, Springer, New York 1987.
[32] *K. Lauter* and *B. Viray*, On singular moduli for arbitrary discriminants, Int. Math. Res. Not. IMRN **2015** (2015), no. 19, 9206–9250.
[33] *S. Lester* and *M. Radziwiłł*, Quantum unique ergodicity for half-integral weight automorphic forms, Duke Math. J. **169** (2020), no. 2, 279–351.
[34] *Y. V. Linnik*, Ergodic properties of algebraic fields. Translated from the Russian by M. S. Keane, Ergeb. Math. Grenzgeb. (3) **45**, Springer, New York 1968.
[35] *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.
[36] *P. Michel*, Equidistribution, periods and subconvexity, in preparation.
[37] *P. Michel* and *A. Venkatesh*, The subconvexity problem for GL_2, Publ. Math. Inst. Hautes Études Sci. **111** (2010), 171–271.
[38] *J. Milne*, Complex multiplication, course notes, Lecture notes 2006, `https://www.jmilne.org/math/CourseNotes/cm.html`.
[39] *V. Platonov* and *A. Rapinchuk*, Algebraic groups and number theory. Translated from the 1991 Russian original by Rachel Rowen, Pure and Applied Mathematics **139**, Academic Press, Boston 1994.
[40] *M. Radziwiłł* and *K. Soundararajan*, Moments and distribution of central L-values of quadratic twists of elliptic curves, Invent. Math. **202** (2015), no. 3, 1029–1068.
[41] *M. Ratner*, Raghunathan's conjectures for Cartesian products of real and p-adic Lie groups, Duke Math. J. **77** (1995), no. 2, 275–382.
[42] *J.-P. Serre*, Complex multiplication, in: Algebraic number theory (Brighton 1965), Thompson, Washington, D.C. (1967), 292–296.
[43] *J.-P. Serre*, A course in arithmetic. Translated from the French, Grad. Texts in Math. **7**, Springer, New York 1973.
[44] *J.-P. Serre* and *J. Tate*, Good reduction of abelian varieties, Ann. of Math. (2) **88** (1968), 492–517.
[45] *J. H. Silverman*, Advanced topics in the arithmetic of elliptic curves, Grad. Texts in Math. **151**, Springer, New York 1994.
[46] *J. H. Silverman*, The arithmetic of elliptic curves, 2nd ed., Grad. Texts in Math. **106**, Springer, Dordrecht 2009.
[47] *A. Sutherland*, Elliptic curves, MIT Course 18.783 2019, `https://math.mit.edu/classes/18.783/2019/lectures.html`.
[48] *V. Vatsal*, Uniform distribution of Heegner points, Invent. Math. **148** (2002), no. 1, 1–46.
[49] *M.-F. Vignéras*, Arithmétique des algèbres de quaternions, Lecture Notes in Math. **800**, Springer, Berlin 1980.
[50] *J. Voight*, Quaternion algebras, Grad. Texts in Math. **288**, Springer, Cham 2021.
[51] *J.-L. Waldspurger*, Sur les valeurs de certaines fonctions L automorphes en leur centre de symétrie, Compos. Math. **54** (1985), no. 2, 173–242.
[52] *W. C. Waterhouse*, Abelian varieties over finite fields, Ann. Sci. Éc. Norm. Supér. (4) **2** (1969), 521–560.
[53] *A. Wieser*, Linnik's problems and maximal entropy methods, Monatsh. Math. **190** (2019), no. 1, 153–208.
[54] *T. Yang*, Minimal CM liftings of supersingular elliptic curves, Pure Appl. Math. Q. **4** (2008), no. 4, 1317–1326.

Menny Aka, Departement Mathematik, ETH Zürich, Rämistr. 101, CH-8092 Zurich, Switzerland
e-mail: mennyaka@math.ethz.ch

Manuel Luethi, Institute of Mathematics, Ecole Polytechnique Fédérale de Lausanne, EPFL, Station 8, CH-1015 Lausanne, Switzerland
e-mail: manuel.luthi@epfl.ch

Philippe Michel, Institute of Mathematics, Ecole Polytechnique Fédérale de Lausanne, EPFL, Station 8, CH-1015 Lausanne, Switzerland
https://orcid.org/0000-0003-2419-3073
e-mail: philippe.michel@epfl.ch

Andreas Wieser, Einstein Institute of Mathematics, Hebrew University, Edward J. Safra Campus, Jerusalem, Israel
e-mail: andreas.wieser@mail.huji.ac.il

Eingegangen 11. Mai 2020, in revidierter Fassung 23. November 2021