

RESEARCH ARTICLE

Exceptional jumps of Picard ranks of reductions of K3 surfaces over number fields

Ananth N. Shankar¹, Arul Shankar², Yunqing Tang³ and Salim Tayou⁴

¹Department of Mathematics, MIT, 182 Memorial Drive, Cambridge MA 02139, USA; E-mail: ananths@mit.edu.

²Department of Mathematics, University of Toronto, 215 Huron Street, Toronto ON M5T 1R2, Canada;

E-mail: ashankar@math.utoronto.ca.

³Department of Mathematics, University of California, Berkeley, Evans Hall, Berkeley CA 94720, USA;

E-mail: yunqing.tang@berkeley.edu.

⁴École Normale Supérieure, 45, Rue d’Ulm, 75230, Paris, France; E-mail: salim.tayou@ens.psl.eu.

Received: 23 June 2022; Accepted: 12 August 2022

2020 Mathematics Subject Classification: Primary – 11G18; Secondary – 14J28, 11G10

Abstract

Given a K3 surface X over a number field K with potentially good reduction everywhere, we prove that the set of primes of K where the geometric Picard rank jumps is infinite. As a corollary, we prove that either $X_{\bar{K}}$ has infinitely many rational curves or X has infinitely many unirational specialisations.

Our result on Picard ranks is a special case of more general results on exceptional classes for K3 type motives associated to GSpin Shimura varieties. These general results have several other applications. For instance, we prove that an abelian surface over a number field K with potentially good reduction everywhere is isogenous to a product of elliptic curves modulo infinitely many primes of K .

Contents

1	Introduction	2
1.1	Picard rank jumps for K3 surfaces	2
1.2	Rational curves on K3 surfaces	3
1.3	Exceptional splitting of abelian varieties	3
1.4	GSpin Shimura varieties	4
1.5	Strategy of the proof	5
1.6	Organisation of the paper	6
1.7	Notations	7
2	The GSpin Shimura varieties and their special divisors	7
2.1	The GSpin Shimura variety	7
2.2	The Kuga–Satake construction and K3 type motives in characteristic 0	8
2.3	Special divisors on M over \mathbb{Q}	9
2.4	Integral models	10
2.5	Special endomorphisms and integral models of special divisors	10
2.6	Reformulation of Theorem 1.8	11
3	The global height	11
3.1	Arithmetic special divisors and heights	12

3.2	Howard–Madapusi-Pera–Borcherds’ modularity theorem	13
3.3	Asymptotic estimates for the global height	13
4	General results on quadratic forms	15
4.1	Local estimates of representations by quadratic forms	15
4.2	On the number of representations of quadratic forms	19
4.3	An application of Heath-Brown’s theorem and a result of Niedermowwe	21
4.3.1	Assume $T \leq 1$	22
4.3.2	Assume $T \geq 1$	22
5	First step in the archimedean estimate and uniform diophantine bounds	24
5.1	Bruinier’s explicit formula for the Green function Φ_m	24
5.2	Estimating $b'm(k/2)$	25
5.3	Estimates on $\phi_m(x)$	27
5.3.1	Bounding $R_x(0, m)$	28
5.3.2	Estimating $\tilde{\phi}_m(x, 0)$	30
5.4	Conclusions	31
6	Second step in bounding the archimedean contribution	32
6.1	Bounding the main term using the circle method	32
6.2	Bounding the error term using the diophantine bound	33
7	Bounding the contribution from a finite place with good reduction	36
7.1	The lattices of special endomorphisms	37
7.2	Proof of Theorem 7.1	39
7.3	A transcendental example	42
8	Proof of the main theorem	43
9	Applications: Picard rank jumps and exceptional isogenies	44
9.1	Picard rank jumps in families of K3 surfaces and rational curves	44
9.2	Kuga–Satake abelian varieties	45
9.3	Abelian varieties parametrised by unitary Shimura varieties	45

1. Introduction

1.1. Picard rank jumps for K3 surfaces

Let X be a K3 surface over a number field K . Let $\mathcal{X} \xrightarrow{\pi} S$ be a smooth and projective model of X over an open subscheme S of $\text{Spec}(\mathcal{O}_K)$, the spectrum of the ring of integers \mathcal{O}_K of K . For every place \mathfrak{P} of K in S , let $\mathcal{X}_{\mathfrak{P}}$ be the geometric fibre of π at \mathfrak{P} . There is an injective specialisation map between Picard groups (see [Huy16, Chap.17 Prop.2.10]):

$$\text{sp}_{\mathfrak{P}} : \text{Pic}(X_{\overline{K}}) \hookrightarrow \text{Pic}(\mathcal{X}_{\mathfrak{P}}),$$

which implies the inequality between Picard ranks

$$\rho(\mathcal{X}_{\mathfrak{P}}) := \text{rank}_{\mathbb{Z}} \text{Pic}(\mathcal{X}_{\mathfrak{P}}) \geq \rho(X_{\overline{K}}) := \text{rank}_{\mathbb{Z}} \text{Pic}(X_{\overline{K}}).$$

In this paper, our main result implies the following theorem.

Theorem 1.1. *Let X be a K3 surface over a number field K , and assume that X admits, up to a finite extension of K , a projective smooth model $\mathcal{X} \rightarrow \text{Spec}(\mathcal{O}_K)$. Then there are infinitely many finite places \mathfrak{P} of K such that $\rho(\mathcal{X}_{\mathfrak{P}}) > \rho(X_{\overline{K}})$.*

This question has been raised by Charles [Cha14], inspired by the work of Bogomolov–Hassett–Tschinkel [BHT11] and Li–Liedtke [LL12] (see also [CT14], [CEJ16]). By [Cha14, Theorem 1], up to a finite extension of K , the Picard rank $\rho(\mathcal{X}_{\mathfrak{P}})$ for a density one set of primes \mathfrak{P} is completely determined

by $\rho(X_{\overline{K}})$ and the endomorphism field E of the sub-Hodge structure $T(X_{\sigma})$ of $H^2(X_{\sigma}^{an}(\mathbb{C}), \mathbb{Q})$ given by the orthogonal complement of $\text{Pic}(X_{\overline{K}})$ with respect to the intersection form, for any embedding σ of K in \mathbb{C} . For instance, if E is CM or $\dim_E T(X_{\sigma})$ is even, then $\rho(\mathcal{X}_{\mathfrak{P}}) = \rho(X_{\overline{K}})$ for a density one set of primes \mathfrak{P} . In this situation, our theorem proves that the density zero set, where $\rho(\mathcal{X}_{\mathfrak{P}}) > \rho(X_{\overline{K}})$ is in fact infinite.

1.2. Rational curves on K3 surfaces

As an application of the above theorem, let us first recall the following conjecture.

Conjecture 1.2. *Let X be a K3 surface over an algebraically closed field k . Then X contains infinitely many rational curves.*

The first result towards this conjecture is the one attributed to Bogomolov and Mumford and appearing in [MM83, Appendix], which states that every K3 surface over \mathbb{C} contains a rational curve. This conjecture has been settled in recent years in many cases thanks to the work of many people [BHT11, LL12, Cha14, BT05, Tay20b, Che99, CL13]. In characteristic zero, this conjecture has been solved in full generality in [CGL19, Theorem A]. Our theorem implies the following alternative for K3 surfaces over number fields admitting everywhere potentially good reduction.

Corollary 1.3. *Let X be a K3 surface over a number field K , and assume that X has potentially good reduction everywhere. Then either*

1. $X_{\overline{K}}$ contains infinitely many rational curves, or
2. X has infinitely many unirational and hence supersingular specialisations.

1.3. Exceptional splitting of abelian varieties

Let A denote a geometrically simple abelian variety over a number field K . Assuming the Mumford–Tate conjecture for A , Zywina [Zyw14, Corollary 1.3] proved that the mod \mathfrak{P} reduction $A_{\mathfrak{P}}$ is geometrically simple for a density one set of primes of K (up to replacing K by a finite extension) if and only if $\text{End}(A_{\overline{K}})$ is commutative. As an application of the proof of Theorem 1.1 (more precisely, Theorem 2.4), we prove that the density zero set of primes with $A_{\mathfrak{P}}$ geometrically nonsimple is infinite for certain classes of abelian varieties A , which are closely related to Kuga–Satake abelian varieties. We note that the Mumford–Tate conjecture is known (by work of Tankeev [Tan90, Tan95] and Vasiu [Vas08]) for the classes of abelian varieties that we treat.

As a first example, we observe that the moduli space of principally polarised abelian surfaces can be realised as a GSpin Shimura variety of dimension 3 and, in this case, the associated Kuga–Satake abelian varieties are isogenous to powers of abelian surfaces. We therefore obtain:

Theorem 1.4. *Every 2-dimensional abelian scheme over \mathcal{O}_K admits infinitely many places of geometrically nonsimple reduction.*

More generally, consider the setting of (V, Q) , a $(b + 2)$ -dimensional quadratic space over \mathbb{Q} with signature $(b, 2)$.

Assumption 1.5. Suppose that $b \geq 3$, $b \equiv 3 \pmod{4}$ and the even Clifford algebra $C^+(V, Q)$ is isomorphic to the matrix algebra $M_{2^n}(\mathbb{Q})$ with $n = \frac{b+1}{2}$.

Such a quadratic space (and its Clifford algebra) corresponds to a family of abelian varieties called Kuga–Satake abelian varieties (see Section 2.2). Every such abelian variety A has a splitting of the form $A = A^+ \times A^-$ induced by the grading of the Clifford algebra. By the Kuga–Satake construction, it follows that A^+ is isogenous to B^{2^n} for some lower-dimensional abelian variety B . Our next result concerns places of split reduction of B when A is defined over some number field K . Generically, $\text{End}(B_{\overline{K}}) = \mathbb{Z}$ (see Section 9.2), and hence the set of places of geometrically split reductions has density zero by [Zyw14],

as the Mumford–Tate conjecture is known for A and therefore for B . We then prove the following result:

Theorem 1.6. *Consider the above setting, with the assumption that B extends to an abelian scheme $\mathcal{B} \rightarrow \text{Spec}(\mathcal{O}_K)$ (and, therefore, A also extends to an abelian scheme $\mathcal{A} \rightarrow \text{Spec}(\mathcal{O}_K)$). Then there are infinitely many finite places \mathfrak{P} of K such that $\mathcal{B}_{\mathfrak{P}}$ is geometrically nonsimple.*

We also have similar results for abelian varieties parametrised by Shimura varieties associated to the unitary similitude group $\text{GU}(r, 1)$, $r \geq 1$; see Section 9.3 for the precise definitions.

Corollary 1.7. *Let E be an imaginary quadratic field, and let \mathcal{A} be a principally polarised abelian scheme over \mathcal{O}_K . Suppose that there is an embedding $\mathcal{O}_E \subset \text{End}(\mathcal{A})$ compatible with the polarisation on \mathcal{A} and that the action of \mathcal{O}_E on $\text{Lie } \mathcal{A}_K$ has signature $(r, 1)$. Then there are infinitely many finite places \mathfrak{P} of K such that $\mathcal{A}_{\mathfrak{P}}$ admits a geometric isogeny factor, which is an elliptic curve CM by E .*

We should mention that the assumption of potentially good reduction in the above statements has been removed recently by one of the authors in [Tay22] so that all the above results hold unconditionally.

1.4. *GSpin Shimura varieties*

The above theorems can be reformulated within the more general framework of intersections of a (nonspecial) arithmetic 1-cycle and special divisors in GSpin Shimura varieties as follows. Let (L, Q) be an integral quadratic even lattice of signature $(b, 2)$ with $b \geq 3$.¹ Assume that L is a maximal lattice in $V := L \otimes_{\mathbb{Z}} \mathbb{Q}$ over which Q is \mathbb{Z} -valued. Associated to this data is a *GSpin Shimura variety* M , which is a Deligne–Mumford stack over \mathbb{Q} ; see Section 2.1. It is a Shimura variety of Hodge type, which (by the work of Andreatta–Goren–Howard–Madapusi-Pera [AGHMP18]) admits a normal flat integral model \mathcal{M} over \mathbb{Z} . This model is smooth at primes p that do not divide $\text{Disc}(Q)$. Moreover, there is a family of the so-called *Kuga–Satake abelian scheme* $\mathcal{A}^{\text{univ}} \rightarrow \mathcal{M}$; see Section 2.2, 2.4. For every $m \in \mathbb{Z}_{>0}$, a *special divisor* $\mathcal{Z}(m) \rightarrow \mathcal{M}$ is constructed in [AGHMP18]² parametrising Kuga–Satake abelian varieties that admit *special* endomorphisms s such that $s \circ s = [m]$ (see Section 2.5). In particular, the moduli space of polarised K3 surfaces can be embedded in a GSpin Shimura variety (see Section 9.1), and special divisors parametrise K3 surfaces with Picard rank greater than that of the generic K3 surface. Our main theorem is the following.

Theorem 1.8. *Let K be a number field, and let $\mathcal{Y} \in \mathcal{M}(\mathcal{O}_K)$. Assume that $\mathcal{Y}_K \in M(K)$ is Hodge-generic. Then there exist infinitely many finite places \mathfrak{P} of K modulo, for which \mathcal{Y} lies in the image of $\mathcal{Z}(m) \rightarrow \mathcal{M}$ for some $m \in \mathbb{Z}_{>0}$ (here m depends on \mathfrak{P}).*

Here we say that $x \in M(K)$ is *Hodge-generic* if for one embedding (equivalently any) $\sigma : K \hookrightarrow \mathbb{C}$, the point $x^\sigma \in M(\mathbb{C})$ does not lie on any divisor $\mathcal{Z}(m)(\mathbb{C})$. This is a harmless assumption since all $\mathcal{Z}(m)_K$ are unions of GSpin Shimura varieties associated to rational quadratic spaces having signature $(b - 1, 2)$. Hence, we may and will always work with the smallest GSpin sub-Shimura variety of M containing \mathcal{Y}_K .³

Theorem 1.8 is a generalisation of the main results of [Cha18, ST19]. In the complex setting, the analogous results are well understood. More precisely, the Noether–Lefschetz locus of a nontrivial variation of Hodge structures of weight 2 with $h^{2,0} = 1$ over a complex quasi-projective curve is dense for the analytic topology by a well-known result of Green [Voi02, Prop. 17.20]. When this variation is of K3 type, the main result of [Tay20a] shows in fact that this locus is equidistributed with respect to a natural measure. In the global function field setting, the main result of [MST18] shows that given a nonisotrivial ordinary abelian surface over a projective curve C over $\overline{\mathbb{F}}_p$, there are infinitely many

¹In this paper, we focus on $b \geq 3$ case since the essential cases when $b = 1, 2$ have been treated in [Cha18, ST19].

²Also called Heegner divisor in the literature.

³Note that this use of the term Hodge-generic is *not standard* – we do not assume that the Mumford–Tate group associated to \mathcal{Y}_K is equal to the group of Spinor similitudes associated to (V, Q) .

$\overline{\mathbb{F}}_p$ -points in C such that the corresponding abelian surface is not simple. This result is analogous to Theorem 1.8 in the function field setting when $b = 2, 3$.

We now say a word about the potentially good reduction hypothesis (i.e., the fact that we require \mathcal{Y} to be an \mathcal{O}_K -point of \mathcal{M} , up to a finite extension of the base field, as opposed to a $\mathcal{O}_K[1/N]$ -point). The boundary components in the Satake compactification⁴ of M have dimension either 0 or 1, whereas the Shimura variety itself is b -dimensional. As the boundary has large codimension in the ambient Shimura variety, it follows that ‘most’ points have potentially good reduction, so our good-reduction hypothesis is not an especially stringent condition. A large family of points with potentially good reduction everywhere (in the case $b = 2c$) can be obtained as follows: consider a real quadratic field F/\mathbb{Q} and a $(c + 1)$ -dimensional orthogonal space (V', Q') over F with real signatures $(c + 1, 0)$ at one archimedean place and $(c - 1, 2)$ at the other. Then the associated $(c - 1)$ -dimensional Shimura variety of Hodge type is compact and embeds inside the b -dimensional Shimura variety associated to the \mathbb{Q} -rational $(b + 2)$ -dimensional quadratic space obtained by treating V' as a \mathbb{Q} -vector space equipped with the quadratic form $\text{tr}_{F/\mathbb{Q}}(Q')$.

1.5. Strategy of the proof

The proof of Theorem 1.8 follows the lines of [Cha18] and relies on Arakelov intersection theory on the integral model \mathcal{M} of the GSpin Shimura variety M . For every positive integer m , the special divisor $\mathcal{Z}(m)$ parametrises points of \mathcal{M} for which the associated Kuga–Satake abelian variety admits an extra special endomorphism s that satisfies $s \circ s = [m]$; see Section 2.3. By the work of Bruinier [Bru02], this divisor can be endowed with a Green function Φ_m , which is constructed using theta lift of nonholomorphic Eisenstein series of negative weight and thus yields an arithmetic divisor $\widehat{\mathcal{Z}}(m) = (\mathcal{Z}(m), \Phi_m)$ in the first arithmetic Chow group $\widehat{\text{CH}}^1(\mathcal{M})$ of \mathcal{M} . By assumption, we have an abelian scheme $\mathcal{A}_{\mathcal{Y}} \rightarrow \mathcal{Y} = \text{Spec}(\mathcal{O}_K)$ and a map $\iota : \mathcal{Y} \rightarrow \mathcal{M}$. We can express the height $h_{\widehat{\mathcal{Z}}(m)}(\mathcal{Y})$ of \mathcal{Y} with respect to the arithmetic divisor $\widehat{\mathcal{Z}}(m)$ as follows (see Section 3.1):

$$h_{\widehat{\mathcal{Z}}(m)}(\mathcal{Y}) = \sum_{\sigma:K \hookrightarrow \mathbb{C}} \Phi_m(\mathcal{Y}^\sigma) + \sum_{\mathfrak{P} \text{ finite place}} (\mathcal{Y}.\mathcal{Z}(m))_{\mathfrak{P}} \log |\mathcal{O}_K/\mathfrak{P}|. \tag{1.1}$$

By definition, $(\mathcal{Y}.\mathcal{Z}(m))_{\mathfrak{P}} \neq 0$ if and only if the Kuga–Satake abelian variety at $\mathcal{Y}_{\mathfrak{P}}$ admits a special endomorphism s with $s \circ s = [m]$. Therefore, to prove Theorem 1.8, it suffices to show that for a fixed finite place \mathfrak{P} , for most positive integers m , we have

$$(\mathcal{Y}.\mathcal{Z}(m))_{\mathfrak{P}} = o \left(h_{\widehat{\mathcal{Z}}(m)}(\mathcal{Y}) - \sum_{\sigma:K \rightarrow \mathbb{C}} \Phi_m(\mathcal{Y}^\sigma) \right). \tag{1.2}$$

Here are the ingredients of the proof. Let m be a positive integer represented by the lattice (L, Q) :

1. Starting from an explicit expression of Φ_m given by Bruinier in [Bru02, §2.2], we pick the main term out of the archimedean part of equation (1.1), which is a scalar multiple of $m^{\frac{b}{2}} \log m$; see Proposition 5.2.
2. To treat the term $h_{\widehat{\mathcal{Z}}(m)}(\mathcal{Y})$, we use a theorem of Howard and Madapusi-Pera [HM17, Theorem 9.4.1], which asserts that the generating series of $\widehat{\mathcal{Z}}(m)$ is a component of a vector-valued modular form of weight $1 + \frac{b}{2}$ with respect to the Weil representation associated to the lattice (L, Q) . As a consequence, we get $h_{\widehat{\mathcal{Z}}(m)}(\mathcal{Y}) = O(m^{\frac{b}{2}})$. This modularity result was previously known over the complex fibre by the work of Borcherds [Bor99], and a cohomological version was given by Kudla–Millson [KM90].

⁴Which is a projective variety.

3. Based on Bruinier’s explicit formula, we reduce the estimate of the remaining part of the archimedean term into a problem of counting lattice points with weight functions admitting logarithmic singularities; see Proposition 5.4.
4. The treatment of this lattice-counting problem in Section 6 is one of the key novelties here compared to the treatment of the archimedean places in the previous works [Cha18, ST19]. We break the sum into two parts; the first part, which consists of lattice points that are not very close to the singularity of the weight function, is treated using the circle method, and the rest is controlled by the so-called *diophantine bound*. More precisely, the geometrical meaning of controlling the second part is to show that (away from a small set of m) $\mathcal{Y}(\mathbb{C})$ is not very close to $\mathcal{Z}(m)(\mathbb{C})$. Roughly speaking, we prove that if $\mathcal{Y}(\mathbb{C})$ is too close to too many special divisors with m in a certain range, then $\mathcal{Y}(\mathbb{C})$ must be close to a special divisor with much smaller m . This would violate the diophantine bound deduced from the height formula and the estimates in (1)–(3) above; see Theorem 5.8.
5. Now it remains to treat the finite contribution. This part can be translated into a lattice-counting problem on a sequence of lattices $L_n, n \in \mathbb{Z}_{\geq 1}$, where L_n is the lattice of special endomorphisms of the Kuga–Satake abelian variety over $\mathcal{Y} \bmod \mathfrak{B}^n$; see Lemma 7.2. As in [ST19], we use Grothendieck–Messing theory and Serre–Tate theory to describe the asymptotic behaviour of L_n . These results give adequate bounds for the main terms. To deal with the error terms, we use the diophantine bound (see Theorem 5.8) *for individual m to obtain better bounds on average*. This step is crucial for our proof. Indeed, we illustrate the necessity of using the height bound with an example of a transcendental point of \mathcal{M} in Section 7.3, where the finite contribution can be arbitrarily large for an infinite sequence of m . We also remark that our idea of using the global height bound has other applications. Indeed, our idea is a crucial ingredient in proving intersection-theoretic results in characteristic p , as well as in proving the ordinary Hecke-orbit conjecture for GSpin Shimura varieties (see [MST22]). It has also been used to extend the main theorem to the bad reduction situation; see [Tay22]. We note, however, that our theorem applies to K3 surfaces with *potentially* good reduction everywhere. There are very few K3 surfaces with good reduction everywhere, but the condition of potentially good reduction is far less restrictive. Indeed, the moduli spaces of polarised K3 surfaces contain several compact Shimura varieties whose points parametrise K3 surfaces with potentially good reduction everywhere, and our result applies to them.
6. We briefly describe how we use the diophantine bound for *each* m to obtain stronger bounds on the local contribution from finite places on average. The arguments in (1)–(3) actually prove that the quantity inside the little o in the right-hand side of equation (1.2) is bounded by $m^{\frac{b}{2}} \log m$, as $m \rightarrow \infty$ (although we prove that it is also $\gg m^{\frac{b}{2}} \log m$ in (4) for most m). Since each term $(\mathcal{Y} \cdot \mathcal{Z}(m))_{\mathfrak{B}}$ is nonnegative, we have that for any \mathfrak{B} , the local contribution $(\mathcal{Y} \cdot \mathcal{Z}(m))_{\mathfrak{B}} = O(m^{\frac{b}{2}} \log m)$ – this is the diophantine bound that we refer to. By Lemma 7.2, this diophantine bound implies that for $n \gg m^{\frac{b}{2} + \epsilon}, \epsilon > 0$, any nonzero special endomorphism s in the lattice L_n must satisfy $s \circ s = [m']$ with $m' \geq m$. Then a geometry-of-numbers argument suffices to conclude the proof of our theorem.

1.6. Organisation of the paper

In Section 2, we recall the construction of the GSpin Shimura variety associated to the lattice (L, Q) following [AGHMP17, AGHMP18, HM17], as well as the construction of its integral model and the construction of the special divisors using the notion of special endomorphisms; then we give a reformulation of Theorem 1.8. In Section 3, we recall how to associate Green functions to the special divisors on \mathcal{M} , and we state Borcherds–Howard–Madapusi-Pera’s modularity result from [HM17]; then we derive consequences on the growth of the global height of an \mathcal{O}_K -point on \mathcal{M} . In Section 4, we collect some general results on quadratic forms that will be used in the following sections. In Section 5, we give a first-step estimate on the growth of the archimedean terms, and we derive the diophantine bounds on archimedean and nonarchimedean contributions. The second step in estimating the archimedean contributions is performed in Section 6, while the nonarchimedean contributions are treated in Section 7.

In Section 8, we put together all the ingredients to prove Theorem 2.4 and hence Theorem 1.8. Finally, in Section 9, we prove the applications to K3 surfaces. Subsequently, we prove the applications to Kuga–Satake abelian varieties and abelian varieties parametrised by unitary Shimura varieties.

1.7. Notations

If $f, g : \mathbb{N} \rightarrow \mathbb{R}$ are real functions and g does not vanish, then

1. $f = O(g)$, or $f \ll g$, if there exists an integer $n_0 \in \mathbb{N}$, a positive constant $C_0 > 0$ such that

$$\forall n \geq n_0, |f(n)| \leq C_0|g(n)|.$$

2. $f \asymp h$ if $f = O(h)$ and $h = O(f)$.
3. $f = o(g)$ if for every $\epsilon > 0$, there exists n_ϵ such that for every $n \geq n_\epsilon$

$$|f(n)| \leq \epsilon|g(n)|.$$

4. For p a prime number, val_p denotes the p -adic valuation on \mathbb{Q} .
5. For $s \in \mathbb{C}$, $\text{Re}(s)$ is the real part of s .

2. The GSpin Shimura varieties and their special divisors

Let (L, Q) be an integral quadratic even lattice of signature $(b, 2)$, $b \geq 1$, with associated bilinear form defined by

$$(x, y) = Q(x + y) - Q(x) - Q(y),$$

for $x, y \in L$. Let $V := L \otimes_{\mathbb{Z}} \mathbb{Q}$, and assume that L is a maximal lattice in V over which Q is \mathbb{Z} -valued. We recall in this section the theory of GSpin Shimura varieties associated with (L, Q) . Our main references are [AGHMP17, Section 2], [AGHMP18, Section 4] and [MP16, Section 3].

2.1. The GSpin Shimura variety

For a commutative ring R , let L_R denote $L \otimes_{\mathbb{Z}} R$, and the quadratic form Q on L induces a quadratic form Q on L_R . The Clifford algebra $C(L_R)$ of (L_R, Q) is the R -algebra defined as the quotient of the tensor algebra $\bigotimes L_R$ by the ideal generated by $\{(x \otimes x) - Q(x), x \in L_R\}$. It has a $\mathbb{Z}/2\mathbb{Z}$ grading $C(L_R) = C(L_R)^+ \oplus C(L_R)^-$ induced by the grading on $\bigotimes L_R$. When R is a \mathbb{Q} -algebra, we also denote $C(L_R)$ (respectively, $C^\pm(L_R)$) by $C(V_R)$ (respectively, $C^\pm(V_R)$) and note that $C(L)$ is a lattice in $C(V)$.

Let $G := \text{GSpin}(V)$ be the group of spinor similitudes of V . It is the reductive algebraic group over \mathbb{Q} such that

$$G(R) = \{g \in C^+(V_R)^\times, gV_Rg^{-1} = V_R\}$$

for any \mathbb{Q} -algebra R . We denote by $\nu : G \rightarrow \mathbb{G}_m$ the spinor similitude factor as defined in [Bas74, Section 3]. The group G acts on V via $g \bullet v = gvg^{-1}$ for $v \in V_R$ and $g \in G(R)$. Moreover, there is an exact sequence of algebraic groups

$$1 \rightarrow \mathbb{G}_m \rightarrow G \xrightarrow{g \mapsto g \bullet} \text{SO}(V) \rightarrow 1.$$

Let D_L be the period domain associated to (L, Q) defined by⁵

$$D_L = \{x \in \mathbb{P}(V_{\mathbb{C}}) \mid (\bar{x}.x) < 0, (x.x) = 0\}.$$

It is a hermitian symmetric domain, and the group $G(\mathbb{R})$ acts transitively on D_L . As in [AGHMP18, §4.1], (G, D_L) defines a Shimura datum as follows: for any class $[z] \in D_L$ with $z \in V_{\mathbb{C}}$, there is a morphism of algebraic groups over \mathbb{R}

$$h_{[z]} : \mathbb{S} = \text{Res}_{\mathbb{C}/\mathbb{R}} \mathbb{G}_m \rightarrow G_{\mathbb{R}}$$

such that the induced Hodge decomposition on $V_{\mathbb{C}}$ is given by

$$V^{1,-1} = \mathbb{C}z, V^{-1,1} = \mathbb{C}\bar{z}, V_C^{0,0} = (\mathbb{C}z \oplus \mathbb{C}\bar{z})^{\perp}.$$

Indeed, choose a representative $z = u + iw$, where $u, w \in V_{\mathbb{R}}$ are orthogonal and $Q(u) = Q(w) = -1$, then $h_{[z]}$ is the morphism such that $h_{[z]}(i) = uw \in G(\mathbb{R}) \subset C^+(V_{\mathbb{R}})^{\times}$. Hence D_L is identified with a $G(\mathbb{R})$ -conjugacy class in $\text{Hom}(\text{Res}_{\mathbb{C}/\mathbb{R}} \mathbb{G}_m, G_{\mathbb{R}})$. The reflex field of (G, D_L) is equal to \mathbb{Q} by [And96, Appendix 1].

Let $\mathbb{K} \subset G(\mathbb{A}_f)$ be the compact open subgroup

$$\mathbb{K} = G(\mathbb{A}_f) \cap C(\widehat{L})^{\times},$$

where $\widehat{L} = L \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}}$. By [MP16, Lemma 2.6], the image of \mathbb{K} in $\text{SO}(\widehat{L})$ is the subgroup of elements acting trivially on L^{\vee}/L , where L^{\vee} is the dual lattice of L defined by

$$L^{\vee} := \{x \in V \mid \forall y \in L, (x.y) \in \mathbb{Z}\}.$$

By the theory of canonical models, we get a b -dimensional Deligne–Mumford stack M over \mathbb{Q} , the *GSpin Shimura variety associated with L* , such that

$$M(\mathbb{C}) = G(\mathbb{Q}) \backslash D_L \times G(\mathbb{A}_f) / \mathbb{K}.$$

2.2. The Kuga–Satake construction and K3 type motives in characteristic 0

The Kuga–Satake construction was first considered in [KS67] and later in [Del72] and [Del79]. We follow here the exposition of [MP16, Section 3].

Let $G \rightarrow \text{Aut}(N)$ be an algebraic representation of G on a \mathbb{Q} -vector space N , and let $N_{\widehat{\mathbb{Z}}} \subset N_{\mathbb{A}_f}$ be a \mathbb{K} -stable lattice. Then one can construct a local system \mathbf{N}_B on $M(\mathbb{C})$ whose fibre at a point $[[z], g]$ is identified with $N \cap g(N_{\widehat{\mathbb{Z}}})$. The corresponding vector bundle $\mathbf{N}_{dR, M(\mathbb{C})} = \mathcal{O}_{M(\mathbb{C})} \otimes \mathbf{N}_B$ is equipped with a holomorphic filtration $\mathcal{F}^{\bullet} \mathbf{N}_{dR, M(\mathbb{C})}$, which at every point $[[z], g]$ equips the fibre with the Hodge structure determined by the cocharacter $h_{[z]}$. Hence we obtain a functor

$$(N, N_{\widehat{\mathbb{Z}}}) \mapsto (\mathbf{N}_B, \mathcal{F}^{\bullet} \mathbf{N}_{dR, M(\mathbb{C})}) \tag{2.1}$$

from the category of algebraic \mathbb{Q} -representations of G with a \mathbb{K} -stable lattice to variations of \mathbb{Z} -Hodge structures over $M(\mathbb{C})$. Applying this functor to (V, \widehat{L}) , we obtain a variation of \mathbb{Z} -Hodge structures $\{\mathbf{V}_B, \mathcal{F}^{\bullet} \mathbf{V}_{dR, M(\mathbb{C})}\}$ of weight 0 over $M(\mathbb{C})$. The quadratic form Q gives a polarisation on $(\mathbf{V}_B, \mathcal{F}^{\bullet} \mathbf{V}_{dR, M(\mathbb{C})})$ and hence by [Del79, 1.1.15], all $(\mathbf{N}_B, \mathcal{F}^{\bullet} \mathbf{N}_{dR, M(\mathbb{C})})$ are polarisable.

Also, if we denote by H the representation of the group G on $C(V)$ by left multiplication and $H_{\widehat{\mathbb{Z}}} = C(L)_{\widehat{\mathbb{Z}}}$, then applying the functor (2.1) to the pair $(H, H_{\widehat{\mathbb{Z}}})$, we obtain a polarisable variation of \mathbb{Z} -Hodge structures $(\mathbf{H}_B, \mathbf{H}_{dR, M(\mathbb{C})})$ of type $(-1, 0), (0, -1)$ with a right $C(V)$ -action. Therefore,

⁵Here we pick $z \in V_{\mathbb{C}}$ such that $[z] = x$ and $(\bar{x}.x) > 0$ means that $(\bar{z}.z) > 0$ and $(x.x) = 0$ means $(z.z) = 0$; both conditions are independent of the choice of z .

there is a family of abelian schemes $A^{\text{univ}} \rightarrow M$ of relative dimension 2^{b+1} , the *Kuga–Satake abelian scheme*, such that the homology of the family $A^{\text{univ}, \text{an}}(\mathbb{C}) \rightarrow M^{\text{an}}(\mathbb{C})$ is precisely $(\mathbf{H}_B, \mathbf{H}_{dR, M(\mathbb{C})})$. It is equipped with a right $C(L)$ -action and a compatible $\mathbb{Z}/2\mathbb{Z}$ -grading: $A^{\text{univ}} = A^{\text{univ}, +} \times A^{\text{univ}, -}$; see [MP16, 3.5–3.7, 3.10].⁶

Using A^{univ} , one descends $\mathbf{H}_{dR, M(\mathbb{C})}$ to a filtered vector bundle with an integrable connection $(\mathbf{H}_{dR}, \mathcal{F} \bullet \mathbf{H}_{dR})$ over M as the first relative de Rham homology with the Gauss–Manin connection ([MP16, 3.10]). For any prime ℓ , the ℓ -adic sheaf $\mathbb{Z}_\ell \otimes \mathbf{H}_B$ over $M(\mathbb{C})$ descends also canonically to an ℓ -adic étale sheaf $\mathbf{H}_{\ell, \text{ét}}$ over M , which is canonically isomorphic to the ℓ -adic Tate module of A^{univ} ([MP16, 3.13]). Moreover, by Deligne’s theory of absolute Hodge cycles, one descends $\mathbf{V}_{dR, M(\mathbb{C})}$ and $\mathbb{Z}_\ell \otimes \mathbf{V}_B$ to $(\mathbf{V}_{dR}, \mathcal{F} \bullet \mathbf{V}_{dR})$ and $\mathbf{V}_{\ell, \text{ét}}$ over M ([MP16, 3.4, 3.10–3.12]). More precisely, an idempotent

$$\pi = (\pi_{B, \mathbb{Q}}, \pi_{dR, \mathbb{Q}}, \pi_{\ell, \mathbb{Q}}) \in \text{End}(\text{End}(\mathbf{H}_B \otimes \mathbb{Q})) \times \text{End}(\text{End}(\mathbf{H}_{dR})) \times \text{End}(\text{End}(\mathbf{H}_{\ell, \text{ét}} \otimes \mathbb{Q}_\ell))$$

is constructed in ([MP16, 3.4, 3.10–3.12]) such that the fibre of π at each closed point in M is an absolute Hodge cycle and $(\mathbf{V}_B \otimes \mathbb{Q}, \mathbf{V}_{dR}, \mathbf{V}_{\ell, \text{ét}} \otimes \mathbb{Q}_\ell)$ is the image of π . In particular, $(\mathbf{V}_B \otimes \mathbb{Q}, \mathbf{V}_{dR}, \mathbf{V}_{\ell, \text{ét}} \otimes \mathbb{Q}_\ell)$ is a family of absolute Hodge motives over M , and we call each fibre a *K3 type motive*. (For a reference on absolute Hodge motives, we refer to [DMOS82, IV].)

On the other hand, let $\text{End}_{C(V)}(H)$ denote the endomorphism ring of H as a $C(V)$ -module with right $C(V)$ -action. Then the action of V on H as left multiplication induces a G -equivariant embedding $V \hookrightarrow \text{End}_{C(V)}(H)$, which maps $\widehat{L} \hookrightarrow H_{\widehat{\mathbb{Z}}}$. The functoriality of (2.1) induces embeddings

$$\mathbf{V}_B \hookrightarrow \text{End}_{C(L)}(\mathbf{H}_B) \quad \text{and} \quad \mathbf{V}_{dR, M(\mathbb{C})} \hookrightarrow \text{End}_{C(V)}(\mathbf{H}_{dR, M(\mathbb{C})}),$$

the latter being compatible with filtration. By [MP16, 1.2, 1.4, 3.11], these embeddings are the same as the one induced by π above with the natural forgetful map $\text{End}_{C(V)}(\mathbf{H}) \rightarrow \text{End}(\mathbf{H})$. In particular, the embedding $\mathbf{V}_{dR} \hookrightarrow \text{End}_{C(V)}(\mathbf{H}_{dR})$ is compatible with filtrations and connection and $\mathbf{V}_{\ell, \text{ét}} \hookrightarrow \text{End}_{C(V)}(\mathbf{H}_{\ell, \text{ét}})$ as \mathbb{Z}_ℓ -lisse sheaves with compatible Galois action on each fibre.⁷

Moreover, there is a canonical quadratic form $\mathbf{Q} : \mathbf{V}_{dR} \rightarrow \mathcal{O}_M$ given on sections by $v \circ v = \mathbf{Q}(v) \cdot \text{Id}$, where the composition takes places in $\text{End}_{C(V)}(\mathbf{H}_{dR})$. Similarly, there is also a canonical quadratic form on $\mathbf{V}_{\ell, \text{ét}}$ induced by composition in $\text{End}_{C(V)}(\mathbf{H}_{\ell, \text{ét}})$ and valued in the constant sheaf $\underline{\mathbb{Z}_\ell}$.

2.3. Special divisors on M over \mathbb{Q}

For any vector $\lambda \in L_{\mathbb{R}}$ such that $Q(\lambda) > 0$, let λ^\perp be the set of elements of D_L orthogonal to λ . Let $\beta \in L^\vee/L$ and $m \in \mathbb{Q}(\beta) + \mathbb{Z}$ with $m > 0$ and define the complex orbifold

$$Z(\beta, m)(\mathbb{C}) := \bigsqcup_{g \in G(\mathbb{Q}) \backslash G(\mathbb{A}_f) / \mathbb{K}} \Gamma_g \backslash \left(\bigsqcup_{\lambda \in \beta_g + L_g, Q(\lambda) = m} \lambda^\perp \right)$$

where $\Gamma_g = G(\mathbb{Q}) \cap g\mathbb{K}g^{-1}$, $L_g \subset V$ is the lattice determined by $\widehat{L}_g = g \bullet \widehat{L}$ and $\beta_g = g \bullet \beta \in L_g^\vee/L_g$. Then $Z(\beta, m)(\mathbb{C})$ is the set of complex points of a disjoint union of Shimura varieties associated with orthogonal lattices of signature $(b - 1, 2)$ and it admits a canonical model $Z(\beta, m)$ over \mathbb{Q} for $b \geq 2$.⁸ The natural map $Z(\beta, m)(\mathbb{C}) \rightarrow M(\mathbb{C})$ descends to a finite unramified morphism $Z(\beta, m) \rightarrow M$. Étally locally on $Z(\beta, m)$, this map is a closed immersion defined by a single equation, and hence its scheme theoretic image gives an effective Cartier divisor on M , which we will also denote by $Z(\beta, m)$.⁹

⁶Here we follow the convention in [AGHMP18], where H is the homology of A^{univ} . In [MP16], H is the cohomology of A^{univ} .

⁷The compatibility of \mathbb{Z}_ℓ -structure can be deduced from Artin’s comparison theorem and that we have the embedding $\mathbf{V}_B \hookrightarrow \text{End}_{C(L)}(\mathbf{H}_B)$ as \mathbb{Z} -local system over $M(\mathbb{C})$.

⁸When $b = 1$, $Z(\beta, m)$ is 0-dimensional and it is still naturally a Deligne–Mumford stack over \mathbb{Q} .

⁹We need to take the scheme theoretic image since the map $Z(\beta, m) \rightarrow M$ is not a closed immersion. See for instance [Bru02, Ch. 5, p.119] and [KRY04, Remark 9.3].

2.4. Integral models

We recall the construction of an integral model of M from [AGHMP18, 4.4]; see also [HM17, 6.3] and the original work of Kisin [Kis10] and Madapusi Pera [MP16]. Let p be a prime number. We say that L is *almost self-dual* at p if either L is self-dual at p or $p = 2$, $\dim_{\mathbb{Q}}(V)$ is odd and $|L^{\vee}/L|$ is not divisible by 4. The following proposition is parts of [AGHMP18, Proposition 4.4.1, Theorem 4.4.6] and [HM17, Remark 6.3.1].

Proposition 2.1. *There exists a flat, normal Deligne–Mumford \mathbb{Z} -stack \mathcal{M} with the following properties.*

1. $\mathcal{M}_{\mathbb{Z}_{(p)}}$ is smooth over $\mathbb{Z}_{(p)}$ if L is almost self-dual at p ;
2. the Kuga–Satake abelian scheme $A^{\text{univ}} \rightarrow M$ extends to an abelian scheme $\mathcal{A}^{\text{univ}} \rightarrow \mathcal{M}$ and the $C(L)$ -action on A^{univ} also extends to a $C(L)$ -action on $\mathcal{A}^{\text{univ}}$;
3. the line bundle $\mathcal{F}^1 V_{dR}$ extends canonically to a line bundle ω over \mathcal{M} .
4. the extension property: for E/\mathbb{Q}_p finite, $t \in M(E)$ such that A_t^{univ} has potentially good reduction over \mathcal{O}_E , then t extends to a map $\text{Spec}(\mathcal{O}_E) \rightarrow \mathcal{M}$.

For p such that L is self-dual at p , we now discuss the extensions of $\mathbf{V}_{dR}, \mathbf{V}_{\ell, \acute{e}t}, \ell \neq p$ over $\mathcal{M}_{\mathbb{Z}_{(p)}}$ and recall the construction of \mathbf{V}_{cris} . For ease of reading, we will denote the extensions by the same notation. We will use these notions to provide an *ad hoc* definition of the reduction of the K3 type motives defined in Section 2.2.

By (2) in Proposition 2.1, there are natural extensions of $\mathbf{H}_{dR}, \mathbf{H}_{\ell, \acute{e}t}$ as the first relative de Rham homology and the \mathbb{Z}_{ℓ} -Tate module of $\mathcal{A}^{\text{univ}}$, and we define \mathbf{H}_{cris} to be the first relative crystalline homology

$$\text{Hom} \left(R^1 \pi_{\text{cris}, * } \mathcal{O}_{\mathcal{A}_{\mathbb{F}_p}/\mathbb{Z}_p}^{\text{cris}}, \mathcal{O}_{\mathcal{M}_{\mathbb{F}_p}/\mathbb{Z}_p}^{\text{cris}} \right).$$

By [AGHMP18, Remark 4.2.3], there exists a canonical extension of $\mathbf{V}_{\ell, \acute{e}t} \hookrightarrow \text{End}_{C(L)}(\mathbf{H}_{\ell, \acute{e}t})$ over $\mathcal{M}_{\mathbb{Z}_{(p)}}$. Note that $L_{\mathbb{Z}_{(p)}}$ is a $\mathbb{Z}_{(p)}$ -representation of $\text{GSpin}(L_{\mathbb{Z}_{(p)}}, \mathcal{Q})$, then by [AGHMP18, Propositions 4.2.4, 4.2.5], there is a vector bundle with integrable connection \mathbf{V}_{dR} over $\mathcal{M}_{\mathbb{Z}_{(p)}}$ and a canonical embedding into $\text{End}_{C(L)}(\mathbf{H}_{dR})$ extending their counterparts over M ; moreover, there is an F -crystal \mathbf{V}_{cris} with a canonical embedding into $\text{End}_{C(L)}(\mathbf{H}_{\text{cris}})$. Both embeddings realise \mathbf{V}_{dR} and \mathbf{V}_{cris} as local direct summands of $\text{End}_{C(L)}(\mathbf{H}_{dR})$ and $\text{End}_{C(L)}(\mathbf{H}_{\text{cris}})$ and these two embeddings are compatible with the canonical crystalline-de Rham comparison.

For a point $x \in \mathcal{M}(\mathbb{F}_q)$, where q is a power of p , we consider the fibre of $(\mathbf{V}_{\ell, \acute{e}t}, \mathbf{V}_{dR}, \mathbf{V}_{\text{cris}})$ at x of the *ad hoc* motive attached to x , where q -Frobenius Frob_x acts on $\mathbf{V}_{\ell, \acute{e}t, x}$ and semi-linear crystalline Frobenius φ_x acts on $\mathbf{V}_{\text{cris}, x}$. Although these realisations are not as closely related as the analogous characteristic 0 situation, there is a good notion of algebraic cycles in $(\mathbf{V}_{\ell, \acute{e}t}, \mathbf{V}_{dR}, \mathbf{V}_{\text{cris}})$, namely the special endomorphisms of the Kuga–Satake abelian varieties discussed in the following subsection.

2.5. Special endomorphisms and integral models of special divisors

We recall the definition of special endomorphisms from [AGHMP18, §§4.3,4.5]. For an \mathcal{M} -scheme S , we use A_S to denote $\mathcal{A}_S^{\text{univ}}$, the pull-back of the universal Kuga–Satake abelian scheme to S .

Definition 2.2. An endomorphism $v \in \text{End}_{C(L)}(A_S)$ is *special* if

1. for prime p such that L is self-dual at p , all homological realisations of v lie in the image of $\mathbf{V}_{?} \hookrightarrow \text{End}_{C(L)}(\mathbf{H}_{?})$ given in Sections 2.2,2.4;¹⁰ and
2. for p such that L is not self-dual, after choosing an auxiliary maximal lattice L° of signature $(b^{\circ}, 2)$, which is self-dual at p and admits an isometric embedding $L \hookrightarrow L^{\circ}$, the image of v under the

¹⁰More precisely, if p is invertible in S , we take $? = B, dR, (\ell, \acute{e}t)$ and by the theory of absolute Hodge cycles, it is enough to just consider $? = B$; otherwise, we take $? = B, dR, \text{cris}, (\ell, \acute{e}t), \ell \neq p$ (and we drop $? = B$ if $\mathbb{Q} = \emptyset$).

canonical embedding $\text{End}_{C(L)}(A_S) \hookrightarrow \text{End}_{C(L^\circ)}(A_S^\circ)$ has all its homological realisations lying in the image of $\mathbf{V}_?^\circ \hookrightarrow \text{End}_{C(L^\circ)}(\mathbf{H}_?^\circ)$.¹¹

We use $V(A_S)$ to denote the \mathbb{Z} -module of special endomorphisms of A_S .

By [AGHMP18, Prop.4.5.4], there is a positive definite quadratic form $Q : V(A_S) \rightarrow \mathbb{Z}$ such that for each $v \in V(A_S)$, we have $v \circ v = Q(v) \cdot \text{Id}_{A_S}$.¹²

Definition 2.3. When S is a $\mathcal{M}_{\mathbb{Z}(p)}$ -scheme, v is a *special endomorphism* of the p -divisible group $A_S[p^\infty]$ if $v \in \text{End}_{C(L)}(A_S[p^\infty])$ and the crystalline realisation of x (respectively, image of x under the canonical embedding $\text{End}_{C(L)}(A_S[p^\infty]) \hookrightarrow \text{End}_{C(L^\circ)}(A_S^\circ[p^\infty])$) lies in \mathbf{V}_{cris} (respectively, $\mathbf{V}_{\text{cris}}^\circ$) if L is self-dual at p (respectively, otherwise).¹³

For an odd prime p such that L is self-dual at p , for a point $x \in \mathcal{M}(\mathbb{F}_{p^r})$ by [MP15, Theorem 6.4],¹⁴ we have isometries

$$V(\mathcal{A}_x^{\text{univ}}) \otimes \mathbb{Q}_\ell \cong \lim_{n \rightarrow \infty} \mathbf{V}_{\ell, \text{ét}, x}^{\text{Frob}_x^n = 1}, \ell \neq p, \quad V(\mathcal{A}_x^{\text{univ}}) \otimes \mathbb{Q}_p \cong \lim_{n \rightarrow \infty} (\mathbb{Q}_{p^{rn}} \otimes \mathbf{V}_{\text{cris}, x})^{\varphi_x = 1}.$$

Therefore, we view special endomorphisms of $\mathcal{A}_x^{\text{univ}}$ as the algebraic cycles of the *ad hoc* motive $(\mathbf{V}_{\ell, \text{ét}, x}, \mathbf{V}_{dR, x}, \mathbf{V}_{\text{cris}, x})$.

For $m \in \mathbb{Z}_{>0}$, the *special divisor* $\mathcal{Z}(m)$ is defined as the Deligne–Mumford stack over \mathcal{M} with functor of points $\mathcal{Z}(m)(S) = \{v \in V(A_S) \mid Q(v) = m\}$ for any \mathcal{M} -scheme S . More generally, in [AGHMP18, §4.5], for $\beta \in L^\vee/L, m \in Q(\beta) + \mathbb{Z}, m > 0$, there is also a special cycle $\mathcal{Z}(\beta, m)$ defined as a Deligne–Mumford stack over \mathcal{M} parametrising points with certain special quasi-endomorphisms and $\mathcal{Z}(m) = \mathcal{Z}(0, m)$. By [AGHMP18, Proposition 4.5.8], the generic fibre $\mathcal{Z}(\beta, m)_\mathbb{Q}$ is equal to the divisor $Z(\beta, m)$ defined in Section 2.3. Moreover, étale locally on the source, $\mathcal{Z}(\beta, m)$ is an effective Cartier divisor on \mathcal{M} , and we will use the same notation for the Cartier divisor on \mathcal{M} defined by étale descent.

2.6. Reformulation of Theorem 1.8

Using the notion of special endomorphisms, Theorem 1.8 is a direct consequence of the following theorem.

Theorem 2.4. Assume that $b \geq 3$. Let K be a number field, let $D \in \mathbb{Z}_{>0}$ be a fixed integer represented by (L, Q) . Let $\mathcal{Y} \in \mathcal{M}(\mathcal{O}_K)$, and assume that $\mathcal{Y}_K \in M(K)$ is Hodge-generic. Then there are infinitely many places \mathfrak{P} of K such that $\mathcal{Y}_{\mathfrak{P}}$ lies in the image of $\mathcal{Z}(Dm^2) \rightarrow \mathcal{M}$ for some $m \in \mathbb{Z}_{>0}$.¹⁵ Equivalently, for a Kuga–Satake abelian variety \mathcal{A} over \mathcal{O}_K parametrised by \mathcal{M} such that $\mathcal{A}_{\overline{K}}$ does not have any special endomorphisms, there are infinitely many \mathfrak{P} such that $\mathcal{A}_{\mathfrak{P}}$ admits a special endomorphism v such that $v \circ v = [Dm^2]$ for some $m \in \mathbb{Z}_{>0}$.

3. The global height

In this section, we begin the proof of Theorem 2.4 (and, in particular, Theorem 1.8) by studying the height of a given \mathcal{O}_K -point with respect to a sequence of arithmetic special divisors. In Section 3.1, we

¹¹Here $(-)^\circ$ denotes the object defined using L° in previous sections. The existence of the canonical embedding $\text{End}_{C(L)}(A_S) \hookrightarrow \text{End}_{C(L^\circ)}(A_S^\circ)$ follows from [AGHMP18, Proposition 4.4.7 (2)]. By [AGHMP18, Proposition 4.5.1], this definition is independent of the choice of L° .

¹²Here we use the same letter Q for this quadratic form since if every point in S is the reduction of some characteristic 0 point in S , then this quadratic form is the restriction of $(\mathbf{V}_B, \mathbf{Q})$ via the canonical embedding $V(A_S) \hookrightarrow \mathbf{V}_{B, S}$ (recall that \mathbf{Q} is induced by (L, Q) in Section 2.2).

¹³In [AGHMP18, §4.5], the definition of a special endomorphism of a p -divisible group also contains a condition on its p -adic étale realisation over $S[p^{-1}]$. The proof of [MP16, Lemma 5.13] shows that this extra condition is implied by the crystalline condition.

¹⁴Assumption 6.2 in [MP15] follows immediately from [Kis17, Corollary (2.3.1)]

¹⁵Here m may vary as \mathfrak{P} varies.

follow [Bru02], [Bor98] and endow the special divisors $\mathcal{Z}(m)$, $m \in \mathbb{Z}_{>0}$ (defined in Section 2.3, 2.5) with Green functions Φ_m , thereby bestowing on them the structure of arithmetic divisors. In Section 3.2, we recall the modularity theorem of the generating series of arithmetic special divisors $(\mathcal{Z}(m), \Phi_m)$ proved by Howard–Madapusi-Pera [HM17], and in Section 3.3, we use this to deduce asymptotic estimates for the global height $h_{\widehat{\mathcal{Z}}(m)}(\mathcal{Y})$.

For simplicity, we assume that $b \geq 3$ as in [Bru02], and we refer the interested reader to [BK03, BF04, BY09] for related results without this assumption. Note that our quadratic form Q differs from the one in [Bru02, BK03] by a factor of -1 , and hence we shall replace the Weil representation there by its dual. The rest remains the same; namely, we work with the same space of modular forms and harmonic Maass forms and the same Eisenstein series.

3.1. Arithmetic special divisors and heights

Let $\rho_L : \mathrm{Mp}_2(\mathbb{Z}) \rightarrow \mathrm{Aut}_{\mathbb{C}}(\mathbb{C}[L^{\vee}/L])$ denote the unitary Weil representation, where $\mathrm{Mp}_2(\mathbb{Z})$ is the metaplectic double cover of $\mathrm{SL}_2(\mathbb{Z})$; see, for instance, [Bru02, Section 1.1]. Let $k = 1 + \frac{b}{2}$, and let $H_{2-k}(\rho_L^{\vee})$ be the \mathbb{C} -vector space of vector valued harmonic weak Maass forms of weight $2 - k$ with respect to the dual ρ_L^{\vee} of the Weil representation as defined in [BY09, 3.1].

For $\beta \in L^{\vee}/L$, $m \in \mathbb{Z} + Q(\beta)$ with $m > 0$, let $F_{\beta,m} \in H_{2-k}(\rho_L^{\vee})$ denote the Hejhal–Poincaré harmonic Maass form defined in [Bru02, Def. 1.8]. In fact, $F_{\beta,m}(\tau) := F_{\beta,-m}(\tau, \frac{1}{2} + \frac{b}{4})$ in [Bru02, Def. 1.8], where τ lies in the Poincaré upper half plane \mathbb{H} . Let $\Phi_{\beta,m}$ denote the regularised theta lifting of $F_{\beta,m}$ in the sense of Borcherds; see [Bru02, (2.16)] and [BF04, §5.2]. By [Bor98, §6, Thm. 13.3] and [Bru02, §2.2, eqn. (3.40), Thm. 3.16], $\Phi_{\beta,m}$ is a Green function¹⁶ for the divisor $\mathcal{Z}(\beta, m)$, and we use $\widehat{\mathcal{Z}}(\beta, m)$ to denote the arithmetic divisor $(\mathcal{Z}(\beta, m), \Phi_{\beta,m})$. Our main focus is the case when $\beta = 0$, and we set $\Phi_m := \Phi_{0,m}$, $\widehat{\mathcal{Z}}(m) := \widehat{\mathcal{Z}}(0, m)$ for $m \in \mathbb{Z}_{>0}$.

Let $\widehat{\mathrm{CH}}^1(\mathcal{M})_{\mathbb{Q}}$ denote the first arithmetic Chow group of Gillet–Soulé [GS90] as defined in [AGHMP17, §4.1]. Since \mathcal{M} is a normal Deligne–Mumford stack, we have a natural isomorphism, as in [Sou92, III.4],

$$\widehat{\mathrm{Pic}}(\mathcal{M})_{\mathbb{Q}} \otimes \mathbb{Q} \xrightarrow{\sim} \widehat{\mathrm{CH}}^1(\mathcal{M})_{\mathbb{Q}},$$

where $\widehat{\mathrm{Pic}}(\mathcal{M})$ denotes the group of isomorphism classes of metrised line bundles and $\widehat{\mathrm{Pic}}(\mathcal{M})_{\mathbb{Q}} := \widehat{\mathrm{Pic}}(\mathcal{M}) \otimes \mathbb{Q}$; see [AGHMP17, §5.1] for more details. Since $\mathcal{Z}(\beta, m)$ is (étale locally) Cartier, then we view $\widehat{\mathcal{Z}}(\beta, m) \in \widehat{\mathrm{Pic}}(\mathcal{M})_{\mathbb{Q}}$.

Moreover, the line bundle ω from Proposition 2.1 is endowed with the Petersson metric defined as follows: the fibre of ω at a complex point $[[z], g] \in M(\mathbb{C})$ is identified with the isotropic line $\mathbb{C}z \subset V_{\mathbb{C}}$; then we set $\|z\|^2 = -\frac{(z, \bar{z})}{4\pi e^{\gamma}}$, where $\gamma = -\Gamma'(1)$ is the Euler–Mascheroni constant. Hence we get a metrised line bundle $\bar{\omega} \in \widehat{\mathrm{Pic}}(\mathcal{M})$.

Recall that we have a map $\mathcal{Y} \rightarrow \mathcal{M}$, where $\mathcal{Y} = \mathrm{Spec} \mathcal{O}_K$. We now define the notion of the height of \mathcal{M} with respect to the arithmetic divisors $\widehat{\mathcal{Z}}(m)$ and $\bar{\omega}$. As in [AGHMP17, §§5.1, 5.2], [AGHMP18, §6.4], the height $h_{\widehat{\mathcal{Z}}(m)}(\mathcal{Y})$ of \mathcal{Y} with respect to $\widehat{\mathcal{Z}}(m)$ (respectively, $\bar{\omega}$) is defined as the image of $\widehat{\mathcal{Z}}(m)$ (respectively, $\bar{\omega}$) under the composition

$$\widehat{\mathrm{CH}}^1(\mathcal{M})_{\mathbb{Q}} \cong \widehat{\mathrm{Pic}}(\mathcal{M})_{\mathbb{Q}} \rightarrow \widehat{\mathrm{Pic}}(\mathcal{Y})_{\mathbb{Q}} \xrightarrow{\mathrm{deg}} \mathbb{R},$$

where the middle map is the pull-back of metrised line bundles and the arithmetic degree map $\widehat{\mathrm{deg}}$ is the extension over \mathbb{Q} of the one defined in [AGHMP18, 6.4].

¹⁶A priori, the Green function is defined over D_L , but it descends to $M(\mathbb{C})$; we use the same notation for both functions on D_L and on $M(\mathbb{C})$.

Since \mathcal{Y} and $\mathcal{Z}(m)$ intersect properly (recall that we assume \mathcal{Y}_K is Hodge-generic), we have the following description of $h_{\widehat{\mathcal{Z}}(m)}(\mathcal{Y})$. Let \mathcal{A} denote $\mathcal{A}_{\mathcal{Y}}^{\text{univ}}$, where $\mathcal{A}^{\text{univ}}$ is the Kuga–Satake abelian scheme over \mathcal{M} . Using the moduli definition of $\mathcal{Z}(m)$ in Section 2.5, the \mathcal{Y} -scheme $\mathcal{Y} \times_{\mathcal{M}} \mathcal{Z}(m)$ is given by

$$\mathcal{Y} \times_{\mathcal{M}} \mathcal{Z}(m)(S) = \{v \in V(\mathcal{A}_S) \mid v \circ v = [m]\}$$

for any \mathcal{Y} -scheme S . Via the natural map $\mathcal{Y} \times_{\mathcal{M}} \mathcal{Z}(m) \rightarrow \mathcal{Y}$, and using étale descent, we view $\mathcal{Y} \times_{\mathcal{M}} \mathcal{Z}(m)$ as a \mathbb{Q} -Cartier divisor on \mathcal{Y} . Therefore,

$$h_{\widehat{\mathcal{Z}}(m)}(\mathcal{Y}) = \sum_{\sigma: K \hookrightarrow \mathbb{C}} \Phi_m(\mathcal{Y}^\sigma) + \sum_{\mathfrak{P}} (\mathcal{Y} \cdot \mathcal{Z}(m))_{\mathfrak{P}} \log |\mathcal{O}_K / \mathfrak{P}|, \tag{3.1}$$

where for $\sigma : K \hookrightarrow \mathbb{C}$, we use \mathcal{Y}^σ to denote the point in $M(\mathbb{C})$ induced by $\text{Spec}(\mathbb{C}) \xrightarrow{\sigma} \text{Spec } \mathcal{O}_K \xrightarrow{\mathcal{Y}} \mathcal{M}$; and if we denote by $\mathcal{O}_{\mathcal{Y} \times_{\mathcal{M}} \mathcal{Z}(m), v}$ the étale local ring of $\mathcal{Y} \times_{\mathcal{M}} \mathcal{Z}(m)$ at v ,

$$(\mathcal{Y} \cdot \mathcal{Z}(m))_{\mathfrak{P}} = \sum_{v \in \mathcal{Y} \times_{\mathcal{M}} \mathcal{Z}(m)(\overline{\mathbb{F}}_{\mathfrak{P}})} \text{length}(\mathcal{O}_{\mathcal{Y} \times_{\mathcal{M}} \mathcal{Z}(m), v}), \tag{3.2}$$

where $\overline{\mathbb{F}}_{\mathfrak{P}}$ denotes the residue field of \mathfrak{P} .

3.2. Howard–Madapusi-Pera–Borcherds’ modularity theorem

Let $M_{1+\frac{b}{2}}(\rho_L)$ denote the \mathbb{C} -vector space of $\mathbb{C}[L^\vee/L]$ -valued modular forms of weight $1 + \frac{b}{2}$ with respect to ρ_L (see [Bru02, Definition 1.2]). Let $(\mathbf{e}_\beta)_{\beta \in L^\vee/L}$ denote the standard basis of $\mathbb{C}[L^\vee/L]$.

Theorem 3.1 [HM17, Theorem 9.4.1]. *Assume $b \geq 3$, and let $q = e^{2\pi i \tau}$. The formal generating series*

$$\widehat{\Phi}_L = \overline{\omega}^\vee \mathbf{e}_0 + \sum_{\substack{\beta \in L^\vee/L \\ m > 0, m \in Q(\beta) + \mathbb{Z}}} \widehat{\mathcal{Z}}(\beta, m) \cdot q^m \mathbf{e}_\beta$$

is an element of $M_{1+\frac{b}{2}}(\rho_L) \otimes \widehat{\text{Pic}}(\mathcal{M})_{\mathbb{Q}}$. More precisely, for any \mathbb{Q} -linear map $\alpha : \widehat{\text{Pic}}(\mathcal{M})_{\mathbb{Q}} \rightarrow \mathbb{C}$, we have $\alpha(\widehat{\Phi}_L) \in M_{1+\frac{b}{2}}(\rho_L)$.

3.3. Asymptotic estimates for the global height

In this subsection, we provide asymptotic estimates for the global height. First we introduce an Eisenstein series $(\tau, s) \rightarrow E_0(\tau, s)$ for $\tau \in \mathbb{H}$ and $s \in \mathbb{C}$ with $\text{Re}(s) > \frac{1}{2} - \frac{b}{4} = 1 - \frac{k}{2}$, which serves two purposes. First, the Fourier coefficients of its value at $s = 0$ give the main term in the Fourier coefficients of $\widehat{\Phi}_L$; see the proof of Proposition 3.2. Second, we will use the Fourier coefficients of $E_0(\tau, s)$ to describe Φ_m explicitly in Section 5.1.

Let $(\tau, s) \rightarrow E_0(\tau, s)$ denote the Eisenstein series defined in [BK03, Equation (1.4), (3.1) with $\beta = 0, \kappa = 1 + \frac{b}{2}$]. It converges normally on \mathbb{H} for $\text{Re}(s) > 1 - \frac{k}{2}$ and defines a $\text{Mp}_2(\mathbb{Z})$ -invariant real analytic function.

For a fixed $s \in \mathbb{C}$ with $\text{Re}(s) > 1 - \frac{k}{2}$, by [BK03, Proposition 3.1], the Eisenstein series $E_0(\cdot, s)$ has a Fourier expansion of the form

$$E_0(\tau, s) = \sum_{\beta \in L^\vee/L} \sum_{m \in Q(\beta) + \mathbb{Z}} c_0(\beta, m, s, y) e^{2\pi i m x} \mathbf{e}_\beta,$$

where we write $\tau = x + iy, x \in \mathbb{R}, y \in \mathbb{R}_{>0}$. By [BK03, Proposition 3.2], the coefficients $c_0(\beta, m, s, y)$ can be decomposed, for $m \neq 0$, as

$$c_0(\beta, m, s, y) = C(\beta, m, s)\mathcal{W}_s(4\pi my), \tag{3.3}$$

where the function $C(\beta, m, s)$ is independent of y (see [BK03, Equation (3.22)]) and \mathcal{W}_s is defined in [BK03, (3.2)].

By [BK03, Proposition 3.1, (3.3)], the value at $s = 0$ of $E_0(\tau, s)$ is an element of $M_{1+\frac{b}{2}}(\rho_L)$. For $\beta \in L^\vee/L, m \in Q(\beta) + \mathbb{Z}$ with $m \geq 0$, we denote by $c(\beta, m)$ its (β, m) th Fourier coefficient, and we can thus write

$$E_0(\tau) := E_0(\tau, 0) = 2e_0 + \sum_{\substack{\beta \in L^\vee/L \\ m \in Q(\beta) + \mathbb{Z}, m > 0}} c(\beta, m)q^m e_\beta, \text{ where } q = e^{2\pi i \tau}.$$

By definition and [BK03, Proposition 3.1, (3.3)], we have $C(\beta, n, 0) = c(\beta, n)$. By [BK03, Prop.4.8], the coefficient $c(\beta, m)$ encodes the degree of the special divisor $Z(\beta, m)(\mathbb{C})$. Moreover, [BK01, Proposition 4, equation (19)] gives explicit formulas for $c(\beta, m)$. By [BK01, Proposition 14], $c(\beta, m) < 0$ if $m \in Q(L + \beta)$ and $c(\beta, m) = 0$ if $m \notin Q(L + \beta)$. By [Tay20a, Example 2.3], we have that for $m \in Q(L + \beta)$,¹⁷

$$|c(\beta, m)| = -c(\beta, m) \asymp m^{\frac{b}{2}}. \tag{3.4}$$

We will henceforth focus on the case where $\beta = 0$, and we set $C(m, s) := C(0, m, s)$ and $c(m) := c(0, m)$. We are now ready to establish asymptotics for the global height in terms of the Fourier coefficients just defined.

Proposition 3.2. *For every $\epsilon > 0$ and $m \in \mathbb{Z}_{>0}$, we have*

$$h_{\widehat{\mathcal{Z}}(m)}(\mathcal{Y}) = \frac{-c(m)}{2} h_{\overline{\omega}}(\mathcal{Y}) + O_\epsilon(m^{\frac{2+b}{4} + \epsilon}).$$

In particular, we have $h_{\widehat{\mathcal{Z}}(m)}(\mathcal{Y}) = O(m^{\frac{b}{2}})$ as $m \rightarrow \infty$.

The second claim follows from the first claim and equation (3.4).

Proof. The proof is similar to the one in [Tay20a, Proposition 2.5]. For $\widehat{\mathcal{Z}} \in \widehat{\text{CH}}^1(\mathcal{M})_{\mathbb{Q}} \cong \widehat{\text{Pic}}(\mathcal{M})_{\mathbb{Q}}$, the height $h_{\widehat{\mathcal{Z}}}(\mathcal{Y})$ defines a \mathbb{Q} -linear map $\widehat{\text{Pic}}(\mathcal{M})_{\mathbb{Q}} \rightarrow \mathbb{R}$; by Theorem 3.1, the following generating series

$$-h_{\overline{\omega}}(\mathcal{Y})e_0 + \sum_{\substack{\beta \in L^\vee/L \\ m > 0, m \in Q(\beta) + \mathbb{Z}}} h_{\widehat{\mathcal{Z}}(\beta, m)}(\mathcal{Y}) \cdot q^m e_\beta$$

is the Fourier expansion of an element in $M_{1+\frac{b}{2}}(\rho_L)$. By [Bru02, p.27], we write

$$-h_{\overline{\omega}}(\mathcal{Y})e_0 + \sum_{\substack{\beta \in L^\vee/L \\ m > 0, m \in Q(\beta) + \mathbb{Z}}} h_{\widehat{\mathcal{Z}}(\beta, m)}(\mathcal{Y}) \cdot q^m e_\beta = \frac{-h_{\overline{\omega}}(\mathcal{Y})}{2} E_0 + g,$$

where $E_0 = E_0(\tau)$ is the Eisenstein series recalled in Section 3.3 and $g \in M_{1+\frac{b}{2}}(\rho_L)$ is a cusp form; see [Bru02, Def.1.2] for a definition.

¹⁷Recall that $b \geq 3$.

For $m \in \mathbb{Z}_{>0}$, the equation for the e_0 -component implies that

$$h_{\widehat{z}(m)}(\mathcal{Y}) = \frac{-c(m)}{2} h_{\overline{w}}(\mathcal{Y}) + g(m),$$

where $g(m)$ is the m th Fourier coefficient of the e_0 -component of g . We obtain the desired estimate by [Sar90, Prop. 1.5.5], which implies that

$$|g(m)| \leq C_{\epsilon, g} m^{\frac{2+b}{4} + \epsilon}$$

for all $\epsilon > 0$, some constant $C_{\epsilon, g} > 0$ and all $m \in \mathbb{Z}_{>0}$. □

4. General results on quadratic forms

In this section, we collect some general results on quadratic forms that will be used in Sections 5–7. First, in Section 4.1, we prove estimates on the number of local representations of integral quadratic forms that will be used in Section 5.1. Then, in Section 4.2, we state results due to Heath-Brown on the number of integral representations of integral quadratic forms that will be used in Sections 6 and 7. In Section 4.3, we apply Heath-Brown’s results to the lattice (L, Q) in Section 2 and also recall the work of Niedermowwe, which could be viewed as a refinement of Heath-Brown’s work; these results are used in Section 6. The reader may skip this section first and refer back later.

4.1. Local estimates of representations by quadratic forms

Recall that (L, Q) is an even quadratic lattice of signature $(b, 2)$ with $b \geq 3$, and L is maximal in $V = L \otimes \mathbb{Q}$. Let $r = b + 2$ denote the rank of L , and let $\det(L)$ denote the Gram determinant of L . Let p be a fixed prime, and let val_p denote the p -adic valuation. For integers $m \in \mathbb{Z}$ and $n \in \mathbb{Z}_{\geq 0}$, we define the set $\mathcal{N}_m(p^n)$, its size $N_m(p^n)$ and the density $\mu_p(m, n)$ as follows:

$$\begin{aligned} \mathcal{N}_m(p^n) &= \{v \in L/p^n L \mid Q(v) \equiv m \pmod{p^n}\}; \\ N_m(p^n) &= |\mathcal{N}_m(p^n)|; \\ \mu_p(m, n) &= p^{-n(r-1)} N_m(p^n). \end{aligned} \tag{4.1}$$

The goal of this subsection is to study the variation of the quantity $\mu_p(m, n)$. Define the quantity $w_p(m) := 1 + \text{val}_p(m)$ for $p \neq 2$ and $w_2(m) := 1 + 2 \text{val}_2(2m)$. Then we prove the following result.

Proposition 4.1. *If m is an integer representable by Q over \mathbb{Z} , then we have*

$$\left| w_p(m) - \sum_{n=0}^{w_p(m)-1} \frac{\mu_p(m, n)}{\mu_p(m, w_p(m))} \right| \ll \frac{1}{p},$$

where the implied constant is independent of p and m .

We use an inductive method, due to Hanke [Han04], to compute the quantities $\mu_p(m, n)$. Let $L_p := L \otimes \mathbb{Z}_p$ be the completion of L at p . Since L is maximal in V , it follows that L_p is maximal in $V \otimes \mathbb{Q}_p$. Indeed, L being maximal is equivalent to the fact that L^\vee/L has no totally isotropic subgroup; thus its p -torsion, which is equal to L_p^\vee/L_p , has no totally isotropic subgroup implying that L_p is maximal. It is well known that the quadratic lattice (L_p, Q) admits an orthogonal decomposition

$$(L_p, Q) = \bigoplus_j (L_j, p^{v_j} Q_j) \tag{4.2}$$

with $v_j \geq 0$, such that (L_j, Q_j) is a \mathbb{Z}_p -unimodular quadratic lattice of dimension 1 or 2. (See, for example, [Han04, (2.3), Lemma 2.1].) Moreover, when $p \neq 2$, then every L_j is of dimension 1. For every $v \in L_p$, we write $v = (v_j)_j$, and we have

$$Q(v) = \sum_j p^{v_j} Q_j(v_j).$$

Note that since L_p is maximal, we have $v_j \leq 1$ for each j . For $i \in \{0, 1\}$, let S_i denote the set of indices j with $v_j = i$, and let s_i denote the size of S_i .

Following [Han04, Definition 3.1], for $n \geq 1$, $v \in \mathcal{N}_m(p^n)$, we say that v is of

1. *zero type* if $v \equiv 0 \pmod{p}$,
2. *good type* if there exists j such that $v_j \not\equiv 0 \pmod{p}$ and $v_j = 0$, or
3. *bad type* otherwise.

Let $\mathcal{N}_m^{\text{good}}(p^n)$, $\mathcal{N}_m^{\text{bad}}(p^n)$ and $\mathcal{N}_m^{\text{zero}}(p^n)$ be the set of good type, bad type and zero type solutions, respectively, and set $N_m^?(p^n) = |\mathcal{N}_m^?(p^n)|$ and $\mu_p^?(m, n) = p^{-n(r-1)} N_m^?(p^n)$, for $? = \text{good, bad, or zero}$.

Note also from [Han04, Remark 3.4.1] that we have $\mathcal{N}_m(p^n) = \mathcal{N}_m^{\text{good}}(p^n)$ when $p \nmid m$; $\mathcal{N}_m^{\text{zero}}(p^n) = \emptyset$ when $p^2 \nmid m$ and $n \geq 2$; and $\mathcal{N}_m^{\text{bad}}(p^n) = \emptyset$ when $p \nmid 2 \det(L)$.

To state the inductive result on local densities, we need to introduce the auxiliary form Q' , where Q' is obtained from the orthogonal decomposition given by equation (4.2) of Q by replacing v_j with $v'_j = 1 - v_j$ for all j . To distinguish between the local densities of Q and Q' , we use $N_{m,Q}^?(p^n)$ and $\mu_{p,Q}^?(m, n)$ to emphasise the dependence on the quadratic form. We now recall Hanke’s inductive method with the simplification that L is maximal (only used in (2)).

Lemma 4.2 (Hanke). *Let $n \in \mathbb{Z}_{>0}$, and set $\delta = 2 \text{val}_2(p) + 1$.*

1. *For $n \geq \delta$ and all integers m , we have*

$$N_m^{\text{good}}(p^n) = p^{(n-\delta)(r-1)} N_m^{\text{good}}(p^\delta); \quad \mu_p^{\text{good}}(m, n) = \mu_p^{\text{good}}(m, \delta).$$

2. *For m such that $p \mid m$, we have*

$$N_{m,Q}^{\text{bad}}(p^{n+1}) = p^{r-s_0} N_{\frac{m}{p}, Q}^{\text{good}}(p^n); \quad \mu_{p,Q}^{\text{bad}}(m, n+1) = p^{1-s_0} \mu_{p,Q}^{\text{good}}\left(\frac{m}{p}, n\right).$$

3. *For m such that $p^2 \mid m$, we have*

$$N_m^{\text{zero}}(p^{n+2}) = p^r N_{\frac{m}{p^2}}(p^n); \quad \mu_p^{\text{zero}}(m, n+2) = p^{2-r} \mu_p\left(\frac{m}{p^2}, n\right).$$

Proof. All the assertions on μ_p follow from the assertions on N_m by definition. The first assertion of the lemma is [Han04, Lemma 3.2]. The third assertion follows from the last two paragraphs in [Han04, p.359]. To recover the second assertion, note that since L_p is maximal, we have $v_j \leq 1$ for all j . Hence Bad-type II points (see [Han04, p.360]) do not exist. Thus, the claim follows from the discussion on Bad-type I points in [Han04, p.359]. □

Corollary 4.3. *For $p \neq 2$, set $\delta_{p, \det(L)} = 1$ if $p \mid \det(L)$ and 0 otherwise.¹⁸ Recall the quadratic form Q' and the integer s_0 defined above. We have*

¹⁸In the formulas below, we do not need to introduce this term $\delta_{p, \det(L)}$, because by definition, if $p \nmid \det(L)$, then $v'_j = 1$ for all j and hence $\mu_{p,Q'}^{\text{good}}(m, n) = 0$. Nevertheless, we put it here to emphasise that those terms are 0.

1. If $n \geq \text{val}_p(m) + 1$, then $\mu_{p,Q}(m, n)$ is equal to

$$\sum_{u=0}^{\lfloor \frac{\text{val}_p(m)}{2} \rfloor} p^{(2-r)u} \mu_{p,Q}^{\text{good}}\left(\frac{m}{p^{2u}}, 1\right) + \delta_{p,\det(L)} p^{1-s_0} \sum_{u=0}^{\lfloor \frac{\text{val}_p(m)-1}{2} \rfloor} p^{(2-r)u} \mu_{p,Q'}^{\text{good}}\left(\frac{m}{p^{2u+1}}, 1\right).$$

2. If $1 \leq n \leq \text{val}_p(m)$ and n odd, then $\mu_{p,Q}(m, n)$ is equal to

$$p^{\frac{(2-r)(n-1)}{2}} \mu_{p,Q}(mp^{1-n}, 1) + \sum_{u=0}^{\frac{n-3}{2}} p^{(2-r)u} \mu_{p,Q}^{\text{good}}\left(\frac{m}{p^{2u}}, 1\right) + \delta_{p,\det(L)} p^{1-s_0} \sum_{u=0}^{\frac{n-3}{2}} p^{(2-r)u} \mu_{p,Q'}^{\text{good}}\left(\frac{m}{p^{2u+1}}, 1\right).$$

3. If $1 \leq n \leq \text{val}_p(m)$ and n even, then $\mu_{p,Q}(m, n)$ is equal to

$$p^{\frac{(2-r)(n-2)}{2}} \mu_{p,Q}^{\text{zero}}(mp^{2-n}, 2) + \sum_{u=0}^{\frac{n-2}{2}} p^{(2-r)u} \mu_{p,Q}^{\text{good}}\left(\frac{m}{p^{2u}}, 1\right) + \delta_{p,\det(L)} p^{1-s_0} \sum_{u=0}^{\frac{n-2}{2}} p^{(2-r)u} \mu_{p,Q'}^{\text{good}}\left(\frac{m}{p^{2u+1}}, 1\right).$$

Proof. The base cases when $\text{val}_p(m) \leq 1$ or $n \leq 2$ can be checked directly by definition and Lemma 4.2. For $n > 2$ and $p^2 \mid m$, by Lemma 4.2,

$$\begin{aligned} \mu_{p,Q}(m, n) &= \mu_{p,Q}^{\text{good}}(m, n) + \mu_{p,Q}^{\text{zero}}(m, n) + \mu_{p,Q}^{\text{bad}}(m, n) \\ &= \mu_{p,Q}^{\text{good}}(m, 1) + p^{2-r} \mu_{p,Q}\left(\frac{m}{p^2}, n-2\right) + p^{1-s_0} \mu_{p,Q'}^{\text{good}}\left(\frac{m}{p}, n-1\right) \\ &= \mu_{p,Q}^{\text{good}}(m, 1) + p^{2-r} \mu_{p,Q}\left(\frac{m}{p^2}, n-2\right) + p^{1-s_0} \mu_{p,Q'}^{\text{good}}\left(\frac{m}{p}, 1\right). \end{aligned}$$

Then we conclude by induction on $\text{val}_p(m)$ and n . □

The next lemma gives a uniform bound on $|\mu_p(m, n) - \mu_p(m, w_p(m))|$ for primes p , integers m and $n \in \{2, \dots, w_p(m) - 1\}$.

Lemma 4.4. *Let p be prime and m be any integer. For $n \in \{2 + \text{val}_2(p), \dots, w_p(m) - 1\}$, we have*

$$|\mu_p(m, n) - \mu_p(m, w_p(m))| \ll \frac{1}{p^{3\lfloor (n/2) \rfloor - 2}},$$

where the implied constant is absolute.

Proof. First consider the case when p is odd. By Corollary 4.3, we have that for n odd,

$$\begin{aligned} |\mu_p(m, n) - \mu_p(m, w_p(m))| &\leq \left| \frac{\mu_{p,Q}\left(\frac{m}{p^{n-1}}, 1\right)}{p^{\frac{(r-2)(n-1)}{2}}} \right| \\ &\quad + \left| \frac{\sum_{u=\frac{(n-1)}{2}}^{\lfloor \frac{\text{val}_p(m)}{2} \rfloor} \mu_{p,Q}^{\text{good}}\left(\frac{m}{p^{2u}}, 1\right) + \delta_{p,\det(L)} p^{1-s_0} \mu_{p,Q'}^{\text{good}}\left(\frac{m}{p^{2u+1}}, 1\right)}{p^{(r-2)u}} \right| \\ &\leq \left| \frac{p}{p^{\frac{3(n-1)}{2}}} \right| + \sum_{u=\frac{(n-1)}{2}}^{\lfloor \frac{\text{val}_p(m)}{2} \rfloor} \left| \frac{p+p^2}{p^{3u}} \right| \\ &\leq \frac{C_1 p^2}{p^{\frac{3(n-1)}{2}}}. \end{aligned}$$

Here we use the trivial bound that all $|\mu_{p,Q}(\frac{m}{p^{n-1}}, 1)|, |\mu_{p,Q}^{\text{good}}(\frac{m}{p^{2u}}, 1)|, |\mu_{p,Q'}^{\text{good}}(\frac{m}{p^{2u+1}}, 1)|$ are less than p by definition. The case when n is even follows by a similar argument and the trivial bound that $\mu_{p,Q}^{\text{zero}}(mp^{2-n}, 2) \leq p^r/p^{2(r-1)} = p^{2-r}$.

For $p = 2$, by Lemma 4.2, we obtain analogous statements as Corollary 4.3, except that we can only reduce to $\mu_p^{\text{good}}(? , 3)$ (instead of $\mu_p^{\text{good}}(? , 1)$). The rest of the argument is the same as in Lemma 4.4, and since $p = 2$ is fixed, any trivial bound on density is absorbed in the absolute constant. \square

We can actually show that all $\mu_p(m, n)$ are close to 1 when $p \nmid 2 \det(L)$.

Lemma 4.5. *There exists an absolute constant $C_2 > 0$ such that for all $m, n \in \mathbb{Z}_{>0}$, all primes $p \nmid 2 \det(L)$, we have*

$$|\mu_p(m, n) - 1| \leq \frac{C_2}{p}.$$

Proof. By Corollary 4.3(1), Lemma 4.4, we only need to show the claim for $n = 1$ and $n = \text{val}_p(m) + 1$. For $n = 1$, we first consider the case when $p \mid m$. Then $Q(v) \equiv 0 \pmod p$ defines a smooth projective hypersurface in \mathbb{P}^{r-1} ; except the solution $v = 0 \pmod p$, every $p - 1$ solutions of $Q(v) \equiv 0 \pmod p$ (all these are of good type) correspond to a \mathbb{F}_p -point in the hypersurface. Then by the Weil bound (see, for instance, [Del74, Théorème 8.1]),¹⁹ there exists a constant $C_3 > 0$ independent of p and m such that

$$|N_m^{\text{good}}(p) - p^{r-1}| \leq C_3 p^{r-2}.$$

Therefore, $|\mu_p^{\text{good}}(m, 1) - 1| \leq C_3/p$.

For $p \nmid m$, we consider the smooth projective hypersurface in \mathbb{P}^r defined by $Q(v) = my^2$. In this case, $N_m(p) = N_m^{\text{good}}(p)$ is the number of \mathbb{F}_p -points in the hypersurface such that $y \neq 0$ in \mathbb{F}_p . By the Weil bound, the number of \mathbb{F}_p -points in the hypersurface is $p^{r-1} + O_m(p^{r-2})$; the number of $y = 0$ points on the hypersurface is $p^{r-2} + O(p^{r-3})$ by the Weil bound. Then we conclude that there exists a constant $C_4 > 0$ independent²⁰ of p and m such that $|\mu_p^{\text{good}}(m, 1) - 1| \leq C_4/p$. In particular, for any m , we have

$$\mu_p^{\text{good}}(m, 1) \leq 1 + \max\{C_3, C_4\}.$$

For $n = \text{val}_p(m) + 1$ and $p \mid m$, by Corollary 4.3(1), and note that $\delta_{p, \det(L)} = 0$, we have

$$\begin{aligned} |\mu_p(m, \text{val}_p(m) + 1) - 1| &= \left| \mu_p^{\text{good}}(m, 1) - 1 + \sum_{u=1}^{\lfloor \frac{\text{val}_p(m)}{2} \rfloor} \frac{\mu_p^{\text{good}}(\frac{m}{p^{2u}}, 1)}{p^{u(r-2)}} \right| \\ &\leq \frac{C_3}{p} + \sum_{u=1}^{\lfloor \frac{\text{val}_p(m)}{2} \rfloor} \frac{\max\{C_3, C_4\} + 1}{p^{u(r-2)}} \leq \frac{C_5}{p}, \end{aligned}$$

where we take $C_2 = \max\{C_3, C_4, C_5\}$. \square

Due to our assumptions that $r \geq 5$ and L maximal, there is an absolute lower bound for $\mu_p(m, n)$. The following lemma is well known, but we include it for the convenience of the reader.

Lemma 4.6. *Recall that $r \geq 5$ and L is maximal. Then for any $m, n \in \mathbb{Z}_{>0}$, any prime p , we have $\mu_p(m, n) \geq 1/2$.*

¹⁹In our specific case, namely that of a quadratic form, this result was in [Wei49].

²⁰Although the equation of the hypersurface depends on m , the number of solutions only depends on whether m is a quadratic square in \mathbb{F}_p . So we only need to apply the Weil bound for a fixed square m , and for some fixed nonsquare m , to obtain some C_4 independent of m .

Proof. Since $r \geq 5$ and L is maximal, then by, for instance, [Ger08, Lemma 6.36], for every prime p , there exists a basis of L_p such that in the coordinate of this basis, $Q((x_1, \dots, x_r)) = x_1x_2 + Q_1((x_3, \dots, x_r))$, where Q_1 is a quadratic form in $(r - 2)$ variables.

Recall as in Lemma 4.2 that $\delta = 3$ if $p = 2$ and $\delta = 1$ otherwise. Fix an integer δ' satisfying $1 \leq \delta' \leq \delta$. For any $x_1 \in (\mathbb{Z}/p^{\delta'})^\times$ and any $x_i \in \mathbb{Z}/p^{\delta'}$, $3 \leq i \leq r$, there exists a unique $x_2 \in \mathbb{Z}/p^{\delta'}$ such that $Q(x_1, \dots, x_r) = m \pmod{p^{\delta'}}$. Therefore, $\mu_p^{\text{good}}(m, \delta') \geq \frac{p-1}{p} \geq 1/2$, and hence by Lemma 4.2(1), for $n \geq \delta$, $\mu_p(m, n) \geq \mu_p^{\text{good}}(m, \delta) \geq 1/2$. □

Corollary 4.7. *Every large enough $m \in \mathbb{Z}_{>0}$ is representable by (L, Q) .*

Proof. By [HB96, Theorem 4] (recalled in Theorem 4.9 below, from which we borrow the notations), we can choose a non-negative test function ω such that $\mu_\infty(Q, \omega) > 0$. Then by the Proposition above, $\mu(Q, m) > 0$, and hence $N(Q, m, \omega)$ is positive for m large enough. Hence m is representable by (L, Q) . □

Now we are ready to prove the main result of this subsection.

Proof of Proposition 4.1. For simplicity of notation, we denote $w_p(m)$ by w_p .

First case: assume that $p \nmid 2 \det(L)$. By Lemma 4.5,

$$|\mu_p(m, w_p) - \mu_p(m, 1)| \leq |\mu_p(m, w_p) - 1| + |\mu_p(m, 1) - 1| \leq C_7/p. \tag{4.3}$$

Note that $\mu_p(m, 0) = 1$ by definition; see 4.1. Then by Lemmas 4.4, 4.5 and equation (4.3), we get

$$\left| w_p - \sum_{n=0}^{w_p-1} \frac{\mu_p(m, n)}{\mu_p(m, w_p)} \right| \leq \frac{1}{\mu_p(m, w_p)} \left[\sum_{n \geq 2} \frac{C_1 p^2}{p^{3\lfloor n/2 \rfloor}} + \frac{C_7}{p} + \frac{C_2}{p} \right] \leq \frac{C_8}{\mu_p(m, w_p)p}.$$

We conclude by the fact that $\mu_p(m, w_p)$ is uniformly bounded away from 0 by Lemma 4.6.

Second case: assume now that $p \mid 2 \det(L)$. By Lemma 4.4, for any $n \geq 3$,

$$|\mu_p(m, w_p) - \mu_p(m, n)| \leq \frac{C_9 p^2}{p^{3\lfloor n/2 \rfloor}}. \tag{4.4}$$

Then, as in the first case, we have

$$\left| \sum_{n=3}^{w_p-1} \frac{\mu_p(m, w_p) - \mu_p(m, n)}{\mu_p(m, w_p)} \right| \leq \frac{C_{10}}{p}.$$

On the other hand, for $0 \leq n \leq 2$, we have for all $p \mid 2 \det(L)$

$$|\mu_p(m, w_p) - \mu_p(m, n)| \leq |\mu_p(m, w_p) - \mu_p(m, 3)| + |\mu_p(m, 3) - \mu_p(m, n)| \leq C_{11}/p$$

by equation (4.4) and the trivial bound $|\mu_p(m, n)|, |\mu_p(m, 3)| \leq p^3 \leq (2 \det(L))^3$. Then we conclude as in the first case. □

4.2. On the number of representations of quadratic forms

Developing a new form of the circle method, Heath-Brown [HB96] proves a number of results pertaining to the representation of integers by quadratic forms. The purpose of this subsection is to describe the setup used in [HB96] and recall those results necessary for us in the sequel. We do not entirely keep the notations of [HB96] since we will only be concerned with homogeneous quadratic forms, which allows us to make certain simplifications in the notation.

Let $F(\mathbf{x}) = F(x_1, \dots, x_n)$ be an integral quadratic form with nonzero discriminant in $n \geq 5$ variables. A function $\omega : \mathbb{R}^n \rightarrow \mathbb{C}$ is said to be a *smooth weight function* if it is infinitely differentiable of compact support. Given a set S of parameters (see [HB96, Page 6] for what the parameters are allowed to be), Heath-Brown defines a set of weight functions $\mathcal{C}(S)$ in [HB96, §2].

Remark 4.8. The following facts about weight functions will be used later (see, for instance, the observations of [HB96, p. 162]):

1. There exists a function $\omega_0^{(n)}(\mathbf{x}) : \mathbb{R}^n \rightarrow [0, 2]$, with compact support in $[-1, 1]^n$, which belongs to $\mathcal{C}(n)$ such that $\omega_0^{(n)}(\mathbf{x}) \geq 2$ for $x \in [-1/2, 1/2]^n$ (for instance, by rescaling the function defined by [HB96, (2.1),(2.2)]).
2. Let M be an invertible $n \times n$ matrix, such that the coefficients of both M and M^{-1} are bounded in absolute value by K . If ω is a weight function belonging to $\mathcal{C}(S)$, then $\omega(Mx)$ belongs to $\mathcal{C}(S, K)$.

The reason for introducing the set $\mathcal{C}(S)$ is the following. For the quadratic form F fixed as above, an integer $m \neq 0$ and a weight function $\omega \in \mathcal{C}(S)$ for some set of parameters S , we define

$$N(F, m, \omega) := \sum_{\substack{\mathbf{x} \in \mathbb{Z}^n \\ F(\mathbf{x})=m}} \omega\left(\frac{\mathbf{x}}{\sqrt{m}}\right).$$

The quantity $N(F, m, \omega)$ then is a weighted sum of representations of m by F , where the coordinates of these representations are bounded by $O_S(\sqrt{m})$ since ω has compact support. Then [HB96] gives asymptotics for the size of $N(F, m, \omega)$, where the error term only depends on S .

More precisely, define the *singular integral* by²¹

$$\mu_\infty(F, \omega) := \lim_{\epsilon \rightarrow 0} \frac{1}{2\epsilon} \int_{|F(\mathbf{x})-1| \leq \epsilon} \omega(\mathbf{x}) d\mathbf{x}.$$

Recall the Siegel mass at p of the quadratic form F given by²²

$$\mu_p(F, m) := \lim_{k \rightarrow \infty} \frac{1}{p^{(n-1)k}} |\{\mathbf{x} \pmod{p^k} : F(\mathbf{x}) \equiv m \pmod{p^k}\}|$$

and define the *singular series* by

$$\mu(F, m) := \prod_p \mu_p(F, m).$$

In our situation with $n \geq 5$, the singular series always converges absolutely; see also, for instance, [Iwa97, §11.5]. Now [HB96, Theorem 4] states the following.

Theorem 4.9 [HB96, Theorem 4]. *Let the notation be as above, and let $\omega \in \mathcal{C}(S)$ be a weight function for some set of parameters S . Then*

$$N(F, m, \omega) = \mu_\infty(F, \omega)\mu(F, m)m^{n/2-1} + O_{F,S,\epsilon}(m^{(n-1)/4+\epsilon}).$$

Note in particular that the error term depends only on F and S and not on the specific weight function ω or on m .

We also recall a corollary of the above theorem for positive definite quadratic forms, which will be used in Section 7.

²¹As explained on [HB96, p.154-155], for weight functions $\omega \in \mathcal{C}(S)$, this limit exists.

²²Using the notation in Section 4.1, $\mu_p(F, m) = \lim_{k \rightarrow \infty} \mu_{p,F}(m, k)$. From the discussion in Section 4.1, given F, m, p , $\mu_{p,F}(m, k)$ stabilises as $k \gg 1$, and hence the limit automatically exists.

Corollary 4.10 [HB96, Corollary 1]. *Let the notation be as above, and assume further that F is positive definite. Then*

$$|\{\mathbf{x} \in \mathbb{Z}^n : F(\mathbf{x}) = m\}| = \mu_\infty(F, 1)\mu(F, m)m^{n/2-1} + O_{F,\epsilon}(m^{(n-1)/4+\epsilon}).$$

4.3. An application of Heath-Brown’s theorem and a result of Niederreiter

Recall that (L, Q) is an even quadratic lattice of signature $(b, 2)$ with $b \geq 3$. We will apply Heath-Brown’s result to (L, Q) (here we identify L with \mathbb{Z}^{b+2}) after we construct suitable smooth weight functions. Moreover, we recall Niederreiter’s result, which is analogous to Heath-Brown’s result but with sharp weight functions given by characteristic functions of certain expanding domains Ω_T defined below and keeps track of the dependence of the error term on T .

Similar to the definition of the singular integral $\mu_\infty(F, \omega)$ in Section 4.2, we define a measure μ_∞ on

$$L_{\mathbb{R},1} := \{\lambda \in L_{\mathbb{R}} : Q(\lambda) = 1\}$$

as follows. For an open bounded subset W of $L_{\mathbb{R}}$, we set

$$\mu_\infty(W \cap L_{\mathbb{R},1}) := \lim_{\epsilon \rightarrow 0} \frac{1}{2\epsilon} \mu_L(\{\lambda \in W : |Q(\lambda) - 1| < \epsilon\}), \tag{4.5}$$

where μ_L is the Lebesgue measure on $L_{\mathbb{R}}$ normalised so that L has covolume 1.²³

Let x denote a fixed point in the period domain D_L , and let P denote the negative definite plane (with respect to Q) in $L_{\mathbb{R}}$ associated to x . Let P^\perp denote the orthogonal complement of P in $L_{\mathbb{R}}$. Given a vector $\lambda \in L_{\mathbb{R}}$, we let λ_x and λ_{x^\perp} denote the projections of λ to P and P^\perp , respectively.

We introduce notation for the set of elements in $L_{\mathbb{R},1}$ with bounded value of $Q(\lambda_x)$: for $T > 0$, define

$$\Omega_{\leq T} := \{\lambda \in L_{\mathbb{R},1} : -Q(\lambda_x) \in [0, T]\}.$$

Then the following lemma computes the volume of the sets $\Omega_{\leq T}$. Recall that $k = 1 + \frac{b}{2}$.

Lemma 4.11. *Let $T > 0$ be a real number. Then*

$$\mu_\infty(\Omega_{\leq T}) = \frac{(2\pi)^k \left((1+T)^{\frac{b}{2}} - 1 \right)}{\sqrt{|L^\vee/L|} \Gamma(k)}.$$

Proof. For $\epsilon > 0$, let $U_{T,\epsilon} := \{x \in L_{\mathbb{R}} : |Q(x) - 1| < \epsilon, -Q(\lambda_x) < T\}$. Then $\Omega_{\leq T} = U_{T,\epsilon} \cap L_{\mathbb{R},1}$ and by definition

$$\mu_\infty(\Omega_{\leq T}) = \lim_{\epsilon \rightarrow 0} \frac{\mu_L(U_{T,\epsilon})}{2\epsilon}.$$

Let \mathcal{E} be an orthogonal basis of $L_{\mathbb{R}}$ adapted to the decomposition $P \oplus P^\perp$ and in which the bilinear form associated to Q has the intersection matrix

$$\begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & I_b \end{pmatrix},$$

²³Let $\mathbf{1}_W$ be the characteristic function on W . Then by abuse of notation (since $\mathbf{1}_W$ is not smooth), we have $\mu_\infty(Q, \mathbf{1}_W) = \mu_\infty(W \cap L_{\mathbb{R},1})$.

where I_b denotes the $b \times b$ identity matrix. Let $\mu_{\mathcal{E}}$ be the associated Lebesgue measure for which the \mathbb{Z} -span of \mathcal{E} is of covolume 1. By change of variables, we have

$$\begin{aligned} \mu_L(U_T, \epsilon) &= \frac{2^{1+\frac{b}{2}}}{\sqrt{|L^{\vee}/L|}} \mu_{\mathcal{E}}(U_T, \epsilon) \\ &= \frac{2^{1+\frac{b}{2}}}{\sqrt{|L^{\vee}/L|}} \int_{\substack{(x_1, x_2, y_1, \dots, y_b) \in \mathbb{R}^{b+2} \\ |x_1^2+x_2^2-y_1^2-\dots-y_b^2+1| < \epsilon \\ x_1^2+x_2^2 < T}} dx_1 dx_2 dy_1 \cdots dy_b \\ &= \frac{2^{2+\frac{b}{2}} \pi}{\sqrt{|L^{\vee}/L|}} \int_0^{\sqrt{T}} \left(\int_{1+r^2-\epsilon < y_1^2+\dots+y_b^2 < 1+r^2+\epsilon} dy_1 \cdots dy_b \right) r dr \\ &= \frac{2(2\pi)^{1+\frac{b}{2}}}{\sqrt{|L^{\vee}/L|} \Gamma\left(1+\frac{b}{2}\right)} \int_0^{\sqrt{T}} \left((1+r^2+\epsilon)^{\frac{b}{2}} - (1+r^2-\epsilon)^{\frac{b}{2}} \right) r dr \\ &= 2\epsilon \cdot \frac{(2\pi)^{1+\frac{b}{2}} \left((1+T)^{\frac{b}{2}} - 1 \right)}{\sqrt{|L^{\vee}/L|} \Gamma\left(1+\frac{b}{2}\right)} + O(\epsilon^2). \end{aligned}$$

Dividing by 2ϵ and letting ϵ go to zero, we get the desired result. □

We now describe the desired estimates for $\left\{ \lambda \in L : Q(\lambda) = m, \lambda/\sqrt{m} \in \Omega_{\leq T} \right\}$ in two cases.

4.3.1. Assume $T \leq 1$

In this case, we only need a good upper bound, and hence we construct a suitable smooth weight function $\omega : L_{\mathbb{R}} \rightarrow \mathbb{R}$ as follows and apply Heath-Brown’s theorem.

Corollary 4.12. *Given (L, Q) as above, for any $m \in \mathbb{Z}_{>0}$, any $0 < T \leq 1$, we have*

$$\left\{ \lambda \in L : Q(\lambda) = m, \lambda/\sqrt{m} \in \Omega_{\leq T} \right\} = O_Q(m^{\frac{b}{2}} T) + O_{Q,T,\epsilon}(m^{(b+1)/4+\epsilon}).$$

Proof. By Remark 4.8, there exist smooth functions $\omega_P : P \rightarrow [0, 2]$ and $\omega_{P^\perp} : P^\perp \rightarrow [0, 2]$ such that

1. $\omega_P(\lambda_x) \geq 1$ for elements $\lambda_x \in P$ with $Q(\lambda_x) < T$ and $\omega_P(\lambda_x) = 0$ if $Q(\lambda_x) > 2T$.
2. $\omega_{P^\perp}(\lambda_{x^\perp}) \geq 1$ if $Q(\lambda_{x^\perp}) \leq 1$ and $\omega_{P^\perp}(\lambda_{x^\perp}) = 0$ if $Q(\lambda_{x^\perp}) \geq 2$.

We define $\omega(\lambda) = \omega_P(\lambda_x)\omega_{P^\perp}(\lambda_{x^\perp})$, and by construction, $\omega \in \mathcal{C}(b, T)$.

By definition, $\left\{ \lambda \in L : Q(\lambda) = m, \lambda/\sqrt{m} \in \Omega_{\leq T} \right\} \leq N(Q, m, \omega)$. By definition and Lemma 4.11, the singular integral $\mu_\infty(Q, \omega) \ll \mu_\infty(\Omega_{\leq 2T}) = O(T)$. Then the assertion follows by applying Theorem 4.9 to ω and the fact that $\mu(Q, m) = O_F(1)$ (since $b \geq 3$). □

4.3.2. Assume $T \geq 1$

In this case, we will need the exact main term along with an error term with explicit dependence on T , and we will apply Niederreiter’s work [Nie10].

For the convenience of later use, for an integer $m \geq 1$, we define the quantity

$$a(m) = \frac{-c(m)\Gamma(k)\sqrt{|L^{\vee}/L|}}{2(2\pi)^k}, \tag{4.6}$$

where $c(m)$ is the m th Fourier coefficient of the Eisenstein series defined in Section 3.3. Note that $a(m)$ grows as $\asymp m^{\frac{b}{2}}$. We have the following proposition, which follows from work of Niederreiter [Nie10].

Proposition 4.13. *Let $A > 1$ be a positive real number. For any $m \in \mathbb{Z}_{>0}$, $T \geq 1$, we have*

$$|\{\lambda \in L : Q(\lambda) = m, \lambda/\sqrt{m} \in \Omega_{\leq T}\}| = a(m)\mu_\infty(\Omega_{\leq T}) + O(m^{\frac{b}{2}}T^{\frac{b}{2}} \log(mT)^{-A}).$$

Proof. In [Nie10, Theorem 3.6], Niedermowwe estimates the number of lattice points with fixed norm in homogeneously expanding rectangular regions. His proof carries over without change for our region, yielding that²⁴

$$|\{\lambda \in L : Q(\lambda) = m, \lambda/\sqrt{m} \in \Omega_{\leq T}\}| = \mu_\infty(\Omega_{\leq T})m^{\frac{b}{2}}\mu(Q, m) + O(m^{\frac{b}{2}}T^{\frac{b}{2}} \log(mT)^{-A}).$$

We then deduce the desired formula by the explicit formula for $c(m)$ in [BK01, (22),(23)], which asserts

$$c(m) = -\frac{2(2\pi)^{\frac{b}{2}+1}m^{\frac{b}{2}}}{\sqrt{|L^\vee/L|}\Gamma(\frac{b}{2}+1)} \prod_p \mu_p(Q, m). \quad \square$$

We conclude this section by an integral computation similar to Lemma 4.11, which will be used later. For $s \in \mathbb{R}$, consider the function

$$h_s : L_{\mathbb{R}} \rightarrow \mathbb{R}^+ \\ \lambda \mapsto \left(\frac{1}{1-Q(\lambda_x)}\right)^{k-1+s}.$$

Lemma 4.14. *For $s > 0$, we have*

$$\int_{L_{\mathbb{R},1}} h_s(\lambda)d\mu_\infty(\lambda) = \frac{b}{4} \cdot \frac{|c(m)|}{s \cdot a(m)}.$$

Proof. As in the proof of Lemma 4.11, we define $L_\epsilon =: \{x \in L_{\mathbb{R}} : |Q(x) - 1| < \epsilon\}$. Then

$$\begin{aligned} &\lim_{\epsilon \rightarrow 0} \frac{1}{2\epsilon} \int_{L_\epsilon} \left(\frac{1}{1-Q(\lambda_x)}\right)^{k-1+s} d\mu_\infty(\lambda) \\ &= \lim_{\epsilon \rightarrow 0} \frac{2^{\frac{b}{2}}}{\epsilon\sqrt{|L^\vee/L|}} \int_{(x_1, x_2) \in \mathbb{R}^2} \int_{\substack{(y_1, \dots, y_b) \in \mathbb{R}^b \\ |y_1^2 + \dots + y_b^2 - x_1^2 - x_2^2 - 1| < \epsilon}} \frac{dx_1 dx_2 dy_1 \cdots dy_b}{(1+x_1^2+x_2^2)^{k-1+s}} \\ &= \frac{2(2\pi)^{1+\frac{b}{2}}}{\Gamma(\frac{b}{2}) \cdot \sqrt{|L^\vee/L|}} \int_0^{+\infty} \left(\frac{1}{1+r^2}\right)^{s+1} r dr \\ &= \frac{(2\pi)^{1+\frac{b}{2}}}{\Gamma(\frac{b}{2}) \cdot \sqrt{|L^\vee/L|}} \frac{1}{s}. \end{aligned}$$

The lemma now follows from the definition of $a(m)$. □

²⁴The definitions of singular series are the same in [HB96] and [Nie10]. For the definitions of singular integral, it suffices to compare the definitions when ω is a smooth weight function (say, a good approximation of $\mathbf{1}_{U_T}$, where $U_T \subset L_{\mathbb{R}} \cong \mathbb{R}^{b+2}$ with $U_T \cap L_{\mathbb{R},1} = \Omega_{\leq T}$). In [Nie10], the singular integral, denoted by $I_\omega(m)$, is defined to be $\int_{-\infty}^{\infty} \int_{\mathbb{R}^{b+2}} \omega(\mathbf{x}/\sqrt{m}) \exp(2\pi i z(Q(\mathbf{x}) - m)) dx dz$, which is equal to $\int_{Q(\mathbf{x})=m} \omega(\mathbf{x}/\sqrt{m}) (\frac{dQ}{dx_1})^{-1} dx_2 \cdots dx_{b+2}$ by applying the Fourier inversion theorem to $f : \mathbb{R} \rightarrow \mathbb{C}$, $f(y) := \int_{Q(\mathbf{x})=y} \omega(\mathbf{x}/\sqrt{m}) (\frac{dQ}{dx_1})^{-1} dx_2 \cdots dx_{b+2}$. Then by [HB96, Theorem 3] and by a change of variables $\mathbf{x} \mapsto \mathbf{x}/\sqrt{m}$, $I_\omega(m) = m^{\frac{b}{2}} \mu_\infty(Q, \omega)$. Therefore, the leading term in [Nie10] $I_\omega(m)\mu(Q, m)$ coincides with the leading term $\mu_\infty(Q, \omega)\mu(Q, m)m^{\frac{b}{2}}$ in [HB96].

5. First step in the archimedean estimate and uniform diophantine bounds

We keep the notations from Section 2 and Section 3. Namely, (L, Q) is an even maximal lattice of signature $(b, 2)$ with $b \geq 3$. Recall that \mathcal{M} is the integral model over \mathbb{Z} of the associated GSpin Shimura variety M and $\widehat{\mathcal{Z}}(m) := (\mathcal{Z}(m), \Phi_m)$ are the arithmetic special divisor on \mathcal{M} for $m \in \mathbb{Z}_{>0}$. Throughout this section and the rest of the paper, we assume that the equation $Q(v) = m$ has a solution in L – that is, $\mathcal{Z}(m) \neq \emptyset$. As in Theorem 2.4, $\mathcal{Y} \in \mathcal{M}(\mathcal{O}_K)$ such that \mathcal{Y}_K is Hodge-generic and $\mathcal{Y}^\sigma \in M(\mathbb{C})$ via $\sigma : K \hookrightarrow \mathbb{C}$.

The main goal of this section is to give a first estimate of the archimedean term in the height formula given by equation (3.1); more precisely, we show that for a fixed σ and for every m ,

$$\Phi_m(\mathcal{Y}^\sigma) \asymp -m^{\frac{b}{2}} \log m + A(m, \mathcal{Y}^\sigma) + o(m^{\frac{b}{2}} \log m), \tag{5.1}$$

where $A(m, \mathcal{Y}^\sigma)$ is a non-negative real number (see equation (5.7) and Theorem 5.7 for the precise statement).

An important consequence (Theorem 5.8) of this estimate is the following uniform diophantine bounds. For a fixed finite place \mathfrak{P} and a fixed σ , we have

$$(\mathcal{Y} \cdot \mathcal{Z}(m))_{\mathfrak{P}} = O(m^{\frac{b}{2}} \log m), \quad \Phi_m(\mathcal{Y}^\sigma) = O(m^{\frac{b}{2}} \log m). \tag{5.2}$$

This consequence is one of the key inputs for the estimates in Sections 6–7.

Throughout this section, x will denote a \mathbb{C} -point of M , which is not contained in any special divisor. This section is organised as follows. First, in Section 5.1, we follow Bruinier [Bru02] and Bruinier–Kühn [BK03] to express $\Phi_m(x)$ as a sum of two terms

$$\Phi_m(x) = \phi_m(x) - b'm(k/2),$$

where $\phi_m(x)$ and the function $b_m(s)$ are defined in equations (5.3), (5.4) and (5.5). Then, in Section 5.2, we use results from [BK03] to prove that $b'm(k/2) \asymp m^{\frac{b}{2}} \log m$. Next, in Section 5.3, we prove that $\phi_m(x) = A(m, x) + O(m^{\frac{b}{2}})$, where $A(m, x)$, as above, is non-negative. In Section 5.4, we put together the results of Sections 5.1–5.3 to deduce equations (5.1) and (5.2).

5.1. Bruinier’s explicit formula for the Green function Φ_m

There is another expression for the Green function Φ_m introduced in Section 3.1 due to Bruinier (see [Bru02, §2] and [BK03, §4]); this expression will allow us to make explicit computations later. As in Section 3.3, let $k = 1 + \frac{b}{2}$, and $s \in \mathbb{C}$ with $\text{Re}(s) > \frac{k}{2}$. We pick a lift of $x \in M(\mathbb{C})$ to the period domain D_L and still use x to denote the lift. Recall from Section 2.1 that x defines a negative definite plane²⁵ P_x of $L_{\mathbb{R}}$ and for $\lambda \in L_{\mathbb{R}}$, we denote by λ_x the orthogonal projection of λ on P_x . Let

$$F(s, z) = H\left(s - 1 + \frac{k}{2}, s + 1 - \frac{k}{2}, 2s; z\right), \text{ where } H(a, b, c; z) = \sum_{n \geq 0} \frac{(a)_n (b)_n}{(c)_n} \frac{z^n}{n!}$$

is the Gauss hypergeometric function as in [AS64, Chapter 15] and $(a)_n = \frac{\Gamma(a+n)}{\Gamma(a)}$ for $a, b, c, z \in \mathbb{C}$ and $|z| < 1$. Finally, let²⁶

$$\phi_m(x, s) = 2 \frac{\Gamma(s - 1 + \frac{k}{2})}{\Gamma(2s)} \sum_{Q(\lambda) = m, \lambda \in L} \left(\frac{m}{m - Q(\lambda_x)}\right)^{s-1+\frac{k}{2}} F\left(s, \frac{m}{m - Q(\lambda_x)}\right). \tag{5.3}$$

²⁵Using the notation in Section 2.1, for a point $[z] \in D_L$ with $z = u + iw$, $u, w \in L_{\mathbb{R}}$, we have a negative definite plane given by $\text{span}_{\mathbb{R}}\{u, w\}$.

²⁶In [Bru02, Section 2.2, (2.15)], $\phi_m(x, s)$ is defined as a regularised theta lift of $F_{0,m}$; here the regularisation process is slightly different from Borchers’ version.

By [Bru02, Proposition 2.8, Theorem 2.14], the function $\phi_m(x, s)$ admits a meromorphic continuation to $\text{Re}(s) > 1$ with a simple pole at $s = \frac{k}{2}$ with residue $-c(m)$, where $c(m)$ is the Fourier coefficient defined in Section 3.3; see also [BK03, Proposition 4.3] for the value of the residue.

We regularise $\phi_m(x, s)$ at $s = k/2$ by defining $\phi_m(x)$ to be the constant term at $s = \frac{k}{2}$ of the Laurent expansion of $\phi_m(x, s)$. As in [BK03, Prop.4.2], for $x \in D_L$, we have

$$\phi_m(x) = \lim_{s \rightarrow \frac{k}{2}} \left(\phi_m(x, s) + \frac{c(m)}{s - \frac{k}{2}} \right). \tag{5.4}$$

To compare $\phi_m(x)$ with $\Phi_m(x)$, we recall that $C(n, s), n \in \mathbb{Z}, s \in \mathbb{C}, \text{Re}(s) > 1 - \frac{k}{2}$ is part of the Fourier coefficient of $E_0(\tau, s)$ defined in Section 3.3. For $s \in \mathbb{C}$ with $\text{Re}(s) > 1$, define²⁷

$$b_m(s) = -\frac{C\left(m, s - \frac{k}{2}\right) \cdot \left(s - 1 + \frac{k}{2}\right)}{(2s - 1) \cdot \Gamma\left(s + 1 - \frac{k}{2}\right)}. \tag{5.5}$$

By [Bru02, Theorem 1.9], $b_m(s)$ is a holomorphic function of s in the region $\text{Re}(s) > 1$.

Proposition 5.1 [Bru02, Proposition 2.11]. *For $x \in D_L$, we have*

$$\Phi_m(x) = \phi_m(x) - b'm(k/2).$$

This proposition shows in particular that ϕ_m is also a Green function for the arithmetic cycle $\mathcal{Z}(m)$.

5.2. Estimating $b'm(k/2)$

The main result of this subsection is the following.

Proposition 5.2. *Let $m \in \mathbb{Z}_{>0}$ such that $\mathcal{Z}(m) \neq \emptyset$; and if b is odd, we further assume that for a fixed $D, \sqrt{m/D} \in \mathbb{Z}$, as in Theorem 2.4. Then as $m \rightarrow +\infty$, we have*

$$b'm(k/2) = |c(m)| \log m + o(c(m) \log m).$$

In particular, $b'm(k/2) \asymp m^{\frac{b}{2}} \log m$.

Lemma 5.3 below reduces the proposition into computations of certain local invariants of the lattice L at primes p .

In order to state the lemma, we recall some notations from [BK03] and Section 4.1. Recall that $r = b + 2$, and let D be the fixed integer in Theorem 2.4; let d be

$$\begin{aligned} &(-1)^{\frac{r}{2}} \det(L), \text{ if } r \text{ is even;} \\ &2(-1)^{\frac{r+1}{2}} D \det(L), \text{ otherwise,} \end{aligned}$$

where $\det(L)$ denote the Gram determinant of L . Let d_0 denote the fundamental discriminant of number field $\mathbb{Q}(\sqrt{d})$, and let χ_{d_0} be the quadratic character associated to d_0 . The polynomial $L_m^{(p)}(t)$ is defined by

$$L_m^{(p)}(t) = N_m(p^{w_p})t^{w_p} + (1 - p^{r-1}t) \sum_{n=0}^{w_p-1} N_m(p^n)t^n \in \mathbb{Z}[t],$$

²⁷In the notation of [BK03], it is $b(0, 0, s)$ in equation (4.12) [BK03]. The comparison with the formula given above is given in [BK03, (4.20)]. In [Bru02, Theorem 1.9], $b(s)$ is defined as the coefficient of $\gamma = 0, n = 0$ in the Fourier expansion of $F_{0,m}(\cdot, s)$.

where, as in Section 4.1, $N_m(p^n) = \#\{v \in L/p^n L; Q(v) \equiv m \pmod{p^n}\}$ and $w_p := w_p(m) = 1 + \text{val}_p(m)$ for $p \neq 2$ and $w_2 := w_2(m) = 1 + 2 \text{val}_2(2m)$.²⁸

Lemma 5.3 (Bruinier–Kühn). *Let $D \in \mathbb{Z}_{>0}$ be the fixed integer in Theorem 2.4 for all $m \in \mathbb{Z}_{>0}$ such that $\sqrt{m/D} \in \mathbb{Z}$ (and representable by (L, Q)); we have*

$$\frac{b'm\left(\frac{k}{2}\right)}{b_m\left(\frac{k}{2}\right)} = \log(m) + 2\frac{\sigma'_m(k)}{\sigma_m(k)} + O(1),$$

where for $s \in \mathbb{C}$, $\text{Re}(s) > 0$, the function σ_m is given by

$$\sigma_m(s) = \begin{cases} \prod_{p|2m \det(L)} \frac{L_m^{(p)}(p^{1-\frac{r}{2}-s})}{1-\chi_{d_0}(p)p^{-s}}, & \text{if } r \text{ is even,} \\ \prod_{p|2m \det(L)} \frac{1-\chi_{d_0}(p)p^{\frac{1}{2}-s}}{1-p^{1-2s}} L_m^{(p)}(p^{1-\frac{r}{2}-s}), & \text{if } r \text{ is odd.} \end{cases} \tag{5.6}$$

Proof. Taking logarithmic derivatives in equation (5.5) at $s = \frac{k}{2}$ yields

$$\frac{b'm\left(\frac{k}{2}\right)}{b_m\left(\frac{k}{2}\right)} = \frac{C'(m, 0)}{C(m, 0)} - \frac{2}{b} - \Gamma'(1)$$

Then we conclude by [BK03, Theorem 4.11, (4.73), (4.74)], since both d_0 and k are independent of m . (Our definition of d above differs from the definition in [BK03] by m/D , which is a square and hence yields the same d_0 .) □

Proof of Proposition 5.2. By definition, $b_m(k/2) = -c(m) = |c(m)|$. Therefore, by Lemma 5.3, it is enough to show that

$$\frac{\sigma'_m(k)}{\sigma_m(k)} = o(\log(m)).$$

Taking the logarithmic derivative in equation (5.6) at $s = k$, we get for r even

$$\frac{\sigma'_m(k)}{\sigma_m(k)} = - \sum_{p|2m \det(L)} \left(\frac{p^{1-r} L_m^{(p)'}(p^{1-r})}{L_m^{(p)}(p^{1-r})} + \frac{\chi_{d_0}(p)}{p^k - \chi_{d_0}(p)} \right) \log(p),$$

and for r odd

$$\frac{\sigma'_m(k)}{\sigma_m(k)} = - \sum_{p|2m \det(L)} \left(\frac{p^{1-r} L_m^{(p)'}(p^{1-r})}{L_m^{(p)}(p^{1-r})} - \frac{\chi_{d_0}(p)}{p^{k-\frac{1}{2}} - \chi_{d_0}(p)} + \frac{2}{p^{2k-1} - 1} \right) \log(p).$$

Since $k = 1 + \frac{b}{2} \geq \frac{5}{2}$, we have

$$\left| \sum_{p|2m \det(L)} \frac{\chi_{d_0}(p) \log(p)}{p^k - \chi_{d_0}(p)} \right| \leq \sum_p \frac{\log(p)}{p^{5/2} - 1} < +\infty,$$

²⁸In [BK03, (3.18), (3.20)], w_p is defined to be $1 + 2 \text{val}_p(2m)$ for every prime p . Our definition of w_p for odd prime p and the definition in [BK03] give the same definition of $L_m^{(p)}(\tau)$ by the fact that $N_m(p^{n+1}) = p^{r-1} N_m(p^n)$ for all $n \geq 1 + \text{val}_p(m)$ (Corollary 4.3(1)) and a direct computation (see, for instance, [BK01, (21), (22)]).

$$\left| \sum_{p|2m \det(L)} \frac{\chi_{d_0}(p) \log(p)}{p^{k-\frac{1}{2}} - \chi_{d_0}(p)} \right| \leq \sum_p \frac{\log(p)}{p^2 - 1} < +\infty,$$

$$\left| \sum_{p|2m \det(L)} \frac{2 \log p}{p^{2k-1} - 1} \right| \leq \sum_p \frac{2 \log(p)}{p^4 - 1} < +\infty.$$

Hence it remains to treat the $L_m^{(p)}$ term. We have $L_m^{(p)}(p^{1-r}) = N_m(p^{w_p})p^{(1-r)w_p}$ and

$$L_m^{(p)'}(p^{1-r}) = w_p N_m(p^{w_p})p^{(1-r)(w_p-1)} - \sum_{n=0}^{w_p-1} N_m(p^n)p^{(n-1)(1-r)}.$$

Hence

$$\left| \frac{p^{1-r} L_m^{(p)'}(p^{1-r})}{L_m^{(p)}(p^{1-r})} \right| = \left| w_p - \sum_{n=0}^{w_p-1} \frac{N_m(p^n)}{N_m(p^{w_p})} p^{(n-w_p)(1-r)} \right| = \left| w_p - \sum_{n=0}^{w_p-1} \frac{\mu_p(m, n)}{\mu_p(m, w_p)} \right| \leq \frac{C}{p},$$

where $\mu_p(m, n) = p^{-n(r-1)} N_m(p^n)$ as in Section 4.1, and the last inequality follows from Proposition 4.1 with constant C only depending on (L, Q) (i.e., is independent of m, p). Thus we have

$$\left| \sum_{p|2m \det(L)} \frac{p^{1-r} L_m^{(p)'}(p^{1-r})}{L_m^{(p)}(p^{1-r})} \right| \leq C \sum_{p|2m \det(L)} \frac{\log(p)}{p} = O(\log \log(m)).$$

Here we use the fact that for $N \geq 2$, $\sum_{p|N} \frac{\log(p)}{p} = O(\log \log(N))$. Indeed, let $X = \log(N)$, and use Mertens' first theorem to write

$$\begin{aligned} \sum_{p|N} \frac{\log(p)}{p} &= \sum_{p|N, p < X} \frac{\log(p)}{p} + \sum_{p|N, p \geq X} \frac{\log(p)}{p} \leq \log(X) + \frac{1}{X} \sum_{p|N} \log(p) + O(1) \\ &\leq \log(X) + \frac{\log(N)}{X} + O(1) \leq \log(\log(N)) + O(1). \end{aligned}$$

This concludes the proof of the proposition. □

5.3. Estimates on $\phi_m(x)$

Recall that $x \in M(\mathbb{C})$ is a Hodge-generic point, and we pick a lift of x to D_L . We will associate the quantity $A(m, x)$ to x , which is independent of the choice of the lift. Thus, we will also denote this lift by x . Recall from Section 5.1 that for $\lambda \in L_{\mathbb{R}}$, we use λ_x to denote the orthogonal projection of λ onto the negative definite plane in $L_{\mathbb{R}}$ associated to x . Define

$$A(m, x) := -2 \sum_{\substack{\sqrt{m}\lambda \in L \\ |Q(\lambda_x)| \leq 1, Q(\lambda) = 1}} \log(|Q(\lambda_x)|). \tag{5.7}$$

Note that since x is Hodge-generic, for any $\lambda \in L$, $\lambda_x \neq 0$. Hence for any $\lambda \in L_{\mathbb{R}}$ such that $\mathbb{R}\lambda \cap L \neq \{0\}$, we also have $\lambda_x \neq 0$. On the other hand, the conditions $|Q(\lambda_x)| \leq 1, Q(\lambda) = 1$ cut out a compact region in $L_{\mathbb{R}}$, and hence for a fixed m , $A(m, x)$ is the sum of finitely many terms. Therefore $A(m, x)$ is well-defined and non-negative.

The main purpose of this subsection is to prove the following result.

Proposition 5.4. *For $m \in \mathbb{Z}_{>0}$, we have*

$$\phi_m(x) = A(m, x) + O(m^{\frac{b}{2}}).$$

Recall that $F(s, t)$ from Section 5.1. Since $F(s, 0) = 1$, for $z \in \mathbb{C}$ with $|z| < 1$, we may write $F(s, z) = zG(s, z) + 1$. Recall that we set $k = 1 + \frac{b}{2}$. From the definitions, we obtain the following decomposition of $\phi_m(x)$:

$$\begin{aligned} \phi_m(x) &\stackrel{(5.4)}{=} \lim_{s \rightarrow \frac{k}{2}} \left(\phi_m(x, s) + \frac{c(m)}{s - \frac{k}{2}} \right) \\ &\stackrel{(5.3)}{=} \lim_{\substack{s \rightarrow 0 \\ \text{Re } s > 0}} \left(\frac{c(m)}{s} + \frac{4}{b} \sum_{\substack{\lambda \in L \\ Q(\lambda) = m}} \left(\frac{m}{m - Q(\lambda_x)} \right)^{k-1+s} F\left(\frac{k}{2} + s, \frac{m}{m - Q(\lambda_x)}\right) \right) \\ &= \tilde{\phi}_m(x, 0) + \lim_{\substack{s \rightarrow 0 \\ \text{Re } s > 0}} R_x(s, m), \end{aligned} \tag{5.8}$$

where for $s \in \mathbb{C}$ with $\text{Re } s > 0$, we define

$$\begin{aligned} \tilde{\phi}_m(x, s) &= \frac{4}{b} \sum_{\substack{\sqrt{m}\lambda \in L \\ Q(\lambda) = 1}} \left(\frac{1}{1 - Q(\lambda_x)} \right)^{k+s} G\left(\frac{k}{2} + s, \frac{1}{1 - Q(\lambda_x)}\right), \\ R_x(s, m) &= \frac{c(m)}{s} + \frac{4}{b} \sum_{\substack{\sqrt{m}\lambda \in L \\ Q(\lambda) = 1}} \left(\frac{1}{1 - Q(\lambda_x)} \right)^{k-1+s}; \end{aligned}$$

in Section 5.3.2, we will prove that the above series defining $\tilde{\phi}_m(x, s)$ indeed converges uniformly absolutely in a small compact neighbourhood of $s = 0$ in \mathbb{C} , and hence it defines a function holomorphic at 0, and we still denote this function by $\tilde{\phi}_m(x, s)$. In particular, $\tilde{\phi}_m(x, 0)$ is well defined and equal to $\lim_{\text{Re } s > 0, s \rightarrow 0} \tilde{\phi}_m(x, s)$. Therefore, the last equality in equation (5.8) is valid; moreover, since $\phi_m(x, s + \frac{k}{2}) + \frac{c(m)}{s}$ admits a holomorphic continuation to $s = 0$ (see Section 5.1), then $R_x(s, m)$ admits a holomorphic continuation to $s = 0$. We use $R_x(0, m)$ to denote $\lim_{\text{Re } s > 0, s \rightarrow 0} R_x(s, m) = \lim_{s \in \mathbb{R}_{>0}, s \rightarrow 0} R_x(s, m)$ and rewrite equation (5.8) as

$$\phi_m(x) = \tilde{\phi}_m(x, 0) + R_x(0, m). \tag{5.9}$$

Note that the second equality in equation (5.8) also uses the fact that the ratio of Γ -functions in equation (5.3) is holomorphic and has a limit of $2/b$.

In what follows next, we estimate $R_x(0, m)$ and $\tilde{\phi}_m(x, 0)$ using results from Section 4.3, where we use the work of Heath-Brown and Niedermowwe to estimate the number of the lattice points λ in certain regions in L with $Q(\lambda) = m$.

5.3.1. Bounding $R_x(0, m)$

We only consider $s \in \mathbb{R}_{\geq 0}$. Recall from Section 4.3 that for $\lambda \in L_{\mathbb{R},1} = \{\lambda \in L_{\mathbb{R}} : Q(\lambda) = 1\}$, we set $h_s(\lambda) = \left(\frac{1}{1 - Q(\lambda_x)} \right)^{k-1+s}$; $a(m) = \frac{-c(m)\Gamma(k)\sqrt{|L^\vee/L|}}{2(2\pi)^k} > 0$, and μ_∞ denotes the measure on $L_{\mathbb{R},1}$ defined in equation (4.5).

For $s > 0$, Lemma 4.14 yields the equality

$$R_x(s, m) = \frac{4}{b} \sum_{\substack{\sqrt{m}\lambda \in L \\ Q(\lambda)=1}} h_s(\lambda) - \frac{4a(m)}{b} \int_{L_{\mathbb{R},1}} h_s(\lambda) d\mu_\infty(\lambda).$$

Our next result provides the required bound on $R_x(0, m)$.

Proposition 5.5. *For a given $x \in D_L$ Hodge-generic, we have*

$$R_x(0, m) = \lim_{s \in \mathbb{R}_{>0}, s \rightarrow 0} R_x(s, m) = O(m^{\frac{b}{2}}).$$

Proof. Fix $\epsilon > 0$, and we only consider $s \in [0, \epsilon]$. As in Section 4.3, $\Omega_T = \{\lambda \in L_{\mathbb{R},1} : -Q(\lambda_x) \in [0, T]\}$. For an integer $N \geq 0$, define the set $\Theta_N := \Omega_{N+1} \setminus \Omega_N$, and note that for $\lambda \in \Theta_N$, we have

$$h_s(\lambda) = \frac{1}{(N+1)^{s+k-1}} + O\left(\frac{1}{(N+1)^{s+k}}\right).$$

To obtain a uniformly absolutely convergent expression for $R_x(s, m)$ for $s \in]0, \epsilon]$, we write

$$\frac{b}{4} R_x(s, m) = \sum_{N=0}^{\infty} \left(\sum_{\substack{\lambda \in \Theta_N \\ \sqrt{m}\lambda \in L}} h_s(\lambda) - a(m) \int_{\Theta(N)} h_s(\lambda) d\mu_\infty(\lambda) \right).$$

We use the above estimate of $h_s(\lambda)$ for $\lambda \in \Theta_N$ and bound the associated error term using Proposition 4.13 and Lemma 4.11. More precisely, let $C > 0$ be an absolute constant such that for all $\lambda \in \Theta_N$, for all $s \in [0, \epsilon]$, we have $|h_s(\lambda) - (N+1)^{-(s+k-1)}| < C(N+1)^{-(s+k)}$. Then the error term is bounded by

$$\begin{aligned} & C \sum_{N=0}^{\infty} (N+1)^{-(s+k)} \left(\sum_{\substack{\lambda \in \Theta_N \\ \sqrt{m}\lambda \in L}} 1 + a(m) \mu_\infty(\Theta_N) \right) \\ &= C \sum_{N=1}^{\infty} (N^{-(s+k)} - (N+1)^{-(s+k)}) \left(\sum_{\substack{\lambda \in \Omega_N \\ \sqrt{m}\lambda \in L}} 1 + a(m) \mu_\infty(\Omega_N) \right) \tag{5.10} \\ &\ll a(m) \sum_{N=1}^{\infty} N^{-(s+k+1)} \cdot N^{\frac{b}{2}} = a(m) \sum_{N=1}^{\infty} N^{-s-2} \ll a(m) = O(m^{\frac{b}{2}}), \end{aligned}$$

where the first equality is a partial summation and the implicit constants above are absolute.

To bound the main term, we pick some $A > 1$ in Proposition 4.13. By partial summation, we write

$$\begin{aligned} & \sum_{N=0}^{\infty} \frac{1}{(N+1)^{s+k-1}} \left(\sum_{\substack{\lambda \in \Theta_N \\ \sqrt{m}\lambda \in L}} 1 - a(m) \mu_\infty(\Theta_N) \right) \\ &= \sum_{N=1}^{\infty} \left(\frac{1}{N^{s+k-1}} - \frac{1}{(N+1)^{s+k-1}} \right) \left(\sum_{\substack{\lambda \in \Omega_N \\ \sqrt{m}\lambda \in L}} 1 - a(m) \mu_\infty(\Omega_N) \right) \\ &\ll \sum_{N=1}^{\infty} N^{-(s+k)} \cdot N^{\frac{b}{2}} m^{\frac{b}{2}} (\log mN)^{-A} \leq m^{\frac{b}{2}} \sum_{N=1}^{\infty} N^{-1} (\log N)^{-A} \ll m^{\frac{b}{2}}, \end{aligned}$$

which is again sufficient. The proposition follows. □

5.3.2. Estimating $\tilde{\phi}_m(x, 0)$

We fix an $\epsilon \in]0, 1/2]$ and consider $s \in \mathbb{C}$ such that $|s| \leq \epsilon$. Since

$$G\left(s + \frac{k}{2}, z\right) = \sum_{n=1}^{\infty} \frac{\Gamma(s + k - 1 + n)\Gamma(s + 1 + n)\Gamma(2s + k)}{\Gamma(s + k - 1)\Gamma(s + 1)\Gamma(2s + k + n)} \frac{z^{n-1}}{n!}$$

converges uniformly absolutely for $|s| \leq \epsilon, |z| \leq 1/2$, then $G\left(s + \frac{k}{2}, z\right)$ is absolutely bounded for such s and z .

To show that $\tilde{\phi}_m(x, s)$ is holomorphic in $|s| < \epsilon$, we write

$$\begin{aligned} \frac{b}{4} \tilde{\phi}_m(x, s) &= \sum_{\substack{\sqrt{m}\lambda \in L \\ Q(\lambda)=1 \\ |Q(\lambda_x)| > 1}} \left(\frac{1}{1 - Q(\lambda_x)}\right)^{k+s} G\left(\frac{k}{2} + s, \frac{1}{1 - Q(\lambda_x)}\right) \\ &+ \sum_{\substack{\sqrt{m}\lambda \in L \\ Q(\lambda)=1 \\ |Q(\lambda_x)| \leq 1}} \left(\frac{1}{1 - Q(\lambda_x)}\right)^{k+s} G\left(\frac{k}{2} + s, \frac{1}{1 - Q(\lambda_x)}\right), \end{aligned}$$

where, similar to the definition of $A(m, x)$ in equation (5.7), the second term is a finite sum of holomorphic functions. Thus we only need to show that the first term converges absolutely uniformly on $|s| \leq \epsilon$. The uniform absolute convergence follows from the boundedness of $G(s + k/2, z)$ in conjunction with an argument identical to equation (5.10), which indeed implies that

$$\sum_{\substack{\sqrt{m}\lambda \in L \\ Q(\lambda)=1 \\ |Q(\lambda_x)| > 1}} \left(\frac{1}{1 - Q(\lambda_x)}\right)^{k+s} G\left(\frac{k}{2} + s, \frac{1}{1 - Q(\lambda_x)}\right) = O(m^{\frac{b}{2}}).$$

Therefore,

$$\tilde{\phi}_m(x, 0) = \frac{4}{b} \sum_{\substack{\sqrt{m}\lambda \in L \\ Q(\lambda)=1 \\ |Q(\lambda_x)| \leq 1}} \left(\frac{1}{1 - Q(\lambda_x)}\right)^k G\left(\frac{k}{2}, \frac{1}{1 - Q(\lambda_x)}\right) + O(m^{\frac{b}{2}}).$$

Obtaining an estimate on the terms with $|Q(\lambda_x)| \leq 1$ is significantly more difficult since the function

$$\lambda \mapsto \left(\frac{1}{1 - Q(\lambda_x)}\right)^k G\left(\frac{k}{2}, \frac{1}{1 - Q(\lambda_x)}\right)$$

has a logarithmic singularity along $\{\lambda \in L_{\mathbb{R},1}, x \in \lambda^\perp\}$. Since $G(k/2, z) = \sum_{n=1}^{\infty} \frac{k-1}{n+k-1} z^{n-1}$, it follows that there exists an absolute constant $C > 0$ such that for $z \in [1/2, 1[$,

$$\left| z^k G\left(\frac{k}{2}, z\right) + \frac{b}{2} \log(1 - z) \right| \leq C.$$

Hence, noting that $\sum_{\substack{|Q(\lambda_x)| \leq 1 \\ \sqrt{m}\lambda \in L}} 1 = O(m^{\frac{b}{2}})$, which follows from either Corollary 4.12 or Proposition 4.13, we have

$$\begin{aligned} \frac{4}{b} \sum_{\substack{\sqrt{m}\lambda \in L \\ Q(\lambda)=1 \\ |Q(\lambda_x)| \leq 1}} \left(\frac{1}{1-Q(\lambda_x)}\right)^k G\left(\frac{k}{2}, \frac{1}{1-Q(\lambda_x)}\right) &= -2 \sum_{\substack{\sqrt{m}\lambda \in L \\ Q(\lambda)=1 \\ |Q(\lambda_x)| \leq 1}} \log\left(\frac{-Q(\lambda_x)}{1-Q(\lambda_x)}\right) + O(m^{\frac{b}{2}}) \\ &= -2 \sum_{\substack{\sqrt{m}\lambda \in L \\ Q(\lambda)=1 \\ |Q(\lambda_x)| \leq 1}} \log(|Q(\lambda_x)|) + O(m^{\frac{b}{2}}). \end{aligned}$$

Therefore, we have proved the following proposition.

Proposition 5.6. *We have*

$$\tilde{\phi}_m(x, 0) = A(m, x) + O(m^{\frac{b}{2}}).$$

Proposition 5.4 follows immediately from equation (5.9) and Propositions 5.5 and 5.6.

5.4. Conclusions

The following theorems summarise the results proved in the previous subsections. First, we remind the reader that $|c(m)| \asymp m^{b/2}$.

Theorem 5.7. *For every m representable by (L, Q) , we have*

$$\Phi_m(\mathcal{Y}^\sigma) = c(m) \log m + A(m, \mathcal{Y}^\sigma) + o(|c(m)| \log m).$$

Proof. Combine Propositions 5.1, 5.2 and 5.4. □

Theorem 5.8. *For every positive integer m , we have the following bounds:*

- (i) $0 \leq A(m, \mathcal{Y}^\sigma) \ll m^{\frac{b}{2}} \log m$.
- (ii) $(\mathcal{Y} \cdot \mathcal{Z}(m))_{\mathfrak{P}} \log |\mathcal{O}_K/\mathfrak{P}| \ll m^{\frac{b}{2}} \log m$.
- (iii) $\sum_{\sigma: K \hookrightarrow \mathbb{C}} \frac{\Phi_m(\mathcal{Y}^\sigma)}{|\text{Aut}(\mathcal{Y}^\sigma)|} = O(m^{\frac{b}{2}} \log m)$.

Proof. Recall that $\Phi_m(\mathcal{Y}^\sigma) = \phi_m(\mathcal{Y}^\sigma) - b'_m(k/2)$. For every integer $m > 0$, equation (3.1), Proposition 3.2 and Proposition 5.2 yield

$$\sum_{\mathfrak{P}} (\mathcal{Y} \cdot \mathcal{Z}(m))_{\mathfrak{P}} \log |\mathcal{O}_K/\mathfrak{P}| + \sum_{\sigma: K \hookrightarrow \mathbb{C}} \phi_m(\mathcal{Y}^\sigma) \asymp m^{\frac{b}{2}} \log m.$$

By Proposition 5.4, we have $\phi_m(\mathcal{Y}^\sigma) = A(m, \mathcal{Y}^\sigma) + O(m^{\frac{b}{2}})$, where $A(m, \mathcal{Y}^\sigma)$ is a sum of positive quantities and is therefore non-negative. Further, note that $(\mathcal{Y} \cdot \mathcal{Z}(m))_{\mathfrak{P}} \log |\mathcal{O}_K/\mathfrak{P}|$ is also non-negative for every prime \mathfrak{P} . Therefore, it follows that $A(m, \mathcal{Y}^\sigma) \ll m^{\frac{b}{2}} \log m$, $(\mathcal{Y} \cdot \mathcal{Z}(m))_{\mathfrak{P}} \log |\mathcal{O}_K/\mathfrak{P}| \ll m^{\frac{b}{2}} \log m$ and *a fortiori* that $\Phi_m(\mathcal{Y}^\sigma) = O(m^{\frac{b}{2}} \log m)$. □

6. Second step in bounding the archimedean contribution

We keep the notations from Section 5.3. Namely (L, Q) is a quadratic lattice of signature $(b, 2)$. We are given a Hodge-generic point $x = \mathcal{Y}^\sigma$ in the Shimura variety $M(\mathbb{C})$ and choose a lift of x to the period domain D_L , which corresponds to a 2-dimensional negative definite (with respect to Q) plane $P \subset L_{\mathbb{R}}$. Let P^\perp denote the orthogonal complement of P in $L_{\mathbb{R}}$. Then P^\perp is a b -dimensional positive definite space. Given a vector $\lambda \in L_{\mathbb{R}}$, we let λ_x and λ_{x^\perp} denote the projections of λ to P and P^\perp , respectively. For $m \in \mathbb{Z}_{>0}$, recall that we defined the quantity $A(m, x)$ in equation (5.7) by

$$A(m, x) = -2 \sum_{\substack{\sqrt{m}\lambda \in L \\ Q(\lambda)=1 \\ |Q(\lambda_x)| \leq 1}} \log(|Q(\lambda_x)|) = 2 \sum_{\substack{\lambda \in L \\ Q(\lambda)=m \\ |Q(\lambda_x)| \leq m}} \log\left(\frac{m}{|Q(\lambda_x)|}\right).$$

As x is fixed, we denote $A(m, x)$ simply by $A(m)$. Also, for a subset $S \subset \mathbb{Z}_{>0}$, the logarithmic asymptotic density of S is defined to be $\limsup_{X \rightarrow \infty} \frac{\log |S_X|}{\log X}$, where $S_X := \{a \in S \mid X \leq a < 2X\}$. The main result of this section is the following bound on $A(m)$ for positive integers m outside a set of zero logarithmic asymptotic density. Combined with Theorem 5.7, we obtain the estimate for the archimedean term $\Phi_m(\mathcal{Y}^\sigma) \asymp -m^{\frac{b}{2}} \log m$ for such m .

Theorem 6.1. *There exists a subset $S_{\text{bad}} \subset \mathbb{Z}_{>0}$ of logarithmic asymptotic density zero such that for every $m \notin S_{\text{bad}}$, we have*

$$A(m) = o(m^{\frac{b}{2}} \log(m)).$$

To prove Theorem 6.1, we write $A(m) = A_{\text{mt}}(m) + A_{\text{er}}(m)$, where we define the main term $A_{\text{mt}}(m)$ and the error term $A_{\text{er}}(m)$ to be

$$A_{\text{mt}}(m) = 2 \sum_{\substack{\lambda \in L \\ Q(\lambda)=m \\ 1 \leq |Q(\lambda_x)| \leq m}} \log\left(\frac{m}{|Q(\lambda_x)|}\right),$$

$$A_{\text{er}}(m) = 2 \sum_{\substack{\lambda \in L \\ Q(\lambda)=m \\ 0 < |Q(\lambda_x)| < 1}} \log\left(\frac{m}{|Q(\lambda_x)|}\right).$$

In Section 6.1 and Section 6.2, we obtain bounds for the two terms $A_{\text{mt}}(m)$ and $A_{\text{er}}(m)$, respectively. Theorem 6.1 follows directly from Propositions 6.2 and 6.4. Since we only consider the fixed quadratic form Q in this section, we will not specify the dependence of the implicit constants on Q when we apply the circle method results by Heath-Brown recalled in Sections 4.2–4.3.

6.1. Bounding the main term using the circle method

In this section, we prove the following proposition.

Proposition 6.2. *We have*

$$\lim_{m \rightarrow \infty} \frac{A_{\text{mt}}(m)}{m^{\frac{b}{2}} \log m} = 0.$$

Proof. Fix a real number $T > 1$, and let $m > T$ be a positive integer. We break $A_{\text{mt}}(m)$ into two terms $A_1(m)$ and $A_2(m)$, where $A_1(m)$ is the sum over those $\lambda \in L$ such that $|Q(\lambda_x)| \geq m/T$ and $A_2(m)$

is the sum over those $\lambda \in L$ such that $|Q(\lambda_x)| < m/T$. We start by bounding $A_1(m)$. First note that if $\lambda \in L$ with $Q(\lambda) = m$ and $m/T \leq |Q(\lambda_x)| \leq m$, then we have

$$\log\left(\frac{m}{|Q(\lambda_x)|}\right) \leq \log T.$$

Furthermore, by Corollary 4.12,

$$|\{\lambda \in L : Q(\lambda) = m, Q(\lambda_x) \leq m\}| \ll m^{\frac{b}{2}}.$$

Therefore, we obtain the bound

$$A_1(m) \ll m^{\frac{b}{2}} \log T. \tag{6.1}$$

Next we consider $A_2(m)$. Once again, we apply Corollary 4.12 to obtain the bound (take $\epsilon = 1/4$)

$$\left| \left\{ \lambda \in L, Q(\lambda) = m, |Q(\lambda_x)| < \frac{m}{T} \right\} \right| \ll \frac{m^{\frac{b}{2}}}{T} + O_T(m^{\frac{b+2}{4}}). \tag{6.2}$$

Equations (6.1) and (6.2) and the trivial bound $\log(m/|Q(\lambda_x)|) \leq \log m$ for $\lambda \in L$ with $1 \leq |Q(\lambda_x)| \leq m$ yield the following estimate on $A_{\text{mt}}(m) = A_1(m) + A_2(m)$:

$$A_{\text{mt}}(m) \ll m^{\frac{b}{2}} \log T + m^{\frac{b}{2}} (\log m) T^{-1} + O_T(m^{(b+2)/4} \log m).$$

Dividing by $m^{\frac{b}{2}} \log(m)$ and letting m tend to infinity, we see that

$$\limsup_{m \rightarrow \infty} \frac{A_{\text{mt}}(m)}{m^{\frac{b}{2}} \log m} \ll \frac{1}{T}.$$

Since this is true for every T , $\lim_{m \rightarrow \infty} \frac{A_{\text{mt}}(m)}{m^{\frac{b}{2}} \log m}$ exists and is equal to 0. □

6.2. Bounding the error term using the diophantine bound

We start with the following (entirely lattice theoretic) lemma.

Lemma 6.3. *Let $C > 2$ be a fixed constant, let $X > 1$ be a real number, and let $N \geq 2$ be a positive integer. Suppose S is a set of N vectors in $L_{\mathbb{R}}$ such that $C \leq Q(v) \ll X$ and $|Q(v_x)| < e^{-C}$ for all $v \in S$. Then there exist two distinct vectors v and v' in S such that their difference $w := v - v'$ satisfies the following two properties:*

1. $-\log(|Q(w_x)|) \gg \min(-\log(|Q(v_x)|), -\log(|Q(v'_x)|))$
2. $Q(w_{x^\perp}) \ll \frac{X}{N^{\frac{1}{b}}}$.

All implicit constants here are absolute; in particular, they are independent of C, X, N .

Proof. The first property is immediate and is satisfied for every pair v and v' . Indeed, we have $w_x = v_x - v'_x$; and using the triangle inequality, it follows that

$$|Q(w_x)|^{1/2} \leq 2 \max(|Q(v_x)|^{1/2}, |Q(v'_x)|^{1/2}) < 1,$$

since $C > 2$. Hence we obtain the first claim.

To obtain the second claim, we remark that if $v \neq v'$, then $v_{x^\perp} \neq v'_{x^\perp}$ since otherwise $|Q(v - v')| = |Q(v_x - v'_x)| \in]0, 1[$ and $v - v' \in L$. Thus, by considering the projections v_{x^\perp} for $v \in S$, we obtain N vectors in the b -dimensional real vector space P^\perp . Let $2T$ be the smallest distance between the vectors v_{x^\perp} for $v \in S$, where distance is taken with respect to the positive definite form Q on P^\perp . By the triangle inequality, we have the trivial bound $T = O(X^{1/2})$. Then the N balls of radii T around the points v_{x^\perp} are disjoint and all lie within the ball of radius $C_0\sqrt{X}$ around the origin, where C_0 is an absolute constant depending only on the absolute implicit constant in $Q(v) \ll X$. By comparing volumes, we obtain

$$NT^b \ll X^{\frac{b}{2}},$$

from which it follows that $T \ll X^{\frac{1}{2}}/N^{\frac{1}{b}}$. Therefore, there exist two points v and v' in S such that

$$Q(v_{x^\perp} - v'_{x^\perp}) \leq T^2 \ll \frac{X}{N^{\frac{2}{b}}},$$

concluding the proof of the lemma. □

The following result controls the error term in $A(m)$ for most m .

Proposition 6.4. *Let $S_{\text{bad}} \subset \mathbb{N}^\times$ be the set of integers m such that*

$$A_{\text{er}}(m) > m^{\frac{b}{2}}. \tag{6.3}$$

Then S_{bad} has logarithmic asymptotic density zero.

Proof. A crucial ingredient in the proof is the ‘uniform diophantine bound’ in Theorem 5.8 (i). Since $A(m)$ is a sum of the positive terms $\log\left(\frac{m}{|Q(\lambda_x)|}\right)$, each such term must also satisfy the same bound – that is, for all $\lambda \in L$ such that $Q(\lambda) = m$, $|Q(\lambda_x)| \leq m$, we have

$$\log\left(\frac{m}{|Q(\lambda_x)|}\right) \ll m^{\frac{b}{2}} \log m.$$

Let $\epsilon \in]0, 1[$ and $X > 1$, and let $S_{\text{bad},X} =]X, 2X] \cap S_{\text{bad}}$. We pick a fixed constant $C \in [2, 4]$ and break the interval $]C, X^{\frac{b}{2}}]$ into the disjoint union of dyadic intervals $\cup_{i \in I}]Z_i, 2Z_i]$ such that $|I| = O(\log(X))$. Define the three following subsets of $]X, 2X]$.

1. The set $B_{1,X}$ of m such that

$$|\{\lambda \in L, Q(\lambda) = m, |Q(\lambda_x)| < 1\}| \geq X^{\frac{b}{2}-\epsilon}.$$

2. The set $B_{2,X}$ of m such that there exists at least one element $\lambda \in L$ with $Q(\lambda) = m$ and $-\log(|Q(\lambda_x)|) \geq X^{\frac{b}{2}}$.
3. The set $B_{3,X}$ of m for which there exists an index $i_m \in I$ such that

$$|\{\lambda \in L, Q(\lambda) = m, -\log(|Q(\lambda_x)|) \in]Z_{i_m}, 2Z_{i_m}]\}| \geq \frac{X^{\frac{b}{2}-\epsilon}}{Z_{i_m}}.$$

Notice that if $m \in]X, 2X] \setminus (B_{1,X} \cup B_{2,X} \cup B_{3,X})$, then we can write

$$\begin{aligned}
 A_{\text{er}}(m) &= 2 \sum_{\substack{\lambda \in L \\ Q(\lambda)=m \\ |Q(\lambda_x)| < 1}} \log m + 2 \sum_{\substack{\lambda \in L \\ Q(\lambda)=m \\ -\log(|Q(\lambda_x)|) \in [0, C]}} |\log(|Q(\lambda_x)|)| + 2 \sum_{\substack{\lambda \in L \\ Q(\lambda)=m \\ -\log(|Q(\lambda_x)|) \in]C, X^{\frac{b}{2}}]} |\log(|Q(\lambda_x)|)| \\
 &\leq 2X^{\frac{b}{2}-\epsilon} \cdot (\log(m) + C) + 2 \sum_i \sum_{\substack{\lambda \in L, Q(\lambda)=m \\ -\log(|Q(\lambda_x)|) \in]Z_i, 2Z_i]} (|\log(|Q(\lambda_x)|)|) \\
 &\leq 2X^{\frac{b}{2}-\epsilon} \log(2X) + 8X^{\frac{b}{2}-\epsilon} + 4 \sum_i \frac{X^{\frac{b}{2}-\epsilon}}{Z_i} \cdot Z_i \\
 &\leq 14X^{\frac{b}{2}-\epsilon} \log(2X)
 \end{aligned}$$

One can thus find $X_\epsilon > 1$ such that for $X > X_\epsilon$, we have $14X^{\frac{b}{2}-\epsilon} \log(2X) < X^{\frac{b}{2}}$. Hence for all $X > X_\epsilon$, for all $m \in]X, 2X] \setminus (B_{1,X} \cup B_{2,X} \cup B_{3,X})$, we get $A_{\text{er}}(m) \leq m^{\frac{b}{2}}$. In other words, for $X > X_\epsilon$, $S_{\text{bad},X} \subset B_{1,X} \cup B_{2,X} \cup B_{3,X}$. We will obtain upper bounds on the cardinality of $B_{1,X}$, $B_{2,X}$ and $B_{3,X}$.

1. The volume of the region of elements $\lambda \in L_{\mathbb{R}}$ such that $X < Q(\lambda) \leq 2X$ and $|Q(\lambda_x)| < 1$ is bounded by $O(X^{\frac{b}{2}})$, hence a geometry-of-numbers argument implies that the number of elements in L in this region is bounded by $O(X^{\frac{b}{2}})$. More precisely, we break the set of such λ into a finite union of subsets such that for any two elements λ, λ' in each subset, we have $|Q(\lambda_x - \lambda'_x)| < 1$; as Q is negative definite on P and $|Q(\lambda_x)| < 1$, we may choose the subsets using λ_x such that the total number of subsets is a constant only depending on Q . Therefore, as in the proof of Lemma 6.3, for each subset, we count the λ by counting $\lambda_{x^\perp} \in P^\perp$ and then apply a geometry-of-numbers argument on P^\perp . It thus follows that

$$|B_{1,X}| = O(X^\epsilon).$$

2. Let $Y := |B_{2,X}| \geq 1$; and for each $m \in B_{2,X}$, let $\lambda(m)$ be an element of L such that $Q(\lambda(m)) = m$ and $-\log(|Q(\lambda(m)_x)|) \geq X^{\frac{b}{2}}$. By Lemma 6.3, we obtain a nonzero integer vector λ in L such that $-\log(|Q(\lambda_x)|) \gg X^{\frac{b}{2}}$ and $Q(\lambda_{x^\perp}) \ll \frac{X}{Y^{\frac{b}{2}}}$.²⁹ Let $M = Q(\lambda)$, and note that $M = Q(\lambda_x) + Q(\lambda_{x^\perp}) \ll \frac{X}{Y^{\frac{b}{2}}}$. Theorem 5.8(i) implies

$$X^{\frac{b}{2}} \ll -\log(|Q(\lambda_x)|) \ll A(M) \ll M^{\frac{b}{2}} \log M \ll \frac{X^{\frac{b}{2}} \log(X)}{Y}.$$

Therefore, we obtain

$$|B_{2,X}| \ll \log(X).$$

3. The set $B_{3,X}$ is included in the union of the subsets $B_{3,Z_i}, i \in I$ formed by the elements $m \in]X, 2X]$ such that

$$|\{\lambda \in L, Q(\lambda) = m, -\log(|Q(\lambda_x)|) \in]Z_i, 2Z_i]\}| \geq \frac{X^{\frac{b}{2}-\epsilon}}{Z_i}.$$

Suppose that $Y := |B_{3,Z_i}| \geq 1$ for some $i \in I$. Then there are at least $\lceil \frac{Y X^{\frac{b}{2}-\epsilon}}{Z_i} \rceil$ vectors $\lambda \in L$ such that $Q(\lambda) \in]X, 2X]$ and $-\log(|Q(\lambda_x)|) \in]Z_i, 2Z_i]$. We again use Lemma 6.3 to construct an integral

²⁹Although Lemma 6.3 assumes $Y \geq 2$, the above statement is trivial when $Y = 1$.

nonzero vector $\lambda \in L$ such that

$$-\log(|Q(\lambda_x)|) \gg Z_i \text{ and } Q(\lambda_{x^\perp}) \ll \frac{X^{\frac{2\epsilon}{b}} Z_i^{\frac{2}{b}}}{Y^{\frac{2}{b}}}.$$

Let M again denote $Q(\lambda)$, and notice that $M \ll \frac{X^{2\epsilon/b} Z_i^{2/b}}{Y^{2/b}}$. Theorem 5.8(i) implies that

$$Z_i \ll -\log(|Q(\lambda_x)|) \ll A(M) \ll M^{\frac{b}{2}} \log M \ll \frac{X^\epsilon Z_i}{Y}.$$

Thus for every $i \in I$, we have $|B_{3,Z_i}| \ll X^\epsilon$. Summing over all $i \in I$ yields

$$|B_{3,X}| \ll X^\epsilon \log X.$$

Hence we conclude that $\log |S_{\text{bad},X}| \ll \epsilon \log X + \log \log X$. Thus $\limsup_{X \rightarrow \infty} \frac{\log |S_{\text{bad},X}|}{\log X} \leq \epsilon$. As the equality holds for every $\epsilon > 0$, we get the desired result. □

7. Bounding the contribution from a finite place with good reduction

We keep the notations from the beginning of Section 5: namely, \mathcal{M} is the integral model over \mathbb{Z} of the GSpin Shimura variety associated to an even maximal quadratic lattice (L, Q) with signature $(b, 2), b \geq 3$; \mathcal{Y} is an \mathcal{O}_K -point in \mathcal{M} such that \mathcal{Y}_K is Hodge-generic; and $\mathcal{Z}(m)$ denotes the special divisor over \mathbb{Z} associated to an integer $m \in \mathbb{Z}_{>0}$ and is defined in Section 2.5. We denote the Kuga–Satake abelian scheme over \mathcal{O}_K associated to \mathcal{Y} by \mathcal{A} and let A denote \mathcal{A}_K . The assumption of \mathcal{Y}_K being Hodge-generic implies that the lattice of special endomorphisms $V(A_{\overline{K}})$ (see Section 2.5 for the definition) is just $\{0\}$. Fix a prime \mathfrak{P} of \mathcal{O}_K , let p denote the characteristic of the residue field $\mathbb{F}_{\mathfrak{P}}$, and let e denote the ramification index of \mathfrak{P} in K . We use $\mathcal{Y}_{\overline{\mathfrak{P}}}, \mathcal{A}_{\overline{\mathfrak{P}}}$ to denote the geometric special fibres of \mathcal{Y}, \mathcal{A} at \mathfrak{P} .

Recall the intersection multiplicity $(\mathcal{Y} \cdot \mathcal{Z}(m))_{\mathfrak{P}}$ from equation (3.2): let $v \in V(\mathcal{A}_{\overline{\mathfrak{P}}})$ be a special endomorphism of $\mathcal{A}_{\overline{\mathfrak{P}}}$ satisfying $v \circ v = [m]$. We denote by $\mathcal{O}_{\mathcal{Y} \times_{\mathcal{M}} \mathcal{Z}(m), v}$ the étale local ring of $\mathcal{Y} \times_{\mathcal{M}} \mathcal{Z}(m)$ at v . Then we have

$$(\mathcal{Y} \cdot \mathcal{Z}(m))_{\mathfrak{P}} = \sum_{\substack{v \in V(\mathcal{A}_{\overline{\mathfrak{P}}}) \\ v \circ v = [m]}} \text{length}(\mathcal{O}_{\mathcal{Y} \times_{\mathcal{M}} \mathcal{Z}(m), v}). \tag{7.1}$$

In this section, we prove the following result, which controls the above local intersection number on average over m .

Theorem 7.1. *Let $D \in \mathbb{Z}_{\geq 1}$. For $X \in \mathbb{Z}_{>0}$, let $S_{D,X}$ denote the set*

$$\{m \in \mathbb{Z}_{>0} \mid X \leq m < 2X, \frac{m}{D} \in \mathbb{Z} \cap (\mathbb{Q}^\times)^2\}.$$

Then we have

$$\sum_{m \in S_{D,X}} (\mathcal{Y} \cdot \mathcal{Z}(m))_{\mathfrak{P}} = o(X^{\frac{b+1}{2}} \log X).$$

This section is organised as follows. First, in Section 7.1, we express $(\mathcal{Y} \cdot \mathcal{Z}(m))_{\mathfrak{P}}$ as a sum of lattice point counts over a family of p -adically shrinking lattices. We then prove some preliminary properties of these lattices. Finally, in Section 7.2, we evaluate these lattice counts to prove Theorem 7.1. Needless to say, crucial to the proof of Theorem 7.1 is the fact that we have the global height bound (Theorem

5.8) for every individual m . In Section 7.3, we will illustrate this with an example of a $W(\mathbb{F}_q)$ -valued point $\mathcal{Y}' \in \mathcal{M}$ (which is *a posteriori* not defined over a number field) with the property that $(\mathcal{Y}, \mathcal{Z}(m))_p$ is exponential in m for an infinite sequence of positive integers $m \in \{n \in \mathbb{Z}_{>0} : \frac{n}{D} \in \mathbb{Z} \cap (\mathbb{Q}^\times)^2\}$.

7.1. The lattices of special endomorphisms

Let $K_{\mathfrak{P}}$ denote the completion of K at \mathfrak{P} ; let $K_{\mathfrak{P}}^{\text{nr}}$ denote a maximal unramified extension of $K_{\mathfrak{P}}$, and let $\mathcal{O}_{\mathfrak{P}}^{\text{nr}}$ denote its ring of integers. For every $n \in \mathbb{Z}_{\geq 1}$, let L_n denote the lattice of special endomorphisms $V(\mathcal{A}_{\mathcal{O}_{\mathfrak{P}}^{\text{nr}}/\mathfrak{P}^n})$. By definition, $L_{n+1} \subset L_n$ for all n . Since \mathcal{Y}_K is Hodge-generic, then $\bigcap_{n=1}^{\infty} L_n = \{0\}$. Recall from Section 2.5 that all L_n s are equipped with compatible positive definite quadratic forms Q given by

$$v \circ v = Q(v) \cdot \text{Id}_{\mathcal{A} \bmod \mathfrak{P}^n}$$

for every $v \in L_n$.

The next lemma is a direct consequence of the moduli interpretation of $\mathcal{Z}(m)$ in Section 2.5.³⁰

Lemma 7.2. *The local intersection number is given by*

$$(\mathcal{Y}, \mathcal{Z}(m))_{\mathfrak{P}} = \sum_{n=1}^{\infty} |\{v \in L_n \mid Q(v) = m\}|.$$

Note that the right-hand side above is indeed a finite sum since there are only finitely many vectors v in L_1 with $Q(v) = m$; and for each vector v , there exists $n_v \in \mathbb{Z}_{>0}$ such that $v \notin L_{n_v}$.

The following proof uses equation (7.1) and gives a direct description of the length of the étale local rings. Alternatively, one may pick a finite covering of \mathcal{M} over \mathbb{Z}_p and a section of \mathcal{Y} to the covering space and then deduce the intersection number via the projection formula.

Proof. For the proof of this lemma, we may assume (without loss of generality) that $\mathcal{Y} = \text{Spec}(\mathcal{O}_{\mathfrak{P}}^{\text{nr}})$. Consider $v \in V(\mathcal{A}_{\overline{\mathfrak{P}}}^{\text{nr}}) = L_1$ satisfying $v \circ v = [m]$. As \mathcal{Y} is a scheme, we use the moduli interpretation of $\mathcal{Z}(m)$ to see that the étale local ring $\mathcal{O}_{\mathcal{Y} \times_{\mathcal{M}} \mathcal{Z}(m), v}$ represents the following deformation problem.

Consider any local Artin $\mathcal{O}_{\mathfrak{P}}^{\text{nr}}$ -algebra S with residue field $\overline{\mathbb{F}}_{\mathfrak{P}}$. We may view $\text{Spec } S$ as a scheme over \mathcal{M} factoring through \mathcal{Y} , and we refer to this scheme as \mathcal{Y}_S . The deformation problem represented by $\mathcal{O}_{\mathcal{Y} \times_{\mathcal{M}} \mathcal{Z}(m), v}$ associates to the $\mathcal{O}_{\mathfrak{P}}^{\text{nr}}$ -algebra S the data (\mathcal{Y}_S, w) , where w is a special endomorphism of \mathcal{A}_S such that the reduction of w (via $S \rightarrow \overline{\mathbb{F}}_{\mathfrak{P}}$) in $V(\mathcal{A}_{\overline{\mathfrak{P}}}^{\text{nr}})$ is equal to v . Thus the length of $\mathcal{O}_{\mathcal{Y} \times_{\mathcal{M}} \mathcal{Z}(m), v}$ is equal to the largest n such that v lifts to a special endomorphism of $\mathcal{Y}_{\mathcal{O}_{\mathfrak{P}}^{\text{nr}}/\mathfrak{P}^n}$.

Let $\mathbf{1}_{L_n} : L_1 \rightarrow \{0, 1\}$ denote the characteristic function of L_n . Then by equation (7.1), we have

$$(\mathcal{Y}, \mathcal{Z}(m))_{\mathfrak{P}} = \sum_{\substack{v \in V(\mathcal{A}_{\overline{\mathfrak{P}}}^{\text{nr}}) \\ v \circ v = [m]}} \sum_{n=1}^{\infty} \mathbf{1}_{L_n}(v) = \sum_{n=1}^{\infty} \sum_{\substack{v \in L_n \\ v \circ v = [m]}} 1. \text{ here}$$

□

The following proposition generalises [ST19, Thm. 4.1.1, Lem. 4.1.3, Lem. 4.3.2].

Proposition 7.3. *Let Λ denote the \mathbb{Z}_p -lattice of special endomorphisms of the p -divisible group $\mathcal{A}[p^\infty]$ over $\mathcal{O}_{\mathfrak{P}}^{\text{nr}}$ (see Definition 2.3). Then the \mathbb{Z} -rank of L_n is at most $b + 2$ and the \mathbb{Z}_p -rank of Λ is at most b . Moreover, there exists a constant n_0 such that for $n'_0 \geq n_0$,*

$$L_{n'_0+k} = (\Lambda + p^k L_{n'_0} \otimes \mathbb{Z}_p) \cap L_{n_0}$$

for $k \geq 1$. In particular, the rank of L_n is independent of n , and we denote it by r .

³⁰See, for instance, [Con04, Theorems 4.1, 5.1] for similar formulas.

Proof. For the claim on ranks, by [AGHMP18, Lemma 4.5.2], we reduce to the case when L is self-dual at p . In this case, by the Dieudonné theory, $L_n \otimes_{\mathbb{Z}} \mathbb{Z}_p \subseteq L_1 \otimes_{\mathbb{Z}} \mathbb{Z}_p \subseteq \mathbf{V}_{\text{cris}, \mathcal{Y}_{\mathbb{F}}}^{\varphi=1}$, which is a \mathbb{Z}_p -lattice of rank at most $b+2$. Hence $\text{rank}_{\mathbb{Z}} L_n \leq b+2$. For $\text{rank}_{\mathbb{Z}_p} \Lambda$, as in [ST19, Lemma 4.3.2], we make use of the filtration on $\mathbf{V}_{dR, \mathcal{Y}}$. By Grothendieck–Messing theory, $\Lambda \subseteq \mathcal{F}^0 \mathbf{V}_{dR, \mathcal{Y}_{K^{\text{nr}}}} \cap \mathbf{V}_{\text{cris}, \mathcal{Y}_{\mathbb{F}}}^{\varphi=1}$, so $\text{rank}_{\mathbb{Z}_p} \Lambda \leq b+1$, and the equality holds if and only if $\mathcal{F}^0 \mathbf{V}_{dR, \mathcal{Y}_{K^{\text{nr}}}} = \text{span}_{K^{\text{nr}}} \Lambda$. If so, since $\Lambda \subseteq \mathbf{V}_{\text{cris}, \mathcal{Y}_{\mathbb{F}}}^{\varphi=1}$, then $\text{span}_{K^{\text{nr}}} \Lambda$ admits trivial filtration by Mazur’s weak admissibility theorem. This contradicts $\mathcal{F}^1 \mathbf{V}_{dR, \mathcal{Y}_{K^{\text{nr}}}} \neq 0$. We conclude that $\text{rank}_{\mathbb{Z}_p} \Lambda \leq b$.

As in [ST19, Lemma 4.1.3], by Serre–Tate theory,

$$\bigcap_{n=1}^{\infty} (L_n \otimes \mathbb{Z}_p) = \text{End}_{C(L)}(\mathcal{A}[p^{\infty}]_{\mathcal{O}_{\mathbb{F}}^{\text{nr}}}) \cap (L_1 \otimes \mathbb{Z}_p) = \Lambda.$$

To prove the last equality above, by [AGHMP18, Lemma 4.5.2], we reduce to the self-dual case. Then by Definition 2.3, a $C(L)$ -endomorphism of a p -divisible group is special if its crystalline realisation lies in $\mathbf{V}_{\text{cris}, \mathcal{Y}_{\mathbb{F}}}$, which by Dieudonné theory is equivalent in that it lies in $L_1 \otimes \mathbb{Z}_p$.

By [MP16, Lemma 5.9], [AGHMP18, Lemma 4.5.2] and the Néron mapping property, an endomorphism of $\mathcal{A}_{\mathcal{O}_{\mathbb{F}}^{\text{nr}}/\mathbb{F}^n}$ is special if and only if its induced endomorphism in $\text{End}(\mathcal{A}_{\mathbb{F}^n})$ is special. Therefore, a vector $v \in L_1$ lies in L_n if and only if v deforms to an endomorphism of $\mathcal{A}_{\mathcal{O}_{\mathbb{F}}^{\text{nr}}/\mathbb{F}^n}$. Then the rest of the argument is the same as in the proof of [ST19, Theorem 4.1.1]. \square

We now define the successive minima of a lattice following [EK95] and discuss the asymptotics of the successive minima of L_n .

Definition 7.4.

1. For $1 \leq i \leq r$, the successive minimum $\mu_i(n)$ of L_n is defined as

$$\inf\{y \in \mathbb{R}_{>0} : \exists v_1, \dots, v_i \in L_n \text{ linearly independent and } Q(v_j) \leq y^2, 1 \leq j \leq i\}.$$

2. For $n \in \mathbb{Z}_{\geq 1}$, $1 \leq i \leq r$, define $a_i(n) = \prod_{j=1}^i \mu_j(n)$; define $a_0(n) = 1$.

We have the following consequence of Proposition 7.3.

Corollary 7.5. *Every successive minimum $\mu_j(n)$ satisfies $\mu_j(n) \ll p^{n/e}$. If we further assume that $r = b + 2$, then $a_{b+1}(n) \gg p^{n/e}$ and $a_{b+2}(n) \gg p^{2n/e}$.*

Proof. By Proposition 7.3, there exists an absolute bounded $n_0 \equiv n \pmod{e}$ such that

$$L_n = (\Lambda + p^{(n-n_0)/e} L_{n_0} \otimes \mathbb{Z}_p) \cap L_{n_0}.$$

Denote $(n - n_0)/e$ by k , and note that $k \gg n/e$. Since $p^k L_{n_0} \subset L_n$, it follows that $\mu_j(n) \ll p^k$ for every j , proving the first claim.

Now if the rank r of L_n is $b+2$, then (since the rank of Λ is at most b), we clearly have $[L_1 : L_n] \gg p^{2k}$. Thus $\text{Disc}(L_n)^{\frac{1}{2}} \gg p^{2k}$. By [EK95, Equations (5),(6)], this implies that $a_{b+2}(n) \gg p^{2k}$ as required. In conjunction with $\mu_{b+2}(n) \ll p^k$, we also immediately obtain that $a_{b+1}(n) \gg p^k$. \square

Lemma 7.6. *For every $\epsilon > 0$, we have $a_1(n) \gg_{\epsilon} n^{\frac{1}{b+\epsilon}}$. Moreover, $a_i(n) \gg_{\epsilon} n^{\frac{i}{b+\epsilon}}$.*

Proof. Let $\epsilon > 0$. By Theorem 5.8(ii), we have

$$(\mathcal{Y}.\mathcal{Z}(m))_{\mathbb{F}} \ll m^{\frac{b}{2}} \log m \ll_{\epsilon} m^{\frac{b+\epsilon}{2}}. \tag{7.2}$$

Let $w_0 \in L_n$ denote a vector such that $Q(w_0) = a_1(n)^2$. By taking $m = a_1(n)^2$ in equation (7.2), we get

$$n \ll (\mathcal{Y}.\mathcal{Z}(a_1(n)^2))_{\mathbb{F}} \ll_{\epsilon} a_1(n)^{b+\epsilon},$$

where the first bound follows from Lemma 7.2 and the observation that $w_0 \in L_k$ for all $k \leq n$. The second assertion follows directly from the first in conjunction with the bound $a_i(n) \geq a_1(n)^i$. \square

7.2. Proof of Theorem 7.1

We first introduce some notations. For any positive integers $a < b$ and D, X as in Theorem 7.1, define

$$N_D(a, b; X) = \sum_{n=a}^b |\{v \in L_n : Q(v) \in S_{D,X}\}|.$$

It is known that $\text{rank } L_n = b + 2$ if and only if \mathcal{Y} has supersingular reduction at \mathfrak{P} .³¹ When \mathfrak{P} is a prime of supersingular reduction, we write $N_D(1, \infty; X)$ as a sum $N_D(1, \lfloor \frac{\epsilon}{4} \log_p X \rfloor; X) + N_D(\lfloor \frac{\epsilon}{4} \log_p X \rfloor, \infty; X)$. In the following proposition, we follow [ST19, §4.2, §4.3] to bound the finite contributions for primes \mathfrak{P} modulo for which \mathcal{Y} does not have supersingular reduction and also bound $N_D(\lfloor \frac{\epsilon}{4} \log_p X \rfloor, \infty; X)$ for primes \mathfrak{P} modulo for which \mathcal{Y} does have supersingular reduction.

Proposition 7.7. *Let the notation be as above. Then we have*

1. If $r = \text{rank } L_n \leq b + 1$, then

$$\sum_{n=1}^{\infty} |\{v \in L_n \setminus \{0\} : Q(v) < X\}| = O(X^{\frac{b+1}{2}}).$$

2. If $r = b + 2$, then

$$\sum_{n=\lceil \frac{\epsilon}{4} \log_p X \rceil}^{\infty} |\{v \in L_n \setminus \{0\} : Q(v) < X\}| = O(X^{\frac{b+1}{2}}).$$

Proof. Let $\epsilon \in]0, 1[$. By Lemma 7.6, there exists a constant $C_{0,\epsilon}$ such that $a_1(n) \geq C_{0,\epsilon} n^{1/(b+\epsilon)}$. Let $C_{1,\epsilon} = C_{0,\epsilon}^{-(b+\epsilon)}$. If $n > (X^{1/2} C_{0,\epsilon}^{-1})^{b+\epsilon} = C_{1,\epsilon} X^{\frac{b+\epsilon}{2}}$, then $a_1(n) > X^{1/2}$, and hence

$$\{v \in L_n \setminus \{0\} : Q(v) < X\} = \emptyset.$$

Therefore, for (1), we have

$$\begin{aligned} \sum_{n=1}^{\infty} |\{v \in L_n \setminus \{0\} : Q(v) < X\}| &= \sum_{n=1}^{C_{1,\epsilon} X^{\frac{b+\epsilon}{2}}} |\{v \in L_n \setminus \{0\} : Q(v) < X\}| \\ &\stackrel{(i)}{\ll} \sum_{n=1}^{C_{1,\epsilon} X^{\frac{b+\epsilon}{2}}} \sum_{i=0}^r \frac{X^{\frac{i}{2}}}{a_i(n)} \\ &\stackrel{(ii)}{\ll \epsilon} \sum_{n=1}^{C_{1,\epsilon} X^{\frac{b+\epsilon}{2}}} \sum_{i=0}^r \frac{X^{\frac{i}{2}}}{n^{i/(b+\epsilon)}} \\ &= \sum_{i=0}^r \sum_{n=1}^{C_{1,\epsilon} X^{\frac{b+\epsilon}{2}}} \frac{X^{i/2}}{n^{i/(b+\epsilon)}}, \end{aligned}$$

³¹Indeed, $\text{rank } L_n = b + 2$ if and only if the Frobenius φ is isoclinic on $\mathbf{V}_{\text{cris}, \mathcal{Y}_{\mathfrak{P}}}$. The latter claim is equivalent to that $\mathcal{Y}_{\mathfrak{P}}$ lies in the basic (i.e., supersingular) locus in $\mathcal{M}_{\mathfrak{P}}$. Note that we do not need this fact in the proof of Theorem 7.1.

where (i) follows from [EK95, Lemma 2.4, Equations (5),(6)]³² and (ii) follows from Lemma 7.6. For $0 \leq i \leq b$, note that

$$\sum_{n=1}^{C_{1,\epsilon} X^{\frac{b+\epsilon}{2}}} \frac{X^{\frac{i}{2}}}{n^{i/(b+\epsilon)}} \ll_{\epsilon} X^{\frac{i}{2}} \cdot (X^{\frac{b+\epsilon}{2}})^{1-\frac{i}{b+\epsilon}} = O(X^{\frac{b+\epsilon}{2}}).$$

For $i = b + 1$, since $\sum_{n=1}^{\infty} n^{-(b+1)/(b+\epsilon)}$ converges, we have

$$\sum_{n=1}^{C_{1,\epsilon} X^{\frac{b+\epsilon}{2}}} \frac{X^{\frac{i}{2}}}{n^{i/(b+\epsilon)}} = O_{\epsilon}(X^{\frac{b+1}{2}}).$$

For (2), similarly, we have that the left-hand side is bounded by

$$\sum_{n=\lceil \frac{\epsilon}{4} \log_p X \rceil}^{C_{1,\epsilon} X^{\frac{b+\epsilon}{2}}} \frac{X^{(b+2)/2}}{a_{b+2}(n)} + \sum_{i=0}^{b+1} \sum_{n=\lceil \frac{\epsilon}{4} \log_p X \rceil}^{C_{1,\epsilon} X^{\frac{b+\epsilon}{2}}} \frac{X^{\frac{i}{2}}}{n^{i/(b+\epsilon)}}.$$

As in (1), the second term is $O_{\epsilon}(X^{\frac{b+1}{2}})$. For the first term, by Corollary 7.5, we have $a_{b+2}(n) \gg p^{\frac{2n}{e}}$. Since the series $\sum_{n=1}^{\infty} \frac{1}{p^{2n/e}}$ converges and $p^{n/e} \geq X^{1/4}$ when $n \geq \lceil \frac{\epsilon}{4} \log_p X \rceil$, the first term is bounded by $O(\frac{X^{\frac{b+2}{2}}}{\sqrt{X}}) = O(X^{\frac{b+1}{2}})$, and hence the result. □

Remark 7.8. In order to prove Theorem 1.8, we do not have to restrict ourselves to sets like $S_{D,X}$ and can sum over all m . The bounds that the proof of Proposition 7.7 yields are therefore sufficient, even in the case when \mathfrak{F} is a prime of supersingular reduction.

We are now ready to finish the proof of Theorem 7.1.

Proof of Theorem 7.1. By Proposition 7.7(1), we may restrict ourselves to the case where the rank of L_n is equal to $b + 2$. By Proposition 7.7(2), it suffices to prove that $\mathbf{N}_D(1, \lfloor \frac{\epsilon}{4} \log_p X \rfloor, X) = o(X^{\frac{b+1}{2}} \log X)$.

To that end, let $1 \leq T \leq \lfloor \frac{\epsilon}{4} \log_p X \rfloor / e$ be an integer, and let m be an integer satisfying $X \leq m < 2X$. For brevity, let

$$\mathbf{N}_1(m) = |\{v \in L_1 : Q(v) = m\}|, \quad \mathbf{N}_T(m) = |\{v \in L_{eT} : Q(v) = m\}|.$$

Then we have the trivial bound

$$\sum_{n=1}^{\lfloor \frac{\epsilon}{4} \log_p X \rfloor} |\{v \in L_n : Q(v) = m\}| = \sum_{n=1}^{eT} |\{v \in L_n : Q(v) = m\}| + \sum_{n=eT+1}^{\lfloor \frac{\epsilon}{4} \log_p X \rfloor} |\{v \in L_n : Q(v) = m\}| \tag{7.3}$$

$$\leq eT\mathbf{N}_1(m) + \frac{e \log_p X}{4} \mathbf{N}_T(m). \tag{7.4}$$

By Corollary 4.10, $eT\mathbf{N}_1(m) \ll eTm^{\frac{b}{2}} \ll eTX^{\frac{b}{2}}$ and

$$\mathbf{N}_T(m) = \mu_{\infty}(Q_T, 1)\mu(Q_T, m)m^{\frac{b}{2}} + O_{T,\epsilon}(m^{(b+1)/4+\epsilon}),$$

where Q_T is the positive definite quadratic form on L_{eT} . By Lemma 7.9 below,

$$\mu_{\infty}(Q_T, 1)\mu(Q_T, m) \ll p^{-3/5T},$$

³²The authors refer to [Sch68] for a proof of their Lemma 2.4.

so we obtain

$$N_T(m) \ll p^{-3/5T} m^{\frac{b}{2}} + O_{T,\epsilon}(m^{(b+1)/4+\epsilon}).$$

Therefore, by summing equation (7.3) over $m \in S_{D,X}$ and by the above bounds on $N_1(m), N_T(m)$, we have

$$\frac{N_D(1, \lfloor e \log_p X \rfloor, X)}{X^{\frac{b+1}{2}} \log X} \ll \frac{eT}{\log X} + p^{-3/5T} + \frac{O_{T,\epsilon}(X^{(b+3)/4+\epsilon})}{X^{\frac{b+1}{2}} \log X}.$$

Therefore,

$$\limsup_{X \rightarrow \infty} \frac{N_D(1, \lfloor e \log_p X \rfloor, X)}{X^{\frac{b+1}{2}} \log X} \ll p^{-3/5T}.$$

As the above inequality is true for every value of T , we have

$$N_D(1, \lfloor e \log_p X \rfloor, X) = o(X^{\frac{b+1}{2}} \log X),$$

whence the theorem follows. □

Lemma 7.9. *Let Q denote an integral positive definite quadratic form of rank $r \geq 5$, let $m \geq 1$ be any integer, and let p denote a prime. Then we have*

$$\mu_\infty(Q, 1)\mu_p(Q, m) \ll \frac{p^r}{|\text{Disc}(Q)|^{3/20}},$$

where the implicit constant above only depends on r . In particular, for T and p as above, we have

$$\mu_\infty(Q_T, 1)\mu(Q_T, m) \ll p^{-3/5T}.$$

Proof. The definition of $\mu_\infty(Q, 1)$ in Section 4.2 yields that $\mu_\infty(Q, 1) \asymp \text{Disc}(Q)^{-1/2}$, where the implicit constant only depends on the rank r . The assertion about Q_T follows from the first assertion, by the fact that $\text{Disc}(Q_T)^{-1/2} \ll p^{-2T}$ (from Corollary 7.5) and the fact that for a prime $\ell \neq p$, $\mu_\ell(Q_T, m)$ is independent of T for $T \gg 1$ (from Proposition 7.3). Therefore, it suffices to prove the first assertion.

Recall from Sections 4.1–4.2 that we have $\mu_p(Q, m) = \mu_p(m, n)$ for some sufficiently large integer n . Moreover, following [Han04, §3, pp. 359–360], we have

$$\mu_p(m, n) = \mu_p^{\text{good}}(m, n) + \mu_p^{\text{bad1}}(m, n) + \mu_p^{\text{bad2}}(m, n) + \mu_p^{\text{zero}}(m, n),$$

where the summands come from elements of reduction type good, bad1, bad2 and zero, respectively. To prove the first estimate of the lemma, we once again (as in Section 4.1) use the reduction maps from [Han04, §3]. These immediately yield the following inequalities:

$$\begin{aligned} \mu_p^{\text{good}}(m, n) &\leq p^3, \\ \mu_p^{\text{bad1}}(m, n) &\leq p^4, \\ \frac{\mu_p^{\text{bad2}}(m, n)}{\text{Disc}(Q)^{1/2}} &\leq p^{2-r} \frac{\mu'' p(m/p^2, n-2)}{\text{Disc}(Q'')^{1/2}}, \\ \mu_p^{\text{zero}}(m, n) &\leq p^{2-r} \mu_p(m/p^2, n-2), \end{aligned}$$

where in the third line, Q'' is a quadratic form of rank r constructed from Q (see [Han04, p.360] for the definition of Q'') and μ'' is the density corresponding to Q'' . Furthermore, it is easy to check that we

have $\text{Disc}(Q'') \geq \text{Disc}(Q)/p^{2r}$. Then we obtain the bound $\frac{\mu_p(m, n)}{\text{Disc}(Q)^{1/2}} \leq \frac{p^r}{\text{Disc}(Q)^{3/20}}$ by induction on n , along with the observation that in each step of the induction, $\text{Disc}(Q'')$ decreases by at most p^{2r} and $r - 2 \geq 3$. □

7.3. A transcendental example

We now demonstrate an example of a point $\mathcal{Y}' \in \mathcal{M}(W(\mathbb{F}_q))$ with the property that $(\mathcal{Y}' \cdot \mathcal{Z}(m))_p$ is exponential in m for an infinite sequence of $m \in S$, where $S = \{\mathbb{Z}_{>0} \cap (\mathbb{Q}^\times)^2\}$ and $\text{char } \mathbb{F}_q = p$. Similar examples can be analogously constructed with $m \in S_D = \{\mathbb{Z}_{>0} \cap D \cdot (\mathbb{Q}^\times)^2\}$. As this example isn't necessary for any of the main results and only serves to highlight the importance of the global height bound, we will be brief in our exposition.

For simplicity, assume that the rank of the lattice defining the Shimura variety is even and at least 12. Let $b = 2c$. We may choose our Shimura variety \mathcal{M} such that it admits a map from the modular curve in characteristic 0 and hence contains a CM point \mathcal{Y} whose lattice of special endomorphisms L also has rank $b = 2c$. We may also assume that L represents every large enough positive integer.

Let p be a large enough prime of ordinary reduction for this point. We also assume that p doesn't divide the discriminant of the lattice of special endomorphisms of \mathcal{Y} . Let y denote the mod p reduction of \mathcal{Y} – we may assume (by increasing p if necessary) that \mathcal{Y} is the canonical lift of y and therefore L is also the lattice of special endomorphisms of y . Let q be such that $y \in \mathcal{M}(\mathbb{F}_q)$.

The lemma below follows from Serre–Tate theory and [MP16, Corollaries 5.17, 5.19]:

Lemma 7.10. *Let $\Lambda \subset L \otimes \mathbb{Z}_p$ denote a self-dual³³ \mathbb{Z}_p -submodule. Then there exists a point $\mathcal{Y}_\Lambda \in \mathcal{M}(W(\mathbb{F}_q))$ lifting y whose \mathbb{Z}_p -lattice of special endomorphisms is Λ . Further, we have that the \mathbb{Z} -lattice of special endomorphisms of $\mathcal{Y}_\Lambda \bmod p^{n+1}$ is $(\Lambda + p^n L \otimes \mathbb{Z}_p) \cap L$.*

Our example \mathcal{Y}' will equal \mathcal{Y}_Λ for an appropriate choice of Λ . A choice of Λ that is 'very well approximated' by \mathbb{Z} -sublattices of L will have the property that $(\mathcal{Y}_\Lambda \cdot \mathcal{Z}(m))$ is exponential in terms of m for infinitely many m . Indeed, the following lemma makes this precise.

Lemma 7.11. *Suppose that a rank $r \geq 5$ self-dual sublattice $\Lambda \subset L \otimes \mathbb{Z}_p$ has the following properties:*

1. Λ contains no integer elements – that is, $\Lambda \cap L = \{0\}$.
2. There exists an increasing sequence of rank r sublattices $L_i \subset L$ with discriminants D_i such that $\Lambda \equiv L_{n_i} \bmod p^{N_i}$, where $N_i \geq e^{D_i}$.

Then there exists an increasing sequence of perfect squares m_i such that $(\mathcal{Y}_\Lambda, \mathcal{Z}(m_i))_p$ is exponential in m_i .

Proof. We first note that property 1 implies that \mathcal{Y}_Λ isn't contained in any special divisor $\mathcal{Z}(m)$, so the intersection $(\mathcal{Y}_\Lambda \cdot \mathcal{Z}(m))_p$ is well defined for every positive integer m . Property 2 implies that the lattice of special endomorphisms of $\mathcal{Y}_\Lambda \bmod p^{N_i+1}$ is $L_i + p^{N_i} L$. The lattice L_i , having rank at least 5, must locally represent perfect squares satisfying congruence conditions modulo a power of D_i , where the power depends only on the rank r and nothing else. Therefore, L_i must represent perfect squares (again satisfying these congruence conditions) having size bounded by e^{D_i} , because if a quadratic form having rank at least 4 locally represents integers that are large relative to the discriminant, it must actually represent such integers too.

Pick some perfect square $m_i < e^{D_i}$, which L_i represents. Then we have (by Lemma 7.2) $(\mathcal{Y}_\Lambda \cdot \mathcal{Z}(m_i))_p > N_i$. The lemma follows. □

We now only need to find a \mathbb{Z}_p -sublattice of L that satisfies the properties of Lemma 7.11. To that end, we may assume that L has an integral orthogonal basis $e_1, f_1, \dots, e_c, f_c$. For elements $\mu_1 \dots \mu_c \in \mathbb{Z}_p$, we consider the rank $c\mathbb{Z}_p$ -sublattice defined by $\Lambda = \text{Span}_{\mathbb{Z}_p} \{e_i + \mu_i f_i\}$. The fact that $b \geq 10$ implies that

³³We mean self-dual with respect to the quadratic form on L .

Λ has rank ≥ 5 . Insisting that the μ_i are irrational implies that Λ has property 1. We now pick the μ_i so that Λ satisfies property 2. We will write $\mu = \sum_{i \geq 0} a_i p^i$, with $0 \leq a_i \leq p - 1$ and $a_0 = 1$. We define the a_i as follows: suppose that $a_n \neq 0$; we define $a_i = 0$ for $n + 1 \leq i \leq e^{e^{p^n}}$, and we then define $a_i = 1$ for $i = \lceil e^{e^{p^n}} \rceil$. This implies that $\sum_{i \leq n} a_i p^i \equiv \mu \pmod{p^N}$ with $N \geq e^{e^{p^n}} - 1$ – that is, there is an integer x_n of size $O(p^n)$ that approximates $\mu \pmod{p^N}$, with N double-exponential in the size of x_n . Having defined μ in this way, we pick $\mu_i = \mu$ for all i , and the lattice Λ created this way must also have property 2.

Choosing $\mathcal{Y}' = \mathcal{Y}_\Lambda$, we obtain our example by Lemma 7.11.

8. Proof of the main theorem

Let (L, Q) be a maximal integral quadratic even lattice of signature $(b, 2)$ with $b \geq 3$, and let \mathcal{M} denote the integral model of the Shimura variety associated to (L, Q) defined in Section 2. We recall the statement of the main theorem:

Theorem 2.4. *Let K be a number field, and let $D \in \mathbb{Z}_{>0}$ be a fixed integer represented by (L, Q) . Let $\mathcal{Y} \in \mathcal{M}(\mathcal{O}_K)$, and assume that $\mathcal{Y}_K \in M(K)$ is Hodge-generic. Then there are infinitely many places \mathfrak{P} of K such that $\mathcal{Y}_{\overline{\mathfrak{F}}}$ lies in the image of $\mathcal{Z}(Dm^2) \rightarrow \mathcal{M}$ for some $m \in \mathbb{Z}_{>0}$. Equivalently, for a Kuga–Satake abelian variety \mathcal{A} over \mathcal{O}_K parametrised by \mathcal{M} such that $\mathcal{A}_{\overline{K}}$ does not have any special endomorphisms, there are infinitely many \mathfrak{P} such that $\mathcal{A}_{\overline{\mathfrak{F}}}$ admits a special endomorphism v such that $v \circ v = [Dm^2]$ for some $m \in \mathbb{Z}_{>0}$.*

In this section, we will prove Theorem 2.4 using results proved in the previous sections. First, we recall results and definitions that we will need to prove the main theorem.

We have the expression

$$h_{\widehat{\mathcal{Z}}(m)}(\mathcal{Y}) = \sum_{\sigma: K \hookrightarrow \mathbb{C}} \Phi_m(\mathcal{Y}^\sigma) + \sum_{\mathfrak{P}} (\mathcal{Y} \cdot \mathcal{Z}(m))_{\mathfrak{P}} \log |\mathcal{O}_K / \mathfrak{P}|. \tag{8.1}$$

In Sections 5, 6 and 7, we proved results bounding the terms in equation (8.1), which we restate below for the convenience of the reader.

Theorem 5.7. For every m representable by (L, Q) , we have

$$\Phi_m(\mathcal{Y}^\sigma) = c(m) \log m + A(m, \mathcal{Y}^\sigma) + o(|c(m)| \log m).$$

Theorem 6.1. There exists a subset $S_{\text{bad}} \subset \mathbb{Z}_{>0}$ of logarithmic asymptotic density zero such that for every $m \notin S_{\text{bad}}$, we have

$$A(m, \mathcal{Y}^\sigma) = o(m^{\frac{b}{2}} \log(m)).$$

Theorem 7.1. Given $D, X \in \mathbb{Z}_{>0}$, let $S_{D,X}$ denote the set

$$\{m \in \mathbb{Z}_{>0} \mid X \leq m < 2X, \sqrt{m/D} \in \mathbb{Z}\}.$$

For a fixed prime \mathfrak{P} of K and a fixed D , we have

$$\sum_{m \in S_{D,X}} (\mathcal{Y} \cdot \mathcal{Z}(m))_{\mathfrak{P}} = o(X^{\frac{b+1}{2}} \log X).$$

Proof of Theorem 2.4. Assume for contradiction that there exists $D \in \mathbb{Z}_{>0}$ represented by L such that there are only finitely many \mathfrak{P} for which $\mathcal{Y}_{\overline{\mathfrak{F}}}$ lies in the image of $\mathcal{Z}(m)$, where m/D is a perfect square. Therefore, for such m , $(\mathcal{Y} \cdot \mathcal{Z}(m))_{\mathfrak{P}} = 0$ for all but finitely many \mathfrak{P} .

For $X \in \mathbb{Z}_{>0}$, let $S_{D,X}^{\text{good}}$ denote the set $\{m \in S_{D,X} \mid m \notin S_{\text{bad}}\}$, where $S_{D,X}$ is defined in Theorem 7.1 and S_{bad} is the union of the sets of log asymptotic density 0 in Theorem 6.1 by taking $x = \mathcal{Y}^\sigma$ for all

$\sigma : K \hookrightarrow \mathbb{C}$. Then S_{bad} is also of log asymptotic density 0 and $|S_{D,X}^{\text{good}}| \asymp X^{1/2}$ as $X \rightarrow \infty$. On the other hand, by assumption, D is representable by (L, Q) ; then each $m \in S_{D,X}$ is representable by (L, Q) , and hence $\mathcal{Z}(m) \neq \emptyset$.

We sum (8.1) over $m \in S_{D,X}^{\text{good}}$ and note that for each $m \in S_{D,X}^{\text{good}}$, $m \asymp X$. For the archimedean term, by Theorem 5.7, we have

$$\sum_{m \in S_{D,X}^{\text{good}}} \sum_{\sigma:K \hookrightarrow \mathbb{C}} \frac{\Phi_m(\mathcal{Y}^\sigma)}{|\text{Aut}(\mathcal{Y}^\sigma)|} \asymp -X^{\frac{b+1}{2}} \log X. \tag{8.2}$$

For a fixed \mathfrak{P} , since $(\mathcal{Y}.\mathcal{Z}(m))_{\mathfrak{P}} \geq 0$ for all m , then by Theorem 7.1,

$$\sum_{m \in S_{D,X}^{\text{good}}} (\mathcal{Y}.\mathcal{Z}(m))_{\mathfrak{P}} \log |\mathcal{O}_K/\mathfrak{P}| \leq \sum_{m \in S_{D,X}} (\mathcal{Y}.\mathcal{Z}(m))_{\mathfrak{P}} \log |\mathcal{O}_K/\mathfrak{P}| = o(X^{\frac{b+1}{2}} \log X).$$

Since $(\mathcal{Y}.\mathcal{Z}(m))_{\mathfrak{P}} = 0$ for all but finitely many \mathfrak{P} , we have

$$\sum_{m \in S_{D,X}^{\text{good}}} \sum_{\mathfrak{P}} (\mathcal{Y}.\mathcal{Z}(m))_{\mathfrak{P}} \log |\mathcal{O}_K/\mathfrak{P}| = o(X^{\frac{b+1}{2}} \log X). \tag{8.3}$$

By Proposition 3.2, we have $\sum_{m \in S_{D,X}^{\text{good}}} h_{\widehat{\mathcal{Z}}(m)}(\mathcal{Y}) = O(X^{\frac{b+1}{2}})$, which contradicts equation (8.1). \square

9. Applications: Picard rank jumps and exceptional isogenies

In this section, we will elaborate on a number of applications: K3 surfaces and rational curves on them, exceptional splittings of Kuga-Satake abelian varieties and abelian varieties parametrised by unitary Shimura varieties. Then we set our results in context with past work of Charles [Cha18] and Shankar-Tang [ST19] that deals with Shimura varieties associated to quadratic lattices of signature $(2, 2)$.

9.1. Picard rank jumps in families of K3 surfaces and rational curves

For background on K3 surfaces, we refer to [Huy16]. Let X be a K3 surface over a number field K . By replacing K with a finite extension if necessary, we may assume that $\text{Pic}(X_{\overline{K}}) = \text{Pic}(X)$. For any embedding $\sigma : K \hookrightarrow \mathbb{C}$, the \mathbb{Z} -module $H^2(X_{\sigma}^{\text{an}}, \mathbb{Z})$ endowed with the intersection form Q given by Poincaré duality is an unimodular even lattice of signature $(3, 19)$. The first Chern class map

$$c_1 : \text{Pic}(X) \rightarrow H^2(X_{\sigma}^{\text{an}}, \mathbb{Z})$$

is a primitive embedding. By the Hodge index theorem, $\text{Pic}(X)$ has signature $(1, \rho(X) - 1)$, where $\rho(X)$ is the Picard rank of X . Let (L, Q) be a maximal orthogonal lattice to $\text{Pic}(X)$ in $H^2(X_{\sigma}^{\text{an}}, \mathbb{Q})$. Then $(L, -Q)$ is an even lattice whose genus is independent of the choice of σ and L and has signature $(b, 2)$, where $b = 20 - \rho(X)$. Let \mathcal{M} be the GSpin Shimura variety associated to $(L, -Q)$. By [And96, Main Lemma 1.7.1], up to extending K , the Kuga-Satake abelian variety associated to X , denoted by A , is defined over K and corresponds to a K -point $x \in \mathcal{M}(K)$.

Proof of Theorem 1.1. Since X has everywhere good reduction, up to extending K , by [And96, Lemma 9.3.1], the corresponding Kuga-Satake abelian variety A also has potentially good reduction everywhere. Then by Proposition 2.1(4), it gives rise to an \mathcal{O}_K -point \mathcal{Y} of \mathcal{M} . It is Hodge-generic by construction of the Shimura variety \mathcal{M} and by the Lefschetz theorem on $(1, 1)$ classes. By Theorem 1.8, there exist infinitely many places \mathfrak{P} of K and $m > 0$, such that the geometric fibre of the reduction A , denoted by $A_{\overline{\mathfrak{P}}}$, has a special endomorphism s such that $s \circ s = [m]$. By [And96, Main Lemma 1.7.1 (ii)], a special

endomorphism of $A_{\overline{\mathfrak{F}}}$ corresponds to a line bundle L on $X_{\overline{\mathfrak{F}}}$ such that $Q(L) = -m$ and is orthogonal to the image of $\text{Pic}(X)$ inside $\text{Pic}(X_{\overline{\mathfrak{F}}})$ under the specialisation map. This proves Theorem 1.1. \square

Proof of Corollary 1.3. Let X be a K3 surface defined over a number field that has potentially everywhere good reduction. Then by Theorem 1.1, X has infinitely many specialisations where the geometric Picard rank jumps. If X has finitely many unirational specialisations, then the strategy of [LL12] can be applied; more precisely, the statements [LL12, Proposition 4.2] are satisfied, and we can thus conclude by the proof of [LL12, Theorem 4.3]. \square

9.2. Kuga–Satake abelian varieties

Via the exceptional isomorphism between GSp_4 and $\text{GSpin}(V)$ with $b = 3$, as in [KR00], the moduli space \mathcal{S}_2 of principally polarised abelian surfaces³⁴ is a GSpin Shimura variety. In this case, let B be a principally polarised abelian surface; then as in [KR00], the special endomorphisms are $s \in \text{End}(B)$ such that $s^\dagger = s$ and $\text{tr } s = 0$, where \dagger denotes the Rosati involution. Indeed, let A denote the Kuga–Satake abelian variety (of dimension $2^{2+3-1} = 16$) at the point $[B] \in \mathcal{S}_2$ and $A = A^+ \times A^-$ given in Section 2.2; Kudla and Rapoport gave a moduli interpretation of special divisors by defining special endomorphisms to be $s \in \text{End}_{C^+(L)}(A^+)$ such that $s^\dagger = s$ and $\text{tr } s = 0$ (see [KR00, §1, Definition 2.1]). By [KR00, §1], we have $C^+(V) \cong M_4(\mathbb{Q})$, and hence A^+ is isogenous to B^4 ; moreover, the special endomorphisms induces $s_B \in \text{End}(B) \otimes \mathbb{Q}$ such that $s_B^\dagger = s_B$ and $\text{tr } s_B = 0$.

The Kudla–Rapoport version of special endomorphisms allows us to deduce Theorem 1.4 from Theorem 2.4. We now work with the general setting as in Assumption 1.5 since the argument is the same. Recall that $b = 2n - 1$ for $n \in \mathbb{Z}_{>0}$, and we assume that $C^+(V) \cong M_{2n}(\mathbb{Q})$; then A^+ is isogenous to B^{2^n} , where B is an abelian variety with $\dim B = 2^n$. By [vG08, §5.2], if $[A]$ is a Hodge generic point in \mathcal{M} , then $\text{End}(A_{\overline{K}}^+) \otimes \mathbb{Q} = C^+(V)$, and in particular, $\text{End}(B_{\overline{K}}) = \mathbb{Z}$ and B is geometrically simple.

To translate a special endomorphism of the Kuga–Satake abelian variety A to a special endomorphism of A^+ , we choose an element $\delta_0 \in Z(C(L)) \cap C(L)^-$ such that $\delta_0^* = \delta_0$, where $Z(C(L))$ denote the centre of $C(L)$ and $(-)^*$ denote the unique involution on $C(V)$ that acts trivially on V (see, for instance, [AGHMP17, §2.1] for a concrete definition). Indeed, let $e_1, \dots, e_{b+2} \in L$ be a basis of V such that $Q(v) = d_1x_1^2 + \dots + d_{b+2}x_{b+2}^2$ for $v = x_1e_1 + \dots + x_{b+2}e_{b+2}$. Since $b \equiv 3 \pmod{4}$, we may take $\delta_0 = e_1 \cdots e_{b+2}$ and note that $\delta_0^2 = \prod_{i=1}^{b+2} d_i$. Via the usual $C(L)$ -action on A , the element $\delta_0 \in C(L)^-$ induces an endomorphism $\delta_0 : A^- \rightarrow A^+$; and hence for any special endomorphism $v \in \text{End}_{C(L)}(A)$ defined in Section 2.5, since $v : A^+ \rightarrow A^-$ and $\delta_0 \in Z(C(L))$, we have $s := \delta_0 \circ v \in \text{End}_{C^+(L)}(A^+)$. Since $C^+(V) \cong M_{2n}(\mathbb{Q})$ and A^+ is isogenous to B^{2^n} , we obtain $s_B \in \text{End}(B) \otimes \mathbb{Q}$. Since s is not a scalar multiplication on A^+ , s_B is not a scalar multiplication on B .

Proof of Theorem 1.4 and Theorem 1.6. Using the notation as above, let $D = \prod_{i=1}^{b+2} d_i$. By Corollary 4.7, without loss of generality, we may multiple D by a square number such that D is representable by (L, Q) . For a finite place \mathfrak{P} , if v is a special endomorphism of $A_{\overline{\mathfrak{F}}}$ such that $v \circ v = [Dm^2]$, then $\delta_0 \circ v$ induces a quasi-endomorphism s_B on $B_{\overline{\mathfrak{F}}}$ such that $s_B \circ s_B = [Q(\delta)Q(v)] = [D^2m^2]$. Since s_B is not a scalar multiplication, $\ker(s_B - [Dm])$ is a nontrivial simple factor of $B_{\overline{\mathfrak{F}}}$, and hence $B_{\overline{\mathfrak{F}}}$ is nonsimple. We conclude by Theorem 2.4 that there are infinitely many such \mathfrak{P} . \square

Via the algorithm in the proof of [vG00, Thm. 7.7], here is an example when $C^+(V) = M_{2n}(\mathbb{Q})$: assume $b \equiv 3 \pmod{8}$, and consider $Q(x) = -x_1^2 - x_2^2 + \sum_{i=3}^{b+1} x_i^2 + dx_{b+2}^2$.

9.3. Abelian varieties parametrised by unitary Shimura varieties

We recall the moduli interpretation of the Shimura varieties attached to $\text{GU}(r, 1)$ following [KR14, §2] (see also [BHK⁺ 17, §2.2]). Recall that E is an imaginary quadratic field. Consider the moduli problem

³⁴They do not need the polarisation degree to be one; here we work with the principally polarised case for simplicity. Indeed, to prove Theorem 1.4, we may enlarge K and work with a principally polarised abelian surface isogenous to the one in question.

that associates to a locally noetherian \mathcal{O}_E -scheme S the groupoid of triples (B, ι, λ) , where B is an abelian scheme over S , $\iota : \mathcal{O}_E \hookrightarrow \text{End}_S(B)$ and $\lambda : B \rightarrow B^\vee$ is a principal polarisation such that

1. $\iota(a)^\dagger = \iota(a^\sigma)$, where \dagger is the Rosati involution and σ is the nontrivial element in $\text{Gal}(E/\mathbb{Q})$; and
2. $\iota(a)$ acts on $\text{Lie } A$ with characteristic polynomial $(T - \varphi(a))^r (T - \varphi(a)^\sigma)$, where $\varphi : \text{Spec } \mathcal{O}_E \rightarrow S$ is the structure morphism.

This moduli space $\mathcal{M}(r, 1)$ is a Deligne–Mumford stack over \mathcal{O}_E such that $\mathcal{M}(r, 1)_E$ is a disjoint union of Shimura varieties attached to $\text{GU}(r, 1)$ (see, for instance, [KR14, Prop. 2.19, Prop. 4.4]). Similarly, we define $\mathcal{M}(1, 0)$. In particular, after enlarging K by a finite extension that contains E , the abelian variety A in Corollary 1.7 gives a K -point on $\mathcal{M}(r, 1)$.

To relate $\mathcal{M}(r, 1)$ to the GSpin Shimura variety \mathcal{M} defined in Section 2, we pick an auxiliary elliptic curve A_0 defined over a finite extension of E such that $\mathcal{O}_E \subset \text{End}(A_0)$ and the action of \mathcal{O}_E on $\text{Lie } A_0$ is given by the embedding of \mathcal{O}_E into the definition field of A_0 , and hence A_0 is a point on $\mathcal{M}(1, 0)$. As in [BHK⁺ 17, §§2.1, 2.2], pick an embedding of the definition field of A_0 (respectively, A) into \mathbb{C} , and let W_0 (respectively, W) denote the E -vector space $H_{1,B}(A_0(\mathbb{C}), \mathbb{Q})$ (respectively, $H_{1,B}(A(\mathbb{C}), \mathbb{Q})$), where the E -vector space structure is induced by the \mathcal{O}_E -action on A_0 (respectively, A). There exists a unique Hermitian form ψ of signature $(r, 1)$ on W such that the symplectic form on $H_{1,B}(A(\mathbb{C}), \mathbb{Q})$ induced by the polarisation is equal to $\text{tr}_{E/\mathbb{Q}}((\text{disc } E)^{-1/2} \psi)$. Similarly, there exists a Hermitian form ψ_0 of signature $(1, 0)$ on W_0 such that $\text{tr}_{E/\mathbb{Q}}((\text{disc } E)^{-1/2} \psi_0)$ induces the polarisation on A_0 . By [BHK⁺ 17, eqns (2.1.4), (2.1.5)], ψ_0 and ψ induce a Hermitian form ϕ on the E -vector space $\text{Hom}_{\mathcal{O}_E}(H_{1,B}(A_0(\mathbb{C}), \mathbb{Q}), H_{1,B}(A(\mathbb{C}), \mathbb{Q}))$ of signature $(r, 1)$. Let V denote the \mathbb{Q} -vector space $\text{Hom}_{\mathcal{O}_E}(H_B^1(A_0(\mathbb{C}), \mathbb{Q}), H_B^1(A(\mathbb{C}), \mathbb{Q}))$ endowed with the quadratic form $\text{tr}_{E/\mathbb{Q}} \phi$; V is of signature $(2r, 2)$.

Let G' denote the subgroup of $\text{GU}(W_0, \psi_0) \times \text{GU}(W, \psi)$ given by pairs whose similitude factors are equal. By [BHK⁺ 17, §§2.1, 6.2] and [Hof14, §4], the induced action of G' on V gives a group homomorphism $G' \rightarrow \text{SO}(V)$, and this group homomorphism is indeed a map between Shimura data (with the Hodge cocharacters given by the ones induced by the Hodge cocharacters of A_0 and A); hence we have a map between Shimura varieties $\text{Sh}(G') \rightarrow \text{Sh}(\text{SO}(V))$ (with the maximal compact open subgroups of $G'(\mathbb{A}_f)$ and $\text{SO}(V)(\mathbb{A}_f)$ defined by lattices in W_0 and W given by $H_{1,B}(A_0(\mathbb{C}), \mathbb{Z})$ and $H_{1,B}(A(\mathbb{C}), \mathbb{Z})$). By [BHK⁺ 17, Prop. 2.2.1], $\text{Sh}(G') \subset \mathcal{M}(1, 0) \times \mathcal{M}(r, 1)$ and (A_0, A) gives a $\overline{\mathbb{Q}}$ -point on $\text{Sh}(G')$ and hence a $\overline{\mathbb{Q}}$ -point on $\text{Sh}(\text{SO}(V))$.

Note that $\text{GSpin}(V) \rightarrow \text{SO}(V)$ induces an open and closed morphism $M \rightarrow \text{Sh}(\text{SO}(V))$ (with a suitable choice of maximal compact subgroups, which does not affect the rest of the argument), where M is the GSpin Shimura variety defined in Section 2.1; therefore, by applying a suitable Hecke translate on $\text{Sh}(\text{SO}(V))$, the image of the point (A_0, A) under the Hecke translate lies in a connected component of $\text{Sh}(\text{SO}(V))$ that lies in the image of M . In particular, there exists a point $Y \in M(\overline{\mathbb{Q}})$ such that Y maps to the Hecke translate of (A_0, A) , and hence as \mathbb{Q} -Hodge structures,

$$\mathbf{V}_{B,Y} \otimes \mathbb{Q} \cong \text{Hom}_{\mathcal{O}_E}(H_{1,B}(A_0(\mathbb{C}), \mathbb{Q}), H_{1,B}(A(\mathbb{C}), \mathbb{Q})),$$

where $\mathbf{V}_{B,Y}$ denotes the fibre at Y of the local system \mathbf{V}_B defined in Section 2.2. We enlarge K by a finite extension so that Y, A_0 and A are all defined over K . Since all Hodge cycles in the category of absolute Hodge motives generated by abelian varieties are absolute Hodge by Deligne’s theorem, then after enlarging K by a finite extension, we have

$$\mathbf{V}_{\ell,\acute{e}t,Y} \cong \text{Hom}_{\mathcal{O}_E}(H_{1,\acute{e}t}(A_0, \mathbb{Q}_\ell), H_{1,\acute{e}t}(A, \mathbb{Q}_\ell)) \tag{9.1}$$

as $\text{Gal}(\overline{K}/K)$ -modules. We use A^{KS} to denote the Kuga–Satake abelian variety corresponding to $Y \in M(K)$.

Proof of Corollary 1.7. Since A and A_0 have potentially good reduction everywhere, then after enlarging by K by a finite extension such that both A and A_0 have good reduction over K , the Galois

representation $\mathrm{Hom}_{\mathcal{O}_E}(H_{1,\acute{e}t}(A_0, \mathbb{Q}_\ell), H_{1,\acute{e}t}(A, \mathbb{Q}_\ell))$ is unramified away from ℓ . By [And96, Lemma 9.3.1] and equation (9.1), the Kuga–Satake abelian variety A^{KS} has potentially good reduction everywhere. Then by Proposition 2.1(4), Y extends to an \mathcal{O}_K -point \mathcal{Y} of \mathcal{M} . By Theorem 1.8 and the definition of special endomorphisms (Definition 2.2), there are infinitely many places \mathfrak{P} such that $V_{\ell,\acute{e}t,\mathcal{Y}_{\mathfrak{P}}}$ admits a Tate cycle (after possible finite extension of the residue field) for ℓ not equal to the residue characteristic of \mathfrak{P} . For such a prime \mathfrak{P} , by equation (9.1), there exists an $n \in \mathbb{Z}_{>0}$ such that $\mathrm{Hom}_{\mathcal{O}_E}(H_{1,\acute{e}t}(A_0, \mathbb{Q}_\ell), H_{1,\acute{e}t}(A, \mathbb{Q}_\ell))^{\mathrm{Frob}_{\mathfrak{P}}^n=1} \neq \emptyset$. In particular, $A_{0,\overline{\mathfrak{P}}}$ is an isogeny factor of $A_{\overline{\mathfrak{P}}}$ by Tate’s theorem. \square

Acknowledgements. We are very grateful to Fabrizio Andreatta, Olivier Benoist, Laurent Clozel, Edgar Costa, Quentin Guignard, Jonathan Hanke, Benjamin Howard, Christian Liedtke, Yifeng Liu, Chao Li, Daves Maulik and Jacob Tsimerman for many helpful conversations. Part of this work has been done in S.T.’s PhD thesis, and he is particularly grateful to François Charles. We’re also very grateful to the referee for several valuable suggestions that have improved this paper.

A.N.S. is partially supported by the NSF grant DMS-2100436. A.S. is supported by an NSERC Discovery grant and a Sloan fellowship. Y.T. is partially supported by the NSF grant DMS-1801237. S.T. has received funding from the European Research Council (ERC) under the European Union’s Horizon 2020 research and innovation programme (grant agreement No 715747).

References

- [AGHMP17] Fabrizio Andreatta, Eyal Z. Goren, Benjamin Howard, and Keerthi Madapusi Pera. Height pairings on orthogonal Shimura varieties. *Compos. Math.*, **153**(3): 474–534, 2017.
- [AGHMP18] Fabrizio Andreatta, Eyal Z. Goren, Benjamin Howard, and Keerthi Madapusi Pera. Faltings heights of abelian varieties with complex multiplication. *Ann. of Math. (2)*, **187**(2): 391–531, 2018.
- [And96] Yves André. On the Shafarevich and Tate conjectures for hyper-Kähler varieties. *Math. Ann.*, **305**(2): 205–248, 1996.
- [AS64] Milton Abramowitz and Irene A. Stegun. *Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables*, volume 55 of *National Bureau of Standards Applied Mathematics Series*. Government Printing Office, Washington, D.C., 1964.
- [Bas74] Hyman Bass. Clifford algebras and spinor norms over a commutative ring. *Amer. J. Math.*, **96**: 156–206, 1974.
- [BF04] Jan Hendrik Bruinier and Jens Funke. On two geometric theta lifts. *Duke Math. J.*, **125**(1): 45–90, 2004.
- [BHK⁺17] Jan Bruinier, Benjamin Howard, Stephen S Kudla, Michael Rapoport, and Tonghai Yang. Modularity of generating series of divisors on unitary Shimura varieties. *arXiv preprint arXiv:1702.07812*, 2017.
- [BHT11] Fedor Bogomolov, Brendan Hassett, and Yuri Tschinkel. Constructing rational curves on K3 surfaces. *Duke Math. J.*, **157**(3): 535–550, 04 2011.
- [BK01] Jan Hendrik Bruinier and Michael Kuss. Eisenstein series attached to lattices and modular forms on orthogonal groups. *Manuscripta Math.*, **106**(4): 443–459, 2001.
- [BK03] Jan Hendrik Bruinier and Ulf Kühn. Integrals of automorphic Green’s functions associated to Heegner divisors. *Int. Math. Res. Not.*, **31**: 1687–1729, 2003.
- [Bor98] Richard E. Borcherds. Automorphic forms with singularities on Grassmannians. *Invent. Math.*, **132**(3): 491–562, 1998.
- [Bor99] Richard E. Borcherds. The Gross-Kohnen-Zagier theorem in higher dimensions. *Duke Math. J.*, **97**(2): 219–233, 1999.
- [Bru02] Jan H. Bruinier. *Borcherds products on $O(2, 1)$ and Chern Classes of Heegner Divisors*, volume 1780 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 2002.
- [BT05] Fedor Bogomolov and Yuri Tschinkel. Rational curves and points on K3 surfaces. *Amer. J. Math.*, **127**(4): 825–835, 2005.
- [BY09] Jan Hendrik Bruinier and Tonghai Yang. Faltings heights of CM cycles and derivatives of L -functions. *Invent. Math.*, **177**(3): 631–681, 2009.
- [CEJ16] Edgar Costa, Andreas-Stephan Elsenhans, and Jörg Jahnel. On the distribution of the Picard ranks of the reductions of a K3 surface. *arXiv e-prints*, page arXiv:1610.07823, Oct 2016.
- [CGL19] Xi Chen, Frank Gounelas, and Christian Liedtke. Curves on K3 surfaces. *arXiv e-prints*, page arXiv:1907.01207, Jul 2019.
- [Cha14] François Charles. On the Picard number of K3 surfaces over number fields. *Algebra Number Theory*, **8**(1): 1–17, 2014.
- [Cha18] François Charles. Exceptional isogenies between reductions of pairs of elliptic curves. *Duke Math. J.*, **167**(11): 2039–2072, 08 2018.
- [Che99] Xi Chen. Rational curves on K3 surfaces. *J. Alg. Geom.*, pages 245–278, 1999.
- [CL13] Xi Chen and James D. Lewis. Density of rational curves on K3 surfaces. *Math. Ann.*, **356**(1): 331–354, 2013.

- [Con04] Brian Conrad. Gross-Zagier revisited. In *Heegner Points and Rankin L-Series*, volume 49 of *Math. Sci. Res. Inst. Publ.*, pages 67–163. Cambridge Univ. Press, Cambridge, 2004. With an appendix by W. R. Mann.
- [CT14] Edgar Costa and Yuri Tschinkel. Variation of Néron-Severi ranks of reductions of K3 surfaces. *Exp. Math.*, **23**(4): 475–481, 2014.
- [Del72] Pierre Deligne. La conjecture de Weil pour les surfaces K3. *Invent. Math.*, **15**: 206–226, 1972.
- [Del74] Pierre Deligne. La conjecture de Weil. I. *Inst. Hautes Études Sci. Publ. Math.*, **43**: 273–307, 1974.
- [Del79] Pierre Deligne. Variétés de Shimura: interprétation modulaire, et techniques de construction de modèles canoniques. In *Automorphic Forms, Representations and L-functions (Proc. Sympos. Pure Math., Oregon State Univ., Corvallis, Ore., 1977), Part 2*, Proc. Sympos. Pure Math., XXXIII, pages 247–289. Amer. Math. Soc., Providence, R.I., 1979.
- [DMOS82] Pierre Deligne, James S. Milne, Arthur Ogus, and Kuang-yeen Shih. *Hodge Cycles, Motives, and Shimura Varieties*, volume 900 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin-New York, 1982.
- [EK95] Alex Eskin and Yonatan R. Katznelson. Singular symmetric matrices. *Duke Math. J.*, **79**(2): 515–547, 1995.
- [Ger08] Larry J. Gerstein. *Basic Quadratic Forms*, volume 90 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2008.
- [GS90] Henri Gillet and Christophe Soulé. Arithmetic intersection theory. *Inst. Hautes Études Sci. Publ. Math.*, **72**:93–174 (1991), 1990.
- [Han04] Jonathan Hanke. Local densities and explicit bounds for representability by a quadratic form. *Duke Math. J.*, **124**(2): 351–388, 2004.
- [HB96] D. R. Heath-Brown. A new form of the circle method, and its application to quadratic forms. *J. Reine Angew. Math.*, **481**: 149–206, 1996.
- [HM17] B. Howard and K. Madapusi Pera. Arithmetic of Borcherds products. *ArXiv e-prints*, October 2017.
- [Hof14] Eric Hofmann. Borcherds products on unitary groups. *Math. Ann.*, **358**(3-4): 799–832, 2014.
- [Huy16] Daniel Huybrechts. *Lectures on K3 Surfaces*, volume 158 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2016.
- [Iwa97] Henryk Iwaniec. *Topics in Classical Automorphic Forms*, volume 17 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 1997.
- [Kis10] Mark Kisin. Integral models for Shimura varieties of abelian type. *J. Amer. Math. Soc.*, **23**(4): 967–1012, 2010.
- [Kis17] Mark Kisin. mod p points on Shimura varieties of abelian type. *J. Amer. Math. Soc.*, **30**(3): 819–914, 2017.
- [KM90] Stephen S. Kudla and John J. Millson. Intersection numbers of cycles on locally symmetric spaces and Fourier coefficients of holomorphic modular forms in several complex variables. *Publ. Math., Inst. Hautes Étud. Sci.*, **71**: 121–172, 1990.
- [KR00] Stephen S. Kudla and Michael Rapoport. Cycles on Siegel threefolds and derivatives of Eisenstein series. *Ann. Sci. École Norm. Sup. (4)*, **33**(5): 695–756, 2000.
- [KR14] Stephen Kudla and Michael Rapoport. Special cycles on unitary Shimura varieties II: Global theory. *J. Reine Angew. Math.*, **697**: 91–157, 2014.
- [KRY04] Stephen S. Kudla, Michael Rapoport, and Tonghai Yang. Derivatives of Eisenstein series and Faltings heights. *Compos. Math.*, **140**(4): 887–951, 2004.
- [KS67] Michio Kuga and Ichirō Satake. Abelian varieties attached to polarized K3-surfaces. *Math. Ann.*, **169**: 239–242, 1967.
- [LL12] Jun Li and Christian Liedtke. Rational curves on K3 surfaces. *Inventiones mathematicae*, **188**(3): 713–727, 2012.
- [MM83] Shigefumi Mori and Shigeru Mukai. *The uniruledness of the moduli space of curves of genus 11*. In *Algebraic Geometry (Tokyo/Kyoto, 1982)*, volume 1016 of *Lecture Notes in Math.*, pages 334–353. Springer, Berlin, 1983.
- [MP15] Keerthi Madapusi Pera. The Tate conjecture for K3 surfaces in odd characteristic. *Invent. Math.*, **201**(2): 625–668, 2015.
- [MP16] Keerthi Madapusi Pera. Integral canonical models for spin Shimura varieties. *Compos. Math.*, **152**(4): 769–824, 2016.
- [MST18] Davesh Maulik, Ananth N. Shankar, and Yunqing Tang. Reductions of abelian surfaces over global function fields. *arXiv e-prints*, page [arXiv:1812.11679](https://arxiv.org/abs/1812.11679), Dec 2018.
- [MST22] Davesh Maulik, Ananth N. Shankar, and Yunqing Tang. Picard ranks of K3 surfaces and the Hecke orbit conjecture. *Invent. Math.*, **228**(3): 1075–1143, 2022.
- [Nie10] N. Niedermowwe. The circle method with weights for the representation of integers by quadratic forms. *Zap. Nauchn. Sem. S.-Peterburg. Otdel. Mat. Inst. Steklov. (POMI)*, **377** (Issledovaniya po Teorii Chisel. 10): 91–110, 243, 2010.
- [Sar90] Peter Sarnak. *Some Applications of Modular Forms*, volume 99 of *Cambridge Tracts in Mathematics*. Cambridge University Press, Cambridge, 1990.
- [Sch68] Wolfgang M. Schmidt. Asymptotic formulae for point lattices of bounded determinant and subspaces of bounded height. *Duke Math. J.*, **35**: 327–339, 1968.
- [Sou92] C. Soulé. *Lectures on Arakelov geometry*, volume 33 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1992. With the collaboration of D. Abramovich, J.-F. Burnol and J. Kramer.
- [ST19] A. N. Shankar and Y. Tang. Exceptional splitting of reductions of abelian surfaces. *Duke Math. J.* 2019.

- [Tan90] S. G. Tankeev. Surfaces of K3 type over number fields and the Mumford-Tate conjecture. *Izv. Akad. Nauk SSSR Ser. Mat.*, **54**(4): 846–861, 1990.
- [Tan95] S. G. Tankeev. Surfaces of K3 type over number fields and the Mumford-Tate conjecture. II. *Izv. Ross. Akad. Nauk Ser. Mat.*, **59**(3): 179–206, 1995.
- [Tay20a] Salim Tayou. On the equidistribution of some Hodge loci. *J. Reine Angew. Math.*, **762**: 167–194, 2020.
- [Tay20b] Salim Tayou. Rational curves on elliptic K3 surfaces. *Math. Res. Lett.*, **27**(4): 1237–1247, 2020.
- [Tay22] Salim Tayou. Picard rank jumps for K3 surfaces with bad reduction. *arXiv e-prints*, page [arXiv:2203.09559](https://arxiv.org/abs/2203.09559), March 2022.
- [Vas08] Adrian Vasiu. Some cases of the Mumford-Tate conjecture and Shimura varieties. *Indiana Univ. Math. J.*, **57**(1): 1–75, 2008.
- [vG00] Bert van Geemen. Kuga-Satake varieties and the Hodge conjecture. In *The Arithmetic and Geometry of Algebraic cycles (Banff, AB, 1998)*, volume 548 of *NATO Sci. Ser. C Math. Phys. Sci.*, pages 51–82. Kluwer Acad. Publ., Dordrecht, 2000.
- [vG08] Bert van Geemen. Real multiplication on K3 surfaces and Kuga-Satake varieties. *Michigan Math. J.*, **56**(2): 375–399, 2008.
- [Voi02] C. Voisin. *Théorie de Hodge et géométrie algébrique complexe. Collection SMF*. Société Mathématique de France, 2002.
- [Wei49] André Weil. Numbers of solutions of equations in finite fields. *Bull. Amer. Math. Soc.*, **55**: 497–508, 1949.
- [Zyw14] David Zywina. The splitting of reductions of an abelian variety. *Int. Math. Res. Not.*, 2014(18): 5042–5083, 2014.