SPLIT ABELIAN SURFACES OVER FINITE FIELDS AND REDUCTIONS OF GENUS-2 CURVES

JEFFREY D. ACHTER AND EVERETT W. HOWE

Dedicated to the memory of Professor Tom M. Apostol

ABSTRACT. For prime powers q, let $\mathrm{split}(q)$ denote the probability that a randomly-chosen principally-polarized abelian surface over the finite field $\mathbb{F}_q$ is not simple. We show that there are positive constants c_1 and c_2 such that for all q,

$$c_1(\log q)^{-3}(\log\log q)^{-4} < \mathrm{split}(q)\sqrt{q} < c_2(\log q)^4(\log\log q)^2,$$

and we obtain better estimates under the assumption of the generalized Riemann hypothesis. If A is a principally-polarized abelian surface over a number field K, let $\pi_{\mathrm{split}}(A/K, z)$ denote the number of prime ideals $\mathfrak{p}$ of K of norm at most z such that A has good reduction at $\mathfrak{p}$ and $A_{\mathfrak{p}}$ is not simple. We conjecture that for sufficiently general A, the counting function $\pi_{\mathrm{split}}(A/K, z)$ grows like $\sqrt{z}/\log z$. We indicate why our theorem on the rate of growth of $\mathrm{split}(q)$ gives us reason to hope that our conjecture is true.

CONTENTS

1. INTRODUCTION

Let A/K be a principally-polarized absolutely simple abelian variety over a number field. Murty and Patankar have conjectured [37, 38] that if the absolute endomorphism ring of A is commutative, then the reduction $A_{\mathfrak{p}}$ is simple for almost all primes $\mathfrak{p}$ of $\mathcal{O}_K$. (See [1, 45] for work on this conjecture.) Given this, it makes sense to try to quantify the (conjecturally density zero) set

Date: 4 October 2016.

1991 *Mathematics Subject Classification.* Primary 14K15; Secondary 11G10, 11G20, 11G30.

Key words and phrases. Abelian surface, curve, Jacobian, reduction, simplicity, reducibility, counting function.

The first author was partially supported by grants from the Simons Foundation (204164) and the NSA (H98230-14-1-0161 and H98230-15-1-0247).

of primes of good reduction for which $A_{\mathfrak{p}}$ is *split*; that is, for which $A_{\mathfrak{p}}$ is isogenous to a product of abelian varieties of smaller dimension. Specifically, define the counting function

$$\pi_{\mathrm{split}}(A/K, z) = \#\{\mathfrak{p} : \mathcal{N}(\mathfrak{p}) \le z \text{ and } A_{\mathfrak{p}} \text{ is split}\}.$$

Some upper bounds for the rate of growth of this function are available. For instance, a special case of [2, Thm. B, p. 42] states that if the image of the ℓ-adic Galois representation attached to the g-dimensional abelian variety A is the full group of symplectic similitudes, then

$$\pi_{\mathrm{split}}(A/K, z) \ll \frac{z(\log\log z)^{1+1/3(2g^2+g+1)}}{(\log z)^{1+1/6(2g^2+g+1)}} \qquad \text{for all } z \ge 3;$$

if one is willing to assume a generalized Riemann hypothesis, one can further show that

$$\pi_{\mathrm{split}}(A/K, z) \ll z^{1-\frac{1}{4g^2+3g+4}} (\log z)^{\frac{2}{4g^2+3g+4}} \qquad \text{for all } z \ge 3. \tag{1}$$

However, there is no reason to believe that even (1) does a very good job of capturing the actual behavior of the function $\pi_{\mathrm{split}}(A/K, z)$. The purpose of the present paper is to explain and support the following hope.

Conjecture 1.1. *Let A/K be a principally-polarizable abelian surface with absolute endomorphism ring $\mathrm{End}_{\overline{K}} A \cong \mathbb{Z}$. Then there is a constant $C_A > 0$ such that*

$$\pi_{\mathrm{split}}(A/K, z) \sim C_A \frac{\sqrt{z}}{\log z} \qquad \text{as } z \to \infty.$$

This statement bears some resemblance to the Lang–Trotter conjecture [32], whose enunciation we briefly recall. Let $E/\mathbb{Q}$ be an elliptic curve with $\mathrm{End}_{\overline{\mathbb{Q}}} E \cong \mathbb{Z}$, and fix a nonzero integer a. Let $\pi(E, a, z)$ be the number of primes $p < z$ such that $E_p(\mathbb{F}_p) - (p+1) = a$. Then Lang and Trotter conjecture that $\pi(E, a, z) \sim C_{E,a}\sqrt{z}/\log z$ as $z \to \infty$, for some constant $C_{E,a}$. They also give a conjectural formula for the constant $C_{E,a}$, but we shall ignore such finer information here.

In Section 2, we review a framework under which one might expect such counting functions to grow like $\sqrt{z}/\log z$. Roughly speaking, the philosophy of Section 2 suggests that Conjecture 1.1 should hold if the probability that a randomly-chosen principally-polarized abelian surface over $\mathbb{F}_q$ is split varies like $q^{-1/2}$. The bulk of our paper is taken up with a proof of a theorem which says that, up to factors of $\log q$, this is indeed the case.

For every positive integer n we let $\mathcal{A}_n$ denote the moduli stack of principally-polarized n-dimensional abelian varieties, so that for every field K the objects of $\mathcal{A}_n(K)$ are the K-isomorphism classes of such principally-polarized varieties over K. For every n and K we also let $\mathcal{A}_{n,\mathrm{split}}(K)$ denote the subset of $\mathcal{A}_n(K)$ consisting of the principally-polarized abelian varieties (A, λ) for which A is not simple over K. This is perhaps an abuse of notation, because there is no geometrically-defined substack $\mathcal{A}_{n,\mathrm{split}}$ giving rise to the sets $\mathcal{A}_{n,\mathrm{split}}(K)$; our definition of 'split' is sensitive to the field of definition.

Theorem 1.2. *We have*

$$\frac{1}{(\log q)^3(\log\log q)^4} \ll \frac{\#\mathcal{A}_{2,\mathrm{split}}(\mathbb{F}_q)}{q^{5/2}} \ll (\log q)^4(\log\log q)^2 \qquad \textit{for all } q.$$

If the generalized Riemann hypothesis is true, we have

$$\frac{1}{(\log q)(\log\log q)^6} \ll \frac{\#\mathcal{A}_{2,\mathrm{split}}(\mathbb{F}_q)}{q^{5/2}} \ll (\log q)^2(\log\log q)^4 \qquad \textit{for all } q.$$

Since $\mathcal{A}_2$ is irreducible of dimension 3, Theorem 1.2 implies that, up to logarithmic factors, the chance that a randomly chosen principally-polarized abelian surface over $\mathbb{F}_q$ is split varies like $q^{-1/2}$.

The paper closes by presenting some numerical data, including evidence in favor of Conjecture 1.1. We also indicate what we believe to be true when one considers varieties that are geometrically split, and not just split over the base field.

After the first-named author gave a preliminary report on this work, including some data obtained using `sage`, William Stein suggested contacting Andrew Sutherland for help with more extensive calculations. Sutherland provided us with the program `smalljac` [28], which we ran on our own computers to obtain data on the mod-p reductions of the curve $y^2 = x^5 + x + 6$ over $\mathbb{Q}$; later, Sutherland kindly used his own computers, running a program based on the algorithm in [14], to provide us with reduction data for this curve for all primes up to 2^{30}. It is a pleasure to acknowledge Sutherland's assistance. The data presented in Sections 11.1 and 11.2 was obtained using gp and MAGMA.

As we were writing up the various asymptotic estimates of number-theoretic functions that appear in this paper, the second-named author thought frequently of Professor Tom M. Apostol, in whose undergraduate Caltech course Math 160 he first became familiar with such computations. Not long after we completed this paper, Apostol passed away. We dedicate this work to his memory.

Notation and conventions. If Z is a set of real numbers and f and g are real-valued functions on Z, we use the Vinogradov notation

$$f(z) \ll g(z) \qquad \text{for } z \in Z$$

to mean that there is a constant C such that $|f(z)| \le C|g(z)|$ for all $z \in Z$. If Z contains arbitrarily large positive reals, we use

$$f(z) \sim g(z) \qquad \text{as } z \to \infty$$

to mean that $f(z)/g(z) \to 1$ as $z \to \infty$, and we write $f(z) \asymp g(z)$ to mean that there are positive constants C_1 and C_2 such that $C_1|g(z)| \le |f(z)| \le C_2|g(z)|$ for all sufficiently large z.

When we are working over a finite field $\mathbb{F}_q$, we will use without further comment the letter p to denote the prime divisor of q. This convention unfortunately conflicts with the standard use in analytic number theory of the letter p as a generic prime, for instance when writing Euler product representations of arithmetic functions. In such situations in this paper (see for example equation (4) in Section 4), we will instead use ℓ to denote a generic prime, and we explicitly allow the possibility that $\ell = p$.

A *curve* over a field K is a smooth, projective, irreducible variety over K of dimension one, and a *Jacobian* is the neutral component of the Picard scheme of such a curve.

2. Conjectures of Lang–Trotter type

Let $\mathcal{M}$ be a moduli space of PEL type [41]. Let K be a number field, let $\Delta \in \mathcal{O}_K$ be nonzero, and let S be the set of primes of K that do not divide Δ. If $\mathfrak{p}$ is a prime of K we let $\mathbb{F}_\mathfrak{p}$ denote its residue field. Equip each finite set $\mathcal{M}(\mathbb{F}_\mathfrak{p})$ with the uniform probability measure, and let $\underline{A}_\mathfrak{p}$ be a random variable on $\mathcal{M}(\mathbb{F}_\mathfrak{p})$. Suppose that for each $\mathfrak{p} \in S$ a subset $T_\mathfrak{p} \subset \mathcal{M}(\mathbb{F}_\mathfrak{p})$ is specified, with indicator function $I_\mathfrak{p}$. Let $\underline{A} = \prod_{\mathfrak{p} \in S} \underline{A}_\mathfrak{p}$, and let

$$\pi(\underline{A}, I, z) = \sum_{\mathfrak{p} \in S:\ \mathcal{N}(\mathfrak{p}) < z} \frac{\#T_\mathfrak{p}}{\#\mathcal{M}(\mathbb{F}_\mathfrak{p})}$$

be the expected value of $\sum_{\mathfrak{p}\in S:\ \mathcal{N}(\mathfrak{p})\le z} I_{\mathfrak{p}}(\underline{A}_{\mathfrak{p}})$. If $\#T_{\mathfrak{p}}/\#\mathcal{M}(\mathbb{F}_{\mathfrak{p}}) \asymp 1/\mathcal{N}(\mathfrak{p})^m$, then Landau's prime ideal theorem [30, p. 670] yields the estimate $\pi(\underline{A}, I, z) \asymp \int_2^z \frac{dx}{x^m \log x}$. In particular, for $m = 1/2$ one finds that $\pi(\underline{A}, I, z) \asymp \sqrt{z}/\log z$.

Henceforth, assume $\mathcal{M}$ and $T_{\mathfrak{p}}$ are chosen so that the above holds with $m = 1/2$. Now suppose that $A \in \mathcal{M}(\mathcal{O}_K[1/\Delta])$, and let

$$\pi(A, I, z) = \sum_{\mathfrak{p}\in S:\ \mathcal{N}(\mathfrak{p})\le z} I_{\mathfrak{p}}(A_{\mathfrak{p}}).$$

If one *assumes* that (A is sufficiently general, and thus) A is well-modeled by the random variable $\underline{A}$, then one predicts that

$$\pi(A, I, z) \asymp \frac{\sqrt{z}}{\log z}. \tag{2}$$

(By "sufficiently general" one might mean, for example, that the Mumford–Tate group of A is the same as the group attached to the Shimura variety $\mathcal{M}$; but this will not be pursued here.)

For instance, let $\mathcal{A}_1$ be the moduli stack of elliptic curves, and let a be a nonzero integer. On one hand, since $\mathcal{A}_1$ is irreducible and one-dimensional, we have the estimate $\#\mathcal{A}_1(\mathbb{F}_q) \asymp q$. On the other hand, the number of isomorphism classes of elliptic curves over $\mathbb{F}_q$ with trace of Frobenius a is the Kronecker class number $H(a^2 - 4q)$. Up to (at worst) logarithmic factors, the class number $H(a^2 - 4q)$ grows like $\sqrt{|a^2 - 4q|} \sim 2\sqrt{q}$ (see Lemma 4.4). In this case, the prediction (2) yields the Lang–Trotter conjecture.

We interpret Theorem 1.2 as saying that the number of principally-polarized split abelian surfaces over $\mathbb{F}_q$ is approximately $q^{5/2}$. This, combined with the fact that $\dim \mathcal{A}_2 = 3$ and thus $\#\mathcal{A}_3(\mathbb{F}_q) \asymp q^3$, is the inspiration behind Conjecture 1.1.

In spite of the apparent depth and difficulty of the Lang–Trotter conjecture, we are certainly not the first to have attempted to formulate analogous conjectures in related contexts. In [36], Murty poses the problem of counting the primes $\mathfrak{p}$ for which, in a given Galois representation $\rho\colon \mathrm{Gal}(K) \to \mathrm{GL}_r(\mathcal{O}_\lambda)$, the trace of Frobenius $\mathrm{tr}(\rho(\sigma_{\mathfrak{p}}))$ is a given number a. The work of Bayer and González [5] is philosophically more similar to the present paper. Bayer and González consider a modular abelian variety $A/\mathbb{Q}$ and study the number of primes p such that the reduction A_p has p-rank zero. Unfortunately, in most situations, both [5, Conj. 8.2, p. 69] and [36, Conj. 2.15, p. 199] predict a counting function $\pi(z)$ which either grows like $\log\log z$ or is absolutely bounded. In contrast, Conjecture 1.1 has the modest virtue of involving functions that grow visibly over the range of computationally-feasible values of z.

3. Split abelian surfaces over finite fields

In this section we articulate the proof of Theorem 1.2, which gives asymptotic upper and lower bounds on the number of principally-polarized abelian surfaces over finite fields such that the abelian surface is isogenous to a product of elliptic curves. There are several different types of such surfaces, each of which we analyze separately.

First, there are the abelian surfaces over $\mathbb{F}_q$ that are isogenous to a product $E_1 \times E_2$ of two ordinary elliptic curves, with E_1 and E_2 lying in two different isogeny classes. We call this the *ordinary split nonisotypic* case.

Proposition 3.1. *The number W_q of principally-polarized ordinary split nonisotypic abelian surfaces over $\mathbb{F}_q$ satisfies*

$$W_q \ll \begin{cases} q^{5/2}(\log q)^4(\log\log q)^2 & \text{for all } q, \text{ unconditionally,} \\ q^{5/2}(\log q)^2(\log\log q)^4 & \text{for all } q, \text{ under GRH.} \end{cases}$$

Second, there are the abelian surfaces over $\mathbb{F}_q$ that are isogenous to the square of an ordinary elliptic curve. We call this the *ordinary split isotypic* case.

Proposition 3.2. *The number X_q of principally-polarized ordinary split isotypic abelian surfaces over $\mathbb{F}_q$ satisfies*

$$X_q \ll \begin{cases} q^2(\log q)^2|\log\log q| & \text{for all } q, \text{ unconditionally,} \\ q^2(\log q)(\log\log q)^2 & \text{for all } q, \text{ under GRH.} \end{cases}$$

Third, there are the abelian surfaces over $\mathbb{F}_q$ that are isogenous to the product of two elliptic curves, exactly one of which is supersingular. We call this the *almost ordinary split* case.

Proposition 3.3. *The number Y_q of principally-polarized almost ordinary split abelian surfaces over $\mathbb{F}_q$ satisfies*

$$Y_q \ll \begin{cases} q^2(\log q)(\log\log q)^2 & \text{for all } q, \text{ unconditionally,} \\ q^2|\log\log q|^3 & \text{for all } q, \text{ under GRH.} \end{cases}$$

And fourth, there are the abelian surfaces over $\mathbb{F}_q$ that are isogenous to the product of two supersingular elliptic curves. We call this the *supersingular split* case.

Proposition 3.4. *The number Z_q of principally-polarized supersingular split abelian surfaces over $\mathbb{F}_q$ satisfies $Z_q \ll q^2$ for all q.*

To prove the lower bound in Theorem 1.2, we estimate the number of ordinary split nonisotypic surfaces.

Proposition 3.5. *The number of W_q of principally-polarized ordinary split nonisotypic abelian surfaces over $\mathbb{F}_q$ satisfies*

$$W_q \gg \begin{cases} \dfrac{q^{5/2}}{(\log q)^3(\log\log q)^4} & \text{for all } q, \text{ unconditionally,} \\ \dfrac{q^{5/2}}{(\log q)(\log\log q)^6} & \text{for all } q, \text{ under GRH.} \end{cases}$$

It is clear that together these propositions provide a proof of Theorem 1.2. We will prove the propositions in the following sections. We begin with some background information and results on endomorphism rings of elliptic curves over finite fields (Section 4) and a review of 'gluing' elliptic curves together (Section 5).

4. Endomorphism rings of elliptic curves over finite fields

In this section we set notation and give some background information on endomorphism rings of elliptic curves over finite fields. With the exception of the concepts of 'strata' and of the 'relative conductor', most of the results on endomorphism rings we mention are standard (see [43, Ch. 4] and [40], and note that [40, Thm. 4.5, p. 194] corrects a small error in [43, Thm. 4.5, p. 541]).

Let E be an elliptic curve over a finite field $\mathbb{F}_q$. The substitution $x \mapsto x^q$ induces an endomorphism $\mathrm{Fr}_E \in \mathrm{End}\, E$ called the *Frobenius* endomorphism. The characteristic polynomial of Fr_E (acting, say, on the ℓ-adic Tate module of E for some $\ell \neq p$) is of the form $f_E(T) = T^2 - a(E)T + q$ for an integer $a(E)$, the *trace of Frobenius*. Two elliptic curves E and E' are isogenous if and only if $a(E) = a(E')$, and Hasse [16, 17, 18] showed that $|a(E)| \leq 2\sqrt{q}$. We will denote the isogeny class corresponding to a by

$$\mathcal{I}(\mathbb{F}_q, a) = \{E/\mathbb{F}_q \colon a(E) = a\}.$$

The isogeny class $\mathcal{I}(\mathbb{F}_q, a)$ is called *ordinary* if $\gcd(a, q) = 1$, and *supersingular* otherwise (see [43, p. 526 and Ch. 7]). The supersingular curves E are characterized by the property that $E[p](\overline{\mathbb{F}}_q) \cong \{0\}$.

If $E/\mathbb{F}_q$ is a supersingular elliptic curve, then $\operatorname{End}_{\overline{\mathbb{F}}_q} E$ is a maximal order in $\mathbb{Q}_{p,\infty}$, the quaternion algebra over $\mathbb{Q}$ ramified exactly at $\{p, \infty\}$. There are two possibilities for $\operatorname{End} E$ itself. It may be that all of the geometric endomorphisms of E are already defined over $\mathbb{F}_q$, so that $\operatorname{End} E$ is a maximal order in $\mathbb{Q}_{p,\infty}$; this happens when q is a square and $a(E)^2 = 4q$. The other possibility is that $\operatorname{End} E$ is an order in an imaginary quadratic field; in this case, the discriminant of $\operatorname{End} E$ is either $-p$, $-4p$, -3, or -4. (See Table 1 in Section 8 for the exact conditions that determine the various cases.)

Suppose $\mathcal{I}(\mathbb{F}_q, a)$ is an isogeny class with $a^2 \neq 4q$. Then $\mathcal{O}_{a,q} := \mathbb{Z}[T]/(T^2 - aT + q)$ is an order in the imaginary quadratic field $K_{a,q} := \mathbb{Q}(\sqrt{a^2 - 4q})$, and is isomorphic to the subring $\mathbb{Z}[\mathrm{Fr}_E]$ of $\operatorname{End} E$ for every $E \in \mathcal{I}(\mathbb{F}_q, a)$. An order $\mathcal{O}$ in $K_{a,q}$ occurs as $\operatorname{End} E$ for some $E \in \mathcal{I}(\mathbb{F}_q, a)$ if and only if $\mathcal{O} \supseteq \mathcal{O}_{a,q}$ and $\mathcal{O}$ is maximal at p (see [43, Thm. 4.2, pp. 538–539] or [40, Thm. 4.3, p. 193]). Note that the maximality at p is automatic when $\mathcal{I}(\mathbb{F}_q, a)$ is ordinary, because in that case q is coprime to the discriminant $a^2 - 4q$ of $\mathcal{O}_{a,q}$. If we let $\mathcal{I}(\mathbb{F}_q, a, \mathcal{O})$ denote the set of isomorphism classes of elliptic curves in $\mathcal{I}(\mathbb{F}_q, a)$ with endomorphism ring $\mathcal{O}$, we can write $\mathcal{I}(\mathbb{F}_q, a)$ as a disjoint union

$$\mathcal{I}(\mathbb{F}_q, a) = \bigsqcup_{\mathcal{O} \supseteq \mathcal{O}_{a,q}} \mathcal{I}(\mathbb{F}_q, a, \mathcal{O}),$$

where $\mathcal{O}$ ranges over all orders of $K_{a,q}$ that contain $\mathcal{O}_{a,q}$ and that are maximal at p. If a is coprime to q, or if $a = 0$ and q is not a square, then each of the sets $\mathcal{I}(\mathbb{F}_q, a, \mathcal{O})$ appearing in the equality above is a torsor for the class group $\mathrm{Cl}(\mathcal{O})$ of the order $\mathcal{O}$. In particular, $\#\mathcal{I}(\mathbb{F}_q, a, \mathcal{O})$ is equal to the class number $h(\mathcal{O})$ of $\mathcal{O}$ (see [40, Thm. 4.5, p. 194]).

We will refer to a nonempty set of the form $\mathcal{I}(\mathbb{F}_q, a, \mathcal{O})$ as a *stratum* of elliptic curves over $\mathbb{F}_q$. Given a stratum $\mathcal{S}$, we will denote the associated trace by $a(\mathcal{S})$ and the associated quadratic order by $\mathcal{O}_{\mathcal{S}}$. If $\mathcal{S}$ and $\mathcal{S}'$ are two strata over $\mathbb{F}_q$, we say that $\mathcal{S}$ and $\mathcal{S}'$ are *isogenous*, and write $\mathcal{S} \sim \mathcal{S}'$, if the elliptic curves in $\mathcal{S}$ are isogenous to those in $\mathcal{S}'$ — that is, if $a(\mathcal{S}) = a(\mathcal{S}')$.

For any imaginary quadratic order $\mathcal{O}$ we let $\Delta(\mathcal{O})$ denote the discriminant of $\mathcal{O}$ and $\Delta^*(\mathcal{O})$ the associated fundamental discriminant — that is, the discriminant of the integral closure of $\mathcal{O}$ in its field of fractions. Then

$$\Delta(\mathcal{O}) = \mathfrak{f}(\mathcal{O})^2 \Delta^*(\mathcal{O}),$$

where $\mathfrak{f}(\mathcal{O})$ is the *conductor* of $\mathcal{O}$. For a trace of Frobenius a with $a^2 \neq 4q$ we will write $\Delta_{a,q}$, $\mathfrak{f}_{a,q}$, and $\Delta^*_{a,q}$ for the corresponding quantities associated to $\mathcal{O}_{a,q}$.

Let $E/\mathbb{F}_q$ be an elliptic curve whose endomorphism ring is a quadratic order. We define the *relative conductor* $\mathfrak{f}_{\mathrm{rel}}(E)$ of E by

$$\mathfrak{f}_{\mathrm{rel}}(E) = \frac{\mathfrak{f}(\mathcal{O}_{a,q})}{\mathfrak{f}(\operatorname{End} E)};$$

this quantity is also equal to the index of $\mathcal{O}_{a,q} \cong \mathbb{Z}[\mathrm{Fr}_E]$ in $\operatorname{End} E$. If $E/\mathbb{F}_q$ is a supersingular elliptic curve with endomorphism ring equal to an order in a quaternion algebra, we adopt the convention $\mathfrak{f}_{\mathrm{rel}}(E) = 0$. The relative conductor depends only on the stratum of E, so for a stratum $\mathcal{S}$ we may define $\mathfrak{f}_{\mathrm{rel}}(\mathcal{S})$ to be the relative conductor of any curve in $\mathcal{S}$.

Proposition 4.1. *Let $E/\mathbb{F}_q$ be an elliptic curve with $\operatorname{End} E$ a quadratic order.*

(a) *The relative conductor $\mathfrak{f}_{\mathrm{rel}}(E)$ is the largest integer r such that there exists an integer b with*

$$\frac{\mathrm{Fr}_E - b}{r} \in \operatorname{End} E.$$

(b) *The relative conductor* $\mathfrak{f}_{\mathrm{rel}}(E)$ *is the largest integer* r *for which* Fr_E *acts as an integer on the group scheme* $E[r]$.
(c) *If* E *is ordinary, the relative conductor* $\mathfrak{f}_{\mathrm{rel}}(E)$ *is the largest integer* r*, coprime to* q*, for which* Fr_E *acts as an integer on the group* $E[r](\overline{\mathbb{F}}_q)$.

Proof. Let $\mathcal{O}$ be the maximal order containing $\mathrm{End}\, E$ and let ω be an element of $\mathcal{O}$ such that $\mathcal{O} = \mathbb{Z}[\omega]$. Write $\mathrm{Fr}_E = u + v\omega$ for integers u and v; then $\mathbb{Z}[\mathrm{Fr}_E] = \mathbb{Z} + v\mathcal{O}$, so $v = \mathfrak{f}(\mathbb{Z}[\mathrm{Fr}_E])$.

On one hand, suppose r is an integer for which there is an integer b with $(\mathrm{Fr}_E - b)/r \in \mathrm{End}\, E$. Then $\mathrm{End}\, E \supseteq \mathbb{Z} + (v/r)\mathcal{O}$, so r is a divisor of the relative conductor. On the other hand, if s is the relative conductor of E, then $\mathrm{End}\, E = \mathbb{Z} + (v/s)\mathcal{O} = \mathbb{Z}[(v/s)\omega]$, so $(\mathrm{Fr}_E - u)/s$ is an element of $\mathrm{End}\, E$. This proves (a).

If Fr_E acts as an integer b on the group scheme $E[r]$, then the endomorphism $\mathrm{Fr}_E - b$ kills $E[r]$. This implies that $\mathrm{Fr}_E - b$ factors through multiplication-by-r, which means that $(\mathrm{Fr}_E - b)/r$ lies in $\mathrm{End}\, E$. Conversely, if $(\mathrm{Fr}_E - b)/r$ lies in $\mathrm{End}\, E$, then Fr_E acts on $E[r]$ as the integer b. Thus, (b) follows from (a).

Suppose E is ordinary. The endomorphism Fr_E does not act as an integer on the group scheme $E[p]$, because it acts non-invertibly (consider the local part of $E[p]$), but not as zero (consider the reduced part of $E[p]$). Therefore, the integer defined by (b) will not change if we add the requirement that r be coprime to p. For integers r coprime to p, the group scheme $E[r]$ is determined by the Galois module $E[r](\overline{\mathbb{F}}_q)$. Thus, (c) follows from (b). □

Corollary 4.2. *Let* $E/\mathbb{F}_q$ *be an elliptic curve with relative conductor* r*, and let* n *be a positive integer. The largest divisor* d *of* n *such that* Fr_E *acts as an integer on* $E[d]$ *is equal to* $\gcd(n, r)$.

Proof. When $\mathrm{End}\, E$ is a quadratic order, this follows immediately from Proposition 4.1. If the endomorphism ring of E is an order in a quaternion algebra, then q is a square and $\mathrm{Fr}_E = \pm\sqrt{q}$; that is, Fr_E *is* an integer, so that $d = n = \gcd(n, 0)$. □

Later in the paper we will need to have bounds on the sizes of the automorphism groups of schemes of the form $E[n]$ for ordinary E and positive integers n. Our bounds will involve the Euler function $\varphi(n)$ as well as the arithmetic function ψ defined by $\psi(n) = n\prod_{\ell|n}(1 + 1/\ell)$.

Proposition 4.3. *Let* E *be an elliptic curve over* $\mathbb{F}_q$*, let* n *be a positive integer, and let* $g = \gcd(n, \mathfrak{f}_{\mathrm{rel}}(E))$. *If* E *is supersingular, assume that* n *is coprime to* q. *Then*

$$\varphi(n) \le \frac{\#\operatorname{Aut} E[n]}{g^2\varphi(n)} \le \psi(n). \tag{3}$$

Proof. Every term in the inequality is multiplicative in n, so it suffices to consider the case where n is a prime power ℓ^e.

Suppose $\ell = p$. In this case, E must be ordinary by assumption. Note that the relative conductor divides the discriminant $a^2 - 4q$, where $a = a(E)$ is coprime to p because E is ordinary. Therefore the relative conductor is coprime to p, so $g = 1$.

The group scheme $E[n]$ is the product of a reduced-local group scheme G_1 and a local-reduced group scheme G_2, each of rank n. The group scheme G_1 is geometrically isomorphic to $\mathbb{Z}/n$, with Frobenius acting as multiplication by an integer (which is congruent to a modulo q). The automorphism group of G_1 is $(\mathbb{Z}/n)^\times$, and has cardinality $\varphi(n)$.

The group scheme G_2 is geometrically isomorphic to $\boldsymbol{\mu}_n$, the group scheme of n-th roots of unity, with Frobenius acting as power-raising by an integer. The automorphism group of G_2 is also $(\mathbb{Z}/n)^\times$, and has cardinality $\varphi(n)$.

Since there are no nontrivial morphisms between G_1 and G_2, the automorphism group of $E[n]$ is the product of the automorphism groups of G_1 and G_2. Thus, when n is a power of p the middle term of (3) is equal to $\varphi(n)$, and the two inequalities of (3) both hold.

Now suppose $\ell \neq p$. In this case, the group scheme $E[n]$ can be understood completely in terms of its geometric points and the action of Frobenius on them. The group $E[n](\overline{\mathbb{F}}_q)$ is isomorphic to $(\mathbb{Z}/n)^2$, and if we fix such an isomorphism the Frobenius endomorphism is given by an element γ of $\mathrm{GL}_2(\mathbb{Z}/n)$ whose trace is a and whose determinant is q. The automorphism group of $E[n]$ is then isomorphic to the subgroup of $\mathrm{GL}_2(\mathbb{Z}/n)$ consisting of those elements that commute with γ; that is, the centralizer $Z(\gamma)$ of γ.

Let r be the largest divisor of n such that Fr_E acts as an integer on $E[r]$; Proposition 4.1 shows that $r = g$. Then there is an integer d (uniquely determined modulo g) and a matrix $\beta \in \mathrm{GL}_2(\mathbb{Z}/n)$ such that $g \cdot \beta \in g\,\mathrm{Mat}_2(\mathbb{Z}/n) \cong \mathrm{Mat}_2(\mathbb{Z}/(n/g))$ is cyclic and such that $\gamma = d \cdot I + g \cdot \beta$. (See [4, 44] for details.)

Given this expression for γ, we can explicitly compute the centralizer $Z(\gamma)$. If $g = n$ then $Z(\gamma) = \mathrm{GL}_2(\mathbb{Z}/n)$, so $Z(\gamma)$ has order $n\psi(n)\varphi(n)^2$. If g is a proper divisor of n then $Z(\gamma)$ is the group of all $\alpha \in \mathrm{GL}_2(\mathbb{Z}/n)$ such that the image of α in $\mathrm{GL}_2(\mathbb{Z}/(n/g)) \subset \mathrm{Mat}_2(\mathbb{Z}/(n/g))$ lies in the $\mathbb{Z}/(n/g)$-span of I and β. The order of this subgroup of $\mathrm{GL}_2(\mathbb{Z}/(n/g))$ is equal to $\varphi(n/g)$ times

$$\begin{cases} \psi(n/g) & \text{if } \beta \bmod \ell \text{ has no eigenvalues in } \mathbb{Z}/\ell; \\ n/g & \text{if } \beta \bmod \ell \text{ has 1 eigenvalue in } \mathbb{Z}/\ell; \\ \varphi(n/g) & \text{if } \beta \bmod \ell \text{ has 2 eigenvalues in } \mathbb{Z}/\ell, \end{cases}$$

so the order of its preimage in $\mathrm{GL}_2(\mathbb{Z}/n)$ is either $g^2\psi(n)\varphi(n)$ or $g^2 n\varphi(n)$ or $g^2\varphi(n)^2$. In every case we find that

$$g^2\varphi(n)^2 \leq \#Z(\gamma) \leq g^2\psi(n)\varphi(n),$$

which gives (3). (Alternative methods of calculating $Z(\gamma)$ can be found in [44].) □

Later in the paper we would like to have estimates for the sizes of isogeny classes and strata; since these sizes are given by class numbers, we close this section by reviewing some bounds on class numbers.

We denote the class number of an imaginary quadratic order $\mathcal{O}$ by $h(\mathcal{O})$; this is the size of the group of equivalence classes of invertible fractional ideals of $\mathcal{O}$. We let $H(\mathcal{O})$ denote the Kronecker class number of $\mathcal{O}$, defined by

$$H(\mathcal{O}) = \sum_{\mathcal{O}' \supseteq \mathcal{O}} h(\mathcal{O}'),$$

where the sum is over all quadratic orders that contain $\mathcal{O}$. If Δ is the discriminant of an imaginary quadratic order $\mathcal{O}$, we write $h(\Delta)$ and $H(\Delta)$ for $h(\mathcal{O})$ and $H(\mathcal{O})$, respectively.

Lemma 4.4. *We have*

$$h(\Delta) \ll \begin{cases} |\Delta|^{1/2}\log|\Delta| & \text{for fundamental } \Delta < 0, \\ |\Delta|^{1/2}\log|\Delta|\log\log|\Delta| & \text{for all } \Delta < 0; \end{cases}$$
$$H(\Delta) \ll |\Delta|^{1/2}\log|\Delta|(\log\log|\Delta|)^2 \quad \text{for all } \Delta < 0.$$

If the generalized Riemann hypothesis is true, we have

$$h(\Delta) \ll \begin{cases} |\Delta|^{1/2}\log\log|\Delta| & \text{for fundamental } \Delta < 0, \\ |\Delta|^{1/2}(\log\log|\Delta|)^2 & \text{for all } \Delta < 0; \end{cases}$$
$$H(\Delta) \ll |\Delta|^{1/2}(\log\log|\Delta|)^3 \quad \text{for all } \Delta < 0.$$

Proof. The unconditional bound on $h(\Delta)$ for fundamental Δ comes from [9, Exer. 5.27, p. 301], and the conditional bound from [33, Thm. 1, p. 367].

For an arbitrary negative discriminant Δ, write $\Delta = \mathfrak{f}^2\,\Delta^*$ for a fundamental discriminant Δ^*, and let χ be the quadratic character modulo Δ^*. Then

$$h(\Delta) = \mathfrak{f}\,h(\Delta^*)\prod_{\ell\mid\mathfrak{f}}\left(1-\frac{\chi(\ell)}{\ell}\right) \le \mathfrak{f}\,h(\Delta^*)\prod_{\ell\mid\mathfrak{f}}\left(1+\frac{1}{\ell}\right) \le h(\Delta^*)\sigma(\mathfrak{f}), \tag{4}$$

where σ is the sum-of-divisors function (and we recall that ℓ ranges over all prime divisors of $\mathfrak{f}$). Since $\sigma(n) \ll n\log\log n$ for $n > 2$ by [13, Thm. 323, p. 266], we find that

$$h(\Delta) \ll \mathfrak{f}\,h(\Delta^*)\log\log|\Delta| \qquad \text{for all } \Delta < 0.$$

Combining this with the class number bounds for fundamental discriminants gives us the bounds for arbitrary discriminant.

For Kronecker class numbers, note that

$$H(\Delta) = \sum_{f\mid\mathfrak{f}} h(f^2\Delta^*) = \sum_{f\mid\mathfrak{f}} f h(\Delta^*)\prod_{\ell\mid f}\left(1-\frac{\chi(\ell)}{\ell}\right) \le h(\Delta^*)\left(\sum_{f\mid\mathfrak{f}} f\right)\prod_{\ell\mid\mathfrak{f}}\left(1+\frac{1}{\ell}\right) \le \mathfrak{f}^{-1}\,h(\Delta^*)\sigma(\mathfrak{f})^2,$$

so that

$$H(\Delta) \ll \mathfrak{f}\,h(\Delta^*)(\log\log|\Delta|)^2 \qquad \text{for all } \Delta < 0.$$

This leads to the desired bounds on $H(\Delta)$. □

5. Gluing elliptic curves

In this section, we review work of Frey and Kani [11] that explains how to construct principally-polarized abelian surfaces from pairs of elliptic curves provided with some extra structure. First, we discuss isomorphisms of torsion subgroups of elliptic curves.

Let E and F be elliptic curves over a field K and let $n > 0$ be an integer. We let $\mathrm{Isom}(E[n], F[n])$ denote the set of group scheme isomorphisms between the n-torsion subschemes of E and F. The Weil pairing gives us nondegenerate alternating pairings

$$E[n]\times E[n] \to \boldsymbol{\mu}_n \quad \text{and} \quad F[n]\times F[n] \to \boldsymbol{\mu}_n$$

from the n-torsion subschemes of E and of F to the n-torsion of the multiplicative group scheme. Via the Weil pairing, we get a map

$$m\colon \mathrm{Isom}(E[n], F[n]) \to \mathrm{Aut}\,\boldsymbol{\mu}_n \cong (\mathbb{Z}/n\mathbb{Z})^\times.$$

For every $i \in (\mathbb{Z}/n\mathbb{Z})^\times$ we let $\mathrm{Isom}^i(E[n], F[n])$ denote the set $m^{-1}(i)$, so that $\mathrm{Isom}^1(E[n], F[n])$ consists of the group scheme isomorphisms that respect the Weil pairing, and $\mathrm{Isom}^{-1}(E[n], F[n])$ consists of the anti-isometries from $E[n]$ to $F[n]$.

If η is an anti-isometry from $E[n]$ to $F[n]$, then the graph G of η is a subgroup scheme of $(E\times F)[n]$ that is maximal isotropic with respect to the product of the Weil pairings. It follows from [35, Cor. to Thm. 2, p. 231] that n times the canonical principal polarization on $E\times F$ descends to a principal polarization λ on the abelian surface $A := (E\times F)/G$. In this situation, we say that the polarized surface (A,λ) is obtained by *gluing* E and F together along their n-torsion subgroups via η.

Frey and Kani [11] show that every principally-polarized abelian surface (A,λ) that is isogenous to a product of two elliptic curves arises in this way; furthermore, if such an A is not isogenous to the square of an elliptic curve, then the E, F, n, and η that give rise to the polarized surface (A,λ) are unique up to isomorphism and up to interchanging the triple (E,F,η) with (F,E,η^{-1}).

Frey and Kani also note that if the polarized surface (A,λ) constructed in this way is the canonically-polarized Jacobian of a curve C, then there are minimal degree-n maps $\alpha\colon C\to E$ and $\beta\colon C\to F$ such that $\alpha_*\beta^* = 0$; here *minimal* means that α and β do not factor through nontrivial isogenies. Conversely, every pair of minimal degree-n maps $\alpha\colon C\to E$ and $\beta\colon C\to F$ such that $\alpha_*\beta^* = 0$ arises in this way.

6. Ordinary split nonisotypic surfaces

In this section we will prove Proposition 3.1. The proof depends on three lemmas, whose proofs we postpone until the end of the section.

Lemma 6.1. *The number W_q of principally-polarized ordinary split nonisotypic abelian surfaces over $\mathbb{F}_q$ is at most*

$$\sum_{\mathcal{S}} \sum_{\mathcal{S}' \not\sim \mathcal{S}} h(\mathcal{O}_{\mathcal{S}}) h(\mathcal{O}_{\mathcal{S}'}) \mathfrak{f}_{\mathrm{rel}}(\mathcal{S}) \mathfrak{f}_{\mathrm{rel}}(\mathcal{S}') \sum_{n \mid (a(\mathcal{S}) - a(\mathcal{S}'))} \psi(n),$$

where the first sum is over ordinary strata $\mathcal{S}$, and the second is over ordinary strata $\mathcal{S}'$ not isogenous to $\mathcal{S}$.

Lemma 6.2. *We have*

$$\sum_{d \mid n} \psi(d) \ll n (\log\log n)^2 \qquad \text{for all } n > 1.$$

Lemma 6.3. *We have*

$$\sum_{\text{ordinary } E/\mathbb{F}_q} \mathfrak{f}_{\mathrm{rel}}(E) \ll \begin{cases} q(\log q)^2 & \text{for all } q, \text{ unconditionally,} \\ q(\log q)|\log\log q| & \text{for all } q, \text{ under GRH.} \end{cases}$$

Given these lemmas, the proof of Proposition 3.1 is straightforward.

Proof of Proposition 3.1. From Lemmas 6.1 and 6.2 we find that

$$W_q \ll q^{1/2} (\log\log q)^2 \sum_{\mathcal{S}} \sum_{\mathcal{S}' \not\sim \mathcal{S}} h(\mathcal{O}_{\mathcal{S}}) h(\mathcal{O}_{\mathcal{S}'}) \mathfrak{f}_{\mathrm{rel}}(\mathcal{S}) \mathfrak{f}_{\mathrm{rel}}(\mathcal{S}') \qquad \text{for all } q.$$

Since

$$\sum_{\mathcal{S}} \sum_{\mathcal{S}' \not\sim \mathcal{S}} h(\mathcal{O}_{\mathcal{S}}) h(\mathcal{O}_{\mathcal{S}'}) \mathfrak{f}_{\mathrm{rel}}(\mathcal{S}) \mathfrak{f}_{\mathrm{rel}}(\mathcal{S}') < \left(\sum_{\mathcal{S}} h(\mathcal{O}_{\mathcal{S}}) \mathfrak{f}_{\mathrm{rel}}(\mathcal{S}) \right)^2 = \left(\sum_{\text{ordinary } E/\mathbb{F}_q} \mathfrak{f}_{\mathrm{rel}}(E) \right)^2,$$

we have

$$W_q \ll q^{1/2} (\log\log q)^2 \left(\sum_{\text{ordinary } E/\mathbb{F}_q} \mathfrak{f}_{\mathrm{rel}}(E) \right)^2 \qquad \text{for all } q.$$

Combining this with Lemma 6.3, we find that we have

$$W_q \ll \begin{cases} q^{5/2} (\log q)^4 (\log\log q)^2 & \text{for all } q, \text{ unconditionally,} \\ q^{5/2} (\log q)^2 (\log\log q)^4 & \text{for all } q, \text{ under GRH.} \end{cases}$$

□

Now we turn to Lemmas 6.1, 6.2, and 6.3. The proof of Lemma 6.1 itself requires some notation and a preparatory result.

Fix an elliptic curve $E/\mathbb{F}_q$ and a stratum $\mathcal{S}$ of elliptic curves over $\mathbb{F}_q$. For a positive integer n, let

$$\mathrm{Isom}(E, \mathcal{S}, n) = \{(E, E', \eta) : E' \in \mathcal{S}, \eta \in \mathrm{Isom}(E[n], E'[n])\}$$
$$\mathrm{Isom}^{-1}(E, \mathcal{S}, n) = \{(E, E', \eta) : E' \in \mathcal{S}, \eta \in \mathrm{Isom}^{-1}(E[n], E'[n])\}.$$

Lemma 6.4. *Suppose that either $\mathcal{S}$ is ordinary, or that $a(\mathcal{S}) = 0$ and q is a nonsquare. If $\mathrm{Isom}^{-1}(E, \mathcal{S}, n)$ is nonempty then $\gcd(n, \mathfrak{f}_{\mathrm{rel}}(E)) = \gcd(n, \mathfrak{f}_{\mathrm{rel}}(\mathcal{S}))$, and we have*

$$\#\,\mathrm{Isom}^{-1}(E, \mathcal{S}, n) \le 2\psi(n) h(\mathcal{O}_{\mathcal{S}}) \gcd(n, \mathfrak{f}_{\mathrm{rel}}(E)) \gcd(n, \mathfrak{f}_{\mathrm{rel}}(\mathcal{S})).$$

In particular, if $\mathfrak{f}_{\mathrm{rel}}(E) \neq 0$, then

$$\#\,\mathrm{Isom}^{-1}(E, \mathcal{S}, n) \le 2\psi(n) h(\mathcal{O}_{\mathcal{S}}) \mathfrak{f}_{\mathrm{rel}}(E) \mathfrak{f}_{\mathrm{rel}}(\mathcal{S}).$$

Proof. Suppose that $\mathrm{Isom}^{-1}(E,\mathcal{S},n)$ is nonempty. Then there is an $E' \in \mathcal{S}$ for which there is an isomorphism $E[n] \cong E'[n]$. Corollary 4.2 then shows that $\gcd(n, \mathfrak{f}_{\mathrm{rel}}(E)) = \gcd(n, \mathfrak{f}_{\mathrm{rel}}(E')) = \gcd(n, \mathfrak{f}_{\mathrm{rel}}(\mathcal{S}))$.

The class group $\mathrm{Cl}(\mathcal{O}_\mathcal{S})$ acts on $\mathcal{S}$, and the assumption that either $\mathcal{S}$ is ordinary or that $a(\mathcal{S}) = 0$ and q is a nonsquare implies that $\mathcal{S}$ is a torsor for the class group. Define an action of $\mathrm{Aut}\, E[n] \times \mathrm{Cl}(\mathcal{O}_\mathcal{S})$ on the nonempty set $\mathrm{Isom}(E,\mathcal{S},n)$ by setting

$$(\alpha, [\mathfrak{a}]) \circ (E, E', \eta) = (E, [\mathfrak{a}] * E', [\mathfrak{a}] \circ \eta \circ \alpha^{-1}).$$

It is clear that $\mathrm{Isom}(E,\mathcal{S},n)$ is a torsor for $\mathrm{Aut}\, E[n] \times \mathrm{Cl}(\mathcal{O}_\mathcal{S})$ under this action, so using Proposition 4.3 we find that

$$\#\mathrm{Isom}(E,\mathcal{S},n) \le \left(\#\mathrm{Aut}\, E[n]\right) h(\mathcal{O}_\mathcal{S}) \le g^2 \varphi(n)\psi(n) h(\mathcal{O}_\mathcal{S}),$$

where $g = \gcd(n, \mathfrak{f}_{\mathrm{rel}}(E))$. Therefore

$$\#\mathrm{Isom}(E,\mathcal{S},n) \le \varphi(n)\psi(n) h(\mathcal{O}_\mathcal{S}) \gcd(n, \mathfrak{f}_{\mathrm{rel}}(E)) \gcd(n, \mathfrak{f}_{\mathrm{rel}}(\mathcal{S})).$$

In the preceding section we defined a map $m\colon \mathrm{Isom}(E[n], E'[n]) \to \mathrm{Aut}\, \boldsymbol{\mu}_n$ that sends a group scheme isomorphism to the automorphism of $\boldsymbol{\mu}_n$ induced by the Weil pairing. This gives rise to a map from $\mathrm{Isom}(E,\mathcal{S},n)$ to $\mathrm{Aut}\, \boldsymbol{\mu}_n$, which we continue to denote by m, that sends a triple (E, E', η) to $m(\eta)$. We claim that the image of this map is a coset of a subgroup of $\mathrm{Aut}\, \boldsymbol{\mu}_n$ of index at most 2.

To see this, we use the theory of complex multiplication, the Galois-equivariance of the Weil pairing, and class field theory for the extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ as follows. Let K be the field of fractions of $\mathcal{O}_\mathcal{S}$. Given $[\mathfrak{a}] \in \mathrm{Cl}(\mathcal{O}_\mathcal{S})$ and $(E, E', \eta) \in \mathrm{Isom}(E,\mathcal{S},n)$, we have

$$m((1, [\mathfrak{a}]) \circ (E, E', \eta)) = (\mathcal{N}_{K/\mathbb{Q}}(\mathfrak{a}), \mathbb{Q}(\zeta_n)/\mathbb{Q}) \circ m(\eta) \in \mathrm{Aut}\, \boldsymbol{\mu}_n,$$

where $(\,\cdot\,, \mathbb{Q}(\zeta_n)/\mathbb{Q})$ denotes the Artin symbol for the extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$. Since the group of norms of idèle classes of K has index $[K : \mathbb{Q}] = 2$ in the group of idèle classes of $\mathbb{Q}$, the image of the map m is a coset of a subgroup of index at most 2.

Therefore, the number of elements in $\mathrm{Isom}^{-1}(E,\mathcal{S},n)$ is at most $2/\varphi(n)$ times the number of elements in $\mathrm{Isom}(E,\mathcal{S},n)$, and we obtain the inequality in the lemma. □

Proof of Lemma 6.1. As we noted in Section 5, every principally-polarized ordinary split nonisotypic surface over $\mathbb{F}_q$ is obtained in exactly two ways by gluing two ordinary nonisogenous curves E and E' together along their n-torsion. Since we must then have $E[n] \cong E'[n]$, the traces of Frobenius of E and E' must be congruent to one another modulo n; that is, $n \mid (a(E) - a(E'))$. Summing over ordinary E and E', we find that

$$\begin{aligned}
2W_q &= \sum_E \sum_{E' \not\sim E} \sum_{n \mid (a(E)-a(E'))} \#\mathrm{Isom}^{-1}(E[n], E'[n]) \\
&= \sum_E \sum_{\mathcal{S}' \not\sim E} \sum_{n \mid (a(E)-a(\mathcal{S}'))} \#\mathrm{Isom}^{-1}(E, \mathcal{S}', n) \\
&\le \sum_E \sum_{\mathcal{S}' \not\sim E} \sum_{n \mid (a(E)-a(\mathcal{S}'))} 2\psi(n) h(\mathcal{O}_{\mathcal{S}'}) \mathfrak{f}_{\mathrm{rel}}(E) \mathfrak{f}_{\mathrm{rel}}(\mathcal{S}') \qquad \text{(by Lemma 6.4)} \\
&\le 2 \sum_E \sum_{\mathcal{S}' \not\sim E} h(\mathcal{O}_{\mathcal{S}'}) \mathfrak{f}_{\mathrm{rel}}(E) \mathfrak{f}_{\mathrm{rel}}(\mathcal{S}') \sum_{n \mid (a(E)-a(\mathcal{S}'))} \psi(n) \\
&= 2 \sum_\mathcal{S} \sum_{\mathcal{S}' \not\sim \mathcal{S}} h(\mathcal{O}_\mathcal{S}) h(\mathcal{O}_{\mathcal{S}'}) \mathfrak{f}_{\mathrm{rel}}(\mathcal{S}) \mathfrak{f}_{\mathrm{rel}}(\mathcal{S}') \sum_{n \mid (a(\mathcal{S})-a(\mathcal{S}'))} \psi(n),
\end{aligned}$$

which proves the lemma. □

Proof of Lemma 6.2. Denote the sum on the left by $f(n)$, so that f is a multiplicative function. We calculate that $f(n)/n \le \prod_{\ell|n}(1+\frac{1}{\ell})/(1-\frac{1}{\ell})$. Taking this inequality and multiplying by the square of the identity $\varphi(n)/n = \prod_{\ell|n}(1-\frac{1}{\ell})$, we find that

$$\frac{f(n)}{n(\log\log n)^2}\left(\frac{\varphi(n)\log\log n}{n}\right)^2 \le \prod_{\ell|n}\left(1-\frac{1}{\ell^2}\right) \le 1.$$

Landau [31] showed that $\liminf \varphi(n)(\log\log n)/n = e^{-\gamma}$, where γ is Euler's constant. The lemma follows. □

Our proof of Lemma 6.3 requires an estimate from analytic number theory. Let C be the multiplicative arithmetic function defined on prime powers ℓ^e by $C(\ell^e) = 2(1+1/\ell)$.

Lemma 6.5. *We have*

$$\sum_{n\le x} C(n) \ll x\log x \qquad \text{for all } x > 1.$$

Proof. Let D be the Dirichlet product ([3, §2.6]) of C with the Möbius function μ, so that

$$C(n) = \sum_{d|n} D(d).$$

We compute that D is the multiplicative function defined on prime powers ℓ^e by

$$D(\ell^e) = \begin{cases} 1+2/\ell & \text{if } e = 1, \\ 0 & \text{if } e > 1. \end{cases}$$

Then

$$\sum_{n\le x} C(n) = \sum_{n\le x}\sum_{d|n} D(d) = \sum_{d\le x} D(d)\left\lfloor \frac{x}{d}\right\rfloor \le x\sum_{d\le x}\frac{D(d)}{d},$$

so we need only show that $\sum_{d\le x} D(d)/d \ll \log x$ for $x > 1$.

Note that

$$\sum_{i=0}^{\infty}\frac{D(\ell^i)}{\ell^i} = 1+\frac{1}{\ell}+\frac{2}{\ell^2},$$

so that

$$\sum_{d\le x}\frac{D(d)}{d} \le \prod_{\ell\le x}\left(1+\frac{1}{\ell}+\frac{2}{\ell^2}\right).$$

Taking logarithms, we find that

$$\begin{aligned}\log\sum_{d\le x}\frac{D(d)}{d} &\le \sum_{\ell\le x}\log\left(1+\frac{1}{\ell}+\frac{2}{\ell^2}\right) \\ &= \sum_{\ell\le x}\frac{1}{\ell} + c + O\left(\frac{1}{x}\right) \\ &= \log\log x + c' + O\left(\frac{1}{\log x}\right),\end{aligned}$$

where c and c' are constants and where the last equality comes from [3, Thm. 4.12, p. 90]. Exponentiating, we find that $\sum_{d\le x} D(d)/d \ll \log x$ for $x \ge 2$, as desired. □

Proof of Lemma 6.3. First we compute a bound on the sum of the relative conductors of the elliptic curves in a fixed ordinary isogeny class. Let a be an integer, coprime to q, with $a^2 < 4q$. Recall from Section 4 that we write $\Delta_{a,q} := a^2 - 4q = \mathfrak{f}_{a,q}^2\,\Delta_{a,q}^*$, where $\Delta_{a,q}^*$ is a fundamental discriminant. Let $\widetilde{\mathcal{O}}_{a,q}$ be the quadratic order of discriminant $\Delta_{a,q}^*$. As we noted in Section 4, the isogeny class

$\mathcal{I}(\mathbb{F}_q, a)$ is the union of strata $\mathcal{S} = \mathcal{I}(\mathbb{F}_q, a, \mathcal{O})$, where the orders $\mathcal{O} \subseteq \widetilde{\mathcal{O}}_{a,q}$ have discriminant $f^2\Delta^*_{a,q}$ for the divisors f of $\mathfrak{f}_{a,q}$. The curves in $\mathcal{S}$ have relative conductor $\mathfrak{f}_{a,q}/f$, and the number of curves in $\mathcal{S}$ is equal to $h(\mathcal{O})$. If we let χ denote the quadratic character modulo $\Delta^*_{a,q}$, then

$$h(\mathcal{O}) = fh(\Delta^*_{a,q}) \prod_{\ell \mid f} \left(1 - \frac{\chi(\ell)}{\ell}\right).$$

Thus,

$$\sum_{E \in \mathcal{I}(\mathbb{F}_q, a)} \mathfrak{f}_{\mathrm{rel}}(E) = \sum_{f \mid \mathfrak{f}_{a,q}} \frac{\mathfrak{f}_{a,q}}{f} fh(\Delta^*_{a,q}) \prod_{\ell \mid f} \left(1 - \frac{\chi(\ell)}{\ell}\right) = \mathfrak{f}_{a,q}\, h(\Delta^*_{a,q}) \sum_{f \mid \mathfrak{f}_{a,q}} \prod_{\ell \mid f} \left(1 - \frac{\chi(\ell)}{\ell}\right).$$

Lemma 4.4 tells us that $h(\Delta) \ll |\Delta|^{1/2} \log |\Delta|$ for all fundamental discriminants $\Delta < 0$. Combining this with the fact that $|f^2_{a,q}\Delta^*_{a,q}| = 4q - a^2 < 4q$ we see that there is a constant c such that for all q and a, we have

$$\sum_{E \in \mathcal{I}(\mathbb{F}_q, a)} \mathfrak{f}_{\mathrm{rel}}(E) < cq^{1/2} (\log q) A(\mathfrak{f}_{a,q}),$$

where A is the arithmetic function defined by

$$A(n) = \sum_{d \mid n} \prod_{\ell \mid d} \left(1 + \frac{1}{\ell}\right) = \sum_{d \mid n} \frac{\psi(d)}{d}.$$

Additionally, if the generalized Riemann hypothesis is true we can use Lemma 4.4 to find that there is a constant c' such that for all q and a we have

$$\sum_{E \in \mathcal{I}(\mathbb{F}_q, a)} \mathfrak{f}_{\mathrm{rel}}(E) < c' q^{1/2} |\log \log q| A(\mathfrak{f}_{a,q}).$$

Thus, to prove the lemma it will suffice to show that we have

$$\sum_{\substack{1 \le a \le 2\sqrt{q} \\ \gcd(a,q)=1}} A(\mathfrak{f}_{a,q}) \ll q^{1/2} \log q \qquad \text{for all } q. \tag{5}$$

Note that the sum on the left side of (5) is equal to

$$\sum_{\substack{1 \le a \le 2\sqrt{q} \\ \gcd(a,q)=1}} \sum_{d \mid \mathfrak{f}_{a,q}} \frac{\psi(d)}{d} = \sum_{1 \le d \le 2\sqrt{q}} \frac{\psi(d)}{d} \#\{a \colon 1 \le a \le 2\sqrt{q} \text{ and } \gcd(a,q) = 1 \text{ and } d \mid \mathfrak{f}_{a,q}\}.$$

If $d \mid \mathfrak{f}_{a,q}$ then $a^2 \equiv 4q \bmod d^2$, so let us first consider, for a fixed d, estimates for the number of a in the interval $[1, 2\sqrt{q}]$ with $a^2 \equiv 4q \bmod d^2$.

We have

$$\begin{aligned} \#\{a \colon 1 \le a \le 2\sqrt{q} \text{ and } a^2 \equiv 4q \bmod d^2\} &\le \#\{a \colon 1 \le a \le d^2 \lceil 2\sqrt{q}/d^2 \rceil \text{ and } a^2 \equiv 4q \bmod d^2\} \\ &= \lceil 2\sqrt{q}/d^2 \rceil \#\{a \colon 1 \le a \le d^2 \text{ and } a^2 \equiv 4q \bmod d^2\}. \end{aligned}$$

Thus, if we let B_q denote the multiplicative arithmetic function given by

$$B_q(n) = \#\{a \colon 1 \le a \le n^2 \text{ and } a^2 \equiv 4q \bmod n^2\}$$

then we have

$$\begin{aligned}\sum_{\substack{1\le a\le 2\sqrt{q}\\ \gcd(a,q)=1}} A(\mathfrak{f}_{a,q}) &\le \sum_{\substack{d\le 2\sqrt{q}\\ \gcd(d,q)=1}} \frac{\psi(d)}{d}\#\{a\colon 1\le a\le 2\sqrt{q} \text{ and } \gcd(a,q)=1 \text{ and } d\mid \mathfrak{f}_{a,q}\}\\ &\le \sum_{\substack{d\le 2\sqrt{q}\\ \gcd(d,q)=1}} \frac{\psi(d)}{d}\lceil 2\sqrt{q}/d^2\rceil B_q(d)\\ &\le \sum_{\substack{d\le 2\sqrt{q}\\ \gcd(d,q)=1}} \frac{2\sqrt{q}}{d^2}\frac{\psi(d)}{d}B_q(d) + \sum_{\substack{d\le 2\sqrt{q}\\ \gcd(d,q)=1}} \frac{\psi(d)}{d}B_q(d). \qquad (6)\end{aligned}$$

If ℓ is a prime that does not divide q and if $e>0$ then

$$B_q(\ell^e)\le\begin{cases}2 & \text{if } \ell\ne 2\\ 8 & \text{if } \ell=2,\end{cases}$$

so

$$\frac{\psi(d)}{d}B_q(d)\le 4C(d)$$

for all d coprime to q, where C is the function from Lemma 6.5. For every $\epsilon>0$ we have $C(d)\ll d^\epsilon$ for all d, so

$$\sum_{\substack{d\le 2\sqrt{q}\\ \gcd(d,q)=1}} \frac{1}{d^2}\frac{\psi(d)}{d}B_q(d)\le 4\sum_{\substack{d\le 2\sqrt{q}\\ \gcd(d,q)=1}}\frac{C(d)}{d^2}\le 4\sum_{d=1}^{\infty}\frac{C(d)}{d^2}<\infty \qquad \text{for all } q. \qquad (7)$$

This shows that the first term on the right side of (6) is $\ll\sqrt{q}$ for all q. To bound the second term on the right side of (6), we compute that

$$\sum_{\substack{d\le 2\sqrt{q}\\ \gcd(d,q)=1}} \frac{\psi(d)}{d}B_q(d)\le 4\sum_{d\le 2\sqrt{q}} C(d)\ll q^{1/2}\log q \qquad \text{for all } q, \qquad (8)$$

by Lemma 6.5. Combining (6) with (7) and (8) proves (5), and completes the proof of the lemma. □

7. Ordinary split isotypic surfaces

In this section we will prove Proposition 3.2. As in the preceding section, we state several lemmas which lead to a quick proof of the proposition. Lemma 7.1 follows from Lemma 6.4. We postpone the proofs of Lemmas 7.2, 7.3, and 7.4 until the end of the section.

Lemma 7.1. *For every ordinary $E/\mathbb{F}_q$ and positive integer n we have*

$$\sum_{E'\sim E}\#\operatorname{Isom}^{-1}(E,E',n)\le 2\psi(n)\,\mathfrak{f}_{\mathrm{rel}}(E)\sum_{E'\sim E}\mathfrak{f}_{\mathrm{rel}}(E'). \qquad \square$$

Lemma 7.2. *Let $E/\mathbb{F}_q$ be an elliptic curve and let $C/\mathbb{F}_q$ be a smooth genus-2 curve with $\operatorname{Jac} C\sim E^2$. Then there is a finite morphism $C\to E$ of degree at most $\sqrt{2q}$. If E is supersingular with all endomorphisms defined over $\mathbb{F}_q$, then there is a finite morphism $C\to E$ of degree at most $q^{1/4}$.*

Lemma 7.3. *We have*

$$\sum_{n\le x}\psi(n)=\frac{15}{2\pi^2}x^2+O(x\log x).$$

For every pair of isogenous curves E and E' over $\mathbb{F}_q$, we let $s(E, E')$ denote the degree of the smallest isogeny from E to E'.

Lemma 7.4. *Let $E/\mathbb{F}_q$ be an ordinary elliptic curve with $\mathfrak{f}_{\mathrm{rel}}(E) = 1$, and let $\mathcal{S}$ be a stratum of curves isogenous to E. Then*

$$\sum_{E' \in \mathcal{S}} \frac{1}{s(E,E')^2} < \frac{\zeta(3)}{\mathfrak{f}_{\mathrm{rel}}(\mathcal{S})^2},$$

where ζ is the Riemann zeta function.

Proof of Proposition 3.2. Proposition 3.2 gives an upper bound on the number of principally-polarized abelian surfaces isogenous to the square of an ordinary elliptic curve. We would like to instead consider Jacobians. This requires that we first dispose of those principally-polarized surfaces that are not Jacobians of smooth curves; according to [12, Thm. 3.1, p. 270], these are the polarized surfaces that are products of elliptic curves with the product polarization, together with the restrictions of scalars of polarized elliptic curves over the quadratic extension of our base field. But the restriction of scalars of an elliptic curve over $\mathbb{F}_{q^2}$ with trace of Frobenius b is an abelian surface over $\mathbb{F}_q$ with Weil polynomial $x^4 - bx^2 + q^2$, and such a surface is never isogenous to the square of an ordinary elliptic curve, because in that case its Weil polynomial would have to be $(x^2 - ax + q)^2$ where a is coprime to q. Therefore, to dispose of the non-Jacobians, we need only consider products of elliptic curves, with the product polarization.

The number of elliptic curves in an ordinary isogeny class with trace of Frobenius equal to a is equal to the Kronecker class number $H(a^2 - 4q)$ of the discriminant $a^2 - 4q$ (see [40, Thm. 4.6, pp. 194–195]). From Lemma 4.4 we know that $H(\Delta) \ll |\Delta|^{1/2} \log|\Delta| (\log\log|\Delta|)^2$ for all negative discriminants Δ. Therefore the number of product surfaces $E \times E'$ with E and E' both in a fixed ordinary isogeny class over $\mathbb{F}_q$ is $\ll q(\log q)^2(\log\log q)^4$; summing over isogeny classes, we find that the number of product surfaces $E \times E'$ with E and E' ordinary and isogenous to one another is $\ll q^{3/2}(\log q)^2(\log\log q)^4$. Thus, the contribution of the non-Jacobians to the ordinary split isotypic polarized surfaces is much less than the bound claimed in Proposition 3.2. (Of course, for present purposes, it suffices to observe that the number of non-Jacobians is bounded by the square of the number of elliptic curves over $\mathbb{F}_q$; but the estimate provided here is closer to the actual truth.)

Fix an integer a with $|a| \le 2\sqrt{q}$ and $\gcd(a, q) = 1$, and let E_a be an elliptic curve over $\mathbb{F}_q$ with $a(E) = a$ and with $\operatorname{End} E_a \cong \mathcal{O}_{a,q}$, so that $\mathfrak{f}_{\mathrm{rel}}(E_a) = 1$. Suppose C is a curve over $\mathbb{F}_q$ whose Jacobian is isogenous to E_a^2. By Lemma 7.2 there is a morphism ϕ from $C \to E_a$ of degree at most $\sqrt{2q}$. We can write this map as a composition of a minimal map $C \to E$ (see Section 5) with an isogeny $E \to E_a$, and it follows that the degree of the minimal map $C \to E$ is at most $\sqrt{2q}/s(E, E_a)$. If we let N_a denote the number of genus-2 curves with Jacobians isogenous to E_a^2, we find that

$$\begin{aligned}
N_a &\le \sum_{E \sim E_a} \#\{C \text{ with minimal maps to } E \text{ of degree at most } \sqrt{2q}/s(E,E_a)\} \\
&\le \sum_{E \sim E_a} \sum_{n \le \sqrt{2q}/s(E,E_a)} \sum_{E' \sim E} \#\operatorname{Isom}^{-1}(E, E', n) \\
&\le \sum_{E \sim E_a} \sum_{n \le \sqrt{2q}/s(E,E_a)} 2\psi(n)\, \mathfrak{f}_{\mathrm{rel}}(E) \sum_{E' \sim E} \mathfrak{f}_{\mathrm{rel}}(E') \qquad (9) \\
&= 2\Bigg(\sum_{E' \sim E_a} \mathfrak{f}_{\mathrm{rel}}(E') \Bigg) \sum_{E \sim E_a} \mathfrak{f}_{\mathrm{rel}}(E) \sum_{n \le \sqrt{2q}/s(E,E_a)} \psi(n) \\
&\ll \Bigg(\sum_{E' \sim E_a} \mathfrak{f}_{\mathrm{rel}}(E') \Bigg) \sum_{E \sim E_a} \mathfrak{f}_{\mathrm{rel}}(E) \frac{2q}{s(E,E_a)^2} \qquad \text{for all } a \text{ and } q. \qquad (10)
\end{aligned}$$

Here (9) follows from Lemma 7.1 and (10) follows from Lemma 7.3. Now we group the curves E isogenous to E_a by their strata. Recall that we have $a^2 - 4q = \mathfrak{f}_{a,q}^2 \, \Delta_{a,q}^*$, and that the strata of curves isogenous to E_a are indexed by the divisors f of $\mathfrak{f}_{a,q}$. We find that

$$N_a \ll q \Bigg(\sum_{E' \sim E_a} \mathfrak{f}_{\mathrm{rel}}(E') \Bigg) \sum_{\mathcal{S} \sim E_a} \mathfrak{f}_{\mathrm{rel}}(\mathcal{S}) \sum_{E \in \mathcal{S}} \frac{1}{s(E, E_a)^2} \qquad \text{for all } a \text{ and } q$$

$$\ll q \Bigg(\sum_{E' \sim E_a} \mathfrak{f}_{\mathrm{rel}}(E') \Bigg) \sum_{f \mid \mathfrak{f}_{a,q}} \frac{1}{f} \qquad \text{for all } a \text{ and } q \tag{11}$$

$$\ll q \Bigg(\sum_{E' \sim E_a} \mathfrak{f}_{\mathrm{rel}}(E') \Bigg) |\log \log q|, \qquad \text{for all } a \text{ and } q, \tag{12}$$

where (11) follows from Lemma 7.4 and (12) follows from the asymptotic upper bound [13, Thm. 323, p. 266]

$$e^\gamma = \limsup_{n>0} \frac{\sum_{d \mid n} d}{n \log \log n} = \limsup_{n>0} \frac{\sum_{d \mid n} d/n}{\log \log n} = \limsup_{n>0} \frac{\sum_{d \mid n} 1/d}{\log \log n}.$$

Recall that X_q is the number of principally-polarized ordinary split isotypic abelian surfaces over $\mathbb{F}_q$. Then X_q is the sum over all a coprime to q of the N_a (together with the negligible contribution from those abelian surfaces that are isomorphic, as principally-polarized abelian varieties, to products of isogenous elliptic curves), and we find that

$$X_q \ll q |\log \log q| \Bigg(\sum_{\text{ordinary } E/\mathbb{F}_q} \mathfrak{f}_{\mathrm{rel}}(E) \Bigg) \qquad \text{for all } q.$$

Proposition 3.2 then follows from Lemma 6.3. □

Proof of Lemma 7.2. Choose a divisor of degree 1 on C, and let L be the additive group of morphisms from C to E that send the given divisor to the identity of E. Let $\mathbf{E}$ be the base extension of E from $\mathbb{F}_q$ to the function field F of C. The *Mordell–Weil lattice* of $\mathbf{E}$ over F is the group $\mathbf{E}(F)/E(\mathbb{F}_q)$ provided with the pairing coming from the canonical height. The natural map $L \to \mathbf{E}(F)/E(\mathbb{F}_q)$ is a bijection, and the quadratic form on L obtained from the height pairing on $\mathbf{E}(F)$ is twice the degree map (see [42, Thm. III.4.3, pp. 217–218]). Let $a = a(E)$, and let π and $\overline{\pi}$ be the roots in $\mathbb{C}$ of the characteristic polynomial of Frobenius for E, so that $\pi + \overline{\pi} = a$. The Birch and Swinnerton-Dyer conjecture for constant elliptic curves over function fields (proved by Milne [34, Thm. 3, pp. 100–101]) shows that the determinant of the Mordell–Weil lattice is a divisor of

$$\begin{cases} (\pi - \overline{\pi})^4 = (a^2 - 4q)^2 & \text{if } \pi \neq \overline{\pi}, \\ q^2 & \text{if } \pi = \overline{\pi}; \end{cases}$$

note that $\pi = \overline{\pi}$ if and only if E is supersingular with all of its endomorphisms rational over $\mathbb{F}_q$.

The $\mathbb{Z}$-rank of L is twice the $\mathbb{Z}$-rank of $\operatorname{End} E$. If $\pi \neq \overline{\pi}$, so that $\operatorname{End} E$ is an imaginary quadratic order, then L is a $\mathbb{Z}$-module of rank 4. Applying [8, Thm. 12.2.1, p. 260] we find that there is a nonzero element of L of degree at most

$$\frac{1}{2} \gamma_4 |a^2 - 4q|^{1/2},$$

where γ_4 is the Hermite constant for dimension 4. Using the fact that $\gamma_4 = \sqrt{2}$ (see [19]), we obtain the bound in the lemma.

If $\pi = \overline{\pi}$ then $\operatorname{End} E$ is an order in a quaternion algebra and L is a $\mathbb{Z}$-module of rank 8. We find that there is a nonzero element of L with degree at most

$$\frac{1}{2} \gamma_8 q^{1/4}.$$

The value of γ_8 was determined by Blichfeldt [6] to be 2, so there is a map from C to E of degree at most $q^{1/4}$. □

Proof of Lemma 7.3. First we note that

$$\psi(n) = \sum_{d|n} |\mu(d)| \frac{n}{d},$$

where μ is the Möbius function. Then, arguing as in the proof of [3, Thm. 3.7, p. 62], we see that

$$\begin{aligned}
\sum_{n\le x} \psi(n) &= \sum_{\substack{d,q \\ dq\le x}} |\mu(d)| q = \sum_{d\le x} |\mu(d)| \sum_{q\le x/d} q \\
&= \sum_{d\le x} |\mu(d)| \left(\frac{1}{2} \left(\frac{x}{d}\right)^2 + O\left(\frac{x}{d}\right)\right) \\
&= \frac{1}{2} x^2 \sum_{d\le x} \frac{|\mu(d)|}{d^2} + O\left(x \sum_{d\le x} \frac{1}{d}\right) \\
&= \frac{1}{2} c x^2 + O(x \log x),
\end{aligned}$$

where

$$c = \sum_{d=1}^{\infty} \frac{|\mu(d)|}{d^2} = \prod_{\ell} \left(1 + \frac{1}{\ell^2}\right) = \prod_{\ell} \frac{(1-1/\ell^4)}{(1-1/\ell^2)} = \frac{\zeta(2)}{\zeta(4)} = \frac{15}{\pi^2}.$$ □

Proof of Lemma 7.4. Let $\mathcal{O} = \mathcal{O}_{\mathcal{S}}$ be the order corresponding to the stratum $\mathcal{S}$. We claim that there is an elliptic curve $\widetilde{E}$ in $\mathcal{S}$ and an isogeny $f\colon E \to \widetilde{E}$ with the property that every isogeny from E to an elliptic curve in $\mathcal{S}$ factors through f. One way to see this is via the theory of Deligne modules [10, 20]. If we let π be the Frobenius for E and let K be the quadratic field $\mathbb{Q}(\pi)$, then the Deligne modules of the elements of $\mathcal{S}$ can be viewed as lattices in K with endomorphism rings equal to $\mathcal{O}$, while the Deligne module for E can be viewed as a lattice $\Lambda \subset K$ with $\operatorname{End}\Lambda = \mathbb{Z}[\pi]$. The curve $\widetilde{E}$ is the elliptic curve corresponding to the Deligne module $\Lambda \otimes \mathcal{O}$, and the isogeny f corresponds to the inclusion $\Lambda \subset \Lambda \otimes \mathcal{O}$. In particular, we see that the degree of f is equal to $\mathfrak{f}_{\mathrm{rel}}(\mathcal{S})$.

The isogenies from $\widetilde{E}$ to the other elements of $\mathcal{S}$ correspond to the invertible ideals $\mathfrak{a} \subset \mathcal{O}$, with different ideals giving rise to different isogenies. Let $\mathfrak{a}_1, \dots, \mathfrak{a}_n$ be the (distinct) ideals corresponding to the smallest isogenies from $\widetilde{E}$ to the elements of $\mathcal{S}$, where $n = \#\mathcal{S}$. Then

$$\sum_{E'\in\mathcal{S}} \frac{1}{s(E,E')^2} = \sum_{i=1}^{n} \frac{1}{\mathfrak{f}_{\mathrm{rel}}(\mathcal{S})^2 \mathcal{N}(\mathfrak{a}_i)^2} < \frac{1}{\mathfrak{f}_{\mathrm{rel}}(\mathcal{S})^2} \sum_{\text{all } \mathfrak{a}} \frac{1}{\mathcal{N}(\mathfrak{a})^2},$$

where the final sum is over all invertible ideals $\mathfrak{a} \subseteq \mathcal{O}$; that is, the final sum is equal to $\zeta_{\mathcal{O}}(2)$, where $\zeta_{\mathcal{O}}$ is the zeta function for the order $\mathcal{O}$.

Kaneko [26, Proposition, p. 202] gives an explicit formula for $\zeta_{\mathcal{O}}(s)$ in terms of the zeta function for K and the conductor of $\mathcal{O}$. It is not hard to check that for real $s > 1$, the Euler factor at ℓ for $\zeta_{\mathcal{O}}(s)$ is bounded above by $1/(1-\ell^{1-2s})$, so that $\zeta_{\mathcal{O}}(s) < \zeta(2s-1)$, where ζ is the Riemann zeta function. In particular, $\zeta_{\mathcal{O}}(2) < \zeta(3)$, and the lemma follows. □

8. Almost ordinary split surfaces

In this section we prove Proposition 3.3, which gives an upper bound on the number of principally-polarized almost ordinary split abelian surfaces. We base the proof on two lemmas, which we prove at the end of the section.

Lemma 8.1. *Let E_0 be a supersingular elliptic curve over a finite field $\mathbb{F}_q$, with q a square, and suppose the Frobenius endomorphism on E_0 is equal to multiplication by s, where $s^2 = q$. Let $\mathcal{S}$ be a stratum of ordinary elliptic curves over $\mathbb{F}_q$, and suppose n is a positive integer such that $\mathrm{Isom}^{-1}(E_0, \mathcal{S}, n)$ is nonempty. Then*

(a) *the integer n is coprime to q,*
(b) *the relative conductor $\mathfrak{f}_{\mathrm{rel}}(\mathcal{S})$ is divisible by n, and*
(c) *the trace $a(\mathcal{S})$ satisfies $4a(\mathcal{S}) \equiv 8s \bmod n^2$.*

Lemma 8.2. *We have*

$$\sum_{n \le x} \frac{\psi(n)}{n} = \frac{15}{\pi^2} x + O(\log x).$$

Proof of Proposition 3.3. In analogy with Section 6, we will bound the number Y_q of principally-polarized almost ordinary split abelian surfaces over $\mathbb{F}_q$ by estimating the number of surfaces obtained by gluing a supersingular E_0 to an ordinary E along their n-torsion subgroups. The methods we use will depend on whether or not E_0 has all of its endomorphisms defined over $\mathbb{F}_q$. Let $Y_{q,1}$ denote the number of principally-polarized surfaces we get from E_0 with all of the endomorphisms defined, and let $Y_{q,2}$ denote the number we get from E_0 with not all endomorphisms defined. We will show that $Y_{q,1}$ and $Y_{q,2}$ each satisfy the bound of Proposition 3.3.

First let us bound $Y_{q,1}$; that is, we consider the case where all of the endomorphisms of E_0 are defined over $\mathbb{F}_q$. In this case, q is a square and the characteristic polynomial of E_0 is $(T - 2s)^2$, where $s^2 = q$; furthermore, [40, Thm. 4.6, pp. 194–195] tells us that there are

$$\frac{1}{12}\left(p + 6 - 4\left(\frac{-3}{p}\right) - 3\left(\frac{-4}{p}\right)\right) \le \frac{\sqrt{q}}{2}$$

such curves for each of the two possible values of s, so at most $\sqrt{q}$ curves in total.

Fix such an E_0 and fix an integer $n > 0$. Suppose $\mathcal{S}$ is an ordinary stratum of elliptic curves over $\mathbb{F}_q$ such that $\mathrm{Isom}^{-1}(E_0, \mathcal{S}, n)$ is nonempty. If n is even let $m = n/2$; otherwise let $m = n$. We see from Lemma 8.1 that the trace $a(\mathcal{S})$ of $\mathcal{S}$ is an integer congruent to $2s$ modulo m^2, but not equal to $2s$. The number of such integers a in the Weil interval is at most $\lfloor 4\sqrt{q}/m^2 \rfloor$.

Given such an integer a, write $a^2 - 4q = \mathfrak{f}_{a,q}^2 \, \Delta_{a,q}^*$ for a fundamental discriminant $\Delta_{a,q}^*$. Let χ be the quadratic character modulo $\Delta_{a,q}^*$, and for each divisor d of $\mathfrak{f}_{a,q}/n$ let $\mathcal{S}_d$ be the stratum $\mathcal{S}$ with $a(\mathcal{S}) = a$ and $\mathfrak{f}(\mathcal{S}) = d$. Using Lemma 6.4 we find that

$$\begin{aligned}
\sum_{E \in \mathcal{I}(\mathbb{F}_q, a)} \#\mathrm{Isom}^{-1}(E_0[n], E[n]) &= \sum_{\substack{\mathcal{S} \text{ with} \\ a(\mathcal{S}) = a \text{ and } n \mid \mathfrak{f}_{\mathrm{rel}}(\mathcal{S})}} \#\mathrm{Isom}^{-1}(E_0, \mathcal{S}, n) \\
&= \sum_{d \mid (\mathfrak{f}_{a,q}/n)} \#\mathrm{Isom}^{-1}(E_0, \mathcal{S}_d, n) \\
&\le 2 \sum_{d \mid (\mathfrak{f}_{a,q}/n)} \psi(n) h(\mathcal{O}_{\mathcal{S}_d}) n^2 \\
&= 2\psi(n) n^2 H\left(\frac{a^2 - 4q}{n^2}\right),
\end{aligned}$$

where $H(x)$ is the Kronecker class number. Thus,

$$\sum_{E \in \mathcal{I}(\mathbb{F}_q, a)} \#\mathrm{Isom}^{-1}(E_0[n], E[n]) \ll \begin{cases} 2\psi(n) n q^{1/2} (\log q)(\log\log q)^2 & \text{for all } a \text{ and } q, \text{ unconditionally,} \\ 2\psi(n) n q^{1/2} |\log\log q|^3 & \text{for all } a \text{ and } q, \text{ under GRH.} \end{cases}$$

Summing over the $\lfloor 4\sqrt{q}/m^2 \rfloor$ possible values of a for a given n, and then summing over the possible $n < 4\sqrt{q}$, and then summing over the possible curves E_0, we find that

$$Y_{q,1} \ll q^{3/2}(\log q)(\log\log q)^2 \sum_{n=1}^{4\sqrt{q}} \frac{\psi(n)}{n} \ll q^2(\log q)(\log\log q)^2 \qquad \text{for all } q.$$

If the generalized Riemann hypothesis holds, we get the better bound

$$Y_{q,1} \ll q^2 |\log\log q|^3 \qquad \text{for all } q.$$

Now we turn to estimating $Y_{q,2}$, the number of principally-polarized split surfaces isogenous to a surface of the form $E_0 \times E$, where E is ordinary and E_0 is supersingular with not all endomorphisms defined. Using [40, Thms. 4.2, 4.3, and 4.5, pp. 194–195], we find that the possible strata of such curves E_0 are as listed in Table 1.

Conditions on q	Conditions on p	$a(\mathcal{S})$	$\Delta(\mathcal{O}_\mathcal{S})$	$\mathfrak{f}_{\mathrm{rel}}(\mathcal{S})$	$\#\mathcal{S}$
q nonsquare	—	0	$-4p$	$\sqrt{q/p}$	$h(-4p)$
	$p \equiv 3 \bmod 4$	0	$-p$	$2\sqrt{q/p}$	$h(-p)$
	$p = 2$	$\pm\sqrt{2q}$	-4	$\sqrt{q/2}$	1
	$p = 3$	$\pm\sqrt{3q}$	-3	$\sqrt{q/3}$	1
q square	—	0	-4	$\sqrt{q}$	$1 - \left(\frac{-4}{p}\right)$
	—	$\pm\sqrt{q}$	-3	$\sqrt{q}$	$1 - \left(\frac{-3}{p}\right)$

TABLE 1. The supersingular strata $\mathcal{S}$ over $\mathbb{F}_q$ with not all endomorphisms defined over $\mathbb{F}_q$. Here q is a power of a prime p.

Let E_0 be a supersingular curve with not all endomorphisms defined. If we are to glue E_0 to an ordinary elliptic curve E along the n-torsion of the two curves, then n must be coprime to q. In that case, the greatest common divisor of $\mathfrak{f}_{\mathrm{rel}}(E_0)$ and n is either 1 or 2, as we see from Table 1. It follows from Lemma 6.4 that for every ordinary stratum $\mathcal{S}$, we have

$$\#\mathrm{Isom}^{-1}(E_0, \mathcal{S}, n) \le 8\psi(n)h(\mathcal{O}_\mathcal{S}),$$

so the total number of curves obtained from gluing E_0 to an ordinary elliptic curve is bounded by

$$8 \sum_{\text{ordinary } \mathcal{S}} h(\mathcal{O}_\mathcal{S}) \sum_{n \mid (a(\mathcal{S}) - a(E_0))} \psi(n) \ll q^{1/2}(\log\log q)^2 \sum_{\text{ordinary } \mathcal{S}} h(\mathcal{O}_\mathcal{S}) \qquad \text{for all } q$$

by Lemma 6.2. This last sum is simply the number of ordinary elliptic curves over $\mathbb{F}_q$, which (one shows) is at most $2q + 4$, so the number of curves obtained as above from a fixed E_0 is $\ll q^{3/2}(\log\log q)^2$ for all q.

If q is a square there are at most 6 possible E_0, and we find that

$$Y_{q,2} \ll q^{3/2}(\log\log q)^2 \qquad \text{for all square } q.$$

If q is not a square, then Lemma 4.4 shows that the number of possible E_0 is $\ll q^{1/2}\log q$ for all q unconditionally, and $\ll q^{1/2}|\log\log q|$ for all q under the generalized Riemann hypothesis. This leads to

$$Y_{q,2} \ll \begin{cases} q^2(\log q)(\log\log q)^2 & \text{for all } q \text{ unconditionally,} \\ q^2|\log\log q|^3 & \text{for all } q \text{ under GRH,} \end{cases}$$

and completes the proof of Proposition 3.3. □

Proof of Lemma 8.1. Since $\mathrm{Isom}^{-1}(E_0, \mathcal{S}, n)$ is nonempty, there is an $E \in \mathcal{S}$ with $E_0[n] \cong E[n]$. The p-torsion of E_0 is a local-local group scheme, while $E[p]$ has no local-local part, so n must not be divisible by p. This proves (a).

Lemma 6.4 shows that $\gcd(n, \mathfrak{f}_{\mathrm{rel}}(E_0)) = \gcd(n, \mathfrak{f}_{\mathrm{rel}}(\mathcal{S}))$. Since $\mathfrak{f}_{\mathrm{rel}}(E_0) = 0$, we find that $n \mid \mathfrak{f}_{\mathrm{rel}}(\mathcal{S})$. This proves (b).

Let $a = a(\mathcal{S})$. From (b) we know that $a^2 - 4q \equiv 0 \bmod n^2$, and we also know that $a \equiv a(E_0) = 2s \bmod n$. Since $a - 2s \equiv 0 \bmod n$ we have

$$0 \equiv a^2 - 4as + 4s^2 \equiv 4s^2 - 4as + 4s^2 \equiv 8s^2 - 4as \bmod n^2.$$

Since s is coprime to n by (a), we can divide through by s to obtain (c). □

Proof of Lemma 8.2. The proof is quite similar to that of Lemma 7.3. We have

$$\sum_{n \le x} \frac{\psi(n)}{n} = \sum_{\substack{d,q \\ dq \le x}} \frac{|\mu(d)|}{d} = \sum_{d \le x} \frac{|\mu(d)|}{d} \left\lfloor \frac{x}{d} \right\rfloor = x \sum_{d \le x} \frac{|\mu(d)|}{d^2} + O(\log x) = cx + O(\log x)$$

where $c = \sum_{d=1}^{\infty} |\mu(d)|/d^2 = 15/\pi^2$. □

9. Supersingular split surfaces

In this section we prove Proposition 3.4, which gives a bound on the number Z_q of principally-polarized supersingular split abelian surfaces over $\mathbb{F}_q$.

We must first introduce some terminology and some background results. Let A be an abelian surface over a finite field $\mathbb{F}_q$ of characteristic p, and let $\boldsymbol{\alpha}_p$ denote the (unique) local-local group scheme of rank p over $\mathbb{F}_q$. The *a-number* of A is the dimension of the $\mathbb{F}_q$-vector space $\mathrm{Hom}(\boldsymbol{\alpha}_p, A)$. If A has a-number 2 then A is called *superspecial*; all superspecial surfaces over $\mathbb{F}_q$ are geometrically isomorphic to one another, and they are all geometrically isomorphic to the square of a supersingular elliptic curve. A supersingular surface A has a-number equal to either 1 or 2; if the a-number is 1, then A has a unique local-local subgroup scheme of rank p, and the quotient of A by this subgroup scheme is a superspecial surface.

Let $\mathcal{A}_2^{\mathrm{ss}}$ denote the supersingular locus of the coarse moduli space of principally-polarized abelian surfaces. Koblitz [29, p. 193] shows that the only singularities of $\mathcal{A}_2^{\mathrm{ss}}$ are at the superspecial points, and from [39, Proof of Cor. 4.7, p. 117] we know that each irreducible component of $\mathcal{A}_{2,\overline{\mathbb{F}}_p}^{\mathrm{ss}}$ is a curve of genus 0. Also, every component contains a superspecial point. Therefore, the non-superspecial locus of $\mathcal{A}_{2,\overline{\mathbb{F}}_p}^{\mathrm{ss}}$ is a disjoint union of components, each of which is isomorphic to an open affine subset of $\mathbf{A}^1$.

Moreover, the number of irreducible components of $\mathcal{A}_{2,\overline{\mathbb{F}}_p}^{\mathrm{ss}}$ is equal to the class number $H_2(1, p)$ of the non-principal genus of $\mathbb{Q}_{p,\infty}^2$ (see [27, Thm. 5.7, p. 133]). Hashimoto and Ibukiyama [15] (see also [24, Rmk. 2.17, p. 147]) provide a formula for $H_2(1, p)$ which shows both that $H_2(1, p) = p^2/2880 + O(p)$ and that $H_2(1, p) \le p^2/4$ for all p.

For convenience, we also state the following lemma.

Lemma 9.1. *Let (A, λ) be a principally-polarized abelian surface over $\overline{\mathbb{F}}_q$ that has a model over $\mathbb{F}_q$. Then the number of distinct $\mathbb{F}_q$-rational models of (A, λ) is at most* 1152.

Proof. The size of the automorphism group of a principally-polarized abelian surface over a finite field is bounded by 1152 (by 72, if the characteristic is greater than 5); for Jacobians, this follows from Igusa's enumeration of the possible automorphism groups [25, §8], and for products of polarized elliptic curves and for restrictions of scalars of elliptic curves it is an easy exercise. (We

know from [12, Thm. 3.1, p. 270] that every principally-polarized abelian surface is of one of these three types.) By [7, Lemma 7.2, pp. 85–86], the number of $\mathbb{F}_q$-rational forms of such a polarized surface is bounded by this same number. □

With these preliminaries out of the way, we may proceed to the proof of Proposition 3.4. The proof splits into cases, depending on whether or not the base field is a prime field. First we consider the case where q ranges over the set of primes p.

We may assume that $p > 3$. In that case, we see from Table 1 that there is only one isogeny class of supersingular elliptic curves, the isogeny class $\mathcal{I}(\mathbb{F}_p, 0)$ of trace-0 curves, which consists of 1 or 2 strata.

Pick a trace-0 elliptic curve $E_0/\mathbb{F}_p$ whose endomorphism ring has discriminant $-4p$. If (A, λ) is a principally-polarized abelian surface over $\mathbb{F}_p$ with A isogenous to E_0^2, then either A is a product of elliptic curves with the product polarization, or A is the restriction of scalars of an elliptic curve over $\mathbb{F}_{p^2}$ with trace $-2p$, or A is the Jacobian of a curve C. (See [12, Thm. 3.1, p. 270].) The number of elliptic curves in $\mathcal{I}(\mathbb{F}_p, 0)$ is $H(-4p)$; using Lemma 4.4 we see that the number of products of such elliptic curves is $\ll p(\log p)^2(\log\log p)^4 \ll p^2$ for all primes p. The number of supersingular elliptic curves over $\mathbb{F}_{p^2}$ with trace $-2p$ is equal to the number of supersingular j-invariants, which is is $p/12 + O(1)$; therefore the number of restrictions of scalars of such curves is $\ll p$. Thus, we may focus our attention on the case where (A, λ) is the Jacobian of a curve C.

In this case, we know from Lemma 7.2 that C has a map of degree at most $\sqrt{2p} < p$ to E_0, so C has a *minimal* map of degree at most p to a curve E in $\mathcal{I}(\mathbb{F}_p, 0)$. We see that the polarized variety (A, λ) can be obtained by gluing together two elliptic curves E and E' in $\mathcal{I}(\mathbb{F}_p, 0)$ along their n-torsion, for some $n < p$. It follows that the a-number of A is 2, so A is superspecial. By [23, Rem. 3, p. 41], the number of principally-polarized superspecial abelian surfaces over $\overline{\mathbb{F}}_p$ which admit a model over $\mathbb{F}_p$ is $\ll ph(-p)$, which in turn is $\ll p^{3/2}(\log p)|\log\log p|$ by Lemma 4.4. By Lemma 9.1, we get the same bound for the number of superspecial curves over $\mathbb{F}_p$. This shows that Proposition 3.4 holds as q ranges over the set of primes.

Now we let q range over the set of proper prime powers. Let $q = p^e$ for some prime p and $e > 1$. First we bound the number of principally-polarized superspecial split surfaces.

By [23, Thm. 2, p. 41], the total number of superspecial curves over $\overline{\mathbb{F}}_q$ is equal to the class number $H_2(1, p) \leq p^2/4$ mentioned above, so by Lemma 9.1 there are at most $1152p^2/4 = 288p^2$ superspecial curves over $\mathbb{F}_q$. Similarly, the number of supersingular j-invariants is $p/12 + O(1)$, so the number of distinct products of polarized supersingular elliptic curves over $\overline{\mathbb{F}}_q$ is also bounded by a constant times p^2; by Lemma 9.1, this shows that the number of principally-polarized superspecial split abelian surfaces over $\mathbb{F}_q$ that are not Jacobians is $\ll p^2$. Since $q \geq p^2$, the number of principally-polarized superspecial split surfaces is $\ll q$.

We are left with the task of estimating the number of non-superspecial supersingular split curves over $\mathbb{F}_q$. To do this, we appeal to a moduli space argument. As noted above, the coarse moduli space of non-superspecial supersingular curves is geometrically a union of $p^2/2880 + O(p)$ components, each one an open subvariety of $\mathbf{A}^1$. Thus, the number of $\mathbb{F}_q$-rational points on this moduli space is at most $p^2q/2800 + O(pq)$. By Lemma 9.1, each rational point on the moduli space corresponds to at most 1152 curves over $\mathbb{F}_q$, so there are $\ll p^2q \ll q^2$ principally-polarized supersingular split abelian surfaces over $\mathbb{F}_q$. □

10. A LOWER BOUND FOR THE NUMBER OF SPLIT SURFACES

In this section we prove Proposition 3.5.

Let ℓ be a prime coprime to q. We say that two elliptic curves E and F over $\mathbb{F}_q$ are *of the same symplectic type modulo* ℓ if (in the notation of Section 5) the set $\mathrm{Isom}^1(E[\ell], F[\ell])$ is nonempty; that

is, if there is an isomorphism $E[\ell] \to F[\ell]$ of group schemes that respects the Weil pairing. Clearly, if E and F have the same symplectic type modulo ℓ then their traces of Frobenius are congruent modulo ℓ, so for each residue class modulo ℓ, the elliptic curves whose traces lie in that residue class are distributed among some number of symplectic types.

Lemma 10.1. *Let ℓ be an odd prime coprime to q and let $a \in \mathbb{Z}/\ell$.*

(a) *If $a^2 \not\equiv 4q \bmod \ell$ then all elliptic curves $E/\mathbb{F}_q$ with $a(E) \equiv a \bmod \ell$ are of the same symplectic type.*
(b) *If $a^2 \equiv 4q \bmod \ell$, there are at most three symplectic types of elliptic curves with trace congruent to a. If we fix an ℓth root of unity $\zeta \in \overline{\mathbb{F}}_q$, these three types are determined as follows:*
   1. *Those E for which Frobenius acts as an integer on $E[\ell]$.*
   2. *Those E for which Frobenius does not act as an integer on $E[\ell]$, and for which the Weil pairing $e(P, \mathrm{Fr}_E(P))$ is of the form ζ^x with $x \in (\mathbb{Z}/\ell)^\times$ a square for all $P \in E[\ell](\overline{\mathbb{F}}_q)$ with $\mathrm{Fr}_E(P) \neq (a/2)P$.*
   3. *Those E for which Frobenius does not act as an integer on $E[\ell]$, and for which the Weil pairing $e(P, \mathrm{Fr}_E(P))$ is of the form ζ^x with $x \in (\mathbb{Z}/\ell)^\times$ a nonsquare for all $P \in E[\ell](\overline{\mathbb{F}}_q)$ with $\mathrm{Fr}_E(P) \neq (a/2)P$.*

Corollary 10.2. *For each odd ℓ coprime to q, there are at most $\ell + 4$ symplectic types of elliptic curves modulo ℓ over $\mathbb{F}_q$.* □

Proof of Lemma 10.1. Let E be an elliptic curve over $\mathbb{F}_q$ and let G be the automorphism group of $E[\ell]$. In Section 5 we defined a map $m\colon G \to \operatorname{Aut} \boldsymbol{\mu}_\ell$. If $a^2 \not\equiv 4q \bmod \ell$ then m is surjective, so there is an isometry between $E[\ell]$ and $F[\ell]$ for any two curves E and F of trace a. Likewise, if Frobenius acts as a constant on $E[\ell]$ then m is surjective, so if Frobenius acts as $a/2$ on $E[\ell]$ and $F[\ell]$ then there is an isometry between those two group schemes.

On the other hand, if Frobenius does not act semisimply then the image of m is a coset of a subgroup of index 2, that is, a coset of the subgroup of squares, and is an isometry between $E[\ell]$ and $F[\ell]$ for two such curves E and F if and only if the image of m is the same for both of them. □

Lemma 10.3. *Let ℓ be a prime coprime to q and with $\ell \equiv 1 \bmod 4$. If two elliptic curves E and F over $\mathbb{F}_q$ have the same symplectic type modulo ℓ, then there are at least $\ell - 1$ elements of* $\operatorname{Isom}^{-1}(E[\ell], F[\ell])$.

Proof. Since E and F have the same symplectic type modulo ℓ there is an isometry $\eta\colon E[\ell] \to F[\ell]$. Let b be an integer with $b^2 \equiv -1 \bmod \ell$. Then $b\eta$ is an anti-isometry, so $\operatorname{Isom}^{-1}(E[\ell], F[\ell])$ is nonempty. From Proposition 4.3 we know that $\#\operatorname{Aut} E[\ell] \geq (\ell-1)^2$, so $\#\operatorname{Isom}^1(E[\ell], E[\ell])$ is at least $\ell - 1$, and it follows that there are at least this many elements of $\operatorname{Isom}^{-1}(E[\ell], F[\ell])$. □

Proof of Proposition 3.5. Let c be a constant such that

$$H(\Delta) < c|\Delta|^{1/2} \log|\Delta| (\log\log|\Delta|)^2$$

for all negative discriminants Δ; such a constant exists by Lemma 4.4. We will show that for every prime $\ell \neq p$ with $\ell \equiv 1 \bmod 4$ and with

$$\ell < \frac{q^{1/2}}{1600c^2(\log q)^2(\log\log q)^4} \tag{13}$$

there are more than $2q^2/5$ triples (E_1, E_2, η), where E_1 and E_2 are nonisogenous ordinary elliptic curves over $\mathbb{F}_q$ and $\eta\colon E_1[\ell] \to E_2[\ell]$ is an anti-isometry. Dirichlet's theorem shows that there are constants $c' \geq 13, c'' > 0$ such that when $q \geq c'$ the number of such primes ℓ is at least

$$\frac{c'' q^{1/2}}{(\log q)^3 (\log\log q)^4},$$

so for $q \geq c'$ we will have at least

$$\frac{c'' q^{5/2}}{5(\log q)^3 (\log\log q)^4}$$

distinct principally-polarized abelian surfaces, thus proving the unconditional part of Proposition 3.5.

Let ℓ be a prime as above, let $t \leq \ell + 4$ be the number of symplectic types of curves modulo ℓ, and let $S_1, \ldots, S_t$ be the sets of ordinary curves of the t different symplectic types. We would like to count the number of pairs of curves (E_1, E_2) where E_1 and E_2 are not isogenous to one another but are of the same symplectic type. The number of ordered pairs (E_1, E_2) where E_1 and E_2 are of the same type is $\sum_{i=1}^{t} (\#S_i)^2$. This sum is minimized when the elliptic curves are evenly distributed across the symplectic types. It is easy check that when $q \geq 13$ there are always at least $5q/3$ ordinary elliptic curves over $\mathbb{F}_q$, so we see that

$$\sum_{i=1}^{t} (\#S_i)^2 \geq t \left(\frac{5q}{3t}\right)^2 \geq \frac{25q^2}{9(\ell+4)} \geq \frac{125q^2}{81\ell} > \frac{3q^2}{2\ell}.$$

On the other hand, the number of ordered pairs (E_1, E_2) of ordinary elliptic curves that are isogenous to one another is

$$\sum_{\substack{-2\sqrt{q} < a < 2\sqrt{q} \\ \gcd(a,q)=1}} H(a^2 - 4q)^2.$$

Using Lemma 4.4 and the definition of c, we see that each summand is at most

$$c^2(4q)(\log(4q))^2(\log\log(4q))^4 < 400c^2 q(\log q)^2(\log\log q)^4.$$

so the number of such ordered pairs is at most

$$1600c^2 q^{3/2}(\log q)^2(\log\log q)^4 \leq q^2/\ell.$$

Thus, the number of ordered pairs (E_1, E_2) of nonisogenous curves that have the same symplectic type is at least $(1/2)(q^2/\ell)$. By Lemma 10.3, this gives us more than $(1/2)(\ell - 1)q^2/\ell > 2q^2/5$ triples (E_1, E_2, η) where E_1 and E_2 are nonisogenous ordinary elliptic curves and $\eta\colon E_1[\ell] \to E_2[\ell]$ is an anti-isometry, as we wanted.

If the generalized Riemann hypothesis holds, we modify our argument as follows. We take c to be a constant such that

$$H(\Delta) < c|\Delta|^{1/2}(\log\log|\Delta|)^3$$

for all negative discriminants Δ, and consider primes $\ell \equiv 1 \bmod 4$ bounded by

$$\ell < \frac{q^{1/2}}{1600c^2(\log\log q)^6}$$

instead of by (13). Again we find that for each such ℓ we have more than $2q^2/5$ triples (E_1, E_2, η), where E_1 and E_2 are nonisogenous ordinary elliptic curves and $\eta\colon E_1[\ell] \to E_2[\ell]$ is an anti-isometry. Dirichlet's theorem then leads to the desired estimate for W_q. □

11. Numerical data, evidence for Conjecture 1.1, and further directions

In this section we present summaries of some computations that help give some indication of the behavior of several of the quantities that we study and provide bounds for, and we give some evidence that seems to support Conjecture 1.1. We close with some thoughts about possible extensions of our results.

11.1. **The sum of the relative conductors.** In Section 6 we proved Proposition 3.1, which gives an upper bound on the number of principally-polarized ordinary split nonisotypic abelian surfaces over a finite field $\mathbb{F}_q$. The key to the argument is Lemma 6.3, which gives an upper bound for the sum of the relative conductors of the ordinary elliptic curves over $\mathbb{F}_q$. The lemma shows that there is a constant c such that for all q this sum is at most $cq(\log q)^2$. However, we suspect that the sum of the relative conductors grows more slowly than this; it is perhaps even $O(q)$.

We computed this sum for all prime powers q less than 10^7. For q in the range $(10^3, 10^4)$, the sum lies between $2.07q$ and $4.27q$; for q in the range $(10^4, 10^5)$, the sum lies between $2.14q$ and $3.95q$; for q in the range $(10^5, 10^6)$, the sum lies between $2.09q$ and $3.82q$; and for q in the range $(10^6, 10^7)$, the sum lies between $2.10q$ and $3.77q$. Note that as q ranges through these successive intervals, the upper bound on $1/q$ times the sum of the relative conductors decreases; this is why we are tempted to suspect that the sum of the relative conductors is $O(q)$.

11.2. **The probability that a principally-polarized abelian surface is split.** If S is a finite collection of geometric objects having finite automorphism groups, we define the *weighted cardinality* $\#'S$ of S by

$$\#'S = \sum_{s \in S} \frac{1}{\#\operatorname{Aut} s}.$$

It is well-known that the weighted cardinality can lead to cleaner formulas than the usual cardinality. For instance, the weighted cardinality of the set of genus-2 curves over $\mathbb{F}_q$ is equal to q^3 ([7, Prop. 7.1, p. 87]). A principally-polarized abelian surface over a field is either a Jacobian, a product of polarized elliptic curves, or the restriction of scalars of a polarized elliptic curve over a quadratic extension of the base field ([12, Thm. 3.1, p. 270]). One can show that the weighted cardinality of the set of products of polarized elliptic curves over $\mathbb{F}_q$ is $q^2/2$, as is the weighted cardinality of the set of restrictions of scalars. Thus, if we let $\mathcal{A}_2$ denote the moduli stack of principally-polarized abelian surfaces, then $\#'\mathcal{A}_2(\mathbb{F}_q) = q^3 + q^2$.

For each prime power q we let

$$c_q = \frac{\sqrt{q} \cdot \#'\mathcal{A}_{2,\mathrm{split}}(\mathbb{F}_q)}{\#'\mathcal{A}_2(\mathbb{F}_q)} = \frac{\sqrt{q} \cdot \#'\mathcal{A}_{2,\mathrm{split}}(\mathbb{F}_q)}{q^3 + q^2}.$$

For all primes $q < 300$ and for $q = 521$ we computed the exact value of c_q by direct enumeration of curves and computation of zeta functions. For $q \in \{1031, 2053, 4099, 16411, 65537\}$ (the smallest primes greater than 2^i for $i = 10, 11, 12, 14, 16$) we computed approximations to c_q by randomly sampling genus-2 curves (with probability inversely proportional to their automorphism groups), and then adjusting the probabilities to account for the non-Jacobians. We computed enough examples for each of these q to determine c_q with a standard deviation of less 0.0005. The result of the computations is displayed in Figure 1; the (almost invisible) error bars on the rightmost five data points indicate the standard deviation. Note that the horizontal axis is $\log\log q$; even so, the graph looks sublinear. This encourages us to speculate that perhaps the c_q are bounded away from 0 and ∞.

11.3. **Reductions of a fixed surface.** Let A/K be a principally-polarizable abelian surface over a number field such that the absolute endomorphism ring $\operatorname{End}_{\overline{K}} A$ is isomorphic to $\mathbb{Z}$, and recall the counting function $\pi_{\mathrm{split}}(A/K, z)$ introduced Section 1. Conjecture 1.1 states that $\pi_{\mathrm{split}}(A/K, z) \sim C_A \sqrt{z}/\log z$; we tested this against actual data on the splitting behavior of a particular surface A over $\mathbb{Q}$.

Let A be the Jacobian of the curve over $\mathbb{Q}$ with affine model $y^2 = x^5 + x + 6$. Using the methods of [14], Andrew Sutherland computed for us the primes $p < 2^{30}$ for which the mod-p reduction of A is split, thereby giving us the exact value of $\pi_{\mathrm{split}}(A/\mathbb{Q}, z)$ for all $z \le 2^{30}$. We numerically fit curves of the form $a\sqrt{z}/(\log z)^b$ and of the form $c\sqrt{z}/\log z$ to this function. For curves of the

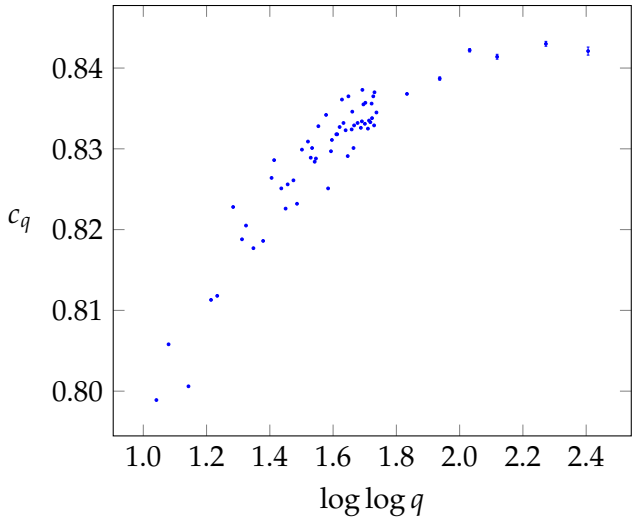

FIGURE 1. The values of c_q for the primes q with $17 \leq q \leq 293$, together with $q \in \{521, 1031, 2053, 4099, 16411, 65537\}$. The values of c_q for the five largest q were computed experimentally; the error bars indicate one standard deviation.

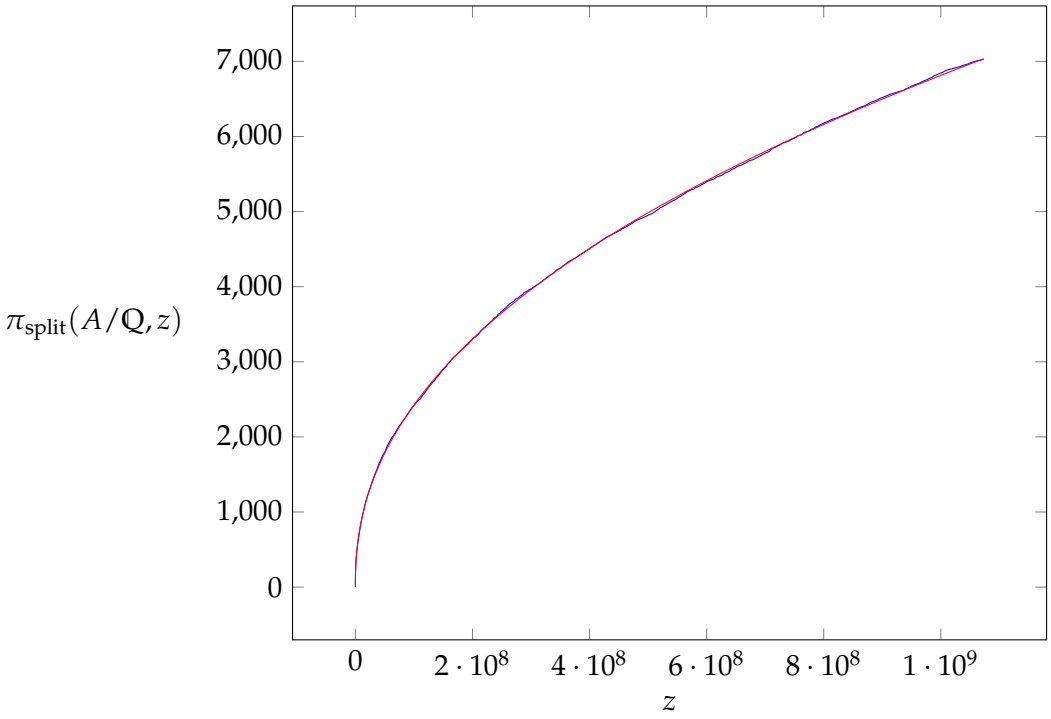

FIGURE 2. The blue curve plots the function $\pi_{\text{split}}(A/\mathbb{Q}, z)$ for the Jacobian A of the curve $y^2 = x^5 + x + 6$ over $\mathbb{Q}$. The red curve is $c\sqrt{z}/\log z$, with $c \approx 4.4651$.

form $a\sqrt{z}/(\log z)^b$, the best-fitting exponent b was $b \approx 1.02269$, reasonably close to our conjectural value of 1. For curves of the form $c\sqrt{z}/\log z$, the best-fitting constant c was $c \approx 4.4651$. In Figure 2 we present the actual data (in blue) alongside the best-fitting function $c\sqrt{z}/\log z$ (in red); the figure shows that the idealized function is in close agreement with the actual function.

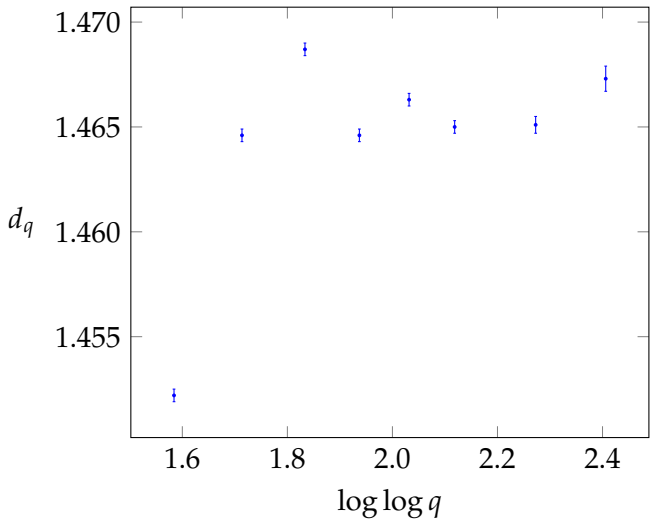

FIGURE 3. The experimentally computed values of d_q for the primes q in $\{131, 257, 521, 1031, 2053, 4099, 16411, 65537\}$. Error bars indicate one standard deviation.

11.4. **Further directions.** We noted in Section 1 that our definition of $\mathcal{A}_{2,\mathrm{split}}(\mathbb{F}_q)$ was perhaps not as natural as it could be — one could also ask about principally-polarized surfaces that split over $\overline{\mathbb{F}}_q$, not just over $\mathbb{F}_q$ itself. We suspect that a result like Theorem 1.2 holds for this more general type of splitting. To prove such a theorem, one would need to estimate the number of principally-polarized surfaces in several types of isogeny classes: the simple ordinary isogeny classes that are geometrically split (which are enumerated in [22, Thm. 6, p. 145]); and the supersingular isogeny classes (which are all geometrically split). There are a number of ways one could try to estimate the number of principally-polarized surfaces in these isogeny classes; for instance, the techniques of [21] might be of use. We will not speculate further on this here.

Let $\mathcal{A}_{2,\text{geom. split}}(\mathbb{F}_q)$ denote the subset of $\mathcal{A}_2(\mathbb{F}_q)$ consisting of those principally-polarized varieties that are not geometrically simple, and for each q let d_q denote the ratio

$$d_q = \frac{\sqrt{q} \cdot \#' \mathcal{A}_{2,\text{geom. split}}(\mathbb{F}_q)}{\#' \mathcal{A}_2(\mathbb{F}_q)} = \frac{\sqrt{q} \cdot \#' \mathcal{A}_{2,\text{geom. split}}(\mathbb{F}_q)}{q^3 + q^2}.$$

While collecting the data presented in Section 11.2 we also collected data on d_q by random sampling of curves. Figure 3 presents the results for $q \in \{131, 257, 521, 1031, 2053, 4099, 16411, 65537\}$. The figure suggests that perhaps d_q is bounded away from 0 and ∞.

REFERENCES

[1] Jeffrey D. Achter, *Split reductions of simple abelian varieties*, Math. Res. Lett. **16** (2009), no. 2, 199–213. MR 2496739 (2010d:14063)

[2] ———, *Explicit bounds for split reductions of simple abelian varieties*, J. Théor. Nombres Bordeaux **24** (2012), no. 1, 41–55. MR 2914900

[3] Tom M. Apostol, *Introduction to analytic number theory*, Springer-Verlag, New York-Heidelberg, 1976, Undergraduate Texts in Mathematics. MR 0434929 (55 #7892)

[4] Nir Avni, Uri Onn, Amritanshu Prasad, and Leonid Vaserstein, *Similarity classes of 3×3 matrices over a local principal ideal ring*, Comm. Algebra **37** (2009), no. 8, 2601–2615. MR 2543507 (2010h:15025)

[5] Pilar Bayer and Josep González, *On the Hasse-Witt invariants of modular curves*, Experiment. Math. **6** (1997), no. 1, 57–76. MR 1464582 (98h:11074)

[6] H. F. Blichfeldt, *The minimum values of positive quadratic forms in six, seven and eight variables*, Math. Z. **39** (1935), no. 1, 1–15. MR 1545485

[7] Bradley W. Brock and Andrew Granville, *More points than expected on curves over finite field extensions*, Finite Fields Appl. **7** (2001), no. 1, 70–91, Dedicated to Professor Chao Ko on the occasion of his 90th birthday. MR 1803936 (2002d:11070)

[8] J. W. S. Cassels, *Rational quadratic forms*, London Mathematical Society Monographs, vol. 13, Academic Press, Inc. [Harcourt Brace Jovanovich, Publishers], London-New York, 1978. MR 522835 (80m:10019)

[9] Henri Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics, vol. 138, Springer-Verlag, Berlin, 1993. MR 1228206 (94i:11105)

[10] Pierre Deligne, *Variétés abéliennes ordinaires sur un corps fini*, Invent. Math. **8** (1969), 238–243. MR 0254059 (40 #7270)

[11] Gerhard Frey and Ernst Kani, *Curves of genus 2 covering elliptic curves and an arithmetical application*, Arithmetic algebraic geometry (Texel, 1989), Progr. Math., vol. 89, Birkhäuser Boston, Boston, MA, 1991, pp. 153–176. MR 1085258 (91k:14014)

[12] Josep González, Jordi Guàrdia, and Victor Rotger, *Abelian surfaces of GL_2-type as Jacobians of curves*, Acta Arith. **116** (2005), no. 3, 263–287. MR 2114780 (2005m:11107)

[13] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, fourth ed., The Clarendon Press, Oxford University Press, New York, 1968.

[14] David Harvey and Andrew V Sutherland, *Computing Hasse–Witt matrices of hyperelliptic curves in average polynomial time, II*, 2014, arXiv:1410.5222 [math.NT]. To appear in *Frobenius Distributions* (D. Kohel, ed.).

[15] Ki-ichiro Hashimoto and Tomoyoshi Ibukiyama, *On class numbers of positive definite binary quaternion Hermitian forms. II*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **28** (1981), no. 3, 695–699 (1982). MR 656045 (83m:10029)

[16] Helmut Hasse, *Zur Theorie der abstrakten elliptischen Funktionenkörper. I. Die Struktur der Gruppe der Divisorenklassen endlicher Ordnung.*, J. Reine Angew. Math. **175** (1936), 55–62.

[17] ———, *Zur Theorie der abstrakten elliptischen Funktionenkörper. II. Automorphismen und Meromorphismen. Das Additionstheorem.*, J. Reine Angew. Math. **175** (1936), 69–88.

[18] ———, *Zur Theorie der abstrakten elliptischen Funktionenkörper. III. Die Struktur des Meromorphismenringes. Die Riemannsche Vermutung.*, J. Reine Angew. Math. **175** (1936), 193–208.

[19] Ch. Hermite, *Extraits de lettres de M. Ch. Hermite à M. Jacobi sur différents objets de la théorie des nombres*, J. Reine Angew. Math. **40** (1850), 261–277.

[20] Everett W. Howe, *Principally polarized ordinary abelian varieties over finite fields*, Trans. Amer. Math. Soc. **347** (1995), no. 7, 2361–2401. MR 1297531 (96i:11065)

[21] ———, *On the non-existence of certain curves of genus two*, Compos. Math. **140** (2004), no. 3, 581–592. MR 2041770 (2005a:11088)

[22] Everett W. Howe and Hui June Zhu, *On the existence of absolutely simple abelian varieties of a given dimension over an arbitrary field*, J. Number Theory **92** (2002), no. 1, 139–163. MR 1880590 (2003g:11063)

[23] Tomoyoshi Ibukiyama and Toshiyuki Katsura, *On the field of definition of superspecial polarized abelian varieties and type numbers*, Compositio Math. **91** (1994), no. 1, 37–46. MR 1273924 (95d:14044)

[24] Tomoyoshi Ibukiyama, Toshiyuki Katsura, and Frans Oort, *Supersingular curves of genus two and class numbers*, Compositio Math. **57** (1986), no. 2, 127–152. MR 827350 (87f:14026)

[25] Jun-ichi Igusa, *Arithmetic variety of moduli for genus two*, Ann. of Math. (2) **72** (1960), 612–649. MR 0114819 (22 #5637)

[26] Masanobu Kaneko, *A generalization of the Chowla-Selberg formula and the zeta functions of quadratic orders*, Proc. Japan Acad. Ser. A Math. Sci. **66** (1990), no. 7, 201–203. MR 1078409 (91i:11166)

[27] Toshiyuki Katsura and Frans Oort, *Families of supersingular abelian surfaces*, Compositio Math. **62** (1987), no. 2, 107–167. MR 898731 (88j:14053)

[28] Kiran S. Kedlaya and Andrew V. Sutherland, *Computing L-series of hyperelliptic curves*, Algorithmic number theory, Lecture Notes in Comput. Sci., vol. 5011, Springer, Berlin, 2008, pp. 312–326. MR 2467855 (2010d:11070)

[29] Neal Koblitz, *p-adic variation of the zeta-function over families of varieties defined over finite fields*, Compositio Math. **31** (1975), no. 2, 119–218. MR 0414557 (54 #2658)

[30] Edmund Landau, *Neuer Beweis des Primzahlsatzes und Beweis des Primidealsatzes*, Math. Ann. **56** (1903), no. 4, 645–670. MR 1511191

[31] ———, *Über den Verlauf der zahlentheoretischen funktion $\varphi(x)$*, Arch. der Math. u. Phys. (3) **5** (1903), 86–91.

[32] Serge Lang and Hale Trotter, *Frobenius distributions in GL_2-extensions*, Lecture Notes in Mathematics, Vol. 504, Springer-Verlag, Berlin-New York, 1976. MR 0568299 (58 #27900)

[33] J. E. Littlewood, *On the class-number of the corpus $P(\sqrt{-k})$*, Proc. London Math. Soc. **S2-27** (1927), no. 1, 358. MR 1575396

[34] J. S. Milne, *The Tate-Šafarevič group of a constant abelian variety*, Invent. Math. **6** (1968), 91–105. MR 0244264 (39 #5581)

[35] David Mumford, *Abelian varieties*, second ed., Tata Institute of Fundamental Research Studies in Mathematics, No. 5, Published for the Tata Institute of Fundamental Research, Bombay; Oxford University Press, London, 1974, With appendices by C. P. Ramanujam and Yuri Manin.

[36] V. Kumar Murty, *Frobenius distributions and Galois representations*, Automorphic forms, automorphic representations, and arithmetic (Fort Worth, TX, 1996), Proc. Sympos. Pure Math., vol. 66.1, Amer. Math. Soc., Providence, RI, 1999, pp. 193–211. MR 1703751 (2000h:11057)
[37] ———, *Splitting of abelian varieties: a new local-global problem*, Algebra and number theory, Hindustan Book Agency, Delhi, 2005, pp. 258–268. MR 2193358 (2006h:11061)
[38] V. Kumar Murty and Vijay M. Patankar, *Splitting of abelian varieties*, Int. Math. Res. Not. IMRN **2008** (2008), no. 12, Art. ID rnn033, 27. MR 2426750 (2009d:14062)
[39] Frans Oort, *Subvarieties of moduli spaces*, Invent. Math. **24** (1974), 95–119. MR 0424813 (54 #12771)
[40] René Schoof, *Nonsingular plane cubic curves over finite fields*, J. Combin. Theory Ser. A **46** (1987), no. 2, 183–211. MR 914657 (88k:14013)
[41] Goro Shimura, *Moduli and fibre systems of abelian varieties*, Ann. of Math. (2) **83** (1966), 294–338. MR 0199190 (33 #7339)
[42] Joseph H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151, Springer-Verlag, New York, 1994. MR 1312368 (96b:11074)
[43] William C. Waterhouse, *Abelian varieties over finite fields*, Ann. Sci. École Norm. Sup. (4) **2** (1969), 521–560. MR 0265369 (42 #279)
[44] Cassandra L. Williams, *Conjugacy classes of matrix groups over local rings and an application to the enumeration of abelian varieties*, ProQuest LLC, Ann Arbor, MI, 2012, Thesis (Ph.D.)–Colorado State University. MR 3078498
[45] David Zywina, *The splitting of reductions of an abelian variety*, Int. Math. Res. Not. IMRN **2014** (2014), no. 18, 5042–5083. MR 3264675

E-mail address: j.achter@colostate.edu

DEPARTMENT OF MATHEMATICS, COLORADO STATE UNIVERSITY, FORT COLLINS, CO 80523
URL: http://www.math.colostate.edu/~achter

E-mail address: however@alumni.caltech.edu

CENTER FOR COMMUNICATIONS RESEARCH, 4320 WESTERRA COURT, SAN DIEGO, CA 92121-1967
URL: http://www.alumni.caltech.edu/~however