DISSERTATION

ABELIAN SURFACES WITH REAL MULTIPLICATION OVER FINITE FIELDS

Submitted by

Hilary Freese

Department of Mathematics

In partial fulfillment of the requirements

For the Degree of Doctor of Philosophy

Colorado State University

Fort Collins, Colorado

Summer 2014

Doctoral Committee:

Advisor: Jeffrey Achter

Rachel Pries
Chris Peterson
Daniele Tavani

ABSTRACT

ABELIAN SURFACES WITH REAL MULTIPLICATION OVER FINITE FIELDS

Given a simple abelian surface $A/\mathbb{F}_q$, the endomorphism algebra, $\mathrm{End}(A) \otimes \mathbb{Q}$, contains a unique real quadratic subfield. We explore two different but related questions about when a particular real quadratic subfield K^+ is the maximal real subfield of the endomorphism algebra. First, we compute the number of principally polarized abelian surfaces $A/\mathbb{F}_q$ such that $K^+ \subset \mathrm{End}(A) \otimes \mathbb{Q}$. Second, we consider an abelian surface $A/\mathbb{Q}$, and its reduction $A_p = A \mod p$, then ask for which primes p is $K^+ \subset \mathrm{End}(A) \otimes \mathbb{Q}$. The result from the first question leads to a heuristic for the second question, namely that the number of $p < x$ for which $K^+ \subset \mathrm{End}(A) \otimes \mathbb{Q}$ grows like $\frac{\sqrt{x}}{\log(x)}$.

ACKNOWLEDGEMENTS

I would like to thank Jeff Achter for all his guidance and patience, and Cassie Williams for her mentorship. Great thanks is also due to Leif Anderson for his endless work on building this LaTeX document class.

TABLE OF CONTENTS

CHAPTER 1

Introduction

An abelian variety is a geometric object that is defined as the projective zero set of polynomials which has a group structure on its points. The first instance of such an object are the abelian varieties of dimension one, elliptic curves. An isogeny between two abelian varieties is a special type of map which defines an equivalence relation on the set of all abelian varieties of a given dimension. One can also define a particular kind of map from an abelian variety to itself called an endomorphism. The collection of such maps forms a ring and the structure of the endomorphism ring also characterizes the abelian variety.

For each endomorphism there is a natural way to represent it as an element of $\mathrm{GL}_{2g}(\mathbb{Z}/\ell)$, where g is the dimension of the variety, by looking at its action on the $\ell-$torsion points of the variety. Furthermore, since any abelian variety also admits a polarization these endomorphisms can be represented by matrices in $\mathrm{GSp}_{2g}(\mathbb{Z}/\ell)$. Given the associated matrix representation one can associate to an endomorphism a characteristic polynomial. For abelian varieties defined over finite fields there is a special endomorphism, namely the Frobenius endomorphism. In 1966 Tate proved that the isogeny classes of abelian varieties over finite fields are determined by the characteristic polynomials of their Frobenius endomorphisms.

Another trait encoded by the characteristic polynomial of the Frobenius endomorphism has to do with the structure of the endomorphism ring. In particular for an ordinary elliptic curves a root of the characteristic polynomial of Frobenius defines an imaginary quadratic extension of $\mathbb{Q}$ inside of which sits the endomorphism ring of the elliptic curve. In the case of abelian surfaces the coefficients of the characteristic polynomial of Frobenius determine the discriminant of the totally real quadratic subfield sitting inside the endomorphism ring of the abelian surface.

An interesting question one can then ask is how many characteristic polynomials correspond to a particular endomorphism structure. Or more broadly one could ask how many abelian varieties have that particular endomorphism structure. Lang and Trotter posed a question similar to this for elliptic curves. Specifically they asked for how many primes $p < x$ does the reduction of an elliptic curve mod p have a prescribed endomorphism structure. What they conjecture is that this number grows like $\frac{\sqrt{x}}{\log(x)}$.

In this paper, we explore a similar question for abelian surfaces: for how many primes $p < x$ does the reduction of an abelian surface mod p have a prescribed real quadratic subfield as a part of its endomorphism structure? In order to answer this question, or conjecture about its rate of growth, we need three main things. First, we need to look at abelian surfaces defined over finite fields and determine which characteristic polynomials of Frobenius admit the same discriminant as a fixed real quadratic field. Second, we need to determine the size of the isogeny class defined by that characteristic polynomial. Finally, we will need to assess the probability that the reduction of an abelian surface mod p has Frobenius endomorphism which corresponds to a characteristic polynomial with discriminant congruent to that of a fixed real quadratic field.

Our main result will give justification for the following conjecture about abelian surfaces.

Conjecture 1.0.1. *[Main Conjecture] Let A be an abelian surface defined over $\mathbb{Q}$ with $End_{\overline{\mathbb{Q}}}(A) \cong \mathbb{Z}$, let $A_p \equiv A \mod p$, and let K^+ be a given real quadratic extension of $\mathbb{Q}$. Define*

$$N_{A,K^+}(x) = \#\{p \leq x \,:\, p \textit{ is prime and } K^+ \subset End(A_p)\}.$$

Then there exists a constant $C(A, K^+) > 0$ *such that*

$$N_{A,K^+}(x) \approx C(A, K^+)\frac{\sqrt{x}}{\log(x)}.$$

CHAPTER 2

Base Case and Motivation: Elliptic Curves and The Lang-Trotter Conjecture

2.1. Elliptic Curves as Abelian Varieties

An elliptic curve is an abelian variety of dimension one. There are various ways one can define an elliptic curve, some of which can be generalized to define abelian varieties of higher dimension. The first definition which generalizes is: an abelian variety is a nonsingular projective zero set of an irreducible polynomial (or set of irreducible polynomials) with a group structure given by regular maps. An elliptic curve is a projective curve given by a polynomial of the form $y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3$, where the a_i are constants [Was08]. In the case that the elliptic curve is defined over a field of characteristic not equal to 2 or 3 this polynomial equation has an affine model of the form $y^2 = x^3 + ax + b$. This definition of an elliptic curve is nice since it allows for good visualization of the affine points, as well as gives an explicit equation of definition, and thus allows for explicit formulas for the addition of points. Let $+_E$ denote elliptic curve addition for the elliptic curve E, and let ∞_E denote the additive identity.

Elliptic curve addition hinges on Bézout's theorem, guaranteeing here that a line (a curve of degree one) will intersect a curve of degree three (the elliptic curve) exactly three times, counting multiplicity. In particular, to determine the point $P +_E Q$ first construct the secant line L_1 between the points P and Q, then determine the third point of intersection of L_1 with the elliptic curve E, call this point $P * Q$. Next, construct the secant line between the point $P * Q$ and the point at infinity, ∞_E, denote this line by L_2. From here determine the third point of intersection of L_2 with E; this is the point defined to be $P +_E Q$. This

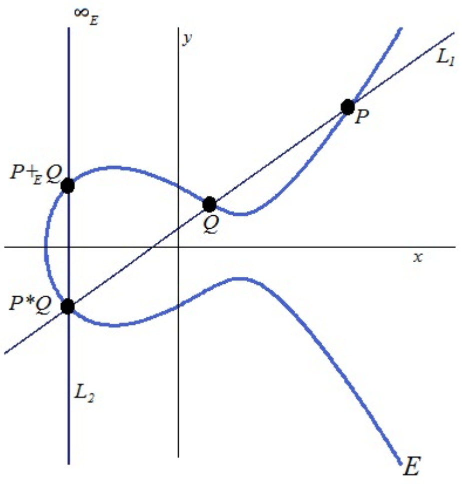


Figure 2.1. Constructing the point $P +_E Q$, for the elliptic curve $E : y^2 = x^3 - 10x + 17$.

construction is illustrated in Figure 2.1 above. Equations for this addition law can be written down explicitly in terms of the coordinates of the point $P = (x, y)$,

Let E be defined over a field k, then the points which lie on E with coordinates in k are denoted by $E(k)$.

Another definition which generalizes is unique to abelian varieties defined over $\mathbb{C}$. In this case the abelian variety is a complex torus; $A(\mathbb{C}) \simeq \mathbb{C}^g/\Lambda$ for some lattice $\Lambda \subset \mathbb{C}^g$. For an elliptic curve $E(\mathbb{C}) \cong \mathbb{C}/L$ where L is a lattice generated by two elements, ω_1 and ω_2, as illustrated in Figure 2.2 below.

The Weierstrass $\wp-$function, $\wp(z; L) : \mathbb{C} \to \mathbb{C}$ gives a way, in some sense, of translating between these two definitions for an elliptic curve [Was08]. In particular, for a lattice $L \subset \mathbb{C}$ and the elliptic curve $E : y^2 = 4x^3 - g_2x - g_3$, the map

$$\Phi : \mathbb{C}/L \to E(\mathbb{C})$$

$$z \mapsto (\wp(z), \wp'(z))$$

$$0 \mapsto \infty_E$$

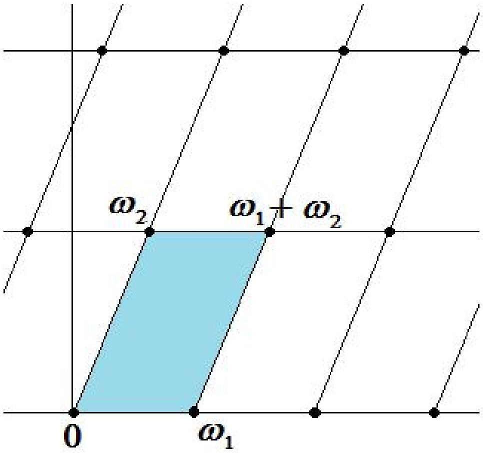


FIGURE 2.2. The lattice L, generated by ω_1 and ω_2.

is an isomorphism of groups, where g_2 and g_3 are explicit constants depending on L [Was08].

Of interest in this paper will be the dimension two abelian varieties, called abelian surfaces. In this case there is a third definition of elliptic curves which generalizes. When the dimension is two, every simple principally polarized abelian variety can be realized as the Jacobian variety of a curve of genus 2 [Mil08]. Every such curve of genus 2 has an equation of the form

$$Y^2Z^4 = c_0X^6 + c_1X^5Z + \cdots + c_6Z^6.$$

Given the group structure on an elliptic curve (and on abelian varieties in general) one might wish to look at the types of maps which can be constructed from E back to itself. Maps from E to itself that are algebraic and fix the identity, ∞_E, are called *endomorphisms.* The set of endomorphisms of an elliptic curve $\text{End}(E) := \{\phi : E \to E \ : \ \phi \text{ is a homomorphism}\}$ forms a ring. Furthermore, $\text{End}^0(E) := \text{End}(E) \otimes \mathbb{Q}$ is an algebra, and is called the *endomorphism algebra* of E.

An endomorphism of E induces a homomorphism on the group of points, $E(k)$. Many of these endomorphisms are of the form multiplication by m, for $m \in \mathbb{Z}$. This map, $[m]$:

$E \to E$, takes the point P to the point $mP = P +_E P +_E ... +_E P$. Thus we have a map $\mathbb{Z} \to \text{End}_k(E)$; and in fact, the following lemma states that this map is injective.

Lemma 2.1.1 ([Sil94]). *For an elliptic curve E defined over a field k, $\mathbb{Z} \hookrightarrow End_k(E)$.*

In many cases the endomorphism ring of E is in fact equal to $\mathbb{Z}$, so that the only endomorphisms of E are the multiplication by m maps. However in some instances the endomorphism ring is bigger; when this happens E is said to have *complex multiplication*.

Example 2.1.1. *Consider the elliptic curve $E : y^2 = x^3 - x$, defined over $\mathbb{C}$. This elliptic curve has an extra endomorphism that takes $(x, y) \mapsto (-x, iy)$. It can be shown that this is not equal to any multiplication by m map, thus $\mathbb{Z} \subsetneq End_{\mathbb{C}}(E)$, and in fact $End_{\mathbb{C}}(E) \cong \mathbb{Z}[i]$, and E is said to have complex multiplication by $\mathbb{Z}[i]$.*

To summarize what is known regarding the endomorphism ring of an elliptic curve we present the following proposition from Silverman.

Proposition 2.1.1 ([Sil09]). *The endomorphism ring of an elliptic curve E/k is either $\mathbb{Z}$, an order in a imaginary quadratic field, or an order in a quaternion algebra. If char$(k) = 0$, then only the first two are possible. If k is a finite field, then only the last two are possible.*

If k is a number field with $n = [k : \mathbb{Q}]$, an *order* $\mathcal{O}$ is a subring of k which is a finitely generated $\mathbb{Z}-$module of dimension n, such that $\mathcal{O}$ contains a $\mathbb{Q}-$basis of k (i.e. $\mathcal{O} \otimes \mathbb{Q} = k$). Every order of k is a subring of the ring of integers $\mathcal{O}_k$, which is the maximal order of k.

Returning to the multiplication by m maps one can define the $m-$torsion points to be the set $E[m](\bar{k}) = \{P \in E(\bar{k}) : mP = \infty_E\}$. In fact, the set $E[m](\bar{k})$ is a group and its structure is either

$$E[m](\bar{k}) \cong \mathbb{Z}/m \oplus \mathbb{Z}/m,$$

if the characteristic of k is zero or does not divide m; or

$$E[m](\bar{k}) \cong \mathbb{Z}/m' \oplus \mathbb{Z}/m' \text{ or } \mathbb{Z}/m \oplus \mathbb{Z}/m'$$

if $\operatorname{char}(k) = p > 0$ and $p|m$, with $m = p^r m'$ and $p \nmid m'$ [Was08]. In the case where one is looking at the $p-$torsion points over the field $\mathbb{F}_p$ then either $E[p](\overline{k}) = (\mathbb{Z}/p)$ and E is called *ordinary*, or $E[p](\overline{k}) = 0$ and E is called *supersingular*.

For a prime $\ell \nmid \operatorname{char}(k)$, define the *$\ell-$adic Tate module of E*,

$$T_\ell(E) = \varprojlim_n E[\ell^n](\bar{k}).$$

The Tate module of E is a free $\mathbb{Z}_\ell-$module of rank 2, [Mil08], and $\operatorname{End}(T_\ell(E))$ is isomorphic to a $\operatorname{Mat}_2(\mathbb{Z}_\ell)$. Thus the ring homomorphism

$$\operatorname{End}(E) \to \operatorname{End}(T_\ell(E))$$

will be used to look at matrix representations for endomorphisms of E; in particular for the Frobenius endomorphism. For an elliptic curve E defined over a finite field $\mathbb{F}_q$ of characteristic p, one can always define the *Frobenius endomorphism* $\operatorname{Frob}_q : E \to E$ which takes $(x, y) \mapsto (x^q, y^q)$. Then for any ℓ relatively prime to p, one can choose a basis for the $\ell-$torsion points, $E[\ell](\overline{\mathbb{F}_q})$, and then the action of Frob_q on $E[\ell](\overline{\mathbb{F}_q})$ can be represented as a matrix in $\operatorname{GL}_2(\mathbb{Z}/\ell)$. In fact, if one looks at the action of Frob_q on the ℓ^n-torsion points of E, then one obtains compatible matrix representations in $\operatorname{GL}_2(\mathbb{Z}/\ell^n)$ for all n. This in turn leads one to consider the action of Frob_q on the $\ell-$adic Tate module of E. In this case, the action of Frob_q can be represented as an element of $\operatorname{GL}_2(\mathbb{Z}_\ell)$. Given the matrix representation of Frob_q in any of these matrix groups one can associate to the endomorphism Frob_q a characteristic polynomial, namely the characteristic polynomial of the corresponding matrix. The characteristic polynomial of Frob_q in $\mathrm{GL}_2(\mathbb{Z}_\ell)$ has coefficients independent of the choice of ℓ, [Mil08], so one can write the characteristic polynomial of Frob_q in the form $f_E(X) = X^2 - a_q X + q$, where $a_q = q + 1 - N_q \in \mathbb{Z}$, and $N_q = \#E(\mathbb{F}_q)$. The roots of $f_E(X)$ are a complex conjugate pair, $\{\sqrt{q}e^{i\theta}, \sqrt{q}e^{-i\theta}\}$. Let $\pi_q = \sqrt{q}e^{i\theta}$. Then $\mathbb{Z}[\pi_q] \subset \mathrm{End}(E)$ and $\mathbb{Q}(\pi_q) \subset \mathrm{End}^0(E) = \mathrm{End}(E) \otimes \mathbb{Q}$, and $\mathrm{End}^0(E)$ is either the quadratic imaginary field $\mathbb{Q}(\pi_q)$ or a quaternion algebra, by Proposition 2.1.1.

2.2. Theorems About Elliptic Curves

Elliptic curves have been studied for centuries and in recent history have become central in number theory and cryptography. Some examples of questions which have been asked regarding elliptic curves have to do with the group of points which lie on the curve. In 1922 Louis Mordell proved that for an elliptic curve defined $\mathbb{Q}$, the group of points $E(\mathbb{Q})$ is a finitely generated abelian group. Such a group is of the form $\mathbb{Z}^r \oplus F$ for some $r \geq 0$ and some finite group F. Soon after, in 1928, Andrè Weil generalized this statement to arbitrary number fields, as well as to abelian varieties. The results are now referred to as The Mordell-Weil Theorem. Since then, questions have been asked regarding the value of r, called the rank of $E(\mathbb{Q})$. Currently it is not known whether r can be arbitrarily large; and only elliptic curves with rank up to 28 have been found [Was08]. Another conjecture regarding the rank of an elliptic curve over $\mathbb{Q}$ is due to Bryan Birch and Peter Swinnerton-Dyer, who, nearly 40 years after Mordell and Weil, used computers to obtain data to support a conjecture that the rank of the group of points $E(\mathbb{Q})$ is related to the value of the zeta function of E at $s = 1$. This is known as the Birch and Swinnerton-Dyer conjecture, and is listed as one of the Millennium Prize Problems by the Clay Mathematics Institute.

Also around this time Mikio Sato and John Tate (independently) were exploring the behavior of the distribution of the number of points that lie on an elliptic curve when reduced mod p. Sato and Tate were working with the class of elliptic curves without complex multiplication; that is, the elliptic curves with $\mathrm{End}_{\overline{\mathbb{Q}}}(E) \cong \mathbb{Z}$. To begin consider an elliptic curve $E/\mathbb{Q}$ without complex multiplication, and then reduce E modulo p for primes of good reduction; for such p define $E_p \equiv E \mod p$. The resulting elliptic curve $E_p/\mathbb{F}_p$ is now an elliptic curve with a Frobenius endomorphism and a corresponding characteristic polynomial. Let θ_p be the angle of the roots of the characteristic polynomial of Frobenius of E_p. The Sato-Tate Conjecture then states that the Frobenius angle, θ_p, is distributed according to the function $\frac{2}{\pi}\sin^2(\theta)$. That is to say, the proportion of the number of primes $p < x$ such that the Frobenius angle θ_p falls within some range $0 \leq \alpha \leq \theta_p \leq \beta \leq \pi$ is asymptotically equal to $\frac{2}{\pi}\int_{\alpha}^{\beta} \sin^2(t)\,dt$. Recently, given the work of Barnet-Lamb, Geraghty, Harris, and Taylor, the Sato-Tate conjecture can now be proved for any elliptic curve defined over a totally real field [BLGHT11].

2.2.1. The Lang-Trotter Conjecture for Elliptic Curves. Following Sato and Tate, Serge Lang and Hale Trotter also chose to explore the properties of the elliptic curves without complex multiplication. Beginning in the same manner, take an elliptic curve $E/\mathbb{Q}$ with $\mathrm{End}_{\overline{\mathbb{Q}}}(E) \cong \mathbb{Z}$, then reduce $E \mod p \equiv E_p$ for the primes of good reduction. Let π_p be a root of the resulting characteristic polynomial of Frobenius. Now, rather than asking about the Frobenius angle, Lang and Trotter asked about the endomorphism structure of E_p. The following is known as the Lang-Trotter Conjecture.

Conjecture 2.2.1. *[[LT76]] Let E be an elliptic curve defined over $\mathbb{Q}$ without complex multiplication and let k be a given quadratic imaginary field. Define $N_{E,k}(x)$ to be the number* *of primes $p \leq x$ such that $\mathbb{Q}(\pi_p) \cong k$. Then there is a constant $C(E,k) > 0$ such that*

$$N_{E,k}(x) \approx C(E,k)\frac{\sqrt{x}}{\log(x)}.$$

The plausibility of this conjecture hinges on the following ideas. First, one can approximate the number of elliptic curves E defined over $\mathbb{F}_p$ with $\mathbb{Q}(\pi_p) \cong k$ to be on the order of $\sqrt{p}$. Second, there are approximately p elliptic curves defined over $\mathbb{F}_p$. Thus

$$\begin{aligned} N_{E,k}(x) &\approx \sum_{p \leq x} \text{Prob(random } E/\mathbb{F}_p \text{ has } \mathbb{Q}(\pi_p) \cong k) \\ &= \sum_{p \leq x} \frac{c\sqrt{p}}{p} = \sum_{p \leq x} \frac{c}{\sqrt{p}}. \end{aligned}$$

Now rather than sum over only the primes, sum over all integers. In order to do this, use the prime number theorem which informally states, that if a random integer is selected between zero and some large integer x, the probability that the selected integer is prime is about $\frac{1}{\log(x)}$. Thus, $N_{E,k}(x)$ can be approximated by

$$\sum_{n \leq x} \frac{c'}{\sqrt{n}\log(n)} \approx \int_2^x \frac{c'}{\sqrt{z}\log(z)}\,dz \approx \frac{C\sqrt{x}}{\log(x)}.$$

While a proof of the Lang-Trotter Conjecture may still be far off, recent work has been done to obtain upper bounds on $N_{E,k}(x)$. Some of the better results have been obtained through the use of various sieve techniques. One such upper bound is given by Cojocaru, Fouvry, and Murty, using a square sieve [CFM05]. For E an elliptic curve over $\mathbb{Q}$, without complex multiplication, and conductor n, then

$$N_{E,\mathbb{Q}(\sqrt{-D})}(x) \ll_n \frac{x(\log(\log(x)))^{13/12}}{(\log(x))^{25/24}}(1 + \#\{p : p \text{ is prime and } p|D\}).$$

Moreover, under the assumption of the Generalized Riemann Hypothesis this bound can be improved to

$$N_{E,\mathbb{Q}(\sqrt{-D})}(x) \ll_n x^{17/18} \log(x).$$

Since abelian surfaces are just higher dimensional analogues of elliptic curves, exploring some of these same questions as related to abelian surfaces seems like a natural progression. This paper will, in particular, pose a Lang-Trotter-like conjecture for abelian surfaces, as well as use a sieve calculation to justify the plausibility of this conjecture.

CHAPTER 3

Abelian Surfaces

3.1. Abelian Varieties

As with elliptic curves, an abelian variety V over a field k, admits regular morphisms which are group homomorphisms $\phi : V \to V$ called endomorphisms. The set of all such endomorphisms is denoted $\mathrm{End}(V)$, and like before let $\mathrm{End}^0(V) = \mathrm{End}(V) \otimes \mathbb{Q}$. An abelian variety is called *simple* if it is not isogenous to a product of abelian varieties of lower dimension. In the case of a simple abelian variety V, $\mathrm{End}^0(V)$ is a division algebra with maximal, totally real subfield, K^+. Also as before, one can define the group of $m-$torsion points $V[m](\overline{k})$. For an abelian variety V of dimension g over a finite field, $\mathbb{F}_p$, there is a number ρ, with $0 \leq \rho \leq g$, called the *$p-$rank* of V such that

$$V[p](\overline{\mathbb{F}_q}) \cong (\mathbb{Z}/p)^{\oplus \rho}.$$

The abelian variety is called *ordinary* if $\rho = g$. If two abelian varieties are isogenous, then they have the same $p-$rank. If $g \in \{1, 2\}$, and the $p-$rank is zero, then the abelian variety is *supersingular*; but in higher dimensions, this is false.

An abelian variety V of dimension g defined over a finite field $\mathbb{F}_q$, like an elliptic curve defined over $\mathbb{F}_q$, also admits a Frobenius endomorphism, Frob_q. By defining the $\ell-$adic Tate module of an abelian variety,

$$T_\ell(V) = \varprojlim_n V[\ell^n](\overline{k}),$$

endomorphisms of V can be represented by $2g \times 2g$ matrices by looking at their action on the $\ell-$adic Tate module. For the Frobenius endomorphism, Frob_q has matrix representation in $\mathrm{GL}_{2g}(\mathbb{Z}_\ell)$, and has corresponding characteristic polynomial with coefficients independent of the choice of ℓ. Furthermore if one chooses a polarization of the abelian variety defined over the base field, this polarization induces a symplectic form on the Tate module, and then the Frobenius endomorphism can be realized as an element of $\mathrm{GSp}_{2g}(\mathbb{Z}_\ell)$. A *polarization* of an abelian variety V is a choice of an ample line bundle $\mathcal{L}$ on V which induces an isogeny from V to its dual $V^\vee$. This isogeny gives rise to a skew symmetric pairing $\langle \cdot, \cdot \rangle$ for each $T_\ell(V)$. This is said to be *principal* if the isogeny is an isomorphism, or equivalently if $\langle \cdot, \cdot \rangle$ has determinant 1. For the remainder of this paper we will assume that V is a principally polarized abelian variety.

As before, given the matrix representation of the Frobenius endomorphism in $\mathrm{GSp}_{2g}(\mathbb{Z}/\ell)$, define the characteristic polynomial of Frobenius to be the characteristic polynomial of the corresponding matrix, denote this by $f_V(X)$. This characteristic polynomial will be of degree $2g$ with coefficients in $\mathbb{Z}$.

Given two abelian varieties, A and B a map between them that is a surjective homomorphism with finite kernel is called an *isogeny.* Isogeny defines an equivalence relation on abelian varieties. This is a more coarse equivalence than isomorphism.

Over finite fields Tate proved that isogeny classes of abelian varieties are determined by the characteristic polynomials of the Frobenius endomorphism. In fact, Tate proved the following:

THEOREM 3.1.1. *[[Tat66], Theorem 1.(c)] Let A and B be abelian varieties over a finite field k, and let f_A and f_B be the characteristic polynomials of their Frobenius endomorphisms relative to k. Then the following statements are equivalent:*

(1) A and B are $k-$isogenous.

(2) $f_A = f_B$.

(3) The zeta functions of A and B are the same.

(4) A and B have the same number of points in k' for every finite extension k' of k.

The zeta function of an abelian variety V over a finite field $\mathbb{F}_q$ is defined to be the series

$$Z(V,t) = \exp\left(\sum_{m\geq 1} \frac{N_m}{m} t^m\right), \text{ where } N_m = |V(\mathbb{F}_{q^m})|.$$

The zeta function of an abelian variety is a rational function. From the definition of the zeta function it is easy to see the equivalence of the last two statements in Tate's theorem. The two equivalences that will be relevant for this paper are (1) and (2).

3.2. Abelian Surfaces

At this point, we would like to turn our attention to abelian varieties of dimension 2, *abelian surfaces*. This will be the main focus for the remainder of this paper, so let us summarize the above for this particular case. An abelian surface A is *simple* if it not isogenous to a product of elliptic curves, $E_1 \times E_2$. Let A be a simple, ordinary, principally polarized abelian surface defined over $\mathbb{F}_q$, then $\mathrm{End}^0(A)$ is a totally imaginary degree 4 extension of $\mathbb{Q}$, and K^+ is its unique, maximal, totally real quadratic subfield. If $K^+ \subset \mathrm{End}^0(A)$, we say that A has *real multiplication, (RM)* by K^+. The endomorphism Frob_q can be realized as a matrix in $\mathrm{GSp}_4(\mathbb{Z}_\ell)$, with characteristic polynomial

$$f_A(X) = X^4 - aX^3 + bX^2 - aqX + q^2,$$

where the coefficients are integers, independent of ℓ. The roots of $f_A(X)$ come in complex conjugate pairs and are of size $\sqrt{q}$; this enforces the following inequalities on the coefficients

a and b:

$$(3.1) \qquad |a| \leq 4\sqrt{q} \qquad \text{and} \qquad 2|a|\sqrt{q} - 2q \leq b \leq \frac{a^2}{4} + 2q.$$

A polynomial satisfying such conditions is called a *q-Weil Polynomial*, and is called *ordinary* if b is relatively prime to p, this condition is compatible with the earlier definition of ordinary. Finally, the coefficients a and b determine the real quadratic field inside $\mathrm{End}^0(A)$, in the sense that the discriminant of the real quadratic subfield inside $\mathrm{End}^0(A)$ is equivalent to $\Delta_A^+ = a^2 - 4b + 8q$ modulo squares. It follows that A has real multiplication by a fixed $K^+ = \mathbb{Q}(\sqrt{d})$ if and only if $\Delta_A^+ = a^2 - 4b + 8q = r^2 d$ for some $r \in \mathbb{Z}$.

Since the characteristic polynomial determines the isogeny class, an interesting question to ask would be how many abelian surfaces are there defined over $\mathbb{F}_q$ such that the Frobenius endomorphism yields a particular characteristic polynomial? Furthermore since the coefficients of the characteristic polynomial of the Frobenius endomorphism can be used to determine the real quadratic subfield sitting inside the division algebra $\mathrm{End}^0(A)$, another question might be how many abelian surfaces are there defined over $\mathbb{F}_q$ such that a particular real quadratic subfield sits inside $\mathrm{End}^0(A)$? Equivalently, how many abelian surfaces defined over $\mathbb{F}_q$ are there such that A has real multiplication by a fixed real quadratic field K^+?

The next part of this paper seeks to answer such a question. To do so, two things must be done: (i) determine the number of isogeny classes of principally polarized abelian surfaces over $\mathbb{F}_q$ with real multiplication by K^+ and, (ii) determine the size of each such isogeny class. Once this question is answered, we look at how this result can be used to pose a Lang-Trotter-like conjecture for abelian surfaces, and then use a large sieve calculation to support the conjecture.

Throughout the remainder of this paper let $\mathbb{F}_q$ be the field of size q of characteristic p. Let A be a principally polarized abelian surface (PPAS) defined over $\mathbb{F}_q$. Let $\mathrm{End}(A)$ denote the endomorphism ring of A, and $\mathrm{End}^0(A)$ denote the division algebra $\mathrm{End}(A) \otimes \mathbb{Q}$. Let $f_A(X)$ be the characteristic polynomial of the Frobenius endomorphism of A. Also set $K^+ = \mathbb{Q}(\sqrt{d})$, a real quadratic extension of $\mathbb{Q}$ with discriminant d, and say that an abelian surface A has real multiplication by K^+ if $K^+ \subset \mathrm{End}^0(A)$.

CHAPTER 4

A Counting Theorem: The Number of Abelian Surfaces with Real Multiplication

In this chapter our goal is to prove the following theorem.

Theorem 4.0.1. *Fix $d \in \mathbb{Z}$ positive and square free, and suppose that p is inert in $K^+ = \mathbb{Q}(\sqrt{d})$. Let $q = p^s$, and define $\mathscr{A}_{q,d}$ be the set of principally polarized abelian surfaces, A, defined over $\mathbb{F}_q$ such that A has real multiplication by K^+. Then for any $\epsilon > 0$ there exist constants $C_<(\epsilon)$ and $C_>(\epsilon)$ such that*

$$C_<(\epsilon)\frac{q^{5/2-\epsilon}}{\sqrt{d}} < \#\mathscr{A}_{q,d} < C_>(\epsilon)\frac{q^{5/2+\epsilon}}{\sqrt{d}}.$$

To prove this theorem we first seek to obtain bounds on the size of an isogeny class of abelian surfaces. This will be done via a theorem of Everett Howe. Second, we will need to determine which isogeny classes (equiv. characteristic polynomials of Frobenius) correspond to abelian surfaces with real multiplication by K^+. This will be done by assessing which characteristic polynomial coefficients a and b satisfy $a^2 - 4b + 8q = r^2 d$. Together these results will prove Theorem 4.0.1.

4.1. The Size of a Simple Ordinary Isogeny Class

4.1.1. The Class Group and The Picard Group. Much of the material in this section can be found in [Neu99]. Let F be a number field, $\mathcal{O}$ be an order in F, and $\mathcal{O}_F$ be the maximal order. Recall the definition of an order following Proposition 2.1.1, and write $\mathcal{O} = \oplus_{i=1}^{n}\mathbb{Z}a_i$ for $a_i \in \mathcal{O}$. Given the a_i basis for $\mathcal{O}$, define the *discriminant* of $\mathcal{O}$

to be $\Delta(\mathcal{O}) = \det(\mathrm{Tr}_{\mathcal{O}/\mathbb{Z}}(a_i a_j))_{i,j=1}^n$. With this definition for the discriminant one gets the following relation:

Lemma 4.1.1. *For any orders $\mathcal{O} \subseteq \mathcal{O}'$ in a number field F, we have that*

$$\Delta(\mathcal{O}) = [\mathcal{O}' : \mathcal{O}]^2 \Delta(\mathcal{O}').$$

The discriminant of an order will be used frequently in this section, and we will use the notation $\Delta(\mathcal{O}_F) = \Delta(F)$ to mean the discriminant of the field F.

For any order $\mathcal{O}$ one can define the set of invertible ideals, i.e. the fractional ideals $\mathfrak{a}$ of $\mathcal{O}$ for which there exists a fractional ideal $\mathfrak{b}$ such that $\mathfrak{a}\mathfrak{b} = \mathcal{O}$. Denote this set of invertible ideals of $\mathcal{O}$ by $J(\mathcal{O})$. Inside $J(\mathcal{O})$ is the set $P(\mathcal{O})$, the set of fractional principal ideals $a\mathcal{O}$ for $a \in F^*$. In fact, each $J(\mathcal{O})$ and $P(\mathcal{O})$ is a group. Define the Picard group of the order $\mathcal{O}$ to be the quotient group $\mathrm{Pic}(\mathcal{O}) = J(\mathcal{O})/P(\mathcal{O})$. In the case where $\mathcal{O} = \mathcal{O}_F$, the Picard group is the ideal class group of F. Let $h(\mathcal{O}) = \#\mathrm{Pic}(\mathcal{O})$, for an order $\mathcal{O}$ in F, and let $h_F = h(\mathcal{O}_F)$ denote the class number of F.

Let us now review some results regarding the class number and the Picard group.

Theorem 4.1.1 ([Neu99], Theorem I.6.3). *The ideal class group $\mathcal{CL}_F = J(\mathcal{O}_F)/P(\mathcal{O}_F)$ is finite. Its order*

$$h_F = [J(\mathcal{O}_F) : P(\mathcal{O}_F)]$$

is called the class number *of F.*

Typically the class number is interpreted as measuring the failure of unique factorization in the ring of integers $\mathcal{O}_F$. In fact, $\mathcal{O}_F$ is a unique factorization domain if and only if $h_F = 1$.

While the class group itself can be difficult to compute, there is an analytic formula that can be used to calculate the class number directly. It depends on the following invariants of the field F: the regulator, R_F; the number of roots of unity, ω_F, of $\mathcal{O}_F^*$; the signature (r_1, r_2) where r_1 is the number of real embeddings $F \to \mathbb{R}$ and r_2 is the number of pairs of complex embeddings $F \to \mathbb{C}$, and $r_1 + 2r_2 = n = [F : \mathbb{Q}]$; the discriminant, $\Delta(F)$; and finally $\zeta_F(s)$, the Dedekind zeta function of F.

Theorem 4.1.2. *(The Analytic Class Number Formula, [Neu99], Chapter VII) Given the field invariants above the following formula can be used to determine the class number of the number field F:*

$$\lim_{s \to 1^+} (s-1)\zeta_F(s) = \frac{2^{r_1}(2\pi)^{r_2} h_F R_F}{\omega_F \sqrt{\Delta(F)}}.$$

Let the residue of $\zeta_F(s)$ at $s = 1$ be denoted by

$$\kappa_F = \lim_{s \to 1^+} (s-1)\zeta_F(s).$$

Then

$$h_F = \frac{\kappa_F \omega_F \sqrt{\Delta(F)}}{2^{r_1}(2\pi)^{r_2} R_F}. \tag{4.1}$$

Now for a general order $\mathcal{O}$, define the ideal $\mathfrak{f} = \{a \in \mathcal{O}_F : a\mathcal{O}_F \subseteq \mathcal{O}\}$ to be the *conductor* of $\mathcal{O}$. This ideal is by definition the largest ideal shared by both $\mathcal{O}$ and $\mathcal{O}_F$. Given the conductor one obtains the following formula for the size of the Picard group.

Theorem 4.1.3 ([Neu99], Theorem I.12.12). *Let $\mathcal{O}$ be an order in an algebraic number field F, $\mathcal{O}_F$ the maximal order, and $\mathfrak{f}$ the conductor of $\mathcal{O}$. Then the groups $\mathcal{O}_F^*/\mathcal{O}^*$ and*

$Pic(\mathcal{O})$ are finite and one has

$$h(\mathcal{O}) = \#Pic(\mathcal{O}) = \frac{h_F}{[\mathcal{O}_F^* : \mathcal{O}^*]} \frac{\#(\mathcal{O}_F/\mathfrak{f})^*}{\#(\mathcal{O}/\mathfrak{f})^*}. \tag{4.2}$$

This theorem gives a useful relation between $h(\mathcal{O})$ and h_F and will be used later to compute the size of an isogeny class.

4.1.2. Simple, Ordinary Abelian Surfaces. In this section we discuss what it means for an abelian surface A to have real multiplication by a field K^+ when A is simple or not, and when A is ordinary or not. We will begin with simplicity. Recall that an abelian surface is simple if it is not isogenous to the product of elliptic curves $E_1 \times E_2$.

Lemma 4.1.2. *If A has real multiplication by $K^+ = \mathbb{Q}(\sqrt{d})$ then either,*

(1) A is simple, or

(2) $A \sim E \times E$.

Proof. Suppose that A is not simple, so that we can write $A \sim E_1 \times E_2$. We make the following observations: (i) by Proposition 2.1.1 we know that for each E_i, $\mathrm{End}^0(E_i)$ is either $\mathbb{Z}$, an order in a quadratic imaginary extension of $\mathbb{Q}$ or an order in a quaternion algebra, which means that $K^+ \not\subseteq \mathrm{End}^0(E_i)$; (ii) for two abelian surfaces (in fact, abelian varieties) if $A \not\sim B$, then

$$\mathrm{End}^0(A \times B) \cong \mathrm{End}^0(A) \times \mathrm{End}^0(B), \qquad \text{and;}$$

(iii) if $A \sim B$ then

$$\mathrm{End}^0(A \times B) \cong \mathrm{Mat}_2\left(\mathrm{End}^0(A)\right).$$

Given these observations we can conclude that if $A \sim E_1 \times E_2$ is not simple, then if $E_1 \not\sim E_2$, by observations (i) and (ii) A cannot have real multiplication by K^+. It follows that if A is not simple but has real multiplication by K^+, then $A \sim E \times E$ for some elliptic curve E. □

Corollary 1. *If A is not simple, then A has real multiplication by any real quadratic extension of $\mathbb{Q}$.*

Proof. Since $A \sim E \times E$, then and K^+ can be embedded into $\mathrm{Mat}_2(\mathbb{Q})$ via the usual, regular representation; and $\mathrm{Mat}_2(\mathbb{Q})$ always sits inside $\mathrm{End}^0(E \times E)$. □

Also note here that when $A \sim E \times E$, then

$$f_A(X) = f_E(X)^2 = (X^2 - aX + q)^2 = X^4 - 2aT^3 + (2q + a^2)T^2 - 2aqT + q^2, \quad \text{and}$$

$$\Delta_A^+ = (2a)^2 - 4(2q + a^2) + 8q = 4a^2 - 8q - 4a^2 + 8q = 0.$$

Thus if one chooses $r = 0$ then $\Delta_A^+ = r^2 d$ for any d if A is not simple.

Next we discuss ordinarily. Recall the $p-$rank ρ of an abelian surface. This can be read off from the coefficients of the q-Weil polynomial $f_A(X)$ of A. This is done by defining the *Newton Polygon* of $f_A(X) = \sum_{0 \leq i \leq 2g} c_i X^i$, where $q = p^j$. In the Cartesian plane, plot the pairs

$$\{(i, \frac{1}{r}\mathrm{ord}_p(c_i)) \ : \ 0 \leq i \leq 2g\},$$

where $\mathrm{ord}_p(c)$ means the power of p dividing c, and is set to be ∞ if $c = 0$. Given these points, form the convex hull. The $p-$rank of A can then be read off by counting the number of line segments of slope zero of the Newton Polygon of $f_A(T)$. This in turn tells us that the $p-$rank is 2 if $p \nmid b$; 1 if $p \nmid a$, but $p|b$; and 0 if $p|a$ and $p|b$. Note that for an abelian surface, $p-$rank 2 is equivalent to ordinary, and $p-$rank 0 is equivalent to supersingular. As for the

$p-$rank 1 case, we deal with this based on the simplicity of A. First if we assume that A is not simple and has real multiplication by $K+$ then by Lemma 4.1.2, $A \sim E^2$. From here we can say that

$$A[p](\overline{k}) \cong (E \times E)\,[p](\overline{k}) \cong E[p](\overline{k}) \times E[p](\overline{k}).$$

The $p-$rank of E is either 0 or 1, this implies that the $p-$rank of A is either $0+0=0$, or $1+1=2$. It follows that if A is not simple then A is either ordinary or supersingular.

It turns out that under a small hypothesis, we can say that any A with real multiplication is either ordinary or supersingular.

Lemma 4.1.3. *Suppose that p is inert in K^+. If $A/\mathbb{F}_q$ is an abelian surface with real multiplication by K^+, then the $p-$rank of A is not* 1.

Proof. Recall an abelian surface A has real multiplication by K^+ if $\Delta_A^+ = a^2 - 4b + 8q = r^2 d$. Suppose $p|b$, then

$$a^2 - 4b + 8q \equiv r^2 d \mod p$$

$$a^2 \equiv r^2 d \mod p.$$

But, since p is inert in K^+, (equiv. $d \not\equiv \square \mod p$), the only solution to this equivalence is $r \equiv a \equiv 0 \mod p$. This means that if $p|b$, then $p|a$. Conversely, if $p \nmid a$ then $p \nmid b$ and we are forced into the ordinary case. Thus $p-$rank 1 cannot happen. □

In the sections that follow we will consider both simple and non-simple, ordinary and supersingular abelian surfaces.

4.1.3. A Theorem of Howe. Let $f(X)$ be an irreducible, ordinary, $q-$Weil polynomial, with π a root of $f(X)$, and $\overline{\pi} = q/\pi$. By Tate's result from Theorem 3.1.1, $f(X)$

determines an isogeny class of abelian varieties over $\mathbb{F}_q$. Let $K = \mathbb{Q}[X]/f(X)$, and let $\mathcal{O}_K$ be the maximal order of K. Then $\mathbb{Z}[\pi] \subset \mathbb{Z}[\pi, \overline{\pi}] \subseteq \mathcal{O}_K$. Now, given any order, $\mathcal{O}$ containing π and $\overline{\pi}$, then $\mathcal{O} \cong \mathrm{End}(A)$ for some A in the isogeny class of $f(X)$ [Wat69].

Let K^+ be the maximal totally real subfield of K, and for any order $\mathcal{O}$ of K let $\mathcal{O}^+ = \mathcal{O} \cap K^+$. Then if $\mathbb{Z}[\pi, \overline{\pi}] \subseteq \mathcal{O}$, we have $\mathbb{Z}[\pi + \overline{\pi}] \subseteq \mathcal{O}^+$.

Given notation as above we state the following due to Everett Howe.

Theorem 4.1.4. *[[How00]] Let $f(X)$ be an irreducible, ordinary, $q-$Weil polynomial and define $K = \mathbb{Q}[X]/f(X)$, which is an imaginary field of degree $2g$ over $\mathbb{Q}$ with maximal totally real subfield K^+. Let π be a root of $f(X)$ and let $\mathcal{O}$ be an order in K containing π and $\overline{\pi}$. Then the set of isomorphism classes of principally polarized abelian varieties defined over $\mathbb{F}_q$, of dimension g, with End$(A) = \mathcal{O}$ has cardinality $h(\mathcal{O})/h(\mathcal{O}^+)$.*

For our purposes we wish to use this result to compute (or at least bound) the size of an isogeny class of simple, ordinary, principally polarized abelian surfaces corresponding to the characteristic polynomial of Frobenius, $f(X)$. Let the pair (A, λ) be an abelian surface, A, along with a principal polarization, λ. Recall the characteristic polynomial of Frobenius of A is $f_A(X)$. Then we may count the size of the isogeny class corresponding to a particular irreducible, ordinary $q-$Weil polynomial $f(X)$ as follows, where $\bigsqcup$ represents a disjoint union:

$$\begin{aligned}\#\{(A,\lambda)/\mathbb{F}_q \,:\, f_A(X) = f(X)\} &= \#\left(\bigsqcup_{\mathbb{Z}[\pi,\overline{\pi}]\subseteq\mathcal{O}} \{(A,\lambda)/\mathbb{F}_q \,:\, \mathrm{End}(A) \cong \mathcal{O}\}\right)\\ &= \sum_{\mathbb{Z}[\pi,\overline{\pi}]\subseteq\mathcal{O}} \#\{(A,\lambda)/\mathbb{F}_q \,:\, \mathrm{End}(A) \cong \mathcal{O}\}\\ &= \sum_{\mathbb{Z}[\pi,\overline{\pi}]\subseteq\mathcal{O}} h(\mathcal{O})/h(\mathcal{O}^+) \qquad \text{by Theorem 4.1.4.} \end{aligned} \tag{4.3}$$

Thus to compute the size of such an isogeny class we must assess the ratio $h(\mathcal{O})/h(\mathcal{O}^+)$. Since $h(\mathcal{O})$ is related to h_K, we will begin by assessing the ratio of the class numbers, h_K/h_{K^+}.

4.1.4. Bounding the Ratio of Class Numbers. In this section we specialize to the case $g = 2$, so that Howe's theorem counts the number of isomorphism classes of simple, ordinary, principally polarized abelian surfaces. In this instance K is a degree 4 extension of $\mathbb{Q}$, K^+ is a totally real quadratic field (and unique), and the characteristic polynomial $f(X)$ is degree 4.

The arguments made in this section will prove the following theorem.

Theorem 4.1.5. *For any $\varepsilon' > 0$, then there exist constants $C_<(\varepsilon')$ and $C_>(\varepsilon')$ such that*

$$C_<(\varepsilon')q^{-\varepsilon'}\sqrt{\frac{\Delta(K)}{\Delta(K^+)}} < \frac{h_k}{h_{K^+}} < C_>(\varepsilon')q^{\varepsilon'}\sqrt{\frac{\Delta(K)}{\Delta(K^+)}}.$$

To begin, consider the field invariants used in the analytic class number formula, equation (4.1). For K, the totally imaginary degree 4 extension of $\mathbb{Q}$, we have: $r_1 = 0$ and $r_2 = 2$, whereas for the totally real quadratic subfield K^+, we have $r_1^+ = 2$ and $r_2^+ = 0$.

Making these substitutions into the class number formula, consider the ratio of the class numbers:

$$\begin{aligned}\frac{h_K}{h_{K^+}} &= \frac{\dfrac{\kappa_K \omega_K \sqrt{\Delta(K)}}{2^0(2\pi)^2 R_K}}{\dfrac{\kappa_{K^+}\omega_{K^+}\sqrt{\Delta(K^+)}}{2^2(2\pi)^0 R_{K^+}}} \\ &= \frac{\kappa_K \omega_K R_{K^+}}{\pi^2 \kappa_{K^+}\omega_{K^+} R_K}\sqrt{\frac{\Delta(K)}{\Delta(K^+)}}. \end{aligned} \tag{4.4}$$

As suggested by the statement of Theorem 4.1.5, our goal is to ultimately get a bound for the ratio of the class numbers in terms of the field discriminants, $\Delta(K)$ and $\Delta(K^+)$. The following lemmas show that the ratios of the regulators and the number of roots of unity can be bounded by constants, while the ratio of the residues can be bounded in terms of the field discriminants.

We begin with the ratio of the regulators R_{K^+}/R_K.

Theorem 4.1.6 ([Was97], Theorem 4.12). *Let K be a totally imaginary number field of degree $2g$ over $\mathbb{Q}$ and let $E = \mathcal{O}_K^*$ be its unit group. Let $E^+ = \mathcal{O}_{K^+}^*$ be the unit group of K^+ and let $\mu(\mathcal{O}_K)$ be the group of roots of unity of K. Then*

$$Q := [E : \mu(\mathcal{O}_K)E^+] = 1 \text{ or } 2.$$

Theorem 4.1.7 ([Was97], Proposition 4.16). *Let K be as above and let K^+ be its maximal real subfield. Then*

$$\frac{R_K}{R_{K^+}} = \frac{1}{Q}2^{(r_2-1)}.$$

Lemma 4.1.4. *Let notation be as above, then*

$$1/2 \leq R_{K^+}/R_K \leq 1.$$

Proof. This follows immediately from Theorem 4.1.6 and Theorem 4.1.7. □

Next we assess the ratio of the number of roots of unity. Recall that for a field F we denote the number roots of unity of F by ω_F.

Lemma 4.1.5. *Let K be a degree 4 totally imaginary extension of $\mathbb{Q}$ with maximal real subfield K^+, then*

$$1 \leq \omega_K/\omega_{K^+} \leq 12.$$

Proof. Since K^+ is a totally real quadratic field, the only units are ± 1, so $\omega_{K^+} = 2$. As for ω_K, let $\mathbb{Q}(\zeta_n)$ be the maximal cyclotomic field contained in K. This is unique, and contains all the roots of unity contained in K. Notice that $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{2n})$ when n is odd, so assume n is odd, or divisible by 4. Let $\varphi(n)$ denote the Euler totient function, which counts the number of positive integers less than or equal to n that are relatively prime to n. Now we have the following tower of extensions $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_n) \subseteq K$, which implies that the index $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$ divides the index $[K : \mathbb{Q}] = 4$, i.e. $\varphi(n)|4$. Together, the facts $\varphi(n)|4$ and n is odd or is divisible by 4 tells us that $n = 1$, 3, 4, 5, 8, or 12. So, the largest ω_K can be is 24 when $\mathbb{Q}(\zeta_{12}) = K$, and the set of roots of unity are $\{\pm\zeta_{12}^i\}_{i=0}^{11}$; whereas the smallest ω_K can be is 2, when $n = 1$, and the only roots of unity in K are ± 1. Thus, $1 \leq \omega_K/\omega_{K^+} \leq 12$. □

Finally let us turn our attention to the ratio of the residues.

Theorem 4.1.8. *For any $\varepsilon > 0$ there exist constants $C_1(\varepsilon)$ and $C_1'(\varepsilon)$ such that*

$$C_1(\varepsilon)\left(\frac{1}{\Delta(K)\Delta(K^+)}\right)^{\varepsilon} < \frac{\kappa_K}{\kappa_{K^+}} < C_1'(\varepsilon)\left(\Delta(K)\Delta(K^+)\right)^{\varepsilon}.$$

First consider the following two theorems:

Theorem 4.1.9 ([CK13]). *Let $\varepsilon > 0$. There exists a number $c(\varepsilon)$ such that for all fields F of degree N over $\mathbb{Q}$, the inequality holds:*

$$\kappa(F) \geq c(\varepsilon)^{-N}\Delta(F)^{-\varepsilon}.$$

Theorem 4.1.10 ([Lou01], Theorem 1). *Let F be a number field of degree $N > 1$. Set* $e = \exp(1)$. *It holds*

$$\kappa(F) \leq \left(\frac{e \log(\Delta(F))}{2(N-1)} \right)^{N-1}.$$

Proof of Theorem 4.1.8. Applying the two theorems above to each of κ_K and κ_{K^+} we get the following bounds given any $\varepsilon, \varepsilon^+ > 0$:

$$c(\varepsilon)^{-4}\Delta(K)^{-\varepsilon} < \kappa_K < \left(\frac{e \log(\Delta(K))}{2(3)} \right)^3$$
$$c(\varepsilon^+)^{-2}\Delta(K^+)^{-\varepsilon^+} < \kappa_{K^+} < \left(\frac{e \log(\Delta(K^+))}{2} \right)$$

These in turn give bounds for their ratio, so that for any $\varepsilon > 0$,

$$\frac{2}{c(\varepsilon)^4\Delta(K)^\varepsilon e \log(\Delta(K^+))} < \frac{\kappa_K}{\kappa_{K^+}} < \frac{e^3 \log^3(\Delta(K))c(\varepsilon)^2\Delta(K^+)^\varepsilon}{216}.$$

Lemma 4.1.6. *For all $\delta > 0$, let $C_\delta = \frac{1}{e \cdot \delta}$. Then for all $x > 0$,*

$$\log(x) < C_\delta x^\delta.$$

Proof. Consider the function $g(x) = \frac{\log(x)}{x^\delta}$. Then calculus can be used to show that $g(x)$ has a maximum at $x = e^{1/\delta}$, and $g(e^{1/\delta}) = \frac{1}{e \cdot \delta}$. Thus for all $x > 0$, we have $\frac{\log(x)}{x^\delta} \leq \frac{1}{e \cdot \delta}$, which means $\log(x) \leq \frac{1}{e \cdot \delta}x^\delta$. □

Using this lemma, for any δ, $\delta^+ > 0$ we may extend the upper and lower bounds:

$$\frac{2}{c(\varepsilon)^4 e\Delta(K)^\varepsilon C_{\delta^+}\Delta(K^+)^{\delta^+}} < \frac{\kappa_K}{\kappa_{K^+}} < \frac{c(\varepsilon)^2 e^3 C_\delta \Delta(K)^\delta \Delta(K^+)^\varepsilon}{216}.$$

To summarize we may say for all $\varepsilon = \delta^+ = \delta > 0$ there exist constants $C_1(\varepsilon)$ and $C_1'(\varepsilon)$ such that

$$C_1(\varepsilon)\left(\frac{1}{\Delta(K)\Delta(K^+)}\right)^{\varepsilon} < \frac{\kappa_K}{\kappa_{K^+}} < C_1'(\varepsilon)\left(\Delta(K)\Delta(K^+)\right)^{\varepsilon}.$$

□

Now that we have bounds for the ratio of the residues, the ratio of the regulators and the ratio of the number of roots of unity we obtain the following (initial) bounds for the ratio of the class numbers. For all $\varepsilon > 0$ there exist constants $C_2(\varepsilon)$ and $C_2'(\varepsilon)$ such that

$$C_2(\varepsilon)\left(\frac{1}{\Delta(K)\Delta(K^+)}\right)^{\varepsilon}\sqrt{\frac{\Delta(K)}{\Delta(K^+)}} < \frac{h_K}{h_{K^+}} < C_2'(\varepsilon)\left(\Delta(K)\Delta(K^+)\right)^{\varepsilon}\sqrt{\frac{\Delta(K)}{\Delta(K^+)}}. \tag{4.5}$$

In terms of Theorem 4.1.4, equation (4.5) tells us that the number of simple, ordinary, principally polarized abelian varieties over $\mathbb{F}_q$ with $\mathrm{End}(A) \cong \mathcal{O}_K$ can be bound in terms of the field discriminants, $\Delta(K)$ and $\Delta(K^+)$. Furthermore, because of the relationship between the class number and the size of the Picard group from equation (4.2), we will see that the ratio of $h(\mathcal{O})/h(\mathcal{O}^+)$ can be bound in terms of the discriminants, $\Delta(\mathcal{O})$ and $\Delta(\mathcal{O}^+)$.

We now have enough to prove Theorem 4.1.5.

Proof of Theorem 4.1.5. The final step is to assess the field discriminants, $\Delta(K)$ and $\Delta(K^+)$.

Consider K, where we have the orders $\mathbb{Z}[\pi] \subset \mathbb{Z}[\pi, \overline{\pi}] \subseteq \mathcal{O}_K$. Note that $\mathbb{Z}[\pi] \cong \mathbb{Z}[X]/f(X)$, so that $\Delta(\mathbb{Z}[\pi]) = \Delta(f)$.

Lemma 4.1.7. *[[AW14]] For $f(X)$, an ordinary $q-$Weil polynomial with roots π and $\overline{\pi} = q/\pi$, we have*

$$[\mathbb{Z}[\pi, \overline{\pi}] : \mathbb{Z}[\pi]] = q.$$

Using Lemma 4.1.1 and Lemma 4.1.7 we can write

$$\Delta(\mathbb{Z}[\pi, \overline{\pi}]) = \frac{\Delta(\mathbb{Z}[\pi])}{[\mathbb{Z}[\pi, \overline{\pi}] : \mathbb{Z}[\pi]]^2} = \frac{\Delta(f)}{q^2} \tag{4.6}$$

and

$$\Delta(K) = \Delta(\mathcal{O}_K) = \frac{\Delta(\mathbb{Z}[\pi, \overline{\pi}])}{[\mathcal{O}_K : \mathbb{Z}[\pi, \overline{\pi}]]^2} = \frac{\Delta(f)}{q^2\,[\mathcal{O}_K : \mathbb{Z}[\pi, \overline{\pi}]]^2}. \tag{4.7}$$

Recall $f(X) = X^4 - aX^3 + bX^2 - aqX + q^2$, thus $\Delta(f) = q^2(a^2 - 4b + 8q)^2(b^2 + 4bq + 4q^2 - 4a^2q)$, so that

$$\Delta(K) = \frac{(a^2 - 4b + 8q)^2(b^2 + 4bq + 4q^2 - 4a^2q)}{[\mathcal{O}_K : \mathbb{Z}[\pi, \overline{\pi}]]^2}. \tag{4.8}$$

As for $\Delta(K^+)$, by Lemma 4.1.1 we have $\Delta(\mathbb{Z}[\pi + \overline{\pi}]) = [\mathcal{O}_{K^+} : \mathbb{Z}[\pi + \overline{\pi}]]^2\Delta(K^+)$. Then recall that $\mathbb{Z}[\pi + \overline{\pi}] = \mathbb{Z}[X]/f^+(X)$ for $f^+(X) = X^2 - aX + b - 2q$, so that $\Delta(\mathbb{Z}[\pi + \overline{\pi}]) = \Delta(f^+) = a^2 - 4b + 8q$. Thus,

$$\Delta(K^+) = \frac{a^2 - 4b + 8q}{[\mathcal{O}_{K^+} : \mathbb{Z}[\pi + \overline{\pi}]]^2}. \tag{4.9}$$

Together equations (4.8) and (4.9) show that

$$\Delta(K)\Delta(K^+) = \frac{(a^2 - 4b + 8q)^3(b^2 + 4bq + 4q^2 - 4a^2q)}{[\mathcal{O}_K : \mathbb{Z}[\pi, \overline{\pi}]]^2[\mathcal{O}_{K^+} : \mathbb{Z}[\pi + \overline{\pi}]]^2}. \tag{4.10}$$

Furthermore, since each index above is positive and the numerator has order q^5, there exists some constant c such that expression (4.10) can be bound above by cq^5. Using cq^5 as an upper bound on $\Delta(K)\Delta(K^+)$ we get the following bounds for any $\varepsilon > 0$

$$C_3(\varepsilon)\sqrt{\frac{\Delta(K)}{\Delta(K^+)}}\left(\frac{1}{q^5}\right)^{\varepsilon} < \frac{h_K}{h_{K^+}} < C_3'(\varepsilon)\sqrt{\frac{\Delta(K)}{\Delta(K^+)}}\left(q^5\right)^{\varepsilon}. \tag{4.11}$$

To summarize we can say that for all $\varepsilon' > 0$ there exist constants $C_<(\varepsilon')$ and $C_>(\varepsilon')$ such that

$$C_<(\varepsilon')q^{-\varepsilon'}\sqrt{\frac{\Delta(K)}{\Delta(K^+)}} < \frac{h_K}{h_{K^+}} < C_>(\varepsilon')q^{\varepsilon'}\sqrt{\frac{\Delta(K)}{\Delta(K^+)}}.$$

□

4.1.5. Bounding the Ratio of the Size of Picard Groups. Recall the formula for the Picard group of $\mathcal{O}$ given in equation (4.2). Using this formula for each $h(\mathcal{O})$ and $h(\mathcal{O}^+)$, take their ratio

$$\begin{aligned}\frac{h(\mathcal{O})}{h(\mathcal{O}^+)} &= \frac{\dfrac{h_K}{[\mathcal{O}_K^* : \mathcal{O}^*]}\dfrac{\#(\mathcal{O}_K/\mathfrak{f})^*}{\#(\mathcal{O}/\mathfrak{f})^*}}{\dfrac{h_{K^+}}{[\mathcal{O}_{K^+}^* : \mathcal{O}^{+*}]}\dfrac{\#(\mathcal{O}_{K^+}/\mathfrak{f}^+)^*}{\#(\mathcal{O}^+/\mathfrak{f}^+)^*}} \\ &= \frac{h_K}{h_{K^+}}\frac{[\mathcal{O}_{K^+}^* : \mathcal{O}^{+*}]}{[\mathcal{O}_K^* : \mathcal{O}^*]}\frac{\#(\mathcal{O}_K/\mathfrak{f})^*}{\#(\mathcal{O}/\mathfrak{f})^*}\frac{\#(\mathcal{O}^+/\mathfrak{f}^+)^*}{\#(\mathcal{O}_{K^+}/\mathfrak{f}^+)^*}. \end{aligned} \tag{4.12}$$

Theorem 4.1.11. *Let us have notation as above. Then for any $\epsilon > 0$ there exists constants $C'_<(\epsilon)$ and $C'_>(\epsilon)$ such that*

$$C'_<(\epsilon)q^{-\epsilon}\sqrt{\frac{\Delta(\mathcal{O})}{\Delta(\mathcal{O}^+)}} < \frac{h(\mathcal{O})}{h(\mathcal{O}^+)} < C'_>(\epsilon)q^{\epsilon}\sqrt{\frac{\Delta(\mathcal{O})}{\Delta(\mathcal{O}^+)}}.$$

Proof. This proof comes in 4 parts, one for each of the ratios in the definition of the ratio $h(\mathcal{O})/h(\mathcal{O}^+)$.

(1) $h(K)/h(K^+)$: In the previous section Theorem 4.1.5 gives bounds for the ratio of the class numbers.

(2) $\left[\mathcal{O}_{K^+}^* : \mathcal{O}^{+*}\right] / [\mathcal{O}_K^* : \mathcal{O}^*]$: Next let us turn our attention to the ratio of the indices of the unit groups. We start with the following theorem of Dirichlet which tells us that the unit group of the ring of integers has a very specific structure.

Theorem 4.1.12 (Dirichlet's Unit Theorem, [Neu99], Theorem I.7.4). *Let F be a number field of degree n with r_1 real and $2r_2$ complex embeddings and let $r = r_1 + r_2 - 1$. Then the group of units $\mathcal{O}_F^*$ of $\mathcal{O}_F$ is of the form*

$$\mathcal{O}_F^* \cong \mu(\mathcal{O}_F) \times \mathbb{Z}^r$$

where $\mu(\mathcal{O}_F)$ is the group of roots of unity of $\mathcal{O}_F^*$.

Call the value r in the theorem above the *rank* of the group of units. This means there are r units u_i called *fundamental units* so that any unit $u \in \mathcal{O}_F^*$ can be written as

$$u = \zeta u_1^{n_1} u_2^{n_2} \cdots u_r^{n_r}$$

with ζ a root of unity. We now apply this theorem to the cases when $F = K$ is a totally imaginary degree 4 extension of $\mathbb{Q}$ and $F = K^+$ a totally real quadratic extension of $\mathbb{Q}$, in order to determine bounds for the ratio of the indices of unit groups.

Theorem 4.1.13. *Let $\mathcal{O}_K^*$ be the group of units of K, $\mathcal{O}_{K^+}^*$ be the group of units of K^+, and let $\mathcal{O}^*$ and $\mathcal{O}^{+*}$ be the group of units of general orders in K and K^+ respectively. Then*

$$\frac{1}{24} \leq \frac{[\mathcal{O}_{K^+}* : \mathcal{O}^{+*}]}{[\mathcal{O}_K^* : \mathcal{O}^*]} \leq 1.$$

Proof. Consider K, a totally imaginary quartic extension of $\mathbb{Q}$, then $r_1 = 0$ and $r_2 = 2$, so that $r = 0 + 2 - 1 = 1$, and $\mathcal{O}_K^* = \mu(\mathcal{O}_K) \times \mathbb{Z}$. For K^+ a totally real quadratic extension of $\mathbb{Q}$, $r_1 = 2$ and $r_2 = 0$ so that $r = 2 + 0 - 1 = 1$ as well, and $\mathcal{O}^*_{K^+} = \mu(\mathcal{O}_{K^+}) \times \mathbb{Z}$. Thus each $\mathcal{O}^*_K$ and $\mathcal{O}^*_{K^+}$ have the same rank, and in fact, they share the same fundamental unit, call it α.

Next, recall from Theorem 4.1.3 that the group $\mathcal{O}^*_F/\mathcal{O}^*$ is finite. In particular this means that $\mathcal{O}^*$ must have the same rank as $\mathcal{O}^*_F$, so that $\mathcal{O}^* = \mu(\mathcal{O}) \times \mathbb{Z}$ and $\mathcal{O}^{+*} = \mu(\mathcal{O}^{+*}) \times \mathbb{Z}$. In fact, these also have the same generator of the free part, α^m, for some positive $m \in \mathbb{Z}$ and α the fundamental unit of $\mathcal{O}^*_K$ and $\mathcal{O}^*_{K^+}$.

Consider now

$$[\mathcal{O}^*_K : \mathcal{O}^*] = \left|\mathcal{O}^*_K/\mathcal{O}^*\right| = \left|\mu(\mathcal{O}_K)/\mu(\mathcal{O}) \times \langle\alpha\rangle/\langle\alpha^m\rangle\right| = \left|\mu(\mathcal{O}_K)/\mu(\mathcal{O})\right| \cdot m.$$

Similarly,

$$\left[\mathcal{O}^*_{K^+} : \mathcal{O}^{+*}\right] = \left|\mathcal{O}^*_{K^+}/\mathcal{O}^{+*}\right| = \left|\mu(\mathcal{O}_{K^+})/\mu(\mathcal{O}^+) \times \langle\alpha\rangle/\langle\alpha^m\rangle\right| = \left|\mu(\mathcal{O}_{K^+})/\mu(\mathcal{O}^+)\right| \cdot m.$$

Thus taking the ratio of these indices yields

$$\frac{\left[\mathcal{O}^*_{K^+} : \mathcal{O}^{+*}\right]}{[\mathcal{O}^*_K : \mathcal{O}^*]} = \frac{\left|\mu(\mathcal{O}_{K^+})/\mu(\mathcal{O}^+)\right| \cdot m}{\left|\mu(\mathcal{O}_K)/\mu(\mathcal{O})\right| \cdot m}.$$

The m's divide out and we are left with assessing the unit groups, both of which we know are at least finite. First, we know that $\mu(\mathcal{O}_{K^+}) = \{\pm 1\}$, and since $\mathbb{Z} \subseteq \mathcal{O}^+$, $\mu(\mathcal{O}^+)$ also is just the set $\{\pm 1\}$, so that $\left[\mathcal{O}^*_{K^+} : \mathcal{O}^{+*}\right] = 1$. Second, by the work done in the proof of Lemma 4.1.5 we have shown that $|\mu(\mathcal{O}_K)| = \omega_K \leq 24$, and because $\mu(\mathcal{O}) \subseteq \mu(\mathcal{O}_K)$ and $\mu(\mathcal{O})$ always contains at least $\{\pm 1\}$, then $\left|\mu(\mathcal{O}_K)/\mu(\mathcal{O})\right| \leq |\mu(\mathcal{O}_K)|/2 \leq 14$. Thus we may conclude that

$$\frac{1}{12} \leq \frac{\left[\mathcal{O}_{K^+}^* : \mathcal{O}^{+*}\right]}{\left[\mathcal{O}_K^* : \mathcal{O}^*\right]} \leq 1.$$

□

The final terms we have left to bound are terms of the form $\#(\mathcal{O}/\mathfrak{a})^*$. Our aim in bounding these terms is to bound them in terms of discriminants, just as we did with the ratio of the class numbers. We proceed as follows.

Define for each order $\mathcal{O}$ in K (or K^+) a generalized Euler totient function $\varphi_{\mathcal{O}}(\mathfrak{a}) = \#\left(\mathcal{O}/\mathfrak{a}\right)^*$ on ideals $\mathfrak{a}$ of $\mathcal{O}$. Let $N_{\mathcal{O}}(\mathfrak{a})$ denote the ideal norm of $\mathfrak{a} \in \mathcal{O}$ which is defined to be $N_{\mathcal{O}}(\mathfrak{a}) = [\mathcal{O} : \mathfrak{a}]$.

Lemma 4.1.8. *For an order $\mathcal{O}$ in a field F and an ideal $\mathfrak{a}$ of $\mathcal{O}$, there exists a constant c_1 such that*

$$\frac{c_1 N_{\mathcal{O}}(\mathfrak{a})}{\log(\log(N_{\mathcal{O}}(\mathfrak{a})))} \leq \varphi_{\mathcal{O}}(\mathfrak{a}) \leq N_{\mathcal{O}}(\mathfrak{a}).$$

Proof. The inequality $\varphi_{\mathcal{O}}(\mathfrak{a}) \leq N_{\mathcal{O}}(\mathfrak{a})$ is clear, since $\varphi_{\mathcal{O}}(\mathfrak{a}) = \#\left(\mathcal{O}/\mathfrak{a}\right)^*$ and $N_{\mathcal{O}}(\mathfrak{a}) = [\mathcal{O} : \mathfrak{a}] = \#\left(\mathcal{O}/\mathfrak{a}\right)$. As for the other inequality, this follows from Theorem 6.3.2 in [Kno90].

□

(3) $\#(\mathcal{O}_K/\mathfrak{f})^* \Big/ \#(\mathcal{O}/\mathfrak{f})^*$:

Theorem 4.1.14. *Let $\mathcal{O}_K$ be the ring of integers of K, and $\mathcal{O}$ be a general order in K of conductor $\mathfrak{f}$. Then for any $\delta > 0$, there exist constants $C_1(\delta)$ and $C_2(\delta)$ such that*

$$C_1(\delta) q^{-\delta} \sqrt{\frac{\Delta(\mathcal{O})}{\Delta(K)}} < \frac{\#\left(\mathcal{O}_K/\mathfrak{f}\right)^*}{\#\left(\mathcal{O}/\mathfrak{f}\right)^*} < C_2(\delta) q^{\delta} \sqrt{\frac{\Delta(\mathcal{O})}{\Delta(K)}}.$$

Proof. Using the bounds given in Lemma 4.1.8, first rewrite $\frac{\#\left(\mathcal{O}_K/\mathfrak{f}\right)^*}{\#\left(\mathcal{O}/\mathfrak{f}\right)^*} = \frac{\varphi_{\mathcal{O}_K}(\mathfrak{f})}{\varphi_{\mathcal{O}}(\mathfrak{f})}$, so that

$$\frac{c_1 N_{\mathcal{O}_K}(\mathfrak{f})}{\log(\log(N_{\mathcal{O}_K}(\mathfrak{f})))N_{\mathcal{O}}(\mathfrak{f})} \leq \frac{\varphi_{\mathcal{O}_K}(\mathfrak{f})}{\varphi_{\mathcal{O}}(\mathfrak{f})} \leq \frac{N_{\mathcal{O}_K}(\mathfrak{f})\log(\log(N_{\mathcal{O}}(\mathfrak{f})))}{c_2 N_{\mathcal{O}}(\mathfrak{f})}. \tag{4.13}$$

With the following lemma we will be able to revise these bounds to eliminate the log terms.

Lemma 4.1.9 ([Neu99]). *Let $f(X)$ be a monic irreducible polynomial, and let $K = \mathbb{Z}[X]/f(X)$. Let $\Delta(f)$ be the discriminant of $f(X)$ and $\mathfrak{D}_{K/\mathbb{Q}}$ be the different of K. Then $f'(\theta)\mathcal{O}_K = \mathfrak{f}\mathfrak{D}_{K/\mathbb{Q}}$.*

Given this lemma, taking the norm of both sides yields $\Delta(f) = N(\mathfrak{f})\cdot|\mathfrak{D}_{K/\mathbb{Q}}| = N(\mathfrak{f})\Delta(K)$. Thus each norm of $\mathfrak{f}$ can be bound above by $\frac{\Delta(f)}{\Delta(K)} \leq \Delta(f)$ which has order q^6. Thus if $N_{\mathcal{O}}(\mathfrak{f}) \leq q^6$, then since $\log(\log(q)) \leq \log(q)$ we may apply Lemma 4.1.6 to say that for all $\delta > 0$ there exists a constant C_δ such that for all $q > 0$ we have $\log(\log(N_{\mathcal{O}}(\mathfrak{f}))) \leq \log(\log(q^6)) < C_\delta q^\delta$. Using this, refine the bounds to be

$$\frac{c_1 N_{\mathcal{O}_K}(\mathfrak{f})}{C_{\delta_1} q^{\delta_1} N_{\mathcal{O}}(\mathfrak{f})} < \frac{\varphi_{\mathcal{O}_K}(\mathfrak{f})}{\varphi_{\mathcal{O}}(\mathfrak{f})} < \frac{N_{\mathcal{O}_K}(\mathfrak{f}) C_{\delta_2} q^{\delta_2}}{c_2 N_{\mathcal{O}}(\mathfrak{f})},$$

which for any $\delta > 0$ we can bound using constants $C_i(\delta)$ so that

$$C_1(\delta) q^{-\delta}\frac{[\mathcal{O}_K : \mathfrak{f}]}{[\mathcal{O} : \mathfrak{f}]} < \frac{\varphi_{\mathcal{O}_K}(\mathfrak{f})}{\varphi_{\mathcal{O}}(\mathfrak{f})} < C_2(\delta) q^{\delta}\frac{[\mathcal{O}_K : \mathfrak{f}]}{[\mathcal{O} : \mathfrak{f}]}. \tag{4.14}$$

Now, consider the inclusions $\mathfrak{f} \subset \mathcal{O} \subset \mathcal{O}_K$ as abelian groups. Then the third isomorphism theorem for groups states

$$\mathcal{O}_K/\mathfrak{f}\Big/\mathcal{O}/\mathfrak{f} \cong \mathcal{O}_K/\mathcal{O},$$

meaning that $\dfrac{[\mathcal{O}_K : \mathfrak{f}]}{[\mathcal{O} : \mathfrak{f}]} = [\mathcal{O}_K : \mathcal{O}]$.

Thus we may rewrite equation (4.14) as

$$C_1(\delta)q^{-\delta}[\mathcal{O}_K : \mathcal{O}] < \frac{\#(\mathcal{O}_K/\mathfrak{f})^*}{\#(\mathcal{O}/\mathfrak{f})^*} < C_2(\delta)q^{\delta}[\mathcal{O}_K : \mathcal{O}],$$

which by Lemma 4.1.1 becomes

$$C_1(\delta)q^{-\delta}\sqrt{\frac{\Delta(\mathcal{O})}{\Delta(K)}} < \frac{\#(\mathcal{O}_K/\mathfrak{f})^*}{\#(\mathcal{O}/\mathfrak{f})^*} < C_2(\delta)q^{\delta}\sqrt{\frac{\Delta(\mathcal{O})}{\Delta(K)}}. \tag{4.15}$$

□

(4) $\#(\mathcal{O}^+/\mathfrak{f}^+)^* \Big/ \#(\mathcal{O}_{K^+}/\mathfrak{f}^+)^*$: In a similar manner as in 3, we state and prove the following theorem.

Theorem 4.1.15. *Let $\mathcal{O}_{K^+}$ be the ring of integers of K^+, and $\mathcal{O}^+$ be an order in K of conductor $\mathfrak{f}^+$, then for any $\delta^+ > 0$ there exist constants $C_3(\delta^+)$ and $C_4(\delta^+)$ such that*

$$C_3(\delta^+)q^{-\delta^+}\sqrt{\frac{\Delta(K^+)}{\Delta(\mathcal{O}^+)}} < \frac{\#\left(\mathcal{O}^+/\mathfrak{f}^+\right)^*}{\#\left(\mathcal{O}_{K^+}/\mathfrak{f}^+\right)^*} < C_4(\delta^+)q^{\delta^+}\sqrt{\frac{\Delta(K^+)}{\Delta(\mathcal{O}^+)}}.$$

Proof. In a similar manner as before we begin by rewriting $\dfrac{\#(\mathcal{O}^+/\mathfrak{f}^+)^*}{\#(\mathcal{O}_{K^+}/\mathfrak{f}^+)^*}$ in terms of the Euler totient functions, and get the following bounds

$$\frac{c_3 N_{\mathcal{O}^+}(\mathfrak{f}^+)}{\log(\log(N_{\mathcal{O}^+}(\mathfrak{f}^+)))N_{\mathcal{O}_{K^+}}(\mathfrak{f}^+)} \leq \frac{\varphi_{\mathcal{O}^+}(\mathfrak{f}^+)}{\varphi_{\mathcal{O}_{K^+}}(\mathfrak{f}^+)} \leq \frac{N_{\mathcal{O}^+}(\mathfrak{f}^+)\log(\log(N_{\mathcal{O}_{K^+}}(\mathfrak{f}^+)))}{c_4 N_{\mathcal{O}_{K^+}}(\mathfrak{f}^+)}.$$

Then bound the $\log(\log(N_{\mathcal{O}_\diamond}(\mathfrak{f}^+)))$ as before so that for any $\delta_i^+ > 0$ there exists a constant $C(\delta_i^+)$ and reduce to

$$\frac{c_3 N_{\mathcal{O}^+}(\mathfrak{f}^+)}{C(\delta_1^+)q^{\delta_1^+} N_{\mathcal{O}_{K^+}}(\mathfrak{f}^+)} < \frac{\varphi_{\mathcal{O}^+}(\mathfrak{f}^+)}{\varphi_{\mathcal{O}_{K^+}}(\mathfrak{f}^+)} < \frac{C(\delta_2^+)q^{\delta_2^+} N_{\mathcal{O}^+}(\mathfrak{f}^+)}{c_4 N_{\mathcal{O}_{K^+}}(\mathfrak{f}^+)}$$

$$C_3(\delta_1^+)q^{-\delta_1^+}\frac{[\mathcal{O}^+ : \mathfrak{f}^+]}{[\mathcal{O}_{K^+} : \mathfrak{f}^+]} < \frac{\varphi_{\mathcal{O}^+}(\mathfrak{f}^+)}{\varphi_{\mathcal{O}_{K^+}}(\mathfrak{f}^+)} < C_4(\delta_2^+)q^{\delta_2^+}\frac{[\mathcal{O}^+ : \mathfrak{f}^+]}{[\mathcal{O}_{K^+} : \mathfrak{f}^+]}. \tag{4.16}$$

This time the first isomorphism theorem for groups tells us $\frac{[\mathcal{O}^+ : \mathfrak{f}^+]}{[\mathcal{O}_{K^+} : \mathfrak{f}^+]} = \frac{1}{[\mathcal{O}_{K^+} : \mathcal{O}^+]}$, which by Lemma 4.1.1 is equal to $\sqrt{\frac{\Delta(K^+)}{\Delta(\mathcal{O}^+)}}$. In summary, for any $\delta^+ > 0$ there exist constants $C_3(\delta^+)$ and $C_4(\delta^+)$ such that

$$C_3(\delta^+)q^{-\delta^+}\sqrt{\frac{\Delta(K^+)}{\Delta(\mathcal{O}^+)}} < \frac{\#(\mathcal{O}^+/\mathfrak{f}^+)^*}{\#(\mathcal{O}_{K^+}/\mathfrak{f}^+)^*} < C_4(\delta^+)q^{\delta^+}\sqrt{\frac{\Delta(K^+)}{\Delta(\mathcal{O}^+)}}. \tag{4.17}$$

□

We have thus bound each of the four terms used in the ratio of the sizes of the Picard groups, and we may now summarize the results to prove Theorem 4.1.11.

Using the lower bounds for the inequalities computed above a lower bound for the ratio of the size of the Picard groups can be written in terms of δ, δ^+, ε' and their corresponding constants:

$$\begin{aligned}\frac{h_K}{h_{K^+}}\frac{[\mathcal{O}_{K^+}^* : \mathcal{O}^{+*}]}{[\mathcal{O}_K^* : \mathcal{O}^*]}\frac{\#(\mathcal{O}_K/\mathfrak{f})^*}{\#(\mathcal{O}/\mathfrak{f})^*}\frac{\#(\mathcal{O}^+/\mathfrak{f}^+)^*}{\#(\mathcal{O}_{K^+}/\mathfrak{f}^+)^*} &= \frac{h(\mathcal{O})}{h(\mathcal{O}^+)}\\ C_<(\varepsilon')q^{\varepsilon'}\sqrt{\frac{\Delta(K)}{\Delta(K^+)}}\cdot\frac{1}{12}\cdot C_1(\delta)q^{-\delta}\sqrt{\frac{\Delta(\mathcal{O})}{\Delta(K)}}\cdot C_3(\delta^+)q^{-\delta^+}\sqrt{\frac{\Delta(K^+)}{\Delta(\mathcal{O}^+)}} &< \frac{h(\mathcal{O})}{h(\mathcal{O}^+)}.\end{aligned}$$

To summarize we can say that for any $\epsilon > 0$ there exists a constant $C'_<(\epsilon)$ such that

$$C'_<(\epsilon)q^{-\epsilon}\sqrt{\frac{\Delta(\mathcal{O})}{\Delta(\mathcal{O}^+)}} < \frac{h(\mathcal{O})}{h(\mathcal{O}^+)}. \tag{4.18}$$

Similarly an upper bound for the ratio of the size of the Picard groups can be written in terms of δ, δ^+, ε' and their corresponding constants:

$$\frac{h(\mathcal{O})}{h(\mathcal{O}^+)} = \frac{h_K}{h_{K^+}}\frac{[\mathcal{O}^*_{K^+} : \mathcal{O}^{+*}]}{[\mathcal{O}^*_K : \mathcal{O}^*]}\frac{\#(\mathcal{O}_K/\mathfrak{f})^*}{\#(\mathcal{O}/\mathfrak{f})^*}\frac{\#(\mathcal{O}^+/\mathfrak{f}^+)^*}{\#(\mathcal{O}_{K^+}/\mathfrak{f}^+)^*}$$
$$\frac{h(\mathcal{O})}{h(\mathcal{O}^+)} < C_>(\varepsilon')q^{\varepsilon'}\sqrt{\frac{\Delta(K)}{\Delta(K^+)}}\cdot 1\cdot C_2(\delta)q^{\delta}\sqrt{\frac{\Delta(\mathcal{O})}{\Delta(K)}}\cdot C_4(\delta^+)q^{\delta^+}\sqrt{\frac{\Delta(K^+)}{\Delta(\mathcal{O}^+)}}.$$

For this upper bound we can say for any $\epsilon > 0$ there exists a constant $C'_>(\epsilon)$ such that

$$\frac{h(\mathcal{O})}{h(\mathcal{O}^+)} < C'_>(\epsilon)q^{\epsilon}\sqrt{\frac{\Delta(\mathcal{O})}{\Delta(\mathcal{O}^+)}}. \tag{4.19}$$

□

Now that we have bound the ratio $h(\mathcal{O})/h(\mathcal{O}^+)$ we will be able to determine bounds for the size of an isogeny class for a simple ordinary principally polarized abelian surface.

4.1.6. The Size of an Isogeny Class. Given the computations done in the previous sections, we may now state and prove the following theorem which gives bounds for the size of a simple, ordinary isogeny class. Let $\mathcal{I}_f$ denote the isogeny class of principally polarized abelian surfaces defined by an irreducible, ordinary $q-$Weil polynomial $f = f(X)$. Define $D(a,b) = \Delta(f)/(q^2(a^2 - 4b + 8q))$.

Theorem 4.1.16. *With notation as above and for any $\epsilon > 0$, there exist constants $C'_<(\epsilon)$ and $C''_>(\epsilon)$ such that*

$$C'_<(\epsilon)q^{-\epsilon}\sqrt{D(a,b)} < \#\mathcal{I}_f < C''_>(\epsilon)q^{\epsilon}\sqrt{D(a,b)}.$$

Proof. We will begin with the lower bound. Recall the sum from equation (4.3) which computes the size of the isogeny class. In order to compute a lower bound it is enough to consider only a single term. In particular, consider the term for which $\mathcal{O} = \mathbb{Z}[\pi, \overline{\pi}]$. Then certainly

$$\sum_{\substack{\mathcal{O} \\ \mathbb{Z}[\pi,\overline{\pi}]\subseteq\mathcal{O}\subseteq\mathcal{O}_K}} \frac{h(\mathcal{O})}{h(\mathcal{O}^+)} > \frac{h(\mathbb{Z}[\pi,\overline{\pi}])}{h(\mathbb{Z}[\pi+\overline{\pi}])} > C'_<(\epsilon)q^{-\epsilon}\sqrt{\frac{\Delta(\mathbb{Z}[\pi,\overline{\pi}])}{\Delta(\mathbb{Z}[\pi+\overline{\pi}])}} \qquad \text{by Theorem 4.1.11}$$

$$= C'_<(\epsilon)q^{-\epsilon}\sqrt{\frac{\Delta(f)}{q^2(a^2-4b+8q)}}$$

$$= C'_<(\epsilon)q^{-\epsilon}\sqrt{D(a,b)}. \tag{4.20}$$

Thus we have for any $\epsilon > 0$ the following lower bound for the size of a simple, ordinary isogeny class

$$C'_<(\epsilon)q^{-\epsilon}\sqrt{D(a,b)} < \#\mathcal{I}_f. \tag{4.21}$$

Now, before we can compute the upper bound for the size of an isogeny class let us first determine an upper bound on the ratio $\Delta(\mathcal{O})/\Delta(\mathcal{O}^+)$.

Lemma 4.1.10. *The ratio $\dfrac{\Delta(\mathcal{O})}{\Delta(\mathcal{O}^+)}$ is maximized when $\mathcal{O} = \mathbb{Z}[\pi,\overline{\pi}]$.*

Proof. Let $[\mathcal{O} : \mathbb{Z}[\pi, \overline{\pi}]] = m$ and $[\mathcal{O}^+ : \mathbb{Z}[\pi + \overline{\pi}]] = n$, then

$$\begin{aligned}\sqrt{\frac{\Delta(\mathcal{O})}{\Delta(\mathcal{O}^+)}} &= \sqrt{\frac{\frac{1}{m^2}\Delta(f)}{q^2\frac{1}{n^2}\Delta(f^+)}} \\ &= \frac{n}{m}\sqrt{\frac{\Delta(f)}{q^2\Delta(f^+)}}.\end{aligned}$$

Now observe that $n \leq m$ since $\mathcal{O}^+/\mathbb{Z}[\pi + \overline{\pi}] \subset \mathcal{O}/\mathbb{Z}[\pi, \overline{\pi}]$. Thus $n/m \leq 1$ and we have the upper bound

$$\begin{aligned}\sqrt{\frac{\Delta(\mathcal{O})}{\Delta(\mathcal{O}^+)}} &\leq \sqrt{\frac{\Delta(f)}{q^2\Delta(f^+)}} \\ &= \sqrt{\frac{q^2(a^2 - 4b + 8q)^2(b^2 + 4bq + 4q^2 - 4a^2q)}{q^2(a^2 - 4b + 8q)}} \\ &= \sqrt{D(a, b)}.\end{aligned}$$

□

In terms of $\sqrt{D(a,b)}$ the upper bound on $h(\mathcal{O})/h(\mathcal{O}^+)$ from equation (4.19) is

$$\begin{aligned}\frac{h(\mathcal{O})}{h(\mathcal{O}^+)} &< C'_>(\epsilon')q^{\epsilon'}\sqrt{\frac{\Delta(\mathcal{O})}{\Delta(\mathcal{O}^+)}} \\ &< C'_>(\epsilon')q^{\epsilon'}\sqrt{D(a, b)}.\end{aligned}$$

Recall the sum from equation (4.3) which computes the size of a simple, ordinary isogeny class. Using $C'_>(\epsilon)q^\epsilon\sqrt{D(a,b)}$ as an upper bound on $h(\mathcal{O})/h(\mathcal{O}^+)$ then we can bound the sum

$$\sum_{\substack{\mathcal{O} \\ \mathbb{Z}[\pi,\overline{\pi}]\subseteq\mathcal{O}\subseteq\mathcal{O}_K}} \frac{h(\mathcal{O})}{h(\mathcal{O}^+)} < \sum_{\substack{\mathcal{O} \\ \mathbb{Z}[\pi,\overline{\pi}]\subseteq\mathcal{O}\subseteq\mathcal{O}_K}} C'_>(\epsilon)q^\epsilon\sqrt{D(a,b)}$$

$$= \#\{\mathcal{O} \,:\, \mathbb{Z}[\pi,\overline{\pi}] \subseteq \mathcal{O} \subseteq \mathcal{O}_K\}\left(C'_>(\epsilon)q^\epsilon\sqrt{D(a,b)}\right). \tag{4.22}$$

Note here that

$$D(a,b) = (a^2 - 4b + 8q)(b^2 + 4bq + 4q^2 - 4a^2q)$$

$$= 32q^3 + (16b - 28a^2)q^2 + (20a^2b - 4a^4 - 8b^2)q + a^2b^2 - 4b^3,$$

has leading term q^3.

Now to count the number of orders between $\mathbb{Z}[\pi,\overline{\pi}]$ and $\mathcal{O}_K$ consider the orders as $\mathbb{Z}-$modules. Given that $\mathbb{Z}[\pi,\overline{\pi}] \subseteq \mathcal{O}_K$ there exist a_i and m_i such that we may write $\mathcal{O}_K = \oplus_{i=1}^4 \mathbb{Z}a_i$, and $\mathbb{Z}[\pi,\overline{\pi}] = \oplus_{i=1}^4 \mathbb{Z}m_ia_i$. Furthermore, any order $\mathcal{O}$ between $\mathbb{Z}[\pi,\overline{\pi}]$ and $\mathcal{O}_K$ can be written as $\oplus_{i=1}^4 \mathbb{Z}n_ia_i$ where n_i is a divisor of m_i for each i.

Lemma 4.1.11. *[Divisor Bound, [Tao08]] Let $d(m)$ denote the number of divisors of m including 1 and m, then the for any $\varepsilon > 0$,*

$$d(m) \leq C_\varepsilon m^\varepsilon.$$

Using Lemma 4.1.11, we can bound the number of possible orders between $\mathbb{Z}[\pi,\overline{\pi}]$ and $\mathcal{O}_K$ by

$$\#\{\mathcal{O} \,:\, \mathbb{Z}[\pi,\overline{\pi}] \subseteq \mathcal{O} \subseteq \mathcal{O}_K\} = \prod_{i=1}^4 d(m_i) \leq C_\varepsilon\left(\prod_{i=1}^4 m_i\right)^\varepsilon. \tag{4.23}$$

In order to say something about this product of the m_i's, recall the definition of the discriminant of an order from Section 4.1.1. Then we can write

$$\Delta(\mathbb{Z}[\pi,\overline{\pi}]) = \det(\mathrm{Tr}_{\mathbb{Z}[\pi,\overline{\pi}]/\mathbb{Z}}(m_i a_i m_j a_j))_{i,j=1}^{n} = \det(m_i m_j \mathrm{Tr}_{\mathbb{Z}[\pi,\overline{\pi}]/\mathbb{Z}}(a_i a_j)).$$

Note that the matrix $\Big(m_i m_j \mathrm{Tr}(a_i a_j)\Big) = \Big(m_i\Big)\Big(\mathrm{Tr}(a_i a_j)\Big)\Big(m_i\Big)$, where $\Big(m_i\Big)$ is the diagonal matrix with m_i in the (i,i) entry and zeros elsewhere. Thus

$$\begin{aligned}
\Delta(\mathbb{Z}[\pi,\overline{\pi}]) &= \det(m_i m_j \mathrm{Tr}_{\mathbb{Z}[\pi,\overline{\pi}]/\mathbb{Z}}(a_i a_j)) \\
&= \det(m_i)\det(\mathrm{Tr}_{\mathbb{Z}[\pi,\overline{\pi}]/\mathbb{Z}}(a_i a_j))\det(m_i) \\
&= \det(\mathrm{Tr}_{\mathbb{Z}[\pi,\overline{\pi}]/\mathbb{Z}}(a_i a_j)) \left(\prod_{i=1}^{n} m_i\right)^2 \\
&= \Delta(\mathcal{O}) \left(\prod_{i=1}^{n} m_i\right)^2.
\end{aligned}$$

Using this we can say that

$$\left(\prod_{i=1}^{n} m_i\right)^2 = \frac{\Delta(\mathbb{Z}[\pi,\overline{\pi}])}{\Delta(\mathcal{O})}.$$

We have seen already that $\Delta(\mathbb{Z}[\pi,\overline{\pi}]) = \frac{\Delta(f)}{q^2}$ and that $\frac{1}{\Delta(\mathcal{O})} \leq 1$, thus we may bound equation (4.23) above by

$$\begin{aligned}
\#\{\mathcal{O} \,:\, \mathbb{Z}[\pi,\overline{\pi}] \subseteq \mathcal{O} \subseteq \mathcal{O}_K\} &\leq C_\varepsilon \left(\prod_{i=1}^{4} m_i\right)^{\varepsilon} \\
&\leq C_\varepsilon \left(\sqrt{\frac{\Delta(f)}{q^2}}\right)^{\varepsilon} \\
&= C_\varepsilon \left(\sqrt{(a^2-4b+8q)D(a,b)}\right)^{\varepsilon} \\
&< C_\varepsilon q^{2\varepsilon}. \qquad (4.24)
\end{aligned}$$

Substituting this into equation (4.22) we get

$$\begin{aligned}
\sum_{\substack{\mathcal{O} \\ \mathbb{Z}[\pi,\overline{\pi}]\subseteq\mathcal{O}\subseteq\mathcal{O}_K}} \frac{h(\mathcal{O})}{h(\mathcal{O}^+)} &< \#\{\mathcal{O} \,:\, \mathbb{Z}[\pi,\overline{\pi}] \subseteq \mathcal{O} \subseteq \mathcal{O}_K\} C'_>(\epsilon) q^{\epsilon}\sqrt{D(a,b)} \\
&< \left(C_\varepsilon q^{2\varepsilon}\right) C'_>(\epsilon) q^{\epsilon}\sqrt{D(a,b)}.
\end{aligned}$$

Now combining the constants and the q terms we can say that for any $\epsilon > 0$ there exists a constant $C''_>(\epsilon)$ so that

$$\#\mathcal{I}_f < C''_>(\epsilon) q^{\epsilon}\sqrt{D(a,b)}.$$

□

Recalling that $D(a,b)$ has leading term q^3, Theorem 4.1.16 bounds the size of a simple, ordinary isogeny class by terms on the order of $q^{3/2}$.

4.2. Set Up for the Proof of the Counting Theorem

Now that we have determined bounds for the size of a simple, ordinary isogeny class, we turn our attention to characteristic polynomials of Frobenius corresponding to abelian surfaces with real multiplication by K^+.

Fix $d \in \mathbb{Z}$, positive and square free and let $K^+ = \mathbb{Q}(\sqrt{d})$, so that K^+ has discriminant, $\Delta(K^+) = d$ or $4d$. Recall that the characteristic polynomial of Frobenius of a principally polarized abelian surface $A/\mathbb{F}_q$ has the form

$$f_A(X) = X^4 - aX^3 + bX^2 - aqX + q^2,$$

and satisfies the Weil inequalities from equation (3.1). Thus for a given q the integer pair (a, b) defines $f_A(X)$. Furthermore, since $f_A(X)$ is a $q-$Weil polynomial, the pair (a, b) must lie in the region of the plane shaped like the swallowtail below.

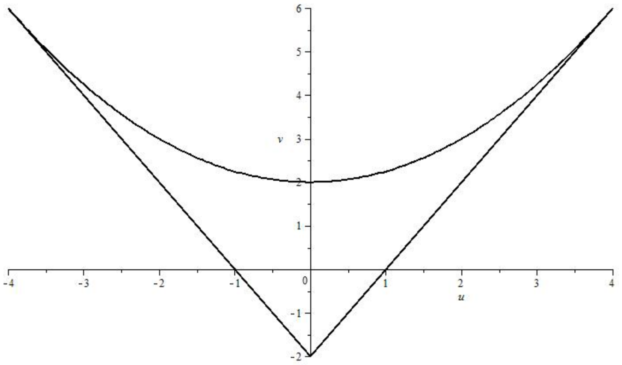


Figure 4.1. The Weil region, scaled so that $u = a/\sqrt{q}$ and $v = b/q$.

The coefficient pairs (a, b) create a lattice inside the Weil region. It will be our task in the following sections to count the number of lattice points in the Weil region that correspond to isogeny classes of abelian surfaces with real multiplication (RM) by K^+.

Recall that the real quadratic subfield inside $\mathrm{End}^0(A)$ has discriminant $\Delta_A^+ = a^2 - 4b + 8q$. Thus for A to have real multiplication by the field K^+ with discriminant $\Delta(K^+) = d$, it must be that either A is simple and $\Delta_A^+ = a^2 - 4b + 8q = r^2 d$, for some integer $r \neq 0$, or $A \sim E^2$ and $r = 0$. In particular, we wish to count the number of abelian surfaces in the set

$$\begin{aligned}\mathscr{A}_{q,d} &= \{A/\mathbb{F}_q \,:\, A \text{ is principally polarized and has RM by } K^+\}\\ &= \{A/\mathbb{F}_q \,:\, K^+ \subset \mathrm{End}^0(A)\}\\ &= \{A/\mathbb{F}_q \,:\, \Delta_A^+ = a^2 - 4b + 8q = r^2 d,\, r \neq 0\} \cup \{A \sim E^2\}. \qquad (4.25)\end{aligned}$$

Definition 4.2.1. *Call the pair (a, b) an* <u>isogeny class representative</u> *if (a, b) lies within the Weil region and a and b are the coefficients of the characteristic polynomial of the abelian surfaces in the isogeny class.*

Define the set of isogeny class representatives corresponding to real multiplication by K^+ to be the set:

$$\mathrm{RMI}(q, d) := \{(a, b) \,:\, X^4 - aX^3 + bX^2 - aqX + q^2 = f_A(X) \text{ for } A \text{ with RM by } K^+\}.$$

Note that the set $\mathrm{RMI}(q, d)$ is a subset of the set of all isogeny class representatives.

Using the definition for the set $\mathscr{A}_{q,d}$ in equation (4.25), consider the equation $a^2 - 4b + 8q = r^2 d$. It turns out to be easier to count pairs (a, r) rather than pairs (a, b) since a and r have the same degree in this equation. Thus we make the following reduction

$$\begin{aligned}\Delta_A^+ &= r^2 d\\ a^2 - 4b + 8q &= r^2 d\\ 4b &= a^2 - r^2 d + 8q\\ b &= \frac{a^2 - r^2 d}{4} + 2q \qquad (4.26)\end{aligned}$$

Since $f_A(X)$ is an integer polynomial equation (4.26) implies $a^2 - r^2d \equiv 0 \mod 4$, so that $b \in \mathbb{Z}$. This equivalence modulo 4 can occur in one of two ways: (i) if $d \equiv 2, 3 \mod 4$ then a, r must both be even; (ii) if $d \equiv 1 \mod 4$ then a, r must have the same parity.

A further reduction can be made by noting if the pair (a, b) is a solution to $\Delta_A^+ = r^2d$, then $(-a, b)$ is also a solution. Thus counting pairs (a, b) with $a > 0$ which satisfy $\Delta_A^+ = r^2d$ is sufficient to be able to compute all pairs in the Weil region which satisfy $\Delta_A^+ = r^2d$. The pairs $(0, b)$ will be counted separately when relevant. For now consider only the part of the Weil region bound by $0 \leq a \leq 4\sqrt{q}$.

As a final reduction we use the following lemma to bound r on the Weil region.

Lemma 4.2.1. *The maximum value of* $\Delta_A^+ = a^2 - 4b + 8q$ *on the Weil region is* $16q$.

Proof. Fix q, and consider the partial derivatives of Δ_A^+ with respect to a and b. The first partial with respect to b is never zero, thus there cannot be a local (or global) extrema of Δ_A^+ on the interior of the Weil region. So take the parabolic upper boundary of the Weil region defined by $b = \frac{a^2}{4} + 2q$, and substitute this in for b in Δ_A^+. It is easy to see that $\Delta_A^+ = 0$ along this boundary. Finally, on the linear segments where $b = 2|a|\sqrt{q} - 2q$, then $\Delta_A^+ = a^2 - 4(2|a|\sqrt{q} - 2q) + 8q$, which simplifies to $\Delta_A^+ = a^2 - 8|a|\sqrt{q} + 16q$. This function has critical points at $a = \pm 4\sqrt{q}$ (the upper corners of the Weil region), however, $\Delta_A^+ = 0$ at both of these points. So it remains to check the remaining endpoint, the lower vertex, $(0, -2q)$. $\Delta_A^+ = 0^2 - 4(-2q) + 8q = 16q$ at this point. Thus $16q$ is the maximum value of Δ_A^+ on the Weil region. □

What this means for the value r is that $r^2 = \frac{\Delta_A^+}{d} \leq \frac{16q}{d}$. Hence, for any ordinary pair (a,b) in the Weil region, which satisfies $\Delta_A^+ = r^2 d$, it must be that

$$0 < r \leq \frac{4\sqrt{q}}{\sqrt{d}}. \tag{4.27}$$

In terms of a and r the Weil inequalities are:

$$2a\sqrt{q} - 2q \leq \frac{a^2 - r^2 d}{4} + 2q \leq \frac{a^2}{4} + 2q.$$

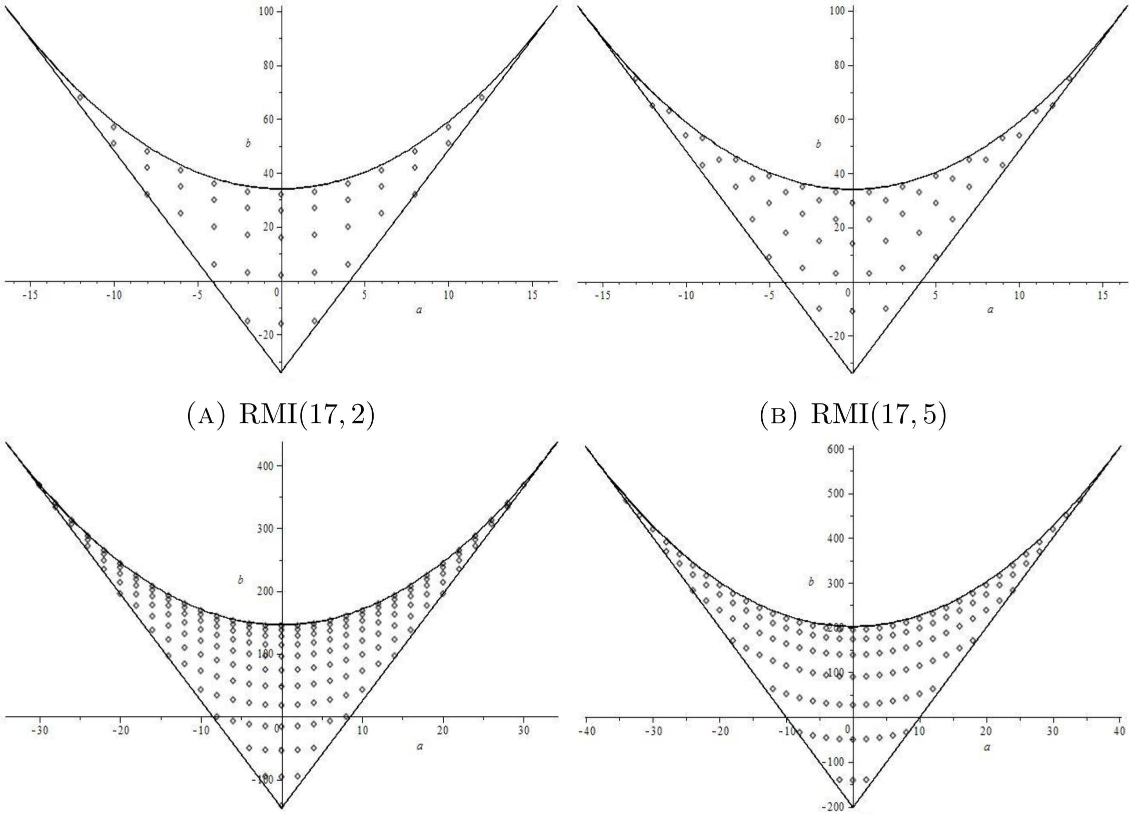
So, for fixed a we can bound r:

$$\begin{aligned}
2a\sqrt{q} - 4q - \frac{a^2}{4} &\leq \frac{-r^2 d}{4} \leq 0 \\
0 &\leq \frac{r^2 d}{4} \leq \frac{a^2}{4} - 2a\sqrt{q} + 4q \\
0 &\leq r^2 \leq \frac{a^2 - 8a\sqrt{q} + 16q}{d} = \frac{(a - 4\sqrt{q})^2}{d} && (4.28) \\
0 &\leq |r| \leq \frac{|a - 4\sqrt{q}|}{\sqrt{d}} && \text{since } a \leq 4\sqrt{q} \Rightarrow |a - 4\sqrt{q}| = 4\sqrt{q} - a \\
0 &\leq |r| \leq \frac{4\sqrt{q} - a}{\sqrt{d}} && (4.29)
\end{aligned}$$

Notice if $0 \leq a \leq 4\sqrt{q}$, then $0 < r \leq \frac{4\sqrt{q}}{\sqrt{d}}$ which is compatible with the bound on r given by the Weil region in equation (4.27).

Given these reductions it is now easier to count (and in fact enumerate) the elements of the set $\mathrm{RMI}(q,d)$ for fixed q and d. To begin, consider even a's and r's. For each even $a \in \{0, ..., \lfloor 4\sqrt{q} \rfloor\}$, list the of possible even r values, $r = 2, ..., \lfloor \frac{4\sqrt{q}-a}{\sqrt{d}} \rfloor$. Then for each even a, define the set of pairs $E_a := \{(a, \frac{a^2 - r^2 d}{4}), (-a, \frac{a^2 - r^2 d}{4}) : r \in \{2, ..., \lfloor \frac{4\sqrt{q}-a}{\sqrt{d}} \rfloor\}$ and even$\}$ which lie in the Weil region, and correspond to a simple abelian surface A with real multiplication by a field K^+ with discriminant d. Then $\bigcup_{a\, even} E_a = \mathrm{RMI}(q,d)$ when $d \equiv 2, 3 \mod 4$. In the case where $d \equiv 1 \mod 4$, define for each odd $a \in \{0, ..., \lfloor 4\sqrt{q} \rfloor\}$, the set of pairs $O_a = \{(a, \frac{a^2-r^2d}{4}), (-a, \frac{a^2-r^2d}{4}) \,:\, r \in \{1, ..., \lfloor \frac{4\sqrt{q}-a}{\sqrt{d}} \rfloor\}$ and odd$\}$. Then $(\bigcup_{a\, even} E_a) \cup (\bigcup_{a\, odd} O_a) = \mathrm{RMI}(q, d)$.

The images below plot the sets $\mathrm{RMI}(q, d)$ for various d values and increasing values of q. These images provide a sense of the distribution of the sets $\mathrm{RMI}(q, d)$ in the Weil region.



(A) $\mathrm{RMI}(17, 2)$

(B) $\mathrm{RMI}(17, 5)$

(C) $\mathrm{RMI}(73, 2)$

(D) $\mathrm{RMI}(101, 7)$

FIGURE 4.2. Plots of the isogeny class representatives in the sets $\mathrm{RMI}(q, d)$.

From the images observe the following:

(1) $(a, b) \in \mathrm{RMI}(q, d)$ occur at integer lattice points since $f_A(X) \in \mathbb{Z}[X]$.

(2) $(a, b) \in \mathrm{RMI}(q, d)$ are uniformly distributed along the horizontal a-axis. In the case that $d \equiv 1 \mod 4$, representatives lie along vertical lines at every integer value of a.

In the case $d \equiv 2, 3 \mod 4$, representatives lie along vertical lines only at even integer values of a.

(3) $(a, b) \in \mathrm{RMI}(q, d)$ accumulate near the quadratic upper boundary of the Weil region.

Now that we have a sense of the distribution of the relevant isogeny class representatives, those which correspond to a simple abelian surfaces with real multiplication by K^+, we wish to count how many there are for a given q and fixed d.

It might help to illustrate how we do this count with an example. In the following example we will compute an upper bound for the size of the set $\mathrm{RMI}(17, 2)$, i.e. we will bound the number of simple isogeny classes of abelian surfaces defined over $\mathbb{F}_{17}$ with real multiplication by $\mathbb{Q}(\sqrt{2})$.

EXAMPLE 4.2.1. *First note $d = 2 \mod 4$ so we are in the case that a and r must both be even to enforce that the isogeny class representatives (a, b) have integer coordinates. Recall if (a, b) is a solution to $\Delta_A^+ = r^2 d$, then $(-a, b)$ is also a solution, so let us begin with pairs (a, b) for $a > 0$. Given $q = 17$ we know that $a \leq 4\sqrt{17} \approx 16.492 < 17$, and a must be even, so say $a \leq 16$. Now for given a we have the bound from equation (4.29) for r. Specifically for this example, we have that $0 < r \leq \frac{4\sqrt{17}-a}{\sqrt{2}}$. In the table below, we compute this bound for r for each positive even $a \leq 16$, then list the possible values of r. The final column lists the number of possible r values. This final column will help us determine the size of the set RMI$(17, 2)$.*

Summing the number of r's in the far right column we get 18. This is the number of relevant isogeny class representatives in the positive half of the Weil region. Doubling this value for the symmetry of the Weil region gives 36 relevant isogeny class representatives with $a \neq 0$. As for the $a = 0$ case, we have $r \leq \frac{4\sqrt{17}-0}{\sqrt{2}} = 11.662$, which means $r = 2, 4, 6, 8, 10$

and we add these 5 *possible* r *values to the* 36 *already counted to get a total of* 41*. What this means is that we have computed* $\#\mathit{RMI}(17,2) = 41$*.*

Table 4.1. Data for valid r values.

a	$\frac{4\sqrt{17}-a}{\sqrt{2}}$	*r values*	*# of r*
2	10.247	$2,4,6,8,10$	5
4	8.833	$2,4,6,8$	4
6	7.419	$2,4,6$	3
8	6.005	$2,4,6$	3
10	4.591	$2,4$	2
12	3.176	2	1
14	1.762	*n/a*	0
16	0.348	*n/a*	0

Looking back at Figure 4.2 above, one can see that the count done here corresponds to the lattice points in Subfigure 4.2a, where $q = 17$ *and* $d = 2$*.*

Note that in this example we only computed an upper bound for the set $\mathrm{RMI}(17,2)$ and not an upper bound for the set $\mathscr{A}_{17,2}$. In order to obtain an upper bound for $\mathscr{A}_{17,2}$ we need to compute an upper bound for the size of a simple, ordinary isogeny class; which at this point amounts to computing an upper bound for $D(a,b)$. This will be done in the following subsection.

Essentially, the method used in this example will be used in the following sections to obtain bounds for the size of the set $\mathscr{A}_{q,d}$.

4.2.1. Bounding $D(a,b)$. We will start by computing an upper bound.

Proposition 4.2.1. *Given $D(a,b) = 32q^3 + (16b - 28a^2)q^2 + (20a^2b - 4a^4 - 8b^2)q + a^2b^2 - 4b^3$, then $D(a,b) \leq \frac{1024}{27}q^3$ for all isogeny class representatives (a,b).*

Proof. Consider $D(a,b) = 32q^3 + (16b - 28a^2)q^2 + (20a^2b - 4a^4 - 8b^2)q + a^2b^2 - 4b^3$. For fixed q, this carves out a surface in 3-space. Multi-variable calculus can be used compute the maximum of $D(a,b)$ on the Weil region. Start by taking derivatives with respect to each variable, a and b:

$$\frac{dD}{da} = 2ab^2 + 40abq - 56aq^2 - 16qa^3 \quad \text{and} \quad \frac{dD}{db} = -12b^2 - 16bq + 16q^2 + 20qa^2 + 2a^2b.$$

Now set each derivative equal to zero to determine the critical points: $(0, -2q)$, $(0, \frac{2}{3}q)$, $(-4\sqrt{q}, 6q)$, $(4\sqrt{q}, 6q)$. Then using the second derivatives and the Hessian, it can be determined that there is a saddle point at $(0, -2q)$, a local (and in fact absolute) maximum at $(0, \frac{2}{3}q)$, and inconclusive behavior at the end points $(\pm 4\sqrt{q}, 6q)$. Comparing the values of $D(a,b)$ at each of these critical points does in fact show that $D(0, \frac{2}{3}q)$ is the absolute maximum with a value of $\frac{1024}{27}q^3$, and $D(a,b) = 0$ at each of the other critical points. It is also not hard to show that along each boundary line of the Weil region $D(a,b) = 0$ as well.

Since the absolute maximum of $D(a,b)$ is $\frac{1024}{27}q^3$, it can be said that for all other valid (a,b) pairs in the Weil region, $D(a,b) \leq \frac{1024}{27}q^3$. □

Note that $D(a,b) = \frac{1024}{27}q^3$ if and only if $a = 0$, $b = \frac{2}{3}q$, and that $b = \frac{2}{3}q \in \mathbb{Z}$ if and only if $3|q$, which will only happen if $p = 3$. Thus as long as $p \neq 3$, then $\frac{32}{3\sqrt{3}}q^{3/2}$ is a strict upper bound for $D(a,b)$.

Given Proposition 4.2.1 and Theorem 4.1.16 a strict upper bound for the size of a simple isogeny class is

$$\#\mathcal{I}_f < C''_{>}(\epsilon)q^{\epsilon}\sqrt{\frac{1024}{27}q^3} = C''_{>}(\epsilon)\frac{32}{3\sqrt{3}}q^{3/2+\epsilon}.$$

As for a lower bound, recall from equation (4.26) a pair (a, r) determines $b = \frac{a^2 - r^2 d}{4} + 2q$, and then such a pair (a, b) satisfies $\Delta_A^+ = r^2 d$. Fix $0 < a \leq 4\sqrt{q}$ and define

$$D_a(r) = D(a, \tfrac{a^2 - r^2 d}{4} + 2q) = \tfrac{1}{16} r^2 d \left(r^4 d^2 - (32qd + 2a^2 d) r^2 + a^4 - 32qa^2 + 256q^2 \right).$$

PROPOSITION 4.2.2. *Fix $0 < a \leq 4\sqrt{q}$, and let $D_a(r)$ be defined as above. Then the square $S_a(r) = \frac{r^2 d}{16} \left(r^2 d - (16q - 8\sqrt{q}a + a^2) \right)^2$ is a lower bound for $D_a(r)$.*

PROOF. Consider the difference

$$D_a(r) - S_a(r) = ar^2 d\sqrt{q} \left(16q - 8\sqrt{q}a + a^2 - r^2 d \right).$$

Since a is positive $ar^2 d\sqrt{q} > 0$. Then from equation (4.28) $r^2 d \leq a^2 - 8\sqrt{q}a + 16q$, so $0 \leq a^2 - 8\sqrt{q}a + 16q - r^2 d$. Together these show that $0 \leq D_a(r) - S_a(r)$, which means $S_a(r) \leq D_a(r)$. □

Computations later will require $\sqrt{S_a(r)}$, so consider

$$\sqrt{S_a(r)} = \left| \frac{1}{4} r\sqrt{d} \right| \left| r^2 d - (16q - 8\sqrt{q}a + a^2) \right|.$$

Using equation (4.28) as before we may reason as above to say that

$$\left| r^2 d - (16q - 8\sqrt{q}a + a^2) \right| = (16q - 8\sqrt{q}a + a^2) - r^2 d.$$

Thus in later sections we will use

$$C'_<(\epsilon) q^{-\epsilon} \left(\tfrac{1}{4} r\sqrt{d} \left(16q - 8a\sqrt{q} + a^2 - r^2 d \right) \right) < \#\mathcal{I}_f \tag{4.30}$$

as a lower bound for the size of a simple isogeny class.

4.3. An Upper Bound for $\#\mathscr{A}_{q,d}$

Recall that $\mathscr{A}_{q,d} = \{A/\mathbb{F}_q \, : \, A \text{ has RM by } K^+\}$. In this section we will obtain an upper bound for $\#\mathscr{A}_{q,d}$. We will need to consider separately the simple, ordinary polarized abelian surfaces with RM by K^+, then those which are non-simple with RM by K^+, and finally any which are supersingular. These, when considered together will give the upper bound

$$\#\mathscr{A}_{q,d} < \left(\sum_{\substack{f(X)\,simple,\\ ordinary,\\ RM\,by\,K^+}} \#\mathcal{I}_f \right) + \ \#\{A \sim E^2\} \ + \ \#\{\text{supersingular } A\}.$$

Lemma 4.3.1. *For any $\epsilon > 0$ there exists a constant $C(\epsilon)$ such that*

$$\sum_{\substack{f(X)\,simple,\\ ordinary,\\ RM\,by\,K^+}} \#\mathcal{I}_f < C(\epsilon)\frac{q^{5/2+\epsilon}}{\sqrt{d}}$$

Proof. In the previous sections we determined bounds for the sizes of simple, ordinary, isogeny classes, and we follow the method used in Example 4.2.1 to bound the total number of simple, ordinary principally polarized abelian surfaces with real multiplication by K^+. We begin with a computation for an upper bound for the size of the set $\mathrm{RMI}(q,d)$. Recall because of the symmetry of the Weil region we need only count pairs (a,b) (correspondingly pairs (a,r)) with $a > 0$, and then double the result, and add in the case where $a = 0$ when necessary, i.e. when $d \equiv 2,3 \mod 4$.

Lemma 4.3.2. *[Case 1] If $d \equiv 2,3 \mod 4$, then*

$$\#RMI(q,d) \leq \frac{4q}{\sqrt{d}}.$$

Proof. Suppose $d \equiv 2, 3 \mod 4$. Then for b to be an integer it must be that a and r are both even. Let $a = 2m$ and $r = 2n$. Then (4.26) simplifies to $m^2 - n^2 d + 2q = b$ and the pair $(a, b) = (2m, m^2 - n^2 d + 2q)$ satisfies $\Delta_A^+ = r^2 d$. The bound on a bounds $m \leq 2\sqrt{q}$, and the bound on r gives $n \leq \frac{2\sqrt{q}-m}{\sqrt{d}}$. Note that if $m = 2\sqrt{q}$, then $n = 0$, which makes $r = 0$. However, when we sum $\sum_a r$, there is no contribution made to the sum when $r = 0$. Thus our sums that follow will only be counting simple abelian surfaces.

To count the relevant (a, r) pairs consider summing over positive, even a (equivalently summing over all $m \leq 2\sqrt{q}$), the number of r's (equiv. n's) that give relevant b values along that line. In particular we sum

$$\sum_{m=1}^{2\sqrt{q}} \left(\frac{2\sqrt{q} - m}{\sqrt{d}} \right) = \frac{2q - \sqrt{q}}{\sqrt{d}}. \tag{4.31}$$

This sum only counts the positive a half of the Weil region, doubling it gives the count for the nonzero portion of the Weil region:

$$\frac{4q - 2\sqrt{q}}{\sqrt{d}}. \tag{4.32}$$

Finally for $a = 0$ (equiv. $m = 0$) there are $\frac{2\sqrt{q}-0}{\sqrt{d}}$ many valid r's (equiv. n's). Adding this to equation (4.32) will give an upper bound for the number of simple isogeny class representatives (a, b) which satisfy $\Delta_A^+ = r^2 d$ with $d \equiv 2, 3 \mod 4$, i.e.

$$\#\mathrm{RMI}(q, d) \leq \frac{4q}{\sqrt{d}}. \tag{4.33}$$

□

Applying Lemma 4.3.2 to $q = 17$ and $d = 2$ we see that $\#\mathrm{RMI}(17, 2) \leq \frac{4\cdot 17}{\sqrt{2}} \approx 48.083$, which is consistent with the direct count of $\mathrm{RMI}(17, 2)$ done in Example 4.2.1 where we found $\mathrm{RMI}(17, 2) = 41$.

Lemma 4.3.3. *[Case 2] If $d \equiv 1 \mod 4$, then for $\gamma > 0$ and $q > \dfrac{1}{16\gamma^2}$,*

$$\#RMI(q, d) \leq \frac{(1 + \gamma)8q}{\sqrt{d}}.$$

Proof. Suppose $d \equiv 1 \mod 4$. Then, in this case, for b to be an integer it must be that a and r have the same parity. From Lemma 4.3.2 an upper bound is known when a and r are both even. Thus it remains to bound above the case when a and r are both odd.

Let $a = 2m + 1$ and $r = 2n + 1$. The bound $a \leq 4\sqrt{q}$ then implies $m \leq 2\sqrt{q} - \frac{1}{2} \leq 2\sqrt{q}$, and the bound for r gives the bound $n \leq \frac{4\sqrt{q}-(2m+1)}{2\sqrt{d}} - \frac{1}{2} = \frac{2\sqrt{q}-m}{\sqrt{d}} - \left(\frac{1}{2\sqrt{d}} + \frac{1}{2}\right) \leq \frac{2\sqrt{q}-m}{\sqrt{d}}$. Note: $m = 2\sqrt{q} - \left(\frac{1}{2} + \frac{\sqrt{d}}{2}\right)$ corresponds to $n = 0$, and $n = 0$ corresponds to $r = 1$. Similarly $m = 0$ corresponds to $a = 1$. Since we are computing an upper bound, we will use the same bounds here as we did in Case 1, which are less restrictive in this case.

As before consider the sum of r (equiv. n) over positive, odd a (equiv. all m):

$$\sum_{m=0}^{2\sqrt{q}} \left(\frac{2\sqrt{q} - m}{\sqrt{d}}\right) = \frac{2q + \sqrt{q}}{\sqrt{d}}.$$

This sum only accounts for the positive a half of the Weil region, doubling it gives the count for the nonzero part of the Weil region:

$$\frac{4q + 2\sqrt{q}}{\sqrt{d}}. \tag{4.34}$$

Finally to get an upper bound for Case 2, with $d \equiv 1 \mod 4$, add this term (equation (4.34)) and the upper bound from Case 1 (equation (4.33)):

$$\frac{4q+2\sqrt{q}}{\sqrt{d}} + \frac{4q}{\sqrt{d}} = \frac{8q+2\sqrt{q}}{\sqrt{d}}.$$

This value is a valid upper bound on the number of isogeny class representatives satisfying $\Delta_A^+ = r^2 d$ with $d \equiv 1 \mod 4$. However it can be improved, for q large enough, to be linear in q.

In particular, given $\gamma > 0$ if $q \geq q_0 = \dfrac{1}{16\gamma^2}$, then $\frac{8}{\sqrt{d}}q + \frac{2}{\sqrt{d}}\sqrt{q} \leq \frac{(1+\gamma)8}{\sqrt{d}}q$. Thus for $d \equiv 1 \mod 4$,

$$\#\mathrm{RMI}(q,d) \leq \frac{(1+\gamma)8q}{\sqrt{d}}.$$

□

Remark 1. *In fact, the bound above can be made independent of γ. Since there are only finitely many $q < q_0$, by assessing this finite set and the constant $(1+\gamma)$ one can determine a constant C that will work for all q.*

To conclude, we may use these upper bounds for the size of the set $\mathrm{RMI}(q,d)$ and the results from Theorem 4.1.16 for the size of a simple, ordinary isogeny class to give a bound for a portion of the upper bound for $\#\mathscr{A}_{q,d}$. For any $\epsilon' > 0$ there exist constants $C^0_>(\epsilon')$ and $C^1_>(\epsilon')$ such that

$$\text{For } d \equiv 2,3 \mod 4: \sum_{\substack{f(X)\,\text{simple},\\ \text{ordinary},\\ \text{RM by } K^+}} \#\mathcal{I}_f < \frac{4q}{\sqrt{d}} C''_>(\epsilon') \frac{32}{3\sqrt{3}} q^{3/2+\epsilon'} = C^0_>(\epsilon') \frac{q^{5/2+\epsilon'}}{\sqrt{d}}.$$

$$\text{For } d \equiv 1 \mod 4: \sum_{\substack{f(X)\,\text{simple},\\ \text{ordinary},\\ \text{RM by } K^+}} \#\mathcal{I}_f < \frac{8(C)q}{\sqrt{d}} C''_>(\epsilon') \frac{32}{3\sqrt{3}} q^{3/2+\epsilon'} = C^1_>(\epsilon') \frac{q^{5/2+\epsilon'}}{\sqrt{d}}.$$

□

To address the final two terms in the bound for $\#\mathscr{A}_{q,d}$ we cite the following lemmas.

Lemma 4.3.4 ([AH14]). *For any $\epsilon > 0$ there exists a constant $C_{split}(\epsilon)$ such that*

$$\#\{A \sim E^2\} < C_{split}(\epsilon) q^{5/2+\epsilon}.$$

Lemma 4.3.5 ([AH14]). *For any $\epsilon > 0$ there exists a constant $c(\epsilon)$ such that*

$$\#\{supersingular, A\} < c(\epsilon) q^{2+\epsilon}.$$

Now we conclude for any $\epsilon > 0$ there exists a constant $C_{>}(\epsilon)$ such that

$$\begin{aligned} \#\mathscr{A}_{q,d} &< \left(\sum_{\substack{f(X)\, simple, \\ ordinary, \\ RM\, by\, K^+}} \#\mathcal{I}_f \right) + \ \#\{A \sim E^2\} \ \ + \#\{\text{supersingular } A\} \\ &< \left(C(\epsilon) \frac{q^{5/2+\epsilon}}{\sqrt{d}} \right) \quad\quad + \ C_{split}(\epsilon) q^{5/2+\epsilon} + c(\epsilon) q^{2+\epsilon} \\ &< C_{>}(\epsilon) q^{5/2+\epsilon}. \end{aligned} \tag{4.35}$$

4.4. A Lower Bound for $\#\mathscr{A}_{q,d}$

In this section to make things a bit easier we make the assumption that p is inert in K^+ so that we may use Lemma 4.1.3 and only consider the ordinary and supersingular abelian surfaces. To determine a lower bound for the number of abelian surfaces A with real multiplication by K^+ a slightly different technique will be used. Rather than first bounding the size of the set $\mathrm{RMI}(q, d)$, and then using bounds for the size of an isogeny classes, a count will be done directly to compute a lower bound by considering isogeny class representatives and the size of their respective isogeny class sizes in tandem. In this case we will get a lower bound by summing over all (a, b) that are relevant and then subtract out the terms that correspond to supersingular abelian surfaces since we only know that the function $D(a, b)$ approximates the size of simple, ordinary isogeny classes. Thus we compute

$$\left(\sum_{\substack{f(X)\,simple,\\ ordinary,\\ RM\,by\,K^+}} \#\mathcal{I}_f \right) - \left(\sum_{\substack{supersingular\\ f(X)}} \#\mathcal{I}_f \right) < \#\mathscr{A}_{q,d}.$$

Recall the lower bound for the size of an isogeny class given in equation (4.30). Consider summing this lower bound over valid (a, b) isogeny class representatives (resp. (a, r) pairs) in the Weil region. This is similar to what was done in the upper bound case except one value, namely $C''_>(\epsilon)\dfrac{32}{3\sqrt{3}}q^{3/2+\epsilon}$, was used for the maximum size of all isogeny classes. As before we must consider the two cases, $d \equiv 2, 3 \mod 4$ and $d \equiv 1 \mod 4$ separately.

Lemma 4.4.1. *[Case 1] If $d \equiv 2, 3 \mod 4$, then for any $\epsilon > 0$ there exists a constant $C^0_<(\epsilon, \beta)$ such that*

$$C^0_<(\epsilon)\frac{q^{5/2-\epsilon}}{\sqrt{d}} < \#\mathscr{A}_{q,d}.$$

Proof. Let $a = 2m$ and $r = 2n$ both be even. Now in terms of m and n, $\sqrt{S_a(r)}$ can be written as

$$\sqrt{S_a(r)} = \sqrt{S_m(n)} = 2n\sqrt{d}\left(4q - 4m\sqrt{q} + m^2 - n^2 d\right).$$

In the following sums we factor out the $C'(\epsilon)q^{-\epsilon}$ term used in the lower bound for the size of an isogeny class, and multiply it back in once the sums have been computed.

Now consider the sum of $\sqrt{S_m(n)}$ over n for fixed m:

$$\begin{aligned}\sum_{n=1}^{\frac{2\sqrt{q}-m}{\sqrt{d}}} \sqrt{S_m(n)} &= \sum_{n=1}^{\frac{2\sqrt{q}-m}{\sqrt{d}}} \left(2n\sqrt{d}\left(4q-4m\sqrt{q}+m^2-n^2d\right)\right) \\ &= \frac{8q^2}{\sqrt{d}} - \frac{16m}{\sqrt{d}}q^{3/2} + \left(-2\sqrt{d}+\frac{12m^2}{\sqrt{d}}\right)q + \left(2m\sqrt{d}-\frac{4m^3}{\sqrt{d}}\right)\sqrt{q} + \frac{m^4-m^2d}{2\sqrt{d}} \qquad (4.36) \\ &= t(m).\end{aligned}$$

Thus along each a line a contribution of (4.36) is made toward $\#\mathscr{A}_{q,d}$. Now we wish to sum $t(m)$ over all $1 \le m \le 2\sqrt{q}$ which are relatively prime to p. This will effectively count the number of non-supersingular abelian surfaces with real multiplication by K^+. Recall by Lemma 4.1.3, if we assume that p is inert in K^+ then non-supersingular is ordinary, and the condition that $p \nmid a$ makes (a,b) a representative of an ordinary isogeny class.

We compute this sum as follows

$$\sum_{\substack{m=1\\ p\nmid m}}^{2\sqrt{q}} t(m) = \sum_{m=1}^{2\sqrt{q}} t(m) - \sum_{\substack{m=1\\ p\mid m}}^{2\sqrt{q}} t(m). \qquad (4.37)$$

Now for the last term, write $m = pj$, then we will sum over $j = 1$ to $2\sqrt{q}/p$. In particular we sum

$$\begin{aligned}\sum_{\substack{m=1\\ p\nmid m}}^{2\sqrt{q}} t(m) &= \sum_{m=1}^{2\sqrt{q}} t(m) - \sum_{j=1}^{2\sqrt{q}/p} t(pj) \\ &= \left[\frac{16}{5\sqrt{d}}q^{5/2} - \frac{4q^2}{\sqrt{d}} + \left(\frac{4}{3\sqrt{d}} - \frac{4\sqrt{d}}{3}\right)q^{3/2} + \sqrt{d}q - \left(\frac{1}{30\sqrt{d}} + \frac{\sqrt{d}}{6}\right)\sqrt{q}\right] - \\ &\qquad \left[\frac{16}{p5\sqrt{d}}q^{5/2} - \frac{4q^2}{\sqrt{d}} + \left(\frac{4p}{3\sqrt{d}} - \frac{4\sqrt{d}}{3p}\right)q^{3/2} + \sqrt{d}q - \left(\frac{p^3}{30\sqrt{d}} + \frac{p\sqrt{d}}{6}\right)\sqrt{q}\right] \\ &= \frac{16}{5\sqrt{d}}\left(1-\frac{1}{p}\right)q^{5/2} + \frac{4}{3\sqrt{d}}\left(1+\frac{d}{p}-d-p\right)q^{3/2} + \frac{(p^3+5dp-5d-1)}{30\sqrt{d}}\sqrt{q}. \qquad (4.38)\end{aligned}$$

This sum accounts for the total number of ordinary principally polarized abelian surfaces with coefficient $a > 0$. Observe that if $p > 1$ then $p^3 + 5dp - 5d - 1 > 0$, thus to get an even smaller lower bound, we may simply drop the $\sqrt{q}$ term. Then, as before, this must be doubled for the symmetry of the Weil region to get the total number of ordinary, principally polarized abelian surfaces with real multiplication by K^+ and coefficient $a \neq 0$. To get the number of pairs with $a = 0$, (resp. $m = 0$), compute $t(0) = \left(8q^2/\sqrt{d}\right) - 2q\sqrt{d}$. Taken together, we can say that the total number of ordinary, principally polarized abelian surfaces with real multiplication by K^+ is bound below by

$$\frac{32}{5\sqrt{d}}\left(1-\frac{1}{p}\right)q^{5/2} + \frac{8}{3\sqrt{d}}\left(1+\frac{d}{p}-d-p\right)q^{3/2} + \frac{8}{\sqrt{d}}q^2 - 2q\sqrt{d} < \#\mathscr{A}_{q,d}. \tag{4.39}$$

Two things to note here so that we may obtain an even smaller lower bound: (i) $8q^2/\sqrt{d} > 0$, so we may drop this term to get a smaller bound; (ii) $(1-(1/p)) \geq 1/2$ for all $p \geq 2$. Thus

$$\frac{32}{5\sqrt{d}}\left(\frac{1}{2}\right)q^{5/2} + \frac{8}{3\sqrt{d}}\left(1+\frac{d}{p}-d-p\right)q^{3/2} - 2q\sqrt{d} < \#\mathscr{A}_{q,d} \tag{4.40}$$

is an even smaller lower bound for $\#\mathscr{A}_{q,d}$. Finally, recall the constant $C'_<(\epsilon)q^{-\epsilon}$, then a lower bound for $\#\mathscr{A}_{q,d}$ is:

$$\left(\frac{32}{5\sqrt{d}}\left(\frac{1}{2}\right)q^{5/2} + \frac{8}{3\sqrt{d}}\left(1+\frac{d}{p}-d-p\right)q^{3/2} - 2q\sqrt{d}\right)C'_<(\epsilon)q^{-\epsilon} < \#\mathscr{A}_{q,d}. \tag{4.41}$$

Consider now

$$\lim_{q\to\infty}\frac{C'_<(\epsilon)\dfrac{16}{5\sqrt{d}}q^{5/2-\epsilon} + \dfrac{C'_<(\epsilon)8}{3\sqrt{d}}\left(1+\frac{d}{p}-d-p\right)q^{3/2-\epsilon} - C'_<(\epsilon)2\sqrt{d}q^{1-\epsilon}}{\dfrac{q^{5/2-\epsilon}}{\sqrt{d}}} = \frac{C'_<(\epsilon)16}{5} > 0.$$

This means, asymptotically a lower bound for $\#\mathscr{A}_{q,d}$ grows like $\frac{C'_<(\epsilon)16}{5\sqrt{d}}q^{5/2-\epsilon}$.

Remark 2. *In fact, for any $0 < \beta < 1$ if $q > q_{\beta,d}$, then*

$$(1-\beta)Wq^{5/2-\epsilon} < Wq^{5/2-\epsilon} + Yq^{3/2-\epsilon} - Zq^{1/2-\epsilon},$$

where $W = \dfrac{C'_<(\epsilon)16}{5\sqrt{d}}$, $Y = \dfrac{C'_<(\epsilon)8\left(1+\frac{d}{p}-d-p\right)}{3\sqrt{d}}$, $Z = C'_<(\epsilon)2\sqrt{d}$ *are the coefficients from equation* (4.41).

Thus if $d \equiv 2, 3 \mod 4$, then for any $\epsilon > 0$, $0 < \beta < 1$, and $q > q_{\beta,d}$ there exists a constant $C^0_<(\epsilon, \beta)$ such that

$$\frac{C'_<(\epsilon)(1-\beta)16}{5\sqrt{d}} q^{5/2-\epsilon} = C^0_<(\epsilon,\beta)\frac{q^{5/2-\epsilon}}{\sqrt{d}} < \#\mathscr{A}_{q,d}. \tag{4.42}$$

As mentioned in Remark 1 by considering the finitely many $q < q_{\beta,d}$ a constant independent of β and d can be determined. □

Lemma 4.4.2 (Case 2). *If $d \equiv 1 \mod 4$, then for any $\epsilon > 0$ there exists a constant $C^1_<(\epsilon)$ such that*

$$C^1_<(\epsilon)\frac{q^{5/2-\epsilon}}{\sqrt{d}} < \#\mathscr{A}_{q,d}.$$

Proof. Since Case 1 (where a and r are both even) is a subset of Case 2 (where a and r are required to have the same parity), we may claim that the lower bound given for Case 1, is also a sufficient lower bound for Case 2.

So in the case where $d \equiv 1 \mod 4$, then for any $\epsilon > 0$ there exists a constant $C^1_<(\epsilon)$ such that

$$C^1_<(\epsilon)\frac{q^{5/2-\epsilon}}{\sqrt{d}} < \#\mathscr{A}_{q,d}.$$

□

4.5. Proof of Theorem 4.0.1

The results of the previous sections may be summarized as follows. Assuming p is inert in K^+, then for any $\epsilon > 0$ there exist constants $C^0_<(\epsilon)$ and $C^1_>(\epsilon)$ such that

$$\begin{aligned} &\text{For } d \equiv 2,3 \mod 4: \ C^0_<(\epsilon)\frac{q^{5/2-\epsilon}}{\sqrt{d}} < \#\mathscr{A}_{q,d} < C^0_>(\epsilon)\frac{q^{5/2+\epsilon}}{\sqrt{d}}; \\ &\text{For } d \equiv 1 \mod 4: \ C^1_<(\epsilon)\frac{q^{5/2-\epsilon}}{\sqrt{d}} < \#\mathscr{A}_{q,d} < C^1_>(\epsilon)\frac{q^{5/2+\epsilon}}{\sqrt{d}}; \end{aligned}$$

thus proving Theorem 4.0.1.

4.6. Heuristics for a Lang-Trotter Conjecture for Abelian Surfaces

Similar to the comments made following Conjecture 2.2.1 one can now argue heuristically for a Lang-Trotter-like conjecture for abelian surfaces. First, since the dimension of $\mathcal{A}_g$ is equal to $\frac{g(g+1)}{2}$, the dimension of $\mathcal{A}_2$ is 3, and there are approximately q^3 abelian surfaces defined over $\mathbb{F}_q$. Now given that Theorem 4.0.1 gave upper and lower bounds for the number of principally polarized abelian surfaces with real multiplication by $\mathbb{Q}(\sqrt{d})$ to be on the order of $q^{5/2}$ one can approximate the probability that a randomly chosen abelian surface defined over $\mathbb{F}_q$ has real multiplication by K^+ to be $\approx \frac{cq^{5/2}}{q^3} = \frac{c}{\sqrt{q}}$. Now suppose $q = p$ and define

$$N_{A,K^+}(x) = \#\{p \leq x \, : \, p \text{ is prime and } A_p \text{ has RM by } K^+\},$$

then

$$\begin{aligned} N_{A,K^+}(x) &\approx \sum_{p \leq x} \text{Prob(random} A/\mathbb{F}_p \text{ has RM by } K^+) \\ &= \sum_{p \leq x} \frac{c}{\sqrt{p}}. \end{aligned}$$

As before, rather than summing only over primes less than x use the prime number theorem to sum over all integers less than x:

$$\sum_{n\leq x}\frac{c}{\sqrt{n}\log(n)}\approx\int_2^x\frac{c}{\sqrt{z}\log(z)}\,dz\approx\frac{C\sqrt{x}}{\log(x)}.$$

Thus given these heuristics we make the following conjecture:

Conjecture 4.6.1. *Let A be an abelian surface defined over $\mathbb{Q}$ with $End_{\overline{\mathbb{Q}}}(A)\cong\mathbb{Z}$ and let K^+ be a given real quadratic extension of $\mathbb{Q}$. Define $N_{A,K^+}(x)$ as above. Then there exists a constant $C(A,K^+)>0$ such that*

$$N_{A,K^+}(x)\approx C(A,K^+)\frac{\sqrt{x}}{\log(x)}.$$

In the following chapter we will explore the matrix group $\mathrm{GSp}_4(\mathbb{Z}/\ell)$ in order to gain understanding about the matrices which correspond to the Frobenius endomorphism Frob_p of an abelian surface $A_p/\mathbb{F}_p$. Specifically we will be looking for matrices with characteristic polynomials which correspond to an abelian surface with real multiplication by K^+. The information learned here will then be used as input for a large sieve calculation to give bounds for $N_{A,K^+}(x)$.

CHAPTER 5

Abelian Surfaces and Random Matrices

Recall from Chapter 3 the connection between an abelian surface over $\mathbb{F}_q$, the Frobenius endomorphism Frob_q, the matrix group $\mathrm{GSp}_4(\mathbb{Z}/\ell)$, the characteristic polynomial of Frobenius and the discriminant of the real quadratic subfield of $\mathrm{End}^0(A)$. Here specifically we consider, given an abelian surface $A_p/\mathbb{F}_p$ the action of Frob_p on the $\ell-$torsion points of A_p. This can be represented as a matrix in $\mathrm{GSp}_4(\mathbb{Z}/\ell)$. From this matrix representation we obtain the characteristic polynomial of Frobenius, $f_{A_P}(X)$, whose coefficients then determine the discriminant of the real quadratic subfield inside the endomorphism algebra of A_p. In this chapter we explore what it means for a matrix $\gamma \in \mathrm{GSp}_4(\mathbb{Z}/\ell)$ and its characteristic polynomial $f_\gamma(X)$, to be compatible with abelian surface $A_p/\mathbb{F}_p$ with real multiplication by a fixed totally real quadratic field K^+.

In the first few sections we begin by developing some background on groups of Lie type and specifically the group $\mathrm{GSp}_4(\mathbb{Z}/\ell)$. From there we define a compatibility condition for a matrix to be compatible with real multiplication by K^+. Finally, we assess the group $\mathrm{GSp}_4(\mathbb{Z}/\ell)$ and determine how the matrices in the group satisfy the compatibility condition.

5.1. Background: Algebraic Groups, Tori, and The Weyl Group

Much of the background given in this section comes from Carter [Car85]. Let k be a field, then an algebraic group G over k is an algebraic variety over k. There are maps $G \times G \to G$ and $G \to G$ which turn the set of points $G(L)$ into a group for each extension L/k. Suppose that G is a connected linear group. An element $M \in G(k)$ is said to be *semisimple* if M is diagonalizable over $\overline{k}$. A smooth connected algebraic group of multiplicative type is called a *torus*. A *split torus* is a smooth connected diagonalizable algebraic group [Mil12]. Call a torus *maximal* if it is not contained in any other torus. An element $M \in G(k)$ is said to be *regular* if the dimension of its centralizer in G is the same as the dimension of the maximal tori of G. The following lemma tells us that most of the matrices $M \in G(k)$ are regular and semisimple.

Lemma 5.1.1. *[[Bor91]] Let G be an algebraic group and let $G^{r,ss}$ denote the locus of regular, semisimple elements of G, then $G^{r,ss}$ is open and dense in G.*

In particular this tells us that there exists a constant C_G, dependent only on G such that, for each ℓ,

$$1 > \frac{\# G^{r,ss}(\mathbb{F}_\ell)}{\# G(\mathbb{F}_\ell)} > 1 - \frac{C_G}{\sqrt{\ell}}.$$

For the remainder of this section let us specialize our discussion to a group G which is connected, reductive, and split. Since G is split, G contains a maximal torus which is split; and since G is connected and reductive, for any maximal torus T, the centralizer of T in G, denoted by $C(T)$, is in fact equal to T. Let $N(T)$ be the normalizer of T in G. Now define $W(T) = N(T)/C(T) = N(T)/T$ to be the *Weyl group* of T. This is a finite group. In the group G all split maximal tori are conjugate, so the Weyl group is uniquely determined up to isomorphism.

Consider G defined over $\overline{\mathbb{F}_p}$. Then G is isomorphic to a closed subgroup of GL_n for some n. Let $q = p^r$, $r \geq 1$, then there exists a map $F_q : \mathrm{GL}_n \to \mathrm{GL}_n$, which on points acts as

$$F_q : (a_{ij}) \to \left(a_{ij}^q\right).$$

This map is in fact a homomorphism of GL_n into itself. A homomorphism $F : G \to G$ is considered a *standard Frobenius map* if there exists an injective homomorphism $\iota : G \to \mathrm{GL}_n$

for some n, such that

$$\iota(F(g)) = F_q(\iota(g)), \quad \text{for some } q = p^r \text{ and all } g \in G(\mathbb{F}_p).$$

Furthermore F is called a *Frobenius map* if some power of F is a standard Frobenius map. Any Frobenius map $F : G \to G$ is bijective.

The choice of a Frobenius map F, induces an $\mathbb{F}_q-$structure on G such that under this structure the $\mathbb{F}_q$ points of G are exactly the $\overline{\mathbb{F}_p}-$points which are fixed by F. Explicitly we have

$$G(\mathbb{F}_q) = G^F(\mathbb{F}_q) = \{g \in G(\overline{\mathbb{F}_p}) \,:\, F(g) = g\}.$$

This group G^F is a finite subgroup of G [[Car85]]. The maximal tori of G^F are the $F-$stable maximal tori of G. The set of $F-$stable maximal tori of G fall into conjugacy classes under the action of $G^F(\mathbb{F}_q)$. Since all tori in $G/\overline{\mathbb{F}_p}$ are conjugate, for each maximal torus T of G^F, there exists $g \in G(\overline{\mathbb{F}_p})$ such that $T = {}^gT_0 = gT_0g^{-1}$.

The following proposition of Carter gives a way of determining the maximal tori of G^F.

Proposition 5.1.1 ([Car85], Theorem 3.3.1). *The torus ${}^gT_0$ is $F-$stable if and only if $g^{-1}F(g) \in N_0 = N(T_0)$.*

Before stating the next two propositions, recall that G is split and T_0 is a maximally split torus of G. This means the action of F on $W_0 = N_0/T_0$ is trivial and $F-$conjugacy is just the usual conjugacy on W_0. Thus we will refer to $F-$conjugacy on W_0 as simply conjugacy. Now the following propositions determine a bijection between G^F-classes of $F-$stable maximal tori of G and the conjugacy classes of W_0. Proposition 5.1.2 defines an equivalence relation on W_0, and Proposition 5.1.3 defines the bijection. Let $\pi : N_0 \to W_0$ be the natural projection map.

Proposition 5.1.2. *[[Car85], Theorem 3.3.2] Suppose* ${}^gT_0 = {}^hT_0$ *is* $F-$*stable. Let* $\pi(g^{-1}F(g)) = w$ *and* $\pi(h^{-1}F(h)) = w'$. *Then there exists* $x \in W_0$ *such that* $w' = x^{-1}wx$.

Proposition 5.1.3. *[[Car85], Theorem 3.3.3] The map* ${}^gT_0 \to \pi(g^{-1}F(g))$ *determines a bijection between the* G^F-*classes of* $F-$*stable maximal tori of* G *and the conjugacy classes of* W_0.

If $w, w' \in W_0$ differ as in Proposition 5.1.2 we say they are conjugate. For T an $F-$stable maximal torus of G and w an element of the corresponding conjugacy class of W_0, we say that T is obtained from the maximally split torus T_0 by twisting with w.

Since the conjugacy classes of W_0 are in bijection with the maximal tori of G^F, it will be advantageous to explore the Weyl group W_0. Moreover, the structure of the conjugacy classes of W_0 determines the Weyl groups of the other maximal tori of G^F as described by the following proposition.

Proposition 5.1.4. *[[Car85], Theorem 3.3.6] Let* T *be an* $F-$*stable maximal torus of* G *obtained from the maximally split torus* T_0 *by twisting with* w. *Let* N *be the normalizer of* T. *Then* $W(T) = N^F/T^F$ *is isomorphic to the set* $C_{W_0,F}(w) = \{x \in W_0 : x^{-1}wx = w\}$.

The set $C_{W_0,F}(w)$ is a subgroup of W_0 and is called the *centralizer* of $w \in W_0$. This group has the property that the index $[W_0 : C_{W_0,F}(w)]$ is the number of elements in the conjugacy class containing w. The isomorphism implies that by computing $C_{W_0,F}(w)$ and determining its size, we will have determined the size of $W(T) = N^F/T^F$, the Weyl group of the torus T obtained by twisting with w.

We will specifically be interested in the Weyl group of the maximal split torus of the group $\mathrm{GSp}_4(\mathbb{Z}/\ell)$. But before we delve into those specifics, let us first review some facts about the group $\mathrm{GSp}_{2g}(R)$ in general.

5.2. The Group $\mathrm{GSp}_{2g}(R)$

Let R be a ring and V a $2g-$dimensional vector space over R. Define the $2g \times 2g$ matrix

$$J = \begin{pmatrix} 0 & I_g \\ -I_g & 0 \end{pmatrix}$$

where I_g is the $g \times g$ identity matrix. Given $\mathbf{x}, \mathbf{y} \in V$, the map

$$\langle \cdot, \cdot \rangle : V \times V \to R; \qquad \langle \mathbf{x}, \mathbf{y} \rangle \mapsto \mathbf{x}^T J \mathbf{y}$$

defines a skew-symmetric bilinear form on V (also called a *pairing*). Let M^T denote the transpose of the matrix M. Then we have the following definitions for the groups $\mathrm{Sp}_{2g}(R)$ the symplectic group, and $\mathrm{GSp}_{2g}(R)$ the general symplectic group.

$$\mathrm{Sp}_{2g}(R) = \{\gamma \in \mathrm{GL}_{2g}(R) \,:\, \langle \gamma\mathbf{x}, \gamma\mathbf{y} \rangle = \langle \mathbf{x}, \mathbf{y} \rangle\} = \{\gamma \in \mathrm{GL}_{2g}(R) \,:\, \gamma^T J \gamma = J\}$$

$$\begin{aligned} \text{and } \ \mathrm{GSp}_{2g}(R) &= \{\gamma \in \mathrm{GL}_{2g}(R) \,:\, \exists m \in R^* \text{ s.t. } \langle \gamma\mathbf{x}, \gamma\mathbf{y} \rangle = m\langle \mathbf{x}, \mathbf{y} \rangle\} \\ &= \{\gamma \in \mathrm{GL}_{2g}(R) \,:\, \exists m \in R^* \text{ s.t. } \gamma^T J \gamma = mJ\}. \end{aligned}$$

In $\mathrm{GSp}_{2g}(R)$ the value m is called the *multiplier* of the matrix γ.

Equivalently one can define $\mathrm{GSp}_{2g}(R)$ by considering a block matrix

$$\gamma = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$$

where $A, B, C, D \in \mathrm{Mat}_g(R)$. Then $\gamma \in \mathrm{GSp}_{2g}(R)$ if and only if

$$A^T C = C^T A, \qquad B^T D = D^T B, \qquad \text{and} \qquad A^T D - C^T B = mI,$$

for some $m \in R^*$.

Let us now specialize to the case where $G = \mathrm{GSp}_4(\mathbb{Z}/\ell)$, and consider the maximal, split torus T_0 which consists of matrices of the form

$$\begin{pmatrix} x_1 & 0 & 0 & 0 \\ 0 & x_2 & 0 & 0 \\ 0 & 0 & m/x_1 & 0 \\ 0 & 0 & 0 & m/x_2 \end{pmatrix}$$

where $x_i, m \in (\mathbb{Z}/\ell)^*$ and m is the multiplier of γ, so that $\gamma^T J \gamma = mJ$.

Then all other maximal tori of G^F are of the form ${}^gT_0$ for some $g \in G$, and by Proposition 5.1.3 these G^F- classes of $F-$stable maximal tori are in bijection with the conjugacy classes of $W_0 = N_0/T_0$. In the next section we explore the Weyl group of this maximally split torus in $\mathrm{GSp}_4(\mathbb{Z}/\ell)$.

5.2.1. The Weyl Group of the Maximally Split Torus. Let T_0 be the maximal, split torus of $G = \mathrm{GSp}_4(\mathbb{Z}/\ell)$, as above, let N_0 be the normalizer of T_0 and $W_0 = N_0/T_0$ be its Weyl group. Given the simple structure of T_0, the elements of W_0 can act on T_0 in the following ways: (i) swap entries $x_1 \leftrightarrow \frac{m}{x_1}$, (ii) swap entries $x_2 \leftrightarrow \frac{m}{x_2}$, (iii) swap both $x_i \leftrightarrow \frac{m}{x_i}$ or (iv) by permuting the indices $x_1 \leftrightarrow x_2$ and $\frac{m}{x_1} \leftrightarrow \frac{m}{x_2}$. Given these actions, one can see that W_0 is the wreath product of $\mathbb{Z}/2$ by S_2, denoted as $\mathbb{Z}/2 \wr S_2$. This group has order 8, and is in fact isomorphic to D_4.

By indexing the coordinates of W_0 by first the two copies of $\mathbb{Z}/2$ (the first copy acting on $\{x_1, \frac{m}{x_1}\}$ and the second copy acting on $\{x_2, \frac{m}{x_2}\}$) and the last coordinate by S_2 (the permutation of the indices $(1 \leftrightarrow 2)$), the elements of W_0 are as follows, where s is the element in $\mathbb{Z}/2$ which swaps $x_i \leftrightarrow \frac{m}{x_i}$ for the appropriate coordinate.

$$W_0 = \{(id, id, ()), (id, id, (12)), (id, s, ()), (id, s, (12)),$$
$$(s, id, ()), (s, id, (12)), (s, s, ()), (s, s, (12))\}.$$

Now that we have a description of W_0 and Proposition 5.1.4 we can use the computer program GAP to compute the conjugacy classes of W_0, hence computing the Weyl groups of the other maximal tori of G^F. The results are five distinct conjugacy classes in W_0, with representatives: $(id, id, ())$, $(id, s, ())$, $(s, s, ())$, $(id, id, (12))$, and $(id, s, (12))$. In Section 5.5 we will explicitly determine the correspondence between these five conjugacy classes and the G^F-classes of $F-$stable maximal tori of G, as described in Proposition 5.1.3.

Before determining the correspondence, we will first approximate the size of a torus in order to determine the probability that a random regular semisimple element $g \in G^F$ is conjugate to some element of that particular torus. We will see that the size of the Weyl group plays a special role in determining the size of a torus; and we will thus use Proposition 5.1.4 to help compute the size of each Weyl group.

5.3. The Size of a Torus

In this section, let us continue with G, a split, reductive, connected group, with the choice of a Frobenius F, so that it has an inherent $\mathbb{F}_q-$structure. Recall that $G(\mathbb{F}_q) = \{g \in G(\overline{\mathbb{F}_p}) : F(g) = g\}$. Let T be an $F-$stable torus, and let $T_{\text{reg}} := \{t \in T(\mathbb{F}_q) : t \text{ is a regular element of } T(\mathbb{F}_q)\}$. Now, in order to approximate the size T we will approximate the number of $g \in G(\mathbb{F}_q)$ which are conjugate ($\sim$) to some element $t \in T_{\text{reg}}$. Recall that an element $g \in G$ is said to be *regular* if the dimension of its centralizer in G is the same as the dimension of the maximal tori of G. Since the regular semisimple elements of

g form an open set in G (Lemma 5.1.1), let us consider only $g \in G$ which are regular and semisimple. For such an element, $g \in G$, then there exists a unique maximal torus in which it is contained [Car85]. We use these two facts to approximate the number of regular elements of $G(\mathbb{F}_q)$ that are conjugate to an element of T to obtain an approximation for the size of T.

Fix $t \in T_{\text{reg}}$ and consider the set $\{g \in G(\mathbb{F}_q) \,:\, g \sim t\}$ which has size $\#G(\mathbb{F}_q)/\#C_G(t)(\mathbb{F}_q)$. Since t is regular, then $C_G(t)(\mathbb{F}_q) = T(\mathbb{F}_q)$, and one might expect the number of elements in $G(\mathbb{F}_q)$ which are conjugate to some element of T to be

$$\sum_{t \in T_{\text{reg}}} \#G(\mathbb{F}_q)/\#C_G(t)(\mathbb{F}_q) = \sum_{t \in T_{reg}} \#G(\mathbb{F}_q)/\#T(\mathbb{F}_q) = \#T_{reg} \cdot (\#G(\mathbb{F}_q)/\#T(\mathbb{F}_q)) \,.$$

However this over counts, because there could be some $s \in T(\mathbb{F}_q)$ such that s is conjugate to t. If s is conjugate to t, then they are conjugate by an element of W_T, so the number of $s \in T(\mathbb{F}_q)$ which are conjugate to t is equal to the size of the Weyl group, $\#W_T$.

Thus the size of the torus T is approximately

$$\#T_{reg} \cdot \frac{\#G(\mathbb{F}_q)}{\#T(\mathbb{F}_q)} \cdot (1/\#W_T) \,.$$

By Lemma 5.1.1, we can say that there exists a constant $c_T > 0$ such that

$$1 > \frac{\#T_{\text{reg}}}{\#T(\mathbb{F}_q)} > 1 - \frac{c_T}{\sqrt{q}},$$

and we may bound the size of the a torus by

$$\#G(\mathbb{F}_q)/\#W_T > \#T(\mathbb{F}_q) > (\#G(\mathbb{F}_q)/\#W_T)\left(1 - \frac{c_T}{\sqrt{q}}\right) .$$

Letting $\delta_T = \frac{c_T}{\sqrt{q}} > 0$ then, one expects that a randomly selected element of $G(\mathbb{F}_q)$ will land in a specific $F-$stable torus, T, approximately $\#T(\mathbb{F}_q)/\#G(\mathbb{F}_q)$ of the time, which can be bound by

$$\frac{1}{\#W_T} > \frac{\#T(\mathbb{F}_q)}{\#G(\mathbb{F}_q)} > \frac{1}{\#W_T}\left(1-\delta_T\right). \tag{5.1}$$

5.4. Relating Random Matrices and Abelian Surfaces with Real Multiplication

Now that we have some information about the matrices in the group $\mathrm{GSp}_4(\mathbb{Z}/\ell)$, we wish to explore what it means for a matrix $\gamma \in \mathrm{GSp}_4(\mathbb{Z}/\ell)$ to be compatible with an abelian surface with real multiplication by $K^+ = \mathbb{Q}(\sqrt{d})$. The first observation to be made here is that if A is an abelian surface defined over $\mathbb{Q}$ with $\mathrm{End}_{\overline{\mathbb{Q}}}(A) \cong \mathbb{Z}$, then for a fixed prime ℓ the reduction of $A \mod p \equiv A_p/\mathbb{F}_p$ has Frobenius endomorphism whose image is equidistributed in $\mathrm{GSp}_4(\mathbb{Z}/\ell)$ as p ranges over primes of good reduction, $p \neq \ell$. This means that if we can determine how a random matrix in $\mathrm{GSp}_4(\mathbb{Z}/\ell)$ behaves, then the matrix corresponding to Frob_p will likely behave the same way.

To begin, consider an element $\gamma \in \mathrm{GSp}_4(\mathbb{Z}/\ell)$ with characteristic polynomial $f_\gamma(X) = X^4 - aX^3 + bX^2 - amX + m^2$ where m is the multiplier of the matrix. Define $\overline{\gamma} = m\gamma^{-1}$. This is also a matrix in $\mathrm{GSp}_4(\mathbb{Z}/\ell)$ with multiplier m. The following lemma defines a quadratic polynomial $f_\gamma^+(X)$ that has discriminant $\Delta_\gamma^+ = a^2 - 4b + 8m$, where a and b are the same coefficients as in the polynomial $f_\gamma(X)$.

Lemma 5.4.1. *Given definitions as above*

$$f_{\gamma+\overline{\gamma}}(X) = \left(f_\gamma^+(X)\right)^2.$$

Proof. First we note that it is enough to prove this for a matrix group over an algebraically closed field F, and second that it is enough to prove this for semisimple matrices (by Lemma 5.1.1). Given these reductions we can assume γ and $\overline{\gamma}$ are of the form

$$\gamma = \begin{pmatrix} \alpha_1 & 0 & 0 & 0 \\ 0 & \alpha_2 & 0 & 0 \\ 0 & 0 & m/\alpha_1 & 0 \\ 0 & 0 & 0 & m/\alpha_2 \end{pmatrix}, \text{ and } \overline{\gamma} = \begin{pmatrix} m/\alpha_1 & 0 & 0 & 0 \\ 0 & m/\alpha_2 & 0 & 0 \\ 0 & 0 & \alpha_1 & 0 \\ 0 & 0 & 0 & \alpha_2 \end{pmatrix}.$$

Then

$$\gamma + \overline{\gamma} = \begin{pmatrix} \alpha_1 + (m/\alpha_1) & 0 & 0 & 0 \\ 0 & \alpha_2 + (m/\alpha_2) & 0 & 0 \\ 0 & 0 & (m/\alpha_1) + \alpha_1 & 0 \\ 0 & 0 & 0 & (m/\alpha_2) + \alpha_2 \end{pmatrix},$$

and it is easy to see that the characteristic polynomial of $\gamma + \overline{\gamma}$ is

$$\begin{aligned} f_{\gamma+\overline{\gamma}}(X) &= \left(X - \left(\alpha_1 + \tfrac{m}{a_1}\right)\right)^2 \left(X - \left(\alpha_2 + \tfrac{m}{\alpha_2}\right)\right)^2 \\ &= \left(X^2 - \left(\alpha_1 + \tfrac{m}{\alpha_1} + \alpha_2 + \tfrac{m}{\alpha_2}\right) X + \left(\alpha_1 + \tfrac{m}{\alpha_1}\right)\left(\alpha_2 + \tfrac{m}{\alpha_2}\right)\right)^2. \end{aligned}$$

The characteristic polynomial of γ is

$$\begin{aligned} f_\gamma(X) &= (X-\alpha_1)(X-\alpha_2)(X-\tfrac{m}{\alpha_1})(X-\tfrac{m}{\alpha_2}) \\ &= X^4 - \left(\alpha_1 + \alpha_2 + \tfrac{m}{\alpha_1} + \tfrac{m}{\alpha_2}\right) X^3 + \left(\tfrac{m^2}{\alpha_1\alpha_2} + \alpha_1\alpha_2 + (\alpha_1+\alpha_2)\left(\tfrac{m}{\alpha_1} + \tfrac{m}{\alpha_2}\right)\right) X^2 \\ &\quad - m\left(\alpha_1 + \alpha_2 + \tfrac{m}{\alpha_1} + \tfrac{m}{\alpha_2}\right) X + m^2 \\ &= X^4 - aX^3 + bX^2 - amX + m^2. \end{aligned}$$

Inspection of the coefficients here shows that $f_\gamma^+(X) = \sqrt{f_{\gamma+\overline{\gamma}}(X)}$ can be written as $f_\gamma^+(X) = X^2 - aX + b - 2m$, where a and b are the coefficients of $f_\gamma(X)$. □

For the remainder of the paper we will let $f_\gamma^+(X) = X^2 - aX + b - 2m$, as defined in Lemma 5.4.1, and will refer to this as *the real characteristic polynomial* of the matrix γ. Also let the discriminant of $f_\gamma^+(X)$ be denoted by $\Delta_\gamma^+ = a^2 - 4b + 8m$.

Given the definition of the real characteristic polynomial we have the tools to discuss compatibility requirements for real multiplication by K^+. Let A_p be an abelian surface defined over $\mathbb{F}_p$ for some prime p. Then for each prime $\ell \neq p$ consider the map $\rho_\ell : \mathrm{End}^0(A_p) \to \mathrm{GSp}_4(\mathbb{Z}/\ell)$ which maps an endomorphism of A_p to its matrix representation. For the Frobenius endomorphism Frob_p, denote its characteristic polynomial by $f_{A_p}(X)$ and the corresponding real characteristic polynomial by $f_{A_p}^+(X)$.

Lemma 5.4.2 (compat(p, d, ℓ)). *If A_p has real multiplication by K^+, the following are equivalent.*

(1) The polynomial $f_{A_p}^+(X)$ splits in $(\mathbb{Z}/\ell)[X]$.

(2) The discriminant of $f_{A_p}^+(X)$ is congruent to a square modulo ℓ.

(3) The prime ℓ splits in K^+.

Proof. Let A be an abelian surface defined over $\mathbb{F}_p$ and write $f_{A_p}^+(X) = X^2 - aX + b - 2p$, with discriminant $\Delta_{A_p}^+ = a^2 - 4b + 8p$. Then since A_p has real multiplication by K^+ it must be that $\Delta_{A_p}^+ = r^2 d$.

(1) ⇔ (2): Note that $f_{A_p}^+(X)$ is a quadratic polynomial, thus it splits in $(\mathbb{Z}/\ell)[X]$ if and only if its discriminant is a square in $\mathbb{Z}/\ell$.

(2) ⇔ (3): Let ℓ be an odd prime, and suppose $\Delta_{A_p}^+ = r^2 d \equiv y^2 \mod \ell$, equivalently that $d \equiv z^2 \mod \ell$. Then $\ell | (z^2 - d)$. Assume $\ell \neq 2$ and does not split in K^+, then since

$z^2 - d = (z+\sqrt{d})(z-\sqrt{d})$ in K^+ either $\ell|(z+\sqrt{d})$ or $\ell|(z-\sqrt{d})$. But, $(z+\sqrt{d})$ and $(z-\sqrt{d})$ are conjugate which mean that if $\ell|(z \pm \sqrt{d})$ then $\overline{\ell}|\overline{(z \pm \sqrt{d})}$. However, $\ell = \overline{\ell}$ since $\ell \in \mathbb{Z}$, so ℓ must in fact divide both $z + \sqrt{d}$ and $z - \sqrt{d}$. If ℓ divides both, then ℓ must also divide their difference, $(z+\sqrt{d}) - (z-\sqrt{d}) = 2\sqrt{d}$. But the only primes which divide $2\sqrt{d}$ is 2. Thus we have reached a contradiction, so ℓ must split in K^+.

(3) $\Leftrightarrow$ (2): Suppose ℓ splits in K^+ so that we may write $\ell = z_1 z_2$. Then since $\ell \in \mathbb{Z}$, $\ell = \overline{\ell} = \overline{z_1 z_2} = \overline{z}_1 \overline{z}_2$ which means $z_1 = \overline{z_2}$, since neither z_1, $z_2 \in \mathbb{Z}$. So write $\ell = (y + z\sqrt{d})(y - z\sqrt{d}) = y^2 - z^2 d$. Now reduce this equation $\mod \ell$:

$$\begin{aligned} 0 &\equiv \widetilde{y}^2 - \widetilde{z^2 d} && \mod \ell \\ \widetilde{z^2 d} &\equiv \widetilde{y}^2 && \mod \ell \\ \widetilde{d} &\equiv \frac{\widetilde{y}^2}{\widetilde{z}^2} = \left(\frac{\widetilde{y}}{\widetilde{z}}\right)^2 && \mod \ell \end{aligned}$$

Thus $d \equiv s^2 \mod \ell$.

Recall that $\Delta^+_{A_p} = r^2 d$, so if d is congruent to a square modulo ℓ then so is $\Delta^+_{A_p}$. □

Call the equivalences of this lemma $\textsc{compat}(p, d, \ell)$. Now consider the contrapositive of Lemma 5.4.2: If there exists an ℓ such that $\textsc{compat}(p, d, \ell)$ fails, then A_p does not have real multiplication by K^+.

Our goal in the following sections is to say something about the probability that a random matrix $\mathrm{GSp}_4(\mathbb{Z}/\ell)$ satisfies such a compatibility requirement. In particular, if Frob_p is conjugate to some matrix γ, does γ satisfy $\textsc{compat}(p, d, \ell)$ in the sense that $\Delta^+_\gamma \equiv \square \mod \ell$ if and only if ℓ splits in K^+.

Once we have assessed this compatibility condition for the matrices in $\mathrm{GSp}_4(\mathbb{Z}/\ell)$, we will have data as input for a large sieve computation. The set up for the sieve is outlined here.

Observe here that the set of primes p for which A_p has real multiplication by K^+ is contained in the set of primes p for which all ℓ satisfy $\textsc{compat}(p, d, \ell)$, i.e.

$$\begin{aligned} N_{p,K^+} &:= \{p : p \text{ is prime and } A_p \text{ has RM by } K^+\} \\ &\subseteq \{p : p \text{ is prime and for all } \ell\, \textsc{compat}(p, d, \ell) \text{ is satisfied}\}. \end{aligned}$$

For a fixed $z > 0$ our goal is to bound above the set

$$N_{A,K^+}(z) := \{p < z : A_p \text{ has RM by } K^+\}.$$

In order to do this we will use a sieve to bound above the set

$$\{p < z : \text{ for all } \ell < Q(z),\ \textsc{compat}(p, d, \ell) \text{ is satisfied}\}.$$

Before we can do the sieve calculation we need to know the proportion of matrices $\gamma \in \mathrm{GSp}_4(\mathbb{Z}/\ell)$ which have $\Delta_\gamma^+ \equiv \square \mod \ell$, and which have $\Delta_\gamma^+ \not\equiv \square \mod \ell$. We explore this in the following section.

5.5. Class Correspondence

In this section we address the class correspondence described in Proposition 5.1.3 and identify each conjugacy class representative of W_0 with an $F-$stable maximal torus of G. The five conjugacy class representatives of W_0 have already been determined, and in [Wil12], Williams describes five conjugacy classes of maximal tori of regular semisimple elements in

$G = \mathrm{GSp}_4(\mathbb{Z}/\ell) = \mathrm{GSp}_4(\mathbb{F}_\ell)$. The matter that remains is to determine the correspondence. Once the correspondence has been determined we assess whether matrices in a given torus have real characteristic polynomials which split or not, equivalently real characteristic polynomials with square or non-square discriminants. Finally, using Proposition 5.1.4 and the approximate probabilities given in Section 5.3 we will determine the approximate probability that a random matrix $g \in G$ lies within a particular torus.

Let T_0 be the maximal split torus of G, and consider another $F-$stable, maximal torus of G^F, $T = {}^gT_0$, and let $w = \pi(g^{-1}F(g))$. Recall, such a torus T is said to be obtained by twisting with w. The terminology here can be understood by looking at the elements of T described as follows:

$$\begin{aligned}
({}^gT_0)^F = T^F &= \{t \in T \,:\, F(t) = t\} \\
&= \{t = gt_0g^{-1} \in {}^gT_0 \,:\, F(gt_0g^{-1}) = gt_0g^{-1}\} \\
&= \{t = gt_0g^{-1} \in {}^gT_0 \,:\, F(t_0) = F(g)^{-1}gt_0g^{-1}F(g)\} \\
&= \{t = gt_0g^{-1} \in {}^gT_0 \,:\, F(t_0) = (g^{-1}F(g))^{-1}t_0(g^{-1}F(g))\} \\
&= \{t_0 \in T_0 \,:\, F(t_0) = \widetilde{w}^{-1}t_0\widetilde{w}\} \qquad (5.2)
\end{aligned}$$

where $\widetilde{w}$ corresponds to the lift of a conjugacy class representative $w \in W_0$ to N_0. This is well defined because of Proposition 5.1.2.

By using this definition of elements in T we will be able to determine which conjugacy class representative $w_i \in W_0$ corresponds to which torus. For the remainder of this section let

$$t_0 = \begin{pmatrix} u & 0 & 0 & 0 \\ 0 & v & 0 & 0 \\ 0 & 0 & x & 0 \\ 0 & 0 & 0 & y \end{pmatrix} \in T_0$$

denote a generic matrix of T_0.

5.5.1. The Identity Conjugacy Class. Let $w_0 = (id, id, ()) \in W_0$ be the identity element. Then w_0 acts trivially on $t_0 \in T_0$, so that w_0 corresponds to the Maximally Split Torus with matrix representative

$$\gamma = \begin{pmatrix} \alpha_1 & 0 & 0 & 0 \\ 0 & \alpha_2 & 0 & 0 \\ 0 & 0 & m/\alpha_1 & 0 \\ 0 & 0 & 0 & m/\alpha_2 \end{pmatrix}.$$

Over $\mathbb{F}_\ell$ this matrix has characteristic polynomial

$$f_\gamma(X) = (X - \alpha_1)(X - \alpha_2)(X - \tfrac{m}{\alpha_1})(X - \tfrac{m}{\alpha_2})$$

with $\alpha_i, \frac{m}{\alpha_i}$ in $\mathbb{F}_\ell^*$, and $\alpha_1 \frac{m}{\alpha_1} = \alpha_2 \frac{m}{\alpha_2} = m \in \mathbb{F}_\ell^*$. Given $f_\gamma(X)$, the corresponding real characteristic polynomial is

$$f_\gamma^+(X) = X^2 - \left(\alpha_1 + \alpha_2 + \tfrac{m}{\alpha_1} + \tfrac{m}{\alpha_2}\right) X + \left(\alpha_1\alpha_2 + \alpha_1 \tfrac{m}{\alpha_2} + \alpha_2 \tfrac{m}{\alpha_1} + \tfrac{m^2}{\alpha_1\alpha_2}\right).$$

Thus the discriminant of $f_\gamma^+(X)$ is

$$\begin{aligned}\Delta_\gamma^+ &= \left(\alpha_1+\alpha_2+\tfrac{m}{\alpha_1}+\tfrac{m}{\alpha_2}\right)^2-4\left(\alpha_1\alpha_2+\alpha_1\tfrac{m}{\alpha_2}+\alpha_2\tfrac{m}{\alpha_1}+\tfrac{m^2}{\alpha_1\alpha_2}\right)\\ &= \left(\alpha_1+\tfrac{m}{\alpha_1}-\alpha_2-\tfrac{m}{\alpha_2}\right)^2,\end{aligned}$$

which is clearly a square in $\mathbb{F}_\ell^*$, since each $\alpha_i, \frac{m}{\alpha_i}$ is defined over $\mathbb{F}_\ell^*$.

Recall that the probability that a random element of $G(\mathbb{F}_\ell)$ is conjugate to an element of an $F-$stable torus T, is approximately $1/W_T$. The Weyl group, W_0, has already been computed for this torus (it was the wreath product $\mathbb{Z}/2 \wr S_2$), and we know that $\#W_0 = 8$. Thus we can conclude that the probability that a random matrix in $G(\mathbb{F}_\ell)$ lies in the Maximally Split Torus (MST) bounded by

$$\frac{1}{8}-\delta_0 \leq \text{Prob}\left(\gamma \sim t \in \text{MST}\right) < \frac{1}{8}.$$

5.5.2. Irreducible Quadratic Split. Consider the element $w_1 = (id, s, ()) \in W_0$, with matrix form

$$w_1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

Now compute $w_1^{-1}t_0w_1$ for generic $t_0 \in T_0$, and given the equality $F(t_0) = w_1^{-1}t_0w_1$ from equation (5.2) equate entries in the matrices

$$\begin{pmatrix} F(u) & 0 & 0 & 0 \\ 0 & F(v) & 0 & 0 \\ 0 & 0 & F(x) & 0 \\ 0 & 0 & 0 & F(y) \end{pmatrix} = \begin{pmatrix} u & 0 & 0 & 0 \\ 0 & y & 0 & 0 \\ 0 & 0 & x & 0 \\ 0 & 0 & 0 & v \end{pmatrix}.$$

Here we see that u and x each remain fixed by F and $F(v) = y$ and $F(y) = v$, meaning that $u, x \in \mathbb{F}_\ell^*$ and $v, y \in \mathbb{F}_{\ell^2}^*$. This tells us that $\pi^{-1}(w_1)$ is a matrix with eigenvalues, two of which are defined over $\mathbb{F}_\ell^*$ and the other two defined only over $\mathbb{F}_{\ell^2}^*$. Such a matrix corresponds to the Irreducible Quadratic Split Torus (IQST) [Wil12]. Matrices in this torus have the form

$$\gamma = \begin{pmatrix} \alpha_1 & 0 & 0 & 0 \\ 0 & \beta_1 & 0 & \beta_2 \\ 0 & 0 & \alpha_2 & 0 \\ 0 & \beta_3 & 0 & \beta_4 \end{pmatrix}.$$

Thus the characteristic polynomial is

$$f_\gamma(X) = h(X)(X - \alpha_1)(X - \alpha_2)$$

with $h(X)$ monic irreducible over $\mathbb{F}_\ell$ and $h(X)$ has constant term m, i.e. $h(X) = X^2 - (\beta_1 + \beta_4)X + m$; (note this means $m = \det((\beta_i))$). Also $\alpha_1 \neq \alpha_2 \in \mathbb{F}_\ell^*$ and $\alpha_1\alpha_2 = m$. In this case

$$f_\gamma^+(X) = X^2 - (\beta_1 + \beta_4 + \alpha_1 + \alpha_2)X + (\beta_1 + \beta_4)(\alpha_1 + \alpha_2), \qquad \text{and}$$

$$\Delta_\gamma^+ = (\beta_1 + \beta_4 - \alpha_1 - \alpha_2)^2.$$

This is also a square in $\mathbb{F}_\ell^*$ since $h(X)$ and α_i are all defined over $\mathbb{F}_\ell$.

Given the above correspondence and the fact that w_1 has centralizer order 4 in W_0, we can bound

$$\frac{1}{4} - \delta_1 < \text{Prob}\,(\gamma \sim t \in \text{IQST}) < \frac{1}{4}.$$

5.5.3. Double Irreducible Quadratic. Let $w_2 = (s, s, ()) \in W_0$ with matrix form

$$w_2 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

As before compute $w_2^{-1} t_0 w_2$ for generic t_0 and equate entries in the matrices, via equation (5.2). Here we see that $F(u) = x$, $F(x) = u$, $F(v) = y$, $F(y) = v$ so that all $u, v, x, y \in \mathbb{F}_{\ell^2}^*$.

There are two tori with eigenvalues all defined only over $\mathbb{F}_{\ell^2}^*$. The Double Irreducible Quadratic Torus (DIQT), and the Double Irreducible Quadratic NonSplit Torus (DIQNST) [Williams]. Here by examining the structure of a matrix representative we can determine which torus corresponds to w_2.

The Double Irreducible Quadratic has matrix form

$$\gamma_1 = \begin{pmatrix} \alpha_1 & 0 & \alpha_2 & 0 \\ 0 & \beta_1 & 0 & \beta_2 \\ \alpha_3 & 0 & \alpha_4 & 0 \\ 0 & \beta_3 & 0 & \beta_4 \end{pmatrix},$$

and the Double Irreducible Quadratic NonSplit has matrix form

$$\gamma_2 = \begin{pmatrix} A & 0 \\ 0 & (A^T)^{-1} \end{pmatrix} = \begin{pmatrix} \sigma_1 & \sigma_2 & 0 & 0 \\ \sigma_3 & \sigma_4 & 0 & 0 \\ 0 & 0 & \sigma_4/\delta & -\sigma_3/\delta \\ 0 & 0 & -\sigma_2/\delta & \sigma_1/\delta \end{pmatrix}$$

where $\delta = \det(A)$.

To determine which of these matrices is associated to w_2 consider the reduction of γ_1 modulo T_0, (i.e. $\pi(\gamma_1) \in W_0$), this would eliminate the diagonal and reduce the scalars, leaving the element $w_2 \in W_0$, since α_2, β_2 and α_3, β_3 are nonzero entries in γ_1. On the other hand, the reduction of γ_2 mod T_0 would leave zero entries where the 1's lie in w_2. Thus we may conclude that γ_1 corresponds to $w_2 \in W_0$.

Given this correspondence, for the Double Irreducible Quadratic matrix $\gamma = \gamma_1$ we have that

$$f_\gamma(X) = h_1(X)h_2(X)$$

where each $h_i(X)$ is defined over the base field, $\mathbb{F}_\ell$, and each has constant term m, i.e. $h_1(X) = X^2 - (\alpha_1 + \alpha_4)X + m$ and $h_2(X) = X^2 - (\beta_1 + \beta_4)X + m$ with $\det((\alpha_i)) = \det((\beta_i)) = m$. Then

$$f_\gamma^+(X) = X^2 - (\alpha_1 + \alpha_4 + \beta_1 + \beta_4)X + (\alpha_1\beta_1 + \alpha_1\beta_4 + \alpha_4\beta_1 + \alpha_4\beta_4 + 2m) - 2m,$$

and

$$\Delta_\gamma^+ = (\alpha_1 + \alpha_4 - \beta_1 - \beta_4)^2.$$

This is clearly a square in $\mathbb{F}_\ell^*$.

Since the corresponding element w_2 has a centralizer of order 8 in W_0, th probability here is bound by

$$\frac{1}{8} - \delta_2 < \text{Prob}\,(\gamma \sim t \in \text{DIQT}) < \frac{1}{8}.$$

5.5.4. Double Irreducible Quadratic NonSplit. Now consider the element $w_3 = (id, id, (12)) \in W_0$. This element has matrix form

$$w_3 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Computing $w_3^{-1} t_0 w_3$ and equating entries with $F(t_0)$, we find again that each entry u, v, x, y is defined only over $\mathbb{F}_{\ell^2}$, since equating entries shows $F(u) = v$, $F(v) = u$, $F(x) = y$, $F(y) = x$.

This element thus corresponds to the Double Irreducible Quadratic NonSplit Tori. This torus has matrix representative as given in the previous subsection:

$$\gamma = \gamma_2 = \begin{pmatrix} A & 0 \\ 0 & (A^T)^{-1} \end{pmatrix} = \begin{pmatrix} \sigma_1 & \sigma_2 & 0 & 0 \\ \sigma_3 & \sigma_4 & 0 & 0 \\ 0 & 0 & \sigma_4/\delta & -\sigma_3/\delta \\ 0 & 0 & -\sigma_2/\delta & \sigma_1/\delta \end{pmatrix}$$

where $\delta = \det(A)$.

For this matrix, $\gamma^T J \gamma = J$, so the multiplier of this matrix is 1. In this case we also have

$$f_\gamma(X) = h_1(X) h_2(X),$$

but here neither $h_i(X)$ has constant term $m = 1$ but the product is $m^2 = 1$; i.e. $h_1(X) = X^2 - \frac{\sigma_1+\sigma_4}{\delta}X + \frac{1}{\delta}$ and $h_2(X) = X^2 - (\sigma_1 + \sigma_4)X + \delta$. Thus

$$f_\gamma(X) = X^4 - \left(\tfrac{\sigma_1+\sigma_4}{\delta} + \sigma_1 + \sigma_4\right) X^3 + \left(\tfrac{(\sigma_1+\sigma_4)^2+1}{\delta} + \delta\right) X^2 - \left(\tfrac{\sigma_1+\sigma_4}{\delta} + \sigma_1 + \sigma_4\right) X + 1,$$

and

$$f_\gamma^+(X) = X^2 - \left(\tfrac{\sigma_1+\sigma_4}{\delta} + \sigma_1 + \sigma_4\right) X + \left(\left(\tfrac{(\sigma_1+\sigma_4)^2+1}{\delta} + \delta\right) - 2\right).$$

From here we can compute

$$\Delta_\gamma^+ = \frac{(\delta-1)^2\left(-4\delta + (\sigma_1+\sigma_4)^2\right)}{\delta^2}.$$

However, Δ_γ^+ cannot be a square, because if $(\sigma_1 + \sigma_4)^2 - 4\delta$ were a square then $h_2(X)$ would factor, but it is the the case that the two quadratics are irreducible.

The element w_3 has centralizer order 4 in W_0, which means

$$\frac{1}{4} - \delta_3 < \text{Prob}\left(\gamma \sim t \in DIQNST\right) < \frac{1}{4}.$$

5.5.5. Irreducible Quartic. Consider the element $w_4 = (id, s, (12)) \in W_0$. This element is represented by the matrix

$$w_4 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

For this element, the equation $F(t_0) = w_4^{-1} t_0 w_4$ shows that $F(u) = y$, $F(v) = u$, $F(x) = v$, $F(y) = x$, which means that each $u, v, x, y \in \mathbb{F}_{\ell^4}^*$. Thus this element $w_4 \in W_0$ corresponds to the torus with irreducible quartic characteristic polynomial. This torus has matrix representative

$$\gamma = \begin{pmatrix} * & * & * & * \\ * & * & * & * \\ * & * & * & * \\ * & * & * & * \end{pmatrix}$$

with characteristic polynomial $f_\gamma(X)$ a monic irreducible quartic polynomial over $\mathbb{F}_\ell$ with constant term m^2:

$$f_\gamma(X) = X^4 - aX^3 + bX^2 - amX + m^2, \qquad \text{so that}$$

$$f_\gamma^+(X) = X^2 - aX + b - 2m, \qquad \text{and} \qquad \Delta_\gamma^+ = a^2 - 4b + 8m.$$

Let π be a root of $f_\gamma(X)$, and let $\overline{\pi}$ be its conjugate so that $\pi\overline{\pi} = m$. Then by Lemma 5.4.1, $f_\gamma^+(X)$ is the minimal polynomial of $\pi + \overline{\pi}$. Now consider the polynomial $g(X) = X^2 - (\pi + \overline{\pi})X + m \in \mathbb{F}_\ell(\pi + \overline{\pi})[X]$, then π is a root of this polynomial. If Δ_γ^+ is a square, then $\mathbb{F}_\ell(\pi + \overline{\pi}) = \mathbb{F}_\ell$, and π has degree two over $\mathbb{F}_\ell$, contradicting the irreducibility of $f_\gamma(X)$. Thus Δ_γ^+ is not a square.

The element w_4 has centralizer order 4 in W_0, so that

$$\frac{1}{4} - \delta_4 < \operatorname{Prob}(\gamma \sim t \in \mathrm{IQT}) < \frac{1}{4}.$$

5.5.6. Class Correspondence Summary. The calculations computed in the subsections above can be summarized in the table below.

Table 5.1. Summary for tori in $\mathrm{GSp}_4(\mathbb{Z}/\ell)$.

Torus	Matrix Representative, γ	$\Delta_\gamma^+ \equiv \Box \mod \ell$	$\#W_T$	Approximate Probability
Full Split	$\begin{pmatrix} \alpha_1 & 0 & 0 & 0 \\ 0 & \alpha_2 & 0 & 0 \\ 0 & 0 & m/\alpha_1 & 0 \\ 0 & 0 & 0 & m/\alpha_2 \end{pmatrix}$	yes	8	1/8
Irreducible Quadratic Split	$\begin{pmatrix} \alpha_1 & 0 & 0 & 0 \\ 0 & \beta_1 & 0 & \beta_2 \\ 0 & 0 & \alpha_2 & 0 \\ 0 & \beta_3 & 0 & \beta_4 \end{pmatrix}$	yes	4	1/4
Double Irreducible Quadratic	$\begin{pmatrix} \alpha_1 & 0 & \alpha_2 & 0 \\ 0 & \beta_1 & 0 & \beta_2 \\ \alpha_3 & 0 & \alpha_4 & 0 \\ 0 & \beta_3 & 0 & \beta_4 \end{pmatrix}$	yes	8	1/8
Double Irreducible Quadratic NonSplit	$\begin{pmatrix} \sigma_1 & \sigma_2 & 0 & 0 \\ \sigma_3 & \sigma_4 & 0 & 0 \\ 0 & 0 & \sigma_4/\delta & -\sigma_3/\delta \\ 0 & 0 & -\sigma_2/\delta & \sigma_1/\delta \end{pmatrix}$	no	4	1/4
Irreducible Quartic	$\begin{pmatrix} * & * & * & * \\ * & * & * & * \\ * & * & * & * \\ * & * & * & * \end{pmatrix}$	no	4	1/4

5.6. Conclusion: Abelian Surfaces and Random Matrices

Summing the probabilities in last column of the table above we see that one expects about half the matrices in $\mathrm{GSp}_4(\mathbb{Z}/\ell)$ to have real characteristic polynomial with square discriminant in $\mathbb{F}_\ell$, while the other half do not. More precisely,

Lemma 5.6.1. *There exists a constant $\alpha > 0$ such that the probability that a random element $g \in GSp_4(\mathbb{Z}/\ell)$ has real characteristic polynomial with square discriminant,*

$Prob\big(\Delta_g^+ \equiv \square \mod \ell\big)$, can be bounded by

$$\frac{1}{2} > Prob\big(\Delta_g^+ \equiv \square \mod \ell\big) > \frac{1}{2} - \alpha.$$

Proof. Consider each of the three tori above for which a matrix representative has square discriminant, then by equation (5.1) for each torus T_i there exist some $\delta_i > 0$ such that the probability that a random element of $\mathrm{GSp}_4(\mathbb{Z}/\ell)$ lies in T_i can be bounded by

$$\frac{1}{\#W_{T_i}} > \frac{\#T_i(\mathbb{F}_\ell)}{\#G(\mathbb{F}_\ell)} > \frac{1}{\#W_{T_i}}\left(1 - \delta_i\right).$$

Thus summing these bounds for each tori with corresponding square discriminant we get the upper sum $\sum_{i=0}^{2} 1/\#W_{T_i} = 1/8{+}1/4{+}1/8 = 1/2$; and the lower sum $\sum_{i=0}^{2} 1/\#W_{T_i}\left(1-\delta_i\right) = 1/8-\delta_0/8+1/4-\delta_1/4+1/8-\delta_2/8 = 1/2-(\delta_0/8+\delta_1/4+\delta_2/8)$. Let $\alpha = \delta_0/8+\delta_1/4+\delta_2/8$, and we are done. □

Lemma 5.6.2. *There exists a constant $\alpha > 0$ such that the probability that a random element $g \in GSp_4(\mathbb{Z}/\ell)$ has real characteristic polynomial with non-square discriminant, $Prob\big(\Delta_g^+ \not\equiv \square \mod \ell\big)$, can be bounded by*

$$\frac{1}{2} > Prob\big(\Delta_g^+ \not\equiv \square \mod \ell\big) > \frac{1}{2} - \alpha.$$

Proof. The proof follows in the same way as Lemma 5.6.1. For the two tori with non-square discriminants, we sum the upper and lower bounds of equation (5.1) to get the upper sum $\sum_{i=3}^{4} 1/\#W_{T_i} = 1/4 + 1/4 = 1/2$; and the lower sum $\sum_{i=3}^{4} 1/\#W_{T_i}\left(1-\delta_i\right) = 1/4 - \delta_3/4 + 1/4 - \delta_4/4 = 1/2 - (\delta_3/4 + \delta_4/4)$. Here let $\alpha = \delta_3/4 + \delta_4/4$ to finish. □

The important thing to note here is that for any ℓ the proportion of matrices $\gamma \in \mathrm{GSp}_4(\mathbb{Z}/l)$ that satisfy the compatibility condition for real multiplication by K^+ is bounded away from zero and one, independently of ℓ.

In the following section we will use this probability data as input for a large sieve calculation to compute an upper bound on the value of $N_{A,K^+}(x)$.

CHAPTER 6

Large Sieve Calculations

First we set up some notation for the chapter. Let k be a number field, $\mathcal{O}_k$ be its ring of integers and Σ_k be the set of non-zero prime ideals of $\mathcal{O}_k$. For each prime $\mathfrak{p} \in \Sigma_k$ let $N(\mathfrak{p})$ denote the norm of $\mathfrak{p}$ which is the cardinality of the residue field $\mathcal{O}_k/\mathfrak{p}$, i.e. $N(\mathfrak{p}) = [\mathcal{O}_k : \mathfrak{p}]$. Finally, let $\Sigma_k(x)$ be the set of primes $\mathfrak{p} \in \Sigma_k$ with $N(\mathfrak{p}) \leq x$.

In [Zyw08], Zywina proves the following theorem:

Theorem 6.0.1. *[[Zyw08], Theorem 3.3] Let F be a number field and let Λ be a set of nonzero ideals of $\mathcal{O}_F$ which are pairwise relatively prime. Let k be a number field and suppose we have a collection of independent Galois representations*

$$\{\rho_\lambda : \mathcal{G}_k \to H_\lambda\}_{\lambda \in \Lambda}.$$

Assume that all the groups $G_\lambda := \rho_\lambda(\mathcal{G}_\lambda)$ are finite and that there exists a real number $r \geq 1$ such that $|G_\lambda| \leq N(\lambda)^r$ for all but finitely many $\lambda \in \Lambda$. Assume further that there is a finite set $S \subseteq \Sigma_k$ such that each ρ_λ is unramified away from $S_\lambda := S \cup \{\mathfrak{p} \in \Sigma_k \,:\, \mathfrak{p} | N(\lambda)\}$.

For every $\lambda \in \Lambda$, fix a non-empty subset C_λ of G_λ that is stable under conjugation. Let $Q = Q(x)$ be a positive function of a real variable x such that $Q(x) \ll \sqrt{x}$ and let $\Lambda(Q)$ be the set of $\lambda \in \Lambda$ with $N(\lambda) \leq Q$. Define the set

$$\mathscr{S}(x) := \{\mathfrak{p} \in \Sigma_k(x) \,:\, \mathfrak{p} \in S_\lambda \text{ or } \rho_\lambda(Frob_\mathfrak{p}) \subseteq C_\lambda \text{ for all } \lambda \in \Lambda(Q)\}.$$

Choose subsets $\mathcal{Z}(Q) \subseteq \{D : D \subseteq \Lambda, \prod_{\lambda \in D} N(\lambda) \leq Q\}$ and define

$$L(Q) = \sum_{D \in \mathcal{Z}(Q)} \prod_{\lambda \in D} \frac{1 - |C_\lambda|/|G_\lambda|}{|C_\lambda|/|G_\lambda|}.$$

For each $D \subseteq \Lambda$, define $G_D = \prod_{\lambda \in D} G_\lambda$.

(1) Let $B > 0$ be a real number. If $Q(x) := c(\log(x)/\log(\log(x))^2)^{1/(6r)}$ for a sufficiently small constant $c > 0$, then

$$|\mathscr{S}(x)| \leq \left(Li(x) + O(x/\log(x)^{1+B})\right) L(Q)^{-1}.$$

(2) Assuming the Generalized Riemann Hypothesis,

$$|\mathscr{S}(x)| \leq \left(Li(x) + O\left(\max_{D' \in \mathcal{Z}(Q)} |G_{D'}| \cdot \sum_{D \in \mathcal{Z}(Q)} |G_D^{\#}||G_D| \cdot x^{1/2}\log(x)\right)\right) L(Q)^{-1}.$$

The implicit constants depend on k, the representations $\{\rho_\lambda\}_{\lambda \in \Lambda}$ and in part (i) also on r and B.

We now see how this large sieve can be applied to our situation with abelian surfaces to study the sequence of primes occurring for A_p with real multiplication by $K^+ = \mathbb{Q}(\sqrt{d})$.

Consider A, an abelian surface (an abelian variety of dimension $g = 2$) defined over $\mathbb{Q}$ with $\mathrm{End}_{\overline{\mathbb{Q}}}(A) = \mathbb{Z}$, and fix a real quadratic field $K^+ = \mathbb{Q}(\sqrt{d})$. We wish to use the large sieve to give an upper bound on the size of the set

$$N_{A,K^+}(x) = \{p \leq x : p \text{ is prime and } A_p \text{ has RM by } K^+\}.$$

To apply Theorem 6.0.1, let $F = \mathbb{Q}$, then Λ is the set of integral primes. Also let $k = \mathbb{Q}$, and for each integer $m \geq 1$, we obtain Galois representations $\rho_{A,m} : \mathcal{G}_{\mathbb{Q}} \to \mathrm{GL}_4(\mathbb{Z}/m)$.

This representation comes from the action of $\mathcal{G}_{\mathbb{Q}}$ on the $m-$torsion points of $A(\overline{\mathbb{Q}})$. In fact by fixing a polarization $\phi : A \to A^{\vee}$, we get

$$\rho_{A,m} : \mathcal{G}_{\mathbb{Q}} \to \mathrm{GSp}_4(\mathbb{Z}/m).$$

Now let $G_\ell = \rho_\ell(\mathcal{G}_{\mathbb{Q}})$, then for all but finitely many ℓ, we have $G_\ell = \mathrm{GSp}_4(\mathbb{Z}/\ell)$. Using this we can bound $|G_\ell|$ above by $|\mathrm{GSp}_4(\mathbb{Z}/\ell)|$.

Lemma 6.0.3. *Fix a prime power q.*

$$|GSp_{2g}(\mathbb{F}_q)| = (q-1)q^{g^2} \prod_{i=1}^{g} (q^{2i} - 1) \leq q^{2g^2+g+1}.$$

Using $g = 2$ and $q = \ell$ in Lemma 6.0.3 we can say that $|G_\ell| \leq \ell^{11}$. Let S be the set of primes for which A has bad reduction, and define $S_\ell = S \cup \{p \in \Sigma_{\mathbb{Q}} : p|\ell\} = S \cup \{\ell\}$.

Recall the discriminant Δ_γ^+ from Chapter 5, defined by the coefficients of the characteristic polynomial of the matrix $\gamma \in \mathrm{GSp}_4(\mathbb{Z}/\ell)$. For $\ell \in \Lambda$, define the set $C_\ell = \{\gamma \in G_\ell : \textsc{compat}(p, d, \ell) \text{ is satisfied}\}$. The compatibility condition in this case is that $\Delta_\gamma^+ \equiv \square \bmod \ell$ if and only if ℓ splits in K^+. Let $Q = Q(x)$ be a positive function of a real variable x with $Q(x) \ll \sqrt{x}$, and let $\Lambda(Q)$ be the set of $\ell \in \Lambda$ such that $\ell \leq Q$. Define the set

$$\mathscr{S}(x) := \{p \in \Sigma_{\mathbb{Q}}(x) : p \in S_\ell \text{ or } \rho_\ell(\mathrm{Frob}_p) \subseteq C_\ell \text{ for all } \ell \in \Lambda(Q)\}.$$

Define $\mathcal{Z}(Q)$ and $L(Q)$ as in Theorem 6.0.1. Here choosing

$$\mathcal{Z}(Q) = \{D : D \subseteq \Lambda, \prod_{\ell \in D} \ell \leq Q\}$$

is appropriate. From the work done in Chapter 5, we know that there exists an $\alpha > 0$ such that $|C_\ell|/|G_\ell| \geq 1/2 - \alpha$. Then

$$L(Q) \geq \sum_{D \in \mathcal{Z}(Q)} \prod_{\ell \in D} \frac{1-(1/2-\alpha)}{1/2-\alpha} = \sum_{D \in \mathcal{Z}(Q)} \prod_{\ell \in D} \frac{1/2+\alpha}{1/2-\alpha}. \tag{6.1}$$

The term in the product is the same for each ℓ. Denote this term by $\mathcal{E} = \frac{1/2+\alpha}{1/2-\alpha}$, and note that $\mathcal{E} > 1$. Then $\prod_{\ell \in D} \mathcal{E} = (\mathcal{E})^{|D|}$.

Since we wish to compute a lower bound for $L(Q)$, consider the case where $|D| = 1$, so that $D = \{\ell\}$, and the sum is then over $\{\ell\} \in \mathcal{Z}(Q)$:

$$L(Q) \geq \sum_{\{\ell\} \in \mathcal{Z}(Q)} \mathcal{E} = \#\mathcal{Z}(Q) \cdot \mathcal{E}.$$

Since $\mathcal{Z}(Q) = \{\{\ell\} \in \Lambda : \ell \leq Q\}$, then $\#\mathcal{Z}(Q) =$ the number of primes $\ell \leq Q$. Asymptotically the number of primes less than Q can be bound below by $\frac{Q}{\log(Q)}$. So, given this lower bound for $L(Q)$ we obtain an upper bound for $L(Q)^{-1}$:

$$L(Q) \geq \mathcal{E} \cdot \#\mathcal{Z}(Q) > \mathcal{E} \frac{Q}{\log(Q)}$$

$$L(Q)^{-1} \leq \frac{\log(Q)}{\mathcal{E} \cdot Q}. \tag{6.2}$$

Using this as the bound for $L(Q)^{-1}$ in Theorem 6.0.1 (i) the bound on $|\mathscr{S}(x)|$ becomes

$$|\mathscr{S}(x)| \leq \left(Li(x) + O(x/\log(x)^{1+B})\right) \frac{\log(Q)}{\mathcal{E} \cdot Q}.$$

Moreover, we follow Zywina's suggestion from Theorem 6.0.1 (i) and let

$$Q(x) = c\left(\log(x)/\log(\log(x))^2\right)^{1/(6r)},$$

which specifically for us is $Q(x) = c\left(\log(x)/\log(\log(x))^2\right)^{1/66}$, since $|G_\ell| \leq \ell^r$ for $r = 11$.

First let us evaluate $\log(Q)/Q$ for the given Q,

$$\begin{aligned}\frac{\log(Q)}{Q} &= \frac{\log(c) + \log(\log(x)^{1/66}) - \log(\log(\log(x))^{2/66})}{c \cdot \dfrac{\log(x)^{1/66}}{\log(\log(x))^{2/66}}} \\ &< \frac{\left(\log(c) + \log(\log(x)^{1/66})\right)\log(\log(x))^{2/66}}{c\log(x)^{1/66}},\end{aligned}$$

where we have dropped the triple log term since it is negative.

Now, for all sufficiently small $0 < c < 1$, (as in (i)), $\log(c) < 0$ so that term may be dropped as well, and

$$\frac{\log(Q)}{Q} < \frac{\log(\log(x)^{1/66}) \cdot \log(\log(x))^{2/66}}{c\log(x)^{1/66}} = \frac{\frac{1}{66}\left(\log(\log(x))^{1+2/66}\right)}{c\log(x)^{1/66}}.$$

As for the term $\left(\mathrm{Li}(x) + O(x/\log(x)^{1+B})\right)$, first consider $O(x/\log(x)^{1+B})$, for all $B > 0$, it is true that $\frac{x}{\log(x)^{1+B}} < \frac{x}{\log(x)}$ for $x > e$. Additionally, $\mathrm{Li}(x) \leq M\frac{x}{\log(x)}$ for some $M \in \mathbb{R}_{\geq 0}$ and $x \gg 0$. Thus we can say that

$$\begin{aligned}\left(\mathrm{Li}(x) + O(x/\log(x)^{1+B})\right)L(Q)^{-1} &\leq \left(M\frac{x}{\log(x)} + \frac{x}{\log(x)}\right)L(Q)^{-1} \\ &= (1+M)\left(\frac{x}{\log(x)}\right)L(Q)^{-1}.\end{aligned}$$

In terms of x we can write the bound as

$$|\mathscr{S}(x)| \leq (1+M)\left(\frac{x}{\log(x)}\right)\left(\frac{\frac{1}{66}\log(\log(x))^{1+2/66}}{\mathcal{E}\cdot c\cdot \log(x)^{1/66}}\right)$$
$$= C_{(M,\mathcal{E})}\frac{x\left(\log(\log(x))\right)^{1+2/66}}{\left(\log(x)\right)^{1+1/66}}.$$

Following the statement of the Large Sieve in [Zyw09] Zywina comments that if there is a number s such that $|G_\lambda^{\#}| < N(\lambda)^s$ for all but finitely many $\ell \in \Lambda$, then the bound for $|\mathscr{S}(x)|$ can be improved.

Lemma 6.0.4 ([Ach12], Lemma 3.1). *Let G be a connected algebraic group over $\mathbb{F}_\ell$, let $d(G)$ be the dimension of G and $t(G)$ be the rank of G. There exists a constant $\alpha = \alpha(G)$ such that*

$$|G(\mathbb{Z}/\ell)| \leq \ell^{d(G)}$$
$$\left|G(\mathbb{Z}/\ell)^\sharp\right| < (\alpha\ell)^{t(G)}.$$

For our case we have $G(\mathbb{Z}/\ell) = \mathrm{GSp}_4(\mathbb{Z}/\ell)$, and we know from before $r = d(G) = 11$. As for $t(G)$, the rank of G, this is just the dimension of the maximal tori of G, which for us is 3.

Using this lemma with $d(G) = r = 11$, and $t(G) = s = 3$, and assuming the Generalized Riemann Hypothesis, Zywina asserts the bound in Theorem 6.0.1(ii) cam be given as the simpler expression

$$|\mathscr{S}(x)| \leq \left(Li(x) + O(Q^{2r+s+1}x^{1/2}\log(x))\right)L(Q)^{-1}.$$

Furthermore, choosing $Q(x) = \left(x^{1/2}/\log(x)^2\right)^{1/(2r+s+1)}$, the bound becomes

$$|\mathscr{S}(x)| \ll \frac{x/\log(x)}{L(Q)}. \tag{6.3}$$

Making the same simple assumptions on the set $\mathcal{Z}(Q)$ as before, so that $D = \{\ell\}$, and taking $s = 3$ and $r = 11$, we can now bound $L(Q)$ below by

$$\begin{aligned}\frac{1}{L(Q)} < \frac{1}{\mathcal{E}\cdot\#\mathcal{Z}(Q)} &< \frac{\log(Q)}{\mathcal{E}\cdot Q} \\ &= \frac{\log\left(\dfrac{x^{1/52}}{\log(x)^{2/26}}\right)}{\mathcal{E}\cdot\dfrac{x^{1/52}}{\log(x)^{2/26}}} \\ &= \frac{\left(\log\left(x^{1/52}\right) - \log\left(\log(x)^{2/26}\right)\right)\log(x)^{2/26}}{\mathcal{E}\cdot x^{1/52}} \\ &< \frac{\frac{1}{52}\log(x)^{1+2/26}}{\mathcal{E}\cdot x^{1/52}} \qquad \text{after dropping the negative } \log \text{ term} \\ &= C_{\mathcal{E}}\frac{\log(x)^{1+2/26}}{x^{1/52}}.\end{aligned}$$

Substituting this upper bound for $L(Q)^{-1}$ into equation (6.3) we get an upper bound on the size of the set $\mathscr{S}(x)$ assuming GRH

$$|\mathscr{S}(x)| \ll C_{\mathcal{E}}x^{1-1/52}\log(x)^{2/26}.$$

6.1. Support for the Lang-Trotter Conjecture for Abelian Surfaces

Assuming the Generalized Riemann Hypothesis we have just shown that the number of primes less than x for which the reduction A_p has real multiplication by K^+ is bounded above by $C_E x^{1-1/52} \log(x)^{2/26}$. In terms of Conjecture 4.6.1 we have the bound

$$\#N_{A,K^+}(x) \ll C_E x^{1-1/52} \log(x)^{2/26}.$$

While this is certainly still far from the conjectured $\sqrt{x}/\log(x)$, it is of a similar form as the best bounds given by Cojocaru, Fouvry and Murty for the Lang-Trotter Conjecture for elliptic curves, as stated in Section 2.2.1.

BIBLIOGRAPHY

[Ach12] Jeffrey D. Achter. Explicit bounds for split reductions of simple abelian varieties. *J. Théor. Nombres Bordeaux*, 24(1):41–55, 2012.

[AH14] J. Achter and E. Howe. Split abelian surfaces. pre-print, 2014.

[AW14] J. Achter and C. Williams. Local heuristics and an exact formula for abelian surfaces over finite fields. *ArXiv e-prints*, March 2014.

[BLGHT11] Tom Barnet-Lamb, David Geraghty, Michael Harris, and Richard Taylor. A family of Calabi-Yau varieties and potential automorphy II. *Publ. Res. Inst. Math. Sci.*, 47(1):29–98, 2011.

[Bor91] Armand Borel. *Linear algebraic groups*, volume 126 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1991.

[Car85] Roger W. Carter. *Finite groups of Lie type*. Pure and Applied Mathematics (New York). John Wiley & Sons Inc., New York, 1985. Conjugacy classes and complex characters, A Wiley-Interscience Publication.

[CFM05] Alina Carmen Cojocaru, Etienne Fouvry, and M. Ram Murty. The square sieve and the Lang-Trotter conjecture. *Canad. J. Math.*, 57(6):1155–1177, 2005.

[CK13] Peter J. Cho and Henry H. Kim. Probabilistic properties of number fields. *J. Number Theory*, 133(12):4175–4187, 2013.

[DF04] David S. Dummit and Richard M. Foote. *Abstract algebra*. John Wiley & Sons Inc., Hoboken, NJ, third edition, 2004.

[GAP14] The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.7.4*, 2014.

[How00] Everett W. Howe. Personal communication, 2000.

[IR90] Kenneth Ireland and Michael Rosen. *A classical introduction to modern number theory*, volume 84 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1990.

[Kno90] John Knopfmacher. *Abstract analytic number theory*. Dover Books on Advanced Mathematics. Dover Publications, Inc., New York, second edition, 1990.

[Lou01] Stéphane Louboutin. Explicit upper bounds for residues of Dedekind zeta functions and values of L-functions at $s = 1$, and explicit lower bounds for relative class numbers of CM-fields. *Canad. J. Math.*, 53(6):1194–1222, 2001.

[LT76] Serge Lang and Hale Trotter. *Frobenius distributions in* GL_2*-extensions*. Lecture Notes in Mathematics, Vol. 504. Springer-Verlag, Berlin, 1976. Distribution of Frobenius automorphisms in $\mathrm{G}L_2$-extensions of the rational numbers.

[Map12] Maplesoft. *Maple 16.01*, 2012.

[Mar77] Daniel A. Marcus. *Number fields*. Springer-Verlag, New York, 1977. Universitext.

[Mil08] James S. Milne. Abelian varieties (v2.00), 2008. Available at www.jmilne.org/math/.

[Mil11] James S. Milne. Algebraic geometry (v5.21), 2011. Available at www.jmilne.org/math/.

[Mil12] James S. Milne. Reductive groups (v1.00), 2012. Available at www.jmilne.org/math/.

[Neu99] Jürgen Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[Oor08] Frans Oort. Abelian varieties over finite fields. In *Higher-dimensional geometry over finite fields*, volume 16 of *NATO Sci. Peace Secur. Ser. D Inf. Commun. Secur.*, pages 123–188. IOS, Amsterdam, 2008.

[S$^+$11] W. A. Stein et al. *Sage Mathematics Software (Version 4.7.1).* The Sage Development Team, 2011. `http://www.sagemath.org`.

[Sil94] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.

[Sil09] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.

[ST92] Joseph H. Silverman and John Tate. *Rational points on elliptic curves*. Undergraduate Texts in Mathematics. Springer-Verlag, New York, 1992.

[Tao08] Terence Tao. The Divisor Bound, 2008.

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

[Was97] Lawrence C. Washington. *Introduction to cyclotomic fields*, volume 83 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1997.

[Was08] Lawrence C. Washington. *Elliptic curves*. Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, second edition, 2008. Number theory and cryptography.

[Wat69] William C. Waterhouse. Abelian varieties over finite fields. *Ann. Sci. École Norm. Sup. (4)*, 2:521–560, 1969.

[Wil12] C. Williams. Conjugacy classes of matrix groups over local rings and an application to the enumeration of abelian varieties. *Digital Collections of Colorado*, June 2012.

[Zyw08] David Zywina. The large sieve and galois representations. *arXiv.org*, pages 1–36, 2008.

[Zyw09] David Zywina. The lang-trotter conjecture and mixed representations. *2000 Mathematics Subject Classification*, pages 1–28, 2009.