ABSTRACT

Title of dissertation: LANG-TROTTER QUESTIONS ON THE REDUCTIONS OF ABELIAN VARIETIES

Samuel Bloom
Doctor of Philosophy, 2018

Dissertation directed by: Professor Lawrence C. Washington
Department of Mathematics

Let A be a geometrically simple g-dimensional abelian variety over the rationals. This thesis investigates the behavior of the reductions A_p of A modulo its primes p of good reduction. Questions about these reductions are called "questions of Lang-Trotter type" after the 1976 memoir of S. Lang and H. Trotter. This thesis studies two aspects of the reductions A_p in particular: the "Frobenius fields," $\mathrm{End}\big(A_p\big)\otimes\mathbb{Q}$, when A_p is simple and ordinary, and the primality (or failure thereof) of the number of rational points, $\#A_p(\mathbb{F}_p)$. Our questions and conjectures generalize the study of the "fixed-field" Conjecture of Lang-Trotter and the Koblitz Conjecture on elliptic curves, and our work generalizes the work by previous authors to this higher-dimensional context: through sieve-theoretic arguments and the use of explicit error bounds for the Chebotarev Density Theorem, we produce various conditional and unconditional upper and lower bounds on the number of primes p at which A_p has a specified behavior.

LANG-TROTTER QUESTIONS ON THE REDUCTIONS OF ABELIAN VARIETIES

by

Samuel Bloom

Dissertation submitted to the Faculty of the Graduate School of the
University of Maryland, College Park in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
2018

Advisory Committee:
Professor Lawrence C. Washington, Chair/Advisor
Professor Patrick Brosnan
Professor Thomas J. Haines
Professor Niranjan Ramachandran
Professor William Gasarch, Dean's Representative

Preface

This thesis consists of the material from two papers prepared for publication, "The square sieve and a Lang-Trotter question for generic abelian varieties" and "Almost prime orders of the reductions of abelian varieties," combined in a logical order. The former has been accepted for publication in Journal of Number Theory, and the latter appears in the arXiV at https://arxiv.org/abs/1803.03698 .

Dedication

for my father,

who has always been there for me

Acknowledgments

There are many people without whom I would not have thrived during my time as a graduate student at the University of Maryland and written this thesis.

I would like to thank my classmates for sharing their time and interests with me, for their help making it through qualifying exams, and for their openness and support during our time together. I especially would like to thank my fellow algebra and number theory students for interesting discussions and an enjoyable student seminar. In particular, I'd like to thank Steve Balady for important conversations and for his mentorship through my time as an early graduate student, and Adam Lizzi for starting me on the road of studying higher-dimensional abelian varieties.

I would like to thank my professors at UMD and during my undergraduate studies at the University of Chicago, who have taught me so much. From the Univesity of Chicago, I'd especially like to thank Diane Herrmann, Benson Farb, Maryanthe Malliaris, and of course the late Paul Sally, Jr. I'll always be a member of Sally's Gang. From the University of Maryland, I'd especially like to thank Niranjan Ramachandran, Patrick Brosnan, Tom Haines, and Chris Laskowski. I would also like to thank Alina Cojocaru at the University of Illinois for helpful communications regarding her research, and Jeff Achter at Colorado State University, who got me started studying questions of Lang-Trotter type.

I have many thanks to give to my advisor, Larry Washington, who has helped me in so many ways. Your interest and encouragement has kept me engaged, and your deep mathematical knowledge has guided me as I explored my own little patch

of unknown territory. Thank you for everything you've done for me.

Lastly, I have so much gratitude and thanks to give to my family and friends, who have supported me with their love throughout my life. You have meant so much for me and done so much to help me thrive in every part of my life. Thank you.

Table of Contents

Preface ii

Dedication iii

Acknowledgements iv

List of Figures viii

List of Abbreviations ix

1 Introduction 1
- 1.1 What is this thesis about? (An introduction for non-experts) 1
- 1.2 Notations 4

2 Questions of Lang-Trotter Type: Introduction and Literature Review 6
- 2.1 Introduction 6
- 2.2 p-Rank. 9
- 2.3 Fixed-Trace. 11
- 2.4 Fixed-Field. 12
- 2.5 Geometrically Simple. 13
- 2.6 Primality of the number of points 14

3 Preliminaries 20
- 3.1 Explicit Chebotarev Density Theorems 20
- 3.2 Generalized Erdös-Kac Theorem 24
- 3.3 The Square Sieve 26
- 3.4 Simplified Greaves' Sieve 27
- 3.5 Galois Representations and Open Image Varieties 29
- 3.6 The Lang-Weil Bound 31
- 3.7 Bounds on the size of sets in GSp_{2g}. 32

4 Fixed-Field Question 34
4.1 Statement of Results . . . 35
4.2 Proof of Theorem 4.1.1 . . . 38
4.2.1 Under GRH. . . . 50
4.2.2 Under GRH + AHC. . . . 51
4.2.3 Under GRH + AHC + PCC. . . . 52
4.2.4 Unconditionally. . . . 53
4.3 Proof of Theorem 4.1.2 . . . 55
4.3.1 Under GRH. . . . 60
4.3.2 Under GRH + AHC. . . . 61
4.3.3 Under GRH + AHC + PCC. . . . 61
4.3.4 Unconditionally. . . . 62
4.4 Proof of Corollaries 4.1.4, 4.1.5, and 4.1.6 . . . 64

5 Almost-Prime Order Question 67
5.1 Statement of Results . . . 67
5.2 Preparations for the Proof of Main Results. . . . 69
5.2.1 Divisibility of $\#A_p(\mathbb{F}_p)$ . . . 70
5.2.2 Setting up the sieve . . . 72
5.2.3 Exploiting subgroups of GSp_{2g} . . . 73
5.2.4 Fitting together the prime-counting estimates . . . 76
5.2.5 Counting matrices . . . 77
5.2.6 Verifying the sieve hypothesis (3.12) . . . 81
5.3 Proof of Main Results. . . . 82
5.3.1 Ensuring (5.1) . . . 83
5.3.2 Ensuring (5.2) . . . 87
5.3.3 Determining the optimal constants. . . . 88
5.3.4 Proof of Theorem 5.1.3 . . . 89
5.3.5 Proof of Theorem 5.1.4 . . . 91
5.4 A Koblitz Conjecture for Higher Dimension and Experimental Evidence 93

6 Concluding Remarks and Further Directions 101

Bibliography 105

List of Figures

1.1 $\mathbb{R}$-valued points of elliptic curve 11.a3, given by $Y^2 + Y = X^3 - X^2$. . 2
1.2 $\mathbb{F}_{1009}$-valued points of elliptic curve $y^2 + y = x^3 - x^2/\mathbb{F}_{1009}$. 3

5.1 curve 971.a.971.1 with equation $Y^2 + Y = X^5 - 2X^3 + X$ 95
5.2 curve 1051.a.1051.a with equation $Y^2 + Y = X^5 - X^4 + X^2 - X$ . . . 96
5.3 curve 1205.a.1205.1 with equation $Y^2 + Y = X^5 + 2X^4 - X^2$ 97
5.4 curve 1385.a.1385.1, with equation $Y^2 + Y = X^5 + 3X^4 + 3X^3 - X$. 98
5.5 genus 3 curve C_3 99
5.6 Computations for the constants $\mathfrak{C}_g$. 99

List of Abbreviations

AHC	Artin Holomorphy Conjecture
CM	complex multiplication
geom.	geometric/geometrically
GRH	Generalized Riemann Hypothesis
IQF	imaginary quadratic number field
PCC	Pair Correlation Conjecture
PNT	Prime Number Theorem
PPAV	principally polarized abelian variety
RH	Riemann Hypothesis
RM	real multiplication

Chapter 1: Introduction

1.1 What is this thesis about? (An introduction for non-experts)

Abelian varieties are objects which are at the intersection of many related fields of mathematics: number theory, algebra, geometry, and complex analysis. In short, they are objects that are defined as the common solution (in a projective space) of a set of equations—in particular, this common solution set must not be a collection of disjoint pieces—that importantly also carry an addition law on their points. The simplest examples of abelian varieties are *elliptic curves,* which are one-dimensional. (An abelian variety has a positive-integer *dimension*, which agrees with the usual notion of the dimension of a complex manifold when the abelian variety can be considered as such.) As an example, Figure 1.1 shows the graph of the elliptic curve, defined over $\mathbb{Q}$ in the projective plane by the equation $Y^2 + Y = X^3 - X^2$, that is considered by many as the "first elliptic curve in nature."

The addition law can be summarized almost completely by this: three points P, Q, R on the elliptic curve add to zero if they are collinear, and zero is the "point at infinity" of the curve in projective space.

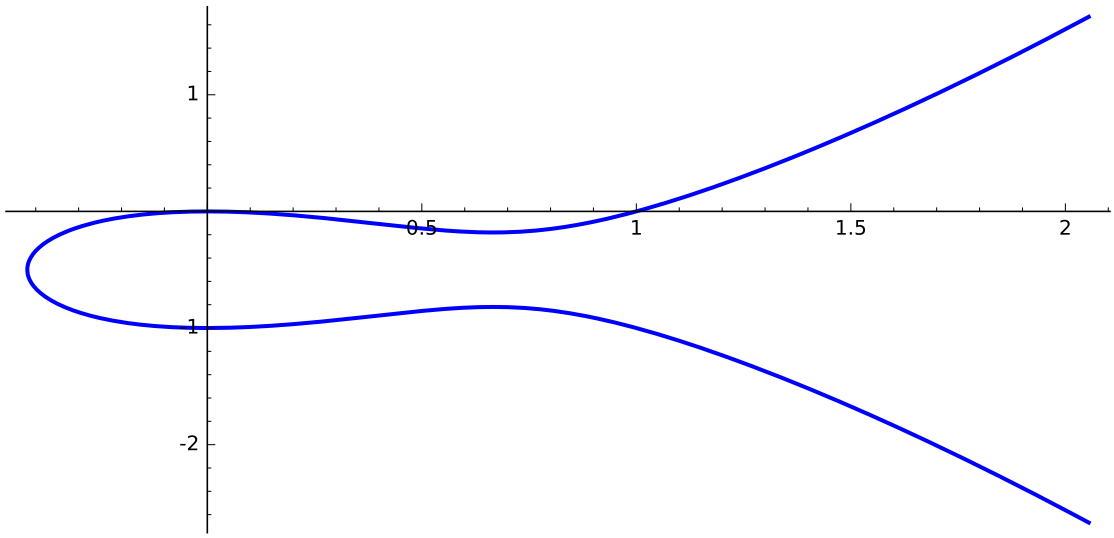

Figure 1.1: $\mathbb{R}$-valued points of elliptic curve 11.a3, given by $Y^2 + Y = X^3 - X^2$.

Abelian varieties can be defined over (that is, their defining equation(s) can have coefficients in) any field, and if two fields are related in some way, then it may be possible to "transfer" an abelian variety from one field to another by processes known as *base-change* and *reduction (or specialization) of the Néron model*. For instance, Figure 1.1 shows the graph of the "same" elliptic curve, but reduced modulo 1009 and considered over $\mathbb{F}_{1009}$ rather than $\mathbb{Q}$.

Thus, we can consider a fixed abelian variety $A/\mathbb{Q}$ to yield a family of abelian varieties A_p, over $\mathbb{F}_p$, as p varies through the prime numbers. (We have to exclude a finite number of *bad* primes at which A modulo p is not an abelian variety, but these primes are negligible for our considerations.) This thesis studies the following family of questions, then, stated broadly:

Question 1.1.1 (Questions of Lang-Trotter Type)**.** *Given an abelian variety $A/\mathbb{Q}$,*

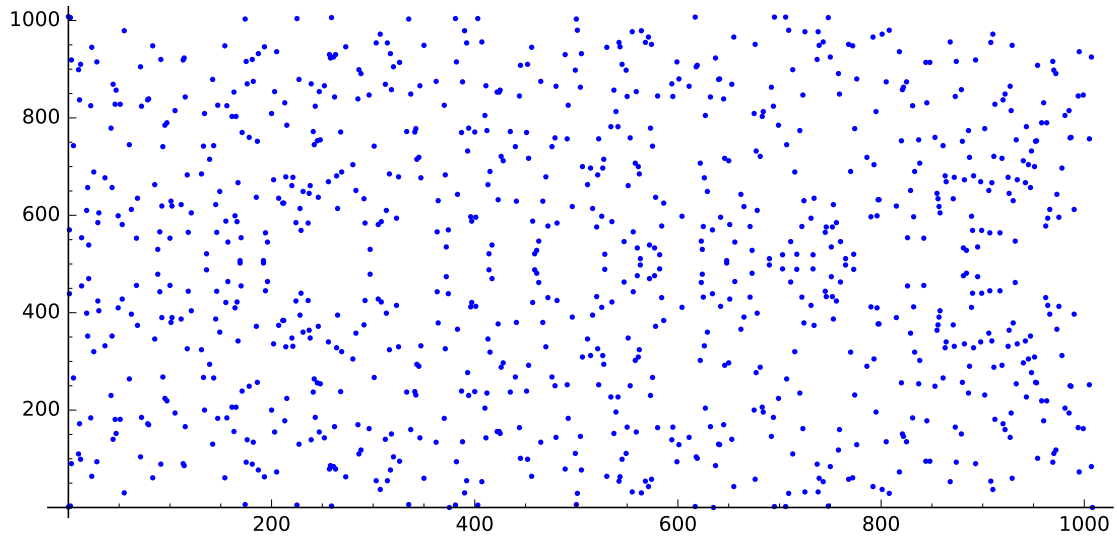

Figure 1.2: $\mathbb{F}_{1009}$-valued points of elliptic curve $y^2 + y = x^3 - x^2/\mathbb{F}_{1009}$.

how do the reductions of A modulo primes behave?

In particular, this thesis studies the following two questions, stated in vague terms to be made precise later:

Question 1.1.2 (Fixed-Field Question)**.** *Given an abelian variety $A/\mathbb{Q}$, what extra "self-similarities" (i.e.,* endomorphisms*) do the reductions A_p attain? In particular, how often does A_p have a specified field of self-similarities?*

Question 1.1.3 (Almost-Prime Orders Question)**.** *Given an abelian variety $A/\mathbb{Q}$, what patterns are there in how many $\mathbb{F}_p$-valued points the reductions A_p have? In particular, how often is the number of these points a prime number or a number with few prime factors?*

There are conjectural answers to these questions (when stated precisely), but to the author's knowledge, proving them is believed to be at least as hard as proving

the Twin Prime Conjecture. The methods currently in use only allow us to find upper and lower bounds on the desired counting functions (or weakened versions thereof).

The original work contained in this thesis is the generalization to the context of arbitrary-dimensional abelian varieties the arguments of other authors studying these questions for elliptic curves.

1.2 Notations

We use the standard Bachmann-Landau and Vinogradov notations for asymptotic growth of functions, which we now recall. A subscript $\star$ will denote that the implied constant depends *only* on the object(s) $\star$, so that if $\star$ is empty, then the implied constant is absolute. We write $X \gg_\star 0$ to mean "for all $X \geq N_\star$." Let $f, g : \mathbb{N} \to \mathbb{R}$. We write $g(X) = O_\star(f(X))$ or $g(X) \ll_\star f(X)$ to mean $\exists C_\star \geq 0$ such that for $X \gg_\star 0$, $\big|g(X)\big| \leq C_\star \big|f(X)\big|$. We write $g(X) = o(f(X))$ to mean $\lim_{X\to\infty} \frac{g(X)}{f(X)} = 0$, and we write $g(X) \sim f(X)$ to mean $\lim_{X\to\infty} \frac{g(X)}{f(X)} = 1$. We write $g(X) \asymp_\star f(X)$ to mean "$g(X) \ll_\star f(X)$ and $f(X) \ll_\star g(X)$."

For a finite set X, we will write $\#X$ for the cardinality. For integers n, we use the standard arithmetic notations,

Notation 1.2.1.

- $\omega(n) \coloneqq$ *the number of distinct prime factors of* n *counted* without *multiplicity;*
- $\Omega(n) \coloneqq$ *the number of distinct prime factors of* n *counted* with *multiplicity;*
- $P_r \coloneqq \{n \in \mathbb{Z}^+ \;\big|\; \Omega(n) \leq r\}$.

For a matrix m, denote by $\mathrm{char}_m(x)$ its characteristic polynomial.

We will use the letters l, p, q, and ℓ to denote rational prime numbers, $\mathfrak{p}$ to denote a prime ideal in a number field, and $\mathfrak{a}$ to denote an integral ideal in a number field. We will use N and Tr to denote "norm" and "trace", respectively, when the meaning is clear from context, and introduce subscripts and superscripts when the meaning is not clear. We will write $\left(\frac{\alpha}{a}\right)$ for the Jacobi (i.e., generalized quadratic residue) symbol of α modulo a. In a number field L, we will write n_L or $n(L)$ for the degree of the extension $L/\mathbb{Q}$, d_L or $d(L)$ for the discriminant of the extension $L/\mathbb{Q}$, and h_L for the class number.

For any set S of prime ideals of a number field (or rational prime numbers), we denote the prime-counting function

$$S(x) \coloneqq \#\left\{\mathfrak{p} \in S \;\middle|\; \mathrm{N}_{\mathbb{Q}}\,\mathfrak{p} \leq x\right\}.$$

We say that S has (natural) density δ if

$$\lim_{x\to\infty} \frac{S(x)}{\#\{\mathfrak{p} \;\middle|\; \mathrm{N}_{\mathbb{Q}}\,\mathfrak{p} \leq x\}} = \delta.$$

For a finite group G and a union of conjugacy classes $C \subseteq G$, we will write $\widetilde{C}$ for the number of conjugacy classes contained in C.

For an abelian variety over a field A/κ, we will always use $\mathrm{End}(A)$ to denote the ring of endomorphisms of A *defined over the base field* κ. For the sake of brevity, *we reserve* p *and* $\mathfrak{p}$ *for places of* κ *at which* A *has good reduction.*

Chapter 2: Questions of Lang-Trotter Type: Introduction and Literature Review

2.1 Introduction

Let $A/\mathbb{Q}$ be a principally polarized abelian variety. The questions that we study in this thesis emanate from the following conjectures on the behavior of the reductions of A modulo its primes p of good reduction.

Conjecture 2.1.1 (Lang-Trotter Conjectures)**.**

1. *Suppose that* $\mathrm{End}\left(E_{\overline{\mathbb{Q}}}\right) \cong \mathbb{Z}$*, or* $t \neq 0$*. Then there exists a constant* $C_{E,t} \geq 0$ *such that*

$$\#\left\{p \leq X \text{ of good reduction} \;\middle|\; \mathrm{Tr}(\pi_p) = t\right\} \sim C_{E,t}\frac{\sqrt{X}}{\log X},$$

   where $C_{E,t} = 0$ *is understood to mean that the set written above is finite.*

2. *Suppose that* $\mathrm{End}\left(E_{\overline{\mathbb{Q}}}\right) \cong \mathbb{Z}$*, and let* $K/\mathbb{Q}$ *be an imaginary quadratic number field. Then there exists a constant* $C_{E,K} > 0$ *such that*

$$\#\left\{p \leq X \text{ of good reduction} \;\middle|\; \mathrm{End}\left(E_p\right) \otimes \mathbb{Q} = \mathbb{Q}(\pi_p) \cong K\right\} \sim C_{E,K}\frac{\sqrt{X}}{\log X}.$$

Conjecture 2.1.2 (Koblitz [Kob88], Conjecture A)**.** *Suppose that every elliptic curve which is $\mathbb{Q}$-isogenous to E (including E itself) has trivial rational torsion. Then,*

$$\#\left\{p \leq x \text{ of good reduction} \;\middle|\; \#E_p\left(\mathbb{F}_p\right) \text{ is prime}\right\} \sim C_E \frac{x}{(\log x)^2}$$

where C_E is an explicit constant depending on the Galois representation of E.

The constants $C_{E,t}$, $C_{E,K}$, and C_E have precise descriptions in terms of the statistical heuristics used and the Chebotarev density theorem.

These conjectures fit within two broad families of questions of number-theoretic interest:

Question 2.1.3. *Given a "naturally-occurring" sequence $\mathcal{A}$ of integers (or tuples of integers), describe the subset Π of terms which have a specified multiplicative-arithmetic behavior.*

Question 2.1.4. *Let A be an abelian variety of dimension g over a global field L. Let $\clubsuit$ be a property of abelian varieties of dimension g over finite fields. Describe*

$$\Pi = \Pi(A, \clubsuit) \coloneqq \left\{\text{places } \mathfrak{p} : \mathcal{A}_{\mathfrak{p}} \text{ has } \clubsuit\right\},$$

where $\mathcal{A}$ is the Néron model of $\mathcal{A}$ over the appropriate one-dimensional scheme ($\operatorname{Spec} \mathcal{O}_L$*, resp. C, if L is a number field, resp. the function field of a curve $C/\mathbb{F}_q$).*

By "describe" we mean either to give a "qualitative" description of Π via congruence conditions, diophantine equations, and/or inequalities; or a "quantitative" description via an asymptotic estimate of the size of Π.

The family of Question 2.1.3 includes—among other questions—the Bateman-Horn Conjecture [BH62] which generalizes the Twin Prime Conjecture; the study of primes, pseudo-primes, and almost-primes in various intervals; and Artin's Conjecture on primitive roots modulo p (see, for instance, [Mor12]). For an elliptic curve $E/\mathbb{Q}$, the family of Question 2.1.4 includes—among other questions, and along with the Lang-Trotter Conjectures— the Sato-Tate Conjecture (see [Sut16] for an expository account) and the study of the structure of the group $E_p(\mathbb{F}_p)$ for a varying prime p (see, for instance, [Coj04]). The generalizations of some these questions to higher-dimensional abelian varieties and/or over non-trivial number fields appear more difficult than their counterparts for elliptic curves over $\mathbb{Q}$. After Achter-Howe [AH17], we call this second family family "**questions of Lang-Trotter type**."

In the remainder of this Chapter, we will provide a further introduction to questions in the family of Question 2.1.4, including the above Conjectures and their generalizations, and we will provide a literature review of the results in their direction. These literature reviews originated in the two articles written by the author, as mentioned in the Preface.

For the Sections following, we let A/L be an absolutely simple abelian variety *without Complex Multiplication (**non-CM**)* of dimension g over a number field; that is to say, $A_{\overline{L}}$ is not isogenous to a product of abelian varieties of smaller dimension, and $\mathrm{End}\big(A_{\overline{L}}\big)\otimes\mathbb{Q}$ is *not* a number field of degree $2g$. We also let E/L be a *non-CM* elliptic curve over a number field. In either context, N is the conductor. We also let $B/\mathbb{F}_p$ be an abelian variety of dimension g.

2.2 p-Rank.

Recall that the group of geometric p-torsion of B has the shape

$$B(\overline{\mathbb{F}}_p) \cong \left(\mathbb{Z}/p\mathbb{Z}\right)^f$$

for some $0 \leq f \leq g$. We call the integer f the **p-rank** of B. If $f = g$, we call B **ordinary**, otherwise we call B **non-ordinary**. If B is an elliptic curve or abelian surface with $f = 0$, we call B **supersingular**.[1]

It is known that, possibly only after a finite extension of the base-field L of A, the set of non-ordinary primes $\Pi(A, f \neq g)$ has density zero if $g = 1$ [Ser68], if $g = 2$ [Ogu81], and for some abelian varieties with $g = 3$ [Tan99] or g a power of 4 [Noo95]. For arbitrary g, $\Pi(A, f \geq 2)$ has density one [Ogu81; BG97], but it is not known in general whether the set of ordinary primes for A has positive density. Because E_p is supersingular iff its trace of Frobenius is 0 (for $p \geq 5$), the Conjecture 2.1.1 predicts the asymptotics of $\Pi(E, f = 0)$ for $E/\mathbb{Q}$.

Various authors have improved upon the upper bound for E/L of [Ser68]. The best known upper bounds for $E/\mathbb{Q}$ are

$$\Pi(E, f = 0)(X) \ll_N \begin{cases} X^{3/4} & \text{unconditionally [Elk87b; Elk87a];} \\ X^{3/4}(\log X)^{-1/2} & \text{under GRH [Zyw15] .} \end{cases}$$

(It is astounding how small an improvement GRH affords with our current technology!) As for lower bounds, [Elk87c; Elk89] prove that if L has a real embedding

[1] This adjective means that the Newton slopes at p of the characteristic polynomial of π_p are all $1/2$. This condition is equivalent to $f = 0$ only when $g \leq 2$.

(e.g., if $L = \mathbb{Q}$), $\Pi(E, f = 0)$ is infinite. For $L = \mathbb{Q}$, various authors improve this lower bound; the best known bound is

$$\Pi(E, f = 0)(X) \gg_N \begin{cases} \log\log X & \text{under GRH [Elk87b];} \\ \frac{\log\log\log X}{(\log\log\log\log X)^{1+\epsilon}} & \text{unconditionally [FM96].} \end{cases}$$

Much less is known about higher-dimensional non-CM abelian varieties A. The author knows of no bounds better than $\Pi(A, f \neq g) = o(\pi(X))$ for only those abelian varieties mentioned in the second paragraph of this Subsection, and he knows of no asymptotic lower bounds if $g \geq 2$, even for a single non-CM abelian variety. Nor is it known whether $\#\Pi(A, f \neq g) = \infty$ for any non-CM abelian variety of dimension $g \geq 2$.

If A **has real multiplication**, which means here that $\mathrm{End}(A) \otimes \mathbb{Q}$ is a totally real number field of degree g and $\mathrm{End}(A) \otimes \mathbb{Q} \cong \mathrm{End}\left(A_{\overline{\mathbb{Q}}}\right) \otimes \mathbb{Q}$, [BG97] conjectures a probabilistic model which yields

$$\Pi(A, f < g)(X) \sim \begin{cases} C_A \frac{\sqrt{X}}{\log X} & \text{if } g = 1, \\ C_A \log\log X & \text{otherwise,} \end{cases}$$

and

$$\Pi(A, f = 0)(X) \sim \begin{cases} C_{A,0} \frac{\sqrt{X}}{\log X} & \text{if } g = 1, \\ C_{A,0} \log\log X & \text{if } g = 2, \\ O(1) & \text{otherwise,} \end{cases}$$

for certain positive constants C_A and $C_{A,0}$. This conjecture remains open.

2.3 Fixed-Trace.

For an elliptic curve $E/\mathbb{Q}$, denote $a_p := \mathrm{Tr}(\pi_p)$. For primes p of good reduction, i.e. if E_p is an elliptic curve, then $\#E_p\left(\mathbb{F}_p\right) = p + 1 - a_p$. The Hasse-Weil bound states that $\left|a_p\right| \leq 2\sqrt{p}$.

For a fixed integer $t \neq 0$, Conjecture 2.1.1 predicts the size of $\Pi(E, a_p = t)(X)$. Various upper bounds (conditional and unconditional) are given in the literature for $\Pi(E, a_p = t)(X)$. (We restrict to $t \neq 0$ because E_p is supersingular iff $a_p = 0$ when $p \geq 5$.) Unconditionally, Serre [Ser81] gives the first bound, $\Pi(E, a_p = t)(X) \ll_N X/(\log X)^{5/4-\epsilon}$. This was improved by Wan [Wan90] and Murty [Mur97]. The best known unconditional upper bound is from the recent preprint [TZ16], which gives

$$\Pi(E, a_p = t)(X) \ll_N \frac{X(\log\log X)^2}{(\log X)^2}.$$

Conditionally on GRH, Serre [Ser81] also gives the first bound, $\Pi(E, a_p = t)(X) \ll_N X^{7/8}(\log X)^{1/2}$. This was improved by Murty-Murty-Saradha [MMS88]. The best known upper bound (conditional on GRH) is

$$\Pi(E, a_p = t)(X) \ll_N X^{4/5}(\log X)^{-3/5}$$

of Zywina [Zyw15]. We also mention the result of [GJ12] which gives a proof of Conjecture 2.1.1 (and its generalization for newforms without CM with weight ≥ 2 and level ≥ 1) conditional on a conjectural convergence rate of $\left\{\frac{a_p}{2\sqrt{p}} | p \leq x\right\}$ towards the Sato-Tate distribution.

For higher-dimensional abelian varieties, this question has just begun investigation. The recent work of Cojocaru-Davis-Silverberg-Stange [Coj+16] studies the

GL_{2g}-trace of Frobenius, $a_{1,p} := \operatorname{Tr} \pi_p$ for the class of abelian varieties $A/\mathbb{Q}$ whose adelic Galois representation $\widehat{\rho}$ (see (3.18)) has open image in $\mathrm{GSp}_{2g} \widehat{\mathbb{Z}}$. They obtain the bounds

$$\Pi(A, a_{1,p} = t)(X) \ll_{A,\epsilon} \begin{cases} X^{1-\frac{1}{2}\theta+\epsilon} & \text{under GRH,} \\ X/(\log X)^{1+\theta-\epsilon} & \text{unconditionally,} \end{cases}$$

where $0 < \theta < 1/4$ decreases as g increases. They obtain improvements upon the above, in the form of larger θ, when $t \neq 2g$, and further improvements when $t = 0$. Moreover, they argue heuristically that with a conjectural assumption on the behavior of the Galois representations of A that generalizes the Sato-Tate Conjecture, it should be true that

$$\Pi(A, a_{1,p} = t)(X) \sim C_{A,t} \frac{\sqrt{X}}{\log X}$$

for some precisely defined constant $C_{A,t} \geq 0$, where, as before, we understand $C_{A,t} = 0$ to mean that the set is finite.

2.4 Fixed-Field.

For any elliptic curve $E/\mathbb{Q}$ and a prime p of good reduction, it is well-known that the endomorphism algebra $\operatorname{End}\big(E_p\big) \otimes \mathbb{Q} = \mathbb{Q}(\pi_p) \cong \mathbb{Q}(\sqrt{D_p})$ is an imaginary quadratic field, where we take D_p to be the squarefree part of $a_p^2 - 4p$. If E_p is supersingular, so that $a_p = 0$ (for $p \geq 5$), then $\operatorname{End}\big(E_p\big) \cong \mathbb{Q}(\sqrt{-p})$, and $\operatorname{End}\Big((E_p)_{\overline{\mathbb{F}}_p}\Big)$ is isomorphic to the quaternion algebra $\mathbb{B}_{p,\infty}/\mathbb{Q}$ ramified only at p and ∞. But if E_p is ordinary, then D_p might possibly take any squarefree value between 0 and $-4p$, not inclusive, and E_p does not pick up any extra endomorphisms over $\overline{\mathbb{F}}_p$.

In particular, if E is *non-CM*, then the endomorphism algebras (or **Frobenius fields**) at ordinary primes vary in the set of imaginary quadratic number fields K. The article of Cojocaru-Fouvry-Murty [CFM05] investigates the sets

$$\Pi(E,K) \coloneqq \Pi\left(E,\ p \text{ ordinary and } \mathrm{End}\big(E_p\big)\otimes\mathbb{Q} \cong K\right)$$

via the Square Sieve (see Subsection 3.3.1) and obtains the first bounds in print. These bounds are of the form $\Pi(E,K)(X) \ll_N X^\theta \log X$, conditional on various conjectural assumptions, and $\ll_{N,d(K/\mathbb{Q})} (\log\log X)^{13/12}(\log X)^{-25/24}$ unconditionally. See the remarks preceding the statement of this Theorem in [CFM05] for a history of remarks made by other authors which indicated bounds on $\Pi(E,K)(X)$. Improvements on these bounds have been made by various authors [CD08; Zyw15; TZ16] using sieves and "mixed representations" as suggested by Serre. The best known upper bounds are

$$\Pi(E,K)(X) \ll_E X^{4/5}(\log X)^{-3/5}h_K^{-3/5} + X^{1/2}(\log X)^3, \qquad \text{under GRH [Zyw15];}$$

$$\Pi(E,K)(X) \ll_{E,K} X(\log\log X)(\log X)^{-2}, \qquad \text{unconditionally [TZ16].}$$

2.5 Geometrically Simple.

Suppose A is geometrically simple, i.e. $A_{\overline{L}}$ is simple. Murty-Patankar [MP08] investigated the set of primes $\Pi(A, \text{geom. simple})$ at which A remains geometrically simple. They show that if A has Complex Multiplication or has Real Multiplication, then $\Pi(A, \text{geom. simple})$ has density one. Moreover, they and Zywina [Zyw13]

conjecture that for any A/L, possibly[2] after a finite extension L'/L,

$$\mathrm{End}\left(A_{\overline{L}}\right) \text{ is commutative} \iff \Pi(A_{L'}, \text{geom. simple}) \text{ has density } \delta_{A_{L'}} = 1 \quad (2.1)$$

Achter [Ach09] proves the backward direction of (2.1), and shows that moreover, if $\mathrm{End}\left(A_{\overline{L}}\right)$ is non-commutative, there is a finite extension L'/L such that $\delta_{A_{L'}} = 0$. He moreover also proves the forward direction of (2.1) if $\mathrm{End}\left(A_{\overline{L}}\right)$ is a totally real or totally imaginary field and if A satisfies a certain parity assumption. The particular case of the forward direction of (2.1) when $\mathrm{End}\left(A_{\overline{L}}\right) \cong \mathbb{Z}$ is an earlier result of Chavdarov [Cha97]. Achter [Ach12] gives explicit bounds on $\Pi(A, \text{geom. split})(X)$ in these cases (and one other). Zywina [Zyw13] proves that if the Manin-Mumford conjecture is true for A, then possibly after a finite extension, the forward direction is true. Murty-Zong [MZ14] prove that if for some prime $\ell \in \mathbb{Z}$, $\mathrm{End}(A) \otimes \mathbb{Q}_\ell \cong \mathrm{End}\left(A_{\overline{L}}\right) \otimes \mathbb{Q}_\ell$ is a field, if the Zariski closure of the image of the ℓ-adic Galois representation ρ_{ℓ^∞} is connected, and if ρ_{ℓ^∞} satisfies an additional technical assumption, then $\delta_A > 0$. Lastly, we mention [AH17] which estimates the number of *split* abelian surfaces over $\mathbb{F}_p$ as approximately $p^{-1/2}\left(\#\mathcal{A}_2\mathbb{F}_p\right)$, from which they conjecture that for an abelian surface $A/\mathbb{Q}$ without extra endomorphisms, $\Pi(A, \text{split})(X) \sim C_A \frac{\sqrt{X}}{\log X}$ for some positive constant C_A.

2.6 Primality of the number of points

We give a brief history of Conjecture 2.1.2 and its generalizations. Koblitz based his conjecture on the heuristics behind the Hardy-Littlewood Conjecture:

[2] As pointed out in [Zyw13], there are counterexamples to the conjecture without the extension.

broadly,

unless there's an obstruction to it being otherwise, polynomials of degree d should (up to a correction factor that comes from congruence conditions) act like random number generators which, on input n, output a number on the order of n^d.

From this heuristic, one finds a conjectural asymptotic count of the subset Π by finding the expected value of a random variable for the probability distribution given by the heuristic. The heuristic probability distribution for Koblitz's Conjecture is based on the Sato-Tate distribution and the Galois representation of E, and states that

unless there's an obstruction otherwise, the probability that $\#E_p(\mathbb{F}_p)$ is prime should be C_E times the probability that a random number on the order of p is prime.

He thus conjectures that

$$\begin{aligned}\pi_E(x) \coloneqq \#\left\{p \leq x \;\middle|\; \#E_p\left(\mathbb{F}_p\right) \text{ is prime}\right\} &\sim \sum_{p\leq x} C_E \frac{1}{\log p} \\ &\sim C_E \frac{x}{(\log x)^2}.\end{aligned}$$

The motivation for Conjecture 2.1.2 was from cryptography: for the purposes of using the Elliptic Curve Discrete Logarithm Problem in a cryptographic protocol (for instance, in the Elliptic Curve Diffie-Helman key agreement protocol) one desires an elliptic curve over a large finite field having a prime number of points. Koblitz's suggestion was to choose an appropriate elliptic curve $E/\mathbb{Q}$, then reduce modulo

appropriately large primes p and find $\#E_p(\mathbb{F}_p)$ (via, for instance, the Schoof-Elkies-Atkin algorithm (see, e.g., [BSS99])) until $\#E_p(\mathbb{F}_p)$ is prime.

The question of finding a lower bound for $\pi_E(x)$ is still completely open: the author knows of no results showing even that $\pi_E(x) \to \infty$ for any specific elliptic curve. However, upper bounds are known. For $E/\mathbb{Q}$ *without* Complex Multiplication (**non-CM**), the first conditional and unconditional upper bounds are given by Cojocaru [Coj05] using the Selberg sieve. Zywina [Zyw08] improves upon these bounds by providing explicit asymptotic constants and extending the bounds to the case where E is defined over a number field and may possibly have non-trivial torsion in its isogeny class. In the case of non-CM $E/\mathbb{Q}$, the best known conditional upper bound is given by David-Wu [DW12] who find

$$\pi_E(x) \leq \left(\frac{5}{1-\theta} + \epsilon\right) C_E \frac{x}{(\log x)^2}$$

for any $\epsilon > 0$, $x \gg_{\epsilon,\theta} 0$, assuming the θ-Hypothesis for the division fields of E. For $E/\mathbb{Q}$ *with* CM, Cojocaru [Coj05] gives the unconditional upper bound $\pi_E(x) \ll_N x/(\log x)^2$.

Two approaches towards generalizing Conjecture 2.1.2 have yielded lower bounds. The first, which we do not pursue generalizing in this article, is to consider $\pi_E(x)$ *on average* for elliptic curves $Y^2 = X^3 + aX + b$ over $\mathbb{Q}$ in a family $\mathcal{C}(x)$, in the parameters a and b which vary in a rectangle that grows with x. That is, the approach is to consider the average

$$\lim_{x\to\infty} \left(\frac{1}{\#\mathcal{C}(x)} \sum_{E\in\mathcal{C}(x)} \pi_E(x)\right).$$

This was first considered in [BCD11] who show that the average is indeed $\sim \mathfrak{C}x/(\log x)^2$ if the rectangle for $\mathcal{C}(x)$ grows sufficiently quickly with respect to x, namely if $A, B > x^\epsilon$ and $AB > x(\log x)^{10}$. Here, $\mathfrak{C}$ is a positive constant to be thought of as an average of the C_E for $E \in \mathcal{C}(x)$ as $x \to \infty$. They conclude then that "most" elliptic curves satisfy Conjecture 2.1.2; still, we cannot conclude Conjecture 2.1.2 for any specific curve. This result (and other "on average" results on the statistics of elliptic curves) has been improved; see, for instance, [DKS17].

The second approach, which we pursue in relation to abelian varieties, is to consider the question of *almost-prime* reductions of $E/\mathbb{Q}$. That is, this approach attempts to estimates

$$\pi_{E,r}(x) := \#\left\{p \leq x \;\middle|\; \#E_p\left(\mathbb{F}_p\right) \in P_r\right\}$$

for fixed r. This was first studied by Miri-Murty [MM01] who shows that for non-CM curves $E/\mathbb{Q}$ with trivial rational torsion, under GRH, $\pi_{E,16}(x) \gg x/(\log x)^2$. Steuding-Weng [SW05] improves this to $r = 9$ for non-CM curves, under GRH and the hypothesis (Triv_E). The best result for non-CM curves is by David-Wu [DW12], who show

$$\pi_{E,8}(x) \geq 2.778 \cdot C_E \frac{x}{(\log x)^2}$$

under the hypothesis (Triv_E) and the $(11/21)$-Hypothesis for the division fields of E. More precisely, their result is of the form

$$\pi_{E,r(\theta)}(x) \geq \frac{1.323}{1-\theta} C_E \frac{x}{(\log x)^2}$$

where the explicit function $r(\theta)$ decreases with the strength of the θ-Hypothesis and is bounded below by 8. We will model our argument to theirs.

For elliptic curves over $\mathbb{Q}$ with CM, the situation is much better: Steuding-Weng first found $\pi_{E,3}(x) \gg x/(\log x)^2$ if E is CM, under GRH and the hypothesis (Triv_E). Cojocaru [Coj05] improved this to $r = 5$ unconditionally. The best result for CM curves is by Iwaniec-Jiménez Urroz [IU10] and Jiménez Urroz [Jim08] who show unconditionally that

$$\#\{p \leq x \text{ of ordinary reduction} \;\Big|\; \#E_p(\mathbb{F}_p) = d_E \cdot P_2\} \gg \frac{x}{(\log x)^2}$$

where $d_E = \gcd\{\#E_p(\mathbb{F}_p) \;\Big|\; p \text{ of ordinary reduction}\}$.

More detailed statistical information of the function $p \mapsto \#E_p(\mathbb{F}_p)$ has been studied. In particular, Miri-Murty [MM01], Cojocaru [Coj05], and finally Y.-R. Liu [Liu06] find an Erdös-Kac result which provides a description of the "usual" behavior of $\#E_p(\mathbb{F}_p)$: they prove that, for any $\gamma \in \mathbb{R}$,

$$\lim_{x\to\infty}\left(\frac{1}{\pi(x)}\#\left\{p \leq x \;\Big|\; \frac{\omega(\#E_p(\mathbb{F}_p)) - \log\log p}{\sqrt{\log\log p}} \leq \gamma\right\}\right) = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\gamma} e^{-t^2/2}\,\mathrm{d}t,$$

unconditionally if E has CM, and conditionally on a θ-Hypothesis on the division fields of E if E is non-CM. Liu concludes this normal distribution from a generalized version of the Erdös-Kac Theorem, which improves upon the generalized Hardy-Ramanujan result of Murty-Murty [MM84] that was used to study the coefficients of modular forms. We will use Liu's Theorem 3 to prove our Theorem 5.1.4.

Lastly, generalizations of Conjecture 2.1.2 to higher-dimensional abelian varieties have been suggested in and have begun to be studied. Weng [Wen14] computes the probability of the statement "$\ell \;\Big|\; \#A(\mathbb{F}_p)$" for the reductions of a generic abelian

variety of $\mathbb{Q}$, which we find in (5.11) in a different form. Weng [Wen15] and Spreckels [Spr17] also consider the "vertical" question of finding the probability, for fixed CM field K and varying p, of the statement "$\exists A/\mathbb{F}_p$ with CM by $\mathcal{O}_K$ s.t. $\#A(\mathbb{F}_p)$ is prime," and conjecture an asymptotic behavior of a weighted counting function of such p, using the same heuristics as before.

Chapter 3: Preliminaries

3.1 Explicit Chebotarev Density Theorems

Let $L/\mathbb{Q}$ be a finite Galois extension with Galois group G, degree n_L, and discriminant d_L. Let C be a union of conjugacy classes of G. Denote by $\mathcal{P}(L/\mathbb{Q})$ the set of rational primes p which ramify in $L/\mathbb{Q}$. Set

$$M(L/\mathbb{Q}) \coloneqq (\#G) \prod_{p \in \mathcal{P}(L/\mathbb{Q})} p.$$

Define the prime counting function for C,

$$\pi_C(X, L/\mathbb{Q}) \coloneqq \#\left\{p \leq X : p \text{ unramified in } L/\mathbb{Q}; \sigma_p \subseteq C\right\}$$

where $\sigma_p \coloneqq \left(\frac{L/\mathbb{Q}}{p}\right)$ is the Artin symbol of p in $L/\mathbb{Q}$. Recall that the Chebotarev density theorem states that as $x \to \infty$,

$$\pi_C(X, L/\mathbb{Q}) \sim \frac{\#C}{\#G} \int_2^X \frac{\mathrm{d}t}{\log t}.$$

We use the notation $\operatorname{li} X \coloneqq \int_2^X \frac{\mathrm{d}t}{\log t}$ for the logarithmic integral to X. We will use "explicit" versions of this theorem; that is, versions with bounds on the error term of the approximation.

Before stating these results, we recall some background. Recall that the

Dedekind zeta function for a number field $L/\mathbb{Q}$,

$$\zeta_L(s) := \sum_{\mathfrak{a}\subset\mathcal{O}_L} \frac{1}{(\mathrm{N}\,\mathfrak{a})^s} = \prod_{\mathfrak{p}\subset\mathcal{O}_L} \left(\frac{1}{1-(\mathrm{N}\,\mathfrak{p})^{-s}}\right)$$

has an analytic continuation to the entire complex plane, except for a simple pole at $s = 1$. Recall also that for a Galois extension L/K of number fields, for each irreducible representation ρ of $G := \mathrm{Gal}(L/K)$ we have the Artin L-function $L(s,\rho)$, that is in general known to be a meromorphic function on $\mathbb{C}$; moreover, we have the factorization

$$\zeta_L(s) = \zeta_K(s) \prod_{\substack{\rho \text{ non-triv. irred.} \\ \text{rep. of G}}} L(s,\rho)^{\deg(\rho)}$$

where $\deg(\rho)$ is the multiplicity of ρ in the standard representation of G. Arithmetic information of L and of L/K is controlled by the zeros and coefficients of ζ_L and the Artin L-functions $L(s,\rho)$. In particular, there are the two following well-known conjectures.

Conjecture 3.1.1 (Generalized Riemann Hypothesis (GRH) for $L/\mathbb{Q}$.)**.** *All zeros of ζ_L in the critical strip lie on the critical line. That is, if $s \in \mathbb{C}$ is a zero of ζ_L with $0 < \Re(s) < 1$, then $\Re(s) = 1/2$.*

Conjecture 3.1.2 (Artin's Holomorphy Conjecture (AHC) for L/K.)**.** *Let ρ be a non-trivial irreducible representation of* $\mathrm{Gal}(L/K)$*. Then, $L(s,\rho)$ is holomorphic on* $\mathbb{C}$*.*

AHC is known for one-dimensional representations of G, since the Artin L-functions are then Hecke L-functions, which are known to be analytic on $\mathbb{C}$.

We will need to impose AHC as well as a generalization of GRH that asserts the existence of a zero-free half-plane region of ζ_L and of the L-functions for L/K. Ultimately, we will impose this hypothesis in Corollary 5.2.9, in the scenario that L is a division field of A and K is a certain subfield.

Hypothesis 3.1.3 (θ-Hypothesis for L/K.)**.** *Let* $1/2 \leq \theta < 1$, *and* $\mathcal{H}_\theta := \{s \in \mathbb{C} \mid \Re(s) > \theta\}$. *Then,* $\zeta_L(s)$ *has no zeros in* $\mathcal{H}_\theta$. *Moreover, AHC holds for* L/K, *and the* L*-functions attached to irreducible representations of* $\mathrm{Gal}(L/K)$ *are zero-free on* $\mathcal{H}_\theta$ *as well.*

We may say that a given L-function satisfies the θ-hypothesis; by this we mean that it is analytic and is non-zero on the region $\mathcal{H}_\theta$.

As mentioned in the beginning of this Section, we require these analytic hypothesis to use versions of the Chebotarev Density Theorem with explicit error bounds. We use the versions ultimately stated by [MMS88], as well as a modification of that result in [DW12] which requires only the θ-hypothesis. We now state these results.

Theorem 3.1.4 ([LO77; Ser81; MMS88; Mur97])**.** *Let the notation be as above. Then, for* $X \gg 0$,

$$\pi_C(X, L/\mathbb{Q}) = \frac{\#C}{\#G} \operatorname{li} X + R_C(X)$$

where the error term $R_C(X)$ *satisfies the following bounds:*

1. *Assume GRH for the Dedekind zeta function of* $L/\mathbb{Q}$. *Then,*

$$R_C(X) = O\left((\#C)X^{1/2}\left(\frac{\log|d_L|}{n_L} + \log X\right)\right)$$

2. *Assume GRH and AHC for $L/\mathbb{Q}$. Then,*

$$R_C(X) = O\left((\#C)^{1/2} X^{1/2} \left(\log M(L/\mathbb{Q}) + \log X\right)\right)$$

3. *Assume GRH, AHC, and PCC for $L/\mathbb{Q}$. Then,*

$$R_C(X) = O\left((\#C)^{1/2} X^{1/2} \left(\frac{\#\widetilde{G}}{\#G}\right)^{1/4} \left(\log M(L/\mathbb{Q}) + \log X\right)\right)$$

4. *Unconditionally, there exist positive constants A, B, B' with A effective and B, B' absolute, such that if*

$$\log X \geq B'(\#G)\left(\log|d_L|\right)^2,$$

then

$$R_C(X) \ll \frac{\#C}{\#G} \operatorname{li}\left(X \exp\left(-B \frac{\log X}{\max\{\,|d_L|^{1/n_L}, \log|d_L|\}}\right)\right) + (\#\tilde{C}) X \exp\left(-A\sqrt{\frac{\log X}{n_L}}\right),$$

The conjectural assumptions are as follows:

GRH: *the Generalized Riemann Hypothesis holds for the Dedekind zeta function of the division fields $\mathbb{Q}(A[lq])/\mathbb{Q}$, for all distinct primes $l, q \gg 0$;*

AHC: *Artin's Holomorphy Conjecture holds for the Artin L-functions attached to the irreducible characters of* $\operatorname{Gal}\mathbb{Q}(A[lq])/\mathbb{Q}$, *for all distinct primes $l, q \gg 0$;*

PCC: *a certain Pair Correlation Conjecture holds for the Artin L-functions attached to the irreducible characters of* $\operatorname{Gal}\mathbb{Q}(A[lq])/\mathbb{Q}$, *for all distinct primes $l, q \gg 0$. See [Mur01] for a precise formulation.*

In all of the above, the implied constants are absolute.

David-Wu extend the second statement to weaker assumptions. (In their notation, we set $K = \mathbb{Q}$.)

Theorem 3.1.5 ([DW12])**.** *Let the notation be as above. Let $H \trianglelefteq G$ be a normal subgroup such that for all irreducible representations ρ of $\mathrm{Gal}(L^H/\mathbb{Q}) \cong G/H$, the Artin L-function $L(s,\rho)$ is analytic and satisfies the θ-quasi GRH. Suppose also that the product $HC \subseteq C$. Then,*

$$R_C(x) \ll \left(\frac{\#C}{\#H}\right)^{1/2} x^{\theta} n_L \left(\log M(L/\mathbb{Q}) + \log x\right). \tag{3.1}$$

This recovers the second part of Theorem 3.1.4 when $\theta = 1/2$ and H is trivial.

We will also employ the following bound on $|d_L|$ from [Ser81].

Lemma 3.1.6. *Let the notation be as above. Then,*

$$\frac{n_L}{2} \sum_{p \in \mathcal{P}(L/\mathbb{Q})} \log p \leq \log|d_L| \leq (n_L - 1) \sum_{p \in \mathcal{P}(L/\mathbb{Q})} \log p + n_L \log n_L.$$

3.2 Generalized Erdös-Kac Theorem

We will use the generalization of the Erdös-Kac Theorem by Y.R. Liu [Liu06] to prove Theorem 5.1.4. The classical Erdös-Kac Theorem [EK40] states that the number of divisors of an integer n has *normal order* $\log\log n$ and essentially follows a Gaussian distribution around that normal order.

Theorem 3.2.1 (Erdös-Kac)**.**

$$\lim_{x\to\infty} \left(\frac{1}{x}\#\left\{n \leq x \;\middle|\; \frac{\omega(n) - \log\log n}{\sqrt{\log\log n}} \leq \gamma\right\}\right) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\gamma} e^{-t^2/2}\, \mathrm{d}t \tag{3.2}$$

Liu's generalization replaces $\omega(n)$ by $\omega(f(n))$ for functions f with a particular shape. We state it here in the slightly more general form given by M. Xiong [Xio09]. In what follows, S is an infinite subset of $\mathbb{N}$, and we use the notation $S(x) := \{n \in S \;\big|\; n \leq x\}$.

Theorem 3.2.2 ([Liu06; Xio09])**.** *Suppose that $\#S(x^{1/2}) = o(\#S(x))$ as $x \to \infty$. Let $f : S \to \mathbb{N}$. For each prime l, choose functions $\lambda_l = \lambda_l(x)$ ("main term") and $e_l = e_l(x)$ ("error term") such that*

$$\frac{1}{\#S(x)} \# \left\{ n \in S(x) \;\middle|\; l \mid f(n) \right\} = \lambda_l + e_l. \tag{3.3}$$

For increasing tuples $(l_1, \ldots, l_u)$ of distinct primes, we define functions $e_{l_1 \cdots l_u}(x)$ via

$$\frac{1}{\#S(x)} \# \left\{ n \in S(x) \;\middle|\; l_1 \cdots l_u \mid f(n) \right\} = \left(\prod_{i=1}^{u} \lambda_{l_i} \right) + e_{l_1 \cdots l_u}. \tag{3.4}$$

Suppose $\exists \beta \in (0, 1], \exists c > 0$, independent of x, and a function $y = y(x)$ such that the following conditions hold:

1. *for all $n \in S(x)$, the number of distinct prime divisors of $f(n)$ that are more than x^β is bounded uniformly (independent of x);*
2. *$\sum_{y < l < x^\beta} \lambda_l = o(\sqrt{\log \log x})$;*
3. *$\sum_{y < l < x^\beta} |e_l| = o(\sqrt{\log \log x})$;*
4. *$\sum_{l < y} \lambda_l = c \log \log x + o(\sqrt{\log \log x})$;*
5. *$\sum_{l < y} \lambda_l^2 = o(\sqrt{\log \log x})$;*

6. *for any* $r \in \mathbb{N}$ *and any integer* u, $1 \leq u \leq r$,

$$\sum_{\star} \left| e_{l_1 \cdots l_u}(x) \right| = o\left((\log\log x)^{-r/2} \right) \tag{3.5}$$

where the sum $\sum_{\star}$ *extends over all increasing tuples* $(l_1, \ldots, l_u)$ *of distinct primes* $l_i < y(x)$.

Then, for $\gamma \in \mathbb{R}$,

$$\lim_{x\to\infty} \left(\frac{1}{\#S(x)} \# \left\{ n \in S(x) \;\middle|\; \frac{\omega(f(n)) - c\log\log n}{\sqrt{\log\log n}} \leq \gamma \right\} \right) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\gamma} e^{-t^2/2} \, \mathrm{d}t. \tag{3.6}$$

3.3 The Square Sieve

As in [CFM05], the sieve-theoretic tool we use for Theorem 4.1.1 is the square sieve, which originates in [Hea84].

Theorem 3.3.1 (Square Sieve)**.** *Let* $\mathcal{A}$ *be a finite sequence of non-zero rational integers, and* $\mathcal{P}$ *a set of distinct odd rational primes. Set*

$$S(\mathcal{A}) := \#\left\{ \alpha \in \mathcal{A} : \alpha \text{ is a square} \right\}.$$

Then,

$$S(\mathcal{A}) \leq \frac{\#\mathcal{A}}{\#\mathcal{P}} + \max_{\substack{l,q\in\mathcal{P} \\ l\neq q}} \left| \sum_{\alpha\in\mathcal{A}} \left(\frac{\alpha}{lq} \right) \right| + \frac{2}{\#\mathcal{P}} \sum_{\alpha\in\mathcal{A}} \sum_{\substack{l\in\mathcal{P} \\ (\alpha,l)\neq 1}} 1 + \frac{1}{(\#\mathcal{P})^2} \sum_{\alpha\in\mathcal{A}} \left(\sum_{\substack{l\in\mathcal{P} \\ (\alpha,l)\neq 1}} 1 \right)^2$$

where $\left(\frac{\cdot}{\cdot}\right)$ *is the Jacobi symbol.*

Proof. See, for instance, Section 2.1 of [CFM05]. □

3.4 Simplified Greaves' Sieve

As in David-Wu, we use a simplified version of the weighted Greaves' Sieve for sieve problems of dimension 1, as given by Halberstam-Richert [HR85a; HR85b], for Theorem 5.1.1. That is to say, in the notation of Halberstam-Richert, we will take $E = V$ and $T = U$.

For a set of primes $\mathcal{P}$, we use the notation

$$P(z) = \prod \left\{ p \;\middle|\; p \in \mathcal{P}, p < z \right\}. \tag{3.7}$$

For a list $\mathcal{A}$ of integers, and d a positive integer, we use the notation

$$\mathcal{A}_d \coloneqq \left\{ a \in \mathcal{A} \;\middle|\; a \equiv 0 \bmod d \right\} \tag{3.8}$$

Theorem 3.4.1 (Simplified Greaves' Sieve, [HR85a; HR85b]). *Let $\mathcal{A}$ be a finite list of integers and $\mathcal{P}$ a set of primes such that the prime divisor(s) of each $a \in \mathcal{A}$ are in $\mathcal{P}$. Let y be a parameter, and $1/2 \le U < 1$ and V be constants such that*

$$V_0 \le V \le 1/4; \quad 1/2 \le U < 1; \quad U + 3V \ge 1 \tag{3.9}$$

where $V_0 = 0.074368\ldots$ is defined in [HR85a]. We suppose that there is a non-negative multiplicative function w that satisfies the hypotheses

$$w(p) = 0 \quad \text{for } p \notin \mathcal{P}, \tag{3.10}$$

$$0 < w(p) < p \quad \text{for } p \in \mathcal{P}, \tag{3.11}$$

$$\left| \sum_{z_1 \le p < z_2, p \in \mathcal{P}} \frac{w(p)}{p} \log p - \log \frac{z_2}{z_1} \right| \le A \quad \text{for } 2 \le z_1 \le z_2. \tag{3.12}$$

Moreover, we suppose that there is an approximation $X \in \mathbb{R}^+$ to $\#\mathcal{A}$ and define the "remainders"

$$r(\mathcal{A}, d) := \#\mathcal{A}_d - \frac{w(d)}{d} X \tag{3.13}$$

for d supported on $\mathcal{P}$. Define the sifting function

$$H(\mathcal{A}, y^V, y^U) := \sum_{a \in \mathcal{A}} \gamma\left(\gcd(a, P(y^U))\right) \tag{3.14}$$

where

$$\gamma(n) := \max\left\{0, 1 - \sum_{p|n, p \in \mathcal{P}} (1 - W(p))\right\}, \tag{3.15}$$

and where

$$W(p) := \begin{cases} \dfrac{1}{U - V}\left(\dfrac{\log(p)}{\log(y)} - V\right) & \text{if } y^U \le p < y^U, \\ 0 & \text{otherwise.} \end{cases} \tag{3.16}$$

Then, we have the lower bound

$$\begin{aligned} H(\mathcal{A}, y^V, y^U) \ge X \cdot V(y) \cdot \frac{2e^\gamma}{U - V}\left(J(U, V) + O\left(\frac{\log\log\log y}{(\log\log y)^{1/5}}\right)\right) \\ - (\log y)^{1/3}\left|\sum_{m<M, n<N, mn | P(y^U)} \alpha_m \beta_n \cdot r(\mathcal{A}, mn)\right| \end{aligned} \tag{3.17}$$

for any two real numbers M, N such that

$$MN = y; \quad M > y^U; \quad N > 1;$$

with the α_m and β_n certain real numbers in $[-1, 1]$; where

$$V(y) := \prod_{p \le y, p \in \mathcal{P}} \left(1 - \frac{w(p)}{p}\right);$$

$$J(U, V) := U \log\frac{1}{U} + (1 - U)\log\frac{1}{(1 - U)} - \log(4/3) + \alpha(V) - V\log 3 - V_0\beta(V),$$

where $\alpha(V)$ and $\beta(V)$ are certain non-negative numbers defined in [HR85b] as integrals, such that $\alpha(1/4) = \beta(1/4) = 0$.

Halberstam-Richert apply this sieve to the problem of counting almost-primes in short intervals; see Theorem C from [HR85b]. Similarly, David-Wu apply the sieve to the problem of counting almost-prime orders of an elliptic curve $E/\mathbb{Q}$. They rely on the following Lemma (in a less general form), which uses the sifting function H to detect these almost-prime orders. We will adapt this strategy to the higher-dimensional setting.

Lemma 3.4.2 ([DW12])**.** *Let $\mathcal{A}$ be a finite list of positive integers, indexed by $\{p \leq x\}$, whose elements have all prime divisors in $\mathcal{P} = \{p \mid \gcd(p, M) = 1\}$. Suppose there exist real constants $U, V, \xi > 0$ and a positive integer r such that $\max \mathcal{A} \leq \left(x^{\xi}\right)^{rU+V}$. (In the notation above, $y = x^{\xi}$.) Then,*

$$\#\left\{a \in \mathcal{A} \;\middle|\; \gcd(a, M) = 1;\ a = P_r\right\} \geq H\left(\mathcal{A}, (x^{\xi})^V, (x^{\xi})^U\right) - \sum_{(x^{\xi})^V \leq p < (x^{\xi})^U} \#\mathcal{A}_{p^2}.$$

3.5 Galois Representations and Open Image Varieties

Let $G_{\mathbb{Q}} := \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$. Let $A/\mathbb{Q}$ be a principally polarized abelian variety ("p.p.a.v.") of dimension g. Recall that for any integer $M \geq 1$, the geometric torsion subgroup

$$A[M](\overline{\mathbb{Q}}) \cong \left(\mathbb{Z}/M\mathbb{Z}\right)^{2g}$$

is naturally a $G_{\mathbb{Q}}$-module by action on the coordinates,

$$\rho_M : G_{\mathbb{Q}} \to \mathrm{GL}\left(A[M](\overline{\mathbb{Q}})\right) \cong \mathrm{GL}_{2g}\left(\mathbb{Z}/M\mathbb{Z}\right),$$

after choosing a basis of $A[M](\overline{\mathbb{Q}})$. However, the Galois action respects the Weil pairing e_M on $A[M]$, so that in fact

$$\rho_M : G_{\mathbb{Q}} \to \mathrm{GSp}\left(A[M](\overline{\mathbb{Q}}), e_M\right) \cong \mathrm{GSp}_{2g}\left(\mathbb{Z}/M\mathbb{Z}\right),$$

after choosing a symplectic basis with respect to the Weil pairing. We call ρ_M the **mod-M Galois representation** of A. Let ℓ be a rational prime. We define the **ℓ-adic Galois representation** as the inverse limit

$$\rho_{\ell^\infty} \coloneqq \varprojlim \rho_{\ell^n} : G_{\mathbb{Q}} \to \mathrm{GSp}_{2g}\,\mathbb{Z}_\ell$$

and the **adelic Galois representation**

$$\widehat{\rho} \coloneqq \prod_\ell \rho_{\ell^\infty} : G_{\mathbb{Q}} \to \prod_\ell \mathrm{GSp}_{2g}\,\mathbb{Z}_\ell \cong \mathrm{GSp}_{2g}\,\widehat{\mathbb{Z}} \tag{3.18}$$

The representations ρ_M, ρ_{ℓ^∞}, and $\widehat{\rho}$ are extremely important objects in the study of A.

Notation 3.5.1. *When we consider $\kappa = \mathbb{F}_p$, denote the Frobenius automorphism of $\overline{\mathbb{F}}_p/\mathbb{F}_p$ by* Frob_p. *When we consider $\kappa = \mathbb{Q}$, for convenience we denote by* Frob_p *an* absolute p-Frobenius automorphism, *namely any choice of element in* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *for which its image in* $\mathrm{Gal}(L/\mathbb{Q})$, *for any subextension L, has as its conjugacy class the Artin symbol $\left(\frac{L/\mathbb{Q}}{p}\right)$. It is well-known that p is unramified in $\mathbb{Q}(A[l])/\mathbb{Q}$ when $\kappa = \mathbb{Q}$ (since $p \nmid lN$ under our notation), so that everything we will do is independent of this choice of conjugacy class.*

It is well-known that for $p \nmid N$ fixed and $\ell \neq p$ varying, the characteristic polynomial of Frobenius, $\mathrm{char}\,\rho_\ell(\pi_p) \in \mathbb{Z}[x]$, is independent of ℓ. We will thus without comment use the notation $\mathrm{char}\,\pi_p$ or char_p for $\mathrm{char}\,\rho_\ell(\pi_p)$.

As stated in the Introduction, we study here those p.p.a.v. whose adelic representation $\widehat{\rho}$ has open image in $\mathrm{GSp}_{2g}\widehat{\mathbb{Z}}$. That is, we study A such that for $\ell \gg_A 0$,

$$\operatorname{im} \rho_{\ell^\infty} \cong \mathrm{GSp}_{2g}\mathbb{Z}_\ell. \tag{3.19}$$

For the curiosity of the reader, we mention that it is a very hard open problem to remove the dependency on A in the quantifier "$\ell \gg_A 0$" of the "open-image" results mentioned in Remark 4.1.3. That is to say, it is not currently known whether there is a uniform bound $\ell \gg_g 0$ such that (3.19) (or an appropriate modification thereof) holds for *every* p.p.a.v. of dimension g. This problem is known as the **Serre uniformity conjecture**. We also mention [Lom15a] and the recent preprint [Lom15b] which give explicit bounds, in terms of g and the stable Faltings height of A, on the quantifier "$\ell \gg_A 0$" of these results.

3.6 The Lang-Weil Bound

We include here the bound of Lang-Weil [LW54] on the number of rational points of a variety over a finite field. We will employ this bound in the proof of our main Theorems.

Theorem 3.6.1 ([LW54])**.** *Let $V \hookrightarrow \mathbb{P}^n_{\mathbb{F}_q}$ be a projective variety of dimension r and degree d over a finite field. Then,*

$$\left|\#V(\mathbb{F}_q) - q^r\right| = (d-1)(d-2)q^{r-\frac{1}{2}} + O_{n,r,d}(q^{r-1}).$$

We note in passing that this nearly recovers the Weil bound for the number of points on an abelian variety over a finite field.

3.7 Bounds on the size of sets in GSp_{2g}.

In the proof of our main Theorems in Chapter 4, we will employ a bound on the size of particular subsets of $\mathrm{GSp}_{2g}\,\mathbb{Z}/l\mathbb{Z}$. The bound appears (essentially) as stated below in [AH03] and originates in [Cha97].

We first recall a few well-known facts. For a prime l,

$$\#\,\mathrm{Sp}_{2g}\,\mathbb{F}_l = l^{g^2}\prod_{i=1}^{g}\left(l^{2i}-1\right) = l^{2g^2+g} - l^{2g^2+g-2} + O_g\left(l^{2g^2+g-6}\right) \tag{3.20}$$

There is the exact sequence $1 \to \mathrm{Sp}_{2g}\,\mathbb{F}_l \to \mathrm{GSp}_{2g}\,\mathbb{F}_l \xrightarrow{\mu} \mathbb{G}_m\mathbb{F}_l \to 1$, where μ is the **multiplicator character**, namely,

$$MJM^t = \mu(M)J$$

where $J = \begin{pmatrix} 0 & I_g \\ -I_g & 0 \end{pmatrix}$ is the matrix for the standard symplectic form. Thus,

$$\#\,\mathrm{GSp}_{2g}\,\mathbb{F}_l = (l-1)l^{g^2}\prod_{i=1}^{g}\left(l^{2i}-1\right) = l^{2g^2+g+1} - l^{2g^2+g} + O_g\left(l^{2g^2+g-1}\right) \tag{3.21}$$

Now let $f \in \mathbb{F}_l[x]$ be a characteristic polynomial of some matrix in $\mathrm{GSp}_{2g}\,\mathbb{F}_l$, and let $\mathrm{char}(M)$ denote the characteristic polynomial of M. Let

$$C(\mathbb{F}_l) := \left\{ M \in \mathrm{GSp}_{2g}\,\mathbb{F}_l \;\middle|\; \mathrm{char}\ M = f \right\}$$

be the set of matrices with specified characteristic polynomial f. ($C(\mathbb{F}_l)$ is the set of $\mathbb{F}_l$-valued points of a subscheme of $\mathrm{GSp}_{2g}/\mathbb{F}_l$, hence the notation.) Then,

Lemma 3.7.1 ([Cha97])**.**

$$\frac{l^{2g^2}}{(l-1)(l+1)^{2g^2+g}} \le \frac{\#C(\mathbb{F}_l)}{\#\,\mathrm{GSp}_{2g}\,\mathbb{F}_l} \le \frac{l^{2g^2}}{(l-1)(l-1)^{2g^2+g}}. \tag{3.22}$$

This immediately implies that $\#C(\mathbb{F}_l) \asymp_g l^{2g^2}$. A form in which this Lemma will be useful to us is to consider the error term

$$Q_C := \frac{\#C(\mathbb{F}_l)}{\#\,\mathrm{GSp}_{2g}\,\mathbb{F}_l} - \frac{l^{2g^2}}{(l-1)(l+1)^{2g^2+g}}$$

which, by the above, satisfies

$$0 \leq Q_C \leq \frac{l^{2g^2}}{(l-1)(l-1)^{2g^2+g}} - \frac{l^{2g^2}}{(l-1)(l+1)^{2g^2+g}} \tag{3.23}$$

$$= \frac{l^{2g^2}}{(l-1)} \cdot \frac{2l\left((l+1)^{(2g+1)(g-1)} + \ldots + (l-1)^{(2g+1)(g-1)}\right)}{(l^2-1)^{2g^2+g}} \tag{3.24}$$

$$\ll l^{2g^2-1+\left(1+(2g+1)(g-1)\right)-2(2g^2+g)} = l^{-3g-1}. \tag{3.25}$$

We will also need to bound the number of conjugacy classes in $\mathrm{GSp}_{2g}\,\mathbb{Z}/lq\mathbb{Z}$, i.e. $\#\widetilde{\mathrm{GSp}_{2g}\,\mathbb{Z}/lq\mathbb{Z}}$. The paper [FG12], based on work of Wall [Wal63], gives the following bounds.

Lemma 3.7.2. *Let $g \geq 1$. Then, $q^g \leq \#\widetilde{\mathrm{Sp}_{2g}\,\mathbb{Z}/q\mathbb{Z}} \leq 10.8q^g$*

With the Chinese Remainder Theorem and the long exact sequence of Section (1.4) of [HK85] that relates $\widetilde{\mathrm{GSp}_{2g}\,\mathbb{Z}/lq\mathbb{Z}}$ with $\widetilde{\mathrm{Sp}_{2g}\,\mathbb{Z}/lq\mathbb{Z}}$ and $\widetilde{\mathbb{F}_l^\times}$, we may thus conclude that

Lemma 3.7.3. $\#\widetilde{\mathrm{GSp}_{2g}\,\mathbb{Z}/lq\mathbb{Z}} \ll l^{g+1}q^{g+1}$.

Chapter 4: Fixed-Field Question

As mentioned earlier, the question that we study in this Chapter is an extension of the "fixed-field" Lang-Trotter question to higher-dimensional abelian varieties. Honda-Tate theory [Hon68; Tat69] tells us that when p is a prime of good, ordinary, non-split reduction for A, then its endomorphism algebra $\mathrm{End}\big(A_p\big)\otimes\mathbb{Q}$ is a CM field of degree $2g$, equal to its **Frobenius field** $\mathbb{Q}(\pi_p)$. It is known as well that $\mathrm{End}(A)$ (the endomorphism ring from characteristic zero) embeds into $\mathbb{Q}(\pi_p)$. Thus, when A does not have CM, its Frobenius fields are CM fields of degree $2g$ that admit an embedding of $\mathrm{End}(A)$ as a subring. We thus ask the following Question.

Question 4.0.1. *Let $A/\mathbb{Q}$ be a non-CM abelian variety of dimension g. Let K be a CM field of degree $2g$. Describe*

$$\Pi(A,K) \coloneqq \left\{ p \text{ of good, ordinary, nonsplit reduction } \;\middle|\; K \cong \mathrm{End}\big(A_p\big)\otimes\mathbb{Q} \right\}.$$

We also ask about supersets of $\Pi(A,K)$; namely, we ask

Question 4.0.2. *Let $A/\mathbb{Q}$ be a non-CM abelian variety of dimension g. Let F be a totally real field of degree g. Describe*

$$\Pi(A,F) \coloneqq \left\{ p \text{ of good, ordinary, nonsplit reduction } \;\middle|\; F \hookrightarrow \mathrm{End}\big(A_p\big)\otimes\mathbb{Q} \right\}.$$

4.1 Statement of Results

We mimic the application in [CFM05] of the Square Sieve (Theorem 3.3.1) to obtain the following.

Theorem 4.1.1. *Let $A/\mathbb{Q}$ be a principally polarized abelian variety of conductor N whose adelic Galois representation $\widehat{\rho}$ has image that is open in $\mathrm{GSp}_{2g}\widehat{\mathbb{Z}}$. (See Section 3.5 for definitions and the Remark below.) Let $K/\mathbb{Q}$ be a CM field of degree $2g$ with discriminant $d = d(K/\mathbb{Q})$. Then,*

$$\Pi(A,K)(X) \ll_{N,g} \begin{cases} X^{1-1/(8g^2+4g+6)}\log X & \text{under GRH;} \\ X^{1-1/(4g^2+4g+6)}\log X & \text{under GRH and AHC;} \\ X^{1-1/(2g^2+4g+6)}\log X & \text{under GRH, AHC, and PCC;} \end{cases}$$

and

$$\Pi(A,K)(X) \ll_{N,g} \frac{X(\log\log X)^{1+1/(4g^2+3g+2)}}{(\log X)^{1+1/(8g^2+6g+4)}}(1+\nu(d)) \quad \text{unconditionally,}$$

where $\nu(d)$ is the number of distinct prime divisors of d.

See [Mur01] for a precise formulation of Conjecture PCC.

Theorem 4.1.2. *Let $A/\mathbb{Q}$ be a principally polarized abelian surface with $\mathrm{End}\left(A_{\overline{\mathbb{Q}}}\right) \cong \mathbb{Z}$. Let $F = \mathbb{Q}(\sqrt{d})$ be a real quadratic number field, where d is squarefree. Then,*

$$\Pi(A,F)(X) \ll_N \begin{cases} X^{45/46}\log X & \text{under GRH;} \\ X^{29/30}\log X & \text{under GRH and AHC;} \\ X^{22/23}\log X & \text{under GRH, AHC, and PCC;} \end{cases}$$

and

$$\Pi(A,F)(X) \ll_N \frac{X(\log\log X)^{23/22}}{(\log X)^{67/66}}\big(1+\nu(d)\big) \quad \text{unconditionally,}$$

where $\nu(d)$ is the number of distinct prime divisors of d. The conjectural assumptions are identical to those above.

Remark 4.1.3. *The hypothesis in Theorem 4.1.1 that $\operatorname{im}\widehat{\rho}$ be open in $\mathrm{GSp}_{2g}\widehat{\mathbb{Z}}$ implies that A without extra endomorphisms, i.e, $\operatorname{End}\left(A_{\overline{\mathbb{Q}}}\right) \cong \mathbb{Z}$. Moreover, the hypothesis is true for a wide class of varieties without extra endomorphisms. Works of Serre [Ser00b; Ser00a] and Pink [Pin98] show that the hypothesis is true when $\operatorname{End}\left(A_{\overline{\mathbb{Q}}}\right) \cong \mathbb{Z}$ if $g = 1, 2$ or if $g \geq 3$ is not in the set*

$$\left\{\frac{1}{2}(2n)^k \;\middle|\; n>0, k\geq 3 \text{ odd}\right\} \cup \left\{\frac{1}{2}\binom{2n}{n} \;\middle|\; n \geq 3 \text{ odd}\right\} = \{4, 10, 16, 32, \ldots\}$$

The hypothesis is also true for those p.p.a.v. satisfying the property "(T)" of [Hal11]. Thus, adding this hypothesis to Theorem 4.1.2 would be redundant.

We also consider the set of those CM fields which appear as Frobenius fields of A,

$$\mathcal{D}_A := \left\{\mathbb{Q}(\pi_p) \;\middle|\; p \text{ good, ordinary, non-split}\right\}$$

and the set of their totally real subfields,

$$\mathcal{D}_A^0 := \left\{ \mathbb{Q}(\pi_p)_0 \;\middle|\; p \text{ good, ordinary, non-split} \right\}.$$

If A is a surface, we index (essentially) by discriminant,

$$\mathcal{D}_A^0(X) := \left\{ \mathbb{Q}(\sqrt{d}) \in \mathcal{D}_A^0 \;\middle|\; d \text{ squarefree}, \, d \leq 48X \right\}$$

For an abelian variety A of dimension g, we index $\mathcal{D}_A$ by certain effective functions $\psi_g(\sqrt{X})$ which are polynomials in $\sqrt{X}$:

$$\mathcal{D}_A(X) := \left\{ K \in \mathcal{D}_A \;\middle|\; \mathrm{sf}(d(K/\mathbb{Q})) \leq \psi_g(\sqrt{X}) \right\}$$

where $\mathrm{sf}(d)$ is the square-free part of d. See the discussion after Corollary 4.2.5 for details.

Using the Pigeonhole Principle, we obtain from our main Theorems the following asymptotic lower bounds on the size of $\#\mathcal{D}_A(X)$ and $\#\mathcal{D}_A^0(X)$.

Corollary 4.1.4. *Let the notations be as above. Let δ be the density of the set of good, ordinary, non-split primes for A. If $g > 2$, assume that $\delta > 0$. Then,*

$$\#\mathcal{D}_A(X) \gg_N \delta \frac{X^\theta}{(\log X)^2},$$

where we may take

$$\theta = \begin{cases} 1/(8g^2+4g+6) & \text{under GRH;} \\ 1/(4g^2+4g+6) & \text{under GRH and AHC;} \\ 1/(2g^2+4g+6) & \text{under GRH, AHC, and PCC.} \end{cases}$$

Corollary 4.1.5. *Let the notations be as above, and suppose that A is a surface. Then,*

$$\#\mathcal{D}_A^0(X) \gg_N \frac{X^\theta}{(\log X)^2},$$

where we may take

$$\theta = \begin{cases} 1/46 & \text{under GRH;} \\ 1/30 & \text{under GRH and AHC;} \\ 1/23 & \text{under GRH, AHC, and PCC.} \end{cases}$$

Corollary 4.1.6. *Let the notations be as above. Unconditionally, $\#\mathcal{D}_A(X) \to \infty$, and if A is a surface, $\#\mathcal{D}_A^0(X) \to \infty$.*

4.2 Proof of Theorem 4.1.1

In this section, $A/\mathbb{Q}$ is a principally polarized abelian variety of dimension g whose adelic Galois representation $\widehat{\rho}$ has open image in $\mathrm{GSp}_{2g}\widehat{\mathbb{Z}}$. This implies that A is simple. Let N be the conductor of A.

Let $p \nmid N$ be a prime of good, ordinary, non-split reduction for A. Then, by Honda-Tate theory, the endomorphism algebra $K \coloneqq \mathrm{End}\big(A_p\big) \otimes \mathbb{Q}$ is a CM field of degree $2g$. Let K_0 be the totally real subfield of K. Then,

$$K \cong \mathbb{Q}(\pi_p) = K_0(\sqrt{r})$$

for some totally negative integer $r \in K_0$.

Because π_p is a p-Weil number, the characteristic polynomial of the Frobenius

endomorphism π_p has the shape

$$\mathrm{char}_p(x) = x^{2g} + a_{1,p}x^{2g-1} + \ldots + a_{g,p}x^g + pa_{g-1,p}x^{g-1} + \ldots + p^g, \tag{4.1}$$

and the Triangle Inequality yields

$$\left|a_{i,p}\right| \leq \binom{2g}{i} p^{i/2}.$$

For convenience, when the prime p is clear from context, we suppress it from the subscripts.

The following Lemmas, specifically Corollary 4.2.5, allow us to apply the Square Sieve.

Lemma 4.2.1. *Let the notation be as above, but with K an arbitrary CM field of degree $2g$. Then,*

$$\mathbb{Q}(\pi_p) \cong K \implies \mathrm{N}_{\mathbb{Q}}^{K_0}\left((\pi_p + \overline{\pi_p})^2 - 4p\right) \cdot d(K/\mathbb{Q}) \in \mathbb{Z}^2$$

Proof. Let $x \mapsto \overline{x}$ be the complex conjugation of K/K_0. Then,

$$K_0 = \mathbb{Q}\left(\pi + \overline{\pi}\right); \quad K = K_0(\pi)$$

so that the ideal $d(K/K_0)$ is equal (up to the square of an ideal) to the discriminant of $x^2 - (\pi + \overline{\pi})x + p$. That is, $d(K/K_0) \cdot \mathfrak{a}^2 = \left((\pi_p + \overline{\pi_p})^2 - 4p\right)\mathcal{O}_{K_0}$ for some ideal $\mathfrak{a}$ of K_0. Then, the formula for the norm of the relative discriminant gives

$$d(K/\mathbb{Q}) = \mathrm{N}_{\mathbb{Q}}^{K_0}\left(\frac{((\pi_p + \overline{\pi_p})^2 - 4p)\mathcal{O}_{K_0}}{\mathfrak{a}^2}\right) d(K_0/\mathbb{Q})^{[K:K_0]}$$

so that

$$\mathrm{N}_{\mathbb{Q}}^{K_0}\left((\pi_p + \overline{\pi_p})^2 - 4p\right) = \frac{d(K/\mathbb{Q})\,\mathrm{N}\,\mathfrak{a}^2}{d(K_0/\mathbb{Q})^2},$$

and the relation follows. □

We note in passing that the sign of both sides is $(-1)^g$, so that in fact the above is an equality in $\mathbb{Z}$ and not just of ideals.

Lemma 4.2.2. *Suppose the integer $\pi + \overline{\pi}$ has minimal polynomial over $\mathbb{Q}$ equal to $x^g + \sum_{j=0}^{g-1} c'_j x^{g-j}$. Then, the c'_j are polynomials of the a_i and of p. These polynomials depend only on g.*

Proof. If $x^g + \sum_{j=0}^{g-1} c'_j x^{g-j} = 0$ is the minimal polynomial of $\pi + \overline{\pi}$, then

$$\begin{aligned} 0 &= \left(\pi + \frac{p}{\pi}\right)^g + c'_1 \left(\pi + \frac{p}{\pi}\right)^{g-1} + \ldots + c'_g \\ &= \sum_{j=0}^{g} c'_j \sum_{k=0}^{g-j} \binom{g-j}{k} \pi^k \left(\frac{p}{\pi}\right)^{g-j-k} \end{aligned}$$

so, multiplying through by π^g,

$$0 = \sum_{j=0}^{g} c'_j \sum_{k=0}^{g-j} \binom{g-j}{k} \pi^{2k+j} p^{g-j-k} \tag{4.2}$$

The result follows from solving the system of equations that results from comparing (4.2) to the minimal polynomial of π. □

Lemma 4.2.3. *Let $n \geq 1$. Let $A \in \mathrm{GL}_n \mathbb{Z}_\ell$ have characteristic polynomial $x^n + \sum_{i=0}^{n-1} \alpha_i x^{n-i}$. Then, the coefficients of the characteristic polynomial of A^2 are polynomials in the α_i. These polynomials do not depend on A, and are at worst quadratic in each of the α_i.*

Proof. A is similar to a matrix in "companion form,"

$$A \sim \begin{pmatrix} 0 & 0 & 0 & \dots & 0 & -\alpha_0 \\ 1 & 0 & 0 & \dots & 0 & -\alpha_1 \\ 0 & 1 & 0 & \dots & 0 & -\alpha_2 \\ 0 & 0 & 1 & \dots & 0 & -\alpha_3 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & -\alpha_{n-1} \end{pmatrix}$$

$$\implies A^2 - xI \sim \begin{pmatrix} -x & 0 & 0 & \dots & 0 & -\alpha_0 & \alpha_{n-1}\alpha_0 \\ 0 & -x & 0 & \dots & 0 & -\alpha_1 & \alpha_{n-1}\alpha_1 - \alpha_0 \\ 1 & 0 & -x & \dots & 0 & -\alpha_2 & \alpha_{n-1}\alpha_2 - \alpha_1 \\ 0 & 1 & 0 & \dots & 0 & -\alpha_3 & \alpha_{n-1}\alpha_3 - \alpha_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & -\alpha_{n-1} & \alpha_{n-1}^2 - \alpha_{n-2} - x \end{pmatrix}.$$

Perform the column operation adding $\alpha_n \cdot (\text{column } n-1)$ to column n:

$$\det(A^2 - xI) = \det \begin{pmatrix} -x & 0 & 0 & \dots & 0 & -\alpha_0 & 0 \\ 0 & -x & 0 & \dots & 0 & -\alpha_1 & -\alpha_0 \\ 1 & 0 & -x & \dots & 0 & -\alpha_2 & -\alpha_1 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & -x & -\alpha_{n-3} & -\alpha_{n-4} \\ 0 & 0 & 0 & \dots & 0 & -\alpha_{n-2} - x & -\alpha_{n-3} - \alpha_{n-1}x \\ 0 & 0 & 0 & \dots & 1 & -\alpha_{n-1} & -\alpha_{n-2} - x \end{pmatrix}$$

Expanding out the determinant of the right-hand side, we see that each term in $\det(A^2 - xI)$ is at worst quadratic in each α_i. $\square$

Lemma 4.2.4. *Suppose the integer $\beta := (\pi + \overline{\pi})^2$ has characteristic equation*

$$\text{charpoly}_\beta(x) := x^g + c_1 x^{g-1} + \ldots + c_g := \prod_{\tau: K_0 \hookrightarrow \overline{\mathbb{Q}}} \big(x - \tau(\beta)\big) = 0$$

when considered as a linear transformation on the vector space $\mathbb{Q}(\pi + \overline{\pi})$ over $\mathbb{Q}$. (That is, considered as the multiplication map $x \mapsto \beta x$.) Then, the c_i are polynomials of the a_i and p, and these polynomials depend only on g. Moreover, these polynomials are at worst quadratic in the a_i.

Proof. This follows from the previous two Lemmas. $\square$

Thus, by noting that

$$\text{N}_{\mathbb{Q}}^{K_0}\left((\pi_p + \overline{\pi_p})^2 - 4p\right) = (-1)^g \cdot \text{charpoly}_{(\pi+\overline{\pi})^2}(4p)$$

and from the previous Lemmas, we see that

Corollary 4.2.5. *With the notations as above,*

$$K \cong \mathbb{Q}(\pi_p) \implies (-1)^g \left((4p)^g + c_1(4p)^{g-1} + \ldots + c_g\right) \cdot d(K/\mathbb{Q}) \in \mathbb{Z}^2$$

We emphasize that the factor

$$\gamma_p := (-1)^g \left((4p)^g + c_1(4p)^{g-1} + \ldots + c_g\right) \tag{4.3}$$

has a *uniform bound* via the Triangle Inequality that is a polynomial in $\sqrt{p}$. We will call this polynomial $\psi_g(\sqrt{p})$. One may compute that, for example, for $g = 2$

$$\gamma_p = a_2^2 - 4pa_1^2 + 4pa_2 + 4p^2$$

so that $\gamma_p \leq 128p^2$; and for $g = 3$,

$$\gamma_p = -\big((4p)^3 + (2a_2 - 6p - a_1^2)(4p)^2 + (a_2^2 - 6a_2p + 9p^2 + 2a_1a_3 - 4pa_1^2)(4p) \\ + a_3^2 - 4pa_1a_3 + 4p^2a_1^2\big)$$

so that $\gamma_p \leq 5072p^3$. We note that these polynomials for the γ_p are indeed quadratic in all of the a_i.

We now proceed to the proof of Theorem 4.1.1.

Proof of Theorem 4.1.1.

Let K be CM field of degree $2g$ and discriminant $d := d(K/\mathbb{Q})$. We sieve the sequence

$$\mathcal{A} := \big(\gamma_p \cdot d\big)_{p \leq X}$$

with the sieving set

$$\mathcal{P} := \left\{ p \;\middle|\; z < p \leq 2z \right\}$$

with z to be chosen optimally later. From Corollary 4.2.5, it is clear that $\Pi(A, K)(X) \leq S(\mathcal{A})$. We recall that the Square Sieve states

$$S(\mathcal{A}) \leq \frac{\#\mathcal{A}}{\#\mathcal{P}} + \max_{\substack{l,q \in \mathcal{P} \\ l \neq q}} \left| \sum_{\alpha \in \mathcal{A}} \left(\frac{\alpha}{lq} \right) \right| + \frac{2}{\#\mathcal{P}} \sum_{\alpha \in \mathcal{A}} \sum_{\substack{l \in \mathcal{P} \\ (\alpha, l) \neq 1}} 1 + \frac{1}{(\#\mathcal{P})^2} \sum_{\alpha \in \mathcal{A}} \left(\sum_{\substack{l \in \mathcal{P} \\ (\alpha, l) \neq 1}} 1 \right)^2.$$

We also recall that integration by parts yields the bounds $\sum_{p \leq X} \log p \sim X$ and $\sum_{p \leq X} (\log p)^2 \sim X \log X$, and we note that d, being bounded by the discriminant of $\mathrm{char}_p(X)$, is bounded by a polynomial in X that depends only on g. Thus,

$$\#\mathcal{A} \ll \frac{X}{\log X}; \qquad \#\mathcal{P} \asymp \frac{z}{\log z}; \qquad \sum_{\substack{l \in \mathcal{P} \\ (\alpha, l) \neq 1}} 1 \ll \log \alpha;$$

$$\sum_{\alpha\in\mathcal{A}} \log\alpha \ll \pi(X)\log d + \sum_{p\leq X}\log(\psi_g(\sqrt{p})) \ll \pi(X)\log X + \pi(X)\log X \asymp X;$$

$$\begin{aligned}\sum_{\alpha\in\mathcal{A}} (\log\alpha)^2 &= \sum_{\alpha\in\mathcal{A}} \left(\log d + \log\psi_g(\sqrt{p})\right)^2 \\ &\ll_g \pi(X)\log(d)^2 + \pi(X)\log X\log d + \pi(X)\log(X)^2 \\ &\ll_g X\log X.\end{aligned}$$

It remains to bound the character sum

$$\left|\sum_{\alpha\in\mathcal{A}}\left(\frac{\alpha}{lq}\right)\right|$$

for distinct primes $l, q \in \mathcal{P}$. We have

$$\begin{aligned}\sum_{\alpha\in\mathcal{A}}\left(\frac{\alpha}{lq}\right) &= \left(\frac{d}{lq}\right)\sum_{\substack{p\leq X\\ p\nmid lqN}}\left(\frac{\gamma_p}{lq}\right) + O(\log N) + 2 \\ &= \pm\sum_{\substack{c \bmod lq\\ (c,lq)=1}}\sum_{\substack{a_1,\ldots,a_g\\ \bmod lq}}\left(\frac{\gamma_p}{lq}\right)\pi_A(X, lq; a_1,\ldots,a_g,c) + O(\log N) \qquad (4.4)\end{aligned}$$

where

$$\pi_A(X, lq; a_1,\ldots,a_g,c) \coloneqq \qquad (4.5)$$

$$\#\left\{p\leq X, p\nmid lqN \;\middle|\; \mathrm{char}_p(x) \equiv x^{2g} + a_1x^{2g-1} + \ldots + a_gx^g + ca_1x^{g-1}\ldots + c^g \bmod lq\right\} \qquad (4.6)$$

(We ignore the possibility that $(d, lq) \neq 1$ because we wish to bound the *maximum* value of the character sum.) Now, $\widehat{\rho}$ has open image in $\mathrm{GSp}_{2g}\widehat{\mathbb{Z}}$, by assumption; so for $z \gg_A 0$,

$$\mathrm{Gal}\left(\mathbb{Q}(A[lq])/\mathbb{Q}\right) \cong \mathrm{GSp}_{2g}\mathbb{Z}/lq\mathbb{Z}.$$

and, under the above isomorphism, specifying $\mathrm{char}_p \mod lq$ is the same as requiring the Artin symbol $\left(\frac{\mathbb{Q}(A[lq])/\mathbb{Q}}{p}\right)$ to be contained in a certain union of conjugacy classes of $\mathrm{Gal}\left(\mathbb{Q}(A[lq])/\mathbb{Q}\right)$. Then, by the Chebotarev density theorem, for $X \gg 0$,

$$\pi_A(X, lq; a_1, \ldots, a_g, c) = \frac{\#C(lq; a_1, \ldots, a_g, c)}{\#\,\mathrm{GSp}_{2g}\,\mathbb{Z}/lq\mathbb{Z}}\pi(X) + R(X; lq; a_1, \ldots, a_g, c),$$

where

$$C(lq; a_1, \ldots, a_g, c) \coloneqq \tag{4.7}$$

$$\left\{h \in \mathrm{GSp}_{2g}\,\mathbb{Z}/lq\mathbb{Z} \;\middle|\; \mathrm{char}_h(x) = x^{2g} + a_1x^{2g-1} + \ldots + a_gx^g + ca_1x^{g-1} \ldots + c^g\right\} \tag{4.8}$$

is the aforementioned union of conjugacy classes, and $R(X; lq; a_1, \ldots, a_g, c)$ is the error term, bounded variously as in Theorem 3.1.4. We let

$$R_{lq} \coloneqq \max\left|R(X; lq; a_1, \ldots, a_g, c)\right|,$$

for notational convenience, where the maximum runs over $a_i, c \in \mathbb{Z}/lq\mathbb{Z}$. The bound (3.22) and the Chinese Remainder Theorem yield

$$\begin{aligned}\frac{\#C(lq; a_1, \ldots, a_g, c)}{\#\,\mathrm{GSp}_{2g}\,\mathbb{Z}/lq\mathbb{Z}} &= \left(\frac{l^{2g^2}}{(l-1)(l+1)^{2g^2+g}} + Q_C(l)\right)\left(\frac{q^{2g^2}}{(q-1)(q+1)^{2g^2+g}} + Q_C(q)\right) \\ &= f(l)f(q) + f(l)Q_C(q) + f(q)Q_C(l) + Q_c(l)Q_C(q)\end{aligned}$$

where

$$f(l) \coloneqq \frac{l^{2g^2}}{(l-1)(l+1)^{2g^2+g}}.$$

Recall that $0 \leq Q_C(l) \ll l^{-3g-1}$ (and similarly for $Q_C(q)$). Now, repeatedly using

the Triangle Inequality,

$$\begin{aligned}
\left|\sum_{\alpha\in\mathcal{A}}\left(\frac{\alpha}{lq}\right)\right| &\leq \left|\sum_{\substack{c \bmod lq\\(c,lq)=1}}\sum_{\substack{a_1,\dots,a_g\\ \bmod lq}}\left(\frac{\gamma_p}{lq}\right)\pi_A(X,lq;a_1,\dots,a_g,c)\right| + O(\log N) + 2\\
&\ll_N \left|\sum_c\sum_{a_1,\dots,a_g}\left(\frac{\gamma_p}{lq}\right)\frac{\#C(lq;a_1,\dots,a_g,c)}{\#\,\mathrm{GSp}_{2g}\,\mathbb{Z}/lq\mathbb{Z}}\right|\pi(X)\\
&\quad + \left|\sum_c\sum_{a_1,\dots,a_g}\left(\frac{\gamma_p}{lq}\right)R(X;lq;a_1,\dots,a_g,c)\right|\\
&\leq f(l)f(q)\left|\sum_c\sum_{a_1,\dots,a_g}\left(\frac{\gamma_p}{lq}\right)\right|\pi(X) + f(l)\left|\sum_c\sum_{a_1,\dots,a_g}\left(\frac{\gamma_p}{lq}\right)Q_C(q)\right|\pi(X)\\
&\quad + f(q)\left|\sum_c\sum_{a_1,\dots,a_g}\left(\frac{\gamma_p}{lq}\right)Q_C(l)\right|\pi(X)\\
&\quad + \left|\sum_c\sum_{a_1,\dots,a_g}\left(\frac{\gamma_p}{lq}\right)Q_C(l)Q_C(q)\right|\pi(X)\\
&\quad + \left|\sum_c\sum_{a_1,\dots,a_g}\left(\frac{\gamma_p}{lq}\right)R(X;lq;a_1,\dots,a_g,c)\right|
\end{aligned}$$

so that

$$\begin{aligned}
\left|\sum_{\alpha\in\mathcal{A}}\left(\frac{\alpha}{lq}\right)\right| &\ll_N (lq)^{-g-1}\left|\sum_c\sum_{a_1,\dots,a_g}\left(\frac{\gamma_p}{lq}\right)\right|\pi(X) + l^{-g-1}(lq)^{g+1}q^{-3g-1}\pi(X)\\
&\quad + q^{-g-1}(lq)^{g+1}l^{-3g-1}\pi(X) + (lq)^{g+1}l^{-3g-1}q^{-3g-1}\pi(X) + R_{lq}(lq)^{g+1}\\
&\asymp z^{-2g-2}\left|\sum_{\substack{c \bmod lq\\(c,lq)=1}}\sum_{\substack{a_1,\dots,a_g\\ \bmod lq}}\left(\frac{\gamma_p}{lq}\right)\right|\pi(X) + z^{-2g}\pi(X) + z^{2g+2}R_{lq} \qquad (4.9)
\end{aligned}$$

It remains to bound the character sum in (4.9). Choose $i \in \{1,\dots,g\}$ such that γ_p is quadratic in a_i. Then, by Lemma 4.2.4, $\gamma_p = \gamma_{i,p}^{(2)}(a_i)^2 + \gamma_{i,p}^{(1)}a_i + \gamma_{i,p}^{(0)}$, and the coefficients $\gamma_{i,p}^{(k)}$ are polynomials in the other a_j and in p. We now break up the

character sum using a_i,

$$\sum_{a_i}\left(\frac{\gamma_p}{lq}\right) = \#\left\{a_i \bmod lq \;\middle|\; \left(\frac{\gamma_p}{l}\right) = \left(\frac{\gamma_p}{q}\right) = 1\right\} \tag{4.10}$$

$$- \#\left\{a_i \bmod lq \;\middle|\; \left(\frac{\gamma_p}{l}\right) = 1, \left(\frac{\gamma_p}{q}\right) = -1\right\}$$

$$- \#\left\{a_i \bmod lq \;\middle|\; \left(\frac{\gamma_p}{l}\right) = -1, \left(\frac{\gamma_p}{q}\right) = 1\right\} \tag{4.11}$$

$$+ \#\left\{a_i \bmod lq \;\middle|\; \left(\frac{\gamma_p}{l}\right) = \left(\frac{\gamma_p}{q}\right) = -1\right\}. \tag{4.12}$$

These numbers are related to the number of points on certain genus-0 curves over $\mathbb{Z}/l\mathbb{Z}$ and $\mathbb{Z}/q\mathbb{Z}$, as follows. Define the projective curve $\mathcal{C}/(\mathbb{Z}/lq\mathbb{Z})$ via the affine model $\mathcal{C}^\circ$ with equation

$$y^2 = \gamma_{i,p}^{(2)}x^2 + \gamma_{i,p}^{(1)}x + \gamma_{i,p}^{(0)}.$$

and let $\mathcal{C}_l^\circ, \mathcal{C}_l$ be the reductions of $\mathcal{C}^\circ, \mathcal{C}$ modulo l, and similarly for q. Then, the number of rational points

$$\#\mathcal{C}_l^\circ\left(\mathbb{Z}/l\mathbb{Z}\right) = 2 \cdot \#\left\{a_i \bmod l \;\middle|\; \left(\frac{\gamma_p}{l}\right) = 1\right\} + \epsilon_l$$

where ϵ_l is the number of rational points $(a_i, y) \in \mathcal{C}_l^\circ\left(\mathbb{Z}/l\mathbb{Z}\right)$ such that $\gamma_p \equiv 0 \bmod l$. Similarly for q. Now, pick a number $\xi \in \mathbb{Z}/lq\mathbb{Z}$ which is neither a square $\bmod l$ nor $\bmod q$. Then, by a similar argument, if we define the projective curve $\mathcal{C}'$ by the affine model $\mathcal{C}'^\circ$ with equation

$$y^2 = \xi\left(\gamma_{i,p}^{(2)}x^2 + \gamma_{i,p}^{(1)}x + \gamma_{i,p}^{(0)}\right)$$

and the reductions $\mathcal{C}_l^\circ, \mathcal{C}_l$ modulo l (and similarly for q), then the number of rational

points

$$\#\mathcal{C}'^{\circ}\left(\mathbb{Z}/l\mathbb{Z}\right) = 2 \cdot \# \left\{ a_i \bmod l \;\middle|\; \left(\frac{\gamma_p}{l}\right) = -1 \right\} + \epsilon_l'$$

with ϵ_l' defined analogously. Also denote by ϵ_q, and ϵ_q' the analogous quantities for q. Then, by the Chinese Remainder Theorem,

$$\# \left\{ a_i \bmod lq \;\middle|\; \left(\frac{\gamma_p}{l}\right) = 1 \neq \left(\frac{\gamma_p}{q}\right) = 1 \right\} = \frac{1}{2}\left(\#\mathcal{C}_l^{\circ}(\mathbb{Z}/l\mathbb{Z}) - \epsilon_l\right) \cdot \frac{1}{2}\left(\#\mathcal{C}_q^{\circ}(\mathbb{Z}/q\mathbb{Z}) - \epsilon_q\right);$$

$$\# \left\{ a_i \bmod lq \;\middle|\; \left(\frac{\gamma_p}{l}\right) = -1, \left(\frac{\gamma_p}{q}\right) = 1 \right\} = \frac{1}{2}\left(\#\mathcal{C}_l'^{\circ}(\mathbb{Z}/l\mathbb{Z}) - \epsilon_l'\right) \cdot \frac{1}{2}\left(\#\mathcal{C}_q^{\circ}(\mathbb{Z}/q\mathbb{Z}) - \epsilon_q\right);$$

and so on for the other two terms in (4.10).

Assume for the moment that $\mathcal{C}_l$ is irreducible. Then, $\mathcal{C}_l$ is an irreducible genus-0 curve with a rational point. Thus, $\mathcal{C}_l \cong \mathbb{P}^1_{\mathbb{Z}/l\mathbb{Z}}$, so that $\#\mathcal{C}_l\left(\mathbb{Z}/l\mathbb{Z}\right) = l+1$. Similarly if $\mathcal{C}_l', \mathcal{C}_q$, and $\mathcal{C}_q'$ are irreducible.

Now, $\mathcal{C}_l$ and $\mathcal{C}_l'$ are reducible iff the discriminant

$$\left(\gamma_{i,p}^{(1)}\right)^2 - 4\gamma_{i,p}^{(2)}\gamma_{i,p}^{(0)} \equiv 0 \bmod l \tag{4.13}$$

and similarly with q. Equation 4.13 defines a hypersurface $\mathcal{Z}_l \hookrightarrow \mathbb{A}^{g-1}_{\mathbb{Z}/l\mathbb{Z}}$ of degree at most 4, which thus has $O_g(1)$ many irreducible components. Thus, by Theorem 3.6.1 the number of rational points $\mathcal{Z}_l\left(\mathbb{Z}/l\mathbb{Z}\right) \ll_g l^{g-2}$. Similarly, we get a hypersurface $\mathcal{Z}_q \hookrightarrow \mathbb{A}^{g-1}_{\mathbb{Z}/q\mathbb{Z}}$ with $\ll_g q^{g-2}$ many rational points. Thus, by the Chinese Remainder Theorem, all of the curves $\mathcal{C}_l, \mathcal{C}_l', \mathcal{C}_q$, and $\mathcal{C}_q'$ are irreducible when the numbers $(a_j)_{j\neq i} \in (\mathbb{Z}/lq\mathbb{Z})^{g-1}$ are outside a set $\mathcal{Z}$ of size $O(z^{2g-3})$.

For notational convenience, denote $\widehat{a} = (a_j)_{j\neq i} \in \left(\mathbb{Z}/lq\mathbb{Z}\right)^{g-1}$. Then, continu-

ing from (4.10),

$$\begin{aligned}\left|\sum_{\widehat{a}}\sum_{a_i}\left(\frac{\gamma_p}{lq}\right)\right| &\leq \left|\sum_{\widehat{a}\in\mathcal{Z}}\sum_{a_i}\left(\frac{\gamma_p}{lq}\right)\right| + \left|\sum_{\widehat{a}\notin\mathcal{Z}}\sum_{a_i}\left(\frac{\gamma_p}{lq}\right)\right| \\ &= O_g\left(z^{2g-3}\right)\cdot(lq) + \left|\sum_{\widehat{a}\notin\mathcal{Z}}\sum_{a_i}\left(\frac{\gamma_p}{lq}\right)\right| \\ &\ll_g z^{2g-1} + \left|\sum_{\widehat{a}\notin\mathcal{Z}}\sum_{a_i}\left(\frac{\gamma_p}{lq}\right)\right|\end{aligned}$$

We briefly let δ (with appropriate subscripts and superscripts) denote the number of rational points at infinity of the projective curve corresponding to the subscripts and superscripts. We thus have, for $\widehat{a}\notin\mathcal{Z}$, continuing from (4.10),

$$\begin{aligned}\sum_{a_i}\left(\frac{\gamma_p}{lq}\right) &= \frac{1}{4}\left(\#\mathcal{C}_l^{\circ}(\mathbb{Z}/l\mathbb{Z})-\epsilon_l\right)\left(\#\mathcal{C}_q^{\circ}(\mathbb{Z}/q\mathbb{Z})-\epsilon_q\right) \\ &\quad+\frac{1}{4}\left(\#\mathcal{C}_l'^{\circ}(\mathbb{Z}/l\mathbb{Z})-\epsilon_l'\right)\left(\#\mathcal{C}_q'^{\circ}(\mathbb{Z}/q\mathbb{Z})-\epsilon_q'\right) \\ &\quad-\frac{1}{4}\left(\#\mathcal{C}_l'^{\circ}(\mathbb{Z}/l\mathbb{Z})-\epsilon_l'\right)\left(\#\mathcal{C}_q^{\circ}(\mathbb{Z}/q\mathbb{Z})-\epsilon_q\right) \\ &\quad-\frac{1}{4}\left(\#\mathcal{C}_l^{\circ}(\mathbb{Z}/l\mathbb{Z})-\epsilon_l\right)\left(\#\mathcal{C}_q'^{\circ}(\mathbb{Z}/q\mathbb{Z})-\epsilon_q'\right) \\ &= \frac{1}{4}\left(l+1-\delta_l-\epsilon_l\right)\left(q+1-\delta_q-\epsilon_q\right) \\ &\quad+\frac{1}{4}\left(l+1-\delta_l'-\epsilon_l'\right)\left(q+1-\delta_q'-\epsilon_q'\right) \\ &\quad-\frac{1}{4}\left(l+1-\delta_l'-\epsilon_l'\right)\left(q+1-\delta_q-\epsilon_q\right) \\ &\quad-\frac{1}{4}\left(l+1-\delta_l-\epsilon_l\right)\left(q+1-\delta_q'-\epsilon_q'\right) \\ &= (\delta_l+\epsilon_l)(\delta_q+\epsilon_q)+(\delta_l'+\epsilon_l')(\delta_q'+\epsilon_q') \\ &\quad-(\delta_l+\epsilon_l)(\delta_q'+\epsilon_q')-(\delta_l'+\epsilon_l')(\delta_q+\epsilon_q). \\ &= O(1).\end{aligned}$$

Thus,

$$\left|\sum_{\widehat{a}}\sum_{a_i}\left(\frac{\gamma_p}{lq}\right)\right| \ll_g z^{2g-1} + \#\left((\mathbb{Z}/lq\mathbb{Z})^{g-1} - \mathcal{Z}\right)\cdot O(1) \ll z^{2g-1},$$

so that, continuing from (4.9),

$$\begin{aligned}\left|\sum_{\alpha\in\mathcal{A}}\left(\frac{\alpha}{lq}\right)\right| &\ll_{N,g} z^{-2g-2}z^{2g-1}\pi(X) + z^{-2g}\pi(X) + z^{2g+2}R_{lq} \\ &\ll z^{-3}\pi(X) + z^{2g+2}R_{lq}\end{aligned}$$

Thus, putting it together,

$$S(\mathcal{A}) \ll_N \frac{X\log z}{z\log X} + z^{-3}\pi(X) + z^{2g-1}\max_{\substack{l,q\in\mathcal{P}\\ l\neq q}} R_{lq} + \frac{2\log z}{z}X + \frac{(\log z)^2}{z^2}X\log X$$

so

$$\boxed{S(\mathcal{A}) \ll \frac{X\log z}{z} + \frac{(\log z)^2 X\log X}{z^2} + z^{2g+2}\max_{l,q\in\mathcal{P}} R_{lq}(X).}$$

4.2.1 Under GRH.

Let $L_{lq} \coloneqq \mathbb{Q}\left(A[lq]\right)$, $n(lq) \coloneqq [L_{lq} : \mathbb{Q}]$, and $d(lq) \coloneqq d(L_{lq}/\mathbb{Q})$. We have the bound

$$\#C(lq; a_1, \ldots, a_g, c) \ll \left(\#\,\mathrm{GSp}_{2g}\,\mathbb{Z}/lq\mathbb{Z}\right)\cdot z^{-2g-2} \ll z^{4g^2}$$

Then, under GRH, for $X \gg 0$, Theorem 3.1.4 yields

$$\begin{aligned}\max R_{lq}(X) &= O\left(\max_{L=L_{lq}}(\#C)X^{1/2}\left(\frac{\log|d_L|}{n_L} + \log X\right)\right) \\ &= O\left(z^{4g^2}X^{1/2}\max_{L=L_{lq}}\left(\frac{\log|d_L|}{n_L} + \log X\right)\right)\end{aligned}$$

where $\operatorname{Gal} L_{lq}/\mathbb{Q} = \mathrm{GSp}_{2g}\,\mathbb{Z}/lq\mathbb{Z}$, so $n(lq) \asymp z^{4g^2+2g+2}$. We also have, by Lemma 3.1.6,

$$\log\left|d(lq)\right| \leq n(lq)\log\left(\prod_{p\in\mathcal{P}(L_{lq}/\mathbb{Q})} p\right) + n(lq)\log n(lq).$$

But the only primes that ramify in L_{lq} divide lqN. Thus,

$$\begin{aligned}\max R_{lq}(X) &= O\left(z^{4g^2}X^{1/2}\left(\max\log(lqN) + \max\log(n(lq)) + \log X\right)\right)\\ &= O_g\left(z^{4g^2}X^{1/2}\left(\log(z^2N) + \log(z) + \log X\right)\right)\\ &= O_{N,g}\left(z^{4g^2}X^{1/2}\left(\log z + \log X\right)\right).\end{aligned}$$

Thus,

$$S(\mathcal{A}) \ll_{N,g} \frac{X\log z}{z} + \frac{(\log z)^2 X\log X}{z^2} + z^{2g+2}\left(z^{4g^2}X^{1/2}\left(\log z + \log X\right)\right).$$

We will choose z so that $\log z \asymp \log X$. Then,

$$S(\mathcal{A}) \ll_{N,g} \frac{X\log X}{z} + z^{4g^2+2g+2}X^{1/2}\log X$$

We choose $z := X^{1/(8g^2+4g+6)}$, which yields $S(\mathcal{A}) \ll_{N,g} X^{1-1/(8g^2+4g+6)}\log X$. □

4.2.2 Under GRH + AHC.

Let the notation be as above. Under GRH and AHC, for $X \gg 0$, Theorem 3.1.4 yields

$$\begin{aligned}\max R_{lq}(X) &= O\left(\max_{L=L_{lq}}(\#C)^{1/2}X^{1/2}\left(\log M(L/\mathbb{Q}) + \log X\right)\right)\\ &= O_{N,g}\left(z^{2g^2}X^{1/2}\left(\log z + \log X\right)\right)\end{aligned}$$

and thus

$$S(\mathcal{A}) \ll_{N,g} \frac{X \log z}{z} + \frac{(\log z)^2 X \log X}{z^2} + z^{2g+2}\left(z^{2g^2} X^{1/2} (\log z + \log X)\right).$$

We choose $z := X^{1/(4g^2+4g+6)}$, which yields $S(\mathcal{A}) \ll_{N,g} X^{1-1/(4g^2+4g+6)} \log X$. □

4.2.3 Under GRH + AHC + PCC.

Let the notation be as above. Under GRH, AHC, and PCC, for $X \gg 0$, Theorem 3.1.4 yields

$$\begin{aligned}\max R_{lq}(X) &= O\left(\max(\#C)^{1/2} X^{1/2} \left(\frac{\#\widetilde{G}}{\#G}\right)^{1/4} \left(\log M(L/\mathbb{Q}) + \log X\right)\right) \\ &= O_{N,g}\left(z^{2g^2} X^{1/2} \left(\frac{\max \#\widetilde{\mathrm{GSp}_4 \mathbb{Z}/lq\mathbb{Z}}}{z^{4g^2+2g+2}}\right)^{1/4} (\log z + \log X)\right)\end{aligned}$$

Thus, with Lemma (3.7.3),

$$\begin{aligned}\max R_{lq}(X) &= O_{N,g}\left(z^{2g^2} X^{1/2} \left(\frac{z^{2g+2}}{z^{4g^2+2g+2}}\right)^{1/4} (\log z + \log X)\right) \\ &= O_{N,g}\left(z^{g^2} X^{1/2} (\log z + \log X)\right)\end{aligned}$$

and thus

$$S(\mathcal{A}) \ll_{N,g} \frac{X \log z}{z} + \frac{(\log z)^2 X \log X}{z^2} + z^{2g+2}\left(z^{g^2} X^{1/2} (\log z + \log X)\right).$$

We choose $z := X^{1/(2g^2+4g+6)}$, which yields $S(\mathcal{A}) \ll_{N,g} X^{1-1/(2g^2+4g+6)} \log X$.

□

4.2.4 Unconditionally.

Let the notation be as above. We recall part 4 of Theorem 3.1.4. Unconditionally, for a number field L, there exist constants $A, B, B' > 0$ such that when

$$\log X \geq B'(\#G)\left(\log|d_L|\right)^2,$$

we have

$$R(X) \ll \frac{\#C}{\#G}\,\mathrm{li}\left(X\exp\left(-B\frac{\log X}{\max\{\,|d_L|^{1/n_L}\,,\log|d_L|\}}\right)\right) \tag{4.14}$$

$$+\,(\#\tilde{C})X\exp\left(-A\sqrt{\frac{\log X}{n_L}}\right). \tag{4.15}$$

We recall Lemma 3.1.6, which states

$$\frac{n_L}{2}\sum_{p\in\mathcal{P}(L/\mathbb{Q})}\log p \leq \log|d_L| \leq (n_L-1)\sum_{p\in\mathcal{P}(L/\mathbb{Q})}\log p + n_L\log n_L.$$

Thus, with $L=\mathbb{Q}(A[lq])/\mathbb{Q}$,

$$\log|d_L| \leq z^{4g^2+2g+2}\left(\log(lqN)+\log(z^{2g^2+g+1})\right) \ll_{N,g} z^{4g^2+2g+2}\log z.$$

Now, l and q do ramify in $\mathbb{Q}(A[lq])/\mathbb{Q}$, since the existence of the Weil pairing on $A[lq]$ implies that $\mathbb{Q}(A[lq])/\mathbb{Q}$ contains an $(lq)^{\text{th}}$ root of unity. Thus,

$$\log|d_L| \gg_N z^{4g^2+2g+2}\log(lq) \asymp z^{4g^2+2g+2}\log z$$

Also,

$$|d_L|^{1/n_L} \geq \left(\prod_{p\in\mathcal{P}(L/\mathbb{Q})} p\right)^{1/2} \geq (lq)^{1/2} \asymp z$$

and

$$|d_L|^{1/n_L} \leq n_L \prod_{p \in \mathcal{P}(L/\mathbb{Q})} p \leq z^{4g^2+2g+2}(lqN) \ll_N z^{4g^2+2g+4}.$$

Thus, the requirement

$$\log X \geq B'(\#G)\left(\log|d_L|\right)^2 \asymp_{N,g} B' z^{8g^2+6g+4}(\log z)^2 \tag{4.16}$$

is satisfied with the choice

$$z := c' \frac{(\log X)^{1/(8g^2+6g+4)}}{(\log\log X)^{1/(4g^2+3g+2)}}$$

for a certain positive constant c' depending only on N and g. The reader may check that there exists such a c' so that (4.16) is satisfied with this choice of z. Moreover, we see from the above that $\max\{\, |d_L|^{1/n_L}, \log|d_L| \} \ll_N z^{4g^2+2g+4}$.

For $l, q \in \mathcal{P}$, arguments above show that

$$\frac{\#C}{\#\operatorname{GSp}_4 \mathbb{Z}/lq\mathbb{Z}} \ll z^{-2g-2}.$$

Using the approximation $\operatorname{li} t \sim \frac{t}{\log t}$, we then have

$$\begin{aligned}
&\frac{\#C}{\#G} \operatorname{li}\left(X \exp\left(-B\frac{\log X}{\max\{\, |d_L|^{1/n_L}, \log|d_L| \}}\right)\right) \\
&\qquad \ll z^{-2g-2} \frac{\left(X \exp\left(-B\frac{\log X}{\max\{\, |d_L|^{1/n_L}, \log|d_L| \}}\right)\right)}{\log\left(X \exp\left(-B\frac{\log X}{\max\{\, |d_L|^{1/n_L}, \log|d_L| \}}\right)\right)} \\
&\qquad \ll_N \frac{z^{-2g-2} X \exp\left(-B\frac{\log X}{z^{4g^2+2g+4}\log z}\right)}{\log X - B(\log X) z^{-(4g^2+2g+4)}(\log z)^{-1}} \\
&\qquad \ll \frac{X^{1-Bz^{-(4g^2+2g+4)}(\log z)^{-1}}}{z^{4g^2+2g+4}\log X}
\end{aligned}$$

From our choice of z, (4.21), the bounds above, and the weak bound $\#\widetilde{C} \leq \#\widetilde{\mathrm{GSp}_{2g}\,\mathbb{Z}/lq\mathbb{Z}} \asymp z^{2g+2}$, we obtain (after a calculation which we omit; see Section 4 of [CFM05]) the bounds

$$\max_{\substack{l,q\in\mathcal{P}\\ l\neq q}}\left|\sum_{\alpha\in\mathcal{A}}\left(\frac{\alpha}{lq}\right)\right| \ll_N \frac{X}{z\log X};$$

$$\sum_{\alpha\in\mathcal{A}}\sum_{\substack{l\in\mathcal{P}\\ (\alpha,l)\neq 1}} 1 \ll_N \frac{X}{\log X}\nu_z(d);$$

$$\sum_{\alpha\in\mathcal{A}}\left(\sum_{\substack{l\in\mathcal{P}\\ (\alpha,l)\neq 1}} 1\right)^2 \ll_N \frac{X}{\log X}\left(\nu_z(d)+(\nu_z(d))^2\right);$$

where $\nu_z(d)$ is the number of distinct prime divisors of d less than or equal to z. Thus, from the Square Sieve and the trivial bounds $\nu_z(d) \leq \nu(d)$ and $\nu_z(d) \leq \pi(z)$ we obtain

$$S(\mathcal{A}) \ll_{N,g} \frac{X\log z}{z\log X}(1+\nu_z(d)) \tag{4.17}$$

$$\ll_{N,g} \frac{X(\log\log X)^{1+1/(4g^2+3g+2)}}{(\log X)^{1+1/(8g^2+6g+4)}}(1+\nu_z(\mathrm{d}(K/\mathbb{Q}))). \tag{4.18}$$

□

4.3 Proof of Theorem 4.1.2

In this Section, $A/\mathbb{Q}$ is a principally polarized abelian surface with $\mathrm{End}\left(A_{\overline{\mathbb{Q}}}\right) \cong \mathbb{Z}$. This implies that A is simple. As mentioned in Remark 4.1.3, works of Serre show that its adelic Galois representation $\widehat{\rho}$ has open image in $\mathrm{GSp}_4\,\widehat{\mathbb{Z}}$. Let N be the conductor of A, and let $F/\mathbb{Q}$ be a real quadratic number field.

Let $p \nmid N$ be a prime of good, ordinary, non-split reduction for A. Then, by Honda-Tate theory, the endomorphism algebra $K := \mathrm{End}\left(A_p\right)\otimes\mathbb{Q} = \mathbb{Q}(\pi_p)$ is a

quartic CM field. Let K_0 be the totally real quadratic subfield of K. Then,

$$K_0 = \mathbb{Q}(\sqrt{d}), \quad K = \mathbb{Q}(\pi_p) = K_0(\sqrt{r})$$

for some squarefree rational integer $d > 0$, and some totally negative integer $r \in \mathcal{O}_{K_0}$.

As in Section 4.2, the characteristic polynomial of the Frobenius endomorphism π_p has the shape

$$\mathrm{char}_p(x) = x^4 + a_{1,p}x^3 + a_{2,p}x^2 + pa_{1,p}x + p^2,$$

and the Triangle Inequality yields

$$\left|a_{1,p}\right| \leq \binom{4}{1}\sqrt{p} = 4\sqrt{p}; \qquad \left|a_{2,p}\right| \leq \binom{4}{2}\left(\sqrt{p}\right)^2 = 6p. \tag{4.19}$$

Remark 4.3.1. *Since A is a simple abelian surface, A is the Jacobian of some smooth curve C of genus 2; it is well known that $a_{1,p}$ and $a_{2,p}$ may be expressed in terms of the number of $\mathbb{F}_p$- and $\mathbb{F}_{p^2}$-points of the reduction of C mod p, as one has the formula of Hasse-Weil,*

$$\#C_p(\mathbb{F}_{p^k}) = p^k + 1 - \sum \lambda^k$$

where the sum is over the roots $\lambda \in \overline{\mathbb{Q}}$ of char_p*. Letting $N_k := \#C_p(\mathbb{F}_{p^k})$, this yields the formulas*

$$a_1 = p + 1 - N_1; \qquad a_2 = \frac{1}{2}\left(N_2 + N_1(N_1 - 2p - 2)\right).$$

Now, the following lemma allows us to apply the Square Sieve to $\Pi(A, F)$.

Lemma 4.3.2. *Let the notation be as above, but with $d > 0$ an arbitrary squarefree rational integer. Then,*

$$K_0 \cong \mathbb{Q}(\sqrt{d}) \iff d(a_1^2 - 4a_2 + 8p) \text{ is a square.}$$

Proof. Let $x \mapsto \overline{x}$ be the complex conjugation of K/K_0. Then,

$$K_0 = \mathbb{Q}(\pi + \overline{\pi}) = \mathbb{Q}\left(\pi + \frac{p}{\pi}\right).$$

(Note that $\pi + \overline{\pi} \notin \mathbb{Q}$ because π satisfies $x^2 - (\pi + \overline{\pi})x + p = 0$ and $[\mathbb{Q}(\pi) : \mathbb{Q}] = 4$.) Let $\beta = \pi + p/\pi$. Then, for $m, n \in \mathbb{Z}$,

$$\beta^2 + m\beta + n = 0 \iff \pi^4 + m\pi^3 + (2p + n)\pi^2 + pm\pi + p^2 = 0$$

so that the minimal polynomial of β is $x^2 + a_1 x + a_2 - 2p$. The result follows from the requirement that d and the discriminant $a_1^2 - 4(a_2 - 2p)$ must have the same squarefree part. □

We now proceed to the proof of Theorem 4.1.2. Because of its similarity to the proof of Theorem 4.1.1, we abbreviate some parts of the proof.

Proof of Theorem 4.1.2.

We apply the Square Sieve to the sequence

$$\mathcal{A} := \left(d(a_{1,p}^2 - 4a_{2,p} + 8p)\right)_{p \le X}$$

with the sieving set

$$\mathcal{P} := \left\{ p \;\middle|\; z < p \le 2z \right\}$$

with z to be chosen optimally later. From Lemma 4.3.2, it is clear that $\Pi(A, F)(X) \le S(\mathcal{A})$.

We recall that the Square Sieve states

$$S(\mathcal{A}) \le \frac{\#\mathcal{A}}{\#\mathcal{P}} + \max_{\substack{l,q \in \mathcal{P} \\ l \ne q}} \left| \sum_{\alpha \in \mathcal{A}} \left(\frac{\alpha}{lq}\right) \right| + \frac{2}{\#\mathcal{P}} \sum_{\alpha \in \mathcal{A}} \sum_{\substack{l \in \mathcal{P} \\ (\alpha, l) \ne 1}} 1 + \frac{1}{(\#\mathcal{P})^2} \sum_{\alpha \in \mathcal{A}} \left(\sum_{\substack{\mathfrak{l} \in \mathcal{P} \\ (\alpha, \mathfrak{l}) \ne 1}} 1 \right)^2.$$

We have again the bounds

$$\#\mathcal{A} \ll \frac{X}{\log X}; \qquad \#\mathcal{P} \asymp \frac{z}{\log z}; \qquad \sum_{\substack{l\in\mathcal{P}\\(\alpha,l)\neq 1}} 1 \ll \log\alpha;$$

$$\sum_{\alpha\in\mathcal{A}} \log\alpha \ll X; \qquad \sum_{\alpha\in\mathcal{A}} (\log\alpha)^2 \ll X\log X.$$

It remains to bound the character sum

$$\left|\sum_{\alpha\in\mathcal{A}} \left(\frac{\alpha}{lq}\right)\right|$$

for distinct primes $l, q \in \mathcal{P}$. We have

$$\begin{aligned}\sum_{\alpha\in\mathcal{A}} \left(\frac{\alpha}{lq}\right) &= \left(\frac{d}{lq}\right) \sum_{\substack{p\leq X\\ p\nmid lqN}} \left(\frac{a_{1,p}^2 - 4a_{2,p} + 8p}{lq}\right) + O(\log N)\\ &= \pm \sum_{\substack{c \bmod lq\\(c,lq)=1}} \sum_{\substack{a_1,a_2\\ \bmod lq}} \left(\frac{a_1^2 - 4a_2 + 8c}{lq}\right) \pi_A(X, lq; a_1, a_2, c) + O(\log N) \quad (4.20)\end{aligned}$$

where $\pi_A(X, lq; a_1, a_2, c)$ is defined as in (4.5). Then, by the Chebotarev density theorem, for $X \gg 0$,

$$\pi_A(X, lq; a_1, a_2, c) = \frac{\#C(lq; a_1, a_2, c)}{\#\,\mathrm{GSp}_4\,\mathbb{Z}/lq\mathbb{Z}}\pi(X) + R(X; lq; a_1, a_2, c),$$

where $C(lq; a_1, a_2, c)$ is defined as in (4.7), and $R(X; lq; a_1, a_2, c)$ is the error term, bounded variously as in Theorem 3.1.4. We let

$$R_{lq} := \max\left|R(X; lq; a_1, a_2, c)\right|$$

for notational convenience, where the max runs over $a_1, a_2, x \in \mathbb{Z}/lq\mathbb{Z}$.

The bound (3.22) with $g = 2$ and the Chinese Remainder Theorem yields

$$\frac{\#C(lq; a_1, a_2, c)}{\#\,\mathrm{GSp}_4\,\mathbb{Z}/lq\mathbb{Z}} = \frac{l^8}{(l-1)(l+1)^{10}} \cdot \frac{q^8}{(q-1)(q+1)^{10}} + Q(lq; a_1, a_2, c)$$

where the error term satisfies

$$0 \leq Q(lq; a_1, a_2, c) = l^{-3} \cdot O(q^{-7}) + q^{-3} \cdot O(l^{-3}) + O\left((lq)^{-7}\right) = O\left(z^{-10}\right).$$

Thus,

$$\left|\sum_{\alpha \in \mathcal{A}} \left(\frac{\alpha}{lq}\right)\right| \ll \left| \sum_{\substack{c \bmod lq \\ (c,lq)=1}} \sum_{\substack{a_1,a_2 \\ \bmod lq}} \left(\frac{a_1^2 - 4a_2 + 8c}{lq}\right) \left(\frac{l^8 q^8 \pi(X)}{(l-1)(l+1)^{10}(q-1)(q+1)^{10}} + Q(lq; a_1, a_2, c)\pi(X)\right)\right|$$

$$+ (lq)^3 R_{lq}(X) + O(\log N),$$

Now, by the orthogonality of characters, once $l, q > 2$,

$$\sum_{a_2 \bmod lq} \left(\frac{a_1^2 - 4a_2 + 8c}{lq}\right) = 0$$

Thus,

$$\left|\sum_{\alpha \in \mathcal{A}} \left(\frac{\alpha}{lq}\right)\right| \ll_N \left| \sum_{\substack{c \bmod lq \\ (c,lq)=1}} \sum_{\substack{a_1,a_2 \\ \bmod lq}} \left(\frac{a_1^2 - 4a_2 + 8c}{lq}\right) Q(lq; a_1, a_2, c)\right| \pi(X) + (lq)^3 R_{lq}(X),$$

and thus, by a similar argument as what led to (4.9),

$$\left|\sum_{\alpha \in \mathcal{A}} \left(\frac{\alpha}{lq}\right)\right| \ll_N (lq)^3 \left(l^{-3}q^{-7} + l^{-7}q^{-3}\right) \pi(X) + (lq)^3 R_{lq}(X)$$

$$\asymp z^{-4} \frac{X}{\log X} + z^6 R_{lq}(X).$$

Putting it together,

$$S(\mathcal{A}) \ll_N \frac{X \log z}{z \log X} + \left(\frac{X}{z^4 \log X} + z^6 \max_{\substack{l,q \in \mathcal{P} \\ l \neq q}} R_{lq}(X)\right) + \frac{2 \log z}{z} X + \frac{(\log z)^2}{z^2} X \log X$$

and thus

$$\boxed{S(\mathcal{A}) \ll_N \frac{X \log z}{z} + \frac{(\log z)^2 X \log X}{z^2} + z^6 \max R_{lq}(X).}$$

4.3.1 Under GRH.

Let $L = L_{lq} := \mathbb{Q}\left(A[lq]\right)$, $n(lq) := [L_{lq} : \mathbb{Q}]$, and $d(lq) := d(L_{lq}/\mathbb{Q})$. We have the bound

$$\#C(lq; a_1, a_2, c) \ll \left(\#\,\mathrm{GSp}_4\,\mathbb{Z}/lq\mathbb{Z}\right) \frac{(lq)^8}{(l-1)(l+1)^{10}(q-1)(q+1)^{10}} \ll (lq)^8$$

Then, under GRH, for $X \gg 0$, Theorem 3.1.4 yields

$$\begin{aligned}\max R_{lq}(X) &= O\left(\max_{L=L_{lq}} (\#C) X^{1/2} \left(\frac{\log|d_L|}{n_L} + \log X\right)\right) \\ &= O\left(z^{16} X^{1/2} \max_{L=L_{lq}} \left(\frac{\log|d_L|}{n_L} + \log X\right)\right)\end{aligned}$$

where $\mathrm{Gal}\, L_{lq}/\mathbb{Q} = \mathrm{GSp}_4\,\mathbb{Z}/lq\mathbb{Z}$, so $n(lq) \asymp (lq)^{10} \asymp z^{20}$. We also have, by Lemma (3.1.6),

$$\log\left|d(lq)\right| \leq n(lq) \log\left(\prod_{p \in \mathcal{P}(L_{lq}/\mathbb{Q})} p\right) + n(lq) \log n(lq).$$

But the only primes that ramify in L_{lq} divide lqN. So,

$$\max R_{lq}(X) = O\left(z^{16} X^{1/2} \left(\max \log(lqN) + \max \log(n_L) + \log X\right)\right)$$

so

$$\begin{aligned}\max R_{lq}(X) &= O\left(z^{16} X^{1/2} \left(\log(z^2 N) + \log(z^{10} z^{10}) + \log X\right)\right) \\ &= O_N\left(z^{16} X^{1/2} \left(\log z + \log X\right)\right).\end{aligned}$$

Thus,

$$S(\mathcal{A}) \ll_N \frac{X \log z}{z} + \frac{(\log z)^2 X \log X}{z^2} + z^6 \left(z^{16} X^{1/2} \left(\log z + \log X\right)\right).$$

We choose $z := X^{1/46}$, which yields $S(\mathcal{A}) \ll_N X^{45/46} \log X$. □

4.3.2 Under GRH + AHC.

Let the notation be as above. Under GRH and AHC, for $X \gg 0$, Theorem 3.1.4 yields

$$\begin{aligned}\max R_{lq}(X) &= O\left(\max_{L=L_{lq}}(\#C)^{1/2}X^{1/2}\left(\log M(L/\mathbb{Q})+\log X\right)\right)\\ &= O\left(z^8X^{1/2}\left(\log(z^2N)+\log X\right)\right)\\ &= O_N\left(z^8X^{1/2}\left(\log z+\log X\right)\right)\end{aligned}$$

and thus

$$S(\mathcal{A}) \ll_N \frac{X\log z}{z}+\frac{(\log z)^2X\log X}{z^2}+z^6\left(z^8X^{1/2}\left(\log z+\log X\right)\right).$$

We choose $z := X^{1/30}$, which yields $S(\mathcal{A}) \ll_N X^{29/30}\log X$. □

4.3.3 Under GRH + AHC + PCC.

Let the notation be as above. Under GRH, AHC, and PCC, for $X \gg 0$, Theorem 3.1.4 yields

$$\begin{aligned}\max R_{lq}(X) &= O\left(\max(\#C)^{1/2}X^{1/2}\left(\frac{\#\widetilde{G}}{\#G}\right)^{1/4}\left(\log M(L/\mathbb{Q})+\log X\right)\right)\\ &= O\left(z^8X^{1/2}\left(\frac{\max\#\widetilde{\mathrm{GSp}_4\,\mathbb{Z}/lq\mathbb{Z}}}{z^{20}}\right)^{1/4}\left(\log(z^2N)+\log X\right)\right)\end{aligned}$$

Thus, with Lemma (3.7.3),

$$\begin{aligned}\max R_{lq}(X) &= O\left(z^8X^{1/2}\left(\frac{z^6}{z^{20}}\right)^{1/4}\left(\log(z^2N)+\log X\right)\right)\\ &= O_N\left(z^{9/2}X^{1/2}(\log z+\log X)\right)\end{aligned}$$

and thus

$$S(\mathcal{A}) \ll_N \frac{X \log z}{z} + \frac{(\log z)^2 X \log X}{z^2} + z^6 \left(z^{9/2} X^{1/2} (\log z + \log X) \right).$$

We choose $z := X^{1/23}$, which yields $S(\mathcal{A}) \ll_N X^{22/23} \log X$. □

4.3.4 Unconditionally.

Let the notation be as above. We recall part 4 of Theorem 3.1.4. Unconditionally, there exist constants $A, B, B' > 0$ such that when

$$\log X \geq B'(\#G) \left(\log |d_L| \right)^2,$$

we have

$$R(X) \ll \frac{\#C}{\#G} \operatorname{li} \left(X \exp \left(-B \frac{\log X}{\max\{ |d_L|^{1/n_L}, \log |d_L| \}} \right) \right) \tag{4.21}$$

$$+ (\#\tilde{C}) X \exp \left(-A \sqrt{\frac{\log X}{n_L}} \right). \tag{4.22}$$

We recall Lemma (3.1.6), which states

$$\frac{n_L}{2} \sum_{p \in \mathcal{P}(L/\mathbb{Q})} \log p \leq \log |d_L| \leq (n_L - 1) \sum_{p \in \mathcal{P}(L/\mathbb{Q})} \log p + n_L \log n_L.$$

Thus, by arguments identical as in Subsection 4.2.4,

$$\log |d_L| \ll_N z^{22} \log z; \qquad \log |d_L| \gg_N z^{22} \log z;$$

$$|d_L|^{1/n_L} \gg z; \qquad |d_L|^{1/n_L} \ll_N z^{24}$$

so that $\max\{\,|d_L|^{1/n_L}\,, \log|d_L|\} \ll_N z^{24}$. We see that the requirement

$$\log X \geq B'(\#G)\left(\log|d_L|\right)^2 \asymp_N B' z^{66}(\log z)^2 \tag{4.23}$$

is satisfied with the choice

$$z := c' \frac{(\log X)^{1/66}}{(\log\log X)^{1/33}}$$

for a certain positive constant c' depending only on N. The reader may check that there exists such a c' so that 4.23 is satisfied with this choice of z.

For $l, q \in \mathcal{P}$, arguments above show that

$$\frac{\#C}{\#\,\mathrm{GSp}_4\,\mathbb{Z}/lq\mathbb{Z}} \ll z^{-6}.$$

Using the approximation $\mathrm{li}\, t \sim \frac{t}{\log t}$, we then have

$$\begin{aligned}
\frac{\#C}{\#G}\,\mathrm{li}\left(X\exp\left(-B\frac{\log X}{\max\{\,|d_L|^{1/n_L}\,,\log|d_L|\}}\right)\right) &\ll z^{-6}\frac{\left(X\exp\left(-B\frac{\log X}{\max\{\,|d_L|^{1/n_L},\log|d_L|\}}\right)\right)}{\log\left(X\exp\left(-B\frac{\log X}{\max\{\,|d_L|^{1/n_L},\log|d_L|\}}\right)\right)} \\
&\ll_N \frac{z^{-6}X\exp\left(-B\frac{\log X}{z^{22}\log z}\right)}{\log X - B(\log X)z^{-1/2}} \\
&\ll \frac{X^{1-Bz^{-22}(\log z)^{-1}}}{z^6\log X}
\end{aligned}$$

From our choice of z, the bound of (4.21), the bounds above, and the weak bound $\#\widetilde{C} \leq \#\widetilde{\mathrm{GSp}_4\,\mathbb{Z}/lq\mathbb{Z}} \asymp z^6$, we obtain (after another calculation that we omit;

see Section 4 of [CFM05]) the bounds

$$\max_{\substack{l,q\in\mathcal{P}\\ l\neq q}}\left|\sum_{\alpha\in\mathcal{A}}\left(\frac{\alpha}{lq}\right)\right| \ll_N \frac{X}{z^8\log X};$$

$$\sum_{\alpha\in\mathcal{A}}\sum_{\substack{l\in\mathcal{P}\\ (\alpha,l)\neq 1}} 1 \ll_N \frac{X}{\log X}\nu_z(d);$$

$$\sum_{\alpha\in\mathcal{A}}\left(\sum_{\substack{l\in\mathcal{P}\\ (\alpha,l)\neq 1}} 1\right)^2 \ll_N \frac{X}{\log X}\left(\nu_z(d)+\nu_z(d)^2\right);$$

where $\nu_z(d)$ is the number of distinct prime divisors of d less than or equal to z. Thus, from the Square Sieve and the trivial bounds $\nu_z(d)\leq\nu(d)$ and $\nu_z(d)\leq\pi(z)$ we obtain

$$S(\mathcal{A}) \ll_N \frac{X\log z}{z\log X}(1+\nu(d)) \ll_N \frac{X(\log\log X)^{23/22}}{(\log X)^{67/66}}(1+\nu(d)). \tag{4.24}$$

□

4.4 Proof of Corollaries 4.1.4, 4.1.5, and 4.1.6

The proofs for Corollaries 4.1.4 and 4.1.5 are nearly identical, so for brevity we only prove the former. We mimic the argument based on the Pigeonhole Principle in [CFM05].

We recall that, if p is a good ordinary non-split prime for A, then $d(\mathbb{Q}(\pi_p)/\mathbb{Q})$ has squarefree part dividing the number γ_p defined in (4.3). Moreover, the functions $\psi_g(\sqrt{X})$ were defined precisely so that $\left|\gamma_p\right|\leq\psi_g(\sqrt{X})$ when $p\leq X$. In Section 4.1, we defined the field-counting function,

$$\mathcal{D}_A(X) \coloneqq \left\{K\in\mathcal{D}_A \;\middle|\; \mathrm{sf}(d(K/\mathbb{Q}))\leq\psi_g(\sqrt{X})\right\}$$

so that if p is good ordinary non-split for A, then $p \leq X$ implies $\mathbb{Q}(\pi_p) \in \mathcal{D}_A(X)$.

Now, note that because A has *trivial* geometric endomorphism algebra, the set of non-split primes for A has density zero (see Subsection 2.5). Thus, assuming that the set of ordinary primes for A has positive density δ, we may write

$$\begin{aligned}\pi(X) &= (1-\delta)\pi(X) + o(\pi(X)) + \sum_{K \in \mathcal{D}_A(\infty)} \Pi(A,K)(X) \\ &= (1-\delta+o(1))\pi(X) + \sum_{K \in \mathcal{D}_A(X)} \Pi(A,K)(X)\end{aligned}$$

and thus obtain

$$\#\mathcal{D}_A(X) \geq \frac{(\delta - o(1))\pi(X)}{\max_{K \in \mathcal{D}_A(X)} \Pi(A,K)} \tag{4.25}$$

Plugging in the various conditional asymptotic upper bounds of Theorem 4.1.2 on $\Pi(A,K)(X)$ yields the conditional asymptotic lower bounds of Corollary 4.1.4.

Unfortunately, the dependency in $d(K/\mathbb{Q})$ of the unconditional bound for $\Pi(A,K)(X)$ keeps this argument from working in the unconditional case. But to prove Corollary 4.1.6, we argue as follows. By Theorem 4.1.1, we know that each set $\Pi(A,K)$ has density zero in the set of rational primes. Yet the set of primes at which A has good, ordinary, non-split reduction is assumed to have positive density. Thus, there must be infinitely many CM fields K for which $\Pi(A,K) \neq \emptyset$. □

Remark 4.4.1. *We hesitate to give precise conjectures on the asymptotic growth (or boundedness) of the functions $\Pi(A,K)(X)$ and $\Pi(A,F)(X)$ because the heuristic is less clear. We have run small-scale experiments; as an example, let $C/\mathbb{Q}$ be the curve of genus 2 with affine model $y^2 = x^5 - 3x^4 + 2x^3 + 1$, and let $A/\mathbb{Q}$ be the Jacobian of C. (C is the curve 3680.a.29440.1 of [LMFDB].) Since A is an abelian surface*

without extra endomorphisms, its adelic Galois representation has open image in $\mathrm{GSp}_4\widehat{\mathbb{Z}}$*, so our results apply to* A*. We found via a simple program written in Sage [SageMath] that, in fact,* $\Pi(A,K)(10^6) \leq 1$ *for all* K*.*

Chapter 5: Almost-Prime Order Question

5.1 Statement of Results

We continue to let $A/\mathbb{Q}$ be a principally polarized abelian variety of dimension $g \geq 1$ with conductor N and adelic Galois representation $\widehat{\rho} : G_{\mathbb{Q}} \to \mathrm{GSp}_{2g}\widehat{\mathbb{Z}}$. As previously, we will call A **generic** if the image of $\widehat{\rho}$ is open in $\mathrm{GSp}_{2g}\widehat{\mathbb{Z}}$.

Following the argument of [DW12], we use the error bounds of the explicit Chebotarev Density Theorems (see Chapter (REF)) along with the weighted Greaves sieve (see Section 3.4) and find the following.

Theorem 5.1.1. *Suppose that A is generic and that*

(Triv_A)*: all of the abelian varieties over $\mathbb{Q}$ that are $\mathbb{Q}$-isogenous to A have trivial rational torsion.*

Assume the θ-Hypothesis for the division fields of A (i.e., for $\mathbb{Q}(A[n])/\mathbb{Q}$ for all n).[1] *Then, for $x \gg_A 0$,*

$$\#\left\{p \leq x \;\middle|\; \#A_p\left(\mathbb{F}_p\right) = P_r\right\} \geq B \cdot C_A \frac{x}{(\log x)^2}$$

[1] In fact, we only require the θ-Hypothesis for $\mathbb{Q}(A[n])/\mathbb{Q}(A[n])^{B(n)}$, where $B(n)$ is a Borel subgroup of the Galois group of $\mathbb{Q}(A[n])/\mathbb{Q}$. We simplified the hypotheses here for the sake of readability.

where B is an explicit, absolute positive constant depending only on g, C_A is an explicit non-negative constant depending on the Galois representation $\widehat{\rho}$ of A (see (5.4)), and

$$r = r(g,\theta) := \left\lceil \frac{(9/2)g^3 + (1/2)g}{1-\theta} - \frac{1}{3} \right\rceil.$$

The utility of Theorem 5.1.1 is maximized once θ is small enough that $r(g,\theta) = r(g,1/2) = 9g^3 + g$; thus, we obtain

Corollary 5.1.2. *Assume the hypotheses of Theorem 5.1.1, with*

$$\theta = 1 - \frac{(9/2)g^3 + (1/2)g}{9g^3 + g + 1/3}.$$

Then, for $x \gg_A 0$,

$$\#\left\{ p \leq x \;\middle|\; \#A_p\left(\mathbb{F}_p\right) = P_{9g^3+g} \right\} \geq B \cdot C_A \frac{x}{(\log x)^2}.$$

Theorem 5.1.3. *Suppose that A is generic. Assume the θ-Hypothesis for the division fields of A. Then, for all $\epsilon > 0$, for $x \gg_{A,\theta,\epsilon} 0$,*

$$\#\left\{ p \leq x \;\middle|\; \#A_p\left(\mathbb{F}_p\right) \text{ is prime} \right\} \leq \left(\frac{2g^2 + 3g + 6}{1-\theta} + \epsilon \right) C_A \frac{x}{(\log x)^2}.$$

The constant C_A is defined in (5.4) as an Euler product in terms of certain conjugacy classes attached to the Galois representation $\widehat{\rho}$. The assumption (Triv_A) ensures that there is no "obvious" reason for all of the orders $\#A_p\left(\mathbb{F}_p\right)$ to share a common factor. We then understand there to be "congruence obstructions" to $\#A_p\left(\mathbb{F}_p\right)$ being prime infinitely often when $C_A = 0$. This possibility is the reason for the refinement by Zywina [Zyw11] of the constant C_E for elliptic curves E.

We lastly follow the argument of Y.-R. Liu [Liu06], generalizing the Erdös-Kac Theorem, to show that $\#A_p(\mathbb{F}_p)$ essentially follows a normal distribution with *normal order* $\log\log p$.

Theorem 5.1.4. *Suppose that A is generic. Assume the θ-Hypothesis for the division fields of A for some $\theta < 1$. Then, for all $\gamma \in \mathbb{R}$,*

$$\lim_{x\to\infty}\left(\frac{1}{\pi(x)}\#\left\{p \le x \;\middle|\; \frac{\omega(\#A_p(\mathbb{F}_p)) - \log\log p}{\sqrt{\log\log p}} \le \gamma\right\}\right) = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\gamma} e^{-t^2/2}\,\mathrm{d}t.$$

5.2 Preparations for the Proof of Main Results.

Let $A/\mathbb{Q}$ be a generic abelian variety of conductor N. Recall that p denotes a prime of good reduction for A, i.e., $p \nmid N$, and l denotes a prime. Let

$$\begin{aligned} M = M_A &:= \prod\left\{l \;\middle|\; \operatorname{im}\rho_{l^\infty} \neq \mathrm{GSp}_{2g}\,\mathbb{Z}_l\right\}; \\ \mathcal{A} &:= \left\{\#A_p(\mathbb{F}_p) \;\middle|\; p \le x,\ \gcd(\#A_p(\mathbb{F}_p), M) = 1\right\}; \\ \mathcal{P} &:= \left\{p \;\middle|\; p \nmid M\right\}. \end{aligned}$$

Here, $\mathcal{A}$ is a *list,* i.e., might have repetition. We choose to omit from $\mathcal{A}$ those orders not coprime to M so as to obtain the expected correction factor C_A during the sieving process.

Our goal will be, assuming the θ-Hypothesis, to show that for some choice of multiplicative function w, constants $U, V, \xi > 0$, and positive integer r, the hypotheses of Theorem 3.4.1 are satisfied; that

$$\text{right-hand side of (3.17)} \geq B \cdot C_A \frac{x}{(\log x)^2}, \tag{5.1}$$

for some constant $B > 0$; and that

$$\sum_{(x^\xi)^V \leq p < (x^\xi)^U} \#\mathcal{A}_{p^2} = o\left(\frac{x}{(\log x)^2}\right). \tag{5.2}$$

We will then choose such constants, depending on θ, that minimize r. Theorem 5.1.1 will then follow from Lemma 3.4.2 with the constants we have chosen. After these computations, Theorem 5.1.3 will follow from the Selberg linear sieve, and Theorem 5.1.4 will follow from Theorem 3.2.2.

5.2.1 Divisibility of $\#A_p(\mathbb{F}_p)$

We recall some well-known facts about the Galois representations of A and A_p. As in Section 3.5, for each l we fix a $\mathbb{Z}_l$-basis of the l-adic Tate module of A and of A_p that is symplectic with respect to the Weil pairing. (For our purposes, we need not require any compatibility between these bases.) Thus, we may consider the l-adic Galois representations of A and A_p as taking values in $\mathrm{GSp}_{2g}(\mathbb{Z}_l)$.

Let $\pi_p \in \mathrm{End}\left(A_p\right)$ denote the Frobenius endomorphism. Recall the well-known theorem which states that for any abelian variety B over a field κ, the restriction map $\mathrm{End}(B) \to \mathrm{End}_{\mathbb{Z}_l} T_l B$ is *injective.* Thus, we may consider π_p as an element of $\mathrm{GSp}_{2g}(\mathbb{Z}_l)$.

Theorem 5.2.1 (Weil Conjectures [Wei49; Gro66; Del73])**.** *The characteristic polynomial of $\pi_p \in \mathrm{GSp}_{2g}\mathbb{Z}_l$ has integer coefficients and is independent of l. Moreover,*

the eigenvalues of π_p *are* p-***Weil numbers***. *That is, all their embeddings into* $\mathbb{C}$ *have norm* $\sqrt{p}$.

Thus, the characteristic polynomial of π_p has the form

$$\mathrm{char}_{\pi_p}(x) = x^{2g} + a_1 x^{2g-1} + \ldots + a_g x^g + p a_{g-1} x^{g-1} + p^2 a_{g-2} x^{g-2} + \ldots + p^g.$$

From now on, we consider Galois representations over $\kappa = \mathbb{Q}$. The following well-known lemma will allow us to detect information about A_p from global information on A.

Lemma 5.2.2. *The conjugacy class of* π_p *in* $\mathrm{GSp}_{2g}(\mathbb{Z}_l)$ *is* $\rho_{l^\infty}(\mathrm{Frob}_p)$. *In particular,* $\mathrm{char}_{\pi_p} = \mathrm{char}_p$.

From Lemma 5.2.2 and the observation that $\#A_p(\mathbb{F}_p) = \deg(\pi_p - \mathrm{id}_A) = \mathrm{char}_p(1)$, we immediately see that

Lemma 5.2.3. *For any* $n \geq 1$, $n \,\Big|\, \#A_p(\mathbb{F}_p) \iff \mathrm{char}_{\rho_n(\mathrm{Frob}_p)}(1) \equiv 0 \bmod n$.

We are thus led to consider

Definition 5.2.4.

$$C(n) := \left\{ g \in \mathrm{Gal}(\mathbb{Q}(A[n])/\mathbb{Q}) \;\middle|\; \mathrm{char}_g(1) \equiv 0 \right\}, \tag{5.3}$$

so that, for $p \leq x$ such that $(\#A_p(\mathbb{F}_p), M) = 1$,

$$\#A_p(\mathbb{F}_p) \in \mathcal{A}_n \iff \rho_n(\mathrm{Frob}_p) \in C(n).$$

For convenience, for $n \geq 1$, set

Notation 5.2.5. $L_n := \mathbb{Q}(A[n])$, *and* $G(n) := \mathrm{Gal}(L_n/\mathbb{Q})$.

5.2.2 Setting up the sieve

We recall that the hypotheses of Theorem (3.4.1) require an approximation X to $\#\mathcal{A}$ and a multiplicative function w such that the "remainders" $r(\mathcal{A}, d)$ are small.

Mimicking the argument of David-Wu, we see that for squarefree d that are supported on $\mathcal{P}$,

$$\begin{aligned}
\#\mathcal{A}_d &= \sum \left\{ 1 \;\middle|\; p \le x, (\#A_p(\mathbb{F}_p), M_A) = 1, d \mid \#A_p(\mathbb{F}_p) \right\} \\
&= \sum_{m \mid M_A} \mu(m) \cdot \sum \left\{ 1 \;\middle|\; p \le x, dm \mid \#A_p(\mathbb{F}_p) \right\} \\
&= \sum_{m \mid M_A} \mu(m) \cdot \pi_{C(dm)}(x, L_{dm}/\mathbb{Q}) \\
&= \sum_{m \mid M_A} \mu(m) \cdot \# \left\{ p \le x \;\middle|\; \rho_d(\mathrm{Frob}_p) \subseteq C(d), \rho_m(\mathrm{Frob}_p) \subseteq C(m) \right\} \\
&\sim \mathrm{li}(x) \frac{\#C(d)}{\#G(d)} \sum_{m \mid M_A} \left(\mu(m) \frac{\#C(m)}{\#G(m)} \right) \\
&= \mathrm{li}(x) \frac{\#C(d)}{\#G(d)} \cdot \left(1 - \frac{\#C'(M_A)}{\#G(M_A)} \right)
\end{aligned}$$

where

$$C'(M_A) \coloneqq \left\{ g \in G(M_A) \;\middle|\; (\mathrm{char}_g(1), M_A) \neq 1 \right\}.$$

Thus, we choose

$$w(d) \coloneqq \begin{cases} \frac{d \cdot \#C(d)}{\#G(d)} & d \text{ is supported on } \mathcal{P}; \\ 0 & \text{otherwise;} \end{cases} \qquad X \coloneqq \mathrm{li}(x) \left(1 - \frac{\#C'(M_A)}{\#G(M_A)} \right).$$

Then, w is clearly multiplicative because of our assumption on $\widehat{\rho}$ and the Chinese Remainder Theorem. From these choices, the constant C_A produced in the proof of 5.1.1 will then be

$$C_A = \left(1 - \frac{\#C'(M_A)}{\#G(M_A)}\right) \lim_{y\to\infty} \left(\frac{V(y)}{\prod_{l<y}(1-1/l)}\right) \tag{5.4}$$

$$= \frac{1 - \#C'(M_A)/\#G(M_A)}{\prod_{l|M_A}(1-1/l)} \prod_{l\nmid M_A} \frac{1-\#C(l)/G(l)}{1-1/l}. \tag{5.5}$$

In order to show that w satisfies the hypothesis (3.12), to find bounds on the remainders (3.13), and to show the bound (5.2), we will bound various Chebotarev densities, as well as find a bound on the size of $\#C(d)$. In the next subsection, before we begin computations, we describe a refinement of this argument, which we will use.

5.2.3 Exploiting subgroups of GSp_{2g}

Using lemmas from [Ser81], David-Wu exploit the Borel and unipotent subgroups of GL_2 and compare the prime counting functions for a Galois extension and a subextension to find the following.

Theorem 5.2.6 ([DW12], Thm. 3.7)**.** *Let L/K be a Galois extension of number fields and $G = \mathrm{Gal}(L/K)$. Let $H \leq G$ and $C \subset G$ a union of conjugacy classes that intersects H. Let C_H be the union of (H-)conjugacy classes in H generated by $C \cap H$. Then,*

$$\pi_C(x, L/K) = \frac{|H|}{|G|}\frac{|C|}{|C_H|}\pi_{C_H}(x, L/L^H) + O\left(\frac{|C|}{|C_H|\cdot|G|}\log d_L + \frac{|H|}{|G|}\frac{|C|}{|C_H|}[L^H:\mathbb{Q}]x^{1/2} + [K:\mathbb{Q}]x^{1/2}\right).$$

Their idea (for $g = 1$) is to find subextensions

$$L_l^{H'(d)} \subset L_d^{H(d)} \subset L_d$$

where Theorem 5.2.6 applies to the extension $L_d^{H'(d)} \subset L_d$, and the second part of Theorem 3.1.4 applies to the subextension $L_d^{H'(d)} \subset L_d^{H(d)}$.

For this, they consider the subextensions

$$L_d^{B(d)} \subset L_d^{U(d)} \subset L_d$$

where $B(d)$ is the Borel subgroup of upper-triangular matrices in $\mathrm{GL}_2(\mathbb{Z}/d\mathbb{Z})$, and $U(d)$ is the subgroup of unipotent upper triangular matrices. Then,

$$B(d)/U(d) \cong \mathrm{Gal}\left(L_d^{U(d)}/L_d^{B(d)}\right)$$

is abelian, so AHC holds true in that extension. Thus, the second part of Theorem 3.1.4 applies to $L_d^{U(d)}/L_d^{B(d)}$.

We make preparations here to use the same idea in the setting of $g > 1$. *For the rest of this Section, we assume that* $G(d) = \mathrm{GSp}_{2g}\left(\mathbb{Z}/d\mathbb{Z}\right)$.

Notation 5.2.7. *We set:*

- $B(d)$ *to be the (standard) Borel subgroup of* $G(d)$*, namely the subgroup of upper triangular matrices in* $G(d)$*;*
- $U(d) \triangleleft B(d)$ *to be the subgroup of unipotent matrices in* $B(d)$*;*
- $C_B(d) \coloneqq B(d) \cap C(d)$.

We will also need to break up $G(d)$ into multiplicator cosets. Recall that for a commutative ring R with unity,

$$\mathrm{GSp}_{2g}(R) \coloneqq \left\{ M \in \mathrm{GL}_{2g}(R) \;\middle|\; \exists \mu \in R^\times \text{ s.t. } M^t J M = \mu J \right\}$$

where $J = \begin{pmatrix} 0 & I_g \\ -I_g & 0 \end{pmatrix}$ is the matrix for the standard symplectic form. We call the assignment $M \mapsto \mu$ the **multiplicator character** of GSp_{2g}, and there is the exact sequence

$$1 \to \mathrm{Sp}_{2g}(R) \to \mathrm{GSp}_{2g}(R) \xrightarrow{\mu} R^\times \to 1. \tag{5.6}$$

For $m \in R^\times$, we define the **m-symplectic matrices,**

$$\mathrm{GSp}_{2g}^{(m)}(R) \coloneqq \mu_R^{-1}(m)$$

and use the notation

$$G^{(m)}(d) \coloneqq \mathrm{GSp}_{2g}^{(m)}(\mathbb{Z}/d\mathbb{Z}).$$

Now, we have the well-known

Lemma 5.2.8. *The characteristic polynomial of M has the form*

$$\mathrm{char}_M(x) = x^{2g} + a_1 x^{2g-1} + \ldots + a_g x^g + m a_{g-1} x^{g-1} + m^2 a_{g-2} x^{g-2} + \ldots + m^g$$

for some $a_i \in R$ and $m \in R^\times$.

Thus, $B(d)/U(d)$ is the torus whose elements have coset representatives the diagonal matrices in $G(d)$ of the form $\begin{pmatrix} D & 0 \\ 0 & mD^{-1} \end{pmatrix}$ for a $g \times g$ invertible diagonal matrix D, so that $B(d)/U(d) \cong \left(\mathbb{G}_m(\mathbb{Z}/d\mathbb{Z})\right)^g \times \mathbb{G}_m(\mathbb{Z}/d\mathbb{Z})$. In particular,

$B(d)/U(d)$ is abelian, so that, now in the context of $g \geq 1$, AHC holds true in the extension $L_d^{U(d)}/L_d^{B(d)}$. Therefore, by Theorem 3.1.5, we have

Corollary 5.2.9. *Assume the θ-Hypothesis for the extensions $L_n/L_n^{B(n)}$. Then,*

$$\pi_{C_B(n)}(x, L_n/L_n^{B(n)}) = \frac{\#C_B(n)}{\#B(n)}\,\mathrm{li}(x) + R_n(x)$$

where

$$R_n(x) \ll \left(\frac{\#C_B(n)}{\#U(n)}\right)^{1/2} (\#B(n)) \cdot x^{\theta} \left(\log(M(L_n/L_n^{B(n)})) + \log x\right).$$

5.2.4 Fitting together the prime-counting estimates

In this subsection, we combine the discussion of Subsection 5.2.3 and the explicit Chebotarev Density Theorem. Using Theorem 5.2.6 with $G = G(n)$, $H = B(n)$, $C = C(n)$, $C_H = C_B(n)$, and $K = \mathbb{Q}$, we have

$$\pi_{C(n)}(x, L_n/\mathbb{Q}) = \frac{\#B(n)}{\#G(n)}\frac{\#C(n)}{\#C_B(n)}\pi_{C_B(n)}(x, L_n/L_n^{B(n)}) + Q_n(x)$$

where

$$Q_n(x) \ll \frac{\#C(n)}{\#C_B(n)\cdot\#G(n)}\log d_{L_n} + \frac{\#B(n)}{\#G(n)}\frac{\#C(n)}{\#C_B(n)}[L_n^{B(n)} : \mathbb{Q}]x^{1/2} + x^{1/2}. \quad (5.7)$$

Plugging Corollary 5.2.9 into the above and canceling factors, we have

$$\pi_{C(n)}(x, L_n/\mathbb{Q}) = \frac{\#C(n)}{\#G(n)}\,\mathrm{li}(x) + \frac{\#B(n)}{\#G(n)}\frac{\#C(n)}{\#C_B(n)}R_n(x) + Q_n(x) \quad (5.8)$$

where R_n and Q_n have their respective bounds as above (with the bound on R_n assuming the θ-Hypothesis).

5.2.5 Counting matrices

In this subsection, we compute and gather estimates on the sizes of the subsets of $G(d)$ (and their ratios) that have appeared. *We maintain the assumption that* $G(d) = \mathrm{GSp}_{2g}\left(\mathbb{Z}/d\mathbb{Z}\right)$.

To begin, there is the well known formula

$$\#\,\mathrm{Sp}_{2g}\,\mathbb{F}_l = l^{g^2}\prod_{i=1}^{g}\left(l^{2i}-1\right) = l^{2g^2+g} - l^{2g^2+g-2} + O_g\left(l^{2g^2+g-6}\right). \tag{5.9}$$

From this and the exact sequence (5.6), we have

$$\#G(l) = (l-1)l^{g^2}\prod_{i=1}^{g}\left(l^{2i}-1\right) = l^{2g^2+g+1} - l^{2g^2+g} + O_g\left(l^{2g^2+g-1}\right). \tag{5.10}$$

Recall Definition (5.3). For convenience, for an integer m, denote

$$C^{(m)}(d) \coloneqq C(d) \cap G^{(m)}(d).$$

From Castryck et al. [Cas+12], we have

Proposition 5.2.10.

$$\frac{\#C^{(m)}(l)}{\#G^{(m)}(l)} = \begin{cases} -\sum_{r=1}^{g} l^r \prod_{j=1}^{r}(1-l^{2j})^{-1} & \text{if } l \mid m-1, \\ -\sum_{r=1}^{g} \prod_{j=1}^{r}(1-l^{j})^{-1} & \text{otherwise.} \end{cases}$$

Thus,

$$\begin{aligned}
\#C(l) &= \sum_{m\in(\mathbb{Z}/l\mathbb{Z})^\times} \frac{\#C^{(m)}(l)}{\#G^{(m)}(l)}\#G^{(m)}(l) \\
&= \sum_{m\in(\mathbb{Z}/l\mathbb{Z})^\times} \frac{\#C^{(m)}(l)}{\#G^{(m)}(l)}\cdot\frac{\#G(l)}{l-1} \\
&= \frac{\#G(l)}{l-1}\cdot\left(-\sum_{r=1}^{g} l^r \prod_{j=1}^{r}(1-l^{2j})^{-1} + (l-2)\left(-\sum_{r=1}^{g}\prod_{j=1}^{r}(1-l^j)^{-1}\right)\right) \qquad (5.11)
\end{aligned}$$

$$= l^{2g^2+g} - 3l^{2g^2+g-2} + O_g(l^{2g^2+g-3}) \qquad (5.12)$$

When $g = 1$, (5.11) yields $\frac{\#C(l)}{\#G(l)} = \frac{l^2-2}{(l-1)(l^2-1)}$, which agrees with the density written in David-Wu.

Next, we count $\#B(l)$. Since

$$B(l) = \left\{ M \in \mathrm{GL}_{2g}\,\mathbb{Z}/l\mathbb{Z} \;\middle|\; M \text{ upper triangular, } M \in \mathrm{GSp}_{2g}\,\mathbb{Z}/l\mathbb{Z} \right\},$$

then $B(l)$ consists of $M = \begin{pmatrix} T_1 & A \\ 0 & T_2 \end{pmatrix}$ with T_i upper-triangular, such that for some μ,

$$\begin{pmatrix} T_1 & A \\ 0 & T_2 \end{pmatrix}^t J \begin{pmatrix} T_1 & A \\ 0 & T_2 \end{pmatrix} = \mu J,$$

i.e.

$$T_1^t T_2 = \mu I, \qquad A^t T_2 = T_2^t A;$$

i.e.

$$T_2 = \mu \left(T_1^t\right)^{-1}; \qquad A = \mu^{-1} T_1 R$$

for some symmetric matrix R. That is,

$$B(l) = \left\{ \begin{pmatrix} T & \mu^{-1}RT^t \\ 0 & \mu^{-1}(T^t)^{-1} \end{pmatrix} \right\} \tag{5.13}$$

and thus

$$\begin{aligned} \#B(l) &= (l-1)\left((l-1)^g \cdot l^{g(g-1)/2}\right)\left(l^{g(g+1)/2}\right) \\ &= (l-1)^{g+1} \cdot l^{g^2}, \end{aligned}$$

and $\#U(l) = l^{g^2}$. From this description we also see that

$$\frac{\#C_B(l)}{\#B(l)} = 1 - \frac{\#\left\{(T,\mu) \;\middle|\; T \text{ does not have 1 as an eig.val., } \mu^{-1} \notin \{\text{eig.vals. of } T\}\right\}}{\#\{(T,\mu)\}}$$

so that

$$\begin{aligned} \frac{\#C_B(l)}{\#B(l)} &\leq 1 - \frac{\#\left\{T \;\middle|\; T \text{ does not have 1 as an eig.val.}\right\} \cdot (l-1-g)}{(l-1)^{g+1} \cdot l^{g(g-1)/2}}; \\ \frac{\#C_B(l)}{\#B(l)} &\geq 1 - \frac{\#\left\{T \;\middle|\; T \text{ does not have 1 as an eig.val.}\right\} \cdot (l-2)}{(l-1)^{g+1} \cdot l^{g(g-1)/2}} \end{aligned}$$

and thus

$$1 - \frac{(l-2)^g(l-2)}{(l-1)^{g+1}} \leq \frac{\#C_B(l)}{\#B(l)} \leq 1 - \frac{(l-2)^g(l-1-g)}{(l-1)^{g+1}} \tag{5.14}$$

so that $\#C_B(l)/\#B(l) \asymp_g 1/l$.

We also record here for future use that, by the same reasoning,

$$1 - \frac{(l^2-l-1)^g(l^2-l-2)}{(l^2-l)^{g+1}} \leq \frac{\#C_B(l^2)}{\#B(l^2)} \leq 1 - \frac{(l^2-l-1)^g(l^2-l-g)}{(l^2-l)^{g+1}}$$

so that $\#C_B(l^2)/\#B(l^2) \asymp_g 1/l$.

Next, $\#C(l^2)$. It will suffice for our purposes to have an upper bound on $\frac{\#C(l^2)}{\#G(l^2)}$.

Lemma 5.2.11. $\dfrac{\#C(l^2)}{\#G(l^2)} = O_g\left(\dfrac{1}{l^2}\right)$.

Proof. We write

$$\frac{\#C(l^2)}{\#G(l^2)} = \frac{\#C(l^2)}{\#C(l)} \cdot \frac{\#C(l)}{\#G(l)} \cdot \frac{\#G(l)}{\#G(l^2)}$$

Now, consider the mod-l reduction map, which is surjective by Hensel's Lemma (see, e.g., pg. 177 of [Mum99]):

$$1 \to K \to \mathrm{GSp}_{2g}\,\mathbb{Z}/l^2\mathbb{Z} \overset{\phi_l}{\twoheadrightarrow} \mathrm{GSp}_{2g}\,\mathbb{Z}/l\mathbb{Z} \to 1,$$

where

$$K = \left(I + l \cdot M_{g\times g}(\mathbb{Z}/l^2\mathbb{Z})\right) \cap \mathrm{GSp}_{2g}\,\mathbb{Z}/l^2\mathbb{Z}.$$

Then, $\#G(l)/\#G(l^2) = 1/\#K$. From earlier discussion, we also have that $\#C(l)/\#G(l) = O_g(1/l)$.

It remains to bound $\frac{\#C(l^2)}{\#C(l)}$. Note that $C(l^2) \subset \phi_l^{-1}(C(l))$, so in particular the product $K \cdot C(l^2) \subset \phi_l^{-1}(C(l))$. We show that

$$\#C(l^2) \leq \frac{2g}{l}\#\left(K \cdot C(l^2)\right) \leq \frac{2g}{l}\#K \cdot \#C(l);$$

the second inequality is obvious.

Consider the subgroup of scalar matrices $S \coloneqq \left((1 + l\mathbb{Z})/l^2\mathbb{Z}\right) \cdot I \subset K$. For $\alpha I \in S$ and $M \in C(l^2)$, the product αM is in $C(l^2)$ only when one of the eigenvalues,

say β, of M is such that $\alpha\beta \equiv 1 \bmod l^2$. But since $\alpha \in (1 + l\mathbb{Z})/l^2\mathbb{Z}$, the equation $\alpha\beta \equiv 1 \bmod l^2$ has only one solution β.

Thus, accounting for the possible multiplicity of the eigenvalues of M, we have

$$\#S\{M\} \cap C(l^2) \leq 2g.$$

So, partition $C(l^2)$ into subsets of orbits under S; that is, form the set

$$C(l^2)/S := \left\{ SM \cap C(l^2) \;\middle|\; M \in C(l^2) \right\}.$$

Then, $\#C(l^2)/S \geq \#C(l^2)/2g$, so that

$$\#\left(S \cdot C(l^2)\right) = \#S \cdot \#\left(C(l^2)/S\right) \geq \frac{l}{2g}\#C(l^2).$$

But certainly $\#\left(K \cdot C(l^2)\right) \geq \#\left(S \cdot C(l^2)\right)$, and thus the desired inequality follows. □

Lastly, we record the following formulas. A short proof of the first formula is given in `https://mathoverflow.net/questions/87904`. We will only use this formula in the case $k = 2$. The proof of the second formula is clear from (5.13).

Lemma 5.2.12.

$$\#G(l^k) = (l-1)l^{(2k-1)g^2+(k-1)g+1}\prod_{i=1}^{g}(l^{2i}-1). \qquad \#B(l^2) = (l-1)^{g+1}l^{2g^2+g+1}.$$

5.2.6 Verifying the sieve hypothesis (3.12)

We now verify hypothesis (3.12). Recall that we defined

$$w(d) := \begin{cases} \frac{d\cdot\#C(d)}{\#G(d)} & d \text{ is supported on } \mathcal{P}; \\ 0 & \text{otherwise;} \end{cases}$$

.

From (5.11), we have

$$\frac{w(l)}{l} = \frac{1}{l} + O_g\left(\frac{1}{l^2}\right)$$

so that for $z_1 < z_2$,

$$\begin{aligned}\left|\sum_{z_1 \le l < z_2,\ l\in\mathcal{P}} \frac{w(l)}{l}\log l - \log\frac{z_2}{z_1}\right| &= \left|\sum_{z_1 \le l < z_2,\ l\in\mathcal{P}} \left(\frac{1}{l} + O_g\left(\frac{1}{l^2}\right)\right)\log l - \log\frac{z_2}{z_1}\right| \\ &= \left|\sum_{z_1 \le l < z_2,\ l\in\mathcal{P}} \frac{1}{l}\log l - \log\frac{z_2}{z_1}\right| + \left|\sum_{l\in\mathcal{P}} O_g\left(\frac{1}{l^2}\right)\log l\right|.\end{aligned}$$

By the comparison test for series, the second term is $O_g(1)$. Recall now one of Mertens' theorems,

Theorem 5.2.13 ([Mer74])**.** *For all $n \ge 2$,*

$$\left|\sum_{l\le n}\frac{\log(l)}{l} - \log(n)\right| \le 2$$

Thus, via the Triangle Inequality, hypothesis (3.12) is verified, so that Theorem (3.4.1) applies, and so for any valid choice of constants, the lower bound (3.17) holds.

5.3 Proof of Main Results.

We now combine the estimates of this section and the theorems of Section 3.1 in order to show the existence of constants U, V, ξ, r that guarantee the lower bound (5.1) and the upper bound (5.2). We will box the constraints on the constants as we determine them.

First, the hypothesis of Lemma 3.4.2 that $\max \mathcal{A} \le (x^{\xi})^{rU+V}$ requires, by earlier discussion, that $\boxed{g < \xi(rU+V).}$

5.3.1 Ensuring (5.1)

We begin with the lower bound (5.1). Recall that we wish to show that

$$X \cdot V(y) \cdot \frac{2e^{\gamma}}{U-V}\left(J(U,V) + O\left(\frac{\log\log\log y}{(\log\log y)^{1/5}}\right)\right) - (\log y)^{1/3}\left|\sum_{m<M,n<N,mn|P(y^U)} \alpha_m\beta_n \cdot r(\mathcal{A},mn)\right| \geq B \cdot C_A \cdot \frac{x}{(\log x)^2}$$

where

$$\begin{aligned}
X &:= \mathrm{li}(x)\left(1 - \frac{\#C'(M_A)}{\#G(M_A)}\right)\\
V(y) &:= \prod_{p\leq y, p\in\mathcal{P}}\left(1-\frac{w(p)}{p}\right),\\
C_A &:= \frac{1-\#C'(M_A)/\#G(M_A)}{\prod_{l|M_A}(1-1/l)}\prod_{l\nmid M_A}\left(\frac{1-\#C(l)/\#G(l)}{1-1/l}\right),\\
r(\mathcal{A},d) &:= \#\mathcal{A}_d - \frac{w(d)}{d}\cdot\left(1-\frac{\#C'(M_A)}{\#G(M_A)}\right)\mathrm{li}(x),\\
w(d) &:= \begin{cases} \frac{d\cdot\#C(d)}{\#G(d)} & d \text{ is supported on } \mathcal{P};\\ 0 & \text{otherwise;}\end{cases}
\end{aligned}$$

and $M, N, \alpha_m, \beta_n, \alpha(V), \beta(V)$ are as in previous notation.

As in Lemma 3.4.2, we choose

$$y = x^{\xi}.$$

Now, following the argument of David-Wu, assuming that $x^{\xi} > M_A$,

$$
\begin{aligned}
V(x^\xi) &= \prod_{l<x^\xi, l\nmid M_A} \left(1-\frac{1}{l}\right) \prod_{l<x^\xi, l\mid M_A} \left(\frac{1-\#C(l)/\#G(l)}{1-1/l}\right) \\
&= \prod_{l<x^\xi} \left(1-\frac{1}{l}\right) \prod_{l\mid M_A} \left(1-\frac{1}{l}\right)^{-1} \prod_{l<x^\xi, l\nmid M_A} \left(\frac{1-\#C(l)/\#G(l)}{1-1/l}\right) \\
&\overset{\text{Mertens}}{\sim} \frac{e^{-\gamma}}{\xi \log x} \cdot C_A \cdot \left(1-\#C'(M_A)/\#G(M_A)\right)^{-1} \cdot \prod_{l>x^\xi} \left(\frac{1-\#C(l)/\#G(l)}{1-1/l}\right)^{-1}
\end{aligned}
$$

where the asymptotic $\sim$ is as $x^\xi \to \infty$.

Then, considering the "remainder" $r(\mathcal{A}, d)$ for squarefree d supported on $\mathcal{P}$, we have

$$
r(\mathcal{A}, d) = \sum_{m\mid M_A} \left(\mu(m) \cdot \pi_{C(dm)}(x, L_{dm}/\mathbb{Q})\right) - \frac{\#C(d)}{\#G(d)} \left(1-\frac{\#C'(M_A)}{\#G(M_A)}\right) \mathrm{li}(x).
$$

But since $G(dm) = G(d) \times G(m)$ for $m \mid M_A$ and d supported outside of M_A, then, using (5.8)

$$
\begin{aligned}
&\sum_{m\mid M_A} \mu(m) \cdot \pi_{C(dm)}(x, L_{dm}/\mathbb{Q}) = \\
&\quad = \sum_{m\mid M_A} \mu(m) \cdot \left(\frac{\#C(dm)}{\#G(dm)} \mathrm{li}(x) + \frac{\#B(dm)}{\#G(dm)} \frac{\#C(dm)}{\#C_B(dm)} R_{dm}(x) + Q_{dm}(x)\right) \\
&\quad = \sum_{m\mid M_A} \mu(m) \cdot \left(\frac{\#C(d)}{\#G(d)} \frac{\#C(m)}{\#G(m)} \mathrm{li}(x) + \frac{\#B(dm)}{\#G(dm)} \frac{\#C(dm)}{\#C_B(dm)} R_{dm}(x) + Q_{dm}(x)\right) \\
&\quad = \left(1-\frac{\#C'(M)}{\#G(M)}\right) \frac{\#C(d)}{\#G(d)} \mathrm{li}(x) \\
&\qquad\qquad + \frac{\#B(d)}{\#G(d)} \frac{\#C(d)}{\#C_B(d)} \sum_{m\mid M_A} \mu(m) \frac{\#B(m)}{\#G(m)} \frac{\#C(m)}{\#C_B(m)} R_{dm}(x) \\
&\qquad\qquad + \sum_{m\mid M_A} \mu(m) Q_{dm}(x).
\end{aligned}
$$

But $R_{dm}(x) \ll_A R_d(x)$ and $Q_{dm}(x) \ll_A Q_d(x)$, so we have

$$r(\mathcal{A}, d) = \frac{\#B(d)}{\#G(d)} \frac{\#C(d)}{\#C_B(d)} \cdot O_A\left(R_d(x)\right) + O_A\left(Q_d(x)\right).$$

By the Chinese Remainder Theorem, (5.11), and (5.14),

$$\begin{aligned}
\frac{\#B(d)}{\#G(d)} \frac{\#C(d)}{\#C_B(d)} &\leq \prod_{l \mid d} \left(1 - \frac{(l-2)^g(l-1-g)}{(l-1)^{g+1}}\right)^{-1} \\
&\quad \cdot \left(\frac{1}{l-1} \cdot \left(- \sum_{r=1}^{g} l^r \prod_{j=1}^{r} (1-l^{2j})^{-1} \right.\right. \\
&\quad \left.\left. + (l-2)\Big(- \sum_{r=1}^{g} \prod_{j=1}^{r} (1-l^j)^{-1}\Big)\right)\right) \\
&\ll_g \prod_{l \mid d} (l-1) \cdot \frac{1}{l-1} \cdot \frac{l^2-1}{(l^2-2)} \\
&< \prod_{l} \left(1 + \frac{1}{l^2-2}\right) = O(1).
\end{aligned}$$

Next, from Corollary 5.2.9 we have

$$R_d(x) \ll \left(\frac{\#C_B(d)}{\#U(d)}\right)^{1/2} (\#B(d)) \cdot x^{\theta} \left(\log(M(L_d/L_d^{B(d)})) + \log x\right)$$

and so, again by (5.14) and the Chinese Remainder Theorem,

$$\begin{aligned}
R_d(x) &\ll \left(\left(\frac{1}{\#U(d)}\right)^{1/2} \left(\frac{C_B(d)}{\#B(d)}\right)^{1/2} (\#B(d))^{3/2}\right) x^{\theta} \left(\log(M(L_d/L_d^{B(d)})) + \log x\right) \\
&\ll_g d^{g^2+(3/2)g+1} x^{\theta} (\log(d) + \log(x)).
\end{aligned}$$

Next, from (5.7), using Lemma 3.1.6,

$$\begin{aligned}
Q_d(x) &\ll \frac{\#C(d)}{\#C_B(d)\cdot\#G(d)}\log d_{L_d} + \frac{\#B(d)}{\#G(d)}\frac{\#C(d)}{\#C_B(d)}[L_d^{B(d)}:\mathbb{Q}]x^{1/2} + x^{1/2} \\
&\ll \frac{\#C(d)}{\#C_B(d)\cdot\#G(d)}\log d_{L_d} + \frac{\#C(d)}{\#C_B(d)}x^{1/2} + x^{1/2} \\
&\ll \frac{1-\epsilon}{2g\cdot\#B(d)}\log d_{L_d} + \frac{\#G(d)}{\#B(d)}\frac{1}{2g}(1-\epsilon)x^{1/2} + x^{1/2} \\
&\ll_A \frac{1}{d^{g+1}d^{g^2}}\cdot d^{2g^2+g+1}\log(d) + \frac{d^{2g^2+g+1}}{d^{g+1}d^{g^2}}x^{1/2} \\
&= d^{g^2}\left(x^{1/2}+\log(d)\right)
\end{aligned}$$

Thus, since $\theta \geq 1/2$,

$$\begin{aligned}
r(\mathcal{A},d) &\ll_g d^{g^2+(3/2)g+1}x^{\theta}(\log(d)+\log(x)) + d^{g^2}\left(x^{1/2}+\log(d)\right) \\
&\ll_\epsilon d^{g^2+(3/2)g+1}x^{\theta+\epsilon}
\end{aligned}$$

Now, by the Triangle Inequality, the sum

$$\begin{aligned}
\left|\sum_{m<M,n<N,mn|P(y^U)}\alpha_m\beta_n\cdot r(\mathcal{A},mn)\right| &\leq \sum_{m<M,n<N,mn|P(y^U)}\left|r(\mathcal{A},mn)\right| \\
&\ll_{A,\epsilon} x^{\theta+\epsilon}\log(x)\sum_{m<M,n<N,mn|P(x^{\xi U})}(mn)^{g^2+(3/2)g+1}
\end{aligned}$$

Since $P(x^{\xi U})$ is squarefree, we note that for any non-negative function $f(t)$, since $U<1$, we have

$$\sum_{m<M,n<N,mn|P(x^{\xi U})}f(mn) \leq \sum_{d\leq x^{\xi}}\mu(d)^2 3^{\omega(d)}f(d).$$

But $3^{\omega(d)} \leq (3/2)d$, and, of course, $\mu(d)^2 \leq 1$. Thus, integrating by parts, the sum above is

$$\begin{aligned}
&\ll x^{\theta+\epsilon}\int_1^{x^{\xi}} d^{g^2+(3/2)g+2}\cdot \mathrm{d}(\text{sq.free. ints.}) \\
&\ll x^{\theta+\epsilon+\xi(g^2+(3/2)g+3)}.
\end{aligned}$$

Thus, finally, the lower bound (5.1) will be satisfied if

$$\boxed{\theta + \epsilon + \xi\left(g^2 + \frac{3}{2}g + 3\right) < 1}$$

with the constant

$$B = \xi^{-1} \cdot \frac{J(U,V)}{U-V}.$$

5.3.2 Ensuring (5.2)

We now ensure the lower bound (5.2), namely that

$$\sum_{(x^\xi)^V \leq l < (x^\xi)^U} \#\mathcal{A}_{l^2} = o\left(\frac{x}{(\log x)^2}\right).$$

We have that

$$\begin{aligned}
\#\mathcal{A}_{l^2} &= \frac{\#C(l^2)}{\#G(l^2)}\operatorname{li}(x) + \frac{\#B(l^2)}{\#G(l^2)}\frac{\#C(l^2)}{\#C_B(l^2)}R_{l^2}(x) + Q_{l^2}(x) \\
&= O_g\left(\frac{1}{l^2}\right)\operatorname{li}(x) + O_g\left(\frac{1}{l^2}\right)\cdot O_g(l)R_{l^2}(x) + Q_{l^2}(x) \\
&= O_g\left(\frac{1}{l^2}\right)\operatorname{li}(x) + O_g\left(\frac{1}{l}\right)R_{l^2}(x) + Q_{l^2}(x)
\end{aligned}$$

where

$$\begin{aligned}
R_{l^2}(x) &\ll \left(\frac{\#C_B(l^2)}{\#U(l^2)}\right)^{1/2}(\#B(l^2))\cdot x^\theta\left(\log(M(L_{l^2}/L_{l^2}^{B(l^2)})) + \log x\right) \\
&\ll_g \left(\left(\frac{1}{\#U(l^2)}\right)^{1/2}\left(\frac{\#C_B(l^2)}{\#B(l^2)}\right)^{1/2}(\#B(l^2))^{3/2}\right)\cdot x^\theta(\log l + \log x) \\
&\ll_g \left(\left(\frac{1}{l^{3g^2+1}}\right)^{1/2}\left(\frac{1}{l}\right)^{1/2}((l-1)^{g+1}l^{4g^2-g})^{3/2}\right)\cdot x^\theta \log x \\
&\ll l^{(9/2)g^2+1/2}x^\theta \log x
\end{aligned}$$

and

$$\begin{aligned} Q_{l^2}(x) &\ll \frac{\#C(l^2)}{\#C_B(l^2)\cdot\#G(l^2)}\log d_{L_{l^2}} + \frac{\#B(l^2)}{\#G(l^2)}\frac{\#C(l^2)}{\#C_B(l^2)}[L_{l^2}^{B(l^2)}:\mathbb{Q}]x^{1/2}+x^{1/2} \\ &\ll \frac{1}{\#B(l^2)}\cdot O_g\left(\frac{1}{l}\right)\left(\#G(l^2)\log(\#G(l^2))\right) + O_g\left(\frac{1}{l}\right)\frac{\#G(l^2)}{\#B(l^2)}x^{1/2}+x^{1/2} \\ &\ll l^{2g^2-1}\log(l) + l^{2g^2-2g+1}x^{1/2}+x^{1/2}. \end{aligned}$$

We therefore have (since $l \le x$ and $\theta \ge 1/2$)

$$\#\mathcal{A}_{l^2} \ll_g \frac{1}{l^2}\operatorname{li}(x) + l^{(9/2)g^2-1/2}x^{\theta}\log x + x^{1/2},$$

so that, integrating by parts,

$$\sum_{(x^\xi)^V \le l < (x^\xi)^U} \#\mathcal{A}_{l^2} \ll x^{-\xi U}\operatorname{li}(x) + x^{\theta+\xi U\left((9/2)g^2+1/2\right)}\log x + x^{1/2+\xi U}$$

We therefore are ensured of (5.2) as long as

$$\boxed{\xi U < 1} \text{ and } \boxed{\theta + \xi U\left((9/2)g^2+1/2\right) < 1.}$$

5.3.3 Determining the optimal constants.

Collecting the constraints, we see that our goal is achieved as long as

$$g < \xi(rU+V), \quad \theta + \xi\left(g^2+\frac{3}{2}g+3\right) < 1, \quad \xi U < 1, \quad \theta + \xi U\left((9/2)g^2+1/2\right) < 1.$$

To attain minimal r, we minimize the value of

$$\frac{1}{U}\left(\frac{g}{\xi} - V\right),$$

so we wish to maximize ξ, U, and V within our constraints.

Certainly, the constraint $\xi U < 1$ is redundant. Recall that the constraints of the sieve include $V \leq 1/4$ and $1/2 \leq U < 1$. We thus choose $V = 1/4$. Then, in particular, the terms $\alpha(V) = 0$ and $\beta(V) = 0$. Thus, doing a bit of calculus, we see that in order for $J(U, 1/4) > 0$, so that $B > 0$, we must have $\boxed{U < 3/4.}$

Thus, take

$$\xi = \frac{1-\theta}{(9/2)g^2 + 1/2}\left(\frac{4}{3} + \epsilon\right); \quad U = \frac{3}{4} - \epsilon.$$

Then, we see that for $g \geq 2$, the constraint $\theta + \xi\left(g^2 + \frac{3}{2}g + 3\right) < 1$ is satisfied for any $\epsilon > 0$. Thus, we may take

$$r = \left\lceil \frac{(9/2)g^3 + (1/2)g}{1-\theta} - \frac{1}{3} \right\rceil$$

and ϵ sufficiently small. This concludes the proof of Theorem 5.1.1.

5.3.4 Proof of Theorem 5.1.3

We follow the argument of David-Wu to prove Theorem 5.1.3. Write the usual sieving function,

$$S(\mathcal{A}, \mathcal{P}, z) := \#\left(\mathcal{A} \setminus \bigcup_{p \in \mathcal{P}, p \leq z} \mathcal{A}_p\right).$$

Then, from the Weil bound, we see that for any $z < x$,

$$\begin{aligned}
\#\left\{p \leq x \;\middle|\; \#A_p\left(\mathbb{F}_p\right) \text{ is prime}\right\} =& \#\left\{p \leq x \;\middle|\; \#A_p\left(\mathbb{F}_p\right) \text{ is prime}, \#A_p\left(\mathbb{F}_p\right) > z\right\} \\
&+ \#\left\{p \leq x \;\middle|\; \#A_p\left(\mathbb{F}_p\right) \text{ is prime}, \#A_p\left(\mathbb{F}_p\right) \leq z\right\} \\
&\leq S(\mathcal{A}, \mathcal{P}, z) + O(z^{1/g}).
\end{aligned}$$

We now apply the Selberg linear sieve (see Theorem 8.3 of [HR74]), with $q = 1$, and in their notation, $\xi = z$, which yields

$$S(\mathcal{A}, \mathcal{P}, z) \leq XV(z)\left(F(2) + o(1)\right) + \mathcal{R}$$

where

$$\begin{aligned}\mathcal{R} &= \sum_{d<z^2, d\mid P(z)} 3^{\omega(d)}\left|r(\mathcal{A}, d)\right| \\ &\ll_g \sum_{d<z^2} \mu(d)^2 3^{\omega(d)} d^{g^2+(3/2)g+1} x^\theta \log(x) \\ &\ll x^\theta z^{2g^2+3g+6}\log(x)\end{aligned}$$

which is $o\left(x/(\log x)^2\right)$ if $\log(z)/\log(x) < (1-\theta)/(2g^2+3g+6)$.

Choose $\epsilon > 0$ and define z via $\log(x)/\log(z) = (2g^2+3g+6)/(1-\theta) + \epsilon$. Then, the definition of $F(u)$ tells us that $F(2) = e^\gamma$, so

$$\begin{aligned}X \cdot V(z)\left(F(2)+o(1)\right) &= C_A \frac{\mathrm{li}(x)}{\log z} \cdot \prod_{l>z}\left(\frac{1-\#C(l)/\#G(l)}{1-1/l}\right)^{-1}(1+o(1)) \\ &= C_A \frac{x}{(\log x)^2}\cdot\frac{\log(x)}{\log(z)}\cdot(1+o(1)) \\ &\leq \left(\frac{2g^2+3g+6}{1-\theta}+\epsilon'\right) C_A \frac{x}{(\log x)^2}\end{aligned}$$

for $x \gg_{A,\theta,\epsilon'} 0$, and the result follows.

5.3.5 Proof of Theorem 5.1.4

We continue the assumption that $A/\mathbb{Q}$ is generic and that the θ-Hypothesis holds for A. We will employ Theorem 3.2.2 with the data

$$S := \{p \leq x\};$$

$$f(p) := \#A_p(\mathbb{F}_p);$$

$$\lambda_l := \#C(l)/\#G(l);$$

and the functions $e_l(x)$ and $e_{l_1 \cdots l_u}(x)$ defined accordingly. We let $\beta \in (0, 1]$ be arbitrary, and $\alpha = \alpha(x)$ arbitrary such that $0 < \alpha(x) < \beta$. We define $y = x^\alpha$, and will determine sufficient conditions on α and β for conditions (1)-(6) of Theorem 3.2.2 to be satisfied.

We note that our choice of S does not agree with our methods in this article so far; here, we do not exclude those p for which $\#A_p(\mathbb{F}_p)$ shares a factor with M_A. It is clear, though, that the bound $r(\mathcal{A}, d) \ll d^{g^2+(3/2)g+1}x^\theta \log x$, for squarefree d, holds as well for the error function in this context: that is,

$$\pi(x) \cdot e_d(x) \ll d^{g^2+(3/2)g+1}x^\theta \log x.$$

We proceed:

1. Let $p \in S(x)$. Then, $f(p) = (1 + o(1))p^g$, by the Weil Conjectures. Thus, for any chosen β, the number of distinct prime divisors of $f(p)$ that are more than x^β is bounded by $(\log(g) + o(1))/\log(\beta)$.

2. We have

$$\begin{aligned}\sum_{y<l<x^\beta} \lambda_l &= \sum_{y<l<x^\beta} l^{-1} + O_g(l^{-2}) \\ &= \log\log(x^\beta) - \log\log(x^\alpha) + O(1) \\ &= -\log\alpha + O(1).\end{aligned}$$

We must thus require $\log\alpha = o(\sqrt{\log\log x})$.

3. We have

$$\begin{aligned}\sum_{y<l<x^\beta} |e_l| &\ll \sum_{y<l<x^\beta} l^{g^2+(3/2)g+1} x^{-1+\theta} (\log x)^2 \\ &\leq x^{-1+\theta}(\log x)^2 x^{\beta\cdot(g^2+(3/2)g+2)}\end{aligned}$$

This quantity is $o(\sqrt{\log\log x})$ if

$$\beta < \frac{1-\theta}{g^2+(3/2)g+2},$$

and α satisfies the condition in item 2. (Since $\theta < 1$, such a β exists.)

4. As in item 2, we have

$$\sum_{l\leq y} \lambda_l = \log\log x + \log\alpha + O(1)$$

which is of the desired form (with the constant $c = 1$) assuming the condition in item 2.

5. The quantity $\sum_{l\leq y} \lambda_l^2$ is clearly $O(1)$ from the previous discussion.

6. Lastly, mimicking [Liu06], we have

$$\sum_{\star}|e_{l_1\cdot l_u}| \ll x^{-1+\theta}(\log x)^2\left(\sum_{l\leq x^{\alpha}} l^{g^2+(3/2)g+1}\right)^u$$
$$\ll x^{-1+\theta+\alpha\cdot u\cdot(g^2+(3/2)g+2)}(\log x)^2$$

which, assuming that $\alpha(x)\to 0$, is asymptotic to $x^{-1+\theta+o(1)} = o((\log\log x)^{-r/2})$ for any r, since $\theta < 1$.

We thus require the existence of $\alpha(x)$ such that

$$\alpha = o(1) \quad \text{and} \quad \log(\alpha(x)) = o(\sqrt{\log\log x}),$$

which is clear: take, for instance, $\alpha = (\log\log x)^{-1}$. This concludes the proof of Theorem 5.1.4.

5.4 A Koblitz Conjecture for Higher Dimension and Experimental Evidence

The heuristics of the Koblitz Conjecture suggest the following conjecture.

Conjecture 5.4.1. *Let $A/\mathbb{Q}$ be an abelian variety satisfying the hypothesis* (Triv_A) *such that $C_A \neq 0$. Then,*

1. $\#\{p \leq x \mid \#A_p(\mathbb{F}_p) \text{ is prime}\} \asymp_A \dfrac{x}{(\log(x))^2}$.
2. *In particular, if A is generic,* $\#\{p \leq x \mid \#A_p(\mathbb{F}_p) \text{ is prime}\} \sim C_A\dfrac{x}{g(\log(x))^2}$.

Our Conjecture appears to be consistent with the generalizations by Weng and Spreckels, and has been recently stated independently by Spreckels-Stein [SS17]. We

also believe that part (2) of Conjecture 5.4.1 could be extended to those abelian varieties A with $\mathrm{End}(A)$ larger than $\mathbb{Z}$, analogously to Conjecture B of [Kob88], but we hesitate to do so for concern about stating the asymptotic constant correctly.

We provide experimental evidence for Conjecture 5.4.1 in the reminder of this Section. We collected from the LMFDB [LMFDB] some hyperelliptic curves $C/\mathbb{Q}$ of genus $g = 2$ whose Jacobians J_C are generic and satisfy condition (Triv_{J_C}). We also considered the hyperelliptic genus 3 curve C_3 given by the equation

$$y^2 = x^7 - 14085x^6 + 33804x^5 - 27231x^4 + 27231x^3 - 35995x^2 - 33803x + 25039;$$

this curve was produced in the recent paper of Arias-de-Reyna et al. [Ari+16] as an example of a genus 3 curve whose Jacobian is proven to be generic by their Theorem 4.1. We ran a Sage program to collect the group orders $\#(J_C)_p(\mathbb{F}_p)$, with $p \leq 2^{20}$ for the genus 2 curves, and $p \leq 6 \cdot 10^4$ for C_3. (We had difficulty computing the group orders for larger p.) We then graphed the ratio

$$\frac{\#\{p \leq x \mid \#(J_C)_p(\mathbb{F}_p) \text{ is prime}\}}{\pi(x)/(\log x)} \tag{5.15}$$

for x at prime values q for which $\#(J_C)_q(\mathbb{F}_q)$ is prime. We display these graphs in Figures 5.1, 5.2, 5.3, 5.4, and 5.5. This evidence supports part (1) of the Conjecture, and if we were able to compute the constant C_A, we could check whether the evidence also supports part (2).

In the spirit of the questions of Lang-Trotter results "on average" (see, for instance, [BCD11]), we also approximated what we might call the "average constants"

$$\mathfrak{C}_g := \prod_{\ell} \left(\frac{1 - \#C(\ell)/\#G(\ell)}{1 - 1/\ell} \right)$$

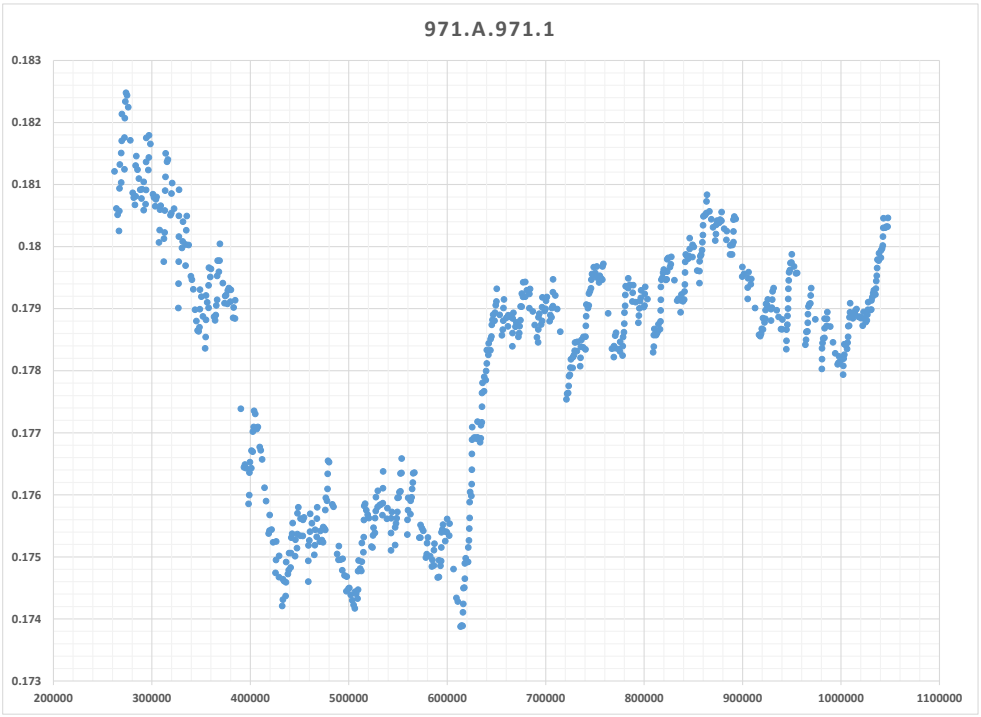

Figure 5.1: curve 971.a.971.1 with equation $Y^2 + Y = X^5 - 2X^3 + X$

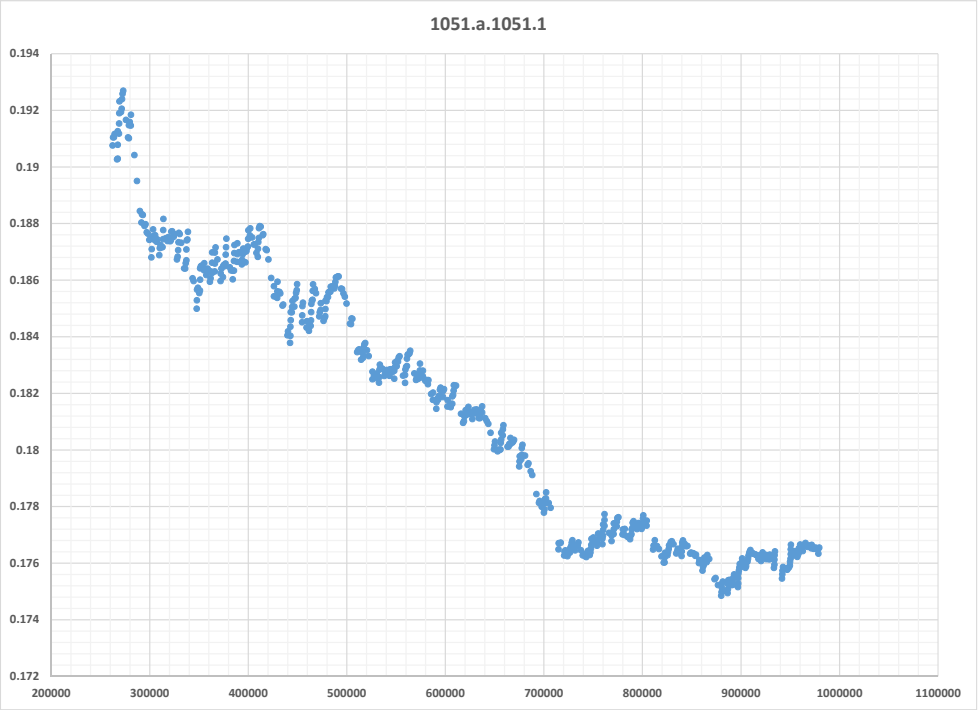

Figure 5.2: curve 1051.a.1051.a with equation $Y^2 + Y = X^5 - X^4 + X^2 - X$

Figure 5.3: curve 1205.a.1205.1 with equation $Y^2 + Y = X^5 + 2X^4 - X^2$

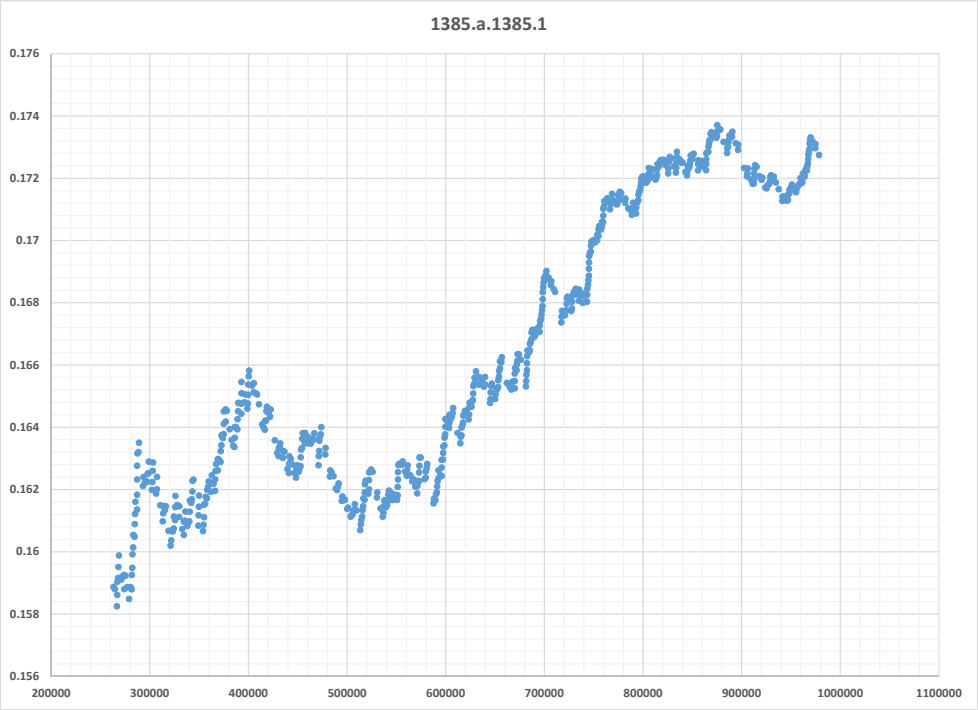

Figure 5.4: curve 1385.a.1385.1, with equation $Y^2 + Y = X^5 + 3X^4 + 3X^3 - X$

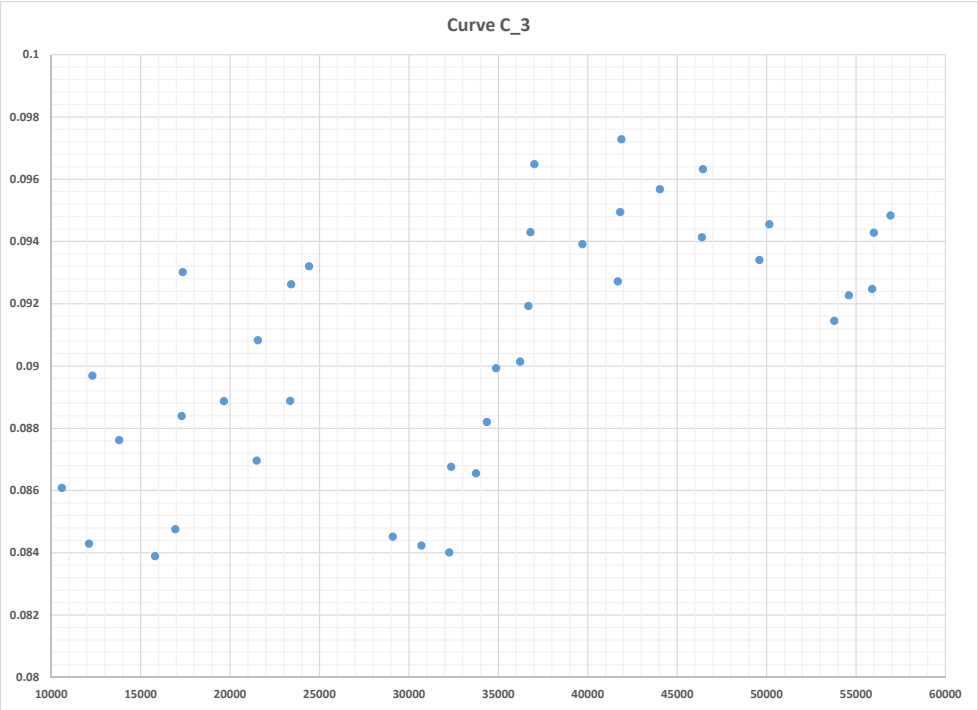

Figure 5.5: genus 3 curve C_3

n	$\mathfrak{C}_1$	$\mathfrak{C}_2$	$\mathfrak{C}_3$	$\mathfrak{C}_4$
2	0.562500000000000	0.760989583333333	0.754354887320847	0.754413616554689
4	0.513926644244210	0.706235456622878	0.700012977803311	0.700067571267533
8	0.505468861944026	0.695053638628807	0.688929626754209	0.688983355837062
16	0.505166809270517	0.694639169901420	0.688521872595408	0.688572506891267
24	0.505166169952616	0.694638290801478	0.688517938493554	0.688571635469346

Figure 5.6: Computations for the constants $\mathfrak{C}_g$.

where $G(l) = \mathrm{GSp}_{2g}(\mathbb{Z}/l\mathbb{Z})$, and $C(l)$ is the union of conjugacy classes in $G(l)$ defined in (5.3). For a given generic abelian variety A, the constant C_A differs from $\mathfrak{C}_g$ only by a factor depending on its non-surjective primes. We computed these approximations by finding the product for $\ell < 2^n$, for $n \leq 24$; they appear in Figure 5.6.

Interestingly, the functions (5.15) for the genus 2 curves that we ran our program for appear to converge to values which differ from $\mathfrak{C}_2/2$ by approximately half. This is perhaps more than one might expect: the author expects that the Euler factors at which C_A and $\mathfrak{C}_2$ disagree (namely, those for the non-surjective primes of A) are not significantly different in magnitude, and he expects that there are not many such Euler factors.

It also appears that the limit $\lim_{g\to\infty} \mathfrak{C}_g$ exists. Very similar constants were computed in [Cas+12] in the context of Jacobians of hyperelliptic and non-hyperelliptic curves, though of course once $g \geq 3$, not all curves are hyperelliptic, and once $g \geq 4$, not all ppav's are Jacobians. Their constants, for $g \to \infty$, are also conjectured to converge.

Chapter 6: Concluding Remarks and Further Directions

Based on the heuristics, existing conjectures, and experimental data on the growth of the counting functions for the Lang-Trotter questions that we have considered in this thesis, we presume that the asymptotic bounds in our main Theorems are not sharp. We expect that more sophisticated sieving techniques will yield, up to a point, better asymptotic bounds. (In particular, we expect the methods of the works mentioned in Section 2.4 will improve our results on the Fixed-Field question.) However, like the attempts to date to prove the Twin Prime Conjecture, we expect that sieve theory alone will not be able to prove any of the conjectures mentioned here.

We mention here some other questions of Lang-Trotter type, as well as extensions of the work in this thesis, that would be interesting to consider. Most of these are variants or generalizations of questions asked about elliptic curves.

Remark 6.0.1. *It would be interesting to extend the results of this thesis to abelian varieties other than those whose adelic Galois representation $\widehat{\rho}$ has open image in $\mathrm{GSp}_{2g}\widehat{\mathbb{Z}}$. For the methods of this paper to work, one would need to require that the image of $\widehat{\rho}$ be open in $\mathcal{G}(\widehat{\mathbb{Z}})$ for some "reasonable" sub-group-scheme $\mathcal{G} \hookrightarrow \mathrm{GSp}_{2g}$.*

Remark 6.0.2. *Question 4.0.2 and variants thereof are easily extended to non-*

CM abelian varieties of any dimension $g \geq 2$. Namely, we may ask about the set of primes p for which any specified ring R embeds into the endomorphism algebra $\mathrm{End}\big(A_p\big) \otimes \mathbb{Q}$. *(Of course, one would specify that R must be a ring which embeds into the endomorphism algebra of some abelian variety of dimension g over a finite field.)*

Question 6.0.3. *How often is the order of the group of rational points, $\#A_p(\mathbb{F}_p)$ pseudoprime to a fixed base? On the analogous questions for elliptic curves, see for instance [Kob88; MM01; CLS09], and see [BCD11] for the study of the primality of $\#E_p(\mathbb{F}_p)$ on average.*

Question 6.0.4. *Let $F/\mathbb{Q}$ be a totally real field of degree g, and $K/\mathbb{Q}$ a primitive CM field of degree $2g$. What are the values of $\Pi(A, F)(X)$ and $\Pi(A, K)(X)$* on average for generic A? *One would need to specify how to average. For $g = 2$ or $g = 3$, one could averaging over boxes for the coefficients of genus-g curves $C/\mathbb{Q}$, considering these counting functions for the Jacobian of C. (Once $g \geq 4$, not all abelian varieties are Jacobians of curves.) See, for instance, [Shp13; AJ] on the analogous question for elliptic curves.*

Question 6.0.5. *Similarly, what are the values of the counting function for the Koblitz Conjecture, $\#\{p \leq x \mid \Omega(\#A_p(\mathbb{F}_p)) \leq r\}$, on average, for $r = 1$ or $r > 1$? See, for instance, [BCD11].*

Question 6.0.6. *Let A_1 and A_2 be abelian varieties over $\mathbb{Q}$ (generic or otherwise). How can we describe the set of primes at which both the A_i are good ordinary non-split, and*

1. $\mathbb{Q}(\pi_{p,A_1}) \cong \mathbb{Q}(\pi_{p,A_2})$? *or* $\mathbb{Q}(\pi_{p,A_1}) \cong \mathbb{Q}(\pi_{p,A_2}) \cong K$ *for a specified primitive CM field* K?

2. $\mathbb{Q}(\pi_{p,A_1})_0 \cong \mathbb{Q}(\pi_{p,A_2})_0$? *or* $\mathbb{Q}(\pi_{p,A_1})_0 \cong \mathbb{Q}(\pi_{p,A_2})_0 \cong F$ *for a specified totally real field* F?

3. $a_{i,p,A_1} = a_{i,p,A_2}$ *for specified* i? *or* $a_{i,p,A_1} = a_{i,p,A_2} = t$ *for specified* i *and* t? *(See [Coj+16] for* $i = 1$ *and a single abelian variety, as well as an Erdős-Kac style result for* $a_{1,p}$.*)*

4. $\mathrm{char}_{p,1} = \mathrm{char}_{p,2}$; *that is, the* A_i *are isogenous mod* p? *Here,* $\mathrm{char}_{p,i}$ *is the characteristic polynomial of the Frobenius endomorphism of* $(A_i)_p$. *(The Isogeny Theorem of Faltings [Fal86] implies that if* A_1 *and* A_2 *are not isogenous over* $\overline{\mathbb{Q}}$*, then the set of primes at which* A_1 *and* A_2 *are isogenous mod* p*, regardless of ordinarity of the* p*, does not have density 1.)*

One may also ask these questions without the requirement that p *be* ordinary *for the* A_i.

Question 6.0.7. *Let* A_1 *and* A_2 *be abelian varieties over* $\mathbb{Q}$. *How can we describe the set of primes* p *at which both the* A_i *satisfy* $\Omega(\#(A_i)_p(\mathbb{F}_p)) \leq r$*, for* $r = 1$ *or* $r > 1$?

Question 6.0.8. *Let* A *be an abelian variety over* $\mathbb{Q}$ *of dimension* ≥ 4 *which is not isomorphic (over* $\mathbb{Q}$*, or perhaps over* $\overline{\mathbb{Q}}$*) to the Jacobian of a curve. At what (or how many) primes is* A_p *isomorphic (over* $\mathbb{F}_p$*, or* $\overline{\mathbb{F}}_p$*) to a Jacobian?*

Question 6.0.9. *Let $A/\mathbb{Q}$ be generic. Is there a Cohen-Lenstra phenomenon for the (ring class groups of the) endomorphism rings $\mathrm{End}\big(A_p\big)$ at ordinary primes p? Or for the (class groups of the) endomorphism fields $\mathrm{End}\big(A_p\big)\otimes\mathbb{Q}$? See, for instance, [DS14] for the study of a Cohen-Lenstra phenomenon on the group structure of $E_p(\mathbb{F}_p)$ for an elliptic curve $E/\mathbb{Q}$.*

Question 6.0.10. *Let $A/\mathbb{Q}$ be generic, and $n \geq 2$. Is there a bias, like the Chebyshev bias, to the sequence $\big(\mathrm{disc}(\mathrm{char}_p) \bmod n\big)_p$? Or to the sequence*

$$\Big(d(\mathrm{End}\big(A_p\big)\otimes\mathbb{Q}/\mathbb{Q}) \bmod n\Big)_{p \text{ ordinary}}?$$

Bibliography

[Ach09] Jeffrey D. Achter. "Split reductions of simple abelian varieties". In: *Mathematical Research Letters* 16.2 (2009), pp. 199–213. URL: http://dx.doi.org/10.4310/MRL.2009.v16.n2.a1.

[Ach12] Jeffrey D. Achter. "Explicit bounds for split reductions of simple abelian varieties". eng. In: *Journal de Théorie des Nombres de Bordeaux* 24.1 (Mar. 2012), pp. 41–55. URL: http://eudml.org/doc/251138.

[AH03] Jeffrey D. Achter and Joshua Holden. "Notes on an analogue of the Fontaine-Mazur conjecture". eng. In: *Journal de théorie des nombres de Bordeaux* 15.3 (2003), pp. 627–637. URL: http://eudml.org/doc/249110.

[AH17] Jeffrey Achter and Everett Howe. "Split abelian surfaces over finite fields and reductions of genus-2 curves". In: *Algebra Number Theory* 11.1 (2017), pp. 39–76. DOI: 10.2140/ant.2017.11.39.

[AJ] H. Iwaniec A. C. Cojocaru and N. Jones. "The average asymptotic behaviour of the Frobenius fields of an elliptic curve". In: (). Preprint.

[Ari+16] Sara Arias-De-Reyna, Cécile Armana, Valentijn Karemaker, Marusia Rebolledo, Lara Thomas, and Núria Vila. "Large Galois images for Jacobian varieties of genus 3 curves". In: *Acta Arithmetica* 174.4 (Aug. 2016), pp. 339–366. DOI: 10.4064/aa8250-4-2016.

[BCD11] Antal Balog, Alina Carmen Cojocaru, and Chantal David. "Average twin prime conjecture for elliptic curves". In: *American Journal of Mathematics* 133.5 (2011), pp. 1179–1229. DOI: 10.1353/ajm.2011.0033..

[BG97] Pilar Bayer and Josep González. "On the Hasse-Witt invariants of modular curves". In: *Experiment. Math.* 6.1 (1997), pp. 57–76. URL: http://projecteuclid.org/euclid.em/1047565284.

[BH62] Paul T. Bateman and Roger A. Horn. "A heuristic asymptotic formula concerning the distribution of prime numbers". In: *Math. Comp.* 16 (1962), pp. 363–367. DOI: https://doi.org/10.1090/S0025-5718-1962-0148632-7.

[BSS99] Ian F Blake, Nigel P. Smart, and G. Seroussi. *Elliptic curves in cryptography*. Cambridge : Cambridge University Press, 1999.

[Cas+12] Wouter Castryck, Amanda Folsom, Hendrik Hubrechts, and Andrew V. Sutherland. "The probability that the number of points on the Jacobian of a genus 2 curve is prime". In: *Proceedings of the London Mathematical Society* 104.6 (2012), pp. 1235–1270. DOI: 10.1112/plms/pdr063.

[CD08] Alina Carmen Cojocaru and Chantal David. "Frobenius Fields for Elliptic Curves". In: *American Journal of Mathematics* 130.6 (2008), pp. 1535–1560.

[CFM05] Alina Carmen Cojocaru, Etienne Fouvry, and M. Ram Murty. "The square sieve and the Lang-Trotter conjecture". In: *Canad. J. Math.* 57.6 (2005), pp. 1155–1177.

[Cha97] Nick Chavdarov. "The generic irreducibility of the numerator of the zeta function in a family of curves with large monodromy". In: *Duke Math. J.* 87.1 (Mar. 1997), pp. 151–180. DOI: 10.1215/S0012-7094-97-08707-X.

[CLS09] Alina Carmen Cojocaru, Florian Luca, and Igor E. Shparlinski. "Pseudoprime reductions of elliptic curves". In: *Mathematical Proceedings of the Cambridge Philosophical Society* 146.3 (May 2009), pp. 513–522. DOI: 10.1017/S0305004108001758.

[Coj+16] Alina Carmen Cojocaru, Rachel Davis, Alice Silverberg, and Katherine E. Stange. "Arithmetic properties of the Frobenius traces defined by a rational abelian variety (with two appendices by J-P. Serre)". In: *International Mathematics Research Notices* (2016). DOI: 10.1093/imrn/rnw058.

[Coj04] Alina Carmen Cojocaru. "Questions about the reductions modulo primes of an elliptic curve". In: *CRM Proceedings and Lecture Notes* 36 (2004), pp. 61–79.

[Coj05] Alina Carmen Cojocaru. "Reductions of an elliptic curve with almost prime orders". eng. In: *Acta Arithmetica* 119.3 (2005), pp. 265–289. URL: http://eudml.org/doc/278842.

[Del73] Pierre Deligne. "La conjecture de Weil. I." French. In: *Publ. Math., Inst. Hautes Étud. Sci.* 43 (1973), pp. 273–307.

[DKS17] Chantal David, Dimitris Koukoulopoulos, and Ethan Smith. "Sums of Euler products and statistics of elliptic curves". In: *Mathematische Annalen* 368.1 (June 2017), pp. 685–752. DOI: 10.1007/s00208-016-1482-2.

[DS14] Chantal David and Ethan Smith. "A Cohen–Lenstra phenomenon for elliptic curves". In: *Journal of the London Mathematical Society* 89.1 (2014), pp. 24–44. DOI: 10.1112/jlms/jdt036.

[DW12] Chantal David and J Wu. "Almost prime values of the order of elliptic curves over finite fields". In: *Forum Mathematicum* (2012). DOI: 10.1515/form.2011.051.

[EK40] P. Erdös and M. Kac. "The Gaussian Law of Errors in the Theory of Additive Number Theoretic Functions". In: *American Journal of Mathematics* 62.1 (1940), pp. 738–742. URL: http://www.jstor.org/stable/2371483.

[Elk87a] Noam D. Elkies. "Distribution of supersingular primes". In: *Astérisque* 198-199-200. proceedings of Journées Arithmétiques 1989 (1987), pp. 127–132. URL: http://eudml.org/doc/143494.

[Elk87b] Noam D. Elkies. "Supersingular primes of a given elliptic curve over a number field". PhD thesis. Harvard Univ., 1987.

[Elk87c] Noam D. Elkies. "The existence of infinitely many supersingular primes for every elliptic curve over Q." In: *Inventiones mathematicae* 89 (1987), pp. 561–568. URL: http://eudml.org/doc/143494.

[Elk89] Noam D. Elkies. "Supersingular primes for elliptic curves over real number fields". eng. In: *Compositio Mathematica* 72.2 (1989), pp. 165–172. URL: http://eudml.org/doc/89986.

[Fal86] G. Faltings. "Finiteness Theorems for Abelian Varieties over Number Fields." In: *Arithmetic Geometry*. Ed. by Silverman J.H. Cornell G. Springer, New York, NY, 1986. DOI: 10.1007/978-1-4613-8655-1_2.

[FG12] Jason Fulman and Robert Guralnick. "Bounds on the number and sizes of conjugacy classes in finite Chevalley groups with applications to derangements". In: *Trans. Amer. Math. Soc.* 364.6 (2012), pp. 3023–3070.

[FM96] Etienne Fouvry and M. Ram Murty. "On the distribution of supersingular primes". In: *Can. J. Math.* 48.1 (1996), pp. 81–104.

[GJ12] Josep González and Jorge Jiménez-Urroz. "The Sato–Tate Distribution and the Values of Fourier Coefficients of Modular Newforms". In: *Experiment. Math.* 21.1 (2012), pp. 84–102. URL: https://projecteuclid.org:443/euclid.em/1338430816.

[Gro66] Alexander Grothendieck. "Formule de Lefschetz et rationalité des fonctions L". fre. In: *Séminaire Bourbaki* 9 (1964-1966), pp. 41–55. URL: http://eudml.org/doc/109708.

[Hal11] Chris Hall. "An open-image theorem for a general class of abelian varieties". In: *Bulletin of the London Mathematical Society* 43.4 (2011), pp. 703–711. DOI: 10.1112/blms/bdr004. eprint: http://blms.oxfordjournals.org/content/43/4/703.full.pdf+html.

[Hea84] D.R. Heath-Brown. "The Square Sieve and Consecutive Square-Free Numbers." In: *Mathematische Annalen* 266 (1984), pp. 251–260. URL: http://eudml.org/doc/163852.

[HK85] K. A. Hardie and K. H. Kamps. "Exact sequence interlocking and free homotopy theory". In: *Cahiers de Topologie et Géométrie Différentielle Catégoriques* 26.1 (1985), pp. 3–31. URL: http://eudml.org/doc/91355.

[Hon68] Taira Honda. "Isogeny classes of abelian varieties over finite fields". In: *J. Math. Soc. Japan* 20.1-2 (Apr. 1968), pp. 83–95. DOI: 10.2969/jmsj/02010083.

[HR74] H. Halberstam and H.-E. Richert. *Sieve Methods*. Vol. 504. L.M.S. Monographs. Academic Press, 1974.

[HR85a] H. Halberstam and H.-E. Richert. "A weighted sieve of Greaves' type I". eng. In: *Banach Center Publications* 17.1 (1985), pp. 155–182. URL: http://eudml.org/doc/267871.

[HR85b] H. Halberstam and H.-E. Richert. "A weighted sieve of Greaves' type II". eng. In: *Banach Center Publications* 17.1 (1985), pp. 183–215. URL: http://eudml.org/doc/268192.

[IU10] Henryk Iwaniec and Jorge Jiménez Urroz. "Orders of CM elliptic curves modulo p with at most two primes". English. In: *Ann. Sc. Norm. Super. Pisa, Cl. Sci. (5)* 9.4 (2010), pp. 815–832. DOI: 10.2422/2036-2145.2010.4.05.

[Jim08] Jorge Jiménez Urroz. "Almost Prime Orders of CM Elliptic Curves Modulo p." In: *Algorithmic Number Theory. ANTS 2008.* Ed. by Stein A. van der Poorten A.J. Lecture Notes in Computer Science. Heidelberg: Springer, Berlin, 2008. DOI: 10.1007/978-3-540-79456-1_4.

[Kob88] Neal Koblitz. "Primality of the number of points on an elliptic curve over a finite field." In: *Pacific J. Math.* 131.1 (1988), pp. 157–165. URL: http://projecteuclid.org/euclid.pjm/1102690074.

[Liu06] Yu-Ru Liu. "Prime analogues of the Erdös–Kac theorem for elliptic curves". In: *Journal of Number Theory* 119.2 (2006), pp. 155–170. DOI: https://doi.org/10.1016/j.jnt.2005.10.014.

[LMFDB] The LMFDB Collaboration. *The L-functions and Modular Forms Database*. http://www.lmfdb.org. [Online; accessed 16 September 2013]. 2013.

[LO77] J. C. Lagarias and A. M. Odlyzko. "Effective versions of the Chebotarev density theorem". In: *Algebraic number fields: L-functions and Galois properties*. Academic Press London ; New York, 1977, pp. 409–464.

[Lom15a] Davide Lombardo. "Bounds for Serre's open image theorem for elliptic curves over number fields". In: *Algebra and Number Theory* 9.2015 (2015), pp. 2347–2395. URL: http://dx.doi.org/10.2140/ant.2015.9.2347.

[Lom15b] Davide Lombardo. "Explicit open image theorems for abelian varieties with trivial endomorphism ring". In: *ArXiv e-prints* (Aug. 2015). arXiv: 1508.01293 [math.NT].

[LW54] Serge Lang and Andre Weil. "Number of Points of Varieties in Finite Fields". In: *American Journal of Mathematics* 76.4 (1954), pp. 819–827. URL: http://www.jstor.org/stable/2372655.

[Mer74] Franz Mertens. "Ein Beitrag zur analytischen Zahlentheorie." ger. In: *Journal für die reine und angewandte Mathematik* 78 (1874), pp. 46–62. URL: http://eudml.org/doc/148244.

[MM01] S. Ali Miri and V. Kumar Murty. "An Application of Sieve Methods to Elliptic Curves". In: *Progress in Cryptology — INDOCRYPT 2001: Second International Conference on Cryptology in India Chennai, India, December 16–20, 2001 Proceedings*. Ed. by C. Pandu Rangan and Cunsheng Ding. Berlin, Heidelberg: Springer Berlin Heidelberg, 2001, pp. 91–98. DOI: 10.1007/3-540-45311-3_9.

[MM84] V. Kumar Murty and M. Ram Murty. "An analogue of the Erdös-Kac theorem for Fourier coefficients of modular forms". In: *Indian J. Pure and Appl. Math.* 15.10 (1984), pp. 1090–1101.

[MMS88] M. Ram Murty, V. Kumar Murty, and N. Saradha. "Modular forms and the Chebotarev density theorem". In: *American Journal of Mathematics* 110.2 (1988), pp. 253–281.

[Mor12] Pieter Moree. "Artin's Primitive Root Conjecture -a survey-". In: *Integers* 12.6 (2012), pp. 1305–1416. DOI: 10.1515/integers-2012-0043.

[MP08] V. Kumar Murty and Vijay M. Patankar. "Splitting of Abelian Varieties". In: *International Mathematics Research Notices* 2008 (2008), rnn033. DOI: 10.1093/imrn/rnn033. eprint: /oup/backfile/Content_public/Journal/imrn/2008/10.1093/imrn/rnn033/2/rnn033.pdf.

[Mum99] David Mumford. *The Red Book of Varieties and Schemes*. Vol. 1358. Lecture Notes in Mathematics. Springer Berlin / Heidelberg, 1999. DOI: 10.1007/978-3-540-46021-3.

[Mur01] M. Ram Murty. "An introduction to Artin L-functions". In: *Journal of the Ramanujan Mathematical Society* 16.3 (2001), pp. 294–303.

[Mur97] V. Kumar Murty. "Modular forms and the Chebotarev density theorem. II". In: *Analytic number theory (Kyoto, 1996) , volume 247 of London Math. Soc. Lecture Note Ser. ,* 247 (1997), pp. 287–308.

[MZ14] V. Kumar Murty and Ying Zong. "Splitting of abelian varieties". In: *Advances in Mathematics of Communications* 8.4 (2014), pp. 511–519. DOI: 10.3934/amc.2014.8.511.

[Noo95] Rutger Noot. "Abelian varieties–Galois representation and properties of ordinary reduction". eng. In: *Compositio Mathematica* 97.1-2 (1995), pp. 161–171. URL: http://eudml.org/doc/90372.

[Ogu81] Arthur Ogus. "Hodge Cycles and Crystalline Cohomology". In: *Hodge Cycles, Motives, and Shimura Varieties*. Berlin, Heidelberg: Springer Berlin Heidelberg, 1981, pp. 357–414. DOI: 10.1007/978-3-540-38955-2_8.

[Pin98] Richard Pink. "l-adic algebraic monodromy groups, cocharacters, and the Mumford-Tate conjecture". In: *J. reine angew. Math* 495 (1998).

[SageMath] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 7.3)*. 2017. URL: http://www.sagemath.org.

[Ser00a] Jean-Pierre Serre. "Letter to M-F. Vigneras, January 1st, 1983." In: *Oeuvres. Collected papers. IV.* (2000).

[Ser00b] Jean-Pierre Serre. "Resume des cours de 1985-1986, Annuaire du College de France". In: *Oeuvres. Collected papers. IV.* (2000).

[Ser68] Jean-Pierre Serre. *Abelian l-adic representations and elliptic curves*. Benjamin Publ., 1968.

[Ser81] Jean-Pierre Serre. "Quelques applications du theoreme de densite de Chebotarev". In: *Inst. Hautes Etudes Sci. Publ. Math.* 54.4 (1981), pp. 323–401.

[Shp13] Igor Shparlinski. "On the Lang-Trotter and Sato-Tate conjectures on average for polynomial families of elliptic curves". In: *Michigan Math. J.* 62.3 (Sept. 2013), pp. 491–505. DOI: 10.1307/mmj/1378757885.

[Spr17] Ute Spreckels. "On the order of CM abelian varieties over finite prime fields". In: *Finite Fields and Their Applications* 45.Supplement C (2017), pp. 386–405. DOI: https://doi.org/10.1016/j.ffa.2017.01.004.

[SS17] Ute Spreckels and Andreas Stein. "Koblitz's Conjecture for Abelian Varieties". In: *Algorithmic and Experimental Methods in Algebra, Geometry, and Number Theory*. Ed. by Gebhard Böckle, Wolfram Decker, and Gunter Malle. Cham: Springer International Publishing, 2017, pp. 611–622. DOI: 10.1007/978-3-319-70566-8_27.

[Sut16] A. V. Sutherland. "Sato-Tate Distributions". In: *ArXiv e-prints* (Apr. 2016). arXiv: 1604.01256 [math.NT].

[SW05] Jörn Steuding and Annegret Weng. "On the number of prime divisors of the order of elliptic curves modulo p". In: *Acta Arithmetica* 117 (2005). DOI: 10.4064/aa117-4-2.

[Tan99] Sergei G Tankeev. "On weights of the l-adic representation and arithmetic of Frobenius eigenvalues". In: *Izvestiya: Mathematics* 63.1 (1999), p. 181. URL: http://stacks.iop.org/1064-5632/63/i=1/a=A08.

[Tat69] John Tate. "Classes d'isogénie des variétés abéliennes sur un corps fini". fre. In: *Séminaire Bourbaki* 11 (1968-1969), pp. 95–110. URL: http://eudml.org/doc/109770.

[TZ16] J. Thorner and A. Zaman. "A Chebotarev variant of the Brun-Titchmarsh theorem and bounds for the Lang-Trotter conjectures". In: *ArXiv e-prints* (June 2016). arXiv: 1606.09238 [math.NT].

[Wal63] G. E. Wall. "On the conjugacy classes in the unitary, symplectic and orthogonal groups". In: *Journal of the Australian Mathematical Society* 3.1 (Feb. 1963), pp. 1–62. DOI: 10.1017/S1446788700027622.

[Wan90] Daqing Wan. "On the Lang-Trotter conjecture". In: *Journal of Number Theory* 35.3 (1990), pp. 247–268. DOI: http://dx.doi.org/10.1016/0022-314X(90)90117-A.

[Wei49] André Weil. "Numbers of solutions of equations in finite fields". In: *Bull. Amer. Math. Soc.* 55 (1949), pp. 497–508. DOI: 10.1090/S0002-9904-1949-09219-4.

[Wen14] Annegret Weng. "On the Order of Abelian Varieties with Trivial Endomorphism Ring Reduced Modulo a Prime". In: *Finite Fields Appl.* 28.C (July 2014), pp. 115–122. DOI: 10.1016/j.ffa.2014.01.002.

[Wen15] Annegret Weng. "On the order of abelian surfaces of cm-type over finite prime fields". In: *Quaestiones Mathematicae* 38.6 (2015), pp. 771–787. DOI: 10.2989/16073606.2014.981720. eprint: https://doi.org/10.2989/16073606.2014.981720.

[Xio09] Maosheng Xiong. "The Erdős-Kac Theorem for Polynomials of Several Variables". In: *Proceedings of the American Mathematical Society* 137.8 (2009), pp. 2601–2608. URL: http://www.jstor.org/stable/20536025.

[Zyw08] D. Zywina. "The Large Sieve and Galois Representations". In: *ArXiv e-prints* (Dec. 2008). arXiv: 0812.2222 [math.NT].

[Zyw11] David Zywina. "A refinement of Koblitz's conjecture". In: *International Journal of Number Theory* 07.03 (2011), pp. 739–769. DOI: 10.1142/S1793042111004411. eprint: http://www.worldscientific.com/doi/pdf/10.1142/S1793042111004411.

[Zyw13] David Zywina. "The Splitting of Reductions of an Abelian Variety". In: *International Mathematics Research Notices* 2014.18 (2013), p. 5042. DOI: 10.1093/imrn/rnt113. eprint: /oup/backfile/Content_public/Journal/imrn/2014/18/10.1093/imrn/rnt113/2/rnt113.pdf.

[Zyw15] David Zywina. “Bounds for the Lang-Trotter Conjectures”. In: *SCHOLAR – a Scientific Celebration Highlighting Open Lines of Arithmetic Research*. Ed. by A. Cojocaru et al. Contemporary Mathematics, 2015, pp. 235–256.