Annales Henri Lebesgue
5 (2022) 677-702

ANNALES
HENRI LEBESGUE

EVERETT W. HOWE

VARIATIONS IN THE DISTRIBUTION OF PRINCIPALLY POLARIZED ABELIAN VARIETIES AMONG ISOGENY CLASSES

VARIATIONS DANS LA DISTRIBUTION DES VARIÉTÉS ABÉLIENNES PRINCIPALEMENT POLARISÉES AU SEIN DES CLASSES D'ISOGÉNIE

Abstract. — We show that for a large class of rings R, the number of principally polarized abelian varieties over a finite field in a given simple ordinary isogeny class and with endomorphism ring R is equal either to 0, or to a ratio of class numbers associated to R, up to some small computable factors. This class of rings includes the maximal order of the CM field K associated to the isogeny class (for which the result was already known), as well as the order R generated over $\mathbf{Z}$ by Frobenius and Verschiebung.

For this latter order, we can use results of Louboutin to estimate the appropriate ratio of class numbers in terms of the size of the base field and the Frobenius angles of the isogeny class. The error terms in our estimates are quite large, but the trigonometric terms in the estimate are suggestive: Combined with a result of Vlăduţ on the distribution of Frobenius angles of isogeny classes, they give a heuristic argument in support of the theorem of Katz and Sarnak on the limiting distribution of the multiset of Frobenius angles for principally polarized abelian varieties of a fixed dimension over finite fields.

Keywords: Abelian variety, Frobenius eigenvalue, distribution, isogeny, complex multiplication, Katz–Sarnak.
2020 *Mathematics Subject Classification:* 11G10, 11G15, 11G25, 14G15, 14K15, 14K22.
DOI: `https://doi.org/10.5802/ahl.133`

Résumé. — Nous montrons que pour une grande classe d'anneaux R, le nombre de variétés abéliennes principalement polarisées sur un corps fini dans une classe d'isogénie ordinaire simple avec un anneau d'endomorphismes R est égal soit à 0, soit à un rapport de nombres de classes associés à R, à quelques petits facteurs calculables près. Cette classe d'anneaux comprend l'ordre maximal du corps CM K associé à la classe d'isogénie (ce résultat était déjà connu), ainsi que l'ordre R engendré sur $\mathbf{Z}$ par le Frobenius et le Verschiebung.

Pour ce dernier ordre, on peut utiliser les résultats de Louboutin pour estimer la rapport approprié des nombres de classes en fonction de la taille du corps de base et des angles de Frobenius de la classe d'isogénie. Les termes d'erreur dans nos estimations sont assez grands, mais les termes trigonométriques de l'estimée sont suggestifs : combinés avec un résultat de Vlăduţ sur la distribution des angles de Frobenius dans les classes d'isogénie, elles donnent une explication heuristique du théorème de Katz et Sarnak sur la distribution limite du multi-ensemble des angles de Frobenius pour les variétés abéliennes principalement polarisées de dimension fixée sur les corps finis.)

1. Introduction

In this paper we consider the problem of estimating the number of isomorphism classes of principally polarized abelian varieties (A,λ) such that A lies in a given isogeny class of simple ordinary abelian varieties over a finite field. We approach this problem by subdividing isogeny classes into their *strata*, which are the subsets of an isogeny class consisting of abelian varieties sharing the same endomorphism ring. (To avoid awkward locutions, we will say that a principally polarized variety (A,λ) lies in an isogeny class $\mathcal{C}$ or a stratum $\mathcal{S}$ when A lies in $\mathcal{C}$ or $\mathcal{S}$.)

Our main result concerns strata corresponding to endomorphism rings R that are *convenient*. A convenient ring is an order in a CM field with the properties that, first, R is stable under complex conjugation; second, the maximal real subring R^+ of R is Gorenstein; and third, the trace dual of R is generated by its pure imaginary elements. (We explain these terms and present results on convenient rings in Section 2.) If $\mathcal{S}$ is a stratum of an isogeny class corresponding to a convenient order R, we can express the number of principally polarized varieties in $\mathcal{S}$ in terms of the sizes of the Picard group of R and the narrow Picard group of the maximal real subring R^+ of R; the definitions of these groups are also reviewed in Section 2.

Theorem 1.1. — *Let $\mathcal{S}$ be a stratum of an isogeny class of simple ordinary abelian varieties over a finite field, corresponding to an endomorphism ring R. Suppose that R is convenient and that the norm map N_{Pic} from the Picard group of R to the narrow Picard group of R^+ is surjective. Let U be the unit group of R and let $U^+_{>0}$ be the group of totally positive units of R^+. Then the number of varieties $A\in\mathcal{S}$ that have principal polarizations is equal to $\#\ker N_{\mathrm{Pic}}$, and each such A has $[U^+_{>0} : N(U)]$ principal polarizations up to isomorphism, where N is the norm map from R to R^+.*

Corollary 1.2. — *Under the hypotheses of Theorem 1.1, the total number of principally polarized varieties (A,λ) in the stratum $\mathcal{S}$, counted up to isomorphism, is equal to*

$$\frac{1}{[N(U) : (U^+)^2]}\,\frac{\#\operatorname{Pic} R}{\#\operatorname{Pic} R^+},$$

where U is the unit group of R and U^+ is the unit group of R^+. Furthermore, the index $[N(U) : (U^+)^2]$ is equal to either 1 or 2, and is equal to 1 if K/K^+ is ramified at an odd prime.

In Section 4 we prove these two results and give some reasonably weak sufficient condition for N_{Pic} to be surjective. Special cases of these results are known already; in the most fundamental case, when R is a maximal order, these results can be obtained from the work of Shimura and Taniyama [ST61, § 14], combined with the theory of canonical lifts. Other examples occur, for instance, in [LPP02, § 8], [How04, Proposition 2, p. 583], and [IT20, Lemma 19]. But none of the previous results we are aware of apply as generally as Theorem 1.1 and Corollary 1.2.

To every n-dimensional abelian variety A over $\mathbf{F}_q$ one associates its characteristic polynomial of Frobenius f_A, sometimes called the *Weil polynomial* of A. This is a polynomial of degree $2n$, whose multiset of complex roots can be written in the form

$$\left\{\sqrt{q}e^{\pm i\theta_j}\right\}_{j=1}^{n}$$

for an n-tuple $s_A = (\theta_1, \ldots, \theta_n)$ of real numbers, the *Frobenius angles* of A, normalized so that[(1)]

$$0 \leqslant \theta_1 \leqslant \theta_2 \leqslant \cdots \leqslant \theta_n \leqslant \tau/2. \tag{1.1}$$

The theorem of Honda and Tate [Tat71, Théorème 1, p. 96] gives a complete description of the set of Weil polynomials. In particular, Tate showed that two abelian varieties over $\mathbf{F}_q$ are isogenous if and only if they share the same Weil polynomial [Tat66], so it makes sense to speak of the Weil polynomial of an isogeny class. We see that an isogeny class of abelian varieties over a finite field is determined by its Weil polynomial, by the multiset of roots of its Weil polynomial, and by the multiset of its Frobenius angles. For simple ordinary isogeny classes, all of the inequalities in (1.1) are strict.

We will see (Corollary 3.2) that the ring R generated over $\mathbf{Z}$ by the Frobenius and Verschiebung of a simple ordinary abelian variety A is convenient. We call this ring the *minimal ring* of the isogeny class of A, because every endomorphism ring of a variety in $\mathcal{C}$ contains R, and there are varieties in $\mathcal{C}$ with endomorphism ring equal to R [Wat69, Theorem 6.1, pp. 550–551]. We call the corresponding stratum the *minimal stratum* of the isogeny class. Using results of Louboutin, we can (somewhat crudely) estimate the number of principally polarized varieties in the minimal stratum in terms of the Frobenius angles of the isogeny class. Our theorem uses the following notation: If $\{a_m\}$ and $\{b_m\}$ are two infinite sequences of positive real numbers indexed by integers m, we write $a_m \approxeq b_m$ to mean that for every $\varepsilon > 0$ there are positive constants r and s such that $b_m \leqslant r a_m^{1+\varepsilon}$ and $a_m \leqslant s b_m^{1+\varepsilon}$ for all m.

Theorem 1.3. — *Fix an integer $n > 0$. For each positive integer m, let $\mathcal{C}_m$ be an isogeny class of simple n-dimensional ordinary abelian varieties over a finite field $\mathbf{F}_{q_m}$, and let R_m and $\mathcal{S}_m$ be the minimal ring and minimal stratum for $\mathcal{C}_m$. For each m,*

[(1)] Note: Throughout this paper we use τ to denote the ratio of the circumference of a circle to its radius. We express values in terms of τ not to take sides in a philosophical dispute, but simply because we reserve π for denoting a root of a Weil polynomial.

let $\{\theta_{m,i}\}_{i=1}^{n}$ be the Frobenius angles for $\mathcal{C}_m$. Let P_m be the number of principally polarized varieties in $\mathcal{S}_m$. If $q_m \to \infty$ and if each norm map $\operatorname{Pic} R_m \to \operatorname{Pic}^+ R_m^+$ *is surjective, then*

$$P_m \approxeq q_m^{n(n+1)/4} \prod_{i<j} (\cos\theta_{m,i} - \cos\theta_{m,j}) \prod_i \sin\theta_{m,i}.$$

The relation indicated by the $\approxeq$ symbol is a *very* rough comparison of magnitudes, and indeed, if there is an ε such that $|\theta_{m,i} - \theta_{m,j}| > \varepsilon$ and $|\sin\theta_{m,i}| > \varepsilon$ for all m, i, and j, then the conclusion of the theorem is equivalent to saying simply that $P_m \approxeq q_m^{n(n+1)/4}$. However, if the Frobenius angles of the sequence of isogeny classes do *not* stay a bounded distance from one another and from 0 and $\tau/2$, then the trigonometric factors on the right hand side of the relation do make a difference. We will see examples of this in Section 7.

The trigonometric factors in Theorem 1.3 may have only a tenuous influence on the asymptotic predictions of the theorem, but they provided a key motivation for this work. To explain this, let us consider another approach toward estimating the number of principally polarized abelian varieties in an isogeny class, an approach that considers the question in terms of limiting distributions.

It is well-known that for a fixed positive integer n, the number of principally polarized n-dimensional abelian varieties over a finite field $\mathbf{F}_q$ grows like

$$2q^{n(n+1)/2}$$

as $q \to \infty$, in the sense that the ratio between the two quantities tends to 1; this follows simply from the existence of an irreducible $n(n+1)/2$-dimensional coarse moduli space for these abelian varieties, together with the fact that generically a principally polarized abelian variety over a finite field has two twists. On the other hand, the number of isogeny classes of n-dimensional abelian varieties over $\mathbf{F}_q$ grows like

$$v_n \frac{\varphi(q)}{q} q^{n(n+1)/4} \tag{1.2}$$

as $q \to \infty$, where φ is Euler's totient function and where

$$v_n = \frac{2^n}{n!} \prod_{j=1}^{n} \left(\frac{2j}{2j-1}\right)^{n+1-j} \tag{1.3}$$

(see [DH98, Theorem 1.1, p. 427]). It follows that the average number of principally polarized varieties per isogeny class is

$$\frac{2q}{v_n \varphi(q)} q^{n(n+1)/4}.$$

But there is finer information available. To explain this, we require some notation.

Let S_n be the space of all n-tuples (θ_j) of real numbers satisfying (1.1). There is a map from $\mathrm{USp}_{2n}(q)$ to S_n that sends a symplectic matrix M to the multiset of the arguments of the eigenvalues of M. The Haar measure on $\mathrm{USp}_{2n}(q)$ gives rise to a measure μ_n on S_n; this measure is determined by

$$d\mu_n = c_n \prod_{i<j} (\cos\theta_i - \cos\theta_j)^2 \prod_i \sin^2\theta_i \, d\theta_1 \cdots d\theta_n, \tag{1.4}$$

where $c_n = 2^{n(n+1)}/\tau^n$, so that $\mu_n(S_n) = 1$. (The value of c_n is provided by Weyl [Wey97, Theorem 7.8.B, p. 218]; to see this, one must keep in mind that Weyl's variables φ_i are related to our θ_i by $\theta_i = \tau\varphi_i$, and his functions $c(\varphi)$ and $s(\varphi)$ are given by $c(\varphi) = 2\cos(\tau\varphi)$ and $s(\varphi) = 2\sqrt{-1}\sin(\tau\varphi)$ [Wey97, pp. 180, 217].)

We also get a measure on S_n from the principally polarized n-dimensional abelian varieties over $\mathbf{F}_q$: For every open set U of S_n, we set

$$\mu_{n,q}(U) = c_{n,q} \cdot \#\left\{\text{principally polarized } (A,\lambda) \text{ such that } s_A \in U\right\},$$

where $1/c_{n,q}$ is the total number of principally polarized n-dimensional abelian varieties (A,λ) over $\mathbf{F}_q$, so that $\mu_{n,q}(S_n) = 1$. Katz and Sarnak [KS99, Theorem 11.3.10, p. 330] proved the following:

Theorem 1.4 (Katz–Sarnak). — *Fix a positive integer n. As $q \to \infty$ over the prime powers, the measures $\mu_{n,q}$ converge in measure to μ_n.*

By considering isogeny classes $\mathcal{C}$ of n-dimensional abelian varieties, we get another family of measures. Given any isogeny class $\mathcal{C}$, we let $s_{\mathcal{C}}$ be the n-tuple s_A for any A in $\mathcal{C}$. Given a prime power q, we define a measure $\nu_{n,q}$ on S_n by setting

$$\nu_{n,q}(U) = d_{n,q} \cdot \#\left\{\text{isogeny classes } \mathcal{C} \text{ such that } s_{\mathcal{C}} \in U\right\},$$

where $1/d_{n,q}$ is the total number of isogeny classes of n-dimensional abelian varieties over $\mathbf{F}_q$, so that $\nu_{n,q}(S_n) = 1$. Vlăduţ [Vlă01, Theorem A, p. 128] proved that the $\nu_{n,q}$ have a limiting distribution as well:

Theorem 1.5 (Vlăduţ). — *Fix a positive integer n. As $q \to \infty$ over the prime powers, the measures $\nu_{n,q}$ converge in measure to the measure ν_n defined by*

$$d\nu_n = d_n \prod_{i<j} (\cos\theta_i - \cos\theta_j) \prod_i \sin\theta_i \, d\theta_1 \cdots d\theta_n, \tag{1.5}$$

where

$$d_n = \frac{2^{n(n+1)/2}}{v_n} = 2^{n(n-1)/2}\, n! \prod_{j=1}^{n} \left(\frac{2j-1}{2j}\right)^{n+1-j}.$$

Consider what this means for a region $U \subset S_n$ contained within a small disk around an n-tuple (α_i), where we assume that the α_i are distinct and that none of them is equal to 0 or $\tau/2$. Suppose U has volume u, with respect to the measure $d\theta_1 \cdots d\theta_n$. For large q, the number of isogeny classes with Frobenius angles in U is $\nu_{n,q}(U)/d_{n,q}$, and using Equations (1.2) and (1.3) we see that this is roughly equal to

$$\begin{aligned}\frac{1}{d_{n,q}}\nu_n(U) &\approx \frac{d_n}{d_{n,q}} u \prod_{i<j} (\cos\alpha_i - \cos\alpha_j) \prod_i \sin\alpha_i \\ &\approx 2^{n(n+1)/2} u \frac{\varphi(q)}{q} q^{n(n+1)/4} \prod_{i<j} (\cos\alpha_i - \cos\alpha_j) \prod_i \sin\alpha_i.\end{aligned}$$

On the other hand, the number of principally polarized abelian varieties with Frobenius angles in U is $\mu_{n,q}(U)/c_{n,q}$, which is roughly

$$2q^{n(n+1)/2}\mu_n(U) \approx 2q^{n(n+1)/2} \frac{2^{n(n+1)}}{\tau^n} u \prod_{i<j} (\cos\alpha_i - \cos\alpha_j)^2 \prod_i \sin^2\alpha_i.$$

Therefore, for the isogeny classes with Frobenius angles in U, the average number of principally polarized varieties per isogeny class is roughly

$$\frac{2^{\left(n^2+n+2\right)/2}}{\tau^n}\frac{q}{\varphi(q)}q^{n(n+1)/4}\prod_{i<j}(\cos\alpha_i-\cos\alpha_j)\prod_i\sin\alpha_i. \tag{1.6}$$

Conversely, estimates for the number of principally polarized varieties in a given isogeny class — estimates like our Theorem 1.3 — can be combined with Vlăduţ's result to give a heuristic explanation of the Katz–Sarnak theorem. This line of reasoning was the initial motivation that led to the present work. It is especially suggestive that the trigonometric factors in the expression (1.6) match the those that appear in Theorem 1.3.

A special case of this type of heuristic argument, which is perhaps familiar to some readers, concerns elliptic curves. The case $n=1$ of Theorem 1.4 was proven by Birch [Bir68]. To every elliptic curve $E/\mathbf{F}_q$ we can associate its trace of Frobenius t, which lies in the interval $[-2\sqrt{q},2\sqrt{q}]$. Dividing the trace by $2\sqrt{q}$, we get a *normalized trace* that lies in the interval $[-1,1]$. For each q we can consider the counting measure on $[-1,1]$ that tells us what fraction of the elliptic curves over $\mathbf{F}_q$ have their normalized traces lying in a given set. Birch proved that these counting measures converge in measure to the "semicircular" measure, that is, the measure associated to the differential $(4/\tau)\sqrt{1-x^2}\,dx$. (This is equivalent to the measure $\mu_1=(4/\tau)\sin^2\theta\,d\theta$ on S_1, since $x=\cos\theta$.)

Now, if t is an integer in the interval $[-2\sqrt{q},2\sqrt{q}]$ and if $(t,q)=1$, then the number of elliptic curves over $\mathbf{F}_q$ with trace t is $H(t^2-4q)$, where H denotes the Kronecker class number. But $H(-n)$ grows roughly as $\sqrt{n}$; more precisely, for every $\varepsilon>0$ there are positive constants c and d such that

$$cn^{1/2-\varepsilon}<H(-n)<dn^{1/2+\varepsilon}$$

for all positive $n\equiv 0,3 \bmod 4$, so that $H(-n)\approxeq n^{1/2}$ for these n (compare [Len87, Proposition 1.8, p. 656]), and the average value of $H(-n)/\sqrt{n}$ for discriminants n in quite small intervals is $\tau/12$ (see [Byk97, Theorem 2, p. 722]). Thus it seems reasonable to expect that the number of elliptic curves over $\mathbf{F}_q$ with trace t will be about $c\sqrt{4q-t^2}$ on average, for some constant c. Scaling this down, we find that for any x in $[-1,1]$, we expect there to be about $c'\sqrt{1-x^2}\,\Delta x$ elliptic curves over $\mathbf{F}_q$ having scaled traces in a small interval of size Δx near x. As q increases the constant c' will have to tend to $4/\tau$, and we find that we are led to believe that the counting measures should converge to the semicircular measure.

(Gekeler [Gek03] shows how the crude approximation that "$H(-n)$ grows like $\sqrt{n}$" can be modified with local factors in order to make this interpretation of Birch's result more rigorous, at least in the case of finite prime fields. Achter and Gordon [AG17] provide an alternate explanation for Gekeler's work, and extend it to arbitrary finite fields.)

Unfortunately, there seems to be little hope of turning this heuristic argument into an actual proof of Theorem 1.4. We find it interesting, nevertheless, that the trigonometric factors in the measure given by Equation (1.4) get split evenly between the measure defined by Equation (1.5) and the approximation in Theorem 1.3.

The referee notes that some of the expressions in the Frobenius angles θ_i of an isogeny class that appear in this paper would be simplified if they were rewritten in terms of the coefficients of what we might call the *scaled real Weil polynomial* of the isogeny class — that is, the monic polynomial in $\mathbf{R}[x]$ whose roots are $2\cos\theta_i$. This is indeed true; nevertheless, we have chosen to express our results in terms of Frobenius angles because their use is fairly well-established in the literature on measures associated to abelian varieties.

The structure of this paper is as follows: In Section 2 we explore the properties of convenient orders, give some examples, and define a norm map from the invertible ideals of a convenient order to the invertible ideals of its real subring. In Section 3 we look at convenient orders related to isogeny classes of abelian varieties. In Section 4 we use Deligne's equivalence [Del69] between the category of ordinary abelian varieties over a finite field and the category of Deligne modules [How95] to prove Theorem 1.1 and Corollary 1.2. In Section 5 we review a theorem of Louboutin [Lou06] on minus class numbers of CM fields and extend it to apply to convenient orders. We apply the theorem to the minimal orders of isogeny classes and obtain Theorem 1.3. In Section 6 we give some examples that show that while the *average* number of principally polarized varieties in a given isogeny class is given by Equation (1.6), there are isogeny classes for which this number is significantly larger than the average value. Finally, in Section 7 we give examples showing that the trigonometric terms in Theorem 1.3 are necessary.

Acknowledgments

The basic ideas in this paper first appeared in an email (reproduced as the appendix to [How20]) written by the author to Nick Katz in the year 2000, the contents of which have been shared with a number of researchers over the years and presented in several conference and seminar talks. The author is grateful to Jeff Achter for his continued interest in this work and for his encouragement to write it down more formally. Jeff Achter and Stefano Marseglia had helpful comments on an early draft of this paper, and Marseglia suggested Proposition 2.2, which allowed for a simplification in the definition of convenient orders; the author thanks them both for their help and kindness. Finally, the author thanks the referee for their suggestions and careful reading.

2. Convenient orders

In this section we define convenient orders and prove some results about them. The definition involves the concept of *Gorenstein rings*. Most of what we will need to know about Gorenstein rings can be found in the paper of Picavet-L'Hermitte [PL87]. In particular, we will use the following facts:

(1) An order R in a number field K is Gorenstein if and only if its trace dual is invertible as a fractional R-ideal [PL87, Proposition 4, p. 20], [BL94, Proposition 2.7, p. 230]; here the *trace dual* $R^\dagger$ of R is the set of elements $x \in K$ such that $\operatorname{Tr}_{K/\mathbf{Q}}(xR) \subseteq \mathbf{Z}$.

(2) An order R in a number field K is Gorenstein if and only if every fractional R-ideal $\mathfrak{A}$ with $\operatorname{End}\mathfrak{A} = R$ is invertible [PL87, Proposition 4, p. 20], [BL94, Proposition 2.7, p. 230].
(3) A ring that is a complete intersection over $\mathbf{Z}$ is Gorenstein [Mat86, Theorem 21.3, p. 171], and in particular every monogenic order $\mathbf{Z}[\alpha]$ is Gorenstein [BL94, Example 2.8, p. 231].

Let K be a CM field, that is, a totally imaginary quadratic extension of a totally real number field K^+. We refer to the nontrivial involution $x \mapsto \bar{x}$ of K/K^+ as *complex conjugation*, and we say that an element of K is *pure imaginary* if it is negated by complex conjugation.

Definition 2.1. — *We call an order R in K* convenient *if it satisfies the following properties:*
(1) *R is stable under complex conjugation;*
(2) *the order $R^+ := R \cap K^+$ of K^+ is Gorenstein;*
(3) *the trace dual $R^\dagger$ of R is generated (as a fractional R-ideal) by its pure imaginary elements.*

We call the ring R^+ from property (2) the real subring *of R.*

Proposition 2.2. — *Every convenient order is Gorenstein.*

Proof. — Let ι be a pure imaginary element of R. By assumption $R^\dagger$ is generated by its pure imaginary elements, so $\iota^{-1}R^\dagger = (\iota R)^\dagger$ is generated by its totally real elements. Since clearly $(\iota R : \iota R) = R$ we have $((\iota R)^\dagger : (\iota R)^\dagger) = R$. Let I be the fractional R^+-ideal $(\iota R)^\dagger \cap K^+$. Then $IR = (\iota R)^\dagger$ because $(\iota R)^\dagger$ is generated by its totally real elements, and since $((\iota R)^\dagger : (\iota R)^\dagger) = R$ we must have $(I : I) = R^+$. By assumption, R^+ is Gorenstein, and therefore I is invertible, so there is a fractional R^+-ideal J with $IJ = R^+$. Then we have $(IR)(JR) = R$, so $IR = (\iota R)^\dagger$ is an invertible fractional R-ideal. It follows that $R^\dagger$ is invertible, so R is Gorenstein. □

Proposition 2.3. — *The maximal order $\mathcal{O}$ of K is convenient.*

Proof. — The maximal order $\mathcal{O}$ clearly is stable under complex conjugation, and the real subring $\mathcal{O}^+$ is the maximal order of K^+. Maximal orders are Gorenstein (because their trace duals are invertible), so $\mathcal{O}$ satisfies the first two conditions of Definition 2.1. For the third, we note that the trace dual of $\mathcal{O}$ is generated by pure imaginary elements if and only if its inverse — the different of $\mathcal{O}$ — is generated by pure imaginary elements. Now, the different of $\mathcal{O}$ is the product of the different of $\mathcal{O}^+$ and the relative different of $\mathcal{O}$ over $\mathcal{O}^+$, so it suffices to show that the relative different can be generated by pure imaginary elements. We know ([Nar04, Theorem 4.16, p. 151], [Neu99, Theorem 2.5, p. 198]) that the relative different is generated by the elements $f'_\alpha(\alpha)$ for all $\alpha \in \mathcal{O} \setminus \mathcal{O}^+$, where f_α is the minimal polynomial of α over K^+ and f'_α is the derivative of f_α. But $f'_\alpha(\alpha)$ is equal to $\alpha - \bar{\alpha}$, which is clearly pure imaginary. □

Proposition 2.4. — *Let R be an order in K that is stable under complex conjugation and whose real subring R^+ is Gorenstein. If there are elements α and β of K and invertible fractional ideals $\mathfrak{A}$ and $\mathfrak{B}$ of R^+ such that $R = \mathfrak{A}\alpha \oplus \mathfrak{B}\beta$, then R is convenient.*

Proof. — By hypothesis, R satisfies the first two conditions in Definition 2.1, so we need only check the third.

The trace dual of R is the product of the trace dual of R^+ with the relative trace dual $\mathfrak{D}$ of R over R^+. The trace dual of R^+ is obviously generated by totally real elements, so we just need to check that $\mathfrak{D}$ is generated by pure imaginary elements.

Set

$$\alpha^* = \frac{\bar{\beta}}{\alpha\bar{\beta} - \bar{\alpha}\beta} \quad \text{and} \quad \beta^* = \frac{\bar{\alpha}}{\beta\bar{\alpha} - \bar{\beta}\alpha}.$$

We note that

$$\mathrm{Tr}_{K/K^+}(\alpha\alpha^*) = \mathrm{Tr}_{K/K^+}(\beta\beta^*) = 1 \quad \text{and} \quad \mathrm{Tr}_{K/K^+}(\alpha\beta^*) = \mathrm{Tr}_{K/K^+}(\beta\alpha^*) = 0,$$

so the relative trace dual $\mathfrak{D}$ of R is given by

$$\mathfrak{D} = \mathfrak{A}^{-1}\alpha^* \oplus \mathfrak{B}^{-1}\beta^*$$

and we have

$$\left(\alpha\bar{\beta} - \bar{\alpha}\beta\right)\mathfrak{A}\mathfrak{B}\mathfrak{D} = \mathfrak{A}\bar{\alpha} \oplus \mathfrak{B}\bar{\beta} = \bar{R} = R.$$

Since $\mathfrak{A}$ and $\mathfrak{B}$ are fractional R^+-ideals and $\alpha\bar{\beta} - \bar{\alpha}\beta$ is pure imaginary, we see that $\mathfrak{D}$ is generated as a fractional R-ideal by pure imaginary elements. □

We close this section by showing that there is a natural norm map from the invertible ideals of a convenient order to the invertible ideals of its real subring. We prove the statement in a more general context.

Lemma 2.5. — *Let L/K be a quadratic extension of number fields, with nontrivial involution $x \mapsto \bar{x}$. Let S be an order of L that is stable under the involution, and let $R = S \cap K$. For every invertible fractional ideal $\mathfrak{B}$ of S, there is a unique invertible fractional ideal $\mathfrak{A}$ of R such that $\mathfrak{A} \otimes_R S = \mathfrak{B}\bar{\mathfrak{B}}$.*

We call the ideal $\mathfrak{A}$ the *norm* of $\mathfrak{B}$. Our proof of the lemma follows ideas in [LPP02, § 6].

Proof of Lemma 2.5. — Let $\widehat{\mathbf{Z}} := \varprojlim \mathbf{Z}/n\mathbf{Z} \cong \prod_p \mathbf{Z}_p$ be the profinite completion of the ring $\mathbf{Z}$, and for an arbitrary ring E let $\widehat{E}$ denote the tensor product $E \otimes_{\mathbf{Z}} \widehat{\mathbf{Z}}$. For our order S we find that $\widehat{S} \cong \prod_{\mathfrak{q}} S_{\mathfrak{q}}$, where the product is over the primes $\mathfrak{q}$ of S and where $S_{\mathfrak{q}}$ is the completion of S at $\mathfrak{q}$. Similarly, $\widehat{L} \cong \mathbf{Q} \otimes_{\mathbf{Z}} \widehat{S}$ is the subring of $\prod_{\mathfrak{q}} L_{\mathfrak{q}}$ consisting of those elements all but finitely many of whose components lie in $S_{\mathfrak{q}}$. Finally, the group $\widehat{S}^*$ is the product $\prod_{\mathfrak{q}} S_{\mathfrak{q}}^*$, and the group $\widehat{L}^*$ is the subgroup of $\prod_{\mathfrak{q}} L_{\mathfrak{q}}^*$ consisting of those elements all but finitely many of whose components lie in $S_{\mathfrak{q}}^*$.

The invertible ideals of S are the ideals that are locally principal [Neu99, Proposition 12.4, p. 74], so one sees that the group of invertible ideals of S is isomorphic to the quotient $\widehat{L}^*/\widehat{S}^*$. Likewise, the group of invertible ideals of R is isomorphic to $\widehat{K}^*/\widehat{R}^*$.

The field norm $L \to K$ induces a norm map from $\widehat{L}^*/\widehat{S}^*$ to $\widehat{K}^*/\widehat{R}^*$, and under the isomorphisms just described, this gives us a norm map from the invertible ideals of S to those of R. Since the composition of the field norm $L \to K$ with the inclusion $K \to L$ is given by $x \to x\bar{x}$, we see that the norm $\mathfrak{A}$ of an invertible S-ideal $\mathfrak{B}$

satisfies $\mathfrak{A} \otimes_R S = \mathfrak{B}\bar{\mathfrak{B}}$. The norm is the unique ideal with this property, because if there were another invertible ideal of R that lifted to $\mathfrak{B}\bar{\mathfrak{B}}$, the quotient of $\mathfrak{A}$ by this other ideal would be a nontrivial ideal $\mathfrak{C}$ such that $\mathfrak{C} \otimes_R S = S$. We would then have $\mathfrak{C} \subseteq R$, and also that $\mathfrak{C}$ contains a unit of S. This unit would then also be a unit of R, so $\mathfrak{C} = R$, contradicting the nontriviality of $\mathfrak{C}$. □

Remark 2.6. — Let R be a convenient order. Recall that the *Picard group* $\operatorname{Pic} R$ of R is the group of isomorphism classes of invertible R-ideals. The *narrow Picard group* $\operatorname{Pic}^+ R^+$ of the real order R^+ is the group of strict isomorphism classes of invertible R^+-ideals, where two invertible R^+-ideals $\mathfrak{A}$ and $\mathfrak{B}$ are said to be *strictly isomorphic* if there is a totally positive element x of K^+ such that $x\mathfrak{A} = \mathfrak{B}$. The norm map on invertible ideals gives us a homomorphism N_{Pic} from $\operatorname{Pic} R$ to $\operatorname{Pic}^+ R^+$, which we continue to call the norm.

3. Isogeny classes and convenient orders

In this section we show that some rings associated to a simple ordinary isogeny class of abelian varieties over a finite field are convenient.

Suppose that $\mathcal{C}$ is an isogeny class of simple n-dimensional ordinary abelian varieties over a finite field k with q elements, and let f be its Weil polynomial. Honda–Tate theory shows that f has degree $2n$ and is irreducible, and that the number field K defined by f is a CM field. Let K^+ be the maximal real subfield of K, and let π be a root of f in K.

Proposition 3.1. — *Let B be a Gorenstein order in K^+ that contains $\pi + \bar{\pi}$. Then the ring $R = B[\pi]$ is convenient.*

Proof. — The minimal polynomial of π over K^+ is $x^2 - (\pi + \bar{\pi})x + q$, so 1 and π form a basis for R as a B-module. It follows easily that R is stable under complex conjugation and that $R^+ = B$. The result follows from Proposition 2.4. □

Corollary 3.2. — *The order $R = \mathbf{Z}[\pi, \bar{\pi}]$ of K is convenient.*

Proof. — It is not hard to show that one basis for R as a $\mathbf{Z}$-module is

$$\left\{1, \pi, \bar{\pi}, \pi^2, \bar{\pi}^2, \ldots, \pi^{n-1}, \bar{\pi}^{n-1}, \pi^n\right\},$$

and from this one sees that $R^+ = \mathbf{Z}[\pi + \bar{\pi}]$. The ring R^+ is Gorenstein because it is integral over $\mathbf{Z}$ and monogenic. The corollary follows from Proposition 3.1. □

Example 3.3. — Here we give an example that shows that condition (3) of Definition 2.1 does not follow from conditions (1) and (2), even if we assume that the ring R is Gorenstein.

Let $p = 19$ and let f be the ordinary irreducible Weil polynomial $x^4 - 4x^3 + 10x^2 - 4px + p^2$, corresponding to an isogeny class of abelian surfaces over $\mathbf{F}_p$. One checks that $\pi + \bar{\pi} = 2 + 4\sqrt{2}$ for a choice of $\sqrt{2}$ in K. Let R be the $\mathbf{Z}$-module generated by

$$1, \quad 2\sqrt{2}, \quad \frac{\pi - \bar{\pi}}{2}, \quad \text{and} \quad \frac{(\pi - \bar{\pi})\sqrt{2}}{2}.$$

Using the fact that $(\pi - \bar{\pi})^2/4 = -10 + 4\sqrt{2}$, we see that R is closed under multiplication and is therefore a ring.

It is clear that R is stable under complex conjugation, and that $R^+ = \mathbf{Z}[2\sqrt{2}]$. The ring R^+ is Gorenstein because it is monogenic. Thus R satisfies conditions (1) and (2).

We compute that $R^\dagger$ is the $\mathbf{Z}$-module generated by

$$\frac{1}{4}, \quad \frac{\sqrt{2}}{16}, \quad \frac{1}{2\,(\pi - \bar{\pi})}, \quad \text{and} \quad \frac{\sqrt{2}}{4\,(\pi - \bar{\pi})}.$$

The pure imaginary elements of $R^\dagger$ are the elements of the $\mathbf{Z}$-module generated by

$$\frac{1}{2\,(\pi - \bar{\pi})} \quad \text{and} \quad \frac{\sqrt{2}}{4\,(\pi - \bar{\pi})}.$$

The R-module generated by these elements is spanned as a $\mathbf{Z}$-module by

$$\frac{1}{4}, \quad \frac{\sqrt{2}}{8}, \quad \frac{1}{2\,(\pi - \bar{\pi})}, \quad \text{and} \quad \frac{\sqrt{2}}{4\,(\pi - \bar{\pi})},$$

and this has index 2 in $R^\dagger$. Thus, R does not satisfy condition (3) of Definition 2.1, even though it satisfies conditions (1) and (2). Furthermore, R is Gorenstein: If we let Λ be the $\mathbf{Z}$-module generated by $32 - 40\sqrt{2}$, $136\sqrt{2}$, $8(\pi - \bar{\pi})$, and $4\sqrt{2}(\pi - \bar{\pi})$, then Λ is an R-module and $R^\dagger\Lambda = R$, so $R^\dagger$ is an invertible fractional R-ideal. □

4. Principally polarized varieties and ratios of class numbers

In this section we will prove Theorem 1.1 and Corollary 1.2, and we give some conditions under which the norm map from $\operatorname{Pic} R$ to $\operatorname{Pic}^+ R^+$ is surjective. Throughout the section we continue to use the notation set at the beginning of Section 3: k is a finite field with q elements, $\mathcal{C}$ is an isogeny class of simple n-dimensional ordinary abelian varieties over k, f is the Weil polynomial for $\mathcal{C}$ (and is irreducible and of degree $2n$), K is the CM field defined by f, K^+ is its maximal real subfield, and π is a root of f in K.

Before we begin the proof of Theorem 1.1, let us make one comment on the restriction to strata corresponding to convenient orders. If A is an abelian variety in $\mathcal{C}$ and if A has a principal polarization, then $\operatorname{End} A$ is stable under complex conjugation because the Rosati involution on $(\operatorname{End} A) \otimes \mathbf{Q} = K$ associated to a principal polarization takes $\operatorname{End} A$ to itself, and the only positive involution on K is complex conjugation. Thus, every stratum of $\mathcal{C}$ that contains a principally polarized variety must correspond to an endomorphism ring R which satisfies condition (1) of Definition 2.1. In general, however, $\operatorname{End} A$ need not be convenient.

Proof of Theorem 1.1. — To understand the category of abelian varieties in the ordinary isogeny class $\mathcal{C}$, we turn to the theory of Deligne modules and their polarizations as set forth in [How95], based on Deligne's equivalence of categories [Del69] between ordinary abelian varieties over a finite field and a certain category of modules.

Deligne's equivalence of categories involves picking an embedding of the Witt vectors over $\bar{k}$ into the complex numbers $\mathbf{C}$, and this embedding determines a p-adic valuation v on the algebraic numbers in $\mathbf{C}$. We let

$$\Phi = \{\varphi\colon K \to \mathbf{C} \mid v(\varphi(\pi)) > 0\}$$

so that Φ is a *CM type*, that is, a choice of half of all the embeddings of K into $\mathbf{C}$, one from each complex-conjugate pair.

Following [How95], we see that the abelian varieties A in $\mathcal{S}$ correspond via Deligne's equivalence to the classes of fractional ideals $\mathfrak{A}$ of R with $\operatorname{End}\mathfrak{A} = R$, and since R is Gorenstein these are precisely the classes of invertible fractional R-ideals. According to [How95], if A corresponds to (the class of) an ideal $\mathfrak{A}$, then the dual $\widehat{A}$ of A corresponds to (the class of) the complex conjugate of the trace dual of $\mathfrak{A}$. Let $\mathfrak{d}$ be the different of R; since R is stable under complex conjugation, so is $\mathfrak{d}$. The trace dual of an invertible R-ideal $\mathfrak{A}$ is $\mathfrak{d}^{-1}\mathfrak{A}^{-1}$, and we see that $\widehat{A}$ corresponds to the class of $\mathfrak{d}^{-1}\bar{\mathfrak{A}}^{-1}$ in $\operatorname{Pic} R$.

An isogeny from one Deligne module $\mathfrak{A}$ to another $\mathfrak{B}$ is an element $x \in K$ such that $x\mathfrak{A} \subseteq \mathfrak{B}$. The degree of this isogeny is the index of $x\mathfrak{A}$ in $\mathfrak{B}$. A polarization of A is an isogeny $A \to \widehat{A}$ that satisfies certain symmetry and positivity conditions. In the category of Deligne modules, a polarization is an isogeny x from $\mathfrak{A}$ to $\mathfrak{d}^{-1}\bar{\mathfrak{A}}^{-1}$ such that x is pure imaginary and such that $\varphi(x)$ is positive imaginary (that is, a positive real times the element i of $\mathbf{C}$) for every $\varphi\colon K \to \mathbf{C}$ in the CM type Φ.

Fix an arbitrary pure imaginary $\iota \in K$ such that $\varphi(\iota)$ is positive imaginary for every $\varphi\colon K \to \mathbf{C}$ in the CM type Φ. Then a polarization of a Deligne module $\mathfrak{A}$ is an isogeny ιx from $\mathfrak{A}$ to $\mathfrak{d}^{-1}\bar{\mathfrak{A}}^{-1}$ such that x is a totally positive element of K^+.

It is now easy to characterize the Deligne modules $\mathfrak{A}$, with $\operatorname{End}\mathfrak{A} = R$, that have principal polarizations. We see that such an $\mathfrak{A}$ has a principal polarization if and only if there is a totally positive $x \in K^+$ such that $\iota x\mathfrak{A} = \mathfrak{d}^{-1}\bar{\mathfrak{A}}^{-1}$. This condition is equivalent to $x\mathfrak{A}\bar{\mathfrak{A}} = (\iota\mathfrak{d})^{-1}$.

Since R is convenient, the different $\mathfrak{d}$ can be generated by pure imaginary elements, so the ideal $\iota\mathfrak{d}$ can be generated by real elements. Let $\mathfrak{d}' = (\iota\mathfrak{d}) \cap K^+$. Then $\mathfrak{d}'$ is a fractional R^+-ideal with $\mathfrak{d}'R = \iota\mathfrak{d}$. In fact, we have $\operatorname{End}\mathfrak{d}' = (\operatorname{End}\iota\mathfrak{d}) \cap K^+ = R \cap K^+ = R^+$, and since R^+ is Gorenstein, this means that $\mathfrak{d}'$ is an invertible fractional R^+-ideal.

Let $\mathfrak{D}$ be the norm of $\mathfrak{A}$. Then the equality $x\mathfrak{A}\bar{\mathfrak{A}} = (\iota\mathfrak{d})^{-1}$ of invertible fractional R-ideals is equivalent to the equality $x\mathfrak{D} = (\mathfrak{d}')^{-1}$ of invertible fractional R^+-ideals. In other words, we see that the abelian variety corresponding to the class of $\mathfrak{A}$ in $\operatorname{Pic} R$ has a principal polarization if and only if this class maps, via the norm map $\operatorname{Pic} R \to \operatorname{Pic}^+ R^+$, to the class of $(\mathfrak{d}')^{-1}$. Since this norm map is surjective by assumption, the number of principally polarizable classes $[\mathfrak{A}]$ is simply the quotient $(\#\operatorname{Pic} R)/(\#\operatorname{Pic}^+ R^+)$.

Finally, we count the number of distinct principal polarizations (up to isomorphism) on a Deligne module, given that it has one. Suppose λ and μ are two principal polarizations on a Deligne module $\mathfrak{A}$ with $\operatorname{End}\mathfrak{A} = R$. Then $\mu^{-1}\lambda$ is an automorphism of $\mathfrak{A}$, and it is a totally positive element of R^+. Conversely, if u is a totally positive unit of R^+, then $u\lambda$ is a principal polarization of $\mathfrak{A}$.

Two principal polarizations λ and μ are isomorphic if and only if there is an isomorphism $\alpha\colon \mathfrak{A} \to \mathfrak{A}$ such that $\mu = \widehat{\alpha}\lambda\alpha$, where $\widehat{\alpha}$ is the dual isogeny of α. The Rosati involution on $\operatorname{End} A$ — which is simply complex conjugation — is given by $x \mapsto \lambda^{-1}\widehat{x}\lambda$, so we find that λ and μ are isomorphic if and only if $\mu = \lambda\bar{\alpha}\alpha$. Thus, the isomorphism classes of principal polarizations on $\mathfrak{A}$ correspond to elements of $U^+_{>0}$ modulo $N(U)$. The theorem follows. □

Proof of Corollary 1.2. — By Theorem 1.1, the total number of principally polarized varieties (A, λ) in the stratum $\mathcal{S}$, counted up to isomorphism, is equal to

$$\left[U^+_{>0} : N(U)\right] \frac{\#\operatorname{Pic} R}{\#\operatorname{Pic}^+ R^+},$$

where $U^+_{>0}$ is the group of totally positive units of R^+. Since $U \supseteq U^+$, we can rewrite this expression as

$$\begin{aligned}\left[U^+_{>0} : N(U)\right] \frac{\#\operatorname{Pic} R}{\#\operatorname{Pic}^+ R^+} &= \frac{\left[U^+_{>0} : (U^+)^2\right]}{[N(U) : (U^+)^2]} \frac{\#\operatorname{Pic} R}{\#\operatorname{Pic}^+ R^+}\\ &= \frac{1}{[N(U) : (U^+)^2]} \frac{\#\operatorname{Pic} R}{\#\operatorname{Pic} R^+},\end{aligned}$$

where the second equality is obtained from the fact that $\#\operatorname{Pic}^+ R^+$ is equal to $[U^+_{>0} : (U^+)^2]\,\#\operatorname{Pic} R^+$. We are left to prove the statements about the unit index. (In the case of maximal orders, these statements were proven by Hasse [Has19, Theorem 3.14, p. 76], [Has19, Theorem 3.15, p. 81].)

Given $u \in U$, the quotient $\bar{u}/u$ is an algebraic integer whose image in $\mathbf{C}$ lies on the unit circle under every embedding $K \hookrightarrow \mathbf{C}$, so $\bar{u}/u$ is an element of the group Z of roots of unity in U. The map $U \to Z$ given by $u \mapsto \bar{u}/u$ has kernel U^+, so the induced map $U/U^+ \to Z$ is injective, and therefore U/U^+ is a finite cyclic group. On the other hand, the norm map $U/U^+ \to N(U)/(U^+)^2$ is surjective, so $N(U)/(U^+)^2$ is also cyclic. Every nontrivial element of $N(U)/(U^+)^2$ clearly has order 2, so the order of $N(U)/(U^+)^2$ is either 1 or 2.

If $N(U)/(U^+)^2$ has order 2, then U/U^+ must have even order and hence has an element of order 2. This means there is a $u \in U$ such that $u \notin K^+$ and $u^2 \in U^+$. It follows that K is obtained from K^+ by adjoining the square root of a unit, so K/K^+ is unramified at all odd primes. □

Remark 4.1. — Suppose $\mathcal{S}$ is a stratum corresponding to a convenient order R, and suppose the norm map N_{Pic} is *not* surjective; say that the cokernel has order $n > 1$. If the class of $(\mathfrak{d}')^{-1}$ in $\operatorname{Pic}^+ R^+$ is not in the image of the norm map, then there will be *no* principally polarized varieties $A \in \mathcal{C}$ with $\operatorname{End} A = R$. On the other hand, if the class of $(\mathfrak{d}')^{-1}$ is in the image of the norm, there will be $n(\#\operatorname{Pic} R)/(\#\operatorname{Pic}^+ R^+)$ principally polarizable varieties $A \in \mathcal{C}$ with $\operatorname{End} A = R$, and each such variety will have $[U^+_{>0} : N(U)]$ isomorphism classes of principal polarizations. Likewise, the total number of principally polarized varieties (A, λ) in $\mathcal{S}$, counted up to isomorphism, will be

$$\frac{n}{[N(U) : (U^+)^2]} \frac{\#\operatorname{Pic} R}{\#\operatorname{Pic} R^+}$$

or 0, depending on whether or not the class of $(\mathfrak{d}')^{-1}$ is in the image of the norm.

Remark 4.2. — Let R be the endomorphism ring for a stratum $\mathcal{S}$ of an isogeny class. For an alternative viewpoint on Corollary 1.2, we can consider the so-called *Shimura class group* of R, denoted by $\operatorname{Pic}_* R$ in [LPP02, § 6]. Generalizing the definition given by Shimura and Taniyama in the case of maximal orders [ST61, § 4.5], Lenstra, Pila, and Pomerance [LPP02, § 6] define $\operatorname{Pic}_* R$ as the set of equivalence classes of pairs $(\mathfrak{B}, \beta)$, where $\mathfrak{B}$ is an invertible R-ideal and β is a totally positive element of K^+ such that $N(\mathfrak{B}) = \beta R$, and where two such pairs $(\mathfrak{B}, \beta)$ and $(\mathfrak{C}, \gamma)$ are taken to be equivalent if there is an element $\alpha \in K^*$ such that $\alpha\mathfrak{B} = \mathfrak{C}$ and $\alpha\bar{\alpha}\beta = \gamma$.

The group $\operatorname{Pic}_* R$ acts on the set X of principally polarized abelian varieties (A, λ) in the stratum $\mathcal{S}$, as follows: If (A, λ) corresponds to a Deligne module $\mathfrak{A}$ together with a totally positive $x \in K^+$ such that $x\mathfrak{A}\bar{\mathfrak{A}} = (\iota\mathfrak{d})^{-1}$ (with notation as in the proof of Theorem 1.1), then for every $(\mathfrak{B}, \beta)$ in $\operatorname{Pic}_* R$ we define $(\mathfrak{B}, \beta) \cdot (A, \lambda)$ to be the principally polarized variety corresponding to the Deligne module $\mathfrak{B}\mathfrak{A}$ and the element $x/\beta \in K^+$. It is easy to see that if the set X is nonempty, then it is a principal homogeneous space for the group $\operatorname{Pic}_* R$.

Thus, Corollary 1.2 says that when $\operatorname{Pic} R \to \operatorname{Pic}^+ R^+$ is surjective, the group $\operatorname{Pic}_* R$ has order

$$\frac{1}{[N(U) : (U^+)^2]} \frac{\# \operatorname{Pic} R}{\# \operatorname{Pic} R^+},$$

and there are this many principally polarized varieties in $\mathcal{S}$. More generally, we find (as in Remark 4.1) that

$$\# \operatorname{Pic}_* R = \frac{n}{[N(U) : (U^+)^2]} \frac{\# \operatorname{Pic} R}{\# \operatorname{Pic} R^+},$$

where n is the order of the cokernel of the norm map $\operatorname{Pic} R \to \operatorname{Pic}^+ R^+$.

Next we give some conditions under which the norm map $\operatorname{Pic} R \to \operatorname{Pic}^+ R^+$ is guaranteed to be surjective. Suppose R is a convenient order in a CM field K. Let $\mathfrak{f}$ be the conductor of R^+ and let L/K^+ be the ray class field for the modulus of K^+ determined by $\mathfrak{f}$ together with all of the infinite primes.

Proposition 4.3. — *If K/K^+ is not isomorphic to a subextension of L/K^+, then the norm map $\operatorname{Pic} R \to \operatorname{Pic}^+ R^+$ is surjective.*

Corollary 4.4. — *If K/K^+ is ramified at a finite prime that does not divide the conductor of R^+, then the norm map $\operatorname{Pic} R \to \operatorname{Pic}^+ R^+$ is surjective.* □

Proof of Proposition 4.3. — To better understand the norm map from $\operatorname{Pic} R$ to $\operatorname{Pic}^+ R^+$, we take [LPP02, § 6] as a model and identify the Picard groups with quotients of certain profinite groups, as follows. As in the proof of Lemma 2.5, we let $\widehat{\mathbf{Z}}$ be the profinite completion of $\mathbf{Z}$, and for an arbitrary ring E we let $\widehat{E}$ denote $E \otimes_{\mathbf{Z}} \widehat{\mathbf{Z}}$. Then we have

$$\operatorname{Pic} R \cong \widehat{K}^* / \left(\widehat{R}^* K^*\right) \quad \text{and} \quad \operatorname{Pic}^+ R^+ \cong \left(\widehat{K^+}\right)^* / \left(\left(\widehat{R^+}\right)^* (K^+)^*_{>0}\right),$$

where $(K^+)^*_{>0}$ denotes the multiplicative group of totally positive elements of K^+. The norm map on Picard groups gives us an exact sequence

$$\frac{\widehat{K}^*}{\widehat{R}^*K^*} \xrightarrow{N} \frac{\left(\widehat{K^+}\right)^*}{\left(\widehat{R^+}\right)^*(K^+)^*_{>0}} \longrightarrow \frac{\left(\widehat{K^+}\right)^*}{\left(\widehat{R^+}\right)^*(K^+)^*_{>0}N\left(\widehat{K}^*\right)} \longrightarrow 1.$$

Combining this with the analogous sequence for the maximal orders, we obtain the following diagram with exact rows and columns:

$$\begin{tikzcd}
 & & \frac{\left(\widehat{\mathcal{O}^+}\right)^*(K^+)^*_{>0}N\left(\widehat{K}^*\right)}{\left(\widehat{R^+}\right)^*(K^+)^*_{>0}N\left(\widehat{K}^*\right)} \arrow[d] & \\
\frac{\widehat{K}^*}{\widehat{R}^*K^*} \arrow[r, "N"] \arrow[d] & \frac{\left(\widehat{K^+}\right)^*}{\left(\widehat{R^+}\right)^*(K^+)^*_{>0}} \arrow[r] \arrow[d] & \frac{\left(\widehat{K^+}\right)^*}{\left(\widehat{R^+}\right)^*(K^+)^*_{>0}N\left(\widehat{K}^*\right)} \arrow[r] \arrow[d] & 1 \\
\frac{\widehat{K}^*}{\widehat{\mathcal{O}}^*K^*} \arrow[r, "N"] & \frac{\left(\widehat{K^+}\right)^*}{\left(\widehat{\mathcal{O}^+}\right)^*(K^+)^*_{>0}} \arrow[r] & \frac{\left(\widehat{K^+}\right)^*}{\left(\widehat{\mathcal{O}^+}\right)^*(K^+)^*_{>0}N\left(\widehat{K}^*\right)} \arrow[r] & 1
\end{tikzcd}$$

Let $\mathfrak{m}$ be the modulus consisting of the infinite primes of K^+ and the ideal $\mathfrak{f}$. We claim that the cokernel of the map $\operatorname{Pic} R \to \operatorname{Pic}^+ R^+$ is trivial, under the assumption that K/K^+ is not isomorphic to a subextension of L/K^+, the ray class field of K^+ modulo $\mathfrak{m}$. To prove this, it will suffice to show that the cokernel of the map $\operatorname{Pic}\mathcal{O} \to \operatorname{Pic}^+\mathcal{O}^+$ is trivial and that the group

$$\frac{\left(\widehat{\mathcal{O}^+}\right)^*(K^+)^*_{>0}N\left(\widehat{K}^*\right)}{\left(\widehat{R^+}\right)^*(K^+)^*_{>0}N\left(\widehat{K}^*\right)} \tag{4.1}$$

is trivial.

The extension K/K^+ must be ramified at a finite prime, because otherwise it would be contained in the ray class field of K^+ modulo the infinite primes. By [How95, Proposition 10.1, p. 2385], it follows that $\operatorname{Pic}\mathcal{O} \to \operatorname{Pic}^+\mathcal{O}^+$ is surjective.

We are left to show that the group (4.1) is trivial. To do this, it will suffice to show that for every $a \in (\widehat{\mathcal{O}^+})^*$ we can express a as the product of an element of $(K^+)^*_{>0}$ and an element of $(\widehat{R^+})^*$ and the norm of an element of $\widehat{K}^*$.

First let us recall the structure of the profinite groups in question. The group $\widehat{K}^*$ consists of all vectors $(a_\mathfrak{q})_{\mathfrak{q} \text{ of } \mathcal{O}}$ where each $a_\mathfrak{q}$ is a nonzero element of the completion $K_\mathfrak{q}$, and where all but finitely many $a_\mathfrak{q}$ lie in $\mathcal{O}_\mathfrak{q}^*$. The group $(\widehat{\mathcal{O}^+})^*$ consists of all vectors $(a_\mathfrak{p})_{\mathfrak{p} \text{ of } \mathcal{O}^+}$ where each $a_\mathfrak{p}$ lies in $(\mathcal{O}^+)^*_\mathfrak{p}$. The group $(\widehat{R^+})^*$ has an analogous structure, and can also be viewed as a subgroup of $(\widehat{\mathcal{O}^+})^*$. For us, it will suffice to observe that

$$\left(\widehat{R^+}\right)^* \supseteq \left\{ (a_\mathfrak{p})_{\mathfrak{p}\text{ of }\mathcal{O}^+} \,\middle|\, a_\mathfrak{p} \in \left(\mathcal{O}^+\right)^*_\mathfrak{p}, \text{ with } a_\mathfrak{p} \equiv 1 \bmod \mathfrak{p}^e \text{ when } \ \mathfrak{p}^e \parallel \mathfrak{f} \right\}.$$

Suppose we are given an element $a = (a_\mathfrak{p})$ of $(\widehat{\mathcal{O}^+})^*$. First we choose a totally positive $x \in \mathcal{O}^+$ such that if $\mathfrak{p}^e \parallel \mathfrak{f}$ then $x \equiv a_\mathfrak{p} \bmod \mathfrak{p}^e$. The ideal $x\mathcal{O}^+$ gives us a class χ in the ray class group modulo $\mathfrak{m}$. Because K/K^+ is not isomorphic to a subextension of L/K^+, the Chebotarëv density theorem (applied to the extension $L \cdot K$ of K^+) shows that there is a prime $\mathfrak{P}$ of $\mathcal{O}^+$ that splits in K, that does not divide $\mathfrak{f}$, and whose image in the ray class group is χ^{-1}. This means that there is an element y of $(K^+)^*_{>0}$ with $y \equiv 1 \bmod^* \mathfrak{f}$ such that $\mathcal{O}^+ = xy\mathfrak{P}$.

Let $\mathfrak{Q}$ be a prime of K lying over $\mathfrak{P}$, and let $b = (b_\mathfrak{q})$ be the element of $\widehat{K}^*$ such that $b_\mathfrak{q} = 1$ if $\mathfrak{q} \neq \mathfrak{Q}$ and $b_\mathfrak{Q} = (xy)^{-1}$. Then $N(b)$ is the element of $(\widehat{K^+})^*$ that is equal to 1 at every prime except $\mathfrak{P}$, where it is equal to $(xy)^{-1}$.

We check that for all $\mathfrak{p}^e \parallel \mathfrak{f}$, the $\mathfrak{p}$-components of a and of $xyN(b)$ are congruent modulo $\mathfrak{p}^e$. For all primes $\mathfrak{p} \neq \mathfrak{P}$ that do not divide $\mathfrak{f}$, the $\mathfrak{p}$-component of $xyN(b)$ is a unit of $\mathcal{O}^+_\mathfrak{p}$. Finally, the $\mathfrak{P}$-component of $xyN(b)$ is equal to 1. Therefore, $a/(xyN(b))$ is an element of

$$\left\{ (a_\mathfrak{p})_{\mathfrak{p}\text{ of }\mathcal{O}^+} \,\middle|\, a_\mathfrak{p} \in \left(\mathcal{O}^+\right)^*_\mathfrak{p}, \ \text{ with } a_\mathfrak{p} \equiv 1 \bmod \mathfrak{p}^e \text{ when } \mathfrak{p}^e \parallel \mathfrak{f} \right\},$$

which is contained in $(\widehat{R^+})^*$. Thus, our element a of $(\widehat{\mathcal{O}^+})^*$ is the product of the element xy of $(K^+)^*_{>0}$ and the element $a/(xyN(b))$ of $(\widehat{R^+})^*$ and the norm of the element b of $\widehat{K}^*$.

This shows that the cokernel of the map $\operatorname{Pic} R \to \operatorname{Pic}^+ R^+$ is trivial. □

5. Minus class numbers and discriminants

We continue to use the notation set forth at the beginning of Section 3.

Corollary 1.2 shows that for the strata $\mathcal{S}$ corresponding to certain convenient orders R, the number of principally polarized abelian varieties in $\mathcal{S}$ is equal either to h_R/h_{R^+} or to $(1/2)(h_R/h_{R^+})$, where h_R is the order of the Picard group of R and h_{R^+} is the order of the Picard group of the real subring R^+ of R. We denote the ratio h_R/h_{R^+} by h_R^-, as is commonly done in the case when R is a maximal order, and we call this ratio the *minus class number* of R. In the case where R is a maximal order $\mathcal{O}$, a Brauer–Siegel result for relative class numbers [Lou06] gives us an estimate — a rough estimate, to be sure — for the minus class number $h_\mathcal{O}^-$ in terms of the ratio $\Delta_\mathcal{O}/\Delta_{\mathcal{O}^+}$, where $\Delta_\mathcal{O}$ and $\Delta_{\mathcal{O}^+}$ are the discriminants of $\mathcal{O}$ and $\mathcal{O}^+$. In this section we review this result on relative class numbers and consider the case of minus class numbers of convenient orders that are not maximal. In the case where R is the convenient order $\mathbf{Z}[\pi, \bar{\pi}]$, we also compute an exact formula for the ratio Δ_R/Δ_{R^+} in terms of the Frobenius angles of the isogeny class $\mathcal{C}$. (This argument was sketched in the email reproduced in [How20, Appendix] and given in detail in [GW19]; we present a derivation here for the reader's convenience.)

For CM fields that do not contain imaginary quadratic fields, Louboutin gives effective lower bounds on $h^-_{\mathcal{O}}$ that are better than the crude Brauer–Siegel approximations that we discuss here, but for our purposes the added value of these effective results does not justify the complexity they would add to the discussion. In some sense, we will be satisfied simply to justify the rough heuristic that "minus class numbers grow like the square root of the ratio of discriminants," and we will not try to quantify the known bounds on h^-_R more precisely.

Let us make some remarks on the $\approxeq$ notation set in the introduction. Recall that if $\{a_i\}$ and $\{b_i\}$ are two sequences of positive real numbers indexed by positive integers i, the expression $a_i \approxeq b_i$ means that for every $\varepsilon > 0$ there are positive constants r and s such that $b_i \leqslant r a_i^{1+\varepsilon}$ and $a_i \leqslant s b_i^{1+\varepsilon}$ for all i. The notation is intended to capture the notion that the elements of the two sequences grow *very roughly* at the same rate. The relation $\approxeq$ is clearly symmetric and transitive. Furthermore, if we have sequences $\{a_i\}$, $\{b_i\}$, $\{c_i\}$, and $\{d_i\}$ with $a_i \approxeq b_i$ and $c_i \approxeq d_i$, and if f and g are two functions from $\mathbf{Z}_{>0}$ to itself, then

$$a_{f(i)} c_{g(i)} \approxeq b_{f(i)} d_{g(i)}.$$

Note also that for sequences $\{a_i\}$ and $\{b_i\}$ that tend to infinity, $a_i \approxeq b_i$ if and only if $(\log a_i)/(\log b_i) \to 1$.

For a convenient order R, we let Δ_R and Δ_{R^+} denote the discriminants of R and R^+, respectively.

Theorem 5.1 (Louboutin). — *As $\mathcal{O}$ ranges over the rings of integers of CM fields of a given degree over $\mathbf{Q}$, we have $h^-_{\mathcal{O}} \approxeq \sqrt{|\Delta_{\mathcal{O}}/\Delta_{\mathcal{O}^+}|}$.*

Proof. — This is a combination of [Lou06, Corollary 29, p. 216], which discusses normal CM fields of arbitrary degree with root-discriminants tending to infinity, and [Lou06, Corollary 32, p. 217], which discusses non-normal CM fields of fixed degree. □

Theorem 5.2. — *As R ranges over all convenient orders of a given degree $2n$ over $\mathbf{Q}$ for which the norm map $\operatorname{Pic} R \to \operatorname{Pic}^+ R^+$ is surjective, we have $h^-_R \approxeq \sqrt{|\Delta_R/\Delta_{R^+}|}$.*

Proof. — Let R be a convenient order in a field K for which $\operatorname{Pic} R \to \operatorname{Pic}^+ R^+$ is surjective, let $\mathcal{O}$ be the maximal order of K, and let $\mathcal{O}^+$ be the maximal order of the real subfield K^+. By Remark 4.2, we see that for this order R the relative class number h^-_R is equal to either $\#\operatorname{Pic}_* R$ or $2\#\operatorname{Pic}_* R$, so it will suffice to show that $\#\operatorname{Pic}_* R \approxeq \sqrt{|\Delta_R/\Delta_{R^+}|}$.

Lenstra, Pila, and Pomerance show [LPP02, Lemma 6.3, p. 125] that the order of $\operatorname{Pic}_* R$ is equal to

$$\#\operatorname{Pic}_* R = \#C \cdot \frac{w(R)}{2^n} \cdot \frac{h_{\mathcal{O}} \ \operatorname{reg}\mathcal{O} \ \ w(\mathcal{O}^+)}{h_{\mathcal{O}^+} \operatorname{reg}\mathcal{O}^+ \, w(\mathcal{O})} \cdot \frac{\left[\widehat{\mathcal{O}}^* : \widehat{R}^*\right]}{\left[\left(\widehat{\mathcal{O}^+}\right)^* : \left(\widehat{R^+}\right)^*\right]},$$

where C is the cokernel of the norm map $\operatorname{Pic} R \to \operatorname{Pic}^+ R^+$ (which is trivial in our case), where $w(R)$, $w(\mathcal{O})$, and $w(\mathcal{O}^+)$ denote the number of roots of unity in these orders, where reg denotes the regulator, and where the 'hat' notation is as in the proofs of Lemma 2.5 and Proposition 4.3.

We note that the expression

$$\#C \cdot \frac{w(R)}{2^n} \cdot \frac{\operatorname{reg}\mathcal{O} \quad w(\mathcal{O}^+)}{\operatorname{reg}\mathcal{O}^+ \, w(\mathcal{O})}$$

is bounded above and below in terms depending only on the degree n, so it will suffice for us to show that

$$\frac{h_{\mathcal{O}}}{h_{\mathcal{O}^+}} \cdot \frac{\left[\widehat{\mathcal{O}}^* : \widehat{R}^*\right]}{\left[\left(\widehat{\mathcal{O}^+}\right)^* : \left(\widehat{R^+}\right)^*\right]} \approx \frac{\sqrt{|\Delta_R|}}{\sqrt{|\Delta_{R^+}|}}.$$

Following [LPP02], we let $\mathfrak{F}$ be the conductor of R, we set $\mathfrak{f} = \mathfrak{F} \cap R^+ = \mathfrak{F} \cap \mathcal{O}^+$, and we define finite rings

$$A = \mathcal{O}/\mathfrak{F}, \quad B = \mathcal{O}^+/\mathfrak{f} \subseteq A, \quad C = R/\mathfrak{F} \subseteq A, \quad \text{and } D = R^+/\mathfrak{f} = B \cap C.$$

Then

$$\frac{\left[\widehat{\mathcal{O}}^* : \widehat{R}^*\right]}{\left[\left(\widehat{\mathcal{O}^+}\right)^* : \left(\widehat{R^+}\right)^*\right]} = \frac{[A^* : C^*]}{[B^* : D^*]} = \frac{\#A^*/\#C^*}{\#B^*/\#D^*},$$

and by Corollary 5.8 [LPP02, p. 123] and the remark following its proof, we have

$$\frac{\#A^*/\#C^*}{\#B^*/\#D^*} \approx \frac{\#A/\#C}{\#B/\#D} = \frac{[\mathcal{O} : R]}{[\mathcal{O}^+ : R^+]} = \frac{\sqrt{\Delta_{\mathcal{O}}/\Delta_R}}{\sqrt{\Delta_{\mathcal{O}^+}/\Delta_{R^+}}}$$

as R ranges over the convenient orders of a given degree over $\mathbf{Q}$. This gives us

$$\frac{\left[\widehat{\mathcal{O}}^* : \widehat{R}^*\right]}{\left[\left(\widehat{\mathcal{O}^+}\right)^* : \left(\widehat{R^+}\right)^*\right]} \approx \frac{\sqrt{\Delta_R/\Delta_{\mathcal{O}}}}{\sqrt{\Delta_{R^+}/\Delta_{\mathcal{O}^+}}},$$

and combining this with Theorem 5.1 we find that

$$\frac{h_{\mathcal{O}}}{h_{\mathcal{O}^+}} \cdot \frac{\left[\widehat{\mathcal{O}}^* : \widehat{R}^*\right]}{\left[\left(\widehat{\mathcal{O}^+}\right)^* : \left(\widehat{R^+}\right)^*\right]} \approx \frac{\sqrt{|\Delta_{\mathcal{O}}|}}{\sqrt{|\Delta_{\mathcal{O}^+}|}} \cdot \frac{\sqrt{\Delta_R/\Delta_{\mathcal{O}}}}{\sqrt{\Delta_{R^+}/\Delta_{\mathcal{O}^+}}} = \frac{\sqrt{|\Delta_R|}}{\sqrt{|\Delta_{R^+}|}},$$

which, as we noted above, is enough to prove the theorem. □

The ring $R = \mathbf{Z}[\pi, \bar{\pi}]$ from Corollary 3.2 is contained in the endomorphism ring of every abelian variety A in $\mathcal{C}$, and for this R there is a very nice expression of $\sqrt{|\Delta_R/\Delta_{R^+}|}$ in terms of Frobenius angles.

Theorem 5.3 (See [GW19, § 2]). — *Let $0 < \theta_1 < \cdots < \theta_n < \tau/2$ be the Frobenius angles for the isogeny class $\mathcal{C}$, and let R be the ring $\mathbf{Z}[\pi, \bar{\pi}]$. Then we have*

$$\sqrt{|\Delta_R/\Delta_{R^+}|} = 2^{n(n+1)/2} q^{n(n+1)/4} \prod_{i<j} (\cos\theta_i - \cos\theta_j) \prod_i \sin\theta_i.$$

Proof. — Clearly $R = R^+ \cdot 1 \oplus R^+ \cdot \pi$. Arguing as in the proof of Proposition 2.4, we find that the different of R is $\pi - \bar{\pi}$ times the different of R^+, and since R^+ is generated by $\pi + \bar{\pi}$ we see that the different of R^+ is $g'(\pi + \bar{\pi})$, where g is the minimal polynomial of $\pi+\bar{\pi}$. The discriminant ideal is the norm of the different, so the integers $|\Delta_{R^+}|$ and $|\Delta_R|$ are given by

$$|\Delta_{R^+}| = \left|N_{K^+/\mathbf{Q}}\left(g'\left(\pi+\bar{\pi}\right)\right)\right| \quad \text{and} \quad |\Delta_R| = \left|N_{K/\mathbf{Q}}\left(\pi-\bar{\pi}\right)\right|\Delta_{R^+}^2,$$

and we see that

$$|\Delta_R/\Delta_{R^+}| = \left|N_{K/\mathbf{Q}}\left(\pi-\bar{\pi}\right)\right|\left|N_{K^+/\mathbf{Q}}\left(g'\left(\pi+\bar{\pi}\right)\right)\right|. \tag{5.1}$$

The images of $\pi+\bar{\pi}$ under the various real embeddings of K^+ into $\mathbf{R}$ are

$$\sqrt{q}e^{\theta_i}+\sqrt{q}e^{-\theta_i} = 2\sqrt{q}\cos\theta_i,$$

so

$$\left|N_{K^+/\mathbf{Q}}\left(g'\left(\pi+\bar{\pi}\right)\right)\right| = 2^{n(n-1)}q^{n(n-1)/2}\prod_{i<j}\left(\cos\theta_i-\cos\theta_j\right)^2. \tag{5.2}$$

Similarly, the images of $\pi-\bar{\pi}$ in $\mathbf{C}$ are the values

$$\sqrt{q}e^{\theta_i}-\sqrt{q}e^{-\theta_i} = 2\sqrt{q}\sqrt{-1}\sin\theta_i$$

and their complex conjugates, so

$$\left|N_{K/\mathbf{Q}}\left(\pi-\bar{\pi}\right)\right| = 2^{2n}q^n\prod_i\sin^2\theta_i. \tag{5.3}$$

Combining Equations (5.1), (5.2), and (5.3), we find that

$$|\Delta_R/\Delta_{R^+}| = 2^{n(n+1)}q^{n(n+1)/2}\prod_{i<j}\left(\cos\theta_i-\cos\theta_j\right)^2\prod_i\sin^2\theta_i,$$

and the theorem follows. □

We note that Theorem 1.3 follows from Corollary 1.2, Theorem 5.2, and Theorem 5.3.

6. Isogeny classes containing many principally polarized varieties

Suppose $\mathcal{C}$ is an isogeny class of simple ordinary abelian varieties over $\mathbf{F}_q$ and let $R=\mathbf{Z}[\pi,\bar{\pi}]$ be the minimal ring of $\mathcal{C}$, where π is a root of the Weil polynomial of $\mathcal{C}$. We say that an abelian variety in $\mathcal{C}$ *has minimal endomorphism ring* if its endomorphism ring is R.

We saw in Corollary 3.2 that R is a convenient order, so Corollary 4.4 and Corollary 1.2 show that under a mild hypothesis, the number of principally polarized varieties in $\mathcal{C}$ with minimal endomorphism ring is either h_R^- or $h_R^-/2$, where h_R^- is the minus class number of R. Then Theorems 5.2 and 5.3 say that this number is *very* roughly on the order of

$$q^{n(n+1)/4}\prod_{i<j}\left(\cos\theta_i-\cos\theta_j\right)\prod_i\sin\theta_i,$$

where the θ_i are the Frobenius angles for the isogeny class. Since this is of the same order as the average number of principally polarized varieties with Frobenius angles near $(\theta_1,\ldots,\theta_n)$ given by Equation (1.6), one might be tempted to think that the principally polarized varieties with minimal endomorphism ring account for a nontrivial fraction of the principally polarized varieties in $\mathcal{C}$.

The goal of this short section is simply to demonstrate that one should not succumb to this temptation. Indeed, even for isogeny classes of elliptic curves, the number of curves with minimal endomorphism ring can be a vanishingly small fraction of the curves in the isogeny class.

Theorem 6.1. — *For every $\varepsilon > 0$, there is an isogeny class $\mathcal{C}$ of ordinary elliptic curves over a finite field such that the fraction of curves in $\mathcal{C}$ with minimal endomorphism ring is less than ε.*

Proof. — Let $\mathcal{C}$ be an isogeny class of ordinary elliptic curves over $\mathbf{F}_q$, say with trace t, and let $\Delta = t^2 - 4q$, so that Δ is the discriminant of the ring $R = \mathbf{Z}[\pi, \bar{\pi}]$, where π is a root of $x^2 - tx + q$. Write $\Delta = F^2\Delta_0$ for a fundamental discriminant Δ_0, and for ease of exposition let us suppose that Δ_0 is neither -3 nor -4.

The number of elliptic curves in $\mathcal{C}$ is equal to the Kronecker class number $H(\Delta)$ of Δ (see [Sch87, Theorem 4.6, pp. 194–195]), which is the sum of the class numbers of all orders that contain R:

$$H(\Delta) = \sum_{f|F} h\left(f^2\Delta_0\right).$$

Let χ be the quadratic character modulo Δ_0. Since the only roots of unity in the order of discriminant Δ_0 are ± 1, we have

$$h\left(f^2\Delta_0\right) = h(\Delta_0) f \prod_{p|f}\left(1 - \tfrac{\chi(p)}{p}\right), \tag{6.1}$$

so that

$$\begin{aligned} H(\Delta) &= h(\Delta_0)\sum_{f|F} f \prod_{p|f}\left(1 - \tfrac{\chi(p)}{p}\right) \\ &= h(\Delta_0)\prod_{p^e\|F}\left(1 + \left(1 - \tfrac{\chi(p)}{p}\right)(p + \cdots + p^e)\right) \end{aligned}$$

and

$$\begin{aligned} \frac{H(\Delta)}{h(\Delta)} &= \prod_{p^e\|F}\left(p^{-e}\left(1 - \tfrac{\chi(p)}{p}\right)^{-1} + 1 + \frac{1}{p} + \cdots + \frac{1}{p^{e-1}}\right) \\ &\geqslant \prod_{p^e\|F}\left(\frac{1}{p^{e-1}(p+1)} + \frac{p^e - 1}{p^{e-1}(p-1)}\right) \\ &\geqslant \prod_{p|F}\left(\frac{p+2}{p+1}\right) \end{aligned}$$

so

$$\frac{h(\Delta)}{H(\Delta)} \leqslant \prod_{p|F}\left(\frac{p+1}{p+2}\right). \tag{6.2}$$

The product $\prod_p(\frac{p+1}{p+2})$ diverges to 0, so to prove the theorem we need only show that for every integer $m > 0$, there are isogeny classes $\mathcal{C}$ for which the conductor of the minimal endomorphism ring is divisible by m.

Suppose we are given an $m > 0$. Let $\Delta_0 < -4$ be a fundamental discriminant and let $n = m^2|\Delta_0|$. Let p be a prime of the form $x^2 + ny^2$ (see [Cox13, Theorem 9.2, p. 163]), and let $t = 2x$. Then $t^2 < 4p$ and $p \nmid t$, so by a result of Deuring (see [Sch87, Theorem 4.2, p. 193]) there is an isogeny class of elliptic curves over $\mathbf{F}_p$ with trace t. We see that the discriminant Δ of this isogeny class is

$$\Delta = t^2 - 4p = 4x^2 - 4\left(x^2 + m^2\left|\Delta_0\right|y^2\right) = m^2y^2\Delta_0,$$

so the conductor for the minimal endomorphism ring is my, and is divisible by m, as we wished to show. □

7. Examples

In this section, we give three families of strata of abelian surfaces such that, in the notation of Theorem 1.3, we do *not* have $P_m \approxeq q_m^{3/2}$, but instead have $P_m \approxeq q_m^{5/4}$ (for the first family), $P_m \approxeq q_m$ (for the second), and $P_m \approxeq q_m^{1/2}$ (for the third). This shows that the trigonometric factors in Theorem 1.3 are essential.

We repeatedly use the fact that if a polynomial of the shape $f = x^4 + ax^3 + bx^2 + aqx + q^2$ is irreducible and defines a CM field, where q is a power of a prime and where the middle coefficient b is coprime to q, then f is the Weil polynomial of an isogeny class of ordinary abelian surfaces over $\mathbf{F}_q$; see [How95, § 3].

Example 7.1. — For every prime p that is congruent to 7 modulo 8, let a_p be the largest integer less than $\sqrt{p} - 1$, and let f_p be the polynomial

$$f_p = x^4 - 2a_px^3 + \left(a_p^2 + p\right)x^2 - 2a_ppx + p^2.$$

We claim that f_p is the Weil polynomial of a simple ordinary isogeny class over $\mathbf{F}_p$. Since the middle coefficient of f_p is clearly coprime to p, it will be enough for us to show that the algebra $K = \mathbf{Q}[x]/(f_p)$ is a CM field.

Let π be the image of the polynomial variable x in K and let $\bar{\pi} = p/\pi$. We check that $\alpha := \pi + \bar{\pi}$ satisfies $\alpha^2 - 2a_p\alpha + a_p^2 - p = 0$, so that $\alpha = a_p + s$ where $s^2 = p$. Therefore the algebra K contains the quadratic field $K^+ = \mathbf{Q}(\sqrt{p})$. In fact, K is the extension of K^+ obtained by adjoining a root of $y^2 - \alpha y + p$, so to show that K is a CM field we just need to show that $\alpha^2 - 4p$ is totally negative. But this is clear, because under the two embeddings of K^+ into $\mathbf{R}$ the element α^2 gets sent to real numbers smaller than $4p$. Thus, f_p is the Weil polynomial of a simple ordinary isogeny class $\mathcal{C}_p$ of abelian surfaces over $\mathbf{F}_p$.

Let $R_p = \mathbf{Z}[\pi, \bar{\pi}]$ be the minimal ring for $\mathcal{C}_p$. As we have just seen, R_p^+ contains a square root of p and is therefore the maximal order of K^+.

We claim that the extension K/K^+ is ramified at an odd prime. We prove this by contradiction: Since K is obtained from K^+ by adjoining a square root of $\alpha^2 - 4p$, if K/K^+ were unramified at all odd primes then the norm of $\alpha^2 - 4p$ would be either a square or twice a square. We compute that

$$N_{K^+/\mathbf{Q}}\left(\alpha^2 - 4p\right) = \left(p - a_p^2\right)\left(9p - a_p^2\right),$$

and since a_p is coprime to p, the greatest common divisor of the two factors is a divisor of 8. Thus, if this norm were a square or twice a square, each factor would also be. But there is no integer b such that $p = a_p^2 + b^2$ or $p = a_p^2 + 2b^2$, because $p \equiv 7 \bmod 8$. Therefore, K/K^+ is ramified at an odd prime.

Let $\mathcal{S}_p$ be the minimal stratum of $\mathcal{C}_p$ and let P_p be the number of isomorphism classes of principally polarized varieties in $\mathcal{S}_p$. Since R_p is the minimal order of $\mathcal{C}_p$, it is convenient by Corollary 3.2. Since R_p^+ is the maximal order of K^+ it has trivial conductor, and since K/K^+ is ramified at an odd prime, Corollary 4.4 tells us that the norm map $\operatorname{Pic} R_p \to \operatorname{Pic}^+ R_p^+$ is surjective. Then from Corollary 1.2 we find that $P_p = h_{R_p}^-$, the minus class number of R_p.

As we noted at the beginning of the proof of Theorem 5.3, we have

$$\left|\Delta_{R_p}\right| = \left|N_{K/\mathbf{Q}}(\pi - \bar{\pi})\right| \Delta_{R_p^+}^2.$$

Since $|N_{K/\mathbf{Q}}(\pi - \bar{\pi})| = N_{K^+/\mathbf{Q}}(\alpha^2 - 4p)$, we find that $|\Delta_{R_p}| = (p - a_p^2)(9p - a_p^2)(4p)^2$ and

$$\left|\Delta_{R_p}/\Delta_{R_p^+}\right| = 4p\left(p - a_p^2\right)\left(9p - a_p^2\right).$$

If we write $a_p = \sqrt{p} - \varepsilon$ for a real number ε in the interval $(1, 2)$, then

$$\left|\Delta_{R_p}/\Delta_{R_p^+}\right| = 4p\left(2\varepsilon\sqrt{p} - \varepsilon^2\right)\left(8p + 2\varepsilon\sqrt{p} - \varepsilon^2\right),$$

so we have

$$32p^{5/2} < \left|\Delta_{R_p}/\Delta_{R_p^+}\right| < 144p^{5/2}$$

Thus, Theorem 5.2 says that as $p \to \infty$ we have $P_p \approxeq p^{5/4}$. □

Example 7.2. — For every prime p that is congruent to 7 modulo 8, we let f_p be the polynomial

$$f_p = x^4 + x^3 + (2p - 1)x^2 + px + p^2.$$

Again we claim that the polynomial f_p is the Weil polynomial of a simple ordinary isogeny class $\mathcal{C}_p$ over $\mathbf{F}_p$, and since its middle coefficient is visibly coprime to p, all we must show is that the algebra $K = \mathbf{Q}[x]/(f_p)$ is a CM field. The algebra K is certainly at least a *field*, because f_p is irreducible modulo 2.

Let π be a root of f_p in K, let $\bar{\pi} = p/\pi$, and let $\alpha = \pi + \bar{\pi}$. We calculate that $\alpha^2 + \alpha - 1 = 0$, so K contains the quadratic field $K^+ = \mathbf{Q}(\sqrt{5})$. We obtain K from K^+ by adjoining a root of $y^2 - \alpha y + p$, and since the discriminant $\alpha^2 - 4p$ is totally negative (because the images of α^2 in the real numbers are both smaller than 3), K is a CM field and our claim is verified.

The narrow class number of $\mathbf{Q}(\sqrt{5})$ is 1, so every quadratic extension of K^+ is ramified at a finite prime. Since f_p is irreducible modulo 2, the prime 2 is inert in the extension $K/\mathbf{Q}$ and in particular the unique even prime of K^+ is not ramified in K/K^+. This means that K/K^+ is ramified at an odd prime.

Let R_p and $\mathcal{S}_p$ be the minimal ring and minimal stratum of $\mathcal{C}_p$, and let P_p be the number of isomorphism classes of principally polarized varieties in $\mathcal{S}_p$. The ring R_p is convenient by Corollary 3.2. The real order R_p^+ is maximal and so has trivial conductor, and since K/K^+ is ramified at an odd prime, we again find from

Corollary 4.4 that the norm map $\operatorname{Pic} R_p \to \operatorname{Pic}^+ R_p^+$ is surjective. The ramification of K/K^+ at an odd prime, together with Corollary 1.2, tells us that $P_p = h^-_{R_p}$.

We have

$$\left|\Delta_{R_p}\right| = \left|N_{K/\mathbf{Q}}(\pi - \bar{\pi})\right| \Delta^2_{R_p^+} = \left(16p^2 - 12p + 1\right) \cdot 25$$

so that

$$\left|\Delta_{R_p}/\Delta_{R_p^+}\right| = 5\left(16p^2 - 12p + 1\right).$$

Theorem 5.2 then tells us that as $p \to \infty$ we have $P_p \approxeq p$. □

Example 7.3. — For every prime p that is congruent to 7 modulo 8, let c_p be the largest integer less than $2\sqrt{p} - 1$, and let f_p be the polynomial

$$f_p = x^4 + (1 - 2c_p)\,x^3 + \left(2p + c_p^2 - c_p - 1\right)x^2 + p\;(1 - 2c_p)\,x + p^2.$$

Once more we claim that f_p is the Weil polynomial of a simple ordinary isogeny class $\mathcal{C}_p$ over $\mathbf{F}_p$, and again we prove this by showing that the algebra $K = \mathbf{Q}[x]/(f_p)$ is a CM field and that the middle coefficient of f_p is coprime to p.

Let π be the image of the polynomial variable x in K, let $\bar{\pi} = p/\pi$, and let $\alpha = \pi + \bar{\pi}$. We check that

$$\alpha^2 - (2c_p - 1)\,\alpha + \left(c_p^2 - c_p - 1\right) = 0,$$

so $\alpha = c_p - \varphi$, where $\varphi \in K^+$ satisfies $\varphi^2 - \varphi - 1 = 0$. Once again we see that K contains the quadratic field $K^+ = \mathbf{Q}(\sqrt{5})$. The algebra K is obtained from K^+ by adjoining a square root of $\alpha^2 - 4p$. This quantity is totally negative, so K is a CM field.

For $p < 100$, explicit computation shows that the middle coefficient of f_p is coprime to p. For $p > 100$, we write $c_p = 2\sqrt{p} - \varepsilon$ for a real number ε in the interval $(1, 2)$, and we compute that the middle coefficient of f_p is equal to

$$6p - (4\varepsilon + 2)\sqrt{p} + \varepsilon^2 + \varepsilon - 1.$$

This lies strictly between $5p$ and $6p$, so the middle coefficient is not a multiple of p for these primes as well. Thus f_p is the Weil polynomial of a simple ordinary isogeny class $\mathcal{C}_p$ of abelian surfaces over $\mathbf{F}_p$.

Let R_p be the minimal order of $\mathcal{C}_p$. Arguing as in Example 7.2 we find that R_p^+ is the maximal order of $\mathbf{Q}(\sqrt{5})$ and that K/K^+ is ramified at an odd prime. If we let P_p denote the number of isomorphism classes of principally polarized varieties in the minimal stratum of $\mathcal{C}_p$, then once again we have that $P_p = h^-_{R_p}$.

Writing $c_p = 2\sqrt{p} - \varepsilon$ for some $\varepsilon \in (1, 2)$, we compute that

$$\begin{aligned}\left|N_{K/\mathbf{Q}}(\pi - \bar{\pi})\right| &= N_{K^+/\mathbf{Q}}\left(\alpha^2 - 4p\right)\\ &= c_p^4 - 2c_p^3 - (8p + 1)c_p^2 + (8p + 2)c_p + \left(16p^2 - 12p + 1\right)\\ &= \varepsilon^4 - \left(8\sqrt{p} - 2\right)\varepsilon^3 + \left(16p - 12\sqrt{p} - 1\right)\varepsilon^2\\ &\qquad + \left(16p + 4\sqrt{p} - 2\right)\varepsilon - \left(16p - 4\sqrt{p} - 1\right).\end{aligned}$$

If we view this expression as a function of ε, we find that the extreme values of the function on the interval $[1,2]$ are attained at the endpoints, and it follows that

$$16p - 12\sqrt{p} + 1 < \left|N_{K/\mathbf{Q}}(\pi - \bar{\pi})\right| < 80p - 100\sqrt{p} + 25.$$

Since $|\Delta_{R_p}/\Delta_{R_p^+}| = |N_{K/\mathbf{Q}}(\pi - \bar{\pi})|\,\Delta_{R_p^+}$ and $\Delta_{R_p^+} = 5$ and $p \geqslant 7$, we find that

$$58p < \left|\Delta_{R_p}/\Delta_{R_p^+}\right| < 400p,$$

so Theorem 5.2 says that as $p \to \infty$ we have $P_p \approxeq p^{1/2}$. □

Remark 7.4. — In Example 7.1, one of the two Frobenius angles of the isogeny classes approaches 0, while the other remains near $\tau/4$. In Example 7.2, the two Frobenius angles both approach $\tau/4$. And in Example 7.3, both Frobenius angles approach 0.

BIBLIOGRAPHY

[AG17] Jeffrey D. Achter and Julia Gordon, *Elliptic curves, random matrices and orbital integrals*, Pac. J. Math. **286** (2017), no. 1, 1–24, with an appendix by S. Ali Altuğ. ↑682

[Bir68] Bryan J. Birch, *How the number of points of an elliptic curve over a fixed prime field varies*, J. Lond. Math. Soc. **43** (1968), 57–60. ↑682

[BL94] Johannes A. Buchmann and Hendrik W. Lenstra, Jr., *Approximating rings of integers in number fields*, J. Théor. Nombres Bordeaux **6** (1994), no. 2, 221–260. ↑683, 684

[Byk97] Viktor A. Bykovskiĭ, *Density theorems and the mean value of arithmetic functions in short intervals*, J. Math. Sci., New York **83** (1997), 720–730, translation from Russian of *Zap. Nauchn. Sem. S.-Peterburg. Otdel. Mat. Inst. Steklov. (POMI)* **212** (1994) 56–70. ↑682

[Cox13] David A. Cox, *Primes of the form $x^2 + ny^2$: Fermat, class field theory, and complex multiplication*, second ed., Pure and Applied Mathematics, John Wiley & Sons, 2013. ↑697

[Del69] Pierre Deligne, *Variétés abéliennes ordinaires sur un corps fini*, Invent. Math. **8** (1969), 238–243. ↑683, 687

[DH98] Stephen A. DiPippo and Everett W. Howe, *Real polynomials with all roots on the unit circle and abelian varieties over finite fields*, J. Number Theory **73** (1998), no. 2, 426–450, corrigendum in [DH00]. ↑680

[DH00] ______, *Corrigendum: "Real polynomials with all roots on the unit circle and abelian varieties over finite fields"*, J. Number Theory **83** (2000), no. 1, 182.

[Gek03] Ernst-Ulrich Gekeler, *Frobenius distributions of elliptic curves over finite prime fields*, Int. Math. Res. Not. (2003), no. 37, 1999–2018. ↑682

[GW19] Jonathan Gerhard and Cassandra Williams, *Local heuristics and an exact formula for abelian varieties of odd prime dimension over finite fields*, New York J. Math. **25** (2019), 123–144. ↑692, 694

[Has19] Helmut Hasse, *On the class number of Abelian number fields*, Springer, 2019, translated from the German by M. Hirabayashi, and extended with tables by M. Hirabayashi and K.-i. Yoshino. ↑689

[How95] Everett W. Howe, *Principally polarized ordinary abelian varieties over finite fields*, Trans. Am. Math. Soc. **347** (1995), no. 7, 2361–2401. ↑683, 687, 688, 691, 697

[How04] ______, *On the non-existence of certain curves of genus two*, Compos. Math. **140** (2004), no. 3, 581–592. ↑679

[How20] ______, *Variations in the distribution of principally polarized abelian varieties among isogeny classes*, `https://arxiv.org/abs/2005.14365`, 2020. ↑683, 692

[IT20] Sorina Ionica and Emmanuel Thomé, *Isogeny graphs with maximal real multiplication*, J. Number Theory **207** (2020), 385–422. ↑679

[KS99] Nicholas M. Katz and Peter Sarnak, *Random matrices, Frobenius eigenvalues, and monodromy*, Colloquium Publications, vol. 45, American Mathematical Society, 1999. ↑681

[Len87] Hendrik W. Lenstra, Jr., *Factoring integers with elliptic curves*, Ann. Math. **126** (1987), no. 3, 649–673. ↑682

[Lou06] Stéphane R. Louboutin, *Lower bounds for relative class numbers of imaginary abelian number fields and CM-fields*, Acta Arith. **121** (2006), no. 3, 199–220. ↑683, 692, 693

[LPP02] Hendrik W. Lenstra, Jr., Jonathan Pila, and Carl Pomerance, *A hyperelliptic smoothness test. II*, Proc. Lond. Math. Soc. **84** (2002), no. 1, 105–146. ↑679, 685, 690, 693, 694

[Mat86] Hideyuki Matsumura, *Commutative ring theory*, Cambridge Studies in Advanced Mathematics, vol. 8, Cambridge University Press, 1986, translated from the Japanese by M. Reid. ↑684

[Nar04] Władysław Narkiewicz, *Elementary and analytic theory of algebraic numbers*, third ed., Springer Monographs in Mathematics, Springer, 2004. ↑684

[Neu99] Jürgen Neukirch, *Algebraic number theory*, Grundlehren der Mathematischen Wissenschaften, vol. 322, Springer, 1999, translated from the German by N. Schappacher. ↑684, 685

[PL87] Martine Picavet-L'Hermitte, *Ordres de Gorenstein*, Ann. Sci. Univ. Blaise Pascal Clermont-Ferrand II **91** (1987), no. 24, 1–32. ↑683, 684

[Sch87] René Schoof, *Nonsingular plane cubic curves over finite fields*, J. Comb. Theory, Ser. A **46** (1987), no. 2, 183–211. ↑696, 697

[Shi98] Goro Shimura, *Abelian varieties with complex multiplication and modular functions*, Princeton Mathematical Series, vol. 46, Princeton University Press, 1998, revised and expanded version of [ST61].

[ST61] Goro Shimura and Yutaka Taniyama, *Complex multiplication of abelian varieties and its applications to number theory*, Publications of the Mathematical Society of Japan, vol. 6, Mathematical Society of Japan, 1961, revised and expanded in [Shi98]. ↑679, 690

[Tat66] John Tate, *Endomorphisms of abelian varieties over finite fields*, Invent. Math. **2** (1966), 134–144. ↑679

[Tat71] ______, *Classes d'isogénie des variétés abéliennes sur un corps fini (d'après T. Honda)*, Séminaire Bourbaki. Vol. 1968/69: Exposés 347–363, Lecture Notes in Mathematics, vol. 352, Springer, 1971, pp. 95–110. ↑679

[Vlă01] Serge G. Vlăduţ, *Isogeny class and Frobenius root statistics for abelian varieties over finite fields*, Mosc. Math. J. **1** (2001), no. 1, 125–139. ↑681

[Wat69] William C. Waterhouse, *Abelian varieties over finite fields*, Ann. Sci. Éc. Norm. Supér. **2** (1969), 521–560. ↑679

[Wey97] Hermann Weyl, *The classical groups: Their invariants and representations*, second ed., Princeton Landmarks in Mathematics, Princeton University Press, 1997, reprint of the second edition (1946) of the 1939 original, fifteenth printing. ↑681

Manuscript received on 10th December 2020,
accepted on 4th March 2022.

Recommended by Editor B. Edixhoven.

Published under license CC BY 4.0.

This journal is a member of Centre Mersenne.

Everett W. HOWE
Independent mathematician,
San Diego, CA 92104 (USA)
however@alumni.caltech.edu
http://ewhowe.com