DISSERTATION

EXPLICIT AND QUANTITATIVE RESULTS FOR ABELIAN VARIETIES OVER FINITE FIELDS

Submitted by

Elliot Krause

Department of Mathematics

In partial fulfillment of the requirements

For the Degree of Doctor of Philosophy

Colorado State University

Fort Collins, Colorado

Fall 2022

Doctoral Committee:

Advisor: Jeffrey Achter

Rachel Pries
Jamie Juul
Indrajit Ray

ABSTRACT

EXPLICIT AND QUANTITATIVE RESULTS FOR ABELIAN VARIETIES OVER FINITE FIELDS

Let E be an ordinary elliptic curve over a prime field $\mathbb{F}_p$. Attached to E is the characteristic polynomial of the Frobenius endomorphism, $T^2 - a_1T + p$, which controls several of the invariants of E, such as the point count and the size of the isogeny class. As we base change E over extensions $\mathbb{F}_{p^n}$, we may study the distribution of point counts for both of these invariants. Additionally, we look to quantify the rate at which these distributions converge to the expected distribution. More generally, one may consider these same questions for collections of ordinary elliptic curves and abelian varieties.

ACKNOWLEDGEMENTS

I would like to thank Jeff Achter for all his help and insight throughout the writing of this dissertation. I would also like to thank my friends for the good times we shared. Finally, I would like to thank my parents for all their support through the years.

LIST OF NOTATION

E	An elliptic curve
$E^{(1)}, \dots E^{(s)}$	A collection of s elliptic curves, usually geometrically not isogenous
a_n	The trace of Frobenius for $E/\mathbb{F}_{p^n}$
$\overline{a}_n$	The normalized trace in $[-2, 2]$
$\Delta_n^{(j)}$	The Frobenius discriminant for the j^{th}, $E^{(j)}$ elliptic curve over $\mathbb{F}_{p^n}$
D_N	The discrepancy of a sequence
D_N^*	The star-discrepancy for a sequence
$V(f)$	The (Hardy-Krause) variation of a function
η	The type of a vector $\boldsymbol{\alpha}$
T	A periodic function used in construction of the Vinogradov function Ψ
$\Psi(\boldsymbol{\theta})$	The Vinogradov function
$\boldsymbol{\theta}$	A vector with components $(\theta_1, \dots, \theta_s)$.
$r(\boldsymbol{h})$	$r(\boldsymbol{h}) = \prod_{i=1}^{s} \max\{1, \lvert h_i \rvert\}$
$\ll$	Vinogradov complexity notation
$O(f)$	Big O complexity notation
$A(J, N)$	The number of the first N terms of a sequence in the interval J
λ	Lebesgue measure

χ	Indicator/characteristic function
$e(\theta)$	$\exp(2\pi i\theta)$
$\mathscr{E}^k$	A set of functions with a certain constraint on their Fourier expansion
$\|x\|$	The distance from x to the nearest integer.

TABLE OF CONTENTS

Chapter 1

Introduction

1.1 Introduction

Elliptic curves and abelian varieties are frequently studied objects in arithemtic geometry that arise as zero sets of polynomials and exhibit a group structure on their points. The statistics of certain invariants associated with abelian varieties have garnered frequent attention, such as the Sato-Tate conjecture, for example. Chapter 2 will provide background on elliptic curves and abelian varieties. Given an abelian variety $A/\mathbb{F}_p$ of dimension g, we have the characteristic polynomial of Frobenius of degree $2g$. This polynomial has complex conjugate roots of the form $\alpha_j = \sqrt{p}\exp(i\theta_j)$ for $1 \leq j \leq g$, where $\pm\theta$ are called the Frobenius angles. After base change to $\mathbb{F}_{p^n}$, the roots of the p^n Frobenius endomorphism are $\alpha_j^n = \sqrt{p^n}\exp(in\theta_j)$, which then produces a sequence of Frobenius angles $\{n\boldsymbol{\theta}\}_{n=1}^{\infty} = \{(n\theta_1, \ldots, n\theta_g)\}_{n=1}^{\infty}$ corresponding to extensions $\mathbb{F}_{p^n}$. The trace of Frobenius and the discriminant of the Frobenius polynomials are two invariants that can be calculated from trigonometric functions of the Frobenius angles. Thus, we look to quantify the distribution of these invariants as we consider A over extensions of $\mathbb{F}_p$ by working with the sequence $\{n\boldsymbol{\theta}\}_{n=1}^{\infty}$.

Chapter 3 then turns to the methods of quasi-Monte Carlo integration to study the distributions of these invariants through the sequence $\{n\boldsymbol{\theta}\}_{n=1}^{\infty}$. Quasi-Monte Carlo integration aims to give numerical estimates of integrals of a function f by averaging the value of f on points of a sequence. In the case of a one dimensional sequence, we have Koksma's inequality,

$$\left| \frac{1}{N} \sum_{n=1}^{N} f(\theta_n) - \int_0^1 f(x)dx \right| \leq D_N^* V(f)$$

where D_N^* is the discrepancy of the sequence $\{\theta_n\}_{n=1}^{N}$ and $V(f)$ is the variation of f. For higher dimensional sequences, we shall use the following quantitative result. Let $\boldsymbol{\theta} = (\theta_1, \theta_2, \ldots, \theta_s)$

and let $n\boldsymbol{\theta} = (n\theta_1, n\theta_2, \ldots, n\theta_s)$. Let f be a periodic function with a certain condition on its Fourier coefficients. Under a certain assumption on the irrationality properties of $\boldsymbol{\theta}$, we have the asymptotic

$$\frac{1}{N}\sum_{n=1}^{N} f(n\boldsymbol{\theta}) - \int_{I^s} f(\boldsymbol{x})d\boldsymbol{x} = O\left(\frac{1}{N}\right). \tag{1.1}$$

The irrationality measure of $\boldsymbol{\theta}$ will prompt a brief overview of Baker's theorem, and the condition on f will lead us to the construction of a multivariate Vinogradov function from [1].

We then develop the background results necessary to apply quasi-Monte Carlo integration to the sequence of Frobenius angles in Chapter 4. Our main results are then presented in Chapters 5 and 6. Many of these results aim to quantify how often a numerical invariant associated with an abelian variety lands in a certain interval as A is based changed to extension of $\mathbb{F}_{p^n}$. One such result involves explicit bounds for extensions up to degree N as follows. Define $\overline{a}_n \in [-2, 2]$ to be the normalized trace for an elliptic curve over $\mathbb{F}_{p^n}$. Let $E/\mathbb{F}_p$ be an ordinary elliptic curve. The following theorem quantifies the distribution of normalized traces for E over extensions $\mathbb{F}_{p^n}$.

Theorem 5.1.1. *Let $E/\mathbb{F}_p$ be an ordinary elliptic curve with normalized Frobenius angle $\widetilde{\theta}$. Let $I = [a, b] \subset [-2, 2]$ be the target interval for the traces $\overline{a}_n$. Define A_I as the quantity*

$$A_I = \frac{1}{\pi}(\arccos(a/2) - \arccos(b/2)).$$

Then the proportion of extensions of degree up to N where $\overline{a}_n \in I$ satisfies the inequality

$$\mathrm{PropTr}_{E,N,I} \geq A_I - 2D_N^*$$

where D_N^* is the discrepancy of the sequence $\{\widetilde{\theta}_n\}_{n=1}^N$.

For a visualization of this distribution, see the histogram in Figures 1.1.

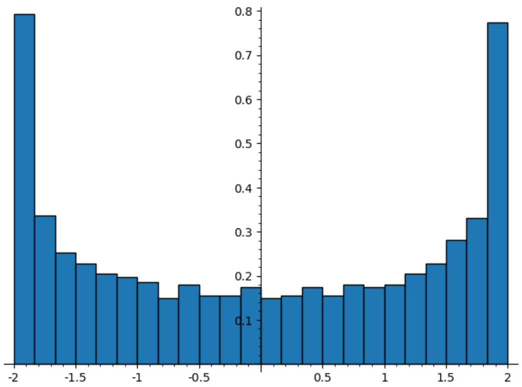


Figure 1.1: Histogram of the normalized traces for $N = 1000$ for the curve $y^2 = x^3 + x + 13$ with $p = 37$.

We also have quantitative results using the Vinogradov function Ψ and the error estimate from (1.1). The construction of Ψ involves region R_1 for which Ψ roughly acts as an indicator function. The angle rank of an abelian variety is a sort of linear independence condition on the Frobenius angles, and maximal angle rank ensures a certain irrationality property for $(\theta_1, \ldots, \theta_g)$. Let A be an abelian variety over $\mathbb{F}_p$. The following theorem considers the distributions of Frobenius traces for A based changed over extensions of $\mathbb{F}_p$.

Theorem 6.1.2. *Let $A/\mathbb{F}_p$ be an abelian variety of dimension g with maximal angle rank, and let $I = [a, b] \subset [-2g, 2g]$ be the target interval for the normalized traces. Then the proportion of extensions where the trace $\overline{a}_n$ lands in I satisfies*

$$\mathrm{PropTr}_{A,N,I} \geq \int_{R_1} \Psi(\boldsymbol{x}) d\boldsymbol{x} - O\left(\frac{1}{N}\right).$$

The data and figures throughout this thesis were produced using SageMath, [2].

Chapter 2

Abelian Varieties

2.1 Abelian Varieties

An abelian variety A of dimension g over K, denoted A/K, is a reduced and irreducible projective variety with a group structure (which is necessarily abelian). This paper will mostly be concerned with elliptic curves and abelian surfaces, which are abelian varieties of dimension 1 and 2, respectively. We first examine a few generalities before specializing to elliptic curves. Much of the general theory can be found in [3], [4], [5] and [6].

Definition 2.1.1. Let A_1, A_2 be abelian varieties of dimension g defined over K. An isogeny $\phi : A_1 \to A_2$ is a surjective homomorphism. If an isogeny exists between A_1 and A_2, then the two abelian varieties are said to be isogenous.

Isogeny is an equivalence relation on abelian varieties of dimension g. For abelian varieties over a finite field, these equivalence classes are parameterized by a certain characteristic polynomials, which we now work towards. First, we need some preliminaries on endomorphisms and the Tate module.

Definition 2.1.2. The endomorphism ring of A/K is the set of isogenies from A to itself,

$$\text{End}(A) = \{\phi : A \to A \ : \ \phi \text{ is an isogeny}\}.$$

The multiplication by m map is one such endomorphism.

Example 2.1.3. Let A/K be an abelian variety. For an integer m, the map

$$[m] : A \longrightarrow A$$

$$P \longmapsto mP = \underbrace{P + P + \ldots P}_{m \text{ times}}$$

is an endomorphism of A. The kernel of this map is the m-torsion: we use $A[m](K)$ to denote the K points of order dividing m, and we use $A_m = A[m](\overline{K})$ for the $\overline{K}$ m-torsion points.

We will mostly be concerned with abelian varieties over finite fields. In this setting, the Tate module and the Frobenius endomorphism are key elements of the theory. Let q be a power of a prime, $q = p^n$, and let $A/\mathbb{F}_q$ be a g-dimensional abelian variety.

Definition 2.1.4. For a prime $\ell \neq p$, define the ℓ-adic Tate module on A by the inverse limit

$$T_\ell(A) = \varprojlim_n A_{\ell^n}$$

over the multiplication by ℓ maps

$$A_{\ell^{n+1}} \xrightarrow{[\ell]} A_{\ell^n}.$$

Let $\phi : A \to A$ be an isogeny. Because ϕ is a group homomorphism it induces a $\mathbb{Z}_\ell$-linear map

$$\phi_\ell : T_\ell(A) \to T_\ell(A)$$

on the Tate module via the action on ℓ^n torsion. Then the map

$$\text{End}(A) \to \text{End}(T_\ell(A))$$

$$\phi \mapsto \phi_\ell$$

is an inclusion of rings. If a basis of $T_\ell(A)$ is chosen, then an isogeny has a representation as a $2g \times 2g$ matrix with entries in $\mathbb{Z}_\ell$.

We continue with $A/\mathbb{F}_q$ of dimension g. The map $x \mapsto x^q$ induces an endomorphism of A, called the Frobenius endomorphism. After a choice of basis for $T_\ell(A)$, the action of Frobenius on the Tate module induces the characteristic polynomial of Frobenius, $f_{A/\mathbb{F}_q}(T)$. In fact, $f_{A/\mathbb{F}_q}(T)$ has coefficients that are independent of ℓ and are integers. In addition, $f_{A/\mathbb{F}_q}(T)$ is monic of degree $2g$, with sizes of the roots controlled by the Weil conjectures. The roots of $f_{A/\mathbb{F}_q}(T)$ (the eigenvalues of the Frobenius endomorphism acting on the Tate module) are complex numbers of the form $\alpha_j = \sqrt{q}\exp(i\theta_j)$ for $\alpha_1, \dots \alpha_g$ and the complex conjugates $\overline{\alpha_1}, \dots \overline{\alpha_g}$. Possibly after rearranging, the numbers $0 \leq \theta_1 \leq \dots \leq \theta_g$ are called the Frobenius angles. A is said to be ordinary if the coefficient of T^g in $f_{A/\mathbb{F}_q}(T)$ is not divisible by p.

As mentioned earlier, a theorem of Tate shows the Frobenius polynomials parameterize isogeny classes.

Theorem 2.1.5. *[7, Thm. 1] Let A and B be abelian varieties over a finite field $\mathbb{F}_q$, with characteristic polynomials $f_{A/\mathbb{F}_q}$ and $f_{B/\mathbb{F}_q}$. Then A and B are $\mathbb{F}_q$-isogenous if and only if $f_{A/\mathbb{F}_q} = f_{B/\mathbb{F}_q}$.*

We now specialize to the setting generally considered in this paper. Let $A/\mathbb{F}_p$ be an abelian variety of dimension g. Then the characteristic polynomial of Frobenius can be factored over $\mathbb{C}$ as

$$f_{A/\mathbb{F}_p}(T) = (T - \alpha_1)\dots(T - \alpha_g)(T - \overline{\alpha}_1)\dots(T - \overline{\alpha_g})$$

for $\alpha_j = \sqrt{p}\exp(i\theta_j)$. Note that α_j is an eigenvalue of the p Frobenius endmorphism, and therefore α_j^n is an eigenvalue of the p^n Frobenius endomorphism. Therefore after base change to $\mathbb{F}_{p^n}$, the p^n Frobenius endomorphism has characteristic polynomial

$$f_{A/\mathbb{F}_{p^n}}(T) = (T - \alpha_1^n)\dots(T - \alpha_g^n)(T - \overline{\alpha_1}^n)\dots(T - \overline{\alpha_g}^n)$$

where $\alpha_j^n = \sqrt{p^n}\exp(in\theta_j)$. Thus, many invariants of A over extensions of $\mathbb{F}_p$ are controlled by the sequence $\{(n\theta_1, \ldots, n\theta_g)\}$. We will eventually need a notion of independence for $\{\theta_1, \ldots, \theta_g\}$, which is called the angle rank of A.

Definition 2.1.6. The angle rank of A is the quantity

$$\delta(A) = \dim_{\mathbb{Q}}(\text{Span}_{\mathbb{Q}}(\{\arg(\alpha_j) \ : \ 1 \leq j \leq 2g\} \cup \{\pi\})) - 1$$

which takes value $\delta(A) \in \{0, \ldots, g\}$.

2.2 Elliptic Curves

We now specialize to elliptic curves, which are abelian varieties of dimension 1. Even the specialized case of elliptic curves has proved important by their use in cryptography, integer factorization, and in the proof of Fermat's last theorem.

2.2.1 Background and Point Counts

An elliptic curve E over a field K is an abelian variety of dimension $g = 1$. It has an affine model given by the Weierstrass equation

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

where $a_1, a_2, a_3, a_3, a_4, a_5, a_6 \in K$. If $\text{char}(K) \neq 2, 3$ then by completing the square and depressing the cubic, this Weierstrass equation can be simplified to

$$E : y^2 = x^3 + ax + b$$

for $a, b \in K$. As previously mentioned, the K points of E form a group, where the addition law for two points is given by a certain rational function in terms of the coordinates of the points. Geometrically, the group law is that any three collinear points sum to the identity. For an elliptic curve over a finite field K, the number of K-rational points of E is denoted $\#E(K)$. By Tate's isogeny theorem (Theorem 2.1.5), if K is a finite field, then the isogeny class of E is determined by $\#E(K)$. Again, the Frobenius endormorphism plays a central role in the theory.

Theorem 2.2.1. *Let q be a power of a prime and let $E/\mathbb{F}_q$ be an elliptic curve. Denote the q^{th}-power Frobenius endomorphism by*

$$\begin{aligned} \phi : E/\mathbb{F}_q &\to E/\mathbb{F}_q \\ (x, y) &\mapsto (x^q, y^q) \end{aligned}$$

and define $a = q + 1 - \#E(\mathbb{F}_q)$.

1. *The Frobenius polynomial $T^2 - aT + q$ in $\mathbb{Z}[T]$ factors over $\mathbb{C}$ as $(T - \alpha)(T - \overline{\alpha})$, with $|\alpha| = \sqrt{q}$, and therefore $|a| \leq 2\sqrt{q}$.*

2. *Over the degree m extension of $\mathbb{F}_q$, the number of points is*

$$\#E(\mathbb{F}_{q^m}) = q^m + 1 - (\alpha^m + \overline{\alpha}^m).$$

The number a is called the trace of Frobenius, and is in fact the trace of the induced matrix $\phi_\ell \in \mathrm{GL}_2(\mathbb{Z}_\ell)$. Knowing the point count $\#E(\mathbb{F}_q)$ is equivalent to knowing a. We often normalize the trace of Frobenius as

$$\overline{a} = \frac{a}{\sqrt{q}} \in [-2, 2].$$

We now consider $E/\mathbb{F}_p$ base changed up to $\mathbb{F}_{p^n}$. Note that ϕ^n is the Frobenius endomorphism on E over $\mathbb{F}_{p^n}$. Therefore we have the characteristic polynomial

$$\det(T - \phi_\ell^n) = T^2 - a_n T + p^n = (T - \alpha^n)(T - \overline{\alpha}^n)$$

where $\alpha^n = \sqrt{p^n}\exp(ni\theta)$. Thus, if one knows θ over $\mathbb{F}_p$, one can easily calculate a_n and the characteristic polynomial over $\mathbb{F}_{p^n}$. In fact, we have the following recurrence relation over extensions in terms of a_1;

$$a_2 = a_1^2 - 2p$$

$$a_n = a_1 a_{n-1} - p a_{n-2}$$

for traces of $p^{n\text{th}}$-power Frobenius endomorphisms (see [5, exercise 5.13]).

The Frobenius angles give a quick way to compute the (absolute value of the) discriminant of the characteristic polynomial of Frobenius over extensions.

Lemma 2.2.2. *Let $E/\mathbb{F}_p$ be an ordinary elliptic curve. Let Δ_n denote the discriminant of the characteristic polynomial of Frobenius over $\mathbb{F}_{p^n}$. Then*

$$|\Delta_n| = 4p^n \sin^2(n\theta), \quad a_n = 2\sqrt{p^n}\cos(n\theta)$$

where θ is the Frobenius angle of E over $\mathbb{F}_p$.

Proof. This quickly follows from the identities $a_n = \alpha^n + \overline{\alpha}^n$ and $\alpha = \sqrt{p^n}\exp(ni\theta)$. □

We'll conclude this subsection with a fact about the Frobenius angles which will be used later.

Lemma 2.2.3. *Let $E/\mathbb{F}_p$ be an ordinary elliptic curve. Then the Frobenius angles are not rational multiples of π.*

Note 2.2.4. In the case of an elliptic curve over $\mathbb{F}_p$ the following are equivalent, due to [3].

- E is ordinary.
- $a_1 \neq 0$.
- For all $n \in \mathbb{Z}_{>0}$, $\alpha^n \notin \mathbb{R}$.

Proof. Suppose $\theta = \frac{x\pi}{y}$ for $x, y \in \mathbb{Z}$. Then

$$\begin{aligned}\alpha^y &= \sqrt{p^y}\exp(ix\pi)\\ &= \mu\sqrt{p^y}\end{aligned}$$

where $\mu = \pm 1$ depending on the parity of x. However, then $\alpha^y \in \mathbb{R}$, but E is ordinary, and therefore θ is not a rational multiple of π. □

2.2.2 Endomorphism Rings and Size of an Isogeny Class

Fix a prime p, an integer $n \geq 1$ and an integer a_n with $|a_n| \leq 2\sqrt{p^n}$. Then, by Tate's isogeny theorem (Theorem 2.1.5) the set of (isomorphism classes of) elliptic curves over $\mathbb{F}_{p^n}$ with $p^n + 1 - a_n$ points defines an isogeny class, which we will denote by $I(a_n)$. By Theorem 4.1 in [4], $I(a_n)$ is not empty.

We will consider the case that a_n and p are coprime (that is, any curve in $I(a_n)$ is ordinary). The endomorphism ring of any curve $E \in I(a_n)$ contains $\mathcal{O}_{a_n,p,n} = \mathbb{Z}[T]/(T^2 - a_nT + p^n)$, which is an order in the quadratic imaginary field $K_{a_n,p,n} = \mathbb{Q}(\sqrt{a_n^2 - 4p^n})$. Conversely, if $\mathcal{O} \subset K_{a_n,p,n}$ is an order containing $\mathcal{O}_{a_n,p,n}$, then $\mathcal{O}$ occurs as the endomorphism ring of an elliptic curve E in $I(a_n)$. Waterhouse shows this in [4, Thm. 4.2], using a lattice and quotient construction in the vector space $V_\ell(E) = T_\ell(E) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$. An isogeny between two elliptic curves $\phi : E_1 \to E_2$ induces an isomorphism $V_\ell(E_2) \to V_\ell(E_2)$ that is equivariant with respect to the Frobenius endomorphism, and therefore the characteristic polynomial of Frobenius is the same for E_1 and E_2.

Thus, to find the number of curves in an isogeny class $I(a_n)$, one may count the number of curves with endomorphism ring $\mathcal{O}$, for each order $\mathcal{O}$ containing $\mathcal{O}_{a_n,p,n}$. This leads to the Kronecker class number.

Definition 2.2.5. Let $\mathcal{O}$ be an order in a quadratic imaginary field with discriminant Δ, let $h(\mathcal{O})$ denote the class number of $\mathcal{O}$, and $h^*(\mathcal{O}) = h(\mathcal{O})/(\#\mathcal{O}^\times)$. Use $\mathcal{O}_{\text{max}}$ to denote the ring of integers in the ambient field. The Kronecker class number, $H^*(\Delta)$, is

$$H^*(\Delta) = \sum_{\mathcal{O} \subset \mathcal{O}' \subset \mathcal{O}_{\text{max}}} h^*(\mathcal{O}').$$

Schoof gives the following count of the size of the isogeny class $I(a_n)$ which relies on the Kronecker class number.

Theorem 2.2.6. *[8, Thm. 4.6] Let a_n be coprime to p, and let $I(a_n)$ be the isogeny class of elliptic curves that have $\#E(\mathbb{F}_{p^n}) = p^n + 1 - a_n$ points. Then the size of the isogeny class is*

$$\#I(a_n) = H^*(a_n^2 - 4p^n).$$

Katz, in [9, cor. 5.2], uses the Brauer-Siegel formula for $h^*(\mathcal{O}_{\text{max}})$ to find the following bounds on the Kronecker class number.

Theorem 2.2.7. *For any real $\epsilon > 0$, there exists $C_\epsilon > 0$ such that for any quadratic imaginary order $\mathcal{O}$ with $|\Delta| \geq C_\epsilon$, we have*

$$|\Delta|^{1/2-\epsilon} \leq H^*(\mathcal{O}) \leq |\Delta|^{1/2+\epsilon}.$$

Recall the notation of 2.2.1 and combine 2.2.6, 2.2.7 and the discriminant calculation in 2.2.2 to get the following corollary.

Corollary 2.2.8. *Let a_n be coprime to p. Then for an isogeny class $I(a_1)$ over $\mathbb{F}_p$ with Frobenius angle θ_1, we have the following bound on the size of the isogeny class over extensions:*

$$\left|4p^n \sin^2(n\theta_1)\right|^{1/2-\epsilon} \leq \#I(a_n) \leq \left|4p^n \sin^2(n\theta_1)\right|^{1/2+\epsilon}.$$

Therefore we expect the size of an isogeny class to be roughly $I(a_n) \approx 2p^{n/2}$, as long as $n\theta_1$ is away from a multiple of π.

We have now seen that, given $E/\mathbb{F}_p$, we can calculate the trace of Frobenius (and by extension, the point count of E) and the discriminant (and therefore roughly the size of the isogeny class) from the values of the sequence $\{\theta_n\}$. Therefore the next chapter will examine explicit and quantitative results for the calculation of traces and discriminants from the sequence $\{\theta_n\}$.

Chapter 3

Quasi-Monte Carlo Theory

Given a function $f(x)$, one might estimate the integral $\int_0^1 f(x)dx$ by taking some collection of points $\{\theta_1, \dots, \theta_N\}$ and calculating the sum $\frac{1}{N}\sum_{n=1}^{N} f(\theta_n)$. Monte Carlo methods aim to pick the terms of the sequence $\{\theta_1, \dots, \theta_N\}$ at random. We, however, will focus on quasi-Monte Carlo integration, in which one picks a sequence $\{\theta_1, \dots, \theta_N\}$ to use in the estimation, instead of picking points at random. The error in the quasi-Monte Carlo integral method can be bounded through properties of $f(x)$ and $\{\theta_1, \dots, \theta_N\}$.

3.1 One dimensional quasi-Monte Carlo

We now turn our attention to sequences and estimation of integrals by finite sums. A reference for much of the general theory is [10].

For this section, let $\{\theta_n\}_{n=1}^{\infty}$ be a real sequence contained in the half-open interval $[0, 1)$. Let $J \subseteq [0, 1)$ and define $A(J, N)$ to be the number of terms of $\{\theta_n\}_{n=1}^{N}$ contained in J, that is

$$A(J, N) = \#\{\theta_n \in J \ : \ 1 \leq n \leq N\}.$$

Let $e(z) = e^{2\pi iz}$ and let λ denote the Lebesgue measure. If J is the interval $J = [a, b] \subset \mathbb{R}$, then $\lambda(J) = b - a$.

Definition 3.1.1. The sequence $\{\theta_n\}_{n=1}^{\infty}$ is equidistributed (sometimes called uniformly distributed) in the interval $[0, 1)$ if for all pairs $a, b \in \mathbb{R}$ with $0 \leq a < b < 1$ we have

$$\lim_{N\to\infty} \frac{A([a, b), N)}{N} = \lambda([a, b)).$$

Roughly, a sequence is equidistributed if, after N terms, any subinterval has about the same number of terms of the sequence as any other subinterval of the same length. Then, one could use an equidistributed sequence on $[0, 1)$ to approximate the average value of a function f by averaging the value of f at the first N terms of the sequence. This leads to the following integral criterion for equidistribution.

Theorem 3.1.2. *The sequence $\{\theta_n\}_{n=1}^{\infty}$ is equidistributed in $[0, 1)$ if and only if, for every Riemann-integrable function $f : [0, 1) \to \mathbb{C}$, we have*

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} f(\theta_n) = \int_0^1 f(x)dx.$$

There also exists the Weyl citerion for equidistribution, which roughly states that the first N terms of an equidistributed sequence are evenly spaced on the unit circle after exponentiation. See Figure 3.1 for a visualization.

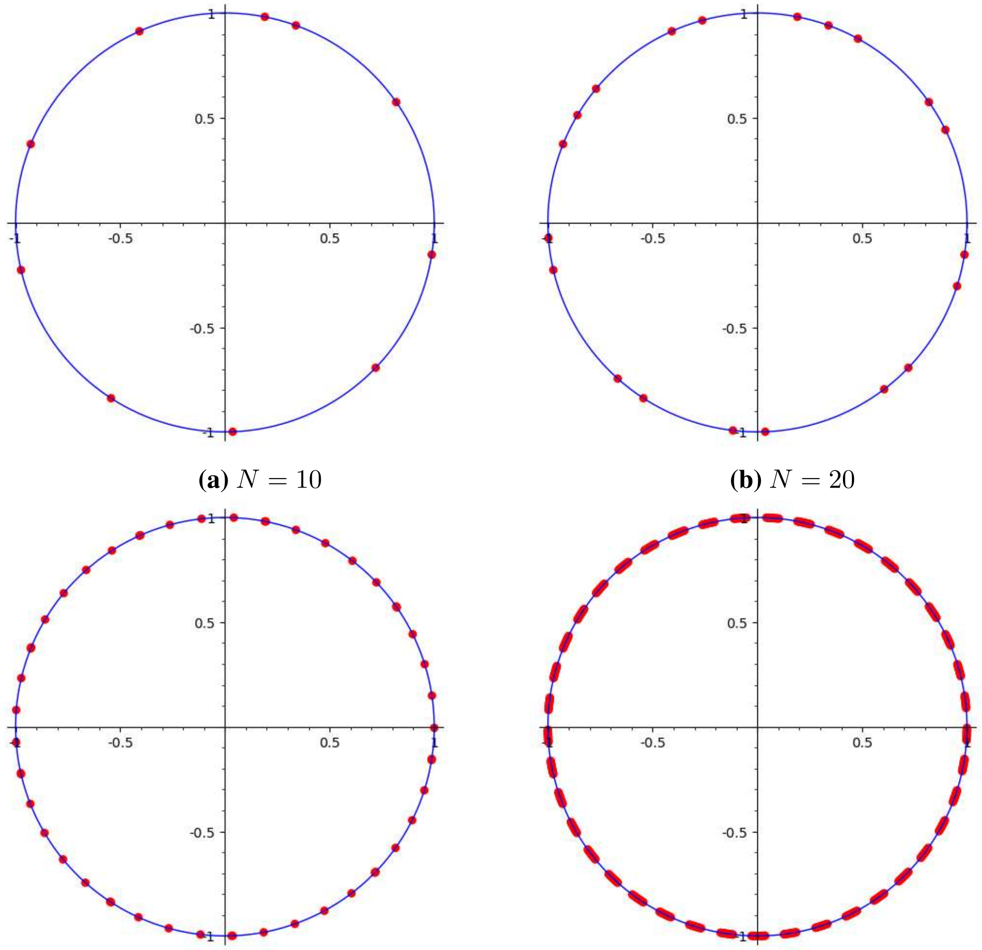
Theorem 3.1.3 (Weyl Criterion)**.** *The sequence $\{\theta_n\}_{n=1}^{\infty}$ is equidistributed in $[0, 1)$ if and only if for all non-zero $h \in \mathbb{Z}$,*

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} e(h\theta_n) = 0.$$

Example 3.1.4. Let θ be an irrational number. Note that for all non-zero $h \in \mathbb{Z}$,

$$\begin{aligned} \frac{1}{N} \sum_{n=1}^{N} e(hn\theta) &= \frac{e(h\theta)(1 - e(hN\theta))}{N(1 - e(h\theta))} \\ \left| \frac{1}{N} \sum_{n=1}^{N} e(hn\theta) \right| &= \left| \frac{e(h\theta)e(hN\theta/2)(e(-hN\theta/2) - e(hN\theta/2))}{Ne(h\theta/2)(e(-h\theta/2) - e(h\theta/2))} \right| \\ &= \left| \frac{\sin(\pi hN\theta)}{N\sin(\pi h\theta)} \right| \\ &\leq \frac{1}{N|\sin(\pi h\theta)|}. \end{aligned}$$

It then follows from the Weyl criterion that the sequence $\{n\theta \pmod 1\}_{n=1}^{\infty}$ (often called a Kronecker sequence) is equidistributed in $[0, 1)$ since $\frac{1}{N|\sin(\pi h\theta)|} \to 0$ as $N \to \infty$.



(a) $N = 10$ **(b)** $N = 20$

(c) $N = 50$ **(d)** $n = 500$

Figure 3.1: The first N terms of an equidistributed sequence exponentiated onto the unit circle.

However, we would like an explicit version of the discrete integration rule from Theorem 3.1.2. That is, we would like a result that gives an explicit bound for the error on estimating an integral by the average function value at the first N terms of a sequence. There are two ways that an error term arises. While $\{\theta_n\}_{n=1}^{\infty}$ may be equidistributed, the first N terms may be bunched together in one subinterval, and further apart in another subinterval. This is measured by the discrepancy of $\{\theta_n\}_{n=1}^{N}$. Another way an error term can appear is the function may oscillate or have many small peaks that may not be seen by evaluating the function at finitely many points. This is measured by the variation of a function. We now formalize these definitions.

Definition 3.1.5. The discrepancy of a finite real valued sequence $\{\theta_1, \ldots, \theta_N\}$ is defined as

$$D_N = \sup_{0 \leq \alpha < \beta \leq 1} \left| \frac{A([\alpha, \beta), N)}{N} - \lambda([\alpha, \beta)) \right|.$$

In the star discrepancy, the supremum simply runs over all intervals of the form $[0, \beta)$ rather than intervals of the form $[\alpha, \beta)$. The rest of this paper will generally focus on the star discrepancy.

Definition 3.1.6. The star discrepancy of a finite real valued sequence $\{\theta_1, \ldots, \theta_N\}$ is defined as

$$D_N^* = \sup_{0 < \beta \leq 1} \left| \frac{A([0, \beta), N)}{N} - \lambda([0, \beta)) \right|.$$

Note that $D_N^* \leq D_N$, as every interval considered in calculating D_N^* is also considered for D_N.

Definition 3.1.7. The variation of a real valued function f on $[0, 1) \subset \mathbb{R}$ is

$$V(f) = \sup_{P \in \mathcal{P}} \sum_{j=0}^{n_P - 1} |f(x_{j+1}) - f(x_j)|$$

where $\mathcal{P}$ is the set of partitions of the form $P = \{x_0 < x_1 < \ldots < x_{n_P}\}$ with $x_i \leq x_{i+1}$. If f has finite variation, then f is of bounded variation.

Example 3.1.8. Let $\chi_J(x)$ be the indicator function of the subinterval $J = [a, b] \subset [0, 1]$, that is

$$\chi_J(x) = \begin{cases} 1 & x \in J \\ 0 & \text{else.} \end{cases}$$

Then $V(\chi_J) = 2$, which is achieved by the partition at the points $\{0 < \frac{b-a}{2} < 1\}$.

The following theorem bounds the error of using a finite sequence to approximate an integral.

Theorem 3.1.9 (Koksma's Inequality). *Let f be a function of bounded variation, and let $\{\theta_1, \ldots, \theta_N\}$ be a sequence in the interval $[0, 1) \subset \mathbb{R}$, with star discrepancy D_N^*. Then*

$$\left| \frac{1}{N} \sum_{n=1}^{N} f(\theta_n) - \int_0^1 f(x)dx \right| \leq V(f) D_N^*.$$

However finding the discrepancy of a sequence is computationally difficult, so in order to find bounds on the above integral estimation, one must find bounds on the discrepancy of a sequence. The Erdős-Turán inequality is one such tool (see [10, eqn. 2.42]).

Theorem 3.1.10. *There exists an absolute constant C such that, for any finite real sequence $\{\theta_1, \ldots, \theta_N\}$ in $[0, 1) \subset \mathbb{R}$, the inequality*

$$D_N^* \leq C \left(\frac{1}{H} + \sum_{h=1}^{H} \frac{1}{h} \left| \frac{1}{N} \sum_{n=1}^{N} e(h\theta_n) \right| \right)$$

holds for any positive $H \in \mathbb{Z}$.

Vaaler gives a more explicit bound on the discrepancy of a sequence, which we will use frequently.

Theorem 3.1.11. *[11, Pg.214] Let $\{\theta_1, \ldots, \theta_N\}$ be a finite sequence in $[0, 1) \in \mathbb{R}$, and let $H \in \mathbb{Z}_{>0}$ be an arbitrary positive integer. Then the star discrepancy of the sequence satisfies*

$$D_N^* \leq \frac{1}{H+1} + 2 \sum_{h=1}^{H} \left(\frac{1}{\pi h} + \frac{1}{H+1} \right) \left| \frac{1}{N} \sum_{n=1}^{N} e(h\theta_n) \right|.$$

3.2 Higher dimensional quasi-monte Carlo

To find results for higher dimensional abelian varieties, or for multiple isogeny classes of elliptic curves, we consider equidistribution and quasi-Monte Carlo in higher dimensions. For this section, fix a dimension $s \in \mathbb{Z}_{>0}$. Let $\boldsymbol{a} = (a_1, \ldots, a_s), \boldsymbol{b} = (b_1, \ldots, b_s)$ be points in $[0, 1)^s \subset \mathbb{R}^s$. If $a_n < b_n$ (respectively, $a_n \leq b_n$) for $1 \leq n \leq s$, then $\boldsymbol{a} < \boldsymbol{b}$ (respectively, $\boldsymbol{a} \leq \boldsymbol{b}$). By $[\boldsymbol{a}, \boldsymbol{b})$ we denote the set of points $\boldsymbol{x}$ such that $\boldsymbol{a} \leq \boldsymbol{x} < \boldsymbol{b}$, and similarly for $[\boldsymbol{a}, \boldsymbol{b}]$.

We again use λ to denote the Lebesgue measure. Let $\{\boldsymbol{\theta}_n\}_{n=1}^{\infty}$ be a sequence with $\boldsymbol{\theta}_n \in [0,1)^s \subset \mathbb{R}^s$, and let $J \subset [0,1)^s$ be a subset. We will again use the notation $A(J,N)$ as

$$A(J,N) = \#\{\boldsymbol{\theta}_n \in J \,:\, 1 \leq n \leq N\}.$$

Definition 3.2.1. The sequence $\{\boldsymbol{\theta}_n\}_{n=1}^{\infty}$ is equidistributed in $[0,1)^s$ if for all $\boldsymbol{a} \leq \boldsymbol{b}$

$$\lim_{N \to \infty} \frac{A([\boldsymbol{a}, \boldsymbol{b}), N)}{N} = \lambda([\boldsymbol{a}, \boldsymbol{b})).$$

Much like the one dimensional case, a sequence is equidistributed if the number of terms in a hypercube is about the same as the number of terms in any other hypercube of the same measure. This again affords a discrete calculation of a function at the points of the sequence to estimate the average value of a function.

Theorem 3.2.2. *The sequence $\{\boldsymbol{\theta}_n\}_{n=1}^{\infty}$ with $\boldsymbol{\theta}_n \in [0,1)^s \in \mathbb{R}^s$ is equidistributed in $[0,1)^s$ if and only if for every continuous $f : [0,1)^s \to \mathbb{R}$ we have*

$$\lim_{N \to \infty} \frac{1}{N} \sum_{n=1}^{N} f(\boldsymbol{\theta}_n) = \int_{[0,1)^s} f(\boldsymbol{x}) d\boldsymbol{x}.$$

We have another criterion for equidistribution which states that, for any lattice point in $\mathbb{Z}^s$, the inner product of the lattice point with points of the sequence evenly generates points on the unit circle. We use $\langle \bullet, \star \rangle$ for the usual inner product on $\mathbb{R}^s$.

Theorem 3.2.3. *The sequence $\{\boldsymbol{\theta}_n\}_{n=1}^{\infty}$ with $\boldsymbol{\theta}_n \in [0,1)^s \in \mathbb{R}^s$ is equidistributed in $[0,1)^s$ if and only if for every point $\boldsymbol{h} \neq \boldsymbol{0}$ of the lattice $\mathbb{Z}^s$ we have*

$$\lim_{N \to \infty} \frac{1}{N} \sum_{n=1}^{N} e(\langle \boldsymbol{h}, \boldsymbol{\theta}_n \rangle) = 0.$$

Similar to the one dimensional case, we would like an explicit version of this integral criterion. To this end, we'll look at multi-dimensional discrepancy.

Definition 3.2.4. Let $\{\boldsymbol{\theta}_1, \ldots \boldsymbol{\theta}_N\}$ be a finite sequence in $[0,1)^s \subset \mathbb{R}^s$, and let λ be the s-dimensional Lebesgue measure. The discrepancy of this sequence is defined as

$$D_N = \sup_J \left| \frac{A(J,N)}{N} - \lambda(J) \right|$$

where the supremum runs over all boxes $[\boldsymbol{a}, \boldsymbol{b})$ in $[0,1)^s$.

Definition 3.2.5. Let $\{\boldsymbol{\theta}_1, \ldots \boldsymbol{\theta}_N\}$ be a finite sequence in $[0,1)^s \subset \mathbb{R}^s$, and let λ be the s-dimensional Lebesgue measure. The star discrepancy of this sequence is defined as

$$D_N^* = \sup_{J^*} \left| \frac{A(J^*,N)}{N} - \lambda(J^*) \right|$$

where the supremum runs over all boxes $[\mathbf{0}, \boldsymbol{b})$ in $[0,1)^s$.

Theorem 3.2.6. *The discrepancy of an s-dimensional sequence satisfies*

$$D_N^* \leq D_N \leq 2^s D_N^*.$$

Definition 3.2.7. Let $\boldsymbol{h} = (h_1, h_2, \ldots h_s) \in \mathbb{Z}^s$ be a lattice point. Define the notation

$$r(\boldsymbol{h}) = \prod_{i=1}^{s} \max\{1, |h_i|\}$$

and

$$||\boldsymbol{h}||_\infty = \max\{|h_1|, |h_2|, \ldots |h_s|\}.$$

The Koksma-Hlawka inequality is the multi-dimensional generalization of Koksma's inequality from Theorem 3.1.9. This result uses variation in the sense of Hardy and Krause. Roughly, the variation in the sense of Hardy and Krause is the sum over all Vitali variations (restricted to the above faces) of dimension d and smaller. See [12] for a full definition, and note the example on [12, pg. 9] that an indicator function on $[0,1]^s$ for the region from $\mathbf{0}$ to $\mathbf{1/2}$ has Hardy-Krause variation $2^s - 1$.

Theorem 3.2.8. *Let $\{\boldsymbol{\theta}_1, \ldots, \boldsymbol{\theta}_N\}$ be a finite sequence in $[0,1)^s \subset \mathbb{R}^s$ with star discrepancy D_N^*. For any function f of bounded variation $V(f)$ (in the sense of Hardy and Krause) on $[0,1)^s$ we have*

$$\left| \frac{1}{N} \sum_{n=1}^{N} f(\boldsymbol{\theta}_n) - \int_{[0,1)^s} f(\boldsymbol{x}) d\boldsymbol{x} \right| \leq V(f) D_N^*.$$

As in the one dimensional case, the discrepancy of a sequence can be hard to compute. The Erdős-Turán-Koksma inequality gives an upper bound (see [13, thm. 1.21]).

Theorem 3.2.9. *Let $\boldsymbol{\theta}_1 \ldots \boldsymbol{\theta}_N$ be a finite sequence in $[0,1)^s \subset \mathbb{R}^s$ and let $H \in \mathbb{Z}_{>0}$ be an arbitrary positive integer. Then the star discrepancy of the sequence satisfies*

$$D_N^* \leq \left(\frac{3}{2}\right)^s \left(\frac{2}{H+1} + \sum_{0<||\boldsymbol{h}||_\infty \leq H} \frac{1}{r(\boldsymbol{h})} \left| \frac{1}{N} \sum_{n=1}^{N} e(\langle \boldsymbol{h}, \boldsymbol{\theta}_n \rangle) \right| \right).$$

3.3 Further results in Quasi-Monte Carlo Theory

The error in Koksma's inequality is much harder to control in dimensions larger than one, as both the discrepancy and variation become more wild. There are several effective results that give better control over the error involved in the integral estimation, which we now study. The first is due to [14], which is a probabilistic result regarding the discrepancy of a Kronecker sequence.

Theorem 3.3.1 (Beck)**.** *Let $\boldsymbol{\theta} = (\theta_1, \ldots \theta_s) \in \mathbb{R}^s$ with $1, \theta_1, \ldots \theta_s$ linearly independent over $\mathbb{Z}$. Consider the sequence $\{n\boldsymbol{\theta} \pmod 1\}$ in which the j^{th} component of the n^{th} term is $n\theta_j \pmod 1$.*

Then for almost every $\boldsymbol{\theta}$ and for every $\epsilon > 0$,

$$D_N^* \ll_{s,\epsilon} \frac{(\log N)^s (\log\log N)^{1+\epsilon}}{N}$$

in Vinogradov notation.

However, given more control over the properties of $\boldsymbol{\theta}$, stronger asymptotics for the sequence $\{n\boldsymbol{\theta} \pmod 1\}$ are possible. The relevant notion is the type of $\boldsymbol{\theta}$, which in the one dimensional case is closely related to the measure of irrationality. We use $\|x\|$ to denote the distance from x to the closest integer.

Definition 3.3.2. For a real number η, an s-tuple $\boldsymbol{\theta} \in (\mathbb{R} \setminus \mathbb{Q})^s$ is said to be of finite type η if η is the infimum of all numbers σ for which there exists a positive constant c (which depends on $\sigma, \boldsymbol{\theta}$) such that

$$r(\boldsymbol{h})^\sigma ||\boldsymbol{h} \cdot \boldsymbol{\theta}|| \geq c \quad \text{for all } \boldsymbol{h} \neq \mathbf{0}$$

for all $\boldsymbol{h} \in \mathbb{Z}^s \setminus \{\mathbf{0}\}$.

For all irrational $\boldsymbol{\theta}$ we have $\eta \geq 1$ (see [15, Prop. 4.18]). There are several explicit constructions of s-tuples with $\eta = 1$, such as algebraic irrationals (due to Schmidt [16]) and $\boldsymbol{\theta} = (e^{r_1}, \ldots, e^{r_s})$ for distinct nonzero $r_1, \ldots r_s \in \mathbb{Q}$ (due to Baker [17]). For dimension $s = 1$, an equivalent notion is called the Liouville-Roth irrationality measure. Under Lebesgue measure almost all real numbers have type $\eta = 1$ [18, Thm E.3].

The type of a point $\boldsymbol{\theta}$ dictates the error involved in Koksma's inequality for the Kronecker sequence $\{n\boldsymbol{\theta} \pmod 1\}$. The first result in this direction uses the type to bound the discrepancy of the Kronecker sequence. See [10, exercise 3.17], [15, Thm. 4.19], or [19, Thm. 9].

Theorem 3.3.3 (Niederreiter)**.** *Let $\boldsymbol{\theta}$ be an s-tuple of finite type η. The discrepancy of the Kronecker sequence $\{n\boldsymbol{\theta} \pmod 1\}$ satisfies*

$$D_N^* \ll_{s,\epsilon} \frac{1}{N^{1/((\eta-1)s+1)-\epsilon}}.$$

We can further improve the error involved in the numerical integration rule if we also apply restrictions upon the function f. Let f be a function on $\mathbb{R}^s$ which is periodic with period 1 in each variable, and has absolutely convergent Fourier series

$$f(\boldsymbol{t}) = \sum_{\boldsymbol{h}} c_{\boldsymbol{h}} e(\boldsymbol{h} \cdot \boldsymbol{t})$$

for lattice points $\boldsymbol{h} = (h_1, \ldots h_s) \in \mathbb{Z}^s$. We will impose a condition on how rapidly the Fourier coefficients of f go to 0.

Definition 3.3.4. For real numbers $k > 1, C > 0$, we say that $f \in \mathscr{E}^k(C)$ if the Fourier coefficients satisfy

$$|c_{\boldsymbol{h}}| \leq Cr(\boldsymbol{h})^{-k} \text{ for all } \boldsymbol{h} \neq \mathbf{0} \tag{3.1}$$

and that $f \in \mathscr{E}^k$ if $f \in \mathscr{E}^k(C)$ for some $C > 0$.

A sufficient condition with C that can be given explicitly is due to Zaremba [20]. Let $k > 1$ be an integer and suppose all partial derivatives

$$\frac{\partial^{q_1+\ldots+q_s} f(\boldsymbol{t})}{\partial t_1^{q_1} \ldots \partial t_s^{q_s}} \;\; 0 \leq q_i \leq k-1 \text{ for } 1 \leq j \leq s \tag{3.2}$$

exist and are of bounded variation in the sense of Hardy and Krause (again see [12] for a description of Hardy-Krause variation). Then $f \in \mathscr{E}^k(C)$ for an explicit C.

Given a such a function f with rapidly vanishing Fourier coefficients and an s-tuple $\boldsymbol{\theta}$ of finite type η, the quasi-Monte Carlo integration rule has error $O(1/N)$. See Niederrieter [21, Thm. 5.2], [22], [23] and Haselgrove [24].

Theorem 3.3.5. *Let $\boldsymbol{\theta} \in \mathbb{R}^s$, $s \geq 1$ be a point of finite type η. Then*

$$\frac{1}{N}\sum_{n=1}^{N} f(n\boldsymbol{\theta}) - \int_{I^s} f(\boldsymbol{t})d\boldsymbol{t} = O\left(\frac{1}{N}\right) \tag{3.3}$$

for every f periodic of period 1 and $f \in \mathscr{E}^k$ with $k > \eta$.

We'll summarize the beginning of the proof to show how the type $\boldsymbol{\theta}$ and the hypothesis of $f \in \mathscr{E}^k$ is used.

Proof Sketch. We'll give an outline of the start of the proof given in [23]. Let $f \in \mathscr{E}^k(M)$, and let $\lambda > 0$ so that there exists a constant M such that $|c_{\boldsymbol{h}}| \leq Mr(\boldsymbol{h})^{-k-\lambda}$. Then f converges absolutely to its Fourier series, so that

$$\begin{aligned}\sum_{n=1}^{N} f(n\boldsymbol{\theta}) &= \sum_{n=1}^{N}\sum_{\boldsymbol{h}} c_{\boldsymbol{h}} e(\boldsymbol{h}\cdot n\boldsymbol{\theta})\\ &= \sum_{\boldsymbol{h}} c_{\boldsymbol{h}} \sum_{n=1}^{N} e(\boldsymbol{h}\cdot n\boldsymbol{\theta})\\ &= Nc_{\boldsymbol{0}} + \sum_{\boldsymbol{h}\neq\boldsymbol{0}} c_{\boldsymbol{h}} \sum_{n=1}^{N} e(\boldsymbol{h}\cdot n\boldsymbol{\theta})\end{aligned}$$

Recall that from the structure of a Fourier series, we have $c_{\boldsymbol{0}} = \int_{[0,1)^s} f(\boldsymbol{x})d\boldsymbol{x}$ to get

$$\begin{aligned}\left|\frac{1}{N}\sum_{n=1}^{N} f(n\boldsymbol{\theta}) - \int_{[0,1)^s} f(\boldsymbol{x})d\boldsymbol{x}\right| &= \left|c_{\boldsymbol{0}} + \frac{1}{N}\sum_{\boldsymbol{h}\neq\boldsymbol{0}} c_{\boldsymbol{h}} \sum_{n=1}^{N} e(\boldsymbol{h}\cdot n\boldsymbol{\theta}) - c_{\boldsymbol{0}}\right|\\ &= \left|\frac{1}{N}\sum_{\boldsymbol{h}\neq\boldsymbol{0}} c_{\boldsymbol{h}} \sum_{n=1}^{N} e(\boldsymbol{h}\cdot n\boldsymbol{\theta})\right|.\end{aligned}$$

Then by the triangle inequality we have

$$\left|\frac{1}{N}\sum_{\boldsymbol{h}\neq\boldsymbol{0}} c_{\boldsymbol{h}} \sum_{n=1}^{N} e(\boldsymbol{h}\cdot n\boldsymbol{\theta})\right| \leq \frac{1}{N}\sum_{\boldsymbol{h}\neq\boldsymbol{0}} |c_{\boldsymbol{h}}| \left|\sum_{n=1}^{N} e(\boldsymbol{h}\cdot n\boldsymbol{\theta})\right|.$$

Recall we use $\|x\|$ to denote the distance to the nearest integer. Then for $x \in \mathbb{R}\setminus\mathbb{Z}$

$$\left|\sum_{n=1}^{N} e(nx)\right| \leq \frac{1}{2\|x\|}.$$

Therefore we have the estimate

$$\begin{aligned} \left|\frac{1}{N}\sum_{n=1}^{N} f(n\boldsymbol{\theta}) - \int_{[0,1)^s} f(\boldsymbol{x})d\boldsymbol{x}\right| &\leq \frac{1}{2N}\sum_{\boldsymbol{h}\neq\boldsymbol{0}} \frac{|c_{\boldsymbol{h}}|}{\|\boldsymbol{h}\cdot\boldsymbol{\theta}\|} && (3.4) \\ &\leq \frac{M}{2N}\sum_{\boldsymbol{h}\neq\boldsymbol{0}} \frac{1}{r^{\eta+\lambda}(\boldsymbol{h})\,\|\boldsymbol{h}\cdot\boldsymbol{\theta}\|}. && (3.5) \end{aligned}$$

where we have used the fact that $f \in \mathscr{E}^k(M)$.

We then have the inequality

$$\sum_{\boldsymbol{h}\neq\boldsymbol{0}} \frac{1}{r^{\eta+\lambda}(\boldsymbol{h})\,\|\boldsymbol{h}\cdot\boldsymbol{\theta}\|} \leq (\eta+\lambda)^s \sum_{n_1,\ldots n_s=1}^{\infty} (n_1\ldots n_s)^{-\eta-\lambda-1} \times \sum_{\substack{\boldsymbol{h}\in\mathbb{Z}^s\setminus\boldsymbol{0} \\ |h_j|\leq n_j}} \|\boldsymbol{h}\cdot\boldsymbol{\theta}\|^{-1}$$

which may be verified by fixing an $\boldsymbol{h}$ and calculating the total coefficient of $\|\boldsymbol{h}\cdot\boldsymbol{\theta}\|^{-1}$ on the right hand side.

The type of $\boldsymbol{\theta}$ is then used to estimate the sum

$$\sum_{\substack{\boldsymbol{h}\in\mathbb{Z}^s\setminus\boldsymbol{0} \\ |h_j|\leq n_j}} \|\boldsymbol{h}\cdot\boldsymbol{\theta}\|^{-1}$$

by the following argument. If the real numbers a, b, d satisfy $\|a+b\| \geq d$ and $\|a-b\| \geq d$, then $\Big|\|a\| - \|b\|\Big| \geq d$. Choose two lattice points $\boldsymbol{h}, \boldsymbol{h}'$ with $\boldsymbol{h} \neq \pm\boldsymbol{h}'$. Then because $\boldsymbol{\theta}$ is of type η, for any $\lambda > 0$ there is a constant C such that

$$\begin{aligned}\|\boldsymbol{h}\cdot\boldsymbol{\theta} \pm \boldsymbol{h}'\cdot\boldsymbol{\theta}\| = \|(\boldsymbol{h} \pm \boldsymbol{h}')\cdot\boldsymbol{\theta}\| \geq & Cr(\boldsymbol{h}+\boldsymbol{h}')^{-\eta-\lambda/3} \\ &= Cr(2\boldsymbol{n})^{-\eta-\lambda/3}.\end{aligned}$$

Define $d = Cr(2\boldsymbol{n})^{-\eta-\lambda/3}$, so

$$\Big|\, \|\boldsymbol{h}\cdot\boldsymbol{\theta}\| - \|\boldsymbol{h}'\cdot\boldsymbol{\theta}\| \,\Big| \geq d.$$

Let $r = \lfloor 1/(2d) \rfloor$. Because $\|\boldsymbol{h}\cdot\boldsymbol{\theta}\| \geq d$, each of the intervals $[0,d), [d,2d), \dots [rd,(r+1)d)$ contains at most two numbers of the form $\|\boldsymbol{h}\cdot\boldsymbol{\theta}\|$ with none in the first interval $[0,d)$. Therefore we have the estimate

$$\sum_{\substack{\boldsymbol{h}\in\mathbb{Z}^s\backslash\boldsymbol{0} \\ |h_j|\leq n_j}} \frac{1}{\|\boldsymbol{h}\cdot\boldsymbol{\theta}\|} \leq 2\sum_{k=1}^{r} \frac{1}{kd}.$$

We have now seen how the hypotheses of $f \in \mathscr{E}^k$ and the finite type of $\boldsymbol{\theta}$ come into play. The result then follows from further estimates on

$$(\eta+\lambda)^s \sum_{n_1,\dots n_s=1}^{\infty} (n_1 \dots n_s)^{-\eta-\lambda-1}$$

and $2\sum_{k=1}^{r} \frac{1}{kd}$. □

3.4 Baker's Theorem

Baker's theorem is a result in transcendental number theory that provides a lower bound for certain logarithmic forms. This theorem finds wide applications, such as proving transcendence of some numbers and finding all imaginary quadratic fields with class number 1. We will later use Baker's theorem to prove that a certain s-tuple $\boldsymbol{\theta}$ has finite type. Wüstholz offers an expository description of the theorem in [25]. See also Baker's textbook [26] and a text from Waldschmidt [27]. The statement of Baker's theorem begins with some notions of heights, which we now state.

Let K be a number field. We'll use M_K to denote the set of normalized absolute values of K, where for the absolute value $|\cdot|_v$ we normalize by

$$\begin{cases} |x|_v = x & x \in \mathbb{Q}, x > 0, v \text{ is Archimedean} \\ |p|_v = 1/p & v \text{ is a } p\text{-adic valuation.} \end{cases}$$

Definition 3.4.1. The absolute logarithmic Weil height of an element α in a number field K is

$$h(\alpha) = \frac{1}{[K:\mathbb{Q}]} \sum_{v \in M_K} [K_v : \mathbb{Q}_v] \log \max\{|\alpha|_v, 1\}.$$

We'll use a modified height. Let $\alpha_1, \ldots, \alpha_n$ be complex numbers that are algebraic, and let $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$.

Definition 3.4.2. Let the number field K be of degree d. For $\alpha \in K$ denote by $h'(\alpha)$ a modified height,

$$h'(\alpha) = \frac{1}{d} \max\{h(\alpha), |\log(\alpha)|, 1\}.$$

Let L be the linear form

$$L = b_1 z_1 + \ldots + b_n z_n \quad (b_1, \ldots b_n) \in \mathbb{Z}^n \setminus \mathbf{0}$$

Let b be the highest common factor of $b_1, \ldots b_n$. Let $h(L)$ be the logarithmic Weil height of L, which is $d \log(\max\{|b_j|/b\})$, and define

$$h'(L) = \frac{1}{d} \max\{h(L), 1\}.$$

Theorem 3.4.3 (Baker and Wüstholz)**.** *Let* $\alpha_1, \dots \alpha_n$ *be algebraic, and not* 0 *or* 1*. If* $\Lambda = L(\log \alpha_1, \dots \log \alpha_n) \neq 0$*, then*

$$\log |\Lambda| > -C(n,d)h'(L) \prod h'(\alpha_i)$$

where

$$C(n,d) = 18(n+1)!n^{n+1}(32d)^{n+2} \log(2nd)$$

and d *is the degree of the extension* $\mathbb{Q}(\alpha_1, \dots \alpha_n)$*.*

3.5 A multivariate Vinogradov function

In [1, Sec. 3.2], Bucur, Fité and Kedlaya construct a multivariate version of a function created by Vinogradov in [28, pg. 32]. This Vinogradov function, Ψ, acts as a continuous approximation of a characteristic function on the preimage of a given interval. Importantly, one has a great deal of control over the decay of the Fourier coefficients of Ψ. We now study the construction of the multivariate Vinogradov function.

Let $\pi_j : [0,1]^s \to [0,1]^{s-1}$ be the map that forgets the j-th component of $\boldsymbol{\theta} \in [0,1]^s$. For $\boldsymbol{\vartheta} \in [0,1]^{s-1}$, define $X_j(\boldsymbol{\vartheta}) = \pi_j^{-1}(\boldsymbol{\vartheta})$.

Definition 3.5.1. Let $T : \mathbb{R}^s \to \mathbb{R}$ be a differentiable function that satisfies the following conditions:

1. T is periodic of period 1.

2. There exists a positive $K \in \mathbb{R}$ such that $|\nabla T(\boldsymbol{\theta})| \leq K$ for all $\boldsymbol{\theta} \in \mathbb{R}^s$.

3. There exists an integer $C > 0$ such that, for every $\gamma \in \mathbb{R}$ and every $\boldsymbol{\vartheta} \in [0,1]^{s-1}$ we have

$$\#\Big(T^{-1}(\gamma) \cap X_j(\boldsymbol{\vartheta})\Big) \leq C$$

for $1 \leq j \leq s$.

Note 3.5.2. The case of $s = 1$ deserves some special attention. If $s = 1$, then the map $\pi_j : [0,1]^s \to [0,1]^{s-1}$ is a map from $[0,1]$ to a one element set. Therefore, for a function $T : \mathbb{R} \to \mathbb{R}$ the third condition can be restated as follows. There exists an integer $C > 0$ such that, for every $\gamma \in \mathbb{R}$, we have

$$\#\Big(T^{-1}(\gamma) \cap [0,1]\Big) \leq C.$$

That is, the number of solutions to $T(x) = \gamma$ with $x \in [0,1]$ is bounded by C.

Let $\alpha, \beta, \Delta \in \mathbb{R}$ be such that $\Delta > 0$ and $2\Delta \leq \beta - \alpha$. Define I to be the interval (α, β) and define the sets

$$\begin{aligned} R_1 &= T^{-1}\Big((\alpha + \Delta, \beta - \Delta)\Big) \cap [0,1]^s \\ R_0 &= T^{-1}\Big(\mathbb{R} \setminus (\alpha - \Delta, \beta + \Delta)\Big) \cap [0,1]^s. \end{aligned}$$

The Vinogradov function will roughly act as an indicator of the preimage of I under T, except for small Δ sized regions around α and β.

Theorem 3.5.3. *Let $T : \mathbb{R}^s \to \mathbb{R}$ be a function satisfying the conditions of Definition 3.5.1 and let α, β, Δ be numbers such that*

$$\Delta > 0, \quad 2\Delta \leq \beta - \alpha.$$

For every $m \in \mathbb{Z}_{\geq 1}$, there exists a continuous function

$$\Psi = \Psi_{\Delta, I} : \mathbb{R}^s \to \mathbb{R}$$

that is periodic of period 1, and satisfies

1. *For $\boldsymbol{\theta} \in R_1$, we have $\Psi(\boldsymbol{\theta}) = 1$.*

2. *For $\boldsymbol{\theta} \in R_0$, we have $\Psi(\boldsymbol{\theta}) = 0$.*

3. *For all $\boldsymbol{\theta}$, we have the bounds $0 \leq \Psi(\boldsymbol{\theta}) \leq 1$.*

4. *Ψ has Fourier expansion $\Psi(\boldsymbol{\theta}) = \sum_{\boldsymbol{h} \in \mathbb{Z}^s} c_{\boldsymbol{h}} e(\boldsymbol{h} \cdot \boldsymbol{\theta})$ where $c_{\mathbf{0}} = \int_{T^{-1}((\alpha,\beta)) \cap [0,1]^s} d\boldsymbol{\theta}$ and for all $\boldsymbol{h} \neq \mathbf{0}$ we have*

$$|c_{\boldsymbol{h}}| \leq \min \left[|c_{\mathbf{0}}|, \quad \left\{ \frac{C}{\pi \max_j\{h_j\}} \prod_{j=1, h_j \neq 0}^{s} \left(\frac{mK\sqrt{s}}{2\pi |h_j| \Delta} \right)^{\rho} \right\}_{\rho=0,\ldots m} \right].$$

Bucur et al. use this Vinogradov function to prove a result for the Frobenius traces of reductions of an Abelian variety defined over $\mathbb{Q}$ (see [1, Thm. 3.8]), which will serve as inspiration for several results in this thesis.

In the construction of the Vinogradov function, condition 2 on T from Definition 3.5.1 is used solely for the mean value theorem,

$$|T(\boldsymbol{\theta} + \boldsymbol{z}) - T(\boldsymbol{\theta})| \leq K|\boldsymbol{z}|. \tag{3.6}$$

Therefore this condition can be relaxed to any function that passes the inequality in (3.7).

Similarly, condition 3 is used solely to find that $T^{-1}((\alpha, \beta)) \cap X_j(\pi(\boldsymbol{\theta}))$ is a union of at most C intervals. Therefore, given an interval (α, β), the function T admits a Vinogradov function if $T^{-1}((\alpha, \beta)) \cap X_j(\pi_j(\boldsymbol{\theta}))$ is a union of at most C intervals.

Theorem 3.5.4. *Let $I = (\alpha, \beta)$. Let $T : \mathbb{R}^s \to \mathbb{R}$ be a differentiable function that satisfies the following conditions:*

1. *T is periodic of period 1.*

2. *There exists a positive $K \in \mathbb{R}$ such that*

$$|T(\boldsymbol{\theta} + \boldsymbol{z}) - T(\boldsymbol{\theta})| \leq K|\boldsymbol{z}|. \tag{3.7}$$

for all $\boldsymbol{\theta} \in \mathbb{R}^s$.

3. *There exists an integer $C > 0$ such $T^{-1}((\alpha, \beta)) \cap X_j(\pi_j(\boldsymbol{\theta}))$ is a union of at most C intervals.*

Then T and I admit a Vinogradov function.

Chapter 4

Preliminary results

4.1 Setup and notation

For the remainder of this paper we assume all elliptic curves are ordinary. Let $E/\mathbb{F}_p$ be an ordinary elliptic curve, and let $E^{(1)}, \ldots, E^{(s)}$ be a collection of geometrically non-isogenous ordinary elliptic curves. Denote the trace of Frobenius over $\mathbb{F}_{p^n}$ by a_n (respectively, $a_n^{(j)}$), and the discriminant of the Frobenius polynomial by Δ_n (respectively, $\Delta_n^{(j)}$). We denote normalized Frobenius traces over $\mathbb{F}_{p^n}$ by $\overline{a}_n = a_n/\sqrt{p^n} \in [-2, 2]$, and the absolutve value of the normalized Frobenius discriminant by $|\overline{\Delta}_n| = |\Delta_n|/(4p^n) \in [0, 1]$.

Recall from Lemma 2.2.2 that we can calculate the discriminant $|\Delta_n|$ over $\mathbb{F}_{p^n}$ from the Frobenius angle over $\mathbb{F}_p$ by

$$|\Delta_n| = 4p^n \sin^2(n\theta_1).$$

so that $|\overline{\Delta}_n| = \sin^2(n\theta_1)$. Similarly, the trace of Frobenius over $\mathbb{F}_{p^n}$ can be calculated from the Frobenius angle over $\mathbb{F}_p$ by

$$a_n = 2\sqrt{p^n}\cos(n\theta_1)$$

and therefore the normalized trace is $\overline{a}_n = 2\cos(n\theta_1)$.

Definition 4.1.1. Let $E/\mathbb{F}_p$ be an ordinary elliptic curve. We have two notions of sequences of normalized Frobenius angles. First, we have the normalization by π,

$$\{\widetilde{\theta}_n\} = \left\{ \frac{n\theta_1 \pmod{\pi}}{\pi} \right\}.$$

We also have the normalization by 2π,

$$\{\hat{\theta}_n\} = \left\{ \frac{n\theta_1 \pmod{2\pi}}{2\pi} \right\}.$$

The motivation for the two normalizations is as follows. The sequence $\{\widetilde{\theta}_n\}$ helps reduce the error bound in explicit results, specifically by reducing the variation of the relevant function, which we use in Sections 5.1 and 5.4. Informally, use of the sequence $\{\widetilde{\theta}_n\}$ tends to give the variation $V(f) = 2$, whereas working with $\{\hat{\theta}_n\}$ would require use of a function g with variation $V(g) = 4$. The normalization $\widetilde{\theta}$ also allows for construction of a Vinogradov function with an auxiliary function such as $T(\theta) = \sin^2(\pi\theta)$, as in Sections 5.5, 5.6.

On the other hand, $\{\hat{\theta}_n\}$ allows for the construction of a Vinogradov function that produces results with complexity analysis $O(1/N)$ for auxiliary functions similar to $T(\theta) = 2\cos(2\pi\theta)$ as in Sections 5.2, 5.3, 6.1, and 6.2.

Because E is ordinary, Lemma 2.2.3 shows that θ_1 is not a rational multiple of π. By Example 3.1.4, the two sequences $\{\widetilde{\theta}_n\}$ and $\{\hat{\theta}_n\}$ are equidistributed in $[0, 1)$.

We can make corresponding equidistribution statement for collections of elliptic curves. Let $\widetilde{\theta}^{(1)}, \ldots, \widetilde{\theta}^{(s)}$ be a collection of normalized Frobenius angles from geometrically not isogenous elliptic curves. Define the sequence

$$\{\widetilde{\boldsymbol{\theta}}_n\} = \{(\widetilde{\theta}_n^{(1)}, \ldots, \widetilde{\theta}_n^{(s)})\}$$

and the sequence $\{\hat{\boldsymbol{\theta}}_n\}$ is defined analogously. If $\theta^{(1)}, \theta^{(2)}, \ldots, \theta^{(s)}$ is a collection of Frobenius angles of s ordinary, geometrically not isogenous elliptic curves, the following statement is due to [3].

Lemma 4.1.2. *The set* $\{1, \widetilde{\theta}_1^{(1)}, \widetilde{\theta}_1^{(2)}, \ldots, \widetilde{\theta}_1^{(s)}\}$ *is linearly independent over* $\mathbb{Q}$*. The set* $\{1, \hat{\theta}_1^{(1)}, \hat{\theta}_1^{(2)}, \ldots, \hat{\theta}_1^{(s)}\}$ *is also linearly independent over* $\mathbb{Q}$*.*

This, combined with [10, ex. 6.1] can be used to show the relevant equidistribution statement.

Lemma 4.1.3. *The sequences* $\{\widetilde{\boldsymbol{\theta}}_n\}$ *and* $\{\hat{\boldsymbol{\theta}}_n\}$ *are equidistributed in* $[0,1)^s$.

4.2 Discrepancy in One Dimension

In Sections 5.1 and 5.4 we will use Koksma's inequality, which relies on the discrepancy of a sequence. In this section, we'll examine methods for calculating discrepancy for the sequence of normalized Frobenius angles. First, we recall the Erdős-Turán-Koksma inequality for the star discrepancy.

Theorem 4.2.1. *Let* $\{\boldsymbol{\theta}_1 \ldots \boldsymbol{\theta}_N\}$ *be a finite sequence in* $[0,1)^s \subset \mathbb{R}^s$ *and let* $H \in \mathbb{Z}_{>0}$ *be an arbitrary positive integer. Then the star discrepancy of the sequence satisfies*

$$D_N^* \leq \left(\frac{3}{2}\right)^s \left(\frac{2}{H+1} + \sum_{0<||\boldsymbol{h}||_\infty \leq H} \frac{1}{r(\boldsymbol{h})} \left| \frac{1}{N} \sum_{n=1}^{N} e(\langle \boldsymbol{h}, \boldsymbol{\theta}_n \rangle) \right| \right).$$

This gives a general bound on the discrepancy for an s-dimensional sequence. For the $s = 1$ case (which is the case of a single isogeny class for this paper), we have the following bound due to [11, pg. 214].

Theorem 4.2.2 (Vaaler)**.** *Let* $\{\theta_1, \ldots, \theta_N\}$ *be a finite sequence in* $[0,1) \in \mathbb{R}$*, and let* $H \in \mathbb{Z}_{>0}$ *be an arbitrary positive integer. Then the star discrepancy of the sequence satisfies*

$$D_N^* \leq \frac{1}{H+1} + 2\sum_{h=1}^{H} \left(\frac{1}{\pi h} + \frac{1}{H+1}\right) \left| \frac{1}{N} \sum_{n=1}^{N} e(h\theta_n) \right|.$$

Given the sequence of normalized Frobenius angles $\{\widetilde{\theta}_n\} = \{n\theta_1 \pmod{\pi}/\pi\}$, the inequality

$$\sum_{n=1}^{N} e(hnz) \leq \frac{2}{|e(hz) - 1|} = \frac{1}{|\sin(\pi hz)|}$$

gives us the discrepancy bound

$$D_N^* \leq \frac{1}{H+1} + \frac{2}{N} \sum_{h=1}^{H} \left(\frac{1}{\pi h} + \frac{1}{H+1}\right) \frac{1}{|\sin(h\theta_1)|} \tag{4.1}$$

in terms of the Frobenius angle θ_1 for $E/\mathbb{F}_p$. We will use (4.1) in Examples 5.1.2 and 5.4.3.

If one instead works with the normalized Frobenius angle, the denominator is $h|\sin(\pi h\widetilde{\theta}_1)|$, which emphasizes how the type η of $\widetilde{\theta}_1$ controls the discrepancy. If integer multiples of $\widetilde{\theta}$ badly approximate integers (the type is small), then the discrepancy is small. See Theorem 3.3.3 for a formal statement relating the type to the discrepancy (we will show in Section 4.3 that $\widetilde{\theta}$ is of finite type).

4.3 The Frobenius angle vector is of finite type

In order to use the $O(1/N)$ quasi-Monte Carlo integration method from Theorem 3.3.5, we must first show that the s-tuples of the normalized Frobenius angles have finite type. Recall the type, η, of the s-tuple $\boldsymbol{\theta}$ is the infimum of numbers σ such that there is a constant $c = c(\sigma, \boldsymbol{\theta})$ for which the inequality

$$r(\boldsymbol{b})^{\sigma}\, \|\boldsymbol{b} \cdot \boldsymbol{\theta}\| \geq c$$

holds for all $\boldsymbol{b} \in \mathbb{Z}^s$ with $\boldsymbol{b} \neq \mathbf{0}$.

We have the following notation for Baker's theorem (from Theorem 3.4.3). Given algebraic numbers $\gamma_1, \ldots, \gamma_s$, let d be the degree of $\mathbb{Q}(\gamma_1, \ldots, \gamma_s)$, and let $h'(\gamma_j)$ be the height of γ_j. Let $\boldsymbol{b} \neq 0$, and for the linear form

$$L_{\boldsymbol{b}}(\boldsymbol{z}) = b_1 z_1 + \ldots + b_{s+1} z_{s+1},$$

let $h(L) = d \log \max\{|b_j|/b\}$ for b the highest common factor of $b_1, \ldots, b_{s+1}$. Then define

$$h'(L) = \frac{1}{d} \max\{h(L), 1\}.$$

Baker's theorem gives a bound on $L(\log \gamma_1, \ldots, \gamma_s)$ in terms of $h'(L)$, $h'(\gamma_j)$ and $C(s,d)$, a constant that depends on s and d.

Our strategy to show $\widetilde{\boldsymbol{\theta}}$ (or $\hat{\boldsymbol{\theta}}$) has finite type is as follows. Let $\boldsymbol{b} = (b_1, b_2, \ldots, b_s)$ be an arbitrary s-tuple and let b_{s+1}, be the integer closest to $b_1\widetilde{\theta}^{(1)} + \ldots + b_s\widetilde{\theta}^{(s)}$. After appropriate set up, Baker's theorem will give a bound on

$$\left|b_1\widetilde{\theta}^{(1)} + \ldots + b_s\widetilde{\theta}^{(s)} - b_{s+1}\right|.$$

This is the same as a bound on $\left\|\boldsymbol{b} \cdot \widetilde{\boldsymbol{\theta}}\right\|$, because b_{s+1} is the closest integer to $\boldsymbol{b} \cdot \widetilde{\boldsymbol{\theta}}$.

Proposition 4.3.1. *The s-tuple of normalized Frobenius angles $\widetilde{\boldsymbol{\theta}} = (\widetilde{\theta}^{(1)}, \ldots, \widetilde{\theta}^{(s)})$ is of finite type.*

Proof. Let $\widetilde{\theta}^{(j)}$ have associated trace of Frobenius $a^{(j)}$, and define the algebraic number

$$\gamma_j = i\sqrt{1 - (\overline{a}^{(j)}/2)^2} + \overline{a}^{(j)}/2$$

Recall $\log(-1) = i\pi$, and note that from the identity

$$\arccos(x) = -i\log(i\sqrt{1-x^2} + x)$$

we can relate the Frobenius angle $\widetilde{\theta}^{(j)}$ with the algebraic number γ_j by

$$\widetilde{\theta}^{(j)} = \frac{\arccos(\overline{a}^{(j)}/2)}{\pi} = \frac{-i\log(\gamma_j)}{\log(-1)/i} = \frac{\log(\gamma_j)}{\log(-1)}. \tag{4.2}$$

Let $\boldsymbol{b} = (b_1, \ldots, b_s) \in \mathbb{Z}^s \setminus \mathbf{0}$ be an arbitrary s-tuple, and let b_{s+1} be the integer closest to $b_1\widetilde{\theta}^{(1)} + \ldots + b_s\widetilde{\theta}^{(s)}$. Define the linear form

$$L_{\boldsymbol{b}}(\boldsymbol{z}) = L(\boldsymbol{z}) = b_1 z_1 + \ldots + b_s z_s - b_{s+1} z_{s+1}.$$

Let $\Lambda = L(\log(\gamma_1), \ldots, \log(\gamma_s), \log(-1))$. Use the identity in equation 4.2 to find

$$\begin{aligned}\Lambda &= b_1 \log(\gamma_1) + \ldots + b_s \log(\gamma_s) - b_{s+1} \log(-1) \\ &= \log(-1) \left(\frac{b_1 \log(\gamma_1)}{\log(-1)} + \ldots \frac{b_s \log(\gamma_s)}{\log(-1)} - b_{s+1} \right) \\ &= i\pi(b_1 \widetilde{\theta}^{(1)} + \ldots + b_s \widetilde{\theta}^{(s)} - b_{s+1}).\end{aligned}$$

Because b_{s+1} is the integer closest to $b_1 \widetilde{\theta}^{(1)} + \ldots + b_s \widetilde{\theta}^{(s)}$ we have

$$|\Lambda| = \pi \left\| b_1 \widetilde{\theta}^{(1)} + \ldots + b_s \widetilde{\theta}^{(s)} \right\|.$$

Baker's theorem then provides a bound on the quantity $\log(|\Lambda|)$ of the form

$$\log(|\Lambda|) > -C_{s+1,d} h'(\gamma_1) \ldots h'(\gamma_s) h'(L)$$

for an explicit constant $C_{s+1,d}$ and for heights defined in Section 3.4. Define the constant

$$\sigma = C_{s+1,d} h'(\gamma_1) \ldots h'(\gamma_s)$$

which depends on s, d and the heights of $\gamma_1, \ldots, \gamma_s$, but is independent of $b_1, \ldots, b_{s+1}$. We now have the inequality

$$\pi \left\| b_1 \widetilde{\theta}^{(1)} + \ldots + b_s \widetilde{\theta}^{(s)} \right\| > \exp\big(-\sigma h'(L)\big). \tag{4.3}$$

Our task is to now translate the right hand side into a term of the form $c/r(\boldsymbol{b})^{\sigma}$. We have two cases depending on the form of $h'(L)$.

1. Consider the case $\max\{h(L), 1\} = h(L)$. Then $h'(L) = \log(\max\{|b_j|/b\})$ for b the highest common factor of $b_1, \ldots, b_{s+1}$. We further break into two cases.

(a) First, assume $\max\{|b_j|/b\}$ is achieved for $1 \le j \le s$, and let $b' = \max\{|b_j|/b\}$. Then $\exp(-\sigma h'(L)) = \exp(-\sigma \log(b'))$ and the inequality from equation (4.3) is now

$$\left\| b_1\widetilde{\theta}^{(1)} + \ldots + b_s\widetilde{\theta}^{(s)} \right\| > \frac{1}{\pi(b')^{\sigma}}.$$

Note that $b' < \prod_{j=1}^{s} \max\{|b_j|, 1\}$, so that $1/b' > 1/r(\boldsymbol{b})$. Thus we have

$$\left\| \boldsymbol{b} \cdot \widetilde{\boldsymbol{\theta}} \right\| > \frac{1}{\pi r(\boldsymbol{b})^{\sigma}}$$

as desired.

(b) Now assume that $\max\{|b_j|/b\}$ is achieved at $j = s+1$. Then the inequality in equation (4.3) is

$$\left\| \boldsymbol{b} \cdot \widetilde{\boldsymbol{\theta}} \right\| > \frac{b^{\sigma}}{\pi |b_{s+1}|^{\sigma}}$$

Note that from Lemma 4.3.2 we then have the inequality

$$\left\| \boldsymbol{b} \cdot \widetilde{\boldsymbol{\theta}} \right\| > \frac{1}{2\pi^2 s r(\boldsymbol{b})^{\sigma}}.$$

Therefore in both case (a) and case (b), we have achieved the desired result.

2. Now consider the case $\max\{h(L), 1\} = 1$. Then $h'(L) = 1/d$, and the inequality in equation 4.3 is

$$\pi \left\| b_1\widetilde{\theta}^{(1)} + \ldots + b_s\widetilde{\theta}^{(s)} \right\| > \exp\big(-\sigma/d\big).$$

and therefore

$$\left\| \boldsymbol{b} \cdot \widetilde{\boldsymbol{\theta}} \right\| > \frac{\exp\big(-\sigma/d\big)}{r(\boldsymbol{b})}$$

We have that $\sigma \geq 1$, so that

$$\left\|\boldsymbol{b} \cdot \widetilde{\boldsymbol{\theta}}\right\| > \frac{\exp\big(-\sigma/d\big)}{r(\boldsymbol{b})^{\sigma}}$$

as desired.

In each of these cases we have found a bound

$$r(\boldsymbol{b})^{\sigma}\left\|\boldsymbol{b} \cdot \widetilde{\boldsymbol{\theta}}\right\| \geq c(\sigma, \widetilde{\boldsymbol{\theta}})$$

for a constant $c(\sigma, \widetilde{\boldsymbol{\theta}}) = \min\{1/\pi, 1/(2\pi^2 s), \exp(-\sigma/d)\}$ that is independent of $\boldsymbol{b} = (b_1, \ldots, b_s)$, and therefore $\widetilde{\boldsymbol{\theta}}$ is of finite type σ. □

To conclude this proposition, we provide a lemma to complete case (1b).

Lemma 4.3.2. *Let $\boldsymbol{b} = (b_1, \ldots, b_s)$ be an s-tuple, and let b_{s+1} be the integer closest to $b_1\widetilde{\theta}^{(1)} + \ldots + b_s\widetilde{\theta}^{(s)}$. Then b_{s+1} satisfies the inequality*

$$|b_{s+1}| < 2\pi s r(\boldsymbol{b})$$

Proof. Without loss of generality, assume each normalized Frobenius angle is positive (taking conjugates of $\alpha^{(j)}$ if necessary). Then the normalized Frobenius angles satisfy $0 < \widetilde{\theta}^{(j)} < \pi$, so that

$$b_1\widetilde{\theta}^{(1)} + \ldots + b_s\widetilde{\theta}^{(s)} < \pi(|b_1| + \ldots + |b_s|).$$

Because b_{s+1} is the integer closest to $b_1\widetilde{\theta}^{(1)} + \ldots + b_s\widetilde{\theta}^{(s)}$, the largest $|b_{s+1}|$ can be is the first integer greater than $|b_1|\widetilde{\theta}^{(1)} + \ldots + |b_s|\widetilde{\theta}^{(s)}$, which is at most $1 + \pi\sum_{j=1}^{s}|b_j|$. Therefore

$$|b_{s+1}| < 1 + \pi\sum_{j=1}^{s}|b_j|.$$

Note that for $1 \leq i \leq s$ we have $|b_i| \leq \prod_{j=1}^{s} \max\{|b_j|, 1\}$, that is, $|b_i| \leq r(\boldsymbol{b})$. Then $|b_1| + \ldots + |b_s| < sr(\boldsymbol{b})$, and therefore

$$0 \leq |b_{s+1}| < 1 + \pi sr(\boldsymbol{b})$$

Because $\pi sr(\boldsymbol{b}) > 1$, we have $2\pi sr(\boldsymbol{b}) > 1 + \pi sr(\boldsymbol{b})$, and therefore

$$0 \leq |b_{s+1}| < 2\pi sr(\boldsymbol{b}).$$

□

Corollary 4.3.3. *The vector of normalized Frobenius angles $\hat{\boldsymbol{\theta}} = (\hat{\theta}^{(1)}, \ldots, \hat{\theta}^{(s)})$ is of finite type.*

Proof. Note that $\hat{\theta}^{(j)} = \widetilde{\theta}^{(j)}/2$, and therefore

$$\hat{\theta}^{(j)} = \frac{\log(\gamma_j)}{2\log(-1)} = \frac{\log(\sqrt{\gamma_j})}{\log(-1)}$$

and therefore we use Baker's theorem on the algebraic numbers $\sqrt{\gamma_1}, \ldots, \sqrt{\gamma_s}$ and follow the proof of Proposition 4.3.1. □

If we have an s-tuple $\boldsymbol{\theta}$ of finite type, then integer multiples of $\boldsymbol{\theta}$ are also of finite type, as shown by the following lemma.

Lemma 4.3.4. *Fix an integer $n \in \mathbb{Z}_{>1}$. Suppose $\boldsymbol{\theta} \in \mathbb{R}^s$ is of finite type η. Then $\boldsymbol{\vartheta} = n\boldsymbol{\theta}$ is of finite type.*

Proof. Because $\boldsymbol{\theta}$ is of finite type there exists a constant $c = c(\sigma, \boldsymbol{\theta})$, such that for all non-zero $\boldsymbol{b} \in \mathbb{Z}^s$ and $\sigma > \eta$, we have the inequality

$$r(\boldsymbol{b})^{\sigma} \left\| \boldsymbol{b} \cdot \boldsymbol{\theta} \right\| \geq c.$$

Now consider the quantity

$$r(\boldsymbol{b})^{\sigma} \left\| \boldsymbol{b} \cdot \boldsymbol{\vartheta} \right\| .$$

Clearly $\|\boldsymbol{b} \cdot \boldsymbol{\vartheta}\| = \|\boldsymbol{b} \cdot n\boldsymbol{\theta}\| = \|n\boldsymbol{b} \cdot \boldsymbol{\theta}\|$ and $r(\boldsymbol{b})^{\sigma} \left\| n\boldsymbol{b} \cdot \boldsymbol{\theta} \right\| \geq c$. Therefore

$$r(\boldsymbol{b})^{\sigma} \left\| \boldsymbol{b} \cdot \boldsymbol{\vartheta} \right\| \geq c$$

and thus $\boldsymbol{\vartheta}$ has finite type. □

4.4 Fourier coefficients of the Vinogradov function

Another ingredient we need before we can use the $O(1/N)$ error estimate in Theorem 3.3.5 is to show that the Vinogradov function of Theorem 3.5.3 is in the class of function $\mathscr{E}^k$ where $k > \eta$, the type of $\widetilde{\boldsymbol{\theta}}$ or $\hat{\boldsymbol{\theta}}$.

For Ψ to be in $\mathscr{E}^k$, the Fourier coefficients must satisfy $|c_{\boldsymbol{h}}| \leq B/r(\boldsymbol{h})^k$ for a constant B. Let $T : \mathbb{R}^s \to \mathbb{R}$ be a function which satisfies Definition 3.5.1. This gives $K \in \mathbb{R}_{>0}$, a bound on the gradient of T, and $C \in \mathbb{Z}_{>0}$ a bound on the cardinality of certain intersections of preimages of T. Let α, β, Δ be real numbers with $\Delta > 0$ and $2\Delta \leq \beta - \alpha$. Then for every $m \in \mathbb{Z}_{>0}$ there exists a Vinogradov function Ψ which roughly acts as the indicator function for values θ such that $a < T(\theta) < b$. Recall Ψ has Fourier coefficients which satisfy

$$|c_{\boldsymbol{h}}| \leq \min \left[|c_{\boldsymbol{0}}|, \quad \left\{ \frac{C}{\pi \max_j \{h_j\}} \prod_{j=1, h_j \neq 0}^{s} \left(\frac{mK\sqrt{s}}{2\pi |h_j| \Delta} \right)^{\rho} \right\}_{\rho=0,\ldots m} \right] .$$

Let η be the type of $\widetilde{\boldsymbol{\theta}}$ (or $\hat{\boldsymbol{\theta}}$). We choose the integer $m = \lfloor \eta \rfloor + 1$. Under this choice, we will see the term $r(\boldsymbol{h})^m$ then appears in the denominator of the product from the $|h_j|$ as desired.

We have that

$$|c_{\boldsymbol{h}}| \leq \frac{C}{\pi \max_j\{h_j\}} \prod_{j=1,h_j\neq 0}^{s} \left(\frac{mK\sqrt{s}}{2\pi|h_j|\Delta}\right)^m .$$

Note that $\frac{C}{\pi \max_j\{h_j\}} \leq \frac{C}{\pi}$ and

$$\prod_{j=1,h_j\neq 0}^{s} \left(\frac{mK\sqrt{s}}{2\pi|h_j|\Delta}\right)^m \leq \left(\frac{mK\sqrt{s}}{2\pi\Delta}\right)^{sm} \prod_{j=1,h_j\neq 0}^{s} \left(\frac{1}{|h_j|}\right)^m .$$

Therefore

$$|c_{\boldsymbol{h}}| \leq \frac{C}{\pi} \left(\frac{mK\sqrt{s}}{2\pi\Delta}\right)^{sm} \frac{1}{r(\boldsymbol{h})^m}$$

which proves the following proposition.

Proposition 4.4.1. *Given an s-tuple of finite type η, and a function T which satisfies Definition 3.5.1, there exists a Vinogradov function Ψ for T that is in the function class $\mathscr{E}^k$ for any $k > \eta$.*

We may now proceed with a general schema for proofs that utilize a Vinogradov function.

4.5 Proof structure for $O(1/N)$ results

Sections 5.2, 5.3, 5.5, 5.6, 6.1 and 6.2 will have results with an $O(1/N)$ error term that all have a similar style of proof. In this section, we outline the general proof structure, and then later fill in details in the relevant sections. The tools we will need are the Vinogradov function from Theorem 3.5.3 and the $O(1/N)$ integration rule for periodic functions from Theorem 3.3.5.

4.5.1 Set up

The general structure of these theorems is as follows. Let $\mathbb{F}_p$ be a finite field. For this section, let $\mathcal{A}$ denote either a collection of s ordinary, not geometrically isogenous elliptic curves, or an abelian variety of dimension s. Let $\widetilde{\boldsymbol{\theta}}$ be the associated normalized Frobenius tuple, and let X

be some quantity relating to the elliptic curves or abelian variety, such as the Frobenius trace or discriminant.

Given an interval $I = [a, b]$, we would like to study how often X takes value in I. Define the quantity $\mathrm{ExtSet}_{\mathcal{A},N,I}$ to be the set of extensions of $\mathbb{F}_p$ of degree up to N such that $X \in I$. Also define $\mathrm{PropX}_{\mathcal{A},N,I}$ to be the proportion of extensions up to degree N for which X is in I. We now give the general framework for proofs that uses a Vinogradov function and the theorem of $O(1/N)$ integration error for periodic functions.

Define a function $T : \mathbb{R}^s \to \mathbb{R}$, such that $T(\widetilde{\boldsymbol{\theta}}) \in I$ (that is, $a \leq T(\widetilde{\boldsymbol{\theta}}) \leq b$) exactly when $X \in I$. Choose Δ to be small, and define the quantities $\alpha = a + \Delta$ and $\beta = b - \Delta$. We have the regions

$$\begin{aligned} R_1 &= T^{-1}\Bigg((\alpha + \Delta, \beta - \Delta)\Bigg) \cap [0,1]^s \\ &= T^{-1}\Bigg((a + 2\Delta, b - 2\Delta)\Bigg) \cap [0,1]^s \\ R_0 &= T^{-1}\Bigg(\mathbb{R} \setminus (\alpha - \Delta, \beta + \Delta)\Bigg) \cap [0,1]^s \\ &= T^{-1}\Bigg(\mathbb{R} \setminus (a, b)\Bigg) \cap [0,1]^s \end{aligned}$$

on the domain of T. From these choices of T, α, β, Δ, we then construct a Vinogradov function $\Psi : \mathbb{R}^s \to \mathbb{R}$. This Vinogradov function takes value 1 on R_1, value 0 on R_0 and it is everywhere bounded $0 \leq \Psi(\boldsymbol{\theta}) \leq 1$. From Proposition 4.3.1 we have that $\widetilde{\boldsymbol{\theta}}$ is of finite type η, and from Proposition 4.4.1, we have that $\Psi(\boldsymbol{\theta}) \in \mathscr{E}^k$ for $k \geq \eta$. Therefore, we can make use of the integration rule from Theorem 3.3.5, which in this case is

$$\frac{1}{N}\sum_{n=1}^{N} \Psi(n\widetilde{\boldsymbol{\theta}}) - \int_{[0,1)^s} \Psi(\boldsymbol{x}) d\boldsymbol{x} = O\left(\frac{1}{N}\right). \tag{4.4}$$

4.5.2 Relation between PropX and $\sum \Psi(n\theta)$

We must now relate the term $\frac{1}{N}\sum_{n=1}^{N}\Psi(n\widetilde{\boldsymbol{\theta}})$ with $\mathrm{PropX}_{\mathcal{A},N,I}$. First, we find a relation between $\sum_{n=1}^{N}\Psi(n\widetilde{\boldsymbol{\theta}})$ and $\#\{\mathrm{ExtSet}_{\mathcal{A},N,I}\}$. We have three cases, depending on if $n\boldsymbol{\theta}$ is in R_1, R_0, or neither.

1. Let $n\widetilde{\boldsymbol{\theta}} \in R_1$, so that $\Psi(n\widetilde{\boldsymbol{\theta}}) = 1$. By definition of R_1, we have that $a + 2\Delta \leq T(n\widetilde{\boldsymbol{\theta}}) \leq b - 2\Delta$, and therefore $T(n\widetilde{\boldsymbol{\theta}}) \in I$. Then $X \in I$ and so the extension of degree n is contained in the set $\mathrm{ExtSet}_{\mathcal{A},N,I}$.

2. Let $n\widetilde{\boldsymbol{\theta}} \in R_0$ and therefore $\Psi(n\widetilde{\boldsymbol{\theta}}) = 0$. By definition of the region R_0, either $T(n\widetilde{\boldsymbol{\theta}}) < a$ or $T(n\widetilde{\boldsymbol{\theta}}) > b$, and therefore $X \notin I$. Thus the extension of degree n is not in $\mathrm{ExtSet}_{\mathcal{A},N,\epsilon}$.

3. Lastly, if $n\widetilde{\boldsymbol{\theta}} \in [0,1]^s \setminus (R_0 \cup R_1)$, then the extension of degree n is in $\mathrm{ExtSet}_{\mathcal{A},N,I}$, because by definition of the sets R_0, R_1, it must be that either $a + 2\Delta \leq T(n\widetilde{\boldsymbol{\theta}}) \leq a$ or $b - 2\Delta \leq T(n\widetilde{\boldsymbol{\theta}}) \leq b$ and therefore $X \in I$. However, for this n we have $\Psi(n\widetilde{\boldsymbol{\theta}}) \leq 1$. In this case Ψ is an underestimate of $\#\,\mathrm{ExtSet}_{\mathcal{A},N,I}$.

Therefore, we may conclude that if $\mathbb{F}_{p^n} \in \mathrm{ExtSet}_{\mathcal{A},N,I}$, then $0 \leq T(n\widetilde{\boldsymbol{\theta}}) \leq 1$, and if $\mathbb{F}_{p^n} \notin \mathrm{ExtSet}_{\mathcal{A},N,I}$, then $T(n\widetilde{\boldsymbol{\theta}}) = 0$. Therefore $\sum_{n=1}^{N}\Psi(n\widetilde{\boldsymbol{\theta}}) \leq \#\,\mathrm{ExtSet}_{N,\epsilon}$, and thus we have

$$\mathrm{PropX}_{\mathcal{A},N,I} \geq \frac{1}{N}\sum_{n=1}^{N}\Psi(n\widetilde{\boldsymbol{\theta}}). \tag{4.5}$$

4.5.3 Estimation of the integral

It remains to give a lower bound for the integral $\int_{I^s}\Psi(\boldsymbol{x})d\boldsymbol{x}$. Because $\Psi(\boldsymbol{\theta})$ is positive, restricting the integral to the subset R_1 of I^s will give the lower bound

$$\int_{R_1}\Psi(\boldsymbol{x})d\boldsymbol{x} \leq \int_{I^s}\Psi(\boldsymbol{x})d\boldsymbol{x}. \tag{4.6}$$

Therefore, we wish to calculate the measure of the region where $T(\widetilde{\boldsymbol{\theta}}) > \epsilon + 2\Delta$. In theorems involving one isogeny class, $s = 1$, the integral $\int_{R_1} \Psi(\boldsymbol{x})d\boldsymbol{x}$ will usually be a straightforward calculation. On the other hand, for theorems involving two isogeny classes, a parameterization of a level set for $T(\widetilde{\boldsymbol{\theta}}) = c$ in the region $[0,1]^2$ will be used to evaluate $\int_{R_1} \Psi(\boldsymbol{x})d\boldsymbol{x}$. Also in the case $s = 2$, the shape of the region R_1 will be sensitive to the value of c, as will be illustrated in the relevant sections.

Final statement

Returning to equation (4.4), for large enough N, there exists a constant M independent of N (see Section 4.5.3 for discussion) such that

$$\left| \frac{1}{N} \sum_{n=1}^{N} \Psi(n\widetilde{\boldsymbol{\theta}}) - \int_{I^s} \Psi(\boldsymbol{x})d\boldsymbol{x} \right| \leq \frac{M}{N}.$$

We can rearrange as

$$\int_{I^s} \Psi(\boldsymbol{x})d\boldsymbol{x} - \frac{M}{N} \leq \frac{1}{N} \sum_{n=1}^{N} \Psi(n\widetilde{\boldsymbol{\theta}}).$$

From the inequalities established in equations (4.5) and (4.6) we then have the main result

$$\mathrm{PropX}_{\mathcal{A},N,I} \geq \int_{R_1} \Psi(\boldsymbol{x})d\boldsymbol{x} - \frac{M}{N}. \tag{4.7}$$

The implied constant

The constant M in equation (4.7) is unfortunately difficult to control. It depends on the bounds of the Fourier coefficients,

$$\left\{ \frac{C}{\pi \max_j\{h_j\}} \prod_{j=1, h_j \neq 0}^{s} \left(\frac{mK\sqrt{s}}{2\pi |h_j| \Delta} \right)^{\rho} \right\}_{\rho=0,\ldots m}$$

for which we have selected $m > \eta$. More challenging is that M depends on the constant from the type of $\widetilde{\boldsymbol{\theta}}$.

Chapter 5

Elliptic Curves

5.1 Explicit Traces

5.1.1 Set up

Given an elliptic curve $E/\mathbb{F}_p$, we have the sequence of Frobenius traces, a_n, corresponding to $E/\mathbb{F}_{p^n}$. These traces relate to the point count of E by $\#E(\mathbb{F}_{p^n}) = p^n + 1 - a_n$. Let $\overline{a}_n = \frac{a_n}{\sqrt{p^n}} \in [-2, 2]$ be the normalized trace of Frobenius. Recall that $\{\widetilde{\theta}_n\}$ is the normalized Frobenius angle of $E/\mathbb{F}_p$ so that the normalized Frobenius trace is $\overline{a}_n = 2\cos(\pi\widetilde{\theta}_n)$. Let $I = [a, b] \subset [-2, 2]$ be the target interval for the normalized traces $\overline{a}_n$. This section quantifies how often the normalized trace lands in the target interval I. Let $\mathrm{ExtSetTr}_{E,N,I} = \{n \leq N \ : \ \overline{a}_n \in I\}$ be the set of (degrees of) extensions such that the Frobenius trace is in the interval I, and let

$$\mathrm{PropTr}_{E,N,I} = \frac{\#\,\mathrm{ExtSetTr}_{E,N,I}}{N} \tag{5.1}$$

be the proportion of extensions up to degree N such that $\overline{a}_n \in I$. This section gives explicit bounds on $\mathrm{PropTr}_{E,N,I}$ in terms of the discrepancy of the sequence $\{\widetilde{\theta}_n\}_{n=1}^{\infty}$. For explicit calculations, one may use the discrepancy bounds from Section 4.2, as is done in Example 5.1.2.

5.1.2 An equidistribution result

We begin by stating a relevant result given in [29, prop. 2.11]. This asymptotic result states that the sequence of traces $\{\overline{a}_n\}$ is equidistributed in $[-2, 2]$ with respect to the measure

$$\mu = \frac{1}{\pi}\frac{dz}{\sqrt{4 - z^2}} \tag{5.2}$$

where dz is Lebesgue measure on $[-2,2]$. Theorem 5.1.1 refines this by an explicit result that gives a lower bound on the number of extensions up to degree N for which the trace is in a chosen subinterval of $[-2,2]$.

Theorem 5.1.1. *Let $E/\mathbb{F}_p$ be an ordinary elliptic curve with normalized Frobenius angle $\widetilde{\theta}$. Let $I = [a,b] \subset [-2,2]$ be the target interval for the traces $\overline{a}_n$. Define A_I as the quantity*

$$A_I = \frac{1}{\pi}(\arccos(a/2) - \arccos(b/2)).$$

Then the proportion of extensions of degree up to N where $\overline{a}_n \in I$ satisfies the inequality

$$\mathrm{PropTr}_{E,N,I} \geq A_I - 2D_N^* \tag{5.3}$$

where D_N^* is the discrepancy of the sequence $\{\widetilde{\theta}_n\}_{n=1}^N$.

Proof. We use Koksma's inequality from Theorem 3.1.9 with the sequence $\{\widetilde{\theta}_n\}$ from Definition 4.1.1. Recall that this sequence is equidistributed in $[0,1]$ because E is an ordinary elliptic curve, and therefore $\widetilde{\theta}_1$ is irrational. Let χ_I be the indicator function of I, that is,

$$\chi_I(x) = \begin{cases} 1 & x \in I \\ 0 & x \notin I \end{cases}.$$

Define

$$f_I(x) = \chi_I(2\cos(\pi x)). \tag{5.4}$$

Then $f_I(\widetilde{\theta}_n) = 1$ exactly when $\overline{a}_n \in I$, and the sum $\sum_{n=1}^N f_I(\widetilde{\theta}_n)$ counts the cardinality of $\mathrm{ExtSet}_{E,N,I}$. The function f_I is the indicator function of an interval, so $V(f) = 2$. One can calculate that

$$\int_0^1 f_I(x)dx = \frac{1}{\pi}(\arccos(a/2) - \arccos(b/2)).$$

Therefore, from Koksma's inequality we have the bound

$$\left| \frac{1}{N}\sum_{n=1}^{N} f_I(\widetilde{\theta}_n) - \int_0^1 f_I(x)dx \right| \leq D_N^* V(f) \tag{5.5}$$

which completes the proof. □

An analogue of the cumulative distribution function for the main term, A_I, of the lower bound in Theorem 5.1.1 appears in Figure 5.1. Also see the histograms from empirical data in Figures 5.2, 5.4 and 5.5.

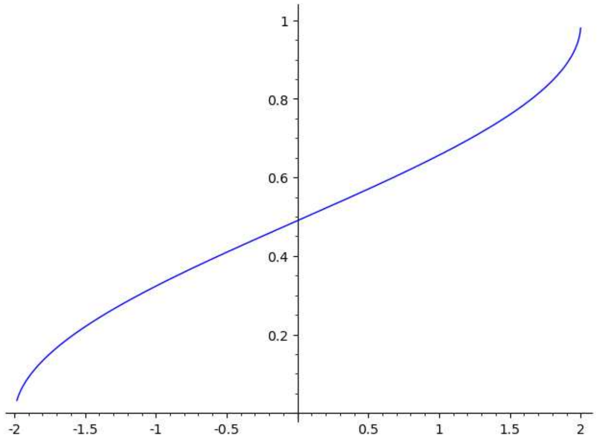


Figure 5.1: The cumulative distribution function of the main term in Theorem 5.1.1. The plot of $\frac{1}{\pi}(\arccos(-1) - \arccos(x/2))$ for $-2 \leq x \leq 2$.

Next, we give an example to cement these ideas, and to demonstrate how one uses the discrepancy bounds given in Section 4.2.

Example 5.1.2. Let $p = 37$, and let E be the curve defined by $y^2 = x^3 + x + 13$ over $\mathbb{F}_p$. Over $\mathbb{F}_p$, this curve has trace of Frobenius $a_1 = 5$. We consider the proportion of extensions for which the normalized Frobenius trace lands in the interval $I = [1, 2]$, up to extension degrees 500 and 1000.

We have the quantity $A_I = \frac{1}{\pi}(\arccos(1/2) - \arccos(1)) = \frac{1}{3}$, thus Theorem 5.1.1 gives the bound

$$\operatorname{PropTr}_{E,N,I} \geq \frac{1}{3} - 2D_N^*.$$

We'll use the discrepancy bound from Vaaler given in Theorem 4.2.2 with the simplification in equation (4.1). For convenience, that bound is

$$D_N^* \leq \frac{1}{H+1} + \frac{2}{N}\sum_{h=1}^{H}\left(\frac{1}{\pi h} + \frac{1}{H+1}\right)\frac{1}{|\sin(h\theta)|} \tag{5.6}$$

where θ is the Frobenius angle of $E/\mathbb{F}_p$ and H is an arbitrary positive integer. Because N is relatively small, we run an exhaustive search $1 \leq H \leq N$ to find a tightest upper bound on the discrepancy, which we denote as D_N^{UB}. Therefore, our explicit lower bound is

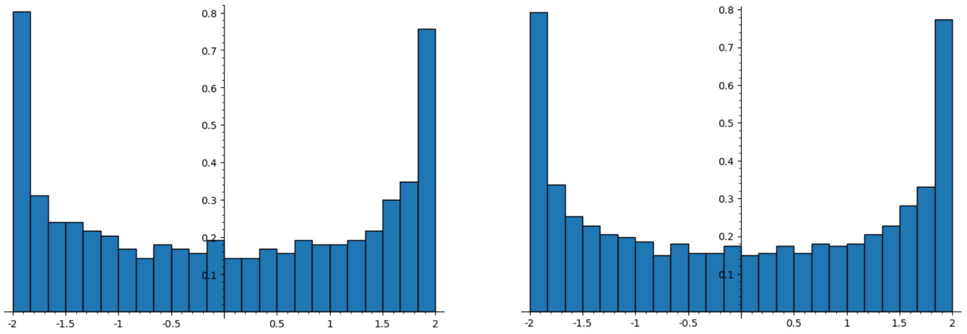
$$\operatorname{PropTr}_{E,N,I} \geq \frac{1}{3} - 2D_N^{\text{UB}}.$$

These results are summarized in Table 5.1.

Table 5.1: Normalized traces in $I = [1, 2]$ up to extension degrees $N = 500, 1000$ for the curve $y^2 = x^3 + x + 13$ with $p = 37$. The column "$\frac{1}{3} - 2D_N^{\text{UB}}$ is the bound from Theorem 5.1.1, and the two right-most columns are the true values.

N	D_N^{UB}	Optimal H choice	$\frac{1}{3} - 2D_N^{\text{UB}}$	# $\operatorname{ExtSetTr}_{E,N,I}$	$\operatorname{PropTr}_{E,N,I}$
500	0.038	114	0.257	166	0.332
1000	0.023	177	0.287	333	0.333

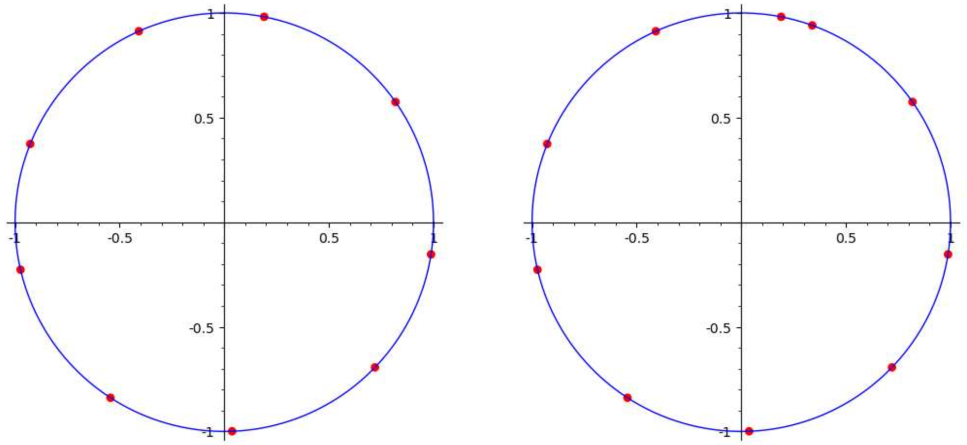
Note 5.1.3. One may note that the empirical values for $\operatorname{PropTr}_{E,N,I}$ are very close to the value A_I



(a) $N = 500$

(b) $N = 1000$

Figure 5.2: Histograms of the normalized traces for $N = 500$ and $N = 1000$ for the curve $y^2 = x^3 + x + 13$ with $p = 37$.



(a) $N = 9$

(b) $N = 10$

Figure 5.3: Illustration of different gaps in the sequence $\theta, 2\theta, \ldots, N\theta$.

in Example 5.1.2. There are several contributing factors to this.

The three gap theorem states that given an angle θ, if one places points on the circle at angles $\theta, 2\theta, \ldots, N\theta$, there will be at most three distinct distances between points in adjacent positions. For subsequences where the three gaps don't change, the points are placed with high regularity, but when a new gap is started we have some irregularity. See Figure 5.3 for an illustration of a new gap. Using the correspondence between the angle $2\pi\theta$ and the irrational number $\theta \in [0, 1)$, we translate to the now familiar sequence $\{n\theta\}$. Therefore, while the gaps remain stable, points will be placed in a given subinterval with high regularity, but when a new gap appears, the pattern of placement changes.

Also recall the theorem of Beck from Theorem 3.3.1 which states that for almost all irrational numbers θ, the Kronecker sequence $\{n\theta \pmod 1\}$ has the discrepancy bound

$$D_N^* \ll_{s,\epsilon} \frac{(\log N)(\log\log N)^{1+\epsilon}}{N}$$

for every $\epsilon > 0$. Thus the error term in the estimate may in fact be smaller than our calculation.

Lastly, such regularity is not inherent in every example, which we consider in more detail in the following discussion.

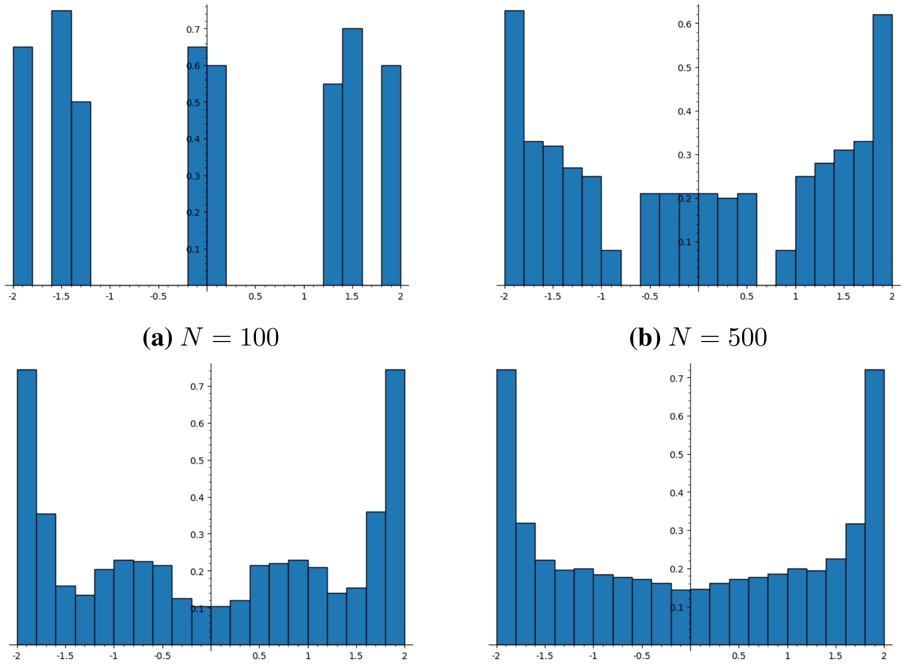
5.1.3 Discrepancy discussion

The data from Example 5.1.2 may prompt the following question: given that the observed data for $\mathrm{PropTr}_{E,N,I}$ is fairly close to the quantity A_I, is the discrepancy term in the lower bound for $\mathrm{PropTr}_{E,N,I}$ really necessary? The histogram in Figure 5.4, and particularly subfigure 5.4a suggests that the discrepancy is in fact necessary. For $I = [1/2, 1]$, the quantity A_I is roughly $A_I \approx 0.086$. Therefore, for $N = 100$ we expect around 8 extensions for which the normalized Frobenius trace is in I. However, in the example of Figure 5.4a there are *no* extensions up to $N = 100$ where the normalized Frobenius trace takes value in I.

In fact, one may even use the discrepancy to predict when such irregular histograms will occur (as opposed to the more smooth set of histograms in Figure 5.5). Given the exponential sum in the discrepancy bound,

$$\frac{2}{N}\sum_{h=1}^{H}\left(\frac{1}{\pi h} + \frac{1}{H+1}\right)\frac{1}{|\sin(h\theta)|},$$

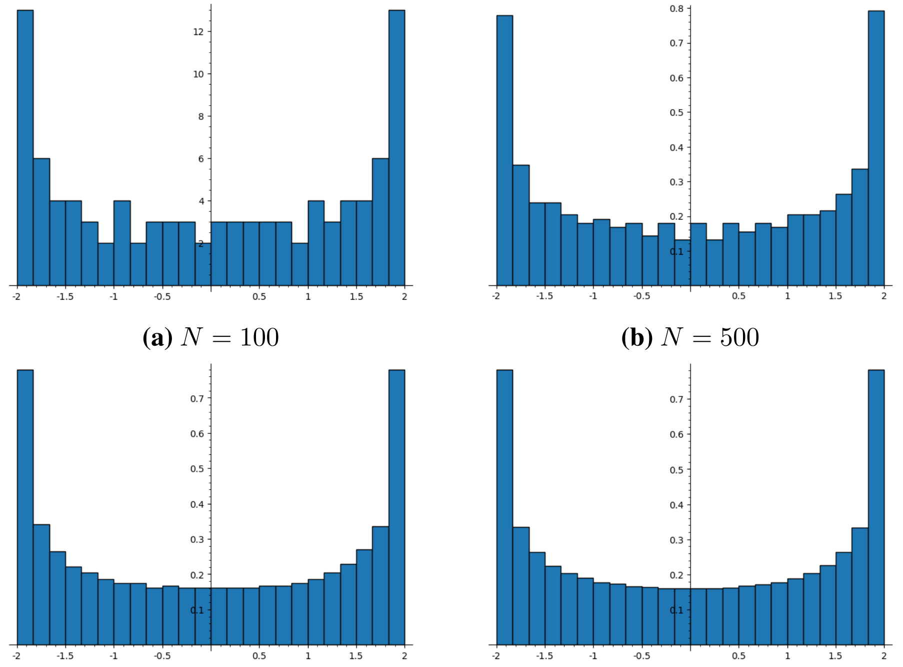
one may expect that an elliptic curve that has a Frobenius angle close to π/m for m a small integer, might be slower to converge (in terms of N) to the value A_I due to the term $1/|\sin(h\theta)|$. Computationally, this is indeed the case; in particular, the curve used in Figure 5.4 has a Frobenius angle θ such that $|\theta - \pi/4| < 0.000604$.



(a) $N = 100$ **(b)** $N = 500$

(c) $N = 1000$ **(d)** $N = 5000$

Figure 5.4: Histograms of the normalized traces for extension degrees $N = 100, 500, 1000, 5000$ for the curve $y^2 = x^3 + 14565x + 9281$ with $p = 15331$, which has trace of Frobenius $a_1 = 175$.



(a) $N = 100$ **(b)** $N = 500$

(c) $N = 1000$ **(d)** $N = 5000$

Figure 5.5: Histograms of the normalized traces for extension degrees $N = 100, 500, 1000, 5000$ for the curve $y^2 = x^3 + 14565x + 9281$ with $p = 15331$ which has trace of Frobenius $a_1 = 130$.

5.2 Quantitative traces

Continue with E an elliptic curve over $\mathbb{F}_p$ with trace a_1. Again, fix an interval $I = [a, b] \subset [-2, 2]$ as the target interval for the normalized traces $\overline{a}_n$. Recall that $\mathrm{ExtSetTr}_{E,N,I} = \{n \leq N \ : \ \overline{a}_n \in I\}$ is the set of (degrees of) extensions such that the Frobenius trace is in I, and continue to use the $\mathrm{PropTr}_{E,N,I} = \frac{\#\,\mathrm{ExtSetTr}_{E,N,I}}{N}$ to denote the proportion of extensions up to degree N such that $\overline{a}_n \in I$. Also recall the normalization of Frobenius angles,

$$\hat{\theta} = \frac{\theta}{2\pi}.$$

The previous section gave explicit lower bounds on $\mathrm{PropTr}_{E,N,I}$; this section aims to give a result on the speed of convergence of $\mathrm{PropTr}_{E,N,I}$ to the probability density function given by (5.2) in terms of N. We will make use of the proof structure outlined in Section 4.5. In particular, we look to make use of a Vinogradov function, which requires the following lemma. We first review some notation.

Recall the setup for Definition 3.5.1. Consider a function $T : \mathbb{R}^s \to \mathbb{R}$. Let $\pi_j : [0, 1]^s \to [0, 1]^{s-1}$ for $1 \leq j \leq s$ be the map that forgets the j^{th} coordinate of the s-tuple $\boldsymbol{\theta} = (\theta_1, \theta_2, \ldots, \theta_s)$. For $\boldsymbol{\vartheta} \in [0, 1]^{s-1}$, define $X_j(\boldsymbol{\vartheta}) = \pi_j^{-1}(\boldsymbol{\vartheta})$. We now verify the conditions of Definition 3.5.1 for the function $T(\theta) = 2\cos(2\pi\theta)$.

Lemma 5.2.1. *The function*

$$\begin{tikzcd} T : \mathbb{R} \arrow[r] & \mathbb{R} \\ \theta \arrow[r, mapsto] & 2\cos(2\pi\theta) \end{tikzcd}$$

meets the criterion of Definition 3.5.1 with Note 3.5.2 for the special case of $s = 1$. That is, it meets the following conditions:

1. *T is periodic of period 1.*

2. *There exists a positive $K \in \mathbb{R}$ such that $|\nabla T(\boldsymbol{\theta})| \leq K$ for all $\boldsymbol{\theta} \in \mathbb{R}$.*

3. *There exists an integer $C > 0$ such that, for every $\gamma \in \mathbb{R}$*

$$\#\Big(T^{-1}(\gamma) \cap [0,1]\Big) \leq C.$$

Proof. The function T is plainly periodic of period 1, and the derivative is bounded by $K = 4\pi$. For the third part, let $\gamma \in \mathbb{R}$ be a fixed number.

The quantity

$$\#\Big(T^{-1}(\gamma) \cap [0,1]\Big)$$

is the number of solutions to $2\cos(2\pi\theta) = \gamma$ for $\theta \in [0,1]$, thus taking $C = 2$ is sufficient. □

Therefore, given an interval $I = [a,b]$, we make use of the Vinogradov function, which measures how often $T(\theta) \in I$. We have shown that $\hat{\theta}$ is of finite type (Corollary 4.3.3), so we will use a Vinogradov function along with the error estimate for quasi-Monte Carlo integration for the following theorem.

Theorem 5.2.2. *Let $E/\mathbb{F}_p$ be an ordinary elliptic curve with normalized Frobenius angle $\hat{\theta}$. Let $I = [a,b] \subset [-2,2]$ be the target interval for the normalized traces $\overline{a}_n$. Let $\Delta > 0$, and define the quantity*

$$A_{I,\Delta} = \frac{1}{\pi}(\arccos((a+2\Delta)/2) - \arccos((b-2\Delta)/2)).$$

Then the proportion of extensions of degree up to N where $\overline{a}_n \in I$ satisfies the inequality

$$\mathrm{PropTr}_{E,N,I} \geq A_{I,\Delta} - O\left(\frac{1}{N}\right). \tag{5.7}$$

Proof. Recall from Corollary 4.3.3 that $\hat{\theta}$ is of finite type. Let T be the function

$$T : \mathbb{R} \longrightarrow \mathbb{R}$$

$$\theta \longmapsto 2\cos(2\pi\theta)$$

so that $T(n\hat{\theta}) = \overline{a}_n$. As previously noted, T admits a Vinogradov function, Ψ. Recall from the definition of the Vinogradov function, that given α, β, Δ, we have the sets

$$R_1 = T^{-1}\left((\alpha + \Delta, \beta - \Delta)\right) \cap [0,1]$$
$$R_0 = T^{-1}\left(\mathbb{R} \setminus (\alpha - \Delta, \beta + \Delta)\right) \cap [0,1]$$

where Ψ takes value 1 on R_1 and value 0 on R_0. Thus, given Δ, define the quantities $\alpha = a + \Delta, \beta = b - \Delta$ and the regions

$$R_1 = T^{-1}\left((a + 2\Delta, b - 2\Delta)\right) \cap [0,1]$$
$$R_0 = T^{-1}\left(\mathbb{R} \setminus (a, b)\right) \cap [0,1].$$

The Vinogradov function $\Psi(\theta)$ takes value 1 on R_1, takes value 0 on R_0, and is everywhere bounded $0 \leq \Psi(\theta) \leq 1$ (note in particular, this holds on the preimages of $[a, a + 2\Delta]$ and $[b - 2\Delta, b]$). By 3.3.5 we have

$$\left| \frac{1}{N} \sum_{n=1}^{N} \Psi(n\hat{\theta}) - \int_0^1 \Psi(x)dx \right| \ll \frac{1}{N}. \tag{5.8}$$

We must now relate the sum $\frac{1}{N}\sum_{n=1}^{N} \Psi(n\hat{\theta})$ to $\mathrm{PropTr}_{E,N,I}$ and give a lower bound on the integral $\int_0^1 \Psi(x)dx$. First, as noted in Section 4.5.2, the sum $\frac{1}{N}\sum_{n=1}^{N} \Psi(n\hat{\theta})$ is an underestimate of $\mathrm{PropTr}_{E,N,I}$ because a term $n\hat{\theta}$ correspond to an extension in $\mathrm{ExtSetTr}_{E,N,I}$, but $\Psi(n\hat{\theta}) < 1$.

We find a lower bound on the integral $\int_0^1 \Psi(x)dx$ by restricting to the region R_1, because

$$\int_{R_1} \Psi(x)dx < \int_0^1 \Psi(x)dx.$$

The integral on R_1 is the measure of the set of θ that satisfies the inequalities $\alpha+2\Delta \leq 2\cos(2\pi\theta) \leq \beta - 2\Delta$. First consider the inequality $\alpha + 2\Delta < 2\cos(2\pi\theta)$. For $\theta \in [0,1]$ this inequality is satisfied exactly by $\theta < \frac{\arccos((\alpha+2\Delta)/2)}{2\pi}$ and $\theta > 1 - \frac{\arccos((\alpha+2\Delta)/2)}{2\pi}$. Therefore the measure of the set that satisfies $\alpha + 2\Delta < 2\cos(2\pi\theta)$ is $\frac{\arccos((\alpha+2\Delta)/2)}{\pi}$. After a similar computation for $2\cos(2\pi\theta) \leq \beta - 2\Delta$, we find

$$A_{I,\Delta} = \int_{R_1} \Psi(x)dx = \frac{1}{\pi}\big(\arccos((a+2\Delta)/2) - \arccos((b-2\Delta)/2)\big).$$

Returning to (5.8), there exists a constant M such that

$$\frac{1}{N}\sum_{n=1}^{N} \Psi(n\hat{\theta}) \geq \int_0^1 \Psi(x)dx - \frac{M}{N}$$

Then combine the inequalities

$$\mathrm{PropTr}_{E,N,I} \geq \frac{1}{N}\sum_{n=1}^{N} \Psi(n\hat{\theta})$$

and

$$A_{I,\Delta} \leq \int_0^1 \Psi(x)dx$$

to finish the result.

□

Example 5.2.3. Let E be an elliptic curve with trace $a_1 = 5$ over $\mathbb{F}_p$ with $p = 19$. One such curve has equation $y^2 = x^3 + 3x + 8$. We consider the proportion of extensions for which the normalized

Frobenius trace lands in the interval $I = [-2, -1]$. Let $\Delta = 0.0001$, and calculate that

$$A_{I,\Delta} \approx 0.3287$$

which is indeed a lower bound on $\mathrm{PropTr}_{E,N,I}$ as one can see from the rightmost column of Table 5.2.

Table 5.2: Counts and proportions of normalized traces that land in $I = [-2, -1]$ up to extensions of degree N for the elliptic curve $y^2 = x^3 + 3x + 8$ over $\mathbb{F}_{19}$.

N	# $\mathrm{ExtSetTr}_{E,N,I}$	$\mathrm{PropTr}_{E,N,I}$
50	18	0.36
100	32	0.32
500	167	0.334
1000	334	0.334
5000	1667	0.3334
10000	3333	0.3333

A natural question is: how accurate is $O(1/N)$? Could the true rate of convergence be faster? To consider this, let

$$\mathrm{Error}_{E,N,I} = \left|\mathrm{PropTr}_{E,N,I} - A_{I,\Delta}\right|.$$

For an elliptic curve over $\mathbb{F}_{19}$ with trace $a_1 = 3$ and target interval $I = [1/2, 1]$, figure 5.6 plots (in the black dots) $\mathrm{Error}_{E,N,I}$. Models of the form A/N (in blue), $B/\sqrt{N}$ (in purple) and $C/N^{1.5}$ for are fitted to the data and plotted along side the data points (the constants A, B, C are found via a built-in SageMath function). While far from conclusive, this figure suggests that $O(1/N^{1.5})$ is unlikely, and $O(1/N)$ visually fits the data well.

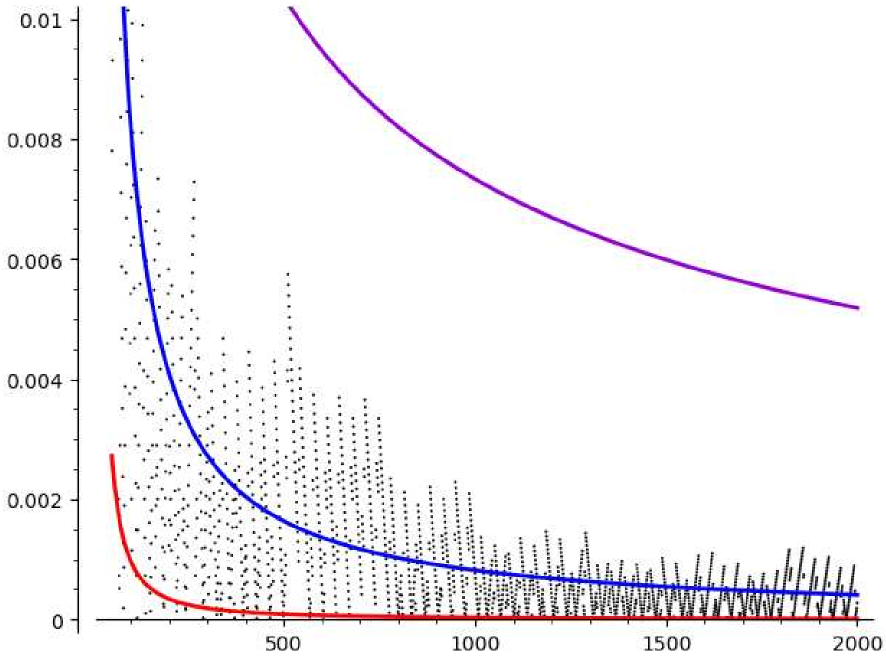


Figure 5.6: Best fits for A/N (blue), $B/\sqrt{N}$ (purple), $C/N^{1.5}$ (red). Here $A = 0.818, B = 0.232, C = 0.964$. For $a_1 = 3, p = 19$, error for normalized traces in the interval $[1/2, 1]$.

5.3 Traces for two isogeny classes

Let p be a prime, and let $E^{(1)}$ and $E^{(2)}$ be ordinary elliptic curves over $\mathbb{F}_p$ that are geometrically not isogenous. Let $\overline{a}_n^{(1)}, \overline{a}_n^{(2)}$ be the normalized traces of $E^{(1)}, E^{(2)}$ (respectively) over $\mathbb{F}_{p^n}$. Let $\hat{\theta}^{(1)}, \hat{\theta}^{(2)}$ be their normalized Frobenius angles, and recall from Corollary 4.3.3 that the tuple $\hat{\boldsymbol{\theta}} = (\hat{\theta}^{(1)}, \hat{\theta}^{(2)})$ is of finite type. In this section, we aim to quantify the set of extensions $\mathbb{F}_{p^n}$ such that the average of the normalized traces lies in a target interval. Let $I = [a, b] \subset [-2, 2]$ be the target interval. Let

$$\mathrm{ExtSetTr}_{E^{(1)},E^{(2)},N,I} = \{n \leq N \ : \ a < \frac{\overline{a}_n^{(1)} + \overline{a}_n^{(2)}}{2} < b\}$$

be the set of degrees of extensions where the average of the normalized traces lands in I. Define

$$\mathrm{PropTr}_{E^{(1)},E^{(2)},N,I} = \frac{\#\,\mathrm{ExtSetTr}_{E^{(1)},E^{(2)},N,I}}{N}$$

to be the proportion of extensions where the average of the traces lands in I. This section aims to give a distribution for $\mathrm{ExtSetTr}_{E^{(1)},E^{(2)},N,I}$ and a rate of convergence in terms of N. The theorem and techniques of this section will be very similar to those from Theorem 5.2.2, and will again follow the scaffolding given in 4.5. We first show that a relevant function T allows for the construction the Vinogradov function. We then provide a calculation of the relevant integral in Lemma 5.3.2 and finally give the main theorem for $\mathrm{PropTr}_{E^{(1)},E^{(2)},N,I}$ in Theorem 5.3.3.

First, recall that the normalized trace for an elliptic curve can be calculated from the normalized Frobenius angle by $\overline{a}_n = 2\cos(2n\pi\hat{\theta})$. Therefore, to calculate the average of two normalized traces, we are interested in the function

$$\begin{aligned} T(\theta_1, \theta_2) &= \frac{1}{2}\left(2\cos(2\pi\theta_1) + 2\cos(2\pi\theta_2)\right) \\ &= \cos(2\pi\theta_1) + \cos(2\pi\theta_2). \end{aligned}$$

Lemma 5.3.1. *The function*

$$\begin{tikzcd} T : \mathbb{R}^2 \arrow[r] & \mathbb{R} \\ (\theta_1, \theta_2) \arrow[r, mapsto] & \cos(2\pi\theta_1) + \cos(2\pi\theta_2) \end{tikzcd}$$

meets the criterion of Definition 3.5.1. That is, it satisfies the following conditions:

1. *T is periodic of period 1.*

2. *There exists a positive $K \in \mathbb{R}$ such that $|\nabla T(\boldsymbol{\theta})| \leq K$ for all $\boldsymbol{\theta} \in \mathbb{R}^2$.*

3. *There exists an integer $C > 0$ such that, for every $\gamma \in \mathbb{R}$ and every $\vartheta \in [0, 1]$ we have*

$$\#\Big(T^{-1}(\gamma) \cap X_j(\vartheta)\Big) \leq C$$

for $1 \leq j \leq 2$.

Proof. T is clearly periodic of period 1, and the gradient of T is bounded by $K = 2\pi$. Now consider the third property. Let $\gamma \in \mathbb{R}$ be fixed. For a given $\vartheta \in [0,1]$, the quantity

$$\#\Big(T^{-1}(\gamma) \cap X_j(\boldsymbol{\vartheta})\Big)$$

is the number of solutions to $\cos(2\pi x) + \cos(2\pi\vartheta) = \gamma$ for $x \in [0,1]$. Thus it suffices to set $C = 2$. □

Therefore, given an interval $I = [a,b]$ and $\Delta > 0$, we make use of the Vinogradov function, Ψ, which measures how often $T(\boldsymbol{\theta}) \in I$. We have the regions

$$R_1 = T^{-1}\Big((a+2\Delta, b-2\Delta)\Big) \cap [0,1]$$
$$R_0 = T^{-1}\Big(\mathbb{R} \setminus (a,b)\Big) \cap [0,1]$$

and Ψ takes value 1 on R_1 and value 0 on R_0. In Theorem 5.3.3 we shall make use $\int_{R_1} \Psi(\boldsymbol{x})d\boldsymbol{x}$ as a lower bound for $\int_{[0,1]^2} \Psi(\boldsymbol{x})d\boldsymbol{x}$. We first provide a computation for this integral.

Lemma 5.3.2. *Let Δ be given (via construction of the Vinogradov function $\Psi(x)$), and define $\hat{a} = a + 2\Delta$ and $\hat{b} = b - 2\Delta$.*

1. *if $\hat{a}, \hat{b} > 0$*

$$\int_{R_1} \Psi(x) = \int_{\hat{a}-1}^{1} \frac{\arccos(\hat{a}-t)}{\pi^2\sqrt{1-t^2}}dt - \int_{\hat{b}-1}^{1} \frac{\arccos(\hat{b}-t)}{\pi^2\sqrt{1-t^2}}dt$$

2. *if $\hat{a}, \hat{b} < 0$,*

$$\int_{R_1} \Psi(x) = \int_{|\hat{b}|-1}^{1} \frac{\arccos(|\hat{b}|-t)}{\pi^2\sqrt{1-t^2}}dt - \int_{|\hat{a}|-1}^{1} \frac{\arccos(|\hat{a}|-t)}{\pi^2\sqrt{1-t^2}}dt$$

3. *If* $\hat{a} < 0$ *and* $\hat{b} > 0$

$$\int_{R_1} \Psi(x) =$$

$$1 - 2\left(\int_{-1}^{\hat{a}+1} \frac{2\pi - \arccos(\hat{a} - t)}{4\pi^2\sqrt{1-t^2}} dt - \int_{-1}^{\hat{a}+1} \frac{\arccos(\hat{a} - t)}{4\pi^2\sqrt{1-t^2}} dt\right) - \int_{\hat{b}-1}^{1} \frac{\arccos(\hat{b} - 1)}{\pi^2\sqrt{1-t^2}} dt.$$

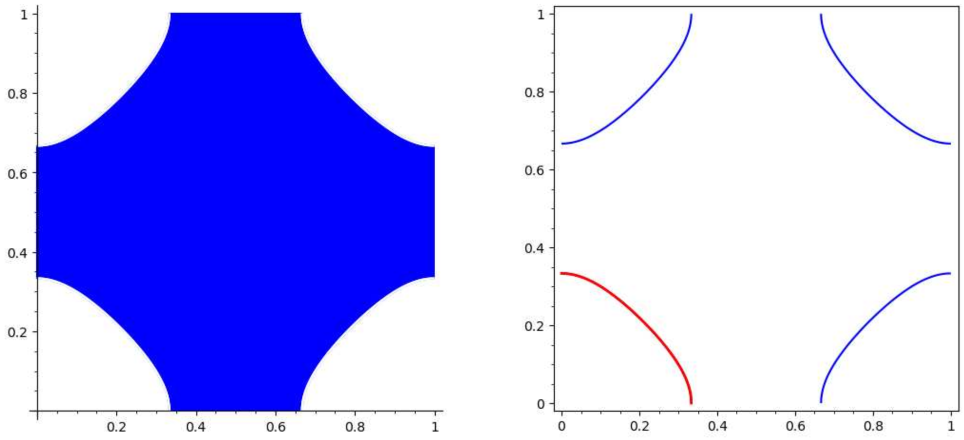
Proof. Let c be a constant in the interval $-2 \leq c \leq 2$. These integral formulas follow from parametrizing the curve given by

$$\cos(2\pi\theta_1) + \cos(2\pi\theta_2) = c.$$

If $c > 0$, we have the parameterization

$$x(t) = \frac{\arccos(t)}{2\pi}, \quad y(t) = \frac{\arccos(c-t)}{2\pi}$$
$$c - 1 \leq t \leq 1$$

For an illustration of the region $\cos(2\pi\theta_1) + \cos(2\pi\theta_2) < c$ along with the parameterization, see Figure 5.7.



(a) The region $\cos(2\pi\theta_1) + \cos(2\pi\theta_2) < 1/2$

(b) The parameterization for $c > 0$ in red.

Figure 5.7: Illustrations of the region $\cos(2\pi\theta_1) + \cos(2\pi\theta_2) < 1/2$ and the associated parameterization.

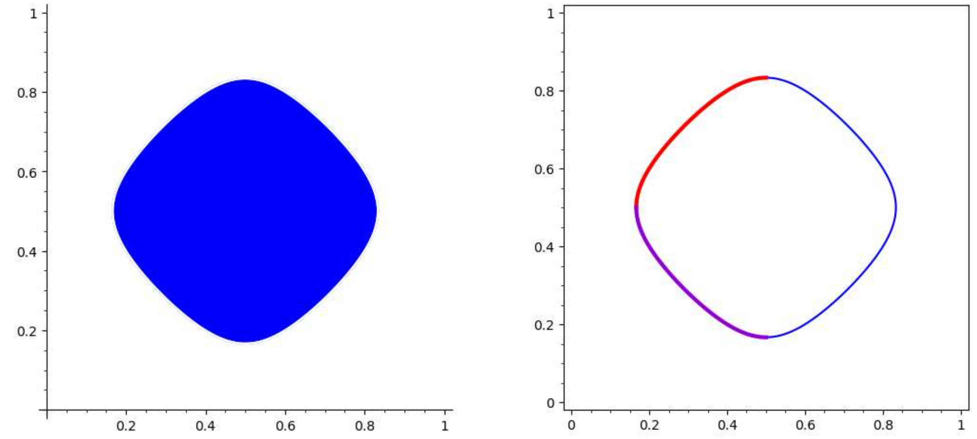
If instead $c < 0$, we need a parametrization of the upper and lower parts, which are given by

$$x_{\text{lower}}(t) = \frac{\arccos(t)}{2\pi}, \quad y_{\text{lower}}(t) = \frac{\arccos(c-t)}{2\pi}$$
$$-1 \leq t \leq -1 - c$$

and

$$x_{\text{upper}}(t) = \frac{\arccos(t)}{2\pi}, \quad y_{\text{upper}}(t) = 1 - \frac{\arccos(c-t)}{2\pi}$$
$$-1 \leq t \leq -1 - c.$$

See Figure 5.8 for an illustration. With the parameterizations in hand, the result is an exercise in calculus via the integrals $\int y dx$ or $\int y_{\text{upper}} dx_{\text{upper}} - \int y_{\text{lower}} dx_{\text{lower}}$.



(a) The region $\cos(2\pi\theta_1) + \cos(2\pi\theta_2) < -1/2$

(b) The parameterization for $c < 0$ in red and purple.

Figure 5.8: Illustrations of the region $\cos(2\pi\theta_1) + \cos(2\pi\theta_2) < -1/2$ and the associated parameterization.

□

We now give a lower bound on $\mathrm{PropTr}_{E^{(1)},E^{(2)},N,I}$ whose main term uses the above parameterizations.

Theorem 5.3.3. *Let $E^{(1)}$ and $E^{(2)}$ be ordinary elliptic curves with over $\mathbb{F}_p$ that are geometrically not isogenous. Let $I = [a, b] \subset [-2, 2]$ be the given target interval for the average of the normalized traces. For any $\Delta > 0$*

$$\mathrm{PropTr}_{E^{(1)},E^{(2)},N,I} \geq \int_{R_1} \Psi(\boldsymbol{x}) d\boldsymbol{x} - O\left(\frac{1}{N}\right).$$

Proof. We follow the proof structure in 4.5. As above, let $T(\theta_1, \theta_2) = \cos(2\pi\theta_1) + \cos(2\pi\theta_2)$. Let $\alpha = a + \Delta, \beta = b - \Delta$ which gives the regions

$$R_1 = T^{-1}\Big((a + 2\Delta, b - 2\Delta)\Big) \cap [0, 1]$$
$$R_0 = T^{-1}\Big(\mathbb{R} \setminus (a, b)\Big) \cap [0, 1]$$

and $\Psi(\boldsymbol{\theta})$ takes value 1 on R_1 and 0 on R_0.

Note that this choice of α, β ensures the undercount

$$\sum_{n=1}^{N} \Psi(n\hat{\boldsymbol{\theta}}) < \# \, \mathrm{ExtSetTr}_{E^{(1)},E^{(2)},N,I} \, .$$

This inequality holds because $a < T(n\hat{\boldsymbol{\theta}}) < b$ implies $n \in \mathrm{ExtSetTr}_{E^{(1)},E^{(2)},N,I}$, however $\Psi(n\hat{\boldsymbol{\theta}})$ is less than or equal to 1. Therefore the sum $\sum_{n=1}^{N} \Psi(n\hat{\boldsymbol{\theta}})$ is less than or equal to $\# \, \mathrm{ExtSetTr}_{E^{(1)},E^{(2)},N,I}$.

Because $\hat{\boldsymbol{\theta}}$ is of finite type (Corollary 4.3.3), we use the complexity analysis from Theorem 3.3.5 to get

$$\left| \frac{1}{N} \sum_{n=1}^{N} \Psi(n\hat{\boldsymbol{\theta}}) - \int_{[0,1]^2} \Psi(\boldsymbol{x}) d\boldsymbol{x} \right| \ll \frac{1}{N}. \tag{5.9}$$

Note that $\int_{R_1} \Psi(\boldsymbol{x}) d\boldsymbol{x} \leq \int_{[0,1]^2} \Psi(\boldsymbol{x}) d\boldsymbol{x}$, and thus the theorem follows. □

It is not immediately clear what the main term of Equation 5.9 looks like. See Figure 5.9 for a visualization, which plots the term $\int_{R_1} \Psi(\boldsymbol{x}) d\boldsymbol{x}$ over intervals $I = [-2, x]$ as x varies from -2 to 2, that is, the figure is the cumulative distribution. This CDF is plotted over the cumulative histogram for the data in Example 5.3.4, which follows shortly. Also see Figure 5.10 for histograms that illustrate the distributions of the normalized traces, again using the data from Example 5.10.

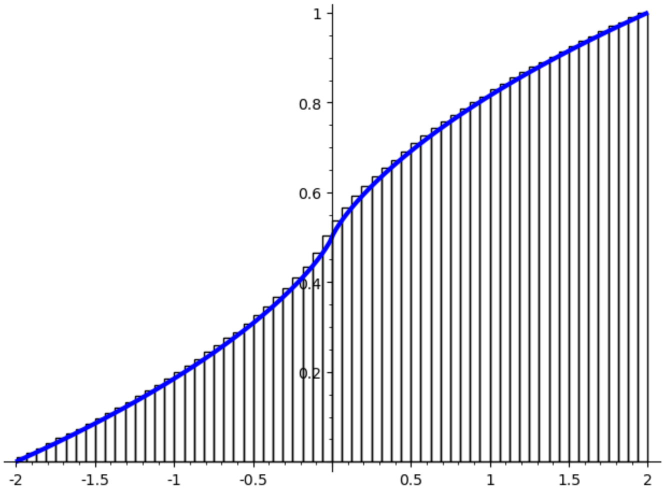


Figure 5.9: In blue is the CDF for the main term $\int_{R_1} \Psi(\boldsymbol{x}) d\boldsymbol{x}$, which is overlayed over the cumulative histogram for Example 5.3.4.

Example 5.3.4. Let $p = 139$, and consider two elliptic curves over $\mathbb{F}_p$. Let $E^{(1)}$ be the elliptic curve with equation $y^2 = x^3 + 56x + 89$ which has trace $a_1^{(1)} = 1$, and let $E^{(2)}$ be the elliptic curve with equation $y^2 = x^3 + 54x + 10$, which has trace $a_1^{(2)} = 16$. We consider the proportion of extensions for which the average of the two normalized traces of Frobenius lands in the interval $I = [-1/2, 1/2]$.

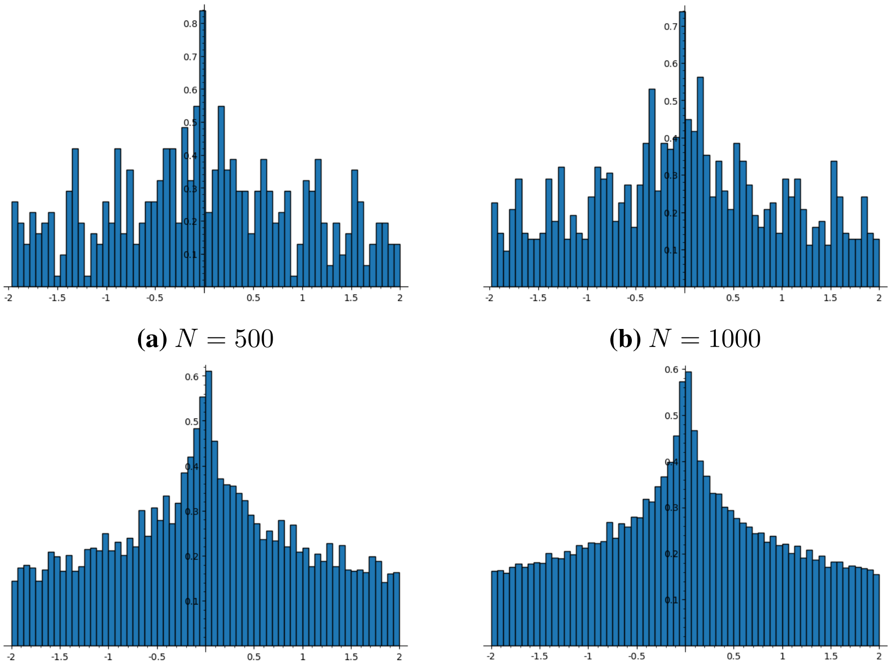
Let $\Delta = .001$. Then

$$0.382 \approx \int_{R_1} \Psi(\boldsymbol{x}) d\boldsymbol{x}$$

which is our lower bound on the rightmost column of Table 5.3. See also the histograms in Figure 5.10.

Table 5.3: Counts and proportions of averages of normalized traces that land in the interval $I = [-1/2, 1/2]$ up to extensions of degree N for two elliptic curves with traces $a_1^{(1)} = 1$ and $a_1^{(2)} = 16$ over $\mathbb{F}_{139}$.

N	$\mathrm{ExtSetTr}_{E^{(1)},E^{(2)},N,I}$	$\mathrm{PropTr}_{E^{(1)},E^{(2)},N,I}$
50	20	0.4
100	37	0.37
500	193	0.386
1000	385	0.385
5000	1921	0.3842
10000	3835	0.3835



(a) $N = 500$

(b) $N = 1000$

(c) $N = 5000$

(d) $N = 10000$

Figure 5.10: Histograms of the average of normalized traces up to extensions of degree N for curves with traces $a_1^{(1)} = 1$ and $a_1^{(2)} = 16$ over $\mathbb{F}_{139}$.

5.4 Explicit Discriminants

5.4.1 Set up

Let $E/\mathbb{F}_p$ be an elliptic curve with Frobenius trace a_1, and let $\Delta_{E,1}$ be the discriminant of the characteristic polynomial of Frobenius over $\mathbb{F}_p$. Recall that the absolute value of the discriminant over $\mathbb{F}_{p^n}$ can be calculated from the Frobenius angle by $|\Delta_{E,n}| = 4p^n \sin^2(n\pi\theta)$, and thus define the normalized discriminant $\overline{\Delta}_{E,n} = \Delta_{E,n}/(4p^n)$. As discussed in Section 2.2.2, the size of the isogeny class is roughly of E over $\mathbb{F}_{p^n}$ is roughly $\sqrt{|\Delta_{E,n}|}$. In Table 5.4 we can see that isogeny classes can be smaller than expected when extensions are ordered by size (as opposed to divisibility). In fact, the size of an isogeny class over extensions of $\mathbb{F}_p$ isn't necessarily monotone. To quantify this phenomenon, we will use quasi-Monte Carlo estimates on the trigonometric factor of the discriminant.

Table 5.4: The size of the isogeny class containing the curve given by $y^2 = x^3 + 32x + 170$. $p = 499, a_1 = 22$ exhibits smaller than expected cardinality at the degree 3 extension.

extension degree, n	$\#I(a_n)$
1	16
2	624
3	364
4	374192

Lemma 5.4.1. *The sequence of normalized discriminants* $\{|\overline{\Delta}_{E,n}|\}$ *is equidistributed with respect to the measure* $dz/(\pi\sqrt{z-z^2})$, *so that*

$$\lim_{N\to\infty} \frac{\#\{\mathbb{F}_{p^n} \,:\, n \le N, a \le |\overline{\Delta}_{E,n}| \le b\}}{N} = \int_a^b \frac{dz}{\pi\sqrt{z-z^2}}.$$

This follows from the ideas of [29, Prop. 2.11]. First, we compute the pushfoward of the uniform measure on $[-\pi, \pi]$ (the space of Frobenius angles) along the measurable map $z = \sin^2(\theta)$.

We then have that $\theta = \arcsin(\sqrt{z})$ and

$$d\theta = \frac{dz}{2\sqrt{z - z^2}}.$$

Note that

$$\int_0^1 \frac{dz}{\sqrt{z - z^2}} = \pi$$

and therefore normalizing so that $[0, 1]$ has measure 1 yields the stated measure.

Let $\epsilon > 0$ be given. We look to quantify the proportion of extensions where $|\overline{\Delta}_{E,n}| > \epsilon$. Define the set $\mathrm{ExtSetDisc}_{E,N,\epsilon} = \{n \leq N \ : \ |\overline{\Delta}_{E,n}| > \epsilon\}$ to be the set of degrees of extensions of $\mathbb{F}_p$ where the normalized discriminant is greater than ϵ. Define the notation

$$\mathrm{PropDisc}_{E,N,\epsilon} = \frac{\#\,\mathrm{ExtSetDisc}_{E,N,\epsilon}}{N} \tag{5.10}$$

to be the proportion of extensions up to degree N such that the normalized discriminant is greater than ϵ. We now give an explicit lower bound on $\mathrm{PropDisc}_{E,N,\epsilon}$.

Theorem 5.4.2. *Let $E/\mathbb{F}_p$ be an ordinary elliptic curve with normalized Frobenius angle $\widetilde{\theta}$. Let $\epsilon > 0$ be given. The proportion of extensions of degrees up to N that have normalized discriminant greater than ϵ satisfies the inequality*

$$\mathrm{PropDisc}_{E,N,\epsilon} \geq 1 - \frac{2\arcsin(\sqrt{\epsilon})}{\pi} - 2D_N^*.$$

Proof. We again use Koksma's inequality with the sequence $\{\widetilde{\theta}_n\}$. Let I be the interval $I = [\epsilon, 1]$, and let f be the function

$$f_I(x) = \chi_I(\sin^2(\pi x))$$

which acts as an indicator for when the normalized discriminant is greater than ϵ. The sum $\sum f_I(\widetilde{\theta}_n)$ counts the extensions in $\mathrm{ExtSetDisc}_{E,N,\epsilon}$. Because this function is an indicator function of an interval, we have $V(f_I) = 2$.

For $x \in [0,1]$, the inequality $\epsilon < \sin^2(\pi x) < 1$ is solved by $\arcsin(\sqrt{\epsilon})/\pi < x < 1 - \arcsin(\sqrt{\epsilon})/\pi$. This interval has length $1 - 2\arcsin(\sqrt{\epsilon})/\pi$, and therefore

$$\int_0^1 f_I(x)dx = 1 - 2\arcsin(\sqrt{\epsilon})/\pi$$

Now use Koksma's inequality to find

$$\left|\sum_{n=1}^{n} f_I(\widetilde{\theta}_n) - \left(1 - \frac{2\arcsin(\sqrt{\epsilon})}{\pi}\right)\right| \leq 2D_N^*$$

which completes the proof. □

The cumulative distribution function for the term $1 - 2\arcsin(\sqrt{x})/\pi$ can be found in Figure 5.11, and histograms from data appear in Figure 5.12.

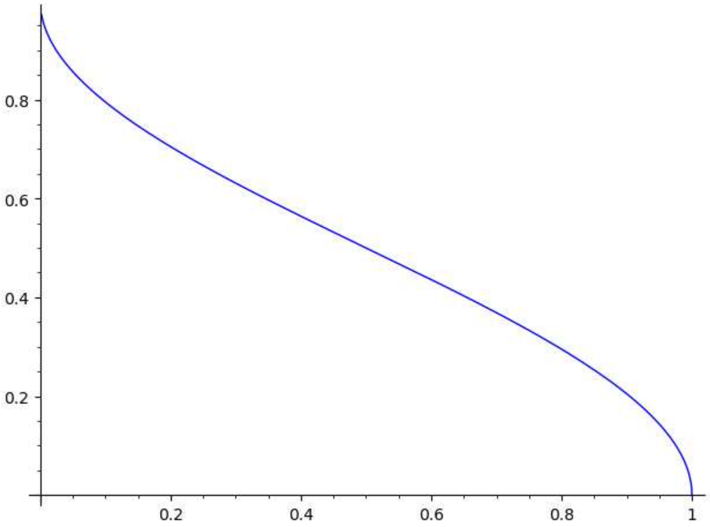


Figure 5.11: The plot of the main term in Theorem 5.4.2, $1 - 2\arcsin(\sqrt{x})/\pi$ for $0 \leq x \leq 1$.

The following example illustrates how to combine Theorem 5.4.2 with the ideas of discrepancy bounds from Section 4.2 to get lower bounds on $\mathrm{PropDisc}_{E,N,\epsilon}$.

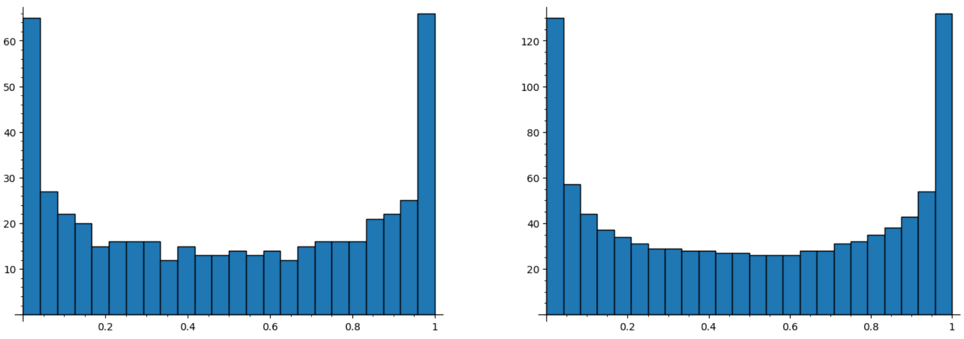
Example 5.4.3. Let $p = 19$, and let E be the curve defined by $y^2 = x^3 + x + 7$ over $\mathbb{F}_p$, which has trace $a_1 = 2$. We consider the proportion of extensions for which the normalized discriminant is greater than $\epsilon = 0.6$. We have the quantity $1 - 2\arcsin(\sqrt{0.6})/\pi \approx 0.4359$, so Theorem 5.4.2 gives the lower bound

$$\mathrm{PropDisc}_{E,N,\epsilon} \geq 0.4359 - 2D_N^*.$$

We again make use of the discrepancy bounds from Theorem 4.2.2 to find an upper bound on the discrepancy, D_N^{UB}. After calculation of D_N^{UB}, our explicit lower bound on $\mathrm{PropDisc}_{E,N,\epsilon}$ is 0.3575 for $N = 500$, and 0.3911 for $N = 1000$. See Table 5.5 for the empirical data, and see Figure 5.12 for the corresponding histograms.

Table 5.5: Computational data for normalized discriminants greater than $\epsilon = 0.6$ for $p = 19$ and trace $a_1 = 3$.

N	D_N^{UB}	Optimal H choice	$0.4359 - 2D_N^{\text{UB}}$	$\#\,\mathrm{ExtSetDisc}_{E,N,\epsilon}$	$\mathrm{PropDisc}_{E,N,\epsilon}$
500	0.0392	121	0.3575	218	0.4357
1000	0.0224	189	0.3911	436	0.436



(a) $N = 500$ **(b)** $N = 1000$

Figure 5.12: Histograms of the normalized discriminants $|\overline{\Delta}_{E,N}|$ for $N = 500$ and $N = 1000$ for the curve $y^2 = x^3 + x + 7$ with $p = 19$.

5.5 Quantitative Discriminants

Continue with E an ordinary elliptic curve over $\mathbb{F}_p$, with normalized Frobenius angle $\hat{\theta}$. Let $|\overline{\Delta}_{E,n}|$ be the absolute value of the normalized discriminant after base change up to $\mathbb{F}_{p^n}$. Recall $\mathrm{ExtSetDisc}_{E,N,\epsilon} = \{n \leq N \ : \ |\overline{\Delta}_{E,n}| > \epsilon\}$ is the set of extensions of $\mathbb{F}_p$ where the normalized discriminant is greater than ϵ. Also recall the quantity $\mathrm{PropDisc}_{E,N,\epsilon} = \frac{\#\,\mathrm{ExtSetDisc}_{E,N,\epsilon}}{N}$ as the proportion of extensions up to degree N such that the normalized discriminant is greater than ϵ. This section aims to give a quantitative lower bound on $\mathrm{PropDisc}_{E,N,\epsilon}$ through the proof structure outlined in section 4.5. That style of proof requires construction of a Vinogradov function, which requires the following lemma.

Lemma 5.5.1. *The function*

$$\begin{tikzcd} T : \mathbb{R} \arrow[r] & \mathbb{R} \\ \theta \arrow[r, mapsto] & \sin^2(\pi\theta) \end{tikzcd}$$

meets the criterion of Definition 3.5.1 with the special case of $s = 1$ in Note 3.5.2. That is, it satisfies the following conditions:

1. *T is periodic of period 1.*

2. *There exists a positive $K \in \mathbb{R}$ such that $|\nabla T(\theta)| \leq K$ for all $\theta \in \mathbb{R}$.*

3. *There exists an integer $C > 0$ such that, for every $\gamma \in \mathbb{R}$ we have*

$$\#\Big(T^{-1}(\gamma) \cap [0,1]\Big) \leq C.$$

Proof. The first two conditions are clearly met. For the third condition, the set

$$\Big(T^{-1}(\gamma) \cap [0,1]\Big)$$

is the set of solutions to $\sin^2(\pi\theta) = \gamma$ for $\theta \in [0,1]$. Thus $C = 2$ is sufficient.

□

Therefore, given $0 < \epsilon < 1$, we will construct a Vinogradov function that measures how often $T(n\theta) \in [\epsilon, 1]$. We'll then combine this with the $O(1/N)$ error estimate since $\hat{\theta}$ is of finite type. This strategy gives the following theorem.

Theorem 5.5.2. *Let $E/\mathbb{F}_p$ be an ordinary elliptic curve. Given $0 < \epsilon < 1$, for every $\Delta > 0$, we have*

$$\mathrm{PropDisc}_{E,N,\epsilon} \geq 1 - \frac{2\arcsin(\sqrt{\epsilon + 2\Delta})}{\pi} - O\left(\frac{1}{N}\right).$$

Proof. This proof follows the framework from Section 4.5, with the necessary details filled in. Let $0 < \epsilon < 1$ be given. Define the function

$$T : \mathbb{R} \longrightarrow \mathbb{R}$$

$$\theta \longmapsto \sin^2(\pi\theta)$$

which allows for the construction of a Vinogradov function $\Psi(\theta)$. Define the quantities $\alpha = \epsilon + \Delta$ and $\beta = 1 + \Delta$. We have the regions

$$\begin{aligned} R_1 &= T^{-1}\Big((\epsilon + 2\Delta, 1)\Big) \cap [0,1] \\ R_0 &= T^{-1}\Big(\mathbb{R} \setminus (\epsilon, 1 + 2\Delta)\Big) \cap [0,1]. \end{aligned}$$

The Vinogradov function $\Psi(\theta)$ takes value 1 on R_1, takes value 0 on R_0, and is bounded $0 \leq \Psi(\theta) \leq 1$ everywhere. Note that this choice for α, β gives the inequality

$$\sum_{n=1}^{N} \Psi(n\hat{\theta}) \leq \# \operatorname{ExtSetDisc}_{E,N,\epsilon}.$$

Because $\hat{\theta}$ is of finite type, Theorem 3.3.5 gives the error estimate

$$\left| \frac{1}{N} \sum_{n=1}^{N} \Psi(n\hat{\theta}) - \int_0^1 \Psi(x)dx \right| \ll \frac{1}{N}. \tag{5.11}$$

From Section 4.5.3, we find a lower bound on $\int_0^1 \Psi(x)dx$ by restricting to the region R_1. The integral on R_1 is simply the length of the region where $\sin^2(\pi\theta) > \epsilon + 2\Delta$, so that

$$\int_{R_1} \Psi(x)d(x) = 1 - \frac{2\arcsin(\sqrt{\epsilon + 2\Delta})}{\pi}.$$

□

Example 5.5.3. Let E be the elliptic curve defined by $y^2 = x^3 + x + 3$ over $\mathbb{F}_{23}$, which has trace $a_1 = -3$. We consider the proportion of extensions where $|\overline{\Delta}_{E,n}|$ is great than $\epsilon = 0.8$. Let $\Delta = 0.001$, then

$$1 - \frac{2\arcsin(\sqrt{\epsilon + 2\Delta})}{\pi} \approx 0.2935$$

and therefore we have the lower bound

$$\mathrm{PropDisc}_{E,N,\epsilon} \geq 0.2935 - O\left(\frac{1}{N}\right).$$

See Table 5.6 for empirical data, and see Figure 5.13 for histograms.

Table 5.6: Counts and proportions of extensions with $|\overline{\Delta}_{E,n}| > .8$ of degree N for the elliptic curve $y^2 = x^3 + x + 3$ over $\mathbb{F}_{23}$.

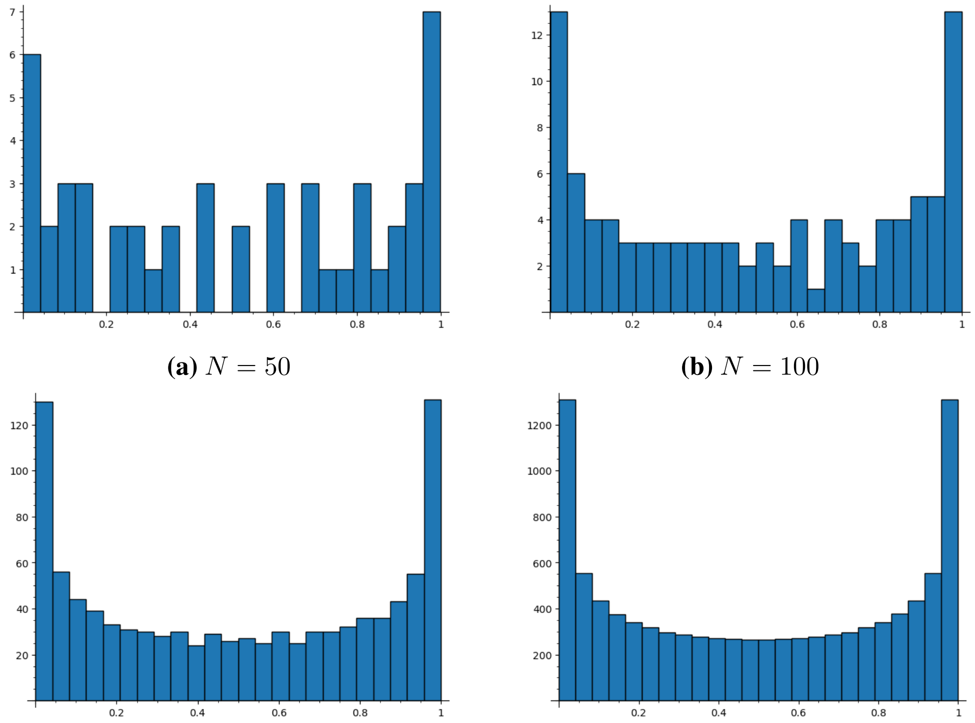
N	# $\mathrm{ExtSetDisc}_{E,N,\epsilon}$	$\mathrm{PropDisc}_{E,N,\epsilon}$
50	16	.32
100	30	.3
500	148	0.296
1000	96	0.296
5000	1477	0.2954
10000	2953	0.2953

5.6 Discriminants for two isogeny class

Let p be a prime, and let $E^{(1)}$ and $E^{(2)}$ be ordinary elliptic curves over $\mathbb{F}_p$ that are geometrically not isogenous. Let $\overline{\Delta}_1^{(1)}, \overline{\Delta}_1^{(2)} \in [0,1]$ be the normalized discriminants of the respective Frobenius polynomials over $\mathbb{F}_p$ and let $\overline{\Delta}_n^{(1)}, \overline{\Delta}_n^{(2)}$ be the normalized discriminants after base change up to $\mathbb{F}_{p^n}$. Let

$$\mathrm{AvgNormDisc}_{E^{(1)},E^{(2)},n} = \frac{|\overline{\Delta}_n^{(1)}| + |\overline{\Delta}_n^{(1)}|}{2}$$

be the average of the normalized discriminants of the two isogeny classes over $\mathbb{F}_{p^n}$. Given $\epsilon > 0$, define the set $\mathrm{ExtSetDisc}_{E^{(1)},E^{(2)},N,\epsilon} = \{n \leq N \ : \ \mathrm{AvgNormDisc}_{E^{(1)},E^{(2)},n} > \epsilon\}$ to be the set of



(a) $N = 50$

(b) $N = 100$

(c) $N = 1000$

(d) $N = 10000$

Figure 5.13: Histograms of $|\overline{\Delta}_{E,N}|$ for extension degrees $N = 50, 100, 1000, 10000$ for the curve $y^2 = x^3 + x + 3$ over $\mathbb{F}_{23}$.

extensions where the average of the normalized discriminants is greater than ϵ. Define the quantity

$$\mathrm{PropDisc}_{E^{(1)},E^{(2)},N,\epsilon} = \frac{\#\,\mathrm{ExtSetDisc}_{E^{(1)},E^{(2)},N,\epsilon}}{N}$$

which is the proportion of extensions up to degree N where the average normalized discriminant is larger than ϵ. This section aims to quantify $\mathrm{PropDisc}_{E^{(1)},E^{(2)},N,\epsilon}$ through the techniques outlined in Section 4.5. We first define a function T that calculates the average of the normalized discriminants, and then show it admits a construction of a Vinogradov function Ψ. We then give an estimate of the integral $\int_{[0,1]^2} \Psi(\boldsymbol{x}) d\boldsymbol{x}$ before applying the quasi-Monte Carlo integral estimate to get the main result of this section in Theorem 5.6.3.

Lemma 5.6.1. *The function*

$$T : \mathbb{R}^2 \longrightarrow \mathbb{R}$$

$$(\theta_1, \theta_2) \longmapsto \tfrac{1}{2}\left(\sin^2(\pi\theta_1) + \sin^2(\pi\theta_2)\right)$$

meets the criterion of Definition 3.5.1. That is, it satisfies the following conditions:

1. *T is periodic of period 1.*
2. *There exists a positive $K \in \mathbb{R}$ such that $|\nabla T(\boldsymbol{\theta})| \leq K$ for all $\boldsymbol{\theta} \in \mathbb{R}^2$.*
3. *there exists an integer $C > 0$ such that, for every $\gamma \in \mathbb{R}$ and every $\vartheta \in [0, 1]$ we have*

   $$\#\Bigg(T^{-1}(\gamma) \cap X_j(\boldsymbol{\vartheta})\Bigg) \leq C.$$

   for $1 \leq j \leq 2$.

Proof. The first two conditions are clear. For the last condition, fix $\gamma \in \mathbb{R}$. For a given $\vartheta \in [0, 1]$, note that

$$\Bigg(T^{-1}(\gamma) \cap X_j(\vartheta)\Bigg)$$

is the set of solutions to $\sin^2(\pi x) + \sin^2(\pi\vartheta) = \gamma$ for $x \in [0, 1)$, so $C = 2$ is sufficient. □

In light of this, we aim to make use of a Vinogradov function, Ψ and the quasi-Monte Carlo integration method from Theorem 3.3.5. Let $\epsilon > 0$ be given. Let $\Delta > 0$, and choose the parameters as $\alpha = \epsilon + \Delta, \beta = 1 + \Delta$. The Vinogradov Ψ function then has the associated regions

$$\begin{aligned} R_1 &= T^{-1}\Big(\alpha + \Delta, \beta - \Delta\Big) \cap [0,1]^2 \\ &= T^{-1}\Big(\epsilon + 2\Delta, 1\Big) \cap [0,1]^2 \\ R_0 &= T^{-1}\Big(\mathbb{R} \setminus (\alpha - \Delta, \beta + \Delta)\Big) \cap [0,1]^2 \\ &= T^{-1}\Big(\mathbb{R} \setminus (\epsilon, 1 + 2\Delta)\Big) \cap [0,1]^2 \end{aligned}$$

where Ψ takes value 1 on R_1, and is bounded $0 \leq \Psi \leq 1$ everywhere else. In order to produce estimates for $\mathrm{PropDisc}_{E^{(1)},E^{(2)},N,\epsilon}$, we use the following integral calculations.

Lemma 5.6.2. *Let Δ be given (via construction from a Vinogradov function Ψ), and define $\hat{\epsilon} = \epsilon + 2\Delta$.*

1. *If $\hat{\epsilon} < 1/2$*

$$\int_{R_1} \Psi(\boldsymbol{x}) d\boldsymbol{x} = 1 - \frac{4}{\pi^2} \int_0^{\sqrt{2\hat{\epsilon}}} \frac{\arcsin(\sqrt{2\hat{\epsilon} - t^2})}{\sqrt{1 - t^2}} dt$$

2. *If $\hat{\epsilon} > 1/2$*

$$\int_{R_1} \Psi(\boldsymbol{x}) d\boldsymbol{x} = \frac{4}{\pi^2} \int_0^{\sqrt{2(1-\hat{\epsilon})}} \frac{\arcsin(\sqrt{2(1 - \hat{\epsilon}) - t^2})}{\sqrt{1 - t^2}} dt$$

3. *If $\hat{\epsilon} = 1/2$, then $\int_{R_1} \Psi(\boldsymbol{x}) d\boldsymbol{x} = \frac{1}{2}$.*

Proof. These integral calculations are found by parameterizing the curve

$$\frac{1}{2}(\sin^2(\pi\theta_1) + \sin^2(\pi\theta_2)) = \hat{\epsilon}.$$

For $\hat{\epsilon} < 1/2$, we have the parameterization

$$x(t) = \frac{\arcsin(t)}{\pi}, \quad y(t) = \frac{\arcsin(\sqrt{2\hat{\epsilon} - t^2})}{\pi} \tag{5.12}$$

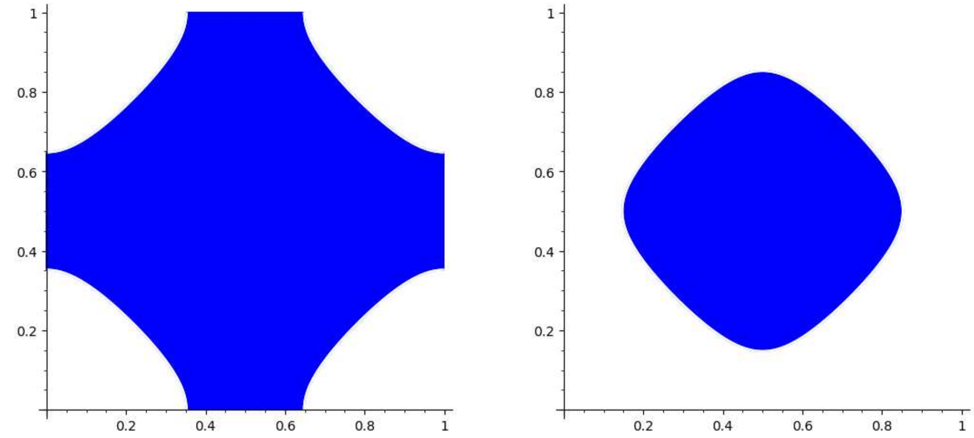
$$0 \leq t \leq \sqrt{2\hat{\epsilon}}. \tag{5.13}$$

The first case then follows from a calculation of $\int y dx$ from the parameterization.

If $\hat{\epsilon} > 1/2$, we exploit the symmetry about $\hat{\epsilon} = 1/2$ of the level set of $T(\boldsymbol{\theta}) = \hat{\epsilon}$. We use a change of coordinates by $\vartheta_i = \theta_1 - 1/2$ and $\varepsilon = 1 - \hat{\epsilon}$ to center the level set at the origin, and again calculate $\int y dx$.

See Figure 5.14 for illustrations of the region $T(\boldsymbol{\theta}) > \hat{\epsilon}$ and Figure 5.15 for the parameterization of the curve $T(\boldsymbol{\theta}) = \hat{\epsilon}$.

□



(a) $\hat{\epsilon} = 0.4$.

(b) $\hat{\epsilon} = 0.6$.

Figure 5.14: Illustrations of the region $(1/2)(\sin^2(\pi\theta_1) + \sin^2(\pi\theta_2)) > \hat{\epsilon}$ for $\hat{\epsilon} = 0.4$ and $\hat{\epsilon} = 0.6$.

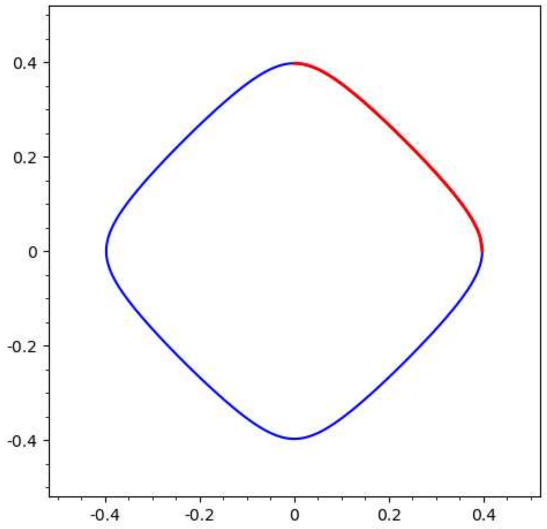


Figure 5.15: In blue, the level set $(1/2)(\sin^2(\pi\theta_1) + \sin^2(\pi\theta_2)) = .45$ with the parameterization shown in red.

Theorem 5.6.3. *Let $E^{(1)}, E^{(2)}$ be ordinary elliptic curves over $\mathbb{F}_p$ that are geometrically not isogenous. Let $\epsilon > 0$ be given. For any $\Delta > 0$,*

$$\mathrm{PropDisc}_{E^{(1)},E^{(2)},N,\epsilon} \geq \int_{R_1} \Psi(\boldsymbol{x}) d\boldsymbol{x} - O\left(\frac{1}{N}\right).$$

Proof. As in Lemma 5.6.2, let T be the function $T(\theta_1, \theta_2) = (1/2)(\sin^2(\pi\theta_1) + \sin^2(\pi\theta_2))$. To construct $\Psi(\boldsymbol{\theta})$, we choose parameters $\alpha = \epsilon + \Delta, \beta = 1 + \Delta$. We then have the regions

$$\begin{aligned} R_1 &= T^{-1}\Bigg(\epsilon + 2\Delta, 1\Bigg) \cap [0,1]^2 \\ R_0 &= T^{-1}\Bigg(\mathbb{R} \setminus (\epsilon, 1 + 2\Delta)\Bigg) \cap [0,1]^2 \end{aligned}$$

and Ψ takes value 1 on R_1 and 0 on R_0. This choice of α, β ensures the inequality

$$\frac{1}{N} \sum_{n=1}^{N} \Psi(n\widetilde{\boldsymbol{\theta}}) \leq \mathrm{PropDisc}_{E^{(1)},E^{(2)},N,\epsilon}.$$

We use the quasi-Monte Carlo integration method from Theorem 3.3.5 to get

$$\left| \frac{1}{N} \sum_{n=1}^{N} \Psi(n\widetilde{\boldsymbol{\theta}}) - \int_{[0,1]^2} \Psi(\boldsymbol{x}) d\boldsymbol{x} \right| \ll \frac{1}{N}.$$

because $\widetilde{\boldsymbol{\theta}}$ is of finite type. The result follows by the inequality $\int_{R_1} \Psi(\boldsymbol{x}) d\boldsymbol{x} \leq \int_{[0,1]^2} \Psi(\boldsymbol{x}) d\boldsymbol{x}$. $\square$

For a visualization of the CDF of $\mathrm{AvgNormDisc}_{E^{(1)},E^{(2)},n}$, see 5.16 which is overlaid on the data of Example 5.6.4. See also the histograms in Figure 5.17.

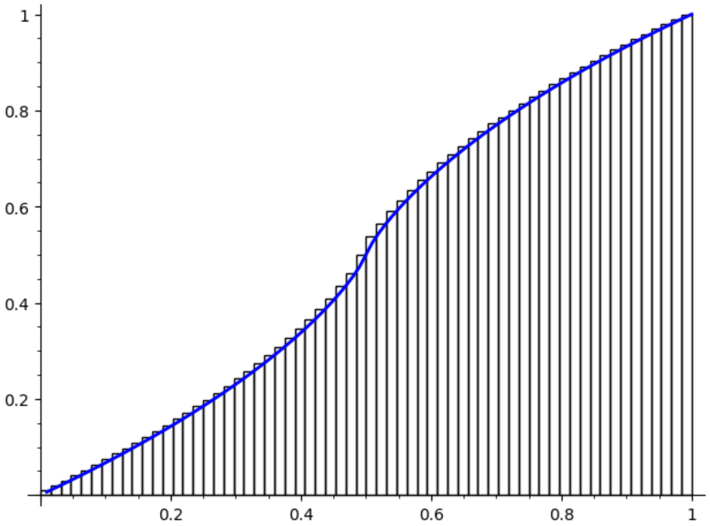


Figure 5.16: The CDF of $\mathrm{AvgNormDisc}_{E^{(1)},E^{(2)},n}$ (in blue), over the cumulative histogram for Example 5.6.4

Example 5.6.4. Let $p = 47$, and consider the curves $E^{(1)} : y^2 = x^3 + 23x + 4$ and $E^{(2)} : y^2 = x^3 + 5x + 39$ which have traces $a_1^{(1)} = 2$ and $a_1^{(2)} = 5$ over $\mathbb{F}_p$. We consider the proportion of extensions for which the average of the normalized discriminants is greater than $\epsilon > 0.8$. Let $\Delta = 0.001$, then

$$0.1411 \approx \int_{R_1} \Psi(\boldsymbol{x}) d\boldsymbol{x}$$

so that $\mathrm{PropDisc}_{E^{(1)},E^{(2)},N,\epsilon} \geq 0.1411 - O(1/N)$ is our lower bound for the rightmost column of table 5.7.

Table 5.7: Counts and proportions of averages of normalized discriminants larger than $\epsilon = 0.8$ up to extensions of degree N. This data is for the curves $E^{(1)} : y^2 = x^3 + 23x + 4$ and $E^{(2)} : y^2 = x^3 + 5x + 39$ over $\mathbb{F}_{47}$.

N	$\mathrm{ExtSetDisc}_{E^{(1)},E^{(2)},N,\epsilon}$	$\mathrm{PropDisc}_{E^{(1)},E^{(2)},N,\epsilon}$
50	7	0.14
100	15	0.15
500	71	0.142
1000	145	0.145
5000	712	0.1424
10000	1423	0.1423

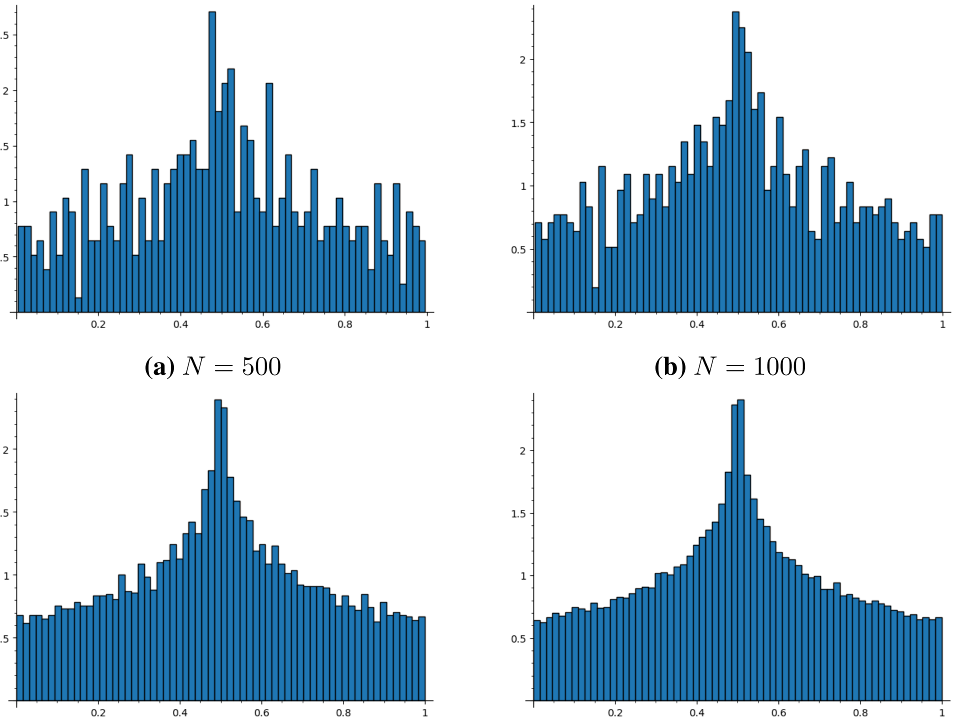
5.7 Arbitrary collections of Isogeny Classes

One might notice that the histogram in Figure 5.10 for two traces looks significantly different than the histograms for one class (for example, Figure 5.5). In essence, the central limit theorem is beginning to determine the distribution of the averages of traces. Throughout this section, we no longer consider a finite bound N on extension degrees, rather, we have a bound m on the number of isogeny classes under consideration. We begin with the Berry-Esseen theorem, which is a quantitative version of the central limit theorem. This theorem roughly states that the average of a collection of random variables converges to a normal distribution at a rate of the square root of the number of random variables.

5.7.1 The Berry-Esseen theorem

Recall for a random variable, X, with density $f(z)$ the n^{th} moment is defined as

$$E[X^n] = \int_{-\infty}^{\infty} z^n f(z) dz.$$



(a) $N = 500$ **(b)** $N = 1000$

(c) $N = 5000$ **(d)** $N = 10000$

Figure 5.17: Histograms of the averages of normalized discriminants for extensions up to degree N for the curves $E^{(1)} : y^2 = x^3 + 23x + 4$ and $E^{(2)} : y^2 = x^3 + 5x + 39$ over $\mathbb{F}_{47}$.

Let $X_1, \ldots X_m$ be independent and identically distributed (i.i.d) random variables with $E(X_j) = 0, E(X_j^2) = \sigma^2, E(|X_j|^3) = \rho < \infty$ (because the X_j are i.i.d, these quantities are the same for each of the X_j). Define

$$Y_m = \frac{X_1 + X_2 + \ldots + X_m}{m}$$

to be the sample mean, and let F_m be the cumulative distribution function of

$$\frac{Y_m \sqrt{m}}{\sigma}.$$

Let Φ be the cumulative distribution function of the standard normal distribution. The Berry-Esseen theorem gives a bound on the error in estimating F_m by Φ in terms of σ, ρ and m.

Theorem 5.7.1 (Berry-Esseen)**.** *There exists a positive constant C such that, for all x and all m, the inequality*

$$|F_m(z) - \Phi(z)| \leq \frac{C\rho}{\sigma^3\sqrt{m}}$$

holds.

The current best bound for C is $C < .4748$, due to [30].

5.7.2 Berry-Esseen for collections of elliptic curves

We now consider the distribution for the average of traces from m geometrically not isogenous elliptic curves over $\mathbb{F}_p$. Let X_j be the random variable of the values of normalized traces $\overline{a}_n^{(j)}$ for the elliptic curve $E^{(j)}$. Then X_j has the density function

$$f(z) = \frac{1}{\pi\sqrt{4-z^2}}$$

and all $X_1, \ldots, X_m$ are i.i.d. Note that $f(z)$ has support on the bounded interval $[-2, 2]$ and thus $f(z)$ takes value 0 outside of $[-2, 2]$. We first check the values of the moments $E(X_j), E(X_j^2) = \sigma^2, E(|X_j|^3) = \rho < \infty$. We find that the mean of X_j is 0, by the following calculation

$$\begin{aligned} E[X_j] &= \int_{-\infty}^{\infty} \frac{zdz}{\pi\sqrt{4-z^2}} \\ &= 0. \end{aligned}$$

We also compute the variance,

$$\begin{aligned} E[X_j^2] &= \int_{-\infty}^{\infty} \frac{z^2}{\pi\sqrt{4-z^2}} dz \\ &= 2 \end{aligned}$$

and therefore the standard deviation of X_j is $\sigma = \sqrt{2}$. Finally, we need that the absolute third moment, ρ, is finite:

$$E(|X_j|^3) = \int_{-\infty}^{\infty} \frac{|z|^3}{\pi\sqrt{4-z^2}} dz = \frac{32}{3\pi}.$$

Theorem 5.7.2. *Let $E^{(1)}, \ldots, E^{(m)}$ be a collection of m ordinary, geometrically not isogenous elliptic curves over $\mathbb{F}_p$, with random variables $X_1, \ldots, X_m$ corresponding to the values of the normalized traces. Let Y_m be the sample mean*

$$Y_m = \frac{X_1 + \ldots X_m}{m}$$

and let $F_m(x)$ be the CDF of

$$\frac{Y_m\sqrt{m}}{\sigma}.$$

Let $\Phi(x)$ be the CDF of the standard normal distribution. Let $\rho = 32/(3\pi)$ and $\sigma = \sqrt{2}$. Then the distance between $F_m(x)$ and $\Phi(x)$ has the bound

$$|F_m(x) - \Phi(x)| \leq \frac{C\rho}{\sigma^3\sqrt{m}}$$

for a constant $C < 0.4748$.

Proof. This follows from the Berry-Esseen theorem along with the previous calculations of the moments $E(X_j), E(X_j^2), E(|X_j|^3)$. □

Example 5.7.3. Consider all isogeny classes with positive Frobenius trace over $\mathbb{F}_{179}$. The histogram for the averages of the normalized traces of these classes over exensions $\mathbb{F}_{179^n}$ appears in Figure 5.18. Figure 5.19a shows the sample mean of the traces, Y_m, along with the probability density of the standard normal distributions, with the corresponding cumulative distribution in Figure 5.19b.

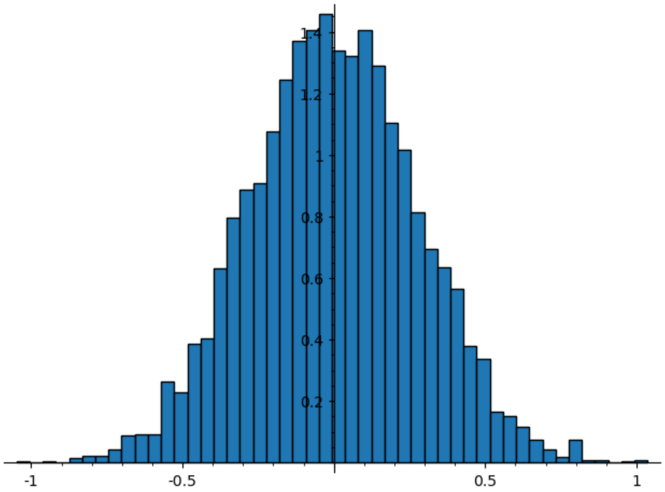
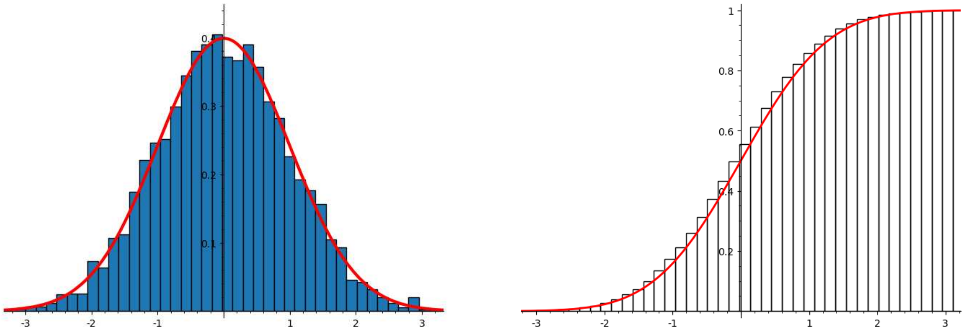


Figure 5.18: The histogram for the average of all normalized traces for isogeny classes that have positive trace over $\mathbb{F}_{179}$.



(a) PDF

(b) CDF

Figure 5.19: Density and cumulative histograms for $Y_m\sqrt{m}/\sigma$ of all isogeny classes with postive trace over $\mathbb{F}_{179}$ up to extension degree $N = 5000$. The standard normal distribution is in red.

Chapter 6

Abelian Varieties

Let A be an abelian variety of dimension g over $\mathbb{F}_p$. Recall that the Frobenius polynomial is of degree $2g$, with roots of the form $\alpha_j = \sqrt{q}\exp(i\theta_j)$ for $1 \leq j \leq g$ along with their complex conjugates $\overline{\alpha_1}, \ldots \overline{\alpha_g}$. Possibly after rearranging, the numbers $0 \leq \theta_1 \leq \ldots \leq \theta_g$ are the Frobenius angles.

Recall the angle rank of A is the quantity

$$\delta(A) = \dim_{\mathbb{Q}}(\text{Span}_{\mathbb{Q}}(\{\theta_j \ : \ 1 \leq j \leq 2g\} \cup \{\pi\})) - 1$$

and A has maximal angle rank if $\delta(A) = g$. See [31] and [32] for more on angle ranks. Under the assumption that A has maximal angle rank, the normalized Frobenius angle tuples $\hat{\boldsymbol{\theta}}$ and $\widetilde{\boldsymbol{\theta}}$ are of finite type. We thus state an analogue of Theorem 5.3.3 for abelian varieties of maximal angle rank.

6.1 Traces of abelian varieties

Let $I = [a, b] \subset [-2g, 2g]$ be a given target interval for the normalized traces $\overline{a}_n$. Let

$$\text{ExtSetTr}_{A,N,I} = \{n \leq N \ : \ a < \overline{a}_n < b\}$$

be the set of degrees of extensions where the normalized trace lands in I. Define

$$\text{PropTr}_{A,N,I} = \frac{\#\,\text{ExtSetTr}_{A,N,I}}{N}$$

to be the proportion of extensions where the normalized trace lands in I. We first define a function T to use in construction of a Vinogradov function.

Lemma 6.1.1. *The function*

$$T : \mathbb{R}^g \longrightarrow \mathbb{R}$$

$$(\theta_1, \ldots, \ldots, \theta_g) \longmapsto \textstyle\sum_{j=1}^{g} 2\cos(2\pi\theta_j)$$

meets the criterion of Definition 3.5.1. That is, T satisfies the following conditions:

1. *T is periodic of period 1.*

2. *There exists a positive $K \in \mathbb{R}$ such that $|\nabla T(\boldsymbol{\theta})| \leq K$ for all $\boldsymbol{\theta} \in \mathbb{R}^g$.*

3. *There exists an integer $C > 0$ such that, for every $\gamma \in \mathbb{R}$ and every $\boldsymbol{\vartheta} \in [0,1]^{g-1}$ we have*

$$\#\Big(T^{-1}(\gamma) \cap X_j(\boldsymbol{\vartheta})\Big) \leq C$$

for $1 \leq j \leq g$.

Proof. Let g be fixed. Condition 1 is clear. For condition 2, we certainly have the bound $|\nabla T(\boldsymbol{\theta})| \leq 4\pi g$.

Now for the third condition. Fix j to be in the range $1 \leq j \leq g$. For a given $\boldsymbol{\vartheta} = (\vartheta_1, \ldots \vartheta_{g-1}) \in [0,1]^{g-1}$,

$$\Big(T^{-1}(\gamma) \cap X_j(\boldsymbol{\vartheta})\Big)$$

is the set of solutions to

$$2\cos(2\pi x) + \sum_{i \neq j} 2\cos(2\pi\vartheta_i) = \gamma$$

for $x \in [0,1]$. Let $\Gamma = \gamma - \sum_{i \neq j} 2\cos(2\pi\vartheta_i)$. Then $2\cos(2\pi x) = \Gamma$ has at most two solutions, therefore $C = 2$ is sufficient.

□

Given $I = [a, b]$, we can construct the Vinogradov function $\Psi(\boldsymbol{x})$, which measures when $T(\boldsymbol{\theta}) \in I$, that is, when $\overline{a}_n \in I$. Let $\alpha = a + \Delta, \beta = b - \Delta$. Then we have the regions

$$\begin{aligned} R_1 &= T^{-1}\Big((a + 2\Delta, b - 2\Delta) \Big) \cap [0,1]^g \\ R_0 &= T^{-1}\Big(\mathbb{R} \setminus (a, b) \Big) \cap [0,1]^g \end{aligned}$$

where $\Psi(\boldsymbol{x})$ takes value j on R_j and is everywhere bounded $0 \leq \Psi(\boldsymbol{x}) < 1$.

Theorem 6.1.2. *Let $A/\mathbb{F}_p$ be an abelian variety of dimension g with maximal angle rank, and let $I = [a, b] \subset [-2g, 2g]$ be the target interval for the normalized traces. Then the proportion of extensions where the trace $\overline{a}_n$ lands in I satisfies*

$$\mathrm{PropTr}_{A,N,I} \geq \int_{R_1} \Psi(\boldsymbol{x}) d\boldsymbol{x} - O\left(\frac{1}{N}\right).$$

Proof. We proceed in the same manner as the previous proofs with an $O(1/N)$ complexity term. Fix Δ. Consider the function T from Lemma 6.1.1 which allows the construction of the Vinogradov function $\Psi(\boldsymbol{x})$. From Theorem 3.3.5 we have

$$\left| \frac{1}{N} \sum_{n=1}^{N} \Psi(n\hat{\boldsymbol{\theta}}) - \int_{[0,1]^g} \Psi(\boldsymbol{x}) d\boldsymbol{x} \right| \ll \frac{1}{N}.$$

The Vinogradov function $\Psi(\boldsymbol{\theta})$ takes value 1 on R_1, value 0 on R_0, and value $0 \leq \Psi(\boldsymbol{\theta}) \leq 1$ everywhere else. Therefore, if $\mathbb{F}_{p^n}$ is an extension in $\mathrm{ExtSetTr}_{A,N,I}$, then $\Psi(n\hat{\boldsymbol{\theta}}) \leq 1$, and if $\mathbb{F}_{p^n}$ is not in $\mathrm{ExtSetTr}_{A,N,I}$, then $\Psi(n\hat{\boldsymbol{\theta}}) = 0$. Thus $\frac{1}{N}\sum_{n=1}^{N} \Psi(n\hat{\boldsymbol{\theta}}) \leq \mathrm{PropTr}_{A,N,I}$. As already seen, $\int_{R_1} \Psi(\boldsymbol{x}) d\boldsymbol{x} \leq \int_{[0,1]^g} \Psi(\boldsymbol{x}) d\boldsymbol{x}$, and thus the result follows. □

Example 6.1.3. Let A be an abelian surface over $\mathbb{F}_7$ with characteristic polynomial

$$f_1(T) = T^4 - 2T^3 + T^2 - 14T + 49.$$

Then A has an angle rank of 2 as verified by the LMFDB in [33, Abelian Variety 2.7.ac_b]. Let $\Delta = 0.001$ be given, and let $I = [0, 2]$ be the target interval in $[-4, 4]$ for the normalized traces $\{\overline{a}_n\}$. We numerically compute $\int_{R_1} \Psi(\boldsymbol{x}) \approx 0.313$ (see Note 6.1.4), so that

$$\mathrm{PropTr}_{A,N,I} \geq 0.313 - O\left(\frac{1}{N}\right).$$

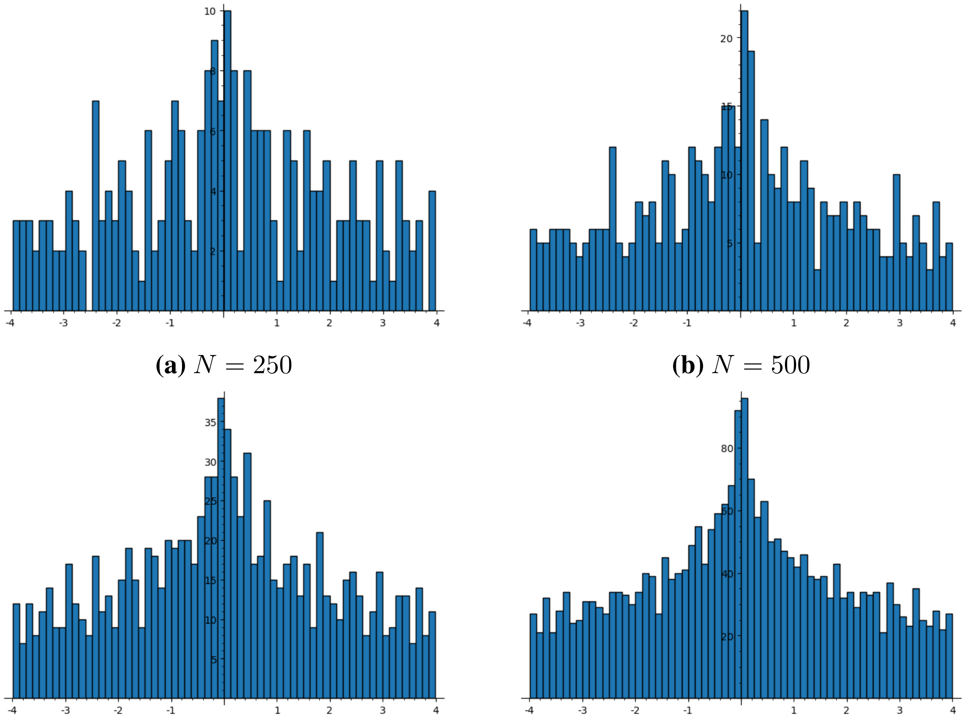
Empirical data for this abelian surface can be found in Table 6.1, and histograms in Figure 6.1.

Note 6.1.4. The numerical calculation of $\int_{R_1} \Psi(\boldsymbol{x})d\boldsymbol{x}$ in the above example was found by the following python script.

```python
from scipy import cos
from scipy import sin
from scipy import pi
from scipy.integrate import dblquad

a = 0
b = 2
delta = .001

def Ind(x, y):
    val = 2*cos(2*pi*x) + 2*cos(2*pi*y)
    if (val > (a+2*delta)) and (val < (b - 2*delta)):
        return 1
    else:
        return 0

predicted_prop = dblquad(Ind, 0, 1, lambda x: 0, lambda x: 1)[0]
print(f"The predicted lower bound = {predicted_prop}")
```

Table 6.1: Counts and proportions of normalized traces that land in $I = [0, 2]$ up to extensions of degree N for the abelian surface with LMFDB label 2.7.ac_b.

N	# $\mathrm{ExtSetTr}_{A,N,I}$	$\mathrm{PropTr}_{A,N,I}$
50	12	0.24
100	28	0.28
500	163	0.326
1000	313	0.313
2500	793	0.3172



(a) $N = 250$

(b) $N = 500$

(c) $N = 1000$

(d) $N = 2500$

Figure 6.1: Histograms of the normalized traces for extension degrees $N = 250, 500, 1000, 2500$ for the abelian surface with LMFDB label 2.7.ac_b.

6.2 Sizes of Isogeny Classes of Abelian Varieties

Given an isogeny class, $\mathcal{C}$, of abelian varieties, we further refine the isogeny class into strata. A stratum of an isogeny class is a subset of the isogeny class of all the abelian varieties sharing the same endomorphism ring. This section examines estimates for sizes of a certain stratum for abelian surfaces.

In [34], Howe gives a result for the size of the minimal stratum of an isogeny class. We first begin with some notation. Let $\{a_n\}$ and $\{b_n\}$ be real-valued sequences. The notation $a_n \approx b_n$ means that, for every $\epsilon > 0$, there are positive constants r, s such that $b_n \leq r a_n^{1+\epsilon}$ and $a_n \leq s b_n^{1+\epsilon}$ for all n. If $\{a_n\}$ and $\{b_n\}$ both tend to infinity, then $a_n \approx b_n$ if and only if $(\log(a_n)/\log(b_n)) \to 1$.

Consider an isogeny class of simple abelian surfaces with Frobenius polynomial $f(T)$. Let K be the field $\mathbb{Q}[T]/f(T)$, and let K^+ be the maximal real subfield of K. For an order $R \subset K$, let $R^+ = R \cap K^+$. We first need the notion of the Picard group and the narrow Picard group.

Definition 6.2.1. The Picard group, $\operatorname{Pic} R$, is the group of isomorphism classes of invertible R-ideals.

Definition 6.2.2. Two R^+ ideals, $\mathfrak{A}, \mathfrak{B}$ are said to be strictly isomorphic if there is a totally positive $x \in K^+$ such $x\mathfrak{A} = \mathfrak{B}$. The narrow Picard group $\operatorname{Pic}^+ R^+$ of the real order R^+ is the group of strict isomorphism classes of invertible R^+-ideals.

The usual norm map of invertible ideals for K over K^+ induces a homomorphism from $\operatorname{Pic} R$ to $\operatorname{Pic}^+ R^+$, which we call the norm $\mathrm{N}_{\mathrm{Pic}} : \operatorname{Pic} R \to \operatorname{Pic}^+ R^+$.

Let α be a root of the characteristic polynomial of Frobenius for the isogeny class $\mathcal{C}$. We say that $R = \mathbb{Z}[\alpha, \overline{\alpha}]$ is the minimal ring for the isogeny class $\mathcal{C}$. This name is justified, as all abelian varieties in $\mathcal{C}$ have an a Frobenius endomorphism F and a Verschiebung endomorphism V. Then $\mathbb{Z}[\alpha, \overline{\alpha}]$ is isomorphic to $\mathbb{Z}[F, V]$, and therefore the endormorphism ring of every abelian variety in $\mathcal{C}$ contains $\mathbb{Z}[\alpha, \overline{\alpha}]$. The stratum of abelian varieties that have R for an endomorphism ring is called the minimal stratum of $\mathcal{C}$. We now consider a theorem of Howe's that estimates the size of the minimal stratum of an isogeny class.

Theorem 6.2.3. *[34, Thm. 1.3] Let $\{q_n\}$ be a sequence of prime powers. For each positive integer n, let $\mathcal{C}_n$ be an isogeny class of simple g-dimensional ordinary abelian varieties over $\mathbb{F}_{q_n}$. Let R_n be the minimal endomorphism ring, and let $\mathcal{S}_n$ be the associated minimal stratum. Let $\{\theta_{n,i}\}_{i=1}^{g}$ be the Frobenius angles for C_n. Define P_n as the number of principally polarized varieties in S_n. If $q_n \to \infty$ and if each norm map $\operatorname{Pic} R_n \to \operatorname{Pic}^+ R_n^+$ is surjective, then*

$$P_n \approxeq q_n^{g(g+1)/4} \left| \prod_{i<j} (\cos(\theta_i) - \cos(\theta_j)) \prod \sin(\theta_i) \right| \tag{6.1}$$

We specialize to the case of abelian surfaces, $g = 2$, and in this case (6.1) becomes

$$P_n \approxeq q_n^{3/2} \left| \sin(\theta_1) \sin(\theta_2)(\cos(\theta_1) - \cos(\theta_2)) \right|. \tag{6.2}$$

Additionally, we work in the case of extensions of $\mathbb{F}_p$, so that $\mathbb{F}_{q_n}$ is the extension $\mathbb{F}_{p^n}$.

A criterion for the surjectivity of the norm map $\operatorname{Pic} R_n \to \operatorname{Pic}^+ R_n^+$ is given by the following lemma.

Lemma 6.2.4. *[34, Cor. 4.4] If K/K^+ is ramified at a finite prime that does not divide the conductor of R^+, then the norm map $\operatorname{Pic} R \to \operatorname{Pic}^+ R^+$ is surjective.*

Recall that for quadratic fields, the conductor of an order can be identified with its index in the ring of integers. We recall a few facts for the quadratic extension K^+. Let $\mathcal{O}_{K^+}$ be the maximal order (i.e. the ring of integers) of K^+.

Definition 6.2.5. Given an order $\mathcal{O}$ in a quadratic field K^+, the index $\mathfrak{f} = [\mathcal{O}_{K^+} : \mathcal{O}]$ is the conductor of $\mathcal{O}$.

We will use another method to calculate the conductor based on the discriminant of $\mathcal{O}$.

Definition 6.2.6. Let $\mathcal{O} = \mathbb{Z}[\alpha, \beta]$ and let $\alpha \mapsto \alpha'$ be the nontrivial automorphism of K^+. The discriminant D of $\mathcal{O}$ is the number

$$D = \left[\det \left(\begin{bmatrix} \alpha & \beta \\ \alpha' & \beta' \end{bmatrix} \right) \right]^2$$

Lemma 6.2.7. *Let $\mathcal{O}$ be an order with discriminant D and conductor $\mathfrak{f}$. Let d_{K^+} be the discriminant of K^+. We have the formula*

$$D = \mathfrak{f}^2 d_{K^+}.$$

For more on orders in quadratic extensions see [35, ch. 7].

Extensions $\mathbb{F}_{p^n}$ with surjective norm map

Given this set up, we aim to take an isogeny class $\mathcal{C}$ over $\mathbb{F}_p$, and give a lower bound on how often the minimal stratum achieves a certain size over extensions $\mathbb{F}_{p^n}$ by estimating the trigonometric factors of (6.2). However, the hypothesis on the sujectivity of the norm map $\operatorname{Pic} R_n \to \operatorname{Pic}^+ R_n^+$ is not always satisfied for every extension of $\mathbb{F}_p$. A finite check will be sufficient to identify which extensions satisfy this constraint, which we now demonstrate.

Consider an isogeny class $\mathcal{C}$ of abelian surfaces with characteristic polynomial $f(T)$ over $\mathbb{F}_p$. Compute the relative discriminant of K/K^+ to find a prime, $\mathfrak{r} \in K^+$ that ramifies in K. In view of Lemma 6.2.4, we would like to find conditions on those n for which $\mathfrak{r}$ divides the conductor of R_n^+.

The characteristic polynomial associated to $\mathcal{C}$ over $\mathbb{F}_{p^n}$ has the form

$$\begin{aligned} f_n &= T^4 - a_n T^3 + b_n T^2 - a_n p^n T + p^{2n} \\ &= (T - \alpha^n)(T - \overline{\alpha}^n)(T - \beta^n)(T - \overline{\beta}^n) \end{aligned}$$

so that $a_n = \alpha^n + \overline{\alpha}^n + \beta^n + \overline{\beta}^n$. Then the real subfield of K is $K_n^+ = \mathbb{Q}[T]/f_n^+(T)$ where

$$\begin{aligned} f_n^+(T) &= T^2 - a_nT + b_n - 2p^n \\ &= \big(T - (\alpha^n + \overline{\alpha}^n)\big)\big(T - (\beta^n + \overline{\beta}^n))\big). \end{aligned}$$

In fact, K_n^+ is independent of n, therefore we drop the subscript and just write K^+. The discriminant of the order $\mathcal{O}_n \subset R_n^+$ is then $D_n = (\alpha^n + \overline{\alpha}^n - (\beta^n + \overline{\beta}^n))^2$. Therefore, using the formula $D_n = \mathfrak{f}_n^2 d_{k^+}$ from Lemma 6.2.7 we have

$$(\alpha^n + \overline{\alpha}^n - (\beta^n + \overline{\beta}^n))^2 = \mathfrak{f}_n^2 d_{K^+}.$$

Then $\mathfrak{r}$ divides the conductor if

$$(1/d_{K^+})(\alpha^n + \overline{\alpha}^n - (\beta^n + \overline{\beta}^n))^2 \equiv 0 \pmod{\mathfrak{r}}. \tag{6.3}$$

Using this, we now characterize extensions for which $\mathfrak{r}$ divides $\mathfrak{f}_n$.

Because $\alpha^n \in K$ and $\mathcal{O}_K/(\mathfrak{r})$ is a finite field, the values of $\alpha^n, \beta^n, \overline{\alpha}^n, \overline{\beta}^n$ are cyclic in n when taken mod $\mathfrak{r}$. Let M be the least common multiple of the orders of $\alpha, \beta \pmod{\mathfrak{r}}$. There is a finite list of values for $\alpha^n + \overline{\alpha}^n - (\beta^n + \overline{\beta}^n) \pmod{\mathfrak{r}}$, which are found in $1 \leq n \leq M$.

Let $B = \{m_1, \ldots, m_w\}$ be the list of integers up to M such that

$$\alpha^{m_j} + \overline{\alpha}^{m_j} - (\beta^{m_j} + \overline{\beta}^{m_j}) \equiv 0 \pmod{\mathfrak{r}}.$$

Recall that $\mathfrak{f}_n = [\mathcal{O}_{K^+} : R_n^+]$. Given that $R_{km}^+ \subset R_m^+$, we have that $\mathfrak{f}_m | \mathfrak{f}_{km}$. Therefore if

$$\alpha^l + \overline{\alpha}^l - (\beta^l + \overline{\beta}^l) \equiv 0 \pmod{\mathfrak{r}}.$$

then $l \equiv m$ for some $m \in B$. We have that B is a subgroup of $\mathbb{Z}/M\mathbb{Z}$, and we define B^{min} to be the set of minimal generators of B.

In the sequel, we will need extensions where $\mathfrak{r}$ does not divide the conductor, which leads to the following condition.

Condition 6.2.8. If B is a proper subgroup of $\mathbb{Z}/M\mathbb{Z}$, we say the isogeny class $\mathcal{C}$ meets the *existence of surjective norm maps condition.* Note that if $B = \mathbb{Z}/M\mathbb{Z}$, then $\mathfrak{r}$ divides the conductor $\mathfrak{f}_n$ at every extension of $\mathbb{F}_p$.

Lemma 6.2.9. *Let $\mathcal{C}$ be the minimal strata of an isogeny class of abelian surfaces over $\mathbb{F}_p$ and let $\overline{n}$ be the reduction $n \pmod M$. If $\overline{n} \notin B$, then the number of principally polarized abelian varieties in the minimal stratum $\mathcal{S}_n$ over $\mathbb{F}_{p^n}$ is*

$$P_n \approxeq q_n^{3/2} \left|\sin(\theta_1)\sin(\theta_2)(\cos(\theta_1) - \cos(\theta_2))\right|.$$

Proof. By the definition of B, we have that $\mathfrak{r}$ does not divide $\mathfrak{f}_n$. by Lemma 6.2.4, the norm map $\mathrm{N}_{\mathsf{Pic}} : \operatorname{Pic} R_n \to \operatorname{Pic}^+ R_n^+$ is surjective, and thus the estimate of (6.2) from Theorem 6.2.3 holds. $\square$

We therefore enforce Condition 6.2.8 so that there are extensions where the estimate of (6.2) does in fact hold.

6.2.1 Modified quasi-Monte Carlo

In light of Lemma 6.2.9, we need to remove certain subsequences of $\{n\hat{\boldsymbol{\theta}}\}$ where the estimate of (6.2) may not hold. The number of terms we must remove is roughly given by

$$N^* \approx \frac{|B|}{M} N.$$

and the subsequences we must remove are of the form $\{mn\hat{\boldsymbol{\theta}}\}$ for $m \in B^{\text{min}}$.

Proposition 6.2.10. *Let $\boldsymbol{\theta} \in \mathbb{R}^g$ be a point of finite type η. Then the sum over $f(n\theta)$ for $\overline{n} \notin B$ converges to $\int f(\boldsymbol{x})d\boldsymbol{x}$ at the rate $O(1/(N))$, that is,*

$$\frac{1}{N-N^*}\sum_{\substack{1\leq n\leq N\\ \overline{n}\notin B}}^{N} f(n\boldsymbol{\theta}) - \int_{[0,1]^g} f(\boldsymbol{x})d\boldsymbol{x} = O\left(\frac{1}{N}\right).$$

Proof. We have from Theorem 3.3.5

$$\sum_{n=1}^{N} f(n\boldsymbol{\theta}) = N\int_{[0,1]^g} f(\boldsymbol{x})d\boldsymbol{x} + O\left(1\right). \tag{6.4}$$

We can break the sum up as

$$\sum_{n=1}^{N} f(n\boldsymbol{\theta}) = \sum_{\substack{1\leq n\leq N\\ \overline{n}\notin B}}^{N} f(n\boldsymbol{\theta}) + \sum_{\substack{1\leq n\leq N\\ \overline{n}\in B}}^{N} f(n\boldsymbol{\theta}). \tag{6.5}$$

Note that

$$\sum_{\substack{1\leq n\leq N\\ \overline{n}\notin B}}^{N} f(n\boldsymbol{\theta})$$

has N^* terms. Let $m \in B^{\text{min}}$. From Lemma 4.3.4, we have that $\boldsymbol{\vartheta} = m_j\boldsymbol{\theta}$ is an irrational g-tuple of finite type. Therefore from Theorem 3.3.5 we have

$$\sum_{n=1}^{\lfloor N/m_j\rfloor} f(n\boldsymbol{\vartheta}) = \left\lfloor\frac{N}{m_j}\right\rfloor\int_{[0,1]^g} f(\boldsymbol{x})d\boldsymbol{x} + O\left(1\right).$$

Then accounting for inclusion-exclusion of multiples in B^{min}, we have

$$\sum_{\substack{1\leq n\leq N\\ \overline{n}\in B}}^{N} f(n\boldsymbol{\theta}) = N^*\int_{[0,1]^g} f(\boldsymbol{x})d\boldsymbol{x} + O\left(1\right).$$

Combining this with equations 6.4 and 6.5 gives

$$\sum_{\substack{1\leq n\leq N \\ n\equiv 0 \bmod m}}^{N} f(n\boldsymbol{\theta}) = (N-N^*)\int_{[0,1]^g} f(\boldsymbol{x})d\boldsymbol{x} + O\left(1\right).$$

Note that $O(1/(N-N^*) = O(1/N)$, which finishes the result. □

6.2.2 Sizes of minimal strata over extensions $\mathbb{F}_{p^n}$

Given the hypotheses of Theorem 6.1, the size of the minimal stratum $\mathcal{S}$ of $\mathcal{C}$ over $\mathbb{F}_{p^n}$ satisfies

$$P_n \approxeq p^{3n/2}\left|\sin(n\theta_1)\sin(n\theta_2)(\cos(n\theta_1)-\cos(n\theta_2))\right|.$$

Suppose we are interested in quantifying how often the minimal stratum is at least a certain size. That is, let $\epsilon > 0$, and consider the number of extensions for which the size of the stratum P_n satisfies

$$\frac{P_n}{p^{3n/2}} > \epsilon.$$

Because of the relatively weak relation implied by $\approxeq$, we restrict to estimating the trigonometric factor of P_n,

$$\text{PTrig}_n = \left|\sin(n\theta_1)\sin(n\theta_2)(\cos(n\theta_1)-\cos(n\theta_2))\right|.$$

Let $\mathcal{C}$ be the minimal stratum of an isogeny class, and assume that Condition 6.2.8, so that there are extensions where the estimate of (6.1) hods. Define the quantity

$$\text{ExtSetStrata}_{\mathcal{C},N,\epsilon} = \{n \leq N : \text{PTrig}_n > \epsilon\}$$

as the set of degrees of extensions where PTrig_n is larger than ϵ. Then define

$$\mathrm{PropMinStrata}_{\mathcal{C},N,\epsilon} = \frac{\#\,\mathrm{ExtSetStrata}_{\mathcal{C},N,\epsilon}}{N}$$

as the proportion of extensions where $\mathrm{PTrig}_n > \epsilon$.

Given $\epsilon > 0$, we have the target interval $I = (\epsilon, 1]$. Let $\alpha = \epsilon + \Delta$ and $\beta = 1 + \Delta$. Then we have the regions

$$\begin{aligned} R_1 &= T^{-1}\Big(\epsilon + 2\Delta, 1\Big) \cap [0,1]^2 \\ R_0 &= T^{-1}\Big(\mathbb{R} \setminus (\epsilon, 1 + 2\Delta)\Big) \cap [0,1]^2. \end{aligned}$$

We require the following lemma before constructing a Vinogradov function.

Lemma 6.2.11. *Let $\epsilon > 0$ be given and let I be the interval $I = (\alpha, \beta)$ as above. Let T be the function*

$$\begin{tikzcd} T : \mathbb{R}^2 \arrow[r] & \mathbb{R} & . \\ (\theta_1, \theta_2) \arrow[r, mapsto] & \lvert \sin(2\pi x)\sin(2\pi y)(\cos(2\pi x) - \cos(2\pi y))\rvert \end{tikzcd}$$

Then T and I meet admit a Vinogradov function by Definition 3.5.1 and Theorem 3.5.4. That is, it is:

1. *T is periodic of period 1.*

2. *There exists a positive $K \in \mathbb{R}$ such that T satisfies the inequality*

$$|T(\boldsymbol{\theta} + \boldsymbol{z}) - T(\boldsymbol{\theta})| \leq K|z|.$$

3. *There exists an integer* $C > 0$ *such that the set*

$$T^{-1}((\alpha, \beta)) \cap X_j(\lambda)$$

is a union of at most C *intervals for any* $\lambda \in [0, 1]$.

Proof. The first condition holds, because $\sin(2\pi x)$ and $\cos(2\pi x)$ are periodic of period 1. For the second condition, note that

$$\widetilde{T} = \sin(2\pi x)\sin(2\pi y)(\cos(2\pi x) - \cos(2\pi y))$$

satisfies the condition for some K, by the multivariate mean value theorem. But then

$$|T(\boldsymbol{\theta} + \boldsymbol{z}) - T(\boldsymbol{\theta})| \leq |\widetilde{T}(\boldsymbol{\theta} + \boldsymbol{z}) - \widetilde{T}(\boldsymbol{\theta})| \leq K|z|$$

because T is always positive, and therefore condition 2 holds for T.

Fix $\lambda \in [0, 1]$. Given $I = (\alpha, \beta)$ we must show that the set

$$T^{-1}((\alpha, \beta)) \cap X_j(\lambda)$$

is a union of at most C intervals. We first consider the function,

$$S_\lambda(\theta) = \sin(2\pi\theta)\sin(2\pi\lambda)(\cos(2\pi\theta) - \cos(2\pi\lambda))$$

First, assume that $\lambda \neq 0$, and therefore S_λ is not a constant function. Then the derivative of $S_\lambda(\theta)$ has 4 critical points, and thus $S_\lambda(\theta)$ changes from increasing to decreasing at most 4 times. Therefore $S_\lambda(\theta)$ intersects the line $y = \gamma$ at most 4 times. But then $T(\theta, \lambda)$ intersects $y = \gamma$ at most 8 times, and therefore $C = 8$ is sufficient.

Now suppose $\lambda = 0$. then S is the constant function $S = 0$. However, $0 \notin (\alpha, \beta)$, and therefore

$T^{-1}(0) \cap T^{-1}((\alpha, \beta)) = \emptyset$.

□

We now quantify $\mathrm{PropMinStrata}_{\mathcal{C},N,\epsilon}$.

Theorem 6.2.12. *Let $\mathcal{C}$ be an isogeny class of abelian surfaces of maximal angle rank over $\mathbb{F}_p$, and let $\epsilon > 0$ be given. Assume that Condition 6.2.8 is met. Then the quantity* $\mathrm{PropMinStrata}_{C,N,\epsilon}$ *satisfies*

$$\mathrm{PropMinStrata}_{C,N,\epsilon} \geq \int_{R_1} \Psi(\boldsymbol{x}) d\boldsymbol{x} - O(1/(N)).$$

Proof. Condition 6.2.8 implies that there are extensions where the estimate of (6.1) holds. Because $\mathcal{C}$ has maximal angle rank, the Frobenius tuple $\hat{\boldsymbol{\theta}}$ has finite type, and thus we aim to construct a Vinogradov function and use the modified quasi-Monte Carlo integration method in Proposition 6.2.10.

Let $\alpha = \epsilon + \Delta, \beta = 1 + \Delta$ and define the interval $I = (\alpha, \beta)$. Define T to be

$$\begin{tikzcd} T : \mathbb{R}^2 \arrow[rr] & & \mathbb{R} & . \\ (\theta_1, \theta_2) \arrow[r, mapsto] & \lvert \sin(2\pi x)\sin(2\pi y)(\cos(2\pi x) - \cos(2\pi y)) \rvert \end{tikzcd}$$

Then T and I admit construction of a Vinogradov function by Lemma 6.2.11. We have the regions

$$\begin{aligned} R_1 &= T^{-1}\Big(\epsilon + 2\Delta, 1\Big) \cap [0,1]^2 \\ R_0 &= T^{-1}\Big(\mathbb{R} \setminus (\epsilon, 1 + 2\Delta)\Big) \cap [0,1]^2 \end{aligned}$$

where the Vinogradov function Ψ takes values 1 on R_1 and value 0 on R_0. Then the sum $\sum \Psi(n\hat{\boldsymbol{\theta}})$ is an underestimate of $\#\, \mathrm{ExtSetStrata}_{\mathcal{C},N,\epsilon}$, so that

$$\mathrm{PropMinStrata}_{\mathcal{C},N,\epsilon} \geq \frac{1}{N} \sum_{n=1}^{N} \Psi(n\hat{\boldsymbol{\theta}}).$$

Finally, we have the in equality

$$\int_{R_1} \Psi(\boldsymbol{x}) d\boldsymbol{x} \leq \int_{[0,1)^2} \Psi(\boldsymbol{x}) d\boldsymbol{x}$$

which concludes the proof. □

Example 6.2.13. Let $\mathcal{C}$ be the isogeny class of abelian surfaces over $\mathbb{F}_7$ with characteristic polynomial

$$f_1(T) = T^4 - 2T^3 + 5T^2 - 14T + 49.$$

The LMFDB numerically verifies that this class has maximal angle rank, [33, Abelian Variety 2.7.ac_f].

Let α be a root of f_1, so that $K = \mathbb{Z}[\alpha, \overline{\alpha}]$ and $K^+ = \mathbb{Z}[\alpha + \overline{\alpha}]$. One can compute that K has absolute discriminant $2^6 \cdot 3 \cdot 5^2 \cdot 83$ and K^+ has discriminant $2^3 \cdot 5$. Therefore a prime, $\mathfrak{r}$, above 3 ramifies in K/K^+. By computer calculation, $\alpha^n \pmod 3$ is periodic of period 12. Again by computer calculation, we see that the conductor fails to be coprime to 3 at extensions of degree $\{4j\}_{j=1}^{\infty}$, and thus the norm map $\operatorname{Pic} R \to \operatorname{Pic}^+ R^+$ is possibly not surjective at the extensions $\{\mathbb{F}_{p^{4j}}\}_{j=1}^{\infty}$.

The hypotheses of Theorem 6.2.12 hold. Given $\epsilon > 0$, we have that

$$\mathrm{PropMinStrata}_{C,N,\epsilon} \geq \int_{R_1} \Psi(\boldsymbol{x}) d\boldsymbol{x} - O(1/(N)).$$

Let $\epsilon = 0.2$, then $\int_{R_1} \Psi(\boldsymbol{x}) d\boldsymbol{x} \approx 0.51$, so that

$$\mathrm{PropMinStrata}_{C,N,\epsilon} \geq 0.51 - O(1/(N)).$$

In the above, the estimation of the integral was done by the following python script.

```python
from scipy import cos
from scipy import sin
from scipy import pi
from scipy.integrate import dblquad

epsilon = .2
Delta = .001

def Ind(x, y):
    val = abs((cos(2*pi*x) - cos(2*pi*y))*sin(2*pi*x)*sin(2*pi*y))
    if (val > epsilon + Delta):
        return 1
    else:
        return 0

print(dblquad(Ind, 0, 1, lambda x: 0, lambda x: 1)[0])
```

Bibliography

[1] Alina Bucur, Francesc Fité, and Kiran S Kedlaya. Effective sato-tate conjecture for abelian varieties and applications. *arXiv preprint arXiv:2002.08807*, 2020.

[2] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 9.0)*, 2022. `https://www.sagemath.org`.

[3] John Tate. Classes d'isogénie des variétés abéliennes sur un corps fini (d'après t. honda). In *Séminaire Bourbaki vol. 1968/69 Exposés 347-363*, pages 95–110. Springer, 1971.

[4] William C Waterhouse. Abelian varieties over finite fields. In *Annales scientifiques de l'École Normale Supérieure*, volume 2, pages 521–560, 1969.

[5] Joseph H Silverman. *The arithmetic of elliptic curves*, volume 106. Springer Science & Business Media, 2009.

[6] James S Milne. Abelian varieties. *Arithmetic geometry*, pages 103–150, 1986.

[7] John Tate. Endomorphisms of abelian varieties over finite fields. *Inventiones mathematicae*, 2(2):134–144, 1966.

[8] René Schoof. Nonsingular plane cubic curves over finite fields. *J. Comb. Theory, Ser. A*, 46(2):183–211, 1987.

[9] Nicholas Katz. Lang-trotter revisited. *Bulletin of the American Mathematical Society*, 46(3):413–457, 2009.

[10] Lauwerens Kuipers and Harald Niederreiter. *Uniform distribution of sequences*. Courier Corporation, 2012.

[11] Jeffrey D Vaaler. Some extremal functions in fourier analysis. *Bulletin (New Series) of The American Mathematical Society*, 12(2):183–216, 1985.

[12] Christoph Aistleitner and Josef Dick. Functions of bounded variation, signed measures, and a general koksma-hlawka inequality. *arXiv preprint arXiv:1406.0230*, 2014.

[13] Michael Drmota and Robert F Tichy. *Sequences, discrepancies and applications*. Springer, 2006.

[14] József Beck. Probabilistic diophantine approximation, i. kronecker sequences. *Annals of Mathematics*, 140(2):449–502, 1994.

[15] Josef Dick, Aicke Hinrichs, and Friedrich Pillichshammer. Proof techniques in quasi-monte carlo theory. *Journal of Complexity*, 31(3):327–371, 2015.

[16] Wolfgang M Schmidt. Simultaneous approximation to algebraic numbers by rationals. *Acta Mathematica*, 125:189–201, 1970.

[17] A Baker. On some diophantine inequalities involving the exponential function. *Canadian Journal of Mathematics*, 17:616–626, 1965.

[18] Yann Bugeaud. *Distribution modulo one and Diophantine approximation*, volume 193. Cambridge University Press, 2012.

[19] Harald Niederreiter. Methods for estimating discrepancy. In *Applications of number theory to numerical analysis*, pages 203–236. Elsevier, 1972.

[20] SC Zaremba. Some applications of multidimensional integration by parts. In *Annales Polonici Mathematici*, volume 1, pages 85–96, 1968.

[21] Harald Niederreiter. Quasi-monte carlo methods and pseudo-random numbers. *Bulletin of the American mathematical society*, 84(6):957–1041, 1978.

[22] Harald Niederreiter. Application of diophantine approximations to numerical integration. *Diophantine approximation and its applications*, pages 129–199, 1973.

[23] Harald Niederreiter. On a number-theoretical integration method. *aequationes mathematicae*, 8(3):304–311, 1972.

[24] CB Haselgrove. A method for numerical integration. *Mathematics of computation*, pages 323–337, 1961.

[25] G Wüstholz. One century of logarithmic forms. *A Panorama in Number Theory or The View from Baker's Garden*, page 1, 2002.

[26] Alan Baker. *Transcendental number theory*. Cambridge university press, 1990.

[27] Michel Waldschmidt. *Diophantine approximation on linear algebraic groups: transcendence properties of the exponential function in several variables*, volume 326. Springer Science & Business Media, 2013.

[28] IM Vinogradov. Method of trigonometrical sums in the theory of numbers (dover books on mathematics).

[29] Andrew V Sutherland. Sato-tate distributions. *arXiv preprint arXiv:1604.01256*, 2016.

[30] Irina Shevtsova. On the absolute constants in the berry-esseen type inequalities for identically distributed summands. *arXiv preprint arXiv:1111.6554*, 2011.

[31] Taylor Dupuy, Kiran S Kedlaya, and David Zureick-Brown. Angle ranks of abelian varieties. *arXiv preprint arXiv:2112.02455*, 2021.

[32] Taylor Dupuy, Kiran Kedlaya, David Roe, and Christelle Vincent. Isogeny classes of abelian varieties over finite fields in the lmfdb, 2020.

[33] The LMFDB Collaboration. The L-functions and modular forms database. http://www.lmfdb.org, 2022. [Online; accessed 1 July 2022].

[34] Everett W Howe. Variations in the distribution of principally polarized abelian varieties among isogeny classes. *arXiv preprint arXiv:2005.14365*, 2020.

[35] David A Cox. *Primes of the form x2+ ny2: Fermat, class field theory, and complex multiplication*, volume 34. John Wiley & Sons, 2011.