Counting Abelian Surfaces with Real Multiplication by $\mathbb{Q}(\sqrt{d})$

Hilary Smallwood (smallwoo@math.colostate.edu), Jeff Achter

Colorado State University

The Question

Let $\mathbb{F}_q$ be the field of size q of characteristic p. Fix a positive integer d.

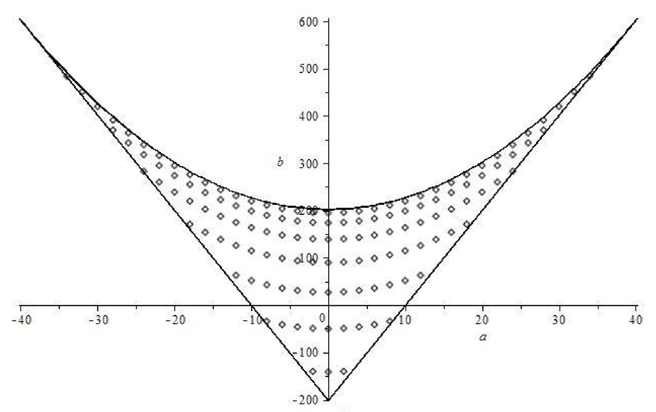
How many principally polarized abelian surfaces (PPAS), $A/\mathbb{F}_q$ are there such that A has real multiplication by $\mathbb{Q}(\sqrt{d})$?

Equivalently, how many abelian surfaces $A/\mathbb{F}_q$, such that $\mathbb{Q}(\sqrt{d}) \subset \mathrm{End}^0(A)$?

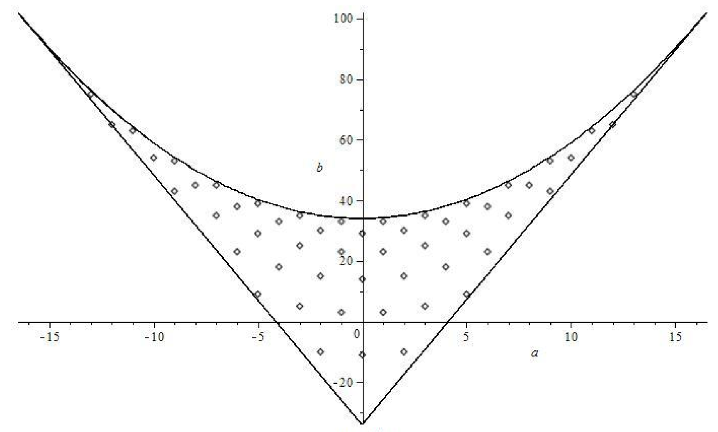
Relevant Definitions

- A a principally polarized abelian surface (PPAS)
- An *endomorphism* of an abelian surface A is a group homomorphism from A to itself.
- Let $\mathrm{End}^0(A) = \mathrm{End}(A) \otimes \mathbb{Q}$ be the algebra of endomorphisms of A with coefficients extended to $\mathbb{Q}$.
- An *isogeny* between two abelian surfaces A and B is a surjective homomorphism with finite kernel.
- An abelian surface A has *real multiplication (RM)* by $\mathbb{Q}(\sqrt{d})$ if $\mathbb{Q}(\sqrt{d}) \subset \mathrm{End}^0(A)$.
- Let $\mathrm{RMI}(d,q) := \{(a,b) \,|\, T^4 - aT^3 + bT^2 - aqT + q^2 = f_A(T)$ for A with RM by $\mathbb{Q}(\sqrt{d})\}$.
- $X(d,q) := \{A \,|\, A/\mathbb{F}_q$ with RM by $\mathbb{Q}(\sqrt{d})\}$.

RMI(d,q)



q=101, d=7



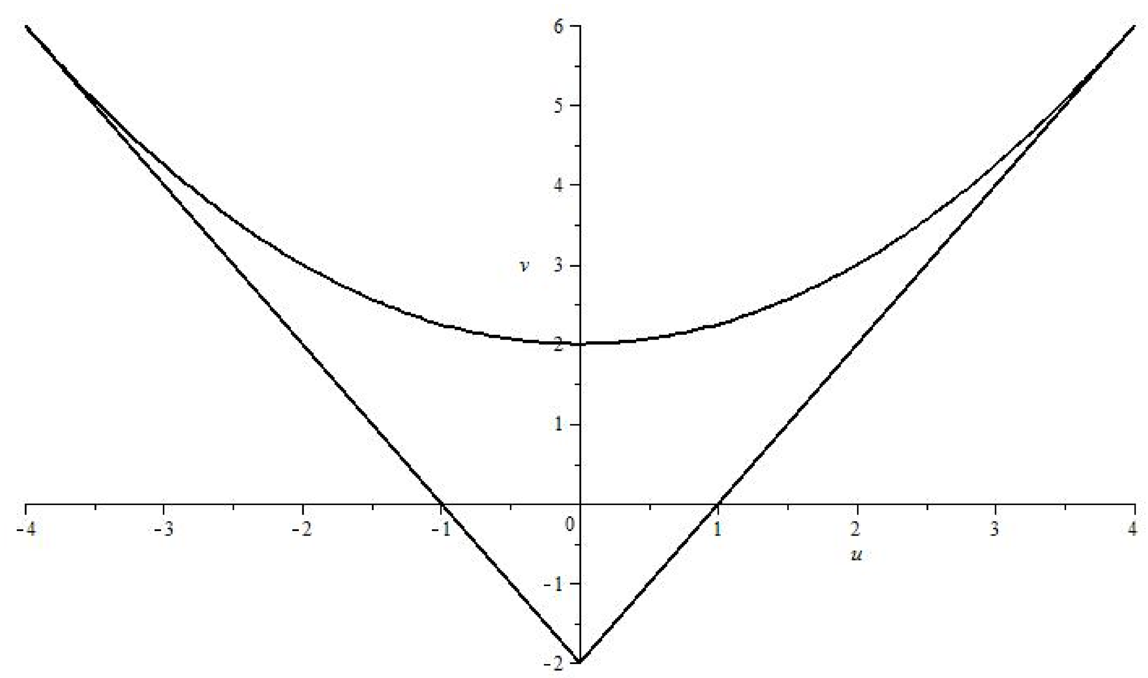
q=17, d=5

Introduction

Let A be an abelian variety defined over $\mathbb{F}_q$. A admits an endomorphism called the Frobenius endomorphism (the q power map). Denote the Frobenius endomorphism by π_A. Then π_A has a matrix representation in GSp_4, and thus has a corresponding characteristic polynomial, we'll denote by $f_A(T)$. We shall use the following facts about abelian surfaces and $f_A(T)$ in order to count the number of $A/\mathbb{F}_q$ such that A has RM by $\mathbb{Q}(\sqrt{d})$.

Facts:

1. Two abelian surfaces A and B are isogenous if and only if $f_A(T) = f_B(T)$.
2. The roots of $f_A(T)$ have size $\sqrt{q}$ and come in complex conjugate pairs, $\sqrt{q}e^{\pm i\theta_k}$.
3. $f_A(T) = T^4 - aT^3 + bT^2 - aqT + q^2$ where $|a| \leq 4\sqrt{q}$ and $2|a|\sqrt{q} - 2q \leq b \leq \frac{a^2}{4} + 2q$. (These conditions define the Weil region as shown at right.)
4. The discriminant of the real quadratic subfield inside $\mathrm{End}^0(A)$ is $\Delta_A^+ = a^2 - 4b + 8q$.



Here the region has been scaled according to: $u = \frac{a}{\sqrt{q}}$ and $v = \frac{b}{q}$.

Summary

Counting the set RMI(d,q)

If $\Delta_A^+ = a^2 - 4b + 8q = r^2 d$, then $\mathbb{Q}(\sqrt{d}) \subset \mathrm{End}^0(A)$

Count coefficient pairs (a,b) which satisfy $\Delta_A^+ = r^2 d$. This effectively counts the number isogeny classes of PPAS with RM by $\mathbb{Q}(\sqrt{d})$, by Fact 1. (Equivalently $\#\mathrm{RMI}(d,q)$.)

Reduce this count to counting pairs (a,r) which satisfy $b \in \mathbb{Z}$. This imposes parity conditions on a and r:

- $d \equiv 2,3 \mod 4, \Rightarrow a$ and r both even.
- $d \equiv 1 \mod 4, \Rightarrow a$ and r have same parity.

The Weil region imposes the bound $|r| \leq \dfrac{4\sqrt{q} - a}{\sqrt{d}}$. For each a define $r_a = \dfrac{4\sqrt{q} - a}{\sqrt{d}}$, then sum $\sum_a r_a$.

The different cases for d are treated separately, first with $a = 2m$ and $r = 2n$ then with $a = 2m+1$ and $r = 2n+1$.

The plots at left illustrate the coordinate points $(a,b) \in \mathrm{RMI}(d,q)$ for different values of d and q.

The size of an isogeny class

Weyl's formula for the Sato-Tate measure is given in terms of the angles of the roots of $f_A(T)$:
$\mu_{ST}(\theta_1,\theta_2) =$

$$2^{2^2}\Big(\cos(\theta_2) - \cos(\theta_1)\Big)^2 \frac{1}{\pi}\sin^2(\theta_1)d\theta_1 \frac{1}{\pi}\sin^2(\theta_2)d\theta_2$$

Through a change of coordinates this can be rewritten in terms of q and the coefficients of $f_A(T)$:
$\mu_{ST}(a,b;q) =$

$$\frac{\sqrt{(a^2 - 4b + 8q)(b^2 + 4bq + 4q^2 - 4a^2q)}}{4q^3\pi^2}dadb$$

Thinking of $\mu_{ST}(a,b;q)$ as the probability that (a,b) appear as the coefficients of $f_A(T)$, one expects $q^3\mu_{ST}$ to approximate the size of the isogeny class associated to the coefficients (a,b).

The plots at right illustrate the surface $q^3\mu_{ST}$ for $q = 5$.

Results

Upper Bounds

$$\#\mathrm{RMI}(d,q) \leq \begin{cases} \dfrac{4q}{\sqrt{d}} & \text{if } d \equiv 2,3 \mod 4 \\ \dfrac{(1+\alpha)8q}{\sqrt{d}} & \text{if } d \equiv 1 \mod 4, \\ & \text{and } \alpha > 0, q \geq \frac{1}{16\alpha^2} \end{cases}$$

The size of an isogeny class is bound above by:

$$q^3\mu_{ST}(a,b;q) \leq \frac{8}{\pi^2 3\sqrt{3}}q^{3/2}.$$

Together these give an upper bound on $\#X(d,q)$:

$$\#X(d,q) \leq \begin{cases} \dfrac{32}{3\sqrt{3}\pi^2\sqrt{d}}q^{5/2} & \text{if } d \equiv 2,3 \mod 4 \\ \dfrac{64(1+\alpha)}{3\sqrt{3}\pi^2\sqrt{d}}q^{5/2} & \text{if } d \equiv 1 \mod 4 \\ & \text{and } \alpha > 0, q \geq \frac{1}{16\alpha^2} \end{cases}$$

Lower Bounds

For given a and r the size of an isogeny class is bound below by $\frac{1}{4\pi^2}\sqrt{S_{(a,r;q)}}$.
To get a lower bound on $\#X(d,q)$, sum

$$\sum_a \sum_r \frac{1}{4\pi^2}\sqrt{S_{(a,r;q)}}.$$

For $0 < \gamma < 1$ there exists $q_{(d,\gamma)}$ such that for $q > q_{(d,\gamma)}$,

$$\#X(d,q) > \begin{cases} \dfrac{(1-\gamma)8}{5\pi^2\sqrt{d}}q^{5/2} & \text{if } d \equiv 2,3 \mod 4 \\ \dfrac{(1-\gamma)16}{5\pi^2\sqrt{d}}q^{5/2} & \text{if } d \equiv 1 \mod 4 \end{cases}$$

$\mu_{ST}(a,b;q)$