©Copyright 2018
Travis Scholl

Abelian Varieties with Small Isogeny Class and Applications to Cryptography

Travis Scholl

A dissertation
submitted in partial fulfillment of the
requirements for the degree of

Doctor of Philosophy

University of Washington

2018

Reading Committee:

Neal Koblitz, Chair

William Stein

Ralph Greenberg

Program Authorized to Offer Degree:
Mathematics

University of Washington

Abstract

Abelian Varieties with Small Isogeny Class and Applications to Cryptography

Travis Scholl

Chair of the Supervisory Committee:
Professor Neal Koblitz
Department of Mathematics

An elliptic curve E over a finite field $\mathbb{F}_q$ is called isolated if it admits few efficiently computable $\mathbb{F}_q$-isogenies from E to a non-isomorphic curve. We present a variation on the CM method that constructs isolated curves. Assuming the Bateman-Horn conjecture, we show that there is negligible probability that a curve of cryptographic size constructed via this method is vulnerable to any known attack on the ECDLP. A special case of isolated curves is when the $\mathbb{F}_q$-isogeny class contains only one $\mathbb{F}_q$-isomorphism class. We call an elliptic curve, or abelian variety, super-isolated if it has this property. We give a simple characterization of super-isolated elliptic curves, and several examples of cryptographic size. We prove that there are only 2 super-isolated surfaces suitable for cryptographic use. Finally, we show that for any $g \geq 3$, there are only finitely many super-isolated ordinary simple abelian varities of genus g. Essentially, we have an existence result in the practical range for genus $g \leq 2$, and a non-existence result for the impractical genera $g \geq 3$.

TABLE OF CONTENTS

LIST OF FIGURES

ACKNOWLEDGMENTS

First I would like to thank my adviser Neal Koblitz for all of his support and guidance throughout my graduate career. His patience and inspiration were invaluable while working towards this thesis.

I would also like to thank William Stein for all the opportunities to work on and learn about `Sage`, which made much of my experimental research possible; Bianca Viray for all the helpful talks, classes, and her incredible advice on writing papers, giving talks, and being a modern professional mathematician in academia; Ralph Greenberg for the insightful research discussions as well as serving on my doctoral committee; and Daniela Witten for serving as the Graduate School Representative in the committee.

Finally, I would like to acknowledge all of my graduate student peers. I am grateful to them for all of the helpful advice, listening to me talk about elliptic curves in every seminar, and being available.

Chapter 1

INTRODUCTION

Elliptic curve cryptography (ECC) is a public key cryptosystem that was independently introduced by Neal Koblitz and Victor Miller around 1985 [46, 64]. The security of ECC relies on the elliptic curve discrete log problem (ECDLP). Let E be an elliptic curve over a finite field $\mathbb{F}_q$, and let $P \in E(\mathbb{F}_q)$. The ECDLP can be stated as follows:

Given a multiple Q of P, find an integer k such that $Q = kP$.

The fastest known generic algorithms for solving the ECDLP are Pollard-Rho and Baby-step giant-step, which run in $\tilde{O}(\sqrt{q})$ time [19, Ch. 19]. For some classes of curves, there are faster specialized algorithms[1]:

Pohlig-Hellman Attack: If $\#E(\mathbb{F}_q)$ is smooth (i.e. has no large prime divisor), then the Pohlig-Hellman algorithm [68] can solve the ECDLP in $\tilde{O}(\sqrt{\ell})$ steps, where ℓ is the largest prime divisor of $\#E(\mathbb{F}_q)$.

MOV Attack: The *embedding degree* of E is the smallest integer k such that $\#E(\mathbb{F}_q)$ divides $q^k - 1$. The Menezes-Okamoto-Vanstone (MOV) attack uses the Weil pairing to transfer the ECDLP to the discrete log in $\mathbb{F}_{q^k}^{\times}$, where sub-exponential algorithms are known [60] (see also [27] for a similar attack that uses the Tate pairing). Essentially if $k \leq \log^2 p$, then this method is faster than Pollard-Rho. For randomly chosen curves, k is usually much larger than $\log^2 p$ [49].

[1] Even though they are important to practical applications, we will not discuss side-channel or protocol specific attacks in this thesis. For an overview of some of these other kinds of attacks, see [9, 19] for references.

Additive Transfer: If $\#E(\mathbb{F}_p) = p$, then the ECDLP can be transferred to a discrete log problem in the additive group $\mathbb{F}_p$, where it can be solved in linear time [70, 74, 79].

GHS Attack: Suppose that E is an elliptic curve over a field $\mathbb{F}_{p^a}$ with p small and $a > 1$. In [31], Galbraith and Smart describe an attack on the ECDLP on E based on a technique using Weil descent introduced by Frey [26]. This led to the Gaudry-Hess-Smart (GHS) attack given in [33]. Hess generalized the GHS attack, increasing the number of vulnerable curves [38].

Similar cryptosystems can be built with Jacobians of curves of genus $g \geq 2$. However, the discrete log problem on the Jacobian of a curve of high genus is easier than the ECDLP on a curve of similar size [1]. The gap in difficulty grows with g. Curves of genus ≥ 3 are generally considered impractical for cryptography, while curves of genus 2 are still competitive with ECC [32].

When selecting parameters for ECC and cryptography using higher genus curves, we need to avoid choosing an elliptic curve that is vulnerable to any of the above attacks. Conventional wisdom is that, besides the restrictions imposed by the above attacks, choosing a random curve is better than a special one. For example, the discriminant of a curve $E/\mathbb{F}_q$ is, up to a possible factor of 2, the square-free part of $t^2 - 4q$, where $t = q + 1 - \#E(\mathbb{F}_q)$. Discriminants of curves over $\mathbb{F}_q$ are distributed between 0 and $-4q$. In the interest of greater randomness, SafeCurves recommends choosing curves whose discriminant is at least 2^{100} in absolute value [8]. Brainpool also requires a large discriminant [52, Sec. 3.2]. The randomly generated NIST curves P-224 and P-256 satisfy this constraint [65, Sec. D.1.1.4].

The belief that random curves are more secure than special curves is also exemplified in official recommendations of ECC parameters. Brainpool [52, Sec. 3.2] states:

> The curves shall be generated in a pseudo-random manner using seeds that are generated in a systematic and comprehensive way.

Certicom [15, Sec. 2.1] justifies their use of random curves as follows:

> [Verifiably random parameters] are therefore extremely unlikely to be susceptible to future special-purpose attacks, and no trapdoors can have been placed in the parameters during their generation.

Some standards include both random and special curves. For example. the curve `secp256k1` recommended by Certicom [15, Sec. 2.4.1] has discriminant -3. This curve is also used in Bitcoin for digital signatures. Both Brainpool and SafeCurves would reject this curve because of its small discriminant.

It is important to note that there is no evidence that randomly chosen curves are more secure than special ones. In fact, it is possible that a future attack may target random curves. For example, in [22], Diem and Thomé give an algorithm that solves the discrete log problem on Jacobians of non-hyperelliptic[2] curves of genus $g \geq 3$. This attack is faster than all known generic attacks. Note that hyperelliptic curves of genus $g \geq 3$ are much rarer than non-hyperelliptic ones (they form a subspace of codimension $g-2$ in the moduli space of genus g curves). This shows that, based on our current knowledge, the discrete log problem on randomly chosen Jacobians of curves with genus $g \geq 3$ is less secure than the discrete log problem on hyperelliptic Jacobians.

It is possible to use isogenies, which are morphisms of elliptic curves that preserve the group structure, to transfer an instance of the ECDLP to another curve. The set of curves which E admits an isogeny to is called the isogeny class of E. For reference, the number of (isomorphism classes of) curves over $\mathbb{F}_q$ is $\approx 2q$, and the number of isogeny classes is $\approx 4\sqrt{q}$. So the average isogeny class contains $\approx \sqrt{q}/2$ curves.

An attacker could try to transfer an instance of the ECDLP on E to another curve E' where the attacker may have a better advantage. This is beneficial to the attacker only if the expected time it takes to compute the isogeny from E to E' and solve the ECDLP on E' is less than the expected time to solve the ECDLP on E directly using generic algorithms.

In [41], Jao, Miller, and Venkatesan gave a polynomial time algorithm (assuming the

[2] This attack was extended to roughly 18% of hyperelliptic curves of genus 3 over a given field by Smith [80].

Generalized Riemann Hypothesis) that transfers the ECDLP on E to a random curve in the same endomorphism class as E (the endomorphism class of E is the subset of the isogeny class containing those curves whose endomorphism ring is the same as E's). The isogeny class of most curves contain only a few endomorphism classes, and isogenies between those classes are usually efficiently computable [41, Sec. 6]. If the ECDLP is easier on some proportion ρ of elliptic curves in the same endomorphism class as E, then the time it would take an attacker to transfer the ECDLP on E to one of these curves is inversely proportional to ρ.

There is one publicly known case where isogenies have been successfully used to attack the ECDLP. In [58], Menezes and Teske showed that a small but non-negligible proportion of curves over certain composite degree extensions of $\mathbb{F}_2$ are "weak" in the sense that the generalized GHS attack can solve the ECDLP significantly faster than Pollard-Rho. Specifically, they found that over the field $\mathbb{F}_{2^{3\cdot 59}}$, the probability that a random curve E is weak is roughly 2^{-58}. Moreover, under some reasonable hypotheses, the expected time it takes to compute a chain of efficiently computable isogenies from a random curve E to a weak curve E', and solve the ECDLP on E', is significantly less than the time it would take to solve the ECDLP on E using Pollard-Rho.

Motivated by the results of Menezes and Teske, suppose that a new algorithm is (or has been) discovered that solves the ECDLP significantly faster than the fastest known generic algorithms, but only applies to a subset of "weak" curves. Assume that, over any fixed field $\mathbb{F}_q$ (including the case $q = p$ is prime), the probability ρ that $E/\mathbb{F}_q$ is weak is independent of the isogeny class and endomorphism class of E. If ρ is too small, say $q^{-1/2}$, then this attack is probably impractical. If ρ is too large, say $1 - q^{-1/2}$, then essentially every curve is vulnerable. Therefore we will assume that ρ is small but non-negligible, say $q^{-1/3}$. Under this hypothesis, we want to find elliptic curves E for which it is computationally infeasible to transfer the ECDLP from E to a weak curve.

In [45, Sec. 11], Koblitz, Koblitz, and Menezes show how to use the complex multiplication (CM) method to construct elliptic curves $E/\mathbb{F}_p$ for which it is computationally infeasible to compute isogenies from E to another curve outside of a small set. We call such curves

isolated. Isolated curves are sparse in the space of all elliptic curves over $\mathbb{F}_p$. However, compared to a random curve, they are more likely to be safe against the hypothetical attack described above. A similar construction for hyperelliptic curves of genus 2 is given by Wang in [87].

In this thesis, we build on and further specialize the notion of isolated curves. In Chapter 2, we extend the example of Koblitz, Koblitz, and Menezes and give a general method for constructing isolated curves. The main step of this method is finding values for which several integer polynomials are simultaneously prime. There are few results about how often such values occur. For example, the Twin Prime conjecture, which is still completely open, counts the number of integers x such that x and $x + 2$ are both prime. Therefore, in order to prove properties of our construction, we rely on the Bateman-Horn conjecture [6], which gives an asymptotic estimate for how often several polynomials are simultaneously prime. Using this conjecture, we show that isolated curves are almost always resistant to the MOV attack.

In Chapters 2 and 3 we introduce *super-isolated* abelian varieties, whose isogeny class contains one isomorphism class. In Chapter 3, we show that there are only 2 super-isolated abelian surfaces that would be practical for cryptography. In Chapter 4, we prove that, for any $g \geq 3$, there are finitely many super-isolated abelian varieties of dimension g. Essentially, we have an existence result in the practical range for genus $g \leq 2$, and a non-existence result for the impractical genera $g \geq 3$.

Chapter 2

ISOLATED ELLIPTIC CURVES AND THE MOV ATTACK

2.1 Introduction

The security of elliptic curve cryptosystems is based on the difficulty of the elliptic curve discrete logarithm problem (ECDLP). For an elliptic curve E over a prime field $\mathbb{F}_p$, the best known generic attack on the ECDLP takes roughly $\sqrt{p}$ operations. Suppose that a new algorithm $\mathcal{X}$ was found that could solve the ECDLP on a subset W of elliptic curves over $\mathbb{F}_p$ faster than all previously known algorithms. Given an instance of the ECDLP on E, if an attacker could construct an isogeny $\varphi : E \to E'$ with $E' \in W$, then they could transfer the instance to E' where they could use $\mathcal{X}$. The total time for this attack is bounded below by the time m that it takes to compute φ. If $m \geq \sqrt{p}$, then this attack is no faster than generic algorithms, no matter how fast $\mathcal{X}$ is. Let $\mathcal{T}$ denote the set of curves E' such that an isogeny $\varphi : E \to E'$ can be computed in less than $\sqrt{p}$ time. We will assume that the probability that a random curve in $\mathcal{T}$ lies in W, is roughly the ratio ϵ of $|W|$ to the number of elliptic curves over $\mathbb{F}_p$. For a random E, we expect that $|\mathcal{T}| \approx \sqrt{p}$, which in practice is $\approx 2^{128}$. However, it is possible for $|\mathcal{T}|$ to be much smaller, so that E is resistant to this attack. For example, if $\epsilon \approx 2^{-50}$ and $|\mathcal{T}| \leq 1000$, then the probability that the ECDLP on E can be efficiently transfered to some $E' \in W$ is about 2^{-40}. In this case, we call E isolated (a precise definition is given below). In this paper, we give an algorithm based on the complex multiplication (CM) method to generate isolated elliptic curves that are suitable for cryptography.

Remark 1. The hypothetical attack outlined above is motivated by the case of elliptic curves over composite degree extensions of prime fields (usually $\mathbb{F}_2$). In that case, Weil descent can sometimes be used to solve the ECDLP significantly faster than generic methods on a small but non-negligible proportion of curves [58, 59].

The *conductor gap* (see Definition 13) between two elliptic curves measures the difficulty of constructing an isogeny between them. If the conductor gap between E and E' is L, then the fastest known algorithm for computing an isogeny between E and E' takes roughly L^3 time. We say an elliptic curve E is (L, T)-*isolated* if there are at most T curves whose conductor gap with E is at most L. For example, if E is $(p^{1/6}, 1000)$-isolated, then there are at most 1000 curves E' for which it would be feasible to construct an isogeny $E \to E'$. Thus E is most likely resistant to the hypothetical attack described above.

In addition to being resistant to the hypothetical attack above, isolated curves should be resistant to known attacks on the ECDLP, such as the MOV attack, named after the authors of [60]. The MOV attack reduces the ECDLP on an elliptic curve $E/\mathbb{F}_p$ to $\mathbb{F}_{p^k}^\times$. The smallest possible k is called the *embedding degree*. This reduction is only practical if k is $< \log^2 p$. Our main theorem shows that, under the Bateman-Horn conjecture, curves produced by our algorithm almost always have embedding degree larger than $\log^2 p$.

Theorem 2. *Assume the Bateman-Horn conjecture. There is an algorithm that takes as input a bound M, and returns an elliptic curve E over a prime field $\mathbb{F}_p$ such that the following hold:*

(i) $M/2 \leq p \leq M$

(ii) $\#E(\mathbb{F}_p) = rf$ *where* r *is prime and* $f \mid 24$

(iii) E *is* $(\sqrt{p/50 - 100}, 8)$*-isolated.*

The expected running time of the algorithm is $O(\log^3 M)$ *multiplied by the time required to test if an integer of size* M *is prime. If* M *is sufficiently large, then the probability that the returned curve has an embedding degree less than* $\log^2 p$*, is bounded above by*

$$C\frac{\log^8 M}{\sqrt{M}}$$

for some effectively computable constant C*.*

Remark 3. The Bateman-Horn conjecture is used to estimate how often several polynomials are simultaneously prime. While the conjecture gives an asymptotic formula for any collection of polynomials, we only require a big-Ω statement for how often three particular polynomials are simultaneously prime (see Problem 34).

Remark 4. Experimentally, our algorithm works well when $M \approx 2^{256}$. After several thousand iterations, it never produced a curve with embedding degree $> \log^2 p$ and finished within the expected time (see Section 2.6.4). However, we are unable prove an explicit lower bound for what "sufficiently large" is, nor can we give a computable upper bound for the implicit constant in the big-O notation for the run time. In Section 2.6, we discuss these points as well as provide a reasonable assumption to solves these issues.

Theorem 2 should be compared with the generic probability that a curve with prime order has embedding degree $< \log^2 p$.

Theorem 5 (Balsubramanian and Koblitz [5, Thm. 2])**.** *Let p be a uniformly random prime in the interval $[M/2, M]$, and E a random elliptic curve over $\mathbb{F}_p$ of prime order. The probability that the embedding degree of E is less than $\log^2 p$, is bounded above by*

$$C\frac{\log^9 M(\log\log M)^2}{M},$$

for some effectively computable constant C.

Remark 6. When giving a conditional theorem in cryptography, it is important to avoid contrived conjectures that are custom built to fill gaps in security proofs [48], [44, Sec. 1.4.2]. The Bateman-Horn conjecture is of independent interest. It predates elliptic curve cryptography, and is a generalization of the well-known hypothesis H from Schinzel [71]. It is supported by substantial theoretical and numerical evidence. For this reason we feel that the use of the conjecture is justified.

The rest of the paper is organized as follows. In Section 4.2 we briefly review background material as well as set notation for the rest of the paper. In Section 2.3 we define isolated curves, and in Section 2.4 we outline a method for generating them. In Section 2.5 we show

that our algorithm has a high probability of producing curves that are resistant to the MOV attack, and prove Theorem 2. In Section 2.6, we explain some limitations of our results and give some heuristics suggesting that these limitations do not appear in practice.

2.2 Background and Notation

Let E be an elliptic curve over a prime field $\mathbb{F}_p$. We will primarily consider primes on the order of 2^{256}. Let $N = |E(\mathbb{F}_p)|$ be the number of points, and $t = p + 1 - N$. If $t \equiv 0 \mod p$ then E is vulnerable to the MOV attack [60], so we will only consider the case when $t \not\equiv 0 \mod p$. In this case E is called *ordinary*.

An *isogeny* is a surjective morphism of elliptic curves with finite kernel. The set of isogenies $E \to E$ defined over the algebraic closure $\overline{\mathbb{F}}_p$ of $\mathbb{F}_p$, together with the 0 map form the *endomophism ring* $\operatorname{End} E = \operatorname{End}_{\overline{\mathbb{F}}_p} E$. If E is ordinary then $\operatorname{End} E$ is isomorphic to an order in an imaginary quadratic field K.

Let $\pi \in \operatorname{End} E$ denote the Frobenius endomorphism, which on the level of points takes $(x, y) \mapsto (x^p, y^p)$. We identify π with an element of K. Then $\operatorname{Trace} \pi = t$ and $\operatorname{Norm}(\pi) = p$ [78, Ch. V]. This means that we can identify $\pi = \frac{t + c\sqrt{-d}}{2}$, where $-d = \operatorname{Disc} K$ and $c > 0$. Notice that $\mathbb{Z}[\pi]$ is the order in K of conductor c, and that

$$4p = t^2 + dc^2. \tag{2.1}$$

Given an elliptic curve E, there is an associated number $j(E)$ which determines the isomorphism type of E over $\overline{\mathbb{F}}_p$. $j(E)$ is called the *j-invariant of* E. Throughout the rest of the paper, unless otherwise noted, E will represent an ordinary elliptic curve over the prime field $\mathbb{F}_p$.

2.2.1 Isogeny Classes

Definition 7. The *isogeny class* I of E is the set of isomorphism classes (over $\mathbb{F}_p$) of elliptic curves that are isogeneous (over $\mathbb{F}_p$) to E.

The isogeny class of E is uniquely determined by $N = \#E(\mathbb{F}_p)$. This follows from Tate's isogeny theorem, which says that two elliptic curves over $\mathbb{F}_p$ are isogeneous if and only if they have the same number of points [78, Exercise. 5.4]. For every integer N in the Hasse interval $[p+1-2\sqrt{p}, p+1+2\sqrt{p}]$, there is an elliptic curve with N points. Thus by Tate's thereom, there are about $4\sqrt{p}$ isogeny classes. One can show using the j-invariant that there are roughly $2p$ isomorphism classes of elliptic curves over $\mathbb{F}_p$. This means that on average, each isogeny class has about $\sqrt{p}/2$ curves.

An *ℓ-isogeny* is an isogeny of degree ℓ. We will only consider ℓ-isogenies with ℓ a prime other than p. Such isogenies are separable and have a kernel of size ℓ. Any separable isogeny between elliptic curves factors into a composition of isogenies of prime degree.

2.2.2 Endomorphism Classes

The isogeny class I of E can be partitioned into endomorphism classes. Let $I_{\mathcal{O}}$ denote the set of curves in I whose endomorphism ring is isomorphic to $\mathcal{O}$, an order in an imaginary quadratic field. We call $I_{\mathcal{O}}$ the *endomorphism class of $\mathcal{O}$ in I*.

Proposition 8. *The endomorphism classes in I are precisely those associated to orders in the quadratic imaginary field $\mathbb{Q}(\pi)$ that contain $\mathbb{Z}[\pi]$. For any $\mathcal{O} \supseteq \mathbb{Z}[\pi]$, the size of $I_{\mathcal{O}}$ is equal to the class number $h(\mathcal{O})$.*

Proof. See Theorems 4.3 and 4.5 from [73]. □

Endomorphism classes have $O(\sqrt{p}\log d)$ curves. To see this, let c' be the conductor of an order appearing in I. Recall that the class number of an order of conductor c' is approximately hc' (see [21, Thm. 7.24] for a precise formula). The class number h is bounded above by $\frac{1}{\pi}\sqrt{d}\log d$ [17, Excercise 5.27b]. We also know that c' divides c because every order appearing in I contains the Frobenius ring $\mathbb{Z}[\pi]$. It follows from (2.1) that $hc' \leq hc \leq \frac{c}{\pi}\sqrt{d}\log d < \frac{2}{\pi}\sqrt{p}\log d$.

For a random curve E over $\mathbb{F}_p$ for a random prime p, we expect that c is close to 1 [41, Sec. 6]. Because the endomorphism classes in I correspond to divisors of c, we do not expect

to find many endomorphism classes. Thus on average, we should expect that $I_{\mathrm{End}\, E}$ usually has roughly $\sqrt{p}$ curves.

2.2.3 Bateman-Horn Conjecture

We will be interested in how often several polynomials are simultaneously prime. For a single polynomial of degree one, we have the prime number theorem and Dirichlet's theorem on primes in arithmetic progressions. Bateman and Horn made the following conjecture based on heuristics derived from the prime number theorem.

Definition 9. We say that a polynomial $f \in \mathbb{Z}[x]$ satisfies *Bunyakovsky's property* if $\gcd_{a\in\mathbb{Z}} f(a) = 1$.

Warning 10. In order for f to satisfy Bunyakovsky's property, it is necessary that the coefficients of f are relatively prime. This condition is not sufficient, for example $\gcd_{a\in\mathbb{Z}}(a^2 + a) = 2$.

Conjecture 11 (Bateman-Horn Conjecture [6])**.** Let $f_1, \ldots, f_k \in \mathbb{Z}[x]$ be distinct irreducible polynomials such that their product $\prod f_i$ satisfies Bunyakovsky's property. Let

$$P_{f_1,\ldots,f_k}(N) = \{a \in \mathbb{Z} \colon 1 \le a \le N \text{ and } f_i(a) \text{ is prime for all } i = 1, \ldots, k\}.$$

Then

$$|P_{f_1,\ldots,f_k}(N)| \sim \frac{C}{D}\frac{N}{\log^k N}. \tag{2.2}$$

Here $D = \prod \deg f_i$, $C = \prod_{\ell \text{ prime}} \frac{1-\omega(\ell)/\ell}{(1-1/\ell)^k}$, and $\omega(\ell)$ denotes the number of roots of $\prod f_i$ in $\mathbb{F}_\ell$.

Remark 12. There is a large amount of theoretical and numerical evidence for the Bateman-Horn conjecture. It reduces to Dirichlet's theorem on primes in arithmetic progressions for a single polynomial of degree 1. It also agrees with the twin prime conjecture and the Sophie Germain prime conjecture [76, Ch. 5.5]. More recently, an analog of the conjecture has been proven for function fields [24].

2.2.4 The MOV Attack

The MOV attack transfers a discrete log from $E(\mathbb{F}_p)$ to $\mathbb{F}_{p^k}^\times$ for some positive integer k. The idea is to leverage sub-exponential time algorithms for solving discrete logs in the multiplicative group of a finite field. A necessary condition for this transfer is that $|E(\mathbb{F}_p)|$ divides $p^k - 1$. The smallest possible k is called the *embedding degree*[1] of E. This is the same as the multiplicative order of p in $(\mathbb{Z}/N\mathbb{Z})^\times$ where $N = |E(\mathbb{F}_p)|$. For more on the MOV attack see [60][2] or [78, Ch. XI.6].

If $k > \log^2 p$, then the MOV attack will not be faster than trying to solve the discrete log on E directly [5]. Therefore we are primarily interested in curves with embedding degree $> \log^2 p$.

2.3 Isolated Curves

Definition 13. The *conductor gap* of two orders in a fixed quadratic imaginary field is the largest prime dividing the conductor of one and not the other. The conductor gap between two isogenous elliptic curves is defined to be the conductor gap of their endomorphism rings. If the curves are not isogeneous, then their conductor gap is ∞. The *L-conductor-gap class* of a curve E is the set of all curves E' such that the conductor gap between E and E' is less than L.

Proposition 14. *Let $\varphi : E \to E'$ be an ℓ-isogeny for some prime ℓ. If $\mathcal{O}$ and $\mathcal{O}'$ are the endomorphism rings of E and E' respectively, then one of the following holds:*

$$[\mathcal{O} : \mathcal{O}'] = \ell, \quad [\mathcal{O}' : \mathcal{O}] = \ell, \quad \mathcal{O} = \mathcal{O}'.$$

[1] The embedding degree may also refer to the multiplicative order of p in $(\mathbb{Z}/r\mathbb{Z})^\times$ where r is the largest prime factor of N. This is because cryptosystems are usually constructed using the largest prime order subgroup of the elliptic curve group, rather than the entire group. We will only be interested in curves with nearly prime order, so the difference between using N or r is not important. Also implicitly we are avoiding anomalous curves where $N = p$, i.e. $t = 1$. Anomalous curves are extremely rare but should be avoided as there are known attacks against them [79].

[2] Technically, the attack of [60] requires that N be relatively prime to $p - 1$. But, if this is not the case then there is an attack described by Frey and Rück [27] which also transfers the ECDLP to $\mathbb{F}_{p^k}^\times$. We will not differentiate between the two since both attacks require a small embedding degree.

Proof. [50, Prop. 21]. □

In the first two cases of Proposition 14, we say that φ is *vertical*; otherwise φ is *horizontal*. Horizontal isogenies stay inside the same endomorphism class while vertical ones move to a new class. The main implication of Proposition 14 is that if two endomorphism classes have conductor gap a prime ℓ, then any isogeny between them factors through an ℓ-isogeny. Unless otherwise noted, throughout the rest of the paper ℓ will denote a prime not equal to p.

Definition 15. Let E be an elliptic curve over $\mathbb{F}_p$. We will say E is *isolated with gap L and set-size T*, or (L, T)-isolated, if the L-conductor-gap class of E has at most T curves.

Remark 16. The observation that isolated curves are resistant to isogeny based attacks has been noted before in the literature. This idea is discussed in [45, Sec.11.2], [42, Sec. 7.1], and [58, Rem. 6]. This idea has also been applied to Jacobians of curves of genus 2 [87].

2.3.1 Computational Complexity of Isogenies

The computational complexity of an isogeny depends on its degree, but the complexity is different for horizontal and vertical isogenies. The fastest known method [50] for constructing a vertical isogeny from E involves constructing the modular polynomial Φ_ℓ. Finding Φ_ℓ mod p is the most expensive step and the best known methods take $\widetilde{O}(\ell^3)$ time and $\widetilde{O}(\ell^2)$ space [14] (recall that $\widetilde{O}(f)$ means $O(f \log^k f)$ for some integer k). Φ_ℓ is a polynomial of degree $\ell+1$ in two variables, so any method which involves computing Φ_ℓ must take $\Omega(\ell)$ time and space. Moreover, because we represent ℓ-isogenies using either polynomials of degree ℓ, or a list of points in the kernel; any algorithm which computes an ℓ-isogeny will need at least $\Omega(\ell)$ space.

For horizontal isogenies where the endomorphism ring has a small discriminant, there are much faster algorithms which are polynomial in $\log \ell$ [13, 43]. These methods do not extend to vertical isogenies crossing a large conductor gap. Therefore we can only effectively

transport the ECDLP to another endomorphism class when the conductor gap is less than $p^{1/6}$.

The best algorithm known for solving the ECDLP on a general elliptic curve takes $\widetilde{O}(\sqrt{p})$ time [63]. If $\ell \geq p^{1/6}$, then computing a vertical ℓ-isogeny takes similar time to solving the ECDLP. If two endomorphism classes have a conductor gap of at least $p^{1/6}$, then there is no significant benefit in transferring the ECDLP across the gap.

2.3.2 Examples

Example 17. Let E be the elliptic curve $y^2 = x^3+6x$ over $\mathbb{F}_p$ where $p = 12475737285765000161 \approx 2^{63.4}$. Note that $\operatorname{End} E \cong \mathbb{Z}[i]$ has class number 1, so E is the only curve in its endomorphism class. The Frobenius endomorphism π generates an order $\mathbb{Z}[\pi]$ with prime conductor $c = 2559154831 \approx 2^{31.2}$. This means that the isogeny class of E has two endomorphism classes: One which contains only E, and another which contains $h(\mathbb{Z}[\pi]) = 1279577416 \approx 2^{30.2}$ curves. Because the conductor gap between the classes is $c \approx \sqrt{p}$, this shows that E is isolated with gap 2^{31} and set-size 1.

Example 18. Let E be the elliptic curve $y^2 = x^3 + 350x$ over $\mathbb{F}_p$ where $p = 122501$. As in the previous example, the endomorphism class of E has only one curve. However, in this case $\mathbb{Z}[\pi]$ has conductor 1, so the isogeny class of E contains only E, and E is $(\infty, 1)$-isolated. This example is highly atypical because the trace $t = 700 = \lfloor 2\sqrt{p} \rfloor$ is at the extreme end of the Hasse bound.

2.4 Generating Isolated Curves

In this section we give an algorithm to generate isolated elliptic curves. We will apply some slight modifications to the algorithm presented here in order to prove Theorem 2. For use in cryptography, we would like to generate prime ordered curves. However there are some basic obstructions to a curve having prime order. For example, consider equation 2.1. In order for p to be an odd prime, if d is even then t must be even. It follows that $N = p+1-t$

is also even. In this case, the choice of d forced a factor of 2 to divide N. Fortunately, the only obstructions to N being prime are a few factors of 2 and 3.

For any integer $a \equiv 0, 3, 4 \mod 8$, define[3] the *cofactor* to be

$$\mathrm{cof}_a = 2^{\nu_2} \cdot 3^{\nu_3}, \tag{2.3}$$

where

$$\nu_2 = \begin{cases} 0 & \text{if } a \equiv 3, 11, 19, 27 \mod 32 \\ 1 & \text{if } a \equiv 4, 8, 20, 24 \mod 32 \\ 2 & \text{if } a \equiv 0, 12, 16 \mod 32 \\ 3 & \text{if } a \equiv 28 \mod 32, \end{cases}$$

$$\nu_3 = \begin{cases} 0 & \text{if } a \not\equiv 2 \mod 3 \\ 1 & \text{if } a \equiv 2 \mod 3. \end{cases}$$

Algorithm 1 Isolated Curve

Input: a positive integer M and fundamental discriminant $-d < 0$.

Output: an elliptic curve defined over $\mathbb{F}_p$ where $\frac{dM}{16} < p < \frac{dM}{4}$

1: **repeat** steps 2-5
2: $t \leftarrow$ random integer in $\left[-\sqrt{M}, \sqrt{M}\right] \setminus \{0, 1, 2\}$
3: $c \leftarrow$ random integer in $\left[\frac{\sqrt{M}}{2}, \sqrt{M}\right]$
4: $p \leftarrow \frac{t^2+dc^2}{4}$
5: $N \leftarrow p + 1 - t$
6: **until** p, N/cof_{dc^2} are integers and $p, c, N/\mathrm{cof}_{dc^2}$ are prime
7: $j \leftarrow$ root of the Hilbert class polynomial for $\mathbb{Q}(\sqrt{-d})$ mod p
8: $E \leftarrow$ elliptic curve over $\mathbb{F}_p$ with $j(E) = j$ and $|E(\mathbb{F}_p)| = N$
9: **return** E

[3]The value of cof_a was calculated by considering the equation $4N = (t-2)^2 + a$ modulo powers of 2 and 3. Here a represents dc^2 from equation 2.1.

Remark 19. Algorithm 1 is not optimized for efficiency. For example, if $d \equiv 0 \mod 4$ then t must be even. Thus by choosing only even values of t in step 2, we expect the runtime to be reduced by a factor of 2. We present the unoptimized version for simplicity.

Remark 20. The reason for removing $0, 1, 2$ from possible values of t is to avoid the attacks described in [79], [60], and [27].

Remark 21. One drawback[4] of using the CM method is that we do not have full control over the prime p. That is, we can not choose p arbitrarily and then construct an isolated curve over $\mathbb{F}_p$. This makes it more difficult to find p with special properties, such as a small Hamming weight (which can lead to more efficient implementations). However, we can lower the Hamming weight of p with the following modifications. Instead of choosing c randomly, fix c to be a large prime of small Hamming weight. Also, restrict the search for t to integers with small Hamming weight. Because p is given by a simple expression in t and c, the resulting value of p will likely have small Hamming weight.

First we will explain the last steps of the algorithm. The following facts are the basis of the well known CM method [19, Ch. 18.1]:

(i) The Hilbert class polynomial of $K = \mathbb{Q}(\sqrt{-d})$ has a root in $\mathbb{F}_p$ by construction.

(ii) There exists an elliptic curve $E/\mathbb{F}_p$ with N points and $j(E) = j$.

An efficient algorithm for finding E, given j and N can be found in [69]. Since $j(E)$ is a root of the Hilbert class polynomial mod p, it follows that $\operatorname{End} E \cong \mathcal{O}_K$ [84, Sec. 2.8]. If the choice of d is bounded by a constant, then steps 7 and 8 in the algorithm have a running time of $O(1)$. The main factor in the running time comes from the loop in steps 2 through 5.

Proposition 22. *If the main loop of Algorithm 1 terminates, then the curve E returned by the algorithm is isolated with gap $\frac{\sqrt{M}}{2}$ and set-size $\frac{1}{\pi}\sqrt{d}\log d$.*

[4] We would like to thank the referee for pointing out this drawback.

Proof. We are assuming $p, c, N/\operatorname{cof}_{dc^2}$ are prime and we want to show that E is isolated. Let $K = \mathbb{Q}(\sqrt{-d})$. By the explanation above, $\operatorname{End} E \cong \mathcal{O}_K$. Let $\pi \in \operatorname{End} E$ denote the Frobenius endomorphism of E. In $\mathcal{O}_K$, π corresponds (up to conjugation) to $\frac{t+c\sqrt{-d}}{2}$. We also know that $c = [\mathcal{O}_K : \mathbb{Z}[\pi]]$. Because c was chosen to be prime, there are two endomorphism classes in the isogeny class of E corresponding to $\mathcal{O}_K$ and $\mathbb{Z}[\pi]$. The endomorphism class of $\mathcal{O}_K$ contains $h(\mathcal{O}_K) \leq \frac{1}{\pi}\sqrt{d}\log d$ curves. Therefore, E is isolated with gap $c \geq \frac{\sqrt{M}}{2}$ and set-size $\frac{1}{\pi}\sqrt{d}\log d$. □

Remark 23. It is easy to alter Algorithm 1 to produce curves that are $(\infty, 1)$-isolated, meaning that the entire isogeny class contains a single curve, similar to Example 18. To do this, we choose d such that $\mathbb{Q}(\sqrt{-d})$ has class number 1, and fix $c = 1$. However, we do not know how to prove that curves generated this way usually have an embedding degree $> \log^2 p$. This is because there are too few values of t such that p and N/cof_d are simultaneously prime. Even though the Bateman-Horn conjecture gives an asymptotic formula, it is not enough to prove a bound on the embedding degree using the methods in Section 2.5. Moreover, due to their rarity, one could argue that $(\infty, 1)$-isolated curves are too special for cryptography, and that there may not be sufficient randomness in their selection.

2.5 Improbability of the MOV Attack on Isolated Curves

2.5.1 Notation

In [5], Balasubramanian and Koblitz proved that a random prime order elliptic curve over a random prime field almost always has a large embedding degree. Their work has been extended in several ways [20, 55]. We want to emulate the main theorem of [5] for isolated curves. The main difference is that in [5], the authors were able to vary the prime and the number of points subject only to the Hasse bound. There is less flexibility in our case due to restrictions on the conductor c and the discriminant d.

We will use the following notation:

$-d =$ fixed small (< 100) fundamental discriminant of a quadratic imaginary field

$$p = p(t,c) = \frac{t^2 + dc^2}{4}, \qquad N = N(t,c) = p + 1 - t,$$
$$\mathrm{cof} = \mathrm{cof}(c) = \mathrm{cof}_{cd^2} \text{ as defined in section 2.4}, \qquad r = r(t,c) = \frac{N}{\mathrm{cof}}.$$

Remark 24. Note that r is *not* a polynomial in t, c because $\mathrm{cof}(c)$ depends only on the valuation of dc^2 at 2 and 3. We will apply a linear change of variables in c in order to fix the cofactor.

Define the following sets:

$$\begin{aligned} S_M &= \left\{(t,c) \in \left[1, \sqrt{M}\right] \times \left[\sqrt{M}/2, \sqrt{M}\right] : p, r, c \text{ are prime}\right\} \\ S_{M,K} &= \left\{(t,c) \in S_M : \text{the order of } p \text{ in } (\mathbb{Z}/r\mathbb{Z})^\times \text{ is at most } K\right\} \\ S_M(t) &= \{c : (t,c) \in S_M\} \\ S_{M,K}(t) &= \{c \in S_M(t) : (t,c) \in S_{M,K}\}. \end{aligned}$$

S_M represents possible pairs t, c that Algorithm 1 could use to generate an isolated curve. In particular, the expected number of pairs t, c sampled by Algorithm 1 is $\frac{|S_M|}{M}$. $S_{M,K}$ represents those pairs which result in a curve with embedding degree at most K. $S_M(t)$ and $S_{M,K}(t)$ represent pairs with a fixed t value.

2.5.2 Main Results

Our goal for this section is to find an upper bound for $\frac{S_{M,K}(t_0)}{S_M(t_0)}$ for a fixed integer t_0. This is roughly the probability that Algorithm 1 returns a curve with embedding degree at most K given that $t = t_0$.

First we give an upper bound for $S_{M,K}(t_0)$.

Proposition 25. *Let K, M be any positive integers. Then there is a universal constant $\mathcal{A}_1$ such that for any integer t_0 with $|t_0| > 1$,*

$$|S_{M,K}(t_0)| < \mathcal{A}_1 K^2 \log |t_0|.$$

Proof. Let $L_k = \{\text{primes } \ell\colon \ell \mid (t_0-1)^k - 1\}$. By construction $r \mid p^k - 1 \Leftrightarrow r \mid (p-N)^k - 1 = (t_0-1)^k - 1$. Hence there is a map $\varphi : S_{M,K}(t_0) \to \bigcup_{k=1}^{K} L_k$ given by $c \mapsto r(t_0, c)$.

Next we will show that $|\varphi^{-1}(\ell)| \leq 16$. Note that $N(t_0, c)$ is a quadratic polynomial in c, so there are at most 2 values of c such that $N(t_0, c)$ is the same. There are 8 possible values of cof_c, hence there are at most 16 values of c which could give the same value of $r(t_0, c)$. Therefore

$$|S_{M,K}(t_0)| = \left|\varphi^{-1}\left(\bigcup_{k=1}^{K} L_k\right)\right| \leq 16\left|\bigcup_{k=1}^{K} L_k\right|.$$

It remains to bound the L_k. The number of prime divisors of $(t_0-1)^k - 1$ is bounded by $\log_2 |t_0-1|^k \leq k \log_2(|t_0|+1)$. Hence

$$\left|\bigcup_{k=1}^{K} L_k\right| \leq \sum_{k=1}^{K} |L_k| \leq \sum_{k=1}^{K} k \log_2(|t_0|+1) = \frac{K(K+1)}{2}\log_2(|t_0|+1) \leq 2.4K^2 \log(|t_0|).$$

The last inequality holds for all $|t_0| \geq 2$, so we may take $\mathcal{A}_1 = 2.4$. □

Next we will to bound $S_M(t_0)$ from below. Because t_0 is fixed, we will be able to apply the Bateman-Horn conjecture. However, in order to apply the conjecture, we first need a change of coordinates which makes p and r into polynomials satisfying Bunyakovsky's property.

Lemma 26. *Let $-d$ be a fundamental discriminant for a quadratic imaginary field such that $d < 100$. Then there are computable constants $m_1, b_1, m_2, b_2 \in \mathbb{Z}_{\geq 0}$, such that the linear change of variables $t' = t'(t) = m_1 t + b_1$ and $c' = c'(c) = m_2 c + b_2$ satisfy:*

(i) $f_{d(c')^2}$ is constant as a function of c.

(ii) $p' = p(t', c')$ and $r' = r(t', c')$ are integer polynomials in t and c.

(iii) For any $t \in \mathbb{Z}$, the product $p' \cdot r' \cdot c' / \gcd(m_2, b_2)$ satisfies Bunyakovsky's property as a polynomial in c.

Remark 27. In condition (iii) of Lemma 26, we include $c'/\gcd(m_2, b_2)$ rather than just c' because of the case $d \equiv 7 \mod 8$. In this case, $p = \frac{t^2+dc^2}{4}$ is an odd integer only if t and

c are even. In particular, we cannot have both c' and p' simultaneously prime when $d \equiv 7 \mod 8$.

Proof of Lemma 26. We will prove the claim in detail for $d = 4$ by showing $t' = 3840t$ and $c' = 2c + 1$ satisfy properties (i)-(iii). The other cases are similar, and the corresponding change of coordinates are given in Table 2.1.

(i) For any c, we have that $d(c')^2 \equiv 4 \mod 32$ and $d(c')^2 \not\equiv 2 \mod 3$. Hence $\mathrm{cof}_{d(c')^2} = 2$ for all c.

(ii) To show p' and r' are integer polynomials, we just have to expand out the definitions:

$$p' = p(t', c') = 3686400t^2 + 4c^2 + 4c + 1$$
$$r' = r(t', c') = N(t', c')/2 = 1843200t^2 + 2c^2 - 1920t + 2c + 1.$$

(iii) Let $g(t, c) = p' \cdot r' \cdot c' \in \mathbb{Z}[t, c]$ and $t_0 \in \mathbb{Z}$. To show that $g(t_0, c) \in \mathbb{Z}[c]$ satisfies Bunyakovsky's property, it is sufficient to check that $\gcd\{g(t_0, 0), \ldots, g(t_0, 5)\} = 1$ as $g(t_0, c)$ is a degree 5 polynomial in c.[5]

A direct computation[6] shows that

$$3g(t, 0) + 4g(t, 1) + 17g(t, 2) - 36g(t, 3) + 23g(t, 4) - 5g(t, 5) = 960.$$

Therefore

$$\begin{aligned}\gcd\{g(t_0, 0), \ldots, g(t_0, 5)\} &= \gcd\{g(t_0, 0), \ldots, g(t_0, 5), 960\} \\ &= \gcd\{g(0, 0), g(0, 1), \ldots, g(0, 5)\} \\ &= 1.\end{aligned}$$

The second to last equality follows from the fact that $t' \equiv 0 \mod 960$ by construction. The last equality follows from the fact that $g(0, 0) = 1$.

d	t'	c'
3	$2160\ t + 1$	$2\ c + 1$
4	$3840\ t$	$2\ c + 1$
7	$94080\ t + 10$	$4\ c$
8	$46080\ t + 6$	$6\ c + 1$
11	$87120\ t + 15$	$6\ c + 1$
15	$432000\ t + 34$	$4\ c$
19	$86640\ t + 1$	$2\ c + 1$
20	$288000\ t + 24$	$6\ c + 1$
23	$82270080\ t + 10$	$12\ c$
24	$138240\ t + 10$	$2\ c + 1$
31	$1845120\ t + 10$	$4\ c$
35	$882000\ t + 3$	$6\ c + 1$
39	$2920320\ t + 10$	$4\ c$
40	$384000\ t + 6$	$2\ c + 1$
43	$443760\ t + 1$	$2\ c + 1$

d	t'	c'
47	$343543680\ t + 10$	$12\ c$
51	$624240\ t + 1$	$2\ c + 1$
52	$648960\ t + 4$	$2\ c + 1$
55	$5808000\ t + 18$	$4\ c$
56	$2257920\ t + 6$	$6\ c + 1$
59	$2506320\ t + 15$	$6\ c + 1$
67	$1077360\ t + 1$	$2\ c + 1$
68	$3329280\ t + 12$	$6\ c + 1$
71	$783976320\ t + 10$	$12\ c$
79	$11982720\ t + 10$	$4\ c$
83	$4960080\ t + 3$	$6\ c + 1$
84	$1693440\ t + 40$	$2\ c + 1$
87	$14532480\ t + 10$	$4\ c$
88	$1858560\ t + 6$	$2\ c + 1$
91	$1987440\ t + 1$	$2\ c + 1$
95	$1403568000\ t + 34$	$12\ c$

Table 2.1: Choices of t',c' in Lemma 26 found using `Sage`.

□

Remark 28. We expect Lemma 26 to hold for all d with many different possibilities for m_i, b_i.

Proposition 29. *Assume the Bateman-Horn conjecture and that* $d < 100$ *and* $d \not\equiv 7 \mod 8$. *Let* m_1, b_1 *be the constants from Lemma 26. For any integer* t_0, *there are constants* $\mathcal{A}_2, \mathcal{B}_2$ *such that for all* $M > \mathcal{B}_2$,

$$|S_M(m_1 t_0 + b_1)| > \mathcal{A}_2 \frac{\sqrt{M}}{\log^3 M}.$$

The constants $\mathcal{A}_2, \mathcal{B}_2$ *depend on* t_0. *Moreover, the constant* $\mathcal{A}_2$ *is effectively computable.*

Proof. Let $t'(t) = m_1 t + b_1$ and $c'(c) = m_2 c + b_2$ be the change of coordinates given by Lemma 26. Then $p' = p(t'(t_0), c')$, $r' = r(t'(t_0), c')$, and c' are integer polynomials in $\mathbb{Z}[t, c]$, and satisfy Bunyakovsky's property. Moreover, p' and r' are irreducible because their roots are linear combinations of the roots of $p(t_0, c)$, $N(t_0, c)$ respectively. The latter are complex as long as $t'(t_0) \neq 0, 2$. Thus p', r', and c' satisfy the hypothesis of the Bateman-Horn conjecture as polynomials in $\mathbb{Z}[c]$.

Let $S'_M(t_0)$ denote the set of c_0 such that $c'(c_0) \in S_M(t'(t_0))$, and

$$P_{p',r',c'}(\sqrt{M}) = \left\{ c_0 \in [1, \sqrt{M}] \colon p'(c_0),\ r'(c_0), \text{ and } c'(c_0) \text{ are prime} \right\}.$$

By above, we can apply the Bateman-Horn conjecture to the polynomials p', r', and c'. This means that there is a constant $\mathcal{C}$, depending on the polynomials p', r', and c' (which depend only on d and t_0), such that

$$\left| P_{p',r',c'}(\sqrt{M}) \right| \sim \mathcal{C} \frac{\sqrt{M}}{\log^3 \sqrt{M}}.$$

Notice that $S'_M(t_0) = P_{p',r',c'}(\sqrt{M}) \cap J(\sqrt{M})$ where $J(M) = [\frac{1}{m_1}(\frac{1}{2}\sqrt{M} - b_1), \frac{1}{m_1}(\sqrt{M} - b_1)]$.

---

[5] This condition is also sufficient, see [16, Exercise 1.3].

[6] This computation was done by constructing the matrix with rows given by the coefficients of the $g(t, i)$, and then computing the Hermite normal form using `Sage`.

We will assume $M \gg \max\{m_1^2, 16b_1^2\}$ so that

$$\begin{aligned}
|S'_M(t_0)| &= \left|P\left(\frac{1}{m_1}\left(\frac{1}{2}\sqrt{M} - b_1\right)\right)\right| - \left|P\left(\frac{1}{m_1}\left(\sqrt{M} - b_1\right)\right)\right| \\
&\sim \mathcal{C}\frac{\frac{1}{m_1}(\frac{1}{2}\sqrt{M} - b_1))}{\log^3 \frac{1}{m_1}(\frac{1}{2}\sqrt{M} - b_1))} - \mathcal{C}\frac{\frac{1}{m}(\sqrt{M} - b_1))}{\log^3 \frac{1}{m_1}(\sqrt{M} - b_1))} \\
&\geq \frac{\mathcal{C}}{2m_1}\frac{\sqrt{M} - 2b_1}{\log^3 M} \\
&> \frac{\mathcal{C}}{4m_1}\frac{\sqrt{M}}{\log^3 M}.
\end{aligned}$$

Thus there is some constant $\mathcal{B}_2$ such that $|S'_M(t_0)| > \frac{\mathcal{C}}{4m_1}\frac{\sqrt{M}}{\log^3 M}$ for all $M > \mathcal{B}_2$. Note that the constant $\mathcal{B}_2$ depends on t_0. The map $c_0 \mapsto c'(c_0)$ gives us an inclusion $S'_M(t_0) \hookrightarrow S_M(t'(t_0))$. Therefore the inequality in the claim holds with $\mathcal{A}_2 = \frac{\mathcal{C}}{4m_1}$.

It remains to show that the constant $\mathcal{C}$ given in the Bateman-Horn conjecture is computable.[7] Let

$$g_1 = t_0^2 + dc^2, \quad g_2 = (t_0 - 2)^2 + dc^2, \quad g_3 = c, \quad \text{and} \quad G = g_1 \cdot g_2 \cdot g_3.$$

Define $\omega_i(p)$ to be the number of roots of $g_i \mod p$ and $\omega(p)$ to be the number of roots of $G \mod p$. Then G differs from $p' \cdot r' \cdot c'$ by a linear change of coordinates and scaling. It follows that the constant $\mathcal{C}$ differs from the product

$$\mathcal{C}_2 = \prod_{p \geq 5} \frac{1 - \omega(p)/p}{(1 - 1/p)^3}$$

in at most a finite number of factors. So it is sufficient to show $\mathcal{C}_2$ is computable. Notice that for any prime $p \geq 5$:

$$\begin{aligned}
g_1(c) \equiv g_2(c) \equiv 0 \mod p \quad &\Rightarrow \quad p \mid t_0 + 2, \\
g_1(c) \equiv g_3(c) \equiv 0 \mod p \quad &\Rightarrow \quad p \mid t_0, \\
g_2(c) \equiv g_3(c) \equiv 0 \mod p \quad &\Rightarrow \quad p \mid t_0 - 2.
\end{aligned}$$

[7] The proof of convergence for the constant in the Bateman-Horn conjecture only relies on the Chebotarev density theorem. Hence by using an effective version [51], one can show that the constant is always effectively computable. However, we present this more direct proof which offers a more concrete picture of the constant.

Let S denote the set of primes dividing $6dt_0(t_0-2)(t_0+2)$. Then for any prime $p \notin S$,

$$\omega(p) = \omega_1(p) + \omega_2(p) + \omega_3(p).$$

Let $\chi(p) = 1$ if $-d$ is a square mod p and -1 otherwise. Then one can show that for any $p \notin S$ we have that

$$\omega_1(p) = \omega_2(p) = \chi(p) + 1$$

therefore

$$\omega(p) = 2(\chi(p)+1) + 1.$$

Note that the product

$$\prod_p \frac{1-(2(\chi(p)+1)+1)/p}{(1-1/p)^3} = \mathcal{C}_3 \prod_p \left(1 - \frac{\chi(p)}{p}\right)^2$$

where $\mathcal{C}_3$ is an effectively computable constant. By Dirichlet's analytic formula,

$$\prod_p \left(1 - \frac{\chi(p)}{p}\right)^2 = \left(\frac{k\sqrt{d}}{2\pi h}\right)^2$$

where k, h are the number of roots of unity and class number of $\mathbb{Q}(\sqrt{-d})$ respectively.

□

Theorem 30. *Assume the Bateman-Horn conjecture and that $d < 100$, and suppose $d \not\equiv 7 \mod 8$. Let m_1, b_1 be the constants from Lemma 26, which depend only on d. For any fixed integer t_0, there are constants $\mathcal{A}_3, \mathcal{B}_3$ such that the probability that $c \in S_{M,K}(m_1t_0+b_1)$ given that $c \in S_M(m_1t_0+b_1)$ is bounded above by*

$$\mathcal{A}_3 \frac{K^2 \log^4 M}{\sqrt{M}}$$

for all $M > \mathcal{B}_3$. The constant $\mathcal{A}_3$ is computable.

Proof. We have to bound $\frac{S_{M,K}(m_1t_0+b_1)}{S_M(m_1t_0+b_1)}$ above. This follows immediately from the previous propositions. Proposition 25 gives an upper bound for $S_{M,K}(m_1t_0+b_1)$, and Proposition 29 gives a lower bound for $S_M(m_1t_0+b_1)$. □

Warning 31. We do not have a computable upper bound for the constant $\mathcal{B}_3$.

2.5.3 Proof of the Theorem 2

We can now prove Theorem 2 using a modified version of Algorithm 1. In order to apply Theorem 30, we need to modify Algorithm 1 so that t lies in an interval independent of the input bound M.

Algorithm 2 Isolated Curve

Input: positive integer M

Output: isolated (with gap $\sqrt{p/50 - 100}$ and set-size 8) elliptic curve defined over $\mathbb{F}_p$ with $M/2 \leq p \leq M$.

1: $-d \leftarrow$ fundamental discriminant such that $1 \leq d \leq 100$ and $d \not\equiv 7 \mod 8$
2: $m_1, b_1, m_2, b_2 \leftarrow$ constants from Lemma 26
3: $t \leftarrow$ integer such that $3 \leq t \leq 100$ and $t \equiv b_1 \mod m_1$
4: **repeat** steps 5-7
5: $c \leftarrow$ random integer in $\left[\sqrt{(2M - t^2)/d}, \sqrt{(4M - t^2)/d}\right]$ with $c \equiv b_2 \mod m_2$
6: $p \leftarrow \frac{t^2+dc^2}{4}$
7: $N \leftarrow p + 1 - t$
8: **until** p, c, and $N/\operatorname{cof}(dc^2)$ are prime
9: $j \leftarrow$ root of the Hilbert class polynomial for $\mathbb{Q}(\sqrt{-d})$ mod p
10: $E \leftarrow$ elliptic curve over $\mathbb{F}_p$ with $j(E) = j$ and $|E(\mathbb{F}_p)| = N$
11: **return** E

Proof of Theorem 2. We will show that Algorithm 2 satisfies the claims in Theorem 2.

By the Bateman-Horn conjecture and Lemma 26, for any fixed d, t as chosen in the algorithm, the number of possible values of $c \leq \sqrt{M}$ such that $p, c, N/\operatorname{cof}(dc^2)$ are simultaneously prime, is $\Omega\left(\sqrt{M}/\log^3 M\right)$. Because there is a finite number of possibilities for t, d, which are independent of M, this implies that the expected number of iterations of the main loop of Algorithm 2 is $O\left(\log^3 M\right)$.

The probability that the embedding degree of the returned curve is less than $\log^2 p$ follows from Theorem 30 using $K = \log^2 M$. Note that here we are using that t, d are bounded

independently of M, in order to average the result of Theorem 30 for all values of t in the interval $[3, 100]$.

The resulting curve E has N points, where $N = r \cdot \mathrm{cof}(dc^2)$ and r is prime. Recall that $\mathrm{cof}(dc^2) \mid 24$ by definition (see Equation 2.3). Also, E is isolated with gap c and set-size 8 because c is prime, and the bound $d \leq 100$ implies that the class number of $\mathbb{Q}(\sqrt{-d})$ is at most 8. The lower bound $c \geq \sqrt{p/50 - 100}$ follows from a straightforward computation. □

Remark 32. The bound on t in Algorithm 2 is mostly arbitrary. It is important that the upper bound on $|t|$ is independent of M. The lower bound $t \geq 3$ is for the same reason as the restriction on t in Algorithm 1.

2.6 Extending the Results

The goal of this section is to discuss the following issues with Theorem 2:

- The algorithm used in the proof (Algorithm 2) places a restriction on t, limiting the amount of randomness in the selection of an isolated curve.

- It does not give a computable bound lower bound for what "sufficiently large" is.

Recall that the main idea of both Algorithm 1 and Algorithm 2 is to search for integers t, c such that three functions ($p(t, c)$, $r(t, c)$ and c) are simultaneously prime. Algorithm 2 imposes a restriction on t that allowed us to reduce to the one variable case and apply the Bateman-Horn conjecture. We expect that the restriction on t is unnecessary, and that the following properties hold:

(i) The expected number integers t, c sampled in Algorithm 1 is $O(\log^3 M)$.

(ii) The probability that a curve returned by Algorithm 1 has an embedding degree $< \log^2 M$ is $O\left(\frac{\log^8 M}{\sqrt{M}}\right)$.

(iii) The implied constants in these estimates are computable.

In the notation of Section 2.5, all three properties reduce to giving computable bounds for S_M and $S_{M,K}$. Recall that the expected number of iterations of the main loop of Algorithm 1 is roughly $\frac{|S_M|}{M}$ and the probability of an embedding degree less than K is about $\frac{|S_{M,K}|}{|S_M|}$. For Theorem 2, we fixed t and gave bounds for $S_{M,K}(t)$ and $S_M(t)$ in Proposition 25 and Proposition 29 respectively. We would like to extend those bounds to $S_{M,K}$ and S_M.

Proposition 33. *There is a computable constant $\mathcal{A}_4$ such that for any positive integers M and K,*

$$|S_{M,K}| \leq \mathcal{A}_4 K^2 \sqrt{M} \log M.$$

Proof. By definition $|S_{M,K}| \leq \sum_{t=1}^{\sqrt{M}} |S_{M,K}(t)|$. Then by Proposition 25,

$$|S_{M,K}| \leq \sum_{t=1}^{\sqrt{M}} \mathcal{A}_1 K^2 \log t \leq \mathcal{A}_1 K^2 \sqrt{M} \log \sqrt{M},$$

where $\mathcal{A}_1$ is the constant from Proposition 25. Hence we may take $\mathcal{A}_4 = \frac{\mathcal{A}_1}{2}$. □

Problem 34. Find a computable number $\mathcal{A}_5$, depending only on the fundamental discriminant d, such that for any positive integer M,

$$|S_M| > \mathcal{A}_5 \frac{M}{\log^3 M}.$$

Remark 35. A solution to Problem 34 would be useless in practice if $\mathcal{A}_5$ is too small (e.g. 2^{-100}). Hence we implicitly require that $\mathcal{A}_5$ lies within a reasonable range, such as $\mathcal{A}_5 > 2^{-20}$.

2.6.1 An Alternative Conjecture

Even under the Bateman-Horn conjecture we are unable to solve Problem 34. This is because the Bateman-Horn conjecture only gives an asymptotic formula; it does not provide information about the error term.[8] However, there is another natural conjecture one may consider related to the Bateman-Horn conjecture.

[8] We do know that any error bound would necessarily depend on the polynomials by [28, Thm. 1].

Conjecture 36. Let $f_1, \ldots, f_k \in \mathbb{Z}[x, y]$ be such that every f_i is irreducible and $\gcd_{a,b\in\mathbb{Z}} \prod f_i(a, b) = 1$. Let $P_{f_1,\ldots,f_k}(N)$ denote the number of pairs a, b such that $0 \leq a, b \leq N$ and $f_1(a, b), \ldots, f_k(a, b)$ are simultaneously prime. Then for any $N_0 > 0$, there exists a computable constant C (depending on N_0 and the f_i) such that

$$P_{f_1,\ldots,f_k}(N) > C\frac{N^2}{\log^k N} \qquad \text{for all } N > N_0.$$

Remark 37. As stated, the constant C in Conjecture 36 depends on N_0. We could have equivalently stated the conjecture with C independent of N_0. However, in practice we usually avoid small values of N.

Recall that before the prime number theorem was proven, Chebyshev showed that $\pi(N) \geq \frac{\log 2}{2}\frac{N}{\log N}$ for all $N \geq 2$ [76, Thm. 5.3]. In a way, Conjecture 36 is to the Bateman-Horn conjecture as Chebyshev's inequality is to the prime number theorem. Conjecture 36 is weaker than the Bateman-Horn conjecture in the sense that it only asks for a lower bound, not an asymptotic formula. In fact, Conjecture 36 would follow from the Bateman-Horn conjecture if it had included a clause about the error term.

2.6.2 Heuristic Evidence

The same heuristics used to justify the Bateman-Horn conjecture suggest that $P_{f_1,\ldots,f_k}$ in Conjecture 36 has the right order of magnitude. Let $f(x, y) \in \mathbb{Z}[x, y]$ such that $\gcd_{x,y\in\mathbb{Z}} f(x, y) = 1$. If we pretend that $f(x, y)$ acts like a random number, then the probability that $f(x, y)$ is prime should be roughly $\frac{1}{\log|f(x,y)|}$. If x, y are chosen independently from a uniform distribution on $[0, N]$, then the probability that $f(x, y)$ is prime should be roughly $\frac{1}{d\log N}$ where d is the degree of f (i.e. the highest total degree of any monomial in f). Given multiple polynomials $f_1, \ldots, f_k$ satisfying the hypothesis in Conjecture 36, we expect that the probability that they are simultaneously prime is the product of the probabilities for each f_i, up to some constant correction factor. This suggests that $P_{f_1,\ldots,f_k} = \Theta\left(\frac{N^2}{\log^k N}\right)$, but gives no insight into the constants.

2.6.3 Theoretical Evidence

Conjecture 36 also differs from the Bateman-Horn conjecture in that it applies to polynomials in two variables. There are many cases where the conjecture can be proven. For example, we can apply the prime number theorem for quadratic fields to estimate how often certain quadratic forms are prime [30, Thm. 21.1]. The Friedlander-Iwaniec theorem [29] gives an asymptotic density of primes of the form $x^2 + y^4$. More recently considered were pairs x, y such that $x^2 - xy + y^2$ and $2x - y$ are both prime [67]. One the examples closest to Problem 34 is the following result of Fouvry and Iwaniec.

Theorem 38 (Fouvry and Iwaniec [30, Thm. 20.3], [25])**.** *Let Λ be the von Mangoldt function defined by*

$$\Lambda(n) = \begin{cases} \log p & \text{if } n = p^k \text{ for some prime } p \\ 0 & \text{otherwise.} \end{cases}$$

Then

$$\sum_{x^2+y^2 \leq N} \Lambda(x)\Lambda(x^2+y^2) = \frac{\pi H}{4} N + O\left(\frac{N}{\log^{1/4} N}\right)$$

where the sum is over positive integer, $H = \prod_p \left(1 - \frac{\chi(p)}{p-1}\right)$, and

$$\chi(p) = \begin{cases} 1 & p \equiv 1 \mod 4 \\ -1 & p \equiv 3 \mod 3 \\ 0 & p = 2. \end{cases}$$

Corollary 39. *Let $P_{x,x^2+y^2}(N)$ denote the number of pairs $x, y \in [0, N]$ such that x and $x^2 + y^2$ are simultaneously prime. Then*

$$P_{x,x^2+y^2}(N) = \Omega\left(\frac{N^2}{\log^2 N}\right).$$

Proof. First notice that

$$\begin{aligned} P_{x,x^2+y^2}(N) &= \sum_{\substack{x,x^2+y^2\text{prime} \\ 0<x,y<N}} 1 \\ &\geq \sum_{\substack{x,x^2+y^2\text{prime} \\ 0<x^2+y^2<N^2}} 1 \\ &\geq \frac{1}{2\log^2 N} \sum_{\substack{x,x^2+y^2\text{prime} \\ 0<x^2+y^2<N^2}} \Lambda(x)\Lambda(x^2+y^2). \end{aligned}$$

The only difference between the last sum and the sum in Theorem 38, is that the latter includes prime powers. The number of prime powers less than N^2 is bounded above by $\log(N)\pi(N) < 2N$. For each prime power p^k less than N, there are at most $4(k+1)$ pairs x, y such that $x^2+y^2 = p^k$. This is because there are at most $k+1$ ideals in $\mathbb{Z}[i]$ with norm p^k, and each has at most 4 distinct generators. Therefore

$$P_{x,x^2+y^2}(N) \geq \frac{1}{2\log^2 N} \sum_{x^2+y^2\leq N^2} \Lambda(x)\Lambda(x^2+y^2) - \frac{4N}{\log N}.$$

The claim now follows from Theorem 38. □

If we restrict to even values of t, then for $d = 4$ we have that $p(t,c) = \left(\frac{t}{2}\right)^2 + c^2$. Hence the corollary above implies that for $d = 4$ we have

$$\#\left\{t, c\colon p = \frac{t^2+dc^2}{4} \text{ and } c \text{ are prime and } p \leq M\right\} = \Omega\left(\frac{M}{\log^2 M}\right).$$

This agrees with our heuristics because we have two polynomials and the probability both are prime is roughly $\frac{1}{\log^2 M}$ when choosing t, c randomly in $[0, \sqrt{M}]$. We expect the same principal term for other values of d. Furthermore, adding the requirement that $r(t,c)$ is prime should change the principle term by a factor of $\frac{1}{\log M}$. It is unclear if the methods used in the proof of Theorem 38 could extend to cover pairs t, c such that all three functions p, r, and c are all simultaneously prime.

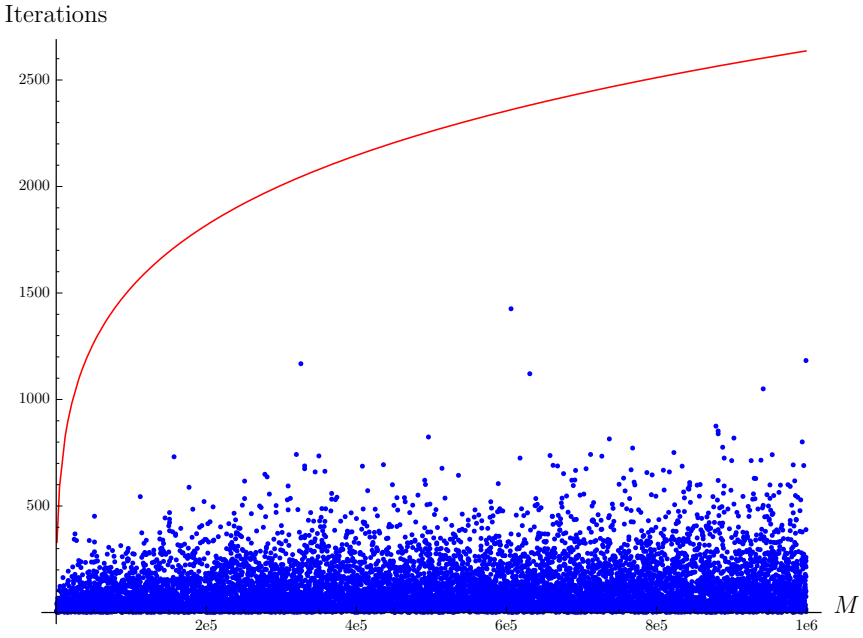

Figure 2.1: Comparing the observed number of samples of t, c used in Algorithm 1 with $\log^3 M$ for various values of M.

2.6.4 Numerical Evidence

We implemented Algorithm 1 with $d = 4$ using a few modifications for efficiency, such as only choosing odd values of c and even values of t. For a few values of M, we counted the number of iterations the main loop ran until the algorithm returned. Equivalently, this is the number of pairs t, c chosen at random until p, r, and c were simultaneously prime. The number of iterations was always below $\log^3 M$ as shown in Figure 2.1.

We also computed the embedding degree of a curve returned by Algorithm 1 with $M = 2^{98}$. In 10000 runs we observed 0 curves with embedding degree $< \log^2(M)$. This should be compared with the bound $\frac{\log^8(M)}{\sqrt{M}} \approx 0.80527$.

2.7 Conclusion

We acknowledge that a solution to Problem 34 may not be as mathematically interesting as proving an asymptotic formula with an optimal error bound for a generalized, two variable Bateman-Horn conjecture. However, a solution to Problem 34 would be enough to:

(i) Prove the efficiency of an algorithm to generate an isolated curve with large embedding degree.

(ii) Prove that the space of isolated curves is large enough to provide sufficient randomness in parameter selection.

These facts are enough to show that isolated curves provide cryptosystems resistant to the isogeny based attacks described in the introduction.

Chapter 3

SUPER-ISOLATED ELLIPTIC CURVES AND ABELIAN SURFACES IN CRYPTOGRAPHY

3.1 Introduction

The security of elliptic curve cryptography depends on the difficulty of the elliptic curve discrete log problem (ECDLP). Given an elliptic curve E over $\mathbb{F}_p$, a cyclic subgroup of $E(\mathbb{F}_p)$ generated by the point P, and a point $Q \in \langle P \rangle$, the ECDLP asks to find an integer k such that $Q = kP$. The fastest known generic algorithm to solve the ECDLP on an elliptic curve is Pollard's rho algorithm, which has an expected runtime of $\tilde{O}(\sqrt{p})$ [61, Ch. 3.6.3].

It is possible to transfer the ECDLP between curves via isogenies. If $\varphi : E \to E'$ is an isogeny[1] that restricts to an isomorphism $\langle P \rangle \to \langle \varphi(P) \rangle$, then $Q = kP$ if and only if $\varphi(Q) = k\varphi(P)$. This reduction is useful for solving the ECDLP if the time it takes to compute $\varphi(Q)$ and $\varphi(P)$, as well as to solve the ECDLP on E', is less than the time it takes to solve the ECDLP on E.

Suppose that there is an attack on the ECDLP that targets a small but non-negligible proportion of curves over $\mathbb{F}_p$. Given any curve $E/\mathbb{F}_p$, we could attempt to transfer the ECDLP on E to a weak curve. If E admits few efficiently computable isogenies, then this transfer is likely infeasible. Note that, including twists, there are $\approx 2p$ isomorphism classes of elliptic curves over $\mathbb{F}_p$, and there are $\approx 4\sqrt{p}$ isogeny classes. So the average size of an isogeny class is $\approx \sqrt{p}/2$. Thus, we expect that a random curve will admit many isogenies.

While there is no known attack that targets a non-negligible proportion of curves over $\mathbb{F}_p$, the concern over the possibility of one is partially motivated by the Gaudry-Hess-Smart

[1] Unless otherwise noted, by isogeny we mean $\mathbb{F}_p$-rational isogeny.

(GHS) attack [35]. Over certain extension fields[2], Menezes and Teske in [58, Sec. 7] used the generalized GHS attack to show that there is a non-negligible proportion of "weak" curves, for which the ECDLP can be solved in significantly less time than it takes Pollard's rho. Under some reasonable assumptions, given a random elliptic curve E over such a field, one can find a chain of efficiently computable isogenies from E to a weak curve. Even though the GHS attack does not apply to prime fields, it is conceivable that a similar attack could be found that does.

In [45, Sec. 11, Ex. 5], Koblitz, Koblitz, and Menezes observed that it is possible to use the complex multiplication (CM) method to construct elliptic curves $E/\mathbb{F}_p$ whose isogeny class is large ($\approx \sqrt{p}$), but contains no curves (besides E itself) whose *conductor gap* with E is small. The conductor gap between two curves measures the computational complexity in computing an isogeny between them. The curve E is called *isolated* because there are no other curves E' for which constructing an isogeny between E and E' is computationally feasible.

So far we have only mentioned elliptic curves, but the same ideas carry over to abelian surfaces. In [87], Wang gave a construction for isolated abelian surfaces that is analogous to the one for curves given in [45]. Note that while these methods construct isolated varieties, they almost always have large isogeny classes.

In this paper, we focus on the special case of *super-isolated* abelian varieties. We call an abelian variety over a finite field super-isolated if its isogeny class contains a single isomorphism class. For increased security and efficiency, we focus on varieties of prime or near-prime order defined over a prime field.

Our main contributions are as follows. First, we outline practical algorithms that search for super-isolated elliptic curves and abelian surfaces. Second, we prove that only two super-isolated surfaces of cryptographic size and near-prime order exist, see Examples 73 and 74. Finally, we give some heuristics on the number of super-isolated varieties. Our results

[2]The attack described in [58] only applies to fields of the form $\mathbb{F}_{2^{3\ell}}$ with $53 \leq \ell \leq 200$.

suggest that, unlike the case of surfaces, there are enough super-isolated elliptic curves of cryptographic size and prime order to use in cryptosystems that require ephemeral curves, such as [62].

The outline of the paper is as follows. Section 3.2 focuses on elliptic curves. Some background and notation is given in Section 3.2.1. In Section 3.2.2, we outline an algorithm to construct super-isolated elliptic curves of prime order over $\mathbb{F}_p$ with p of a given size. We heuristically estimate the number of such curves in Section 3.2.3. Section 3.3 focuses on surfaces. In Section 3.3.1, we show that finding super-isolated surfaces reduces to finding *super-isolated Weil numbers*, which are defined in that section. In Section 3.3.2, we outline an algorithm to search for super-isolated Weil numbers. We also prove the correctness and efficiency of the algorithm in the same section. Two examples of super-isolated surfaces of near-prime order and cryptographic size are given in Section 3.3.3. In Section 3.3.4, we prove these are the only such examples.

3.2 Elliptic Curves

3.2.1 Background and Notation

Let p be a prime. For any $t \in \mathbb{Z}$, let $I(t)$ denote the set of isomorphism classes of elliptic curves $E/\mathbb{F}_p$ such that $\#E(\mathbb{F}_p) = p - t + 1$. A theorem of Tate says that the sets $I(t)$ are isogeny classes of elliptic curves over $\mathbb{F}_p$, see [78, Ch. 5]. The Hasse bound implies that $I(t)$ is empty when $t^2 > 4p$. An elliptic curve is *ordinary* if $t \not\equiv 0 \mod p$.

Remark 40. In this paper, we will focus on varieties defined over prime fields because most cryptosystems used in practice are built over prime fields. However, many of our results can be extended to arbitrary finite fields. We describe how our results generalize in Section 3.4.

Definition 41. An elliptic curve $E/\mathbb{F}_p$ is *super-isolated* if there is only one isomorphism class in its isogeny class, i.e. $\#I(p + 1 - \#E(\mathbb{F}_p)) = 1$.

Definition 42. Let $\mathcal{O}$ be an order in a quadratic imaginary field, and let Δ be the discriminant of $\mathcal{O}$. The *Kronecker class number* $H(\Delta)$ *of* Δ is defined to be

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

where $h(\mathcal{O}')$ denotes the class number of the order $\mathcal{O}'$, and the sum is over all orders $\mathcal{O}'$ of $\mathcal{O} \otimes \mathbb{Q}$ such that $\mathcal{O}' \supseteq \mathcal{O}$.

Theorem 43 ([73, Thm. 4.6])**.** *If* $t^2 < 4p$ *and* $t \not\equiv 0 \mod p$*, then*

$$\#I(t) = H(t^2 - 4p).$$

Remark 44. If $t = p + 1 - \#E(\mathbb{F}_p) \equiv 0 \mod p$, then E is called *supersingular*. The reason that we focus on ordinary curves is because the ECDLP on supersingular curves is vulnerable to the Menezes-Okamoto-Vanstone attack [60]. There do exist super-isolated supersingular curves. For example, $y^2+y = x^3+x$ is the only curve over $\mathbb{F}_2$ with 5 points. See [73, Thm. 4.6, Pg. 194] for a detailed formula for $\#I(t)$ when $t \equiv 0 \mod p$. If $p \geq 5$ then any supersingular curve over $\mathbb{F}_p$ will have an even number of points. Hence we may ignore the supersingular case because we are interested in curves with prime order.

3.2.2 Super-Isolated Elliptic Curves of Prime Order

In this section, we outline a simple method to search for super-isolated elliptic curves which have prime order. The reason for considering curves of prime order is that it increases the security and efficiency of the elliptic curve cryptosystem.

First we will use the results in Section 3.2.1 to give a simple characterization of super-isolated elliptic curves over prime fields.

Corollary 45. *Let* $E/\mathbb{F}_p$ *be an ordinary elliptic curve with trace* $t = p+1-\#E(\mathbb{F}_p)$*. Then* E *is super-isolated if and only if*

$$t^2 - 4p \in \{-3, -4, -7, -8, -11, -19, -43, -67, -163\}.$$

Proof. By Theorem 43, $\#I(t) = 1$ if and only if $t^2 - 4p$ is the discriminant of the maximal order of a quadratic imaginary field with class number 1. It is a well known theorem of Heegner and Stark that the numbers in the statement are precisely the discriminants of such fields [81]. □

Remark 46. Another way to view the condition in Corollary 45 is as follows. Let $K = \mathbb{Q}(\sqrt{-d})$ be an imaginary quadratic field with class number 1 and discriminant $-d$. Then we are searching for algebraic integers $\pi \in \mathcal{O}_K$ of the form $\pi = (t + \sqrt{-d})/2$ such that $\pi\overline{\pi} = (t^2 + d)/4 = p$ is prime and $\mathbb{Z}[\pi] = \mathcal{O}_K$.

Remark 47. Super-isolated elliptic curves are rare in the sense that if we choose a prime p at random, it is unlikely there exists such a curve over $\mathbb{F}_p$. Let $\pi_{SI}(x)$ denote the number of primes $p < x$ such that there exists a super-isolated elliptic curve over $\mathbb{F}_p$. Any such p must be of the form $t^2 + d/4$, where $-d$ is one of the numbers from Corollary 45 and t is an integer. This shows that $\pi_{SI}(x) = O(\sqrt{x})$.

Remark 48. Even when super-isolated curves exist over $\mathbb{F}_p$, such curves are rare in the set of all curves over $\mathbb{F}_p$. There are roughly $2p$ $\mathbb{F}_p$-isomorphism classes of elliptic curves over $\mathbb{F}_p$, but at most 18 are super-isolated. The number 18 is a rough upper bound that comes from the 9 values in Corollary 45, and then multiplying by 2 to account for quadratic twists. Note that a non-quadratic twist of a super-isolated curve is not super-isolated. To see this, suppose that t' is the trace of a non-quadratic twist E' of a super-isolated curve E with trace t. Let π denote a root of $x^2 - tx + p$ and π' a root of $x^2 - t'x + p$. By Remark 46, $\mathbb{Z}[\pi] = \mathcal{O}_K$ where $K = \mathbb{Q}(\pi)$. Because E' is a twist of E, $\mathbb{Z}[\pi'] \subseteq \mathcal{O}_K = \mathbb{Z}[\pi]$, so $\operatorname{Disc}\pi' = (t')^2 - 4p$ is a square-multiple of $\operatorname{Disc}\pi = t^2 - 4p$. Because E' is not a quadratic twist, $\operatorname{Disc}\pi' \neq \operatorname{Disc}\pi$ hence $\mathbb{Z}[\pi'] \subsetneq \mathbb{Z}[\pi]$, so E' is not super-isolated.

Suppose that p, t, and $d = t^2 - 4p$ satisfy the condition in Corollary 45. The fact that $p = (t^2 + d)/4 \in \mathbb{Z}$ implies that $t \equiv d \mod 2$. So we may replace t with $2x$ or $2x + 1$ depending on $d \mod 2$. Then p and $N = p + 1 - t$ can be written as the following integral

polynomials:

$$p(x) = \begin{cases} x^2 + \frac{d}{4} & \text{if } -d \equiv 0 \mod 4 \\ x^2 + x + \frac{d+1}{4} & \text{if } -d \equiv 1 \mod 4 \end{cases}, \quad N(x) = \begin{cases} (x-1)^2 + \frac{d}{4} & \text{if } -d \equiv 0 \mod 4 \\ x^2 - x + \frac{d+1}{4} & \text{if } -d \equiv 1 \mod 4. \end{cases} \tag{3.1}$$

We are interested in values of x such that $p(x)$ and $N(x)$ are simultaneously prime. Two necessary conditions for $p(x)$ and $N(x)$ to be simultaneously prime infinitely often are:

(i) $p(x)$ and $N(x)$ are irreducible over $\mathbb{Z}[x]$.

(ii) $\gcd_{a \in \mathbb{Z}} p(a)N(a) = 1$.

It is clear that condition (i) is satisfied for all values of d. From Table 3.1 below, condition (ii) holds for $d \in \{3, 19, 43, 67, 163\}$ (this can be checked using only a few consecutive values of a [16, Ex. 3.i, Pg. 19]). For other values of d, Table 3.1 shows that one of $p(x)$ or $N(x)$ is always divisible by 2 or 3.

We now give a simple description of our search method.

1. Choose $d \in \{3, 19, 43, 67, 163\}$ and let $p(x), N(x)$ be as in Table 3.2.

2. Choose random integers a in a predetermined range until $p = p(a)$ and $N = N(a)$ are both prime.

3. Use the CM method to recover a curve $E/\mathbb{F}_p$ with N points, see [19, Ch. 18.1].

Example 49. Let $d = 3$ and $a = 321438704914423479101766132343967029098$. Then $p = p(a)$ and $N = N(a)$ are both 256-bit primes. The curve $E/\mathbb{F}_p$ given by $y^2 = x^3 + 244944$ satisfies $\#E(\mathbb{F}_p) = N$. This value of a was found by a `Sage` [86] program that randomly sampled integers from the interval $[0, 2^{128}]$.

Example 50. Let $d = 3$ and $a = 2^{127} + 13906$. Then $p = p(a)$ and $N = N(a)$ are 255-bit primes. Moreover, their binary representations have a Hamming weight of 24 and 27 respectively. The CM method gives the curve $y^2 = x^3 + 279936$. Even though our search method does not have full control over the prime p, it is still possible to find primes with certain desirable properties, such as a low Hamming weight.

$-d$	$p(x)$	$N(x)$	$\gcd_{a\in\mathbb{Z}} p(a)N(a)$
3	$x^2 + x + 1$	$x^2 - x + 1$	1
4	$x^2 + 1$	$x^2 - 2x + 2$	2
8	$x^2 + 2$	$x^2 - 2x + 3$	6
7	$x^2 + x + 2$	$x^2 - x + 2$	4
11	$x^2 + x + 3$	$x^2 - x + 3$	3
19	$x^2 + x + 5$	$x^2 - x + 5$	1
43	$x^2 + x + 11$	$x^2 - x + 11$	1
67	$x^2 + x + 17$	$x^2 - x + 17$	1
163	$x^2 + x + 41$	$x^2 - x + 41$	1

Table 3.1: $\gcd_{a\in\mathbb{Z}} p(a)N(a)$ for values of d.

3.2.3 Estimating the Number of Super-Isolated Curves of Prime Order

In various applications, it is important to have some degree of randomness in the parameter selection. For example, a cryptosystem may require a distinct curve for each user, or use ephemeral keys such as in [62]. In this section, we estimate the number of super-isolated elliptic curves of prime order (note that if $p \geq 5$, then the prime order condition implies that the curve is ordinary), as a way to measure the randomness in the selection of such a curve. We also give some numerical evidence supporting our estimates.

The Bateman-Horn conjecture [6] implies that if $p(x)$ and $N(x)$ are irreducible and satisfy $\gcd_{a\in\mathbb{Z}} p(a)N(a) = 1$, then the number of x, with $0 \leq x \leq M$, such that $p(x)$ and $N(x)$ are simultaneously prime is asymptotic to $C\int_2^M 1/\log^2(t)dt$ for a computable positive constant C. It is clear that $p(x)$ and $N(x)$ are irreducible, and we saw in Table 3.1 the values of d such that the second property holds. For each such d, Table 3.2 gives an approximation of the constant C.

$-d$	C
-3	≈ 0.74
-19	≈ 0.76
-43	≈ 2.67
-67	≈ 4.39
-163	≈ 11.21

Table 3.2: An approximation to the Bateman-Horn constant C.

Example 51. We ran 10000 iterations of the search in Example 49. The average number of x's sampled until $p(x)$ and $N(x)$ were both prime, was 10312. The heuristics above imply that the expected number of x's that need to be sampled is

$$\left(\frac{0.74}{2^{128}}\int_2^{2^{128}} \frac{1}{\log^2 t}\, dt\right)^{-1} \approx 10395.$$

The percent difference between the observed and expected is -0.008.

Combining the heuristics above, we expect that the number of x with $0 \leq x \leq M$ such that $p(x)$ and $N(x)$ are prime for some $d \in \{3, 19, 43, 67, 163\}$ is approximately

$$19.8 \cdot \int_2^M \frac{1}{\log^2 t}\, dt.$$

Since $p(x)$ has degree 2, we can estimate the number of curves over $\mathbb{F}_p$ with $p \leq M$ by choosing x in the range $0 \leq x \leq \sqrt{M}$. Combined with above, we have the following estimate for the number of curves.

Heuristic 52. The number of super-isolated elliptic curves of prime order over $\mathbb{F}_p$ with $p \leq M$ is approximately

$$19.8 \int_2^{\sqrt{M}} \frac{1}{\log^2 t}\, dt.$$

3.3 Abelian Surfaces

3.3.1 Super-Isolated Weil Numbers

We define *super-isolated* for an abelian variety as we did for an elliptic curve: an abelian variety whose isogeny class contains only one isomorphism class. Recall that finding a super-isolated elliptic curve over $\mathbb{F}_p$ is equivalent to finding an algebraic integer π in an imaginary quadratic field K of class number 1 such that $\pi\overline{\pi} = p$ and $\mathbb{Z}[\pi] = \mathcal{O}_K$ (see Remark 46). The general situation is similar, only we replace K with a CM field (defined below), and $\mathbb{Z}[\pi]$ with $\mathbb{Z}[\pi, \overline{\pi}]$.

Definition 53. A number field K is a *complex multiplication field*, or *CM field*, if K is a totally imaginary quadratic extension of a totally real field F. CM fields have a unique non-trivial automorphism fixing F, which we denote by $\alpha \mapsto \overline{\alpha}$ and refer to as complex conjugation.

Definition 54. For any $n \in \mathbb{Z}$, a *Weil n-number* is an algebraic integer that has absolute value $\sqrt{n}$ under every embedding to $\mathbb{C}$. A *Weil number* is a Weil n-number for some n. If K is a CM field, then $\alpha \in \mathcal{O}_K$ is a Weil number if and only if $\alpha\overline{\alpha} \in \mathbb{Z}$. It can be shown that if π is a Weil p-number for a prime p, then either $\mathbb{Q}(\pi)$ is a CM field or $\pi = \pm\sqrt{p}$. The *conjugacy class* of a Weil number π is the set of roots in $\overline{\mathbb{Q}}$ of the minimal polynomial of π over $\mathbb{Q}$.

Let $A/\mathbb{F}_p$ be a simple[3] abelian variety, and let f be the characteristic polynomial of the Frobenius endomorphism of A. It is well known that $\#A(\mathbb{F}_p) = f(1)$ and $f = h^e$ where

[3]In this paper we use simple to mean simple over the base field. Other sources sometimes use the term to mean simple over the algebraic closure.

h is irreducible and e is some integer. Moreover, any root π of f is a Weil p-number and $2 \dim A = e[\mathbb{Q}(\pi) : \mathbb{Q}]$ [90, Thm 8]. For cryptographic reasons, we are interested in varieties with prime or near-prime order, so we will mainly focus on the case where $e = 1$.

Theorem 55. *Let A be a simple abelian variety over $\mathbb{F}_p$, π be a root of the characteristic polynomial of the Frobenius endomorphism, and $K = \mathbb{Q}(\pi)$. Assume that $\pi \neq \pm\sqrt{p}$. Then A is super-isolated if and only if $\mathbb{Z}[\pi, \overline{\pi}] = \mathcal{O}_K$ and K has class number 1.*

Proof. By [89, Thm. 3.5], the endomorphism ring of any variety isogenous to A is an order[4] in $\mathcal{O}_K$ containing $\mathbb{Z}[\pi, \overline{\pi}]$. Because the base field is $\mathbb{F}_p$ and $\pi \neq \pm\sqrt{p}$, the converse holds as well [89, Thm. 6.1]. That is, every order of $\mathcal{O}_K$ containing $\mathbb{Z}[\pi, \overline{\pi}]$ is the endomorphism ring of some variety isogenous to A. We call the set of varieties isogenous to A with endomorphism ring R the *endomorphism class* of R. So there is exactly one endomorphism class if and only if $\mathbb{Z}[\pi, \overline{\pi}] = \mathcal{O}_K$. The proof of [89, Thm. 6.1] shows that the number of isomorphism classes in the endomorphism class of $\mathcal{O}_K$ is equal to the class number of K. Therefore, the entire isogeny class of A contains a single isomorphism class if and only if $\mathbb{Z}[\pi, \overline{\pi}] = \mathcal{O}_K$ and K has class number 1. □

Definition 56. Let K be a CM field with class number 1. A *super-isolated Weil p-number for K* is a Weil number π for a prime p such that $\mathcal{O}_K = \mathbb{Z}[\pi, \overline{\pi}]$.

In this section we are mainly interested in surfaces. The reason for not considering higher dimensional abelian varieties is that the discrete log problem on jacobians[5] of curves of genus ≥ 3 can be solved faster than on comparably sized jacobians of curves of genus ≤ 2 [23, 34, 80]. This means that we would need to use a larger key size in order to achieve comparable security. Hence varieties of dimension ≥ 3 are less efficient in practice. Both genus 2 and 1 are still considered for cryptographic use and have comparable efficiency [7].

The following corollary specializes Theorem 55 to surfaces with $e = 1$.

---

[4] The statement of [89, Thm. 3.5] refers to an order in $\mathrm{End}_{\mathbb{F}_p} A \otimes \mathbb{Q}$, but this is the same as K since the base field is prime, see [89, Ch. 2].

[5] Cryptosystems usually use jacobians of hyperelliptic curves rather than arbitrary varieties because they provide efficient representations necessary for practical use [47].

Corollary 57. *Let A be an abelian surface over $\mathbb{F}_p$. Assume that the characteristic polynomial f of the Frobenius endomorphism of A is irreducible. Then A is super-isolated if and only if the roots π of f are super-isolated Weil p-numbers for a quartic CM field with class number 1.*

Proof. This follows from Theorem 55 after noting that, because f is irreducible, A is simple and $\pm\sqrt{p}$ can not be roots of f. □

Therefore, in order to find super-isolated surfaces of near-prime order (note that the near-prime order condition implies the hypothesis in Corollary 57), it is sufficient to find all super-isolated Weil numbers for all quartic CM fields with class number 1. There are 91 such fields and they can be found in the literature [54, 91]. By [56, Cor. 2.10], if π is a Weil p-number whose minimal polynomial f has degree 4, then there is a simple abelian surface over $\mathbb{F}_p$ such that f is the characteristic polynomial of the Frobenius endomorphism of A (this result uses the fact that $\mathbb{F}_p$ is a prime field). This is a special case of a theorem of Honda, which shows that every Weil p-number is a root of the characteristic polynomial of the Frobenius endomorphism of some simple abelian variety over $\mathbb{F}_p$ [40]. One can recover a representative of the isogeny class of A from π using the two dimensional analogue of the CM method [19, Ch. 18].

3.3.2 Search Algorithm

In this section we describe an efficient algorithm for enumerating all super-isolated Weil numbers for a given quartic CM field up to a certain bound. For the rest of the paper, unless otherwise stated, we will only consider super-isolated Weil numbers for quartic CM fields K.

Remark 58. Our methods are motivated by those Wang used in [87] to parameterize *isolated abelian surfaces*, which are analogues of the isolated elliptic curves described in Section 3.1.

Remark 59. A naive algorithm to find super-isolated Weil p-numbers is as follows. Fix a quartic CM field K with class number 1. For each prime p less than a certain bound, find all possible solutions π in $\mathcal{O}_K$ to the relative norm equation $\pi\overline{\pi} = p$. This can be done

using standard algorithms, see [18, Ch. 7.5.4]. For each solution, check if $\mathbb{Z}[\pi, \overline{\pi}] = \mathcal{O}_K$ by computing discriminants. This method is not practical because primes p which admit super-isolated Weil p-numbers are rare.

First, we will give an informal description of our algorithm. Let K be a quartic CM field with class number 1, and let $\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$ be a basis for $\mathcal{O}_K$. Then any $\pi \in \mathcal{O}_K$ can be written as $\sum a_i \alpha_i$ for some $a_i \in \mathbb{Z}$. We will show that π is a super-isolated Weil number if and only if the a_i satisfy the following properties:

(i) The condition that $\pi\overline{\pi} \in \mathbb{Z}$ is equivalent to $P_0(a_1, a_2, a_3, a_4) = 0$, where P_0 is the polynomial in Equation 3.5 below.

(ii) If (i) holds, then the condition that $\mathbb{Z}[\pi, \overline{\pi}] = \mathcal{O}_K$ is equivalent to the equations

$$f_1(a_1, a_2, a_3, a_4) = \pm 1 \quad \text{and} \quad f_2(a_1, a_2, a_3, a_4) = \pm 1$$

where f_1 and f_2 are the polynomials in Equations (3.2,3.3).

(iii) The condition that $\pi\overline{\pi}$ is prime is equivalent to $P(a_1, a_2, a_3, a_4)$ being prime, where P is the polynomial in Equation 3.4 below.

These equivalences are shown in the proof of Theorem 68 below. Moreover, we will also show that if $\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$ are chosen in a certain way, then finding solutions to the equations $P_0 = 0$, $f_1 = \pm 1$, $f_2 = \pm 1$ essentially reduces to an instance of Pell's equation. Our algorithm starts by choosing such a basis, and proceeds to enumerate tuples (a_1, a_2, a_3, a_4) satisfying the conditions above.

The Algorithm

The algorithm outlined below enumerates super-isolated Weil numbers for a certain field.

1. Choose a quartic CM field K of class number 1, and let F be the real quadratic subfield. Let Δ_K, Δ_F denote the respective discriminants.

2. Choose a basis $\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$ of $\mathcal{O}_K$ such that $\alpha_1 = 1$ and $\{\alpha_1, \alpha_2\}$ form a basis for $\mathcal{O}_F$.

3. Choose non-conjugate embeddings $\phi_1, \phi_2 : K \hookrightarrow \mathbb{C}$.

4. Compute the coefficients of the following polynomials:

$$f_1 = \frac{1}{\sqrt{\Delta_F}} \sum_{i=1}^{4} (\phi_1(\alpha_i + \overline{\alpha}_i) - \phi_2(\alpha_i + \overline{\alpha}_i)) x_i, \tag{3.2}$$

$$f_2 = \frac{\Delta_F}{\sqrt{\Delta_K}} \sum_{1 \le i,j \le 4} \phi_1(\alpha_i - \overline{\alpha}_i)\phi_2(\alpha_j - \overline{\alpha}_j) x_i x_j, \tag{3.3}$$

$$P = \frac{1}{2} \sum_{1 \le i,j \le 4} (\phi_1(\alpha_i \overline{\alpha}_j) + \phi_2(\alpha_i \overline{\alpha}_j))\, x_i x_j, \tag{3.4}$$

$$P_0 = \frac{1}{2\sqrt{\Delta_F}} \sum_{1 \le i,j \le 4} (\phi_1(\alpha_i \overline{\alpha}_j) - \phi_2(\alpha_i \overline{\alpha}_j))\, x_i x_j. \tag{3.5}$$

   By Lemma 63 below, $f_1 \in \mathbb{Z}[x_2, x_3, x_4]$, $f_2 \in \mathbb{Z}[x_3, x_4]$, and $P, P_0 \in \frac{1}{2}\mathbb{Z}[x_1, x_2, x_3, x_4]$.

5. Enumerate solutions $x_3 = a_3$, $x_4 = a_4$ to the equation

$$f_2(x_3, x_4) = \pm 1 \tag{3.6}$$

   up to a given bound. We do this as follows.

   5.1 By Lemma 64 below, we may write $f_2 = ax_3^2 + bx_3x_4 + cx_4^2$ for $a, b, c \in \mathbb{Z}$ with $b^2 - 4ac = \Delta_F$. A straight-forward calculation shows that the $\mathbb{Z}$-module $I = a\mathbb{Z} + \frac{b+\sqrt{\Delta_F}}{2}\mathbb{Z}$ is an ideal of $\mathcal{O}_F$. Here we are abusing notation by writing $\sqrt{\Delta_F}$ as an element of F. Since K is a quartic CM field with class number 1, F has class number 1. So we can choose a principal generator γ for I. Let ϵ be a fundamental unit for F. One can find both γ and ϵ using standard algorithms, see [17, Ch. 4-5].

   5.2 For each $i \in \mathbb{Z}$, with $|i|$ less than a predetermined bound, compute $\sigma = \pm\epsilon^i\gamma$ for each choice of sign.

   5.3 For each σ, find a pair $a_3, a_4 \in \mathbb{Q}$ such that $a_3 a + a_4 \frac{b+\sqrt{\Delta_F}}{2} = \sigma$.

6. For each pair (a_3, a_4), find all a_2 such that $x_2 = a_2$, $x_3 = a_3$, $x_4 = a_4$ is a solution to

$$f_1(x_2, x_3, x_4) = \pm 1. \tag{3.7}$$

   We can find a_2 as follows. By the choice of basis, the coefficient of x_2 in f_1 is non-zero. Thus, there are two possibilities for $a_2 \in \mathbb{Q}$, and they are each given by linear polynomials in a_3, a_4.

7. For each tuple (a_2, a_3, a_4), find all a_1 such that $x_1 = a_1$, $x_2 = a_2$, $x_3 = a_3$, $x_4 = a_4$ is a solution to

$$P_0(x_1, x_2, x_3, x_4) = 0. \tag{3.8}$$

   This can be done as follows. A straightforward computation, using the fact that $\alpha_1 = 1$, shows that $2P_0 = g + f_1 x_1$ for some polynomial $g \in \mathbb{Z}[x_2, x_3, x_4]$. Since $f_1(a_2, a_3, a_4) = \pm 1$, we have $a_1 = \mp g(a_2, a_3, a_4)$.

8. For each tuple (a_1, a_2, a_3, a_4), if every a_i is integral and $P(a_1, a_2, a_3, a_4)$ is prime, then output

$$\pi = a_1\alpha_1 + a_2\alpha_2 + a_3\alpha_3 + a_4\alpha_4.$$

Correctness

In this section, we will prove the correctness of the algorithm of Section 3.3.2. By correctness, we mean that if the algorithm is given a quartic CM field K with class number 1 and outputs π, then π is a super-isolated Weil number for K. Conversely, if π is a super-isolated Weil number for K, then, given a large enough bound, the algorithm will eventually output π.

Remark 60. This section is solely focused on the correctness of the algorithm. For a discussion of the efficiency, see Section 3.3.2.

Our proof of correctness involves several computations, which have been broken down into several lemmas. The main idea is to find explicit polynomials representing the index of $\mathbb{Z}[\pi, \pi]$ in $\mathcal{O}_K$ and the value of $\pi\overline{\pi}$, both with respect to the basis $\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$.

First, we will prove Lemmas 63 and 64, which were used in the description of the polynomials f_1, f_2, P, P_0 in the algorithm in Section 3.3.2. To prove these lemmas, we start with some facts from algebraic number theory.

Lemma 61. *Let K be a quartic CM field, F be the quadratic real subfield of K, and ϕ_1, ϕ_2 be non-conjugate embeddings $K \hookrightarrow \mathbb{C}$. If $\gamma \in \mathcal{O}_K$, then*

$$\phi_1(\gamma + \overline{\gamma}) + \phi_2(\gamma + \overline{\gamma}) \in \mathbb{Z}$$

and

$$\phi_1(\gamma + \overline{\gamma}) - \phi_2(\gamma + \overline{\gamma}) \in \sqrt{\Delta_F}\mathbb{Z}.$$

Proof. The first claim follows from the fact that $\phi_1(\gamma + \overline{\gamma}) + \phi_2(\gamma + \overline{\gamma}) = \mathrm{Trace}_{K/\mathbb{Q}}\,\gamma$. The second claim follows from the fact that $\phi_1(\gamma + \overline{\gamma}) - \phi_2(\gamma + \overline{\gamma}) = \delta_{F/\mathbb{Q}}(\mathrm{Trace}_{K/F}(\gamma))$, where $\delta_{F/\mathbb{Q}}$ is the relative different. More concretely, if we write $\mathrm{Trace}_{K/F}(\gamma)$ as $a + b\sqrt{\Delta_F}$ for some $a, b \in \frac{1}{2}\mathbb{Z}$, then $\delta_{F/\mathbb{Q}}(\mathrm{Trace}_{K/F}(\gamma)) = 2b\sqrt{\Delta_F}$. □

Lemma 62. *Let K be a quartic CM field with maximal totally real subfield F. If $\gamma \in \mathcal{O}_K$ and ϕ_1, ϕ_2 are any non-conjugate pair of embeddings $K \hookrightarrow \mathbb{C}$, then*

$$\phi_1(\gamma - \overline{\gamma})\phi_2(\gamma - \overline{\gamma}) \in \frac{\sqrt{\Delta_K}}{\Delta_F} \cdot \mathbb{Z}.$$

Proof. Let $\delta_{K/F}(\alpha)$ denote the relative different for any $\alpha \in \mathcal{O}_K$. Because K/F is a quadratic imaginary extension, we have that $\delta_{K/F}(\alpha) = \alpha - \overline{\alpha}$.

We may assume $K = F(\gamma)$ otherwise the claim is trivial as $\phi_1(\gamma - \overline{\gamma})\phi_2(\gamma - \overline{\gamma}) = 0$. From the proof of [66, Thm. III.2.5, Pg. 198],

$$\delta_{K/F}(\gamma)\mathcal{O}_K = \mathfrak{f}_{\mathcal{O}_F[\gamma]}\mathcal{D}_{K/F}$$

where $\mathfrak{f}_{\mathcal{O}_F[\gamma]} = \{\alpha \in K \colon \alpha\mathcal{O}_K \subseteq \mathcal{O}_F[\gamma]\}$ is the conductor of the order $\mathcal{O}_F[\gamma]$ in $\mathcal{O}_K$ and $\mathcal{D}_{K/F}$ is the relative different of the extension K/F.

Note that $\gamma + \overline{\gamma} \in \mathcal{O}_F$ implies that $\overline{\gamma} \in \mathcal{O}_F[\gamma]$, hence $\mathcal{O}_F[\gamma]$ is invariant under conjugation. It follows that $\mathfrak{f}_{\mathcal{O}_F[\gamma]}$ is invariant under conjugation, so we may write $\mathfrak{f}_{\mathcal{O}_F[\gamma]} = I \cdot \mathcal{O}_K$ for some

ideal $I \subseteq \mathcal{O}_F$. Then

$$\begin{aligned}(\phi_1(\gamma-\overline{\gamma})\phi_2(\gamma-\overline{\gamma}))^2 &= \mathrm{Norm}_{K/\mathbb{Q}}(\gamma-\overline{\gamma}) \\ &= \mathrm{Norm}_{K/\mathbb{Q}}\left(\delta_{K/F}(\gamma)\right) \\ &= \mathrm{Norm}_{F/\mathbb{Q}}(I)^2 \cdot \mathrm{Norm}_{K/\mathbb{Q}}(\mathcal{D}_{K/F}). \end{aligned} \tag{3.9}$$

The different and discriminant are related by the formula [66, Cor. III.2.10, Pg. 197]

$$\Delta_K = \Delta_F^2 \,\mathrm{Norm}_{K/\mathbb{Q}}\left(\mathcal{D}_{K/F}\right). \tag{3.10}$$

The claim follows from combining Equation 3.9 and Equation 3.10 and taking square roots.

□

Lemma 63. *Let f_1, f_2, P, P_0 be the polynomials from Equations (3.2)-(3.5). Then*

(i) $f_1 \in \mathbb{Z}[x_2, x_3, x_4]$

(ii) $f_2 \in \mathbb{Z}[x_3, x_4]$

(iii) $P \in \frac{1}{2}\mathbb{Z}[x_1, x_2, x_3, x_4]$

(iv) $P_0 \in \frac{1}{2}\mathbb{Z}[x_1, x_2, x_3, x_4]$.

Proof. It is straightforward from the definition of f_1, f_2 and the choice of basis $\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$ that $f_1 \in \mathbb{C}[x_2, x_3, x_4]$ and $f_2 \in \mathbb{C}[x_3, x_4]$. So it remains to check the domain of the coefficients.

The claims for f_1, P, and P_0 all follow directly from Lemma 61. For f_2, note that the coefficient of $x_i x_j$ is $\phi_1(\delta_i)\phi_2(\delta_j) + \phi_1(\delta_j)\phi_2(\delta_i)$, where $\delta_i = \alpha_i - \overline{\alpha}_i$. The claim for f_2 follows from Lemma 62 and the fact that

$$\phi_1(\delta_i)\phi_2(\delta_j) + \phi_1(\delta_j)\phi_2(\delta_i) = \phi_1(\delta_i+\delta_j)\phi_2(\delta_i+\delta_j) - \phi_1(\delta_i)\phi_2(\delta_i) - \phi_1(\delta_j)\phi_2(\delta_j).$$

□

Lemma 64. *f_2 is a integral bilinear quadratic form in x_3, x_4 with discriminant Δ_F.*

Proof. It is clear from the definition that f_2 is a homogeneous polynomial of degree 2, and by Lemma 63, $f_2 \in \mathbb{Z}[x_3, x_4]$. So it remains to calculate the discriminant.

Let $\delta_i = \alpha_i - \overline{\alpha}_i$. By definition,

$$\begin{aligned}\operatorname{Disc} f_2 &= \frac{\Delta_F^2}{\Delta_K}\left(\left(\phi_1(\delta_3)\phi_2(\delta_4) + \phi_2(\delta_3)\phi_1(\delta_4)\right)^2 - 4\phi_1(\delta_3)\phi_2(\delta_3)\phi_1(\delta_4)\phi_2(\delta_4)\right) \\ &= \frac{\Delta_F^2}{\Delta_K}\left(\phi_1(\delta_3)\phi_2(\delta_4) - \phi_2(\delta_3)\phi_1(\delta_4)\right)^2.\end{aligned}$$

Now we compute

$$\begin{aligned}\Delta_K &= \det \begin{pmatrix} 1 & \phi_1(\alpha_2) & \phi_1(\alpha_3) & \phi_1(\alpha_4) \\ 1 & \phi_1(\alpha_2) & \phi_1(\overline{\alpha_3}) & \phi_1(\overline{\alpha}_4) \\ 1 & \phi_2(\alpha_2) & \phi_2(\alpha_3) & \phi_2(\alpha_4) \\ 1 & \phi_2(\alpha_2) & \phi_2(\overline{\alpha}_3) & \phi_2(\overline{\alpha}_4) \end{pmatrix}^2 \\ &= \left(\phi_1(\alpha_2) - \phi_2(\alpha_2)\right)^2 \left(\phi_1(\delta_3)\phi_2(\delta_4) - \phi_2(\delta_3)\phi_1(\delta_4)\right)^2 \\ &= \Delta_F \left(\phi_1(\delta_3)\phi_2(\delta_4) - \phi_2(\delta_3)\phi_1(\delta_4)\right)^2.\end{aligned}$$

□

Next we prove the correctness of step 5 using our previous lemmas.

Lemma 65. *If (a_3, a_4) is outputted in step 5 of the algorithm in Section 3.3.2, then $f_2(a_3, a_4) = \pm 1$. Moreover, if $x_3 = a_3$, $x_4 = a_4$ is an integral solution to $f_2(x_3, x_4) = \pm 1$, then, given a large enough bound, step 5 will eventually output the pair (a_3, a_4).*

Proof. Following the notation from the algorithm, let $f_2(x_3, x_4) = ax_3^2 + bx_3x_4 + cx_4^2$. Recall from Lemma 64 that $a, b, c \in \mathbb{Z}$ and $b^2 - 4ac = \Delta_F$. Note that $\{a, (b + \sqrt{\Delta_F})/2\}$ is a $\mathbb{Q}$-basis for F. Here we are using that $F = \mathbb{Q}(\sqrt{\Delta_F})$. So we can write any $\sigma \in F$ as

$$\sigma = ax + \frac{b + \sqrt{\Delta_F}}{2} y,$$

for some $x, y \in \mathbb{Q}$. Then the norm of σ is

$$\mathrm{Norm}_{F/\mathbb{Q}}(\sigma) = \left(ax + \frac{b+\sqrt{\Delta_F}}{2}y\right)\left(ax + \frac{b-\sqrt{\Delta_F}}{2}y\right) = a\left(ax^2 + bxy + cy^2\right) = af_2(x,y).$$

Therefore $f_2(x,y) = \pm 1$ if and only if the corresponding σ has norm $\pm a$. Moreover, $x, y \in \mathbb{Z}$ if and only if σ lies in the ideal $I = a\mathbb{Z} + (b+\sqrt{\Delta_F})/2\mathbb{Z}$ (one can show this is an ideal using the fact that $b^2 - 4ac = \Delta_F$). Because $\mathrm{Norm}_{F/\mathbb{Q}}(I) = |a|$, it follows that $x_3 = x, x_4 = y$ is an integral solution to $f_2(x_3, x_4) = \pm 1$ if and only if $\sigma\mathcal{O}_F = I$. Therefore, we have a bijection between integral solutions to $f_2(x_3, x_4) = \pm 1$ and generators of I.

The claim follows as steps (5.1)-(5.3) enumerate all generators σ for the ideal I, and compute the associated integral solution to $f_2 = \pm 1$. □

Now we will find an explicit $\mathbb{Z}$-basis for the order $\mathbb{Z}[\pi, \overline{\pi}]$. This will allow us to write down a formula for $\mathrm{Disc}\,\mathbb{Z}[\pi, \overline{\pi}]$ in terms of the coefficients of π with respect to the basis $\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$ for $\mathcal{O}_K$. We will use this formula to determine when $\mathbb{Z}[\pi, \overline{\pi}] = \mathcal{O}_K$.

Lemma 66. *Let K be a quartic CM field and let $\pi \in \mathcal{O}_K$ be an Weil p-number. Then $B = \langle 1, \pi, \overline{\pi}, \pi^2 \rangle$ generates $\mathbb{Z}[\pi, \overline{\pi}]$ as a $\mathbb{Z}$-module.*

Proof. We will show that any power of π or $\overline{\pi}$ is contained in $\mathrm{Span}(B)$. The claim will follow because $\pi\overline{\pi} \in \mathbb{Z}$, so any product $\pi^i\overline{\pi}^j$ can be rewritten as sums of powers of π or $\overline{\pi}$. Because K is a quartic extension, we only have to show $\pi^3, \overline{\pi}^2, \overline{\pi}^3 \in \mathrm{Span}(B)$.

First we will show that $\overline{\pi}^2 \in \mathrm{Span}(B)$. Let F be the real quadratic subfield of K. Note that $\pi + \overline{\pi} \in \mathcal{O}_F$, so it has a characteristic polynomial in F of the form $x^2 + ax + b$ for some $a, b \in \mathbb{Z}$. It follows that

$$\begin{aligned}
(\pi + \overline{\pi})^2 &= -a(\pi + \overline{\pi}) - b \\
\pi^2 + \overline{\pi}^2 &= -a\pi - a\overline{\pi} - b - 2p \\
\overline{\pi}^2 &= -\pi^2 - a\pi - a\overline{\pi} - b - 2p. \qquad (3.11)
\end{aligned}$$

Now recall that the characteristic polynomial of π in K is of the form $x^4 - cx^3 + dx^2 - cpx + p^2$ for some $c, d \in \mathbb{Z}$. Using the fact that $\overline{\pi} = p/\pi$, this shows that

$$0 = \pi^4 - c\pi^3 + d\pi^2 - cp\pi + p^2$$

$$\pi^3 = c\pi^2 - d\pi + cp - p\overline{\pi} \tag{3.12}$$

$$\overline{\pi}^3 = c\overline{\pi}^2 + d\overline{\pi} + cp + p\pi. \tag{3.13}$$

It follows from Equations (3.11)-(3.13) that $\overline{\pi}^2, \pi^3, \overline{\pi}^3 \in \mathrm{Span}(B)$. □

Lemma 67. *Let K be a quartic CM field and let ϕ_1, ϕ_2 be non-conjugate embeddings $K \hookrightarrow \mathbb{C}$. If $\gamma \in \mathcal{O}_K$, then*

$$\mathrm{Disc}(1, \gamma, \overline{\gamma}, \gamma^2) = \left(\phi_1(\gamma + \overline{\gamma}) - \phi_2(\gamma + \overline{\gamma})\right)^4 \left(\phi_1(\gamma - \overline{\gamma})\phi_2(\gamma - \overline{\gamma})\right)^2.$$

Proof. Let $\beta_1 = 1, \beta_2 = \gamma, \beta_3 = \overline{\gamma}, \beta_4 = \gamma^2$. Then $\mathrm{Disc}(1, \gamma, \overline{\gamma}, \gamma^2) = \det \mathrm{Trace}_{K/\mathbb{Q}} \beta_i\beta_j$. Let $\gamma_i = \phi_i(\gamma)$. Because K is a CM field, complex conjugation commutes with embeddings into $\mathbb{C}$, so $\phi_i(\overline{\gamma}) = \overline{\gamma}_i$. Using this, we can compute $\mathrm{Trace}_{K/\mathbb{Q}} \beta_i\beta_j$ in terms of γ_1, γ_2. For example:

$$\mathrm{Trace}_{K/\mathbb{Q}} \beta_3\beta_4 = \mathrm{Trace}_{K/\mathbb{Q}} \gamma^2\overline{\gamma} = \gamma_1^2\overline{\gamma}_1 + \gamma_2^2\overline{\gamma}_2 + \gamma_1\overline{\gamma}_1^2 + \gamma_2\overline{\gamma}_2^2.$$

A straightforward computation shows that $\det \mathrm{Trace}_{K/\mathbb{Q}} \beta_i\beta_j$, when viewed as a polynomial in the ring $\mathbb{Z}[\gamma_1, \gamma_2, \overline{\gamma}_1, \overline{\gamma}_2]$, factors into the desired form. □

We are now ready to prove the correctness of the algorithm.

Theorem 68. *If the algorithm of Section 3.3.2 outputs π, then π is a super-isolated Weil number for K. Moreover, for any fixed super-isolated Weil number π for K, if the algorithm is given a large enough bound, then it will eventually output π.*

Proof. We will use the same notation as in Section 3.3.2. Let $a_1, a_2, a_3, a_4 \in \mathbb{Z}$ and let $\pi = \sum a_i\alpha_i$. A straightforward computation, using Lemma 61, shows that

$$\phi_1(\pi\overline{\pi}) = P(a_1, a_2, a_3, a_4) \pm P_0(a_1, a_2, a_3, a_4)\sqrt{\Delta_F}.$$

It follows that π is a Weil p-number for a prime p if and only if the following hold:

(i) $P_0(a_1, a_2, a_3, a_4) = 0$

(ii) $P(a_1, a_2, a_3, a_4)$ is prime.

Next we will show that if (i) holds, then $\mathbb{Z}[\pi, \overline{\pi}] = \mathcal{O}_K$ if and only if the following hold:

(iii) $f_1(a_1, a_2, a_3, a_4) = \pm 1$

(iv) $f_2(a_1, a_2, a_3, a_4) = \pm 1$.

By Lemma 66, $B = \{1, \pi, \overline{\pi}, \pi^2\}$ spans $\mathbb{Z}[\pi, \overline{\pi}]$ as a $\mathbb{Z}$-module. Therefore $\mathbb{Z}[\pi, \overline{\pi}]$ is an order in K if and only if $\operatorname{Disc} B \neq 0$, in which case B is basis for $\mathbb{Z}[\pi, \overline{\pi}]$. Hence $\mathbb{Z}[\pi, \overline{\pi}] = \mathcal{O}_K$ if and only if $\operatorname{Disc} B = \Delta_K$. By Lemma 67 and the definition of f_1, f_2,

$$\operatorname{Disc} B = \Delta_K f_1(a_1, a_2, a_3, a_4)^4 f_2(a_1, a_2, a_3, a_4)^2.$$

By Lemma 63, f_1 and f_2 are integer polynomials, so $\mathbb{Z}[\pi, \overline{\pi}] = \mathcal{O}_K$ if and only if $|f_1(a_1, a_2, a_3, a_4)| = |f_2(a_1, a_2, a_3, a_4)| = 1$.

We have shown that π is a super-isolated Weil number if and only if properties (i)-(iv) hold. Because the algorithm enumerates integral tuples (a_1, a_2, a_3, a_4) satisfying these properties, this shows that every algebraic integer the algorithm outputs is a super-isolated Weil number.

For the second claim, suppose that $\pi = \sum a_i \alpha_i$ is a super-isolated Weil number. Then by property (iv), $x_3 = a_3$, $x_4 = a_4$ is an integral solution to Equation 3.6. By Lemma 65, for a large enough bound, the algorithm will eventually enumerate a_3, a_4 in step 5. Recall that a_1, a_2 are essentially determined from a_3, a_4 (see steps 6 and 7). That is, for any given solution a_3, a_4 to Equation 3.6, there are two pairs (a_1, a_2) such that (a_1, a_2, a_3, a_4) satisfies Equations (3.6)-(3.8). Both pairs are found by the algorithm, so the algorithm will eventually output π. □

Efficiency

Recall that the algorithm in Section 3.3.2 enumerates solutions $x_1 = a_1$, $x_2 = a_2$, $x_3 = a_3$, $x_4 = a_4$ to Equations (3.6)-(3.8). For each integer i, chosen in step 5.2, the algorithm found several (possibly non-integral) solutions, see steps (5)-(7). In this section, we will show that the algorithm can find all solutions (a_1, a_2, a_3, a_4) with $P(a_1, a_2, a_3, a_4) \leq N$, by checking at most $O(\log N)$ values of i.

To prove the claim, we first show that the value of $|a_4|$ grows exponentially with $|i|$, i.e. $\log |a_4| = \Omega(|i|)$. Then we will show that the function $P(x_1, x_2, x_3, x_4)$, when restricted to solutions to Equations (3.6)-(3.8), is essentially bounded below by $|x_4|$.

Remark 69. The reason we choose a_4 instead of a_3 is that some of the equations turn out to be simpler. The same argument could be made with a_3 instead.

Lemma 70. *There are computable positive constants C_1, C_2, with $C_2 > 1$, such that if the integer i is chosen as in step 5.2, and the pair (a_3, a_4), with $a_4 \neq 0$, is computed as in step 5.3, then*

$$|a_4| \geq C_1 \cdot C_2^{|i|}.$$

The constants C_1, C_2 depend only on the basis chosen in step 2 and the generator chosen in step 5.1.

Proof. We will keep the notation from the algorithm in Section 3.3.2. Recall how the pair (a_3, a_4) is constructed from i in step 5. First we found an algebraic integer $\sigma \in \mathcal{O}_F$ of the form $\sigma = \pm\epsilon^i\gamma$ where γ generates the ideal $I = a\mathbb{Z} + (b + \sqrt{\Delta_F})/2\mathbb{Z}$, and ϵ is a fundamental unit of F. The pair a_3, a_4 are the coefficients of σ with respect to the $\mathbb{Z}$-basis $\{a, (b + \sqrt{\Delta_F})/2\}$ for I.

Using the quadratic formula and the fact that $a_3, a_4 \in \mathbb{Z}$, one can show that $f_2(a_3, a_4) = \pm 1$ implies that $|a_3| \leq C_0|a_4|$ for some constant C_0 that depends only on f_2 (hence C_0

depends on the basis chosen in step 2). So

$$\begin{aligned}\left(|a|C_0 + \frac{|b| + \sqrt{\Delta_F}}{2}\right)|a_4| &\geq |a_3||a| + |a_4|\frac{|b| + \sqrt{\Delta_F}}{2} \\ &\geq \max\left(\left|\phi_1(\gamma\epsilon^i)\right|, \left|\phi_2(\gamma\epsilon^i)\right|\right) \\ &\geq \min\left(|\phi_1(\gamma)|, |\phi_2(\gamma)|\right) \cdot \max(\left|\phi_1(\epsilon^i)\right|, \left|\phi_2(\epsilon^i)\right|) \\ &= \min\left(|\phi_1(\gamma)|, |\phi_2(\gamma)|\right) \cdot \max(|\phi_1(\epsilon)|, |\phi_2(\epsilon)|)^{|i|}.\end{aligned}$$

The last step follows from the fact that $\phi_1(\epsilon)\phi_2(\epsilon) = \pm 1$. □

Next we want to show that, for all integral solutions $x_1 = a_1$, $x_2 = a_2$, $x_3 = a_3$, $x_4 = a_4$ to Equations (3.6)-(3.8), the value of $P(a_1, a_2, a_3, a_4)$ is essentially bounded below by $|a_4|$. Recall that Equations 3.6 and 3.7 involve a choice of sign. To simplify our argument, we will first restrict to a specific set of signs.

Let A be the set of rational tuples $(a_1, a_2, a_3, a_4) \in \mathbb{Q}^4$ such that $x_1 = a_1, x_2 = a_2, x_3 = a_3, x_4 = a_4$ is a solution to the following equations:

$$f_1(x_2, x_3, x_4) = 1 \tag{3.14}$$

$$P_0(x_1, x_2, x_3, x_4) = 0 \tag{3.15}$$

$$x_3 = \frac{-b + \sqrt{b^2 - 4a(c - 1/x_4^2)}}{2a} x_4. \tag{3.16}$$

Equation 3.16 comes from solving $f_2(x_3, x_4) = 1$ for x_3 (recall that $f_2 = ax_3^2 + bx_3x_4 + cx_4^2$ for integers a, b, c). Therefore, every tuple in A is a solution to Equations (3.6)-(3.8) with the positive signs. Note that every integral solution to Equations (3.6)-(3.8) lies in a set defined in a way similar to A, only with a possibly different choice of signs.[6] Our arguments in the lemmas below will not depend on the choice of sign, so they will apply to any such set.

Lemma 71. *There exists an explicit function $P_4(x_4)$ such that for every $(a_1, a_2, a_3, a_4) \in A$,*

$$P(a_1, a_2, a_3, a_4) = P_4(a_4),$$

[6]There are a total of 8 choices of signs we could use to define A. These come from the three choices of signs: one in Equation 3.6, one in Equation 3.7, and one from the quadratic formula when solving Equation 3.6 for x_3. Every solution to Equations (3.6)-(3.8) lies in one of these 8 sets.

where P is the polynomial from Equation 3.4.

Proof. To prove the claim, we first find functions $g_1(x_4), g_2(x_4), g_3(x_4)$ such that for all tuples $(a_1, a_2, a_3, a_4) \in A$, $a_i = g_i(a_4)$ for $i = 1, 2, 3$. Then we will substitute the g_i's into the polynomial P in order to construct $P_4(x_4)$.

Let

$$g_3(x_4) = \frac{-b + \sqrt{b^2 - 4a(c - 1/x_4^2)}}{2a} x_4.$$

Then by construction, $a_3 = g_3(a_4)$ for all $(a_1, a_2, a_3, a_4) \in A$.

Next we will find g_2. Recall that $f_1(x_2, x_3, x_4)$ is a linear polynomial with a non-zero coefficient of x_2 (see step 6 in the algorithm in Section 3.3.2). So we can use Equation 3.14 to write x_2 as a linear function of x_3 and x_4. By substituting g_3 for x_3, we obtain a function g_2 which satisfies $a_2 = g_2(a_4)$ for all $(a_1, a_2, a_3, a_3) \in A$.

Now we will find g_1. Recall that $P_0(x_1, x_2, x_3, x_4) = f_1 x_1 + g$ for some $g \in \mathbb{Z}[x_2, x_3, x_4]$ (see step 7). By Equations 3.14 and 3.15, $a_1 = -g(a_2, a_3, a_4)$ for all $(a_1, a_2, a_3, a_4) \in A$. By replacing x_2, x_3 in $-g$ with g_2, g_3 respectively, we obtain a function $g_1(x_4)$ such that $a_1 = g_1(a_4)$ for all $(a_1, a_2, a_3, a_4) \in A$.

Let

$$P_4(x_4) = P(g_1(x_4), g_2(x_4), g_3(x_4), x_4).$$

Note that P_4 has the desired property because for all $(a_1, a_2, a_3, a_4) \in A$, we have that $g_i(a_4) = a_i$ for $i = 1, 2, 3$. □

Theorem 72. *The algorithm in Section 3.3.2 can find all super-isolated Weil p-numbers with $p \leq N$ in $O(\log N)$ steps. That is, for each quartic CM field K of class number 1, there is at least one set of choices that can be made in steps 2 and 3 such that the algorithm only needs to check $O(\log N)$ values of $|i|$ in step 5.2. Here the implicit constant depends on the choices made.*

Sketch of proof. By Theorem 68, the algorithm will eventually output any specific super-isolated Weil number given a large enough bound. Therefore, it is sufficient to show that

the value of $P(a_1, a_2, a_3, a_4)$ in step 8 grows exponentially in $|i|$. From Lemma 70, we know that $\log |a_4| = \Omega(|i|)$, so it is sufficient to show that $P(a_1, a_2, a_3, a_4) = \Omega(|a_4|)$.

Recall that there are only 91 such fields. For each one, we computed the function P_4 from Lemma 71 after choosing some random values in steps 2 and 3. We found that $|P_4(x_4)| = \Omega(x_4^4)$. We repeated the calculations for every alternative definition of the set A from Lemma 71, and found the same result (this property seems to always hold in practice). Some details for the case of $K = \mathbb{Q}(\zeta_5)$ are given in Appendix A. We also used these calculations in the proof of Theorem 75 below.

Let (a_1, a_2, a_3, a_4) be any integral solution to Equations (3.6)-(3.8). Then $P(a_1, a_2, a_3, a_4) = P_4(a_4)$ for some P_4 (recall the definition of P_4 depended on the set A, so there are 8 possibilities for P_4). Since $|P_4(x_4)| = \Omega(x_4^4)$, it follows that $P(a_1, a_2, a_3, a_4) = \Omega(a_4^4)$. □

3.3.3 Examples

We found the following super-isolated Weil numbers for quartic CM fields with class number 1 by using the algorithm in Section 3.3.2.

Example 73.

$$\pi = \frac{225058681}{16}\left(\sqrt{-19-8\sqrt{2}}\right)^3 + \frac{1}{16}\left(-19-8\sqrt{2}\right) + \frac{6822363251}{16}\sqrt{-19-8\sqrt{2}} - \frac{4404669978983883573}{16}.$$

Here $p = \pi\overline{\pi} = 75785615717819865717549739169971883$ is a 116 bit prime, and $N = \mathrm{Norm}_{K/\mathbb{Q}}(\pi - 1)$ factors as 31 times a 227 bit prime. The associated surface is the jacobian of the following hyperelliptic curve over $\mathbb{F}_p$:

$$\begin{aligned} y^2 = {} & 5189749050536255546947 80x^6 + 1102935355117356837110620x^5 + 9912872922380249405558 12x^4 \\ & + 4785882497866214343330 76x^3 + 1302732035052812016945 44x^2 + 1917953444391234465228 8x \\ & + 1373526256863485541624. \end{aligned}$$

Example 74.

$$\pi = \frac{701408733}{8}\left(\sqrt{-13-2\sqrt{5}}\right)^3 - \frac{1}{8}\left(-13-2\sqrt{5}\right) + \frac{12255108743}{8}\sqrt{-13-2\sqrt{5}} + \frac{18762798022945344405}{8}.$$

Here $p = \pi\overline{\pi} = 55006654632787769594536175901603367 93$ is a 123 bit prime, and $N = \mathrm{Norm}_{K/\mathbb{Q}}(\pi - 1)$ factors as 521 times a 236 bit prime. The associated surface is the jacobian of the following hyperelliptic curve over $\mathbb{F}_p$:

$$\begin{aligned} y^2 = {} & 3166541774481651094230166870474839614x^6 + 1534528670722732390900201720396554 16x^5 \\ & + 4397111106428325553768487123769953829x^4 + 4136411707045872026156847617680586720x^3 \\ & + 8016463193608798020781188016836493 66x^2 + 3958303885280886436811484306434693399x \\ & + 2303639253886822235537433002764323459. \end{aligned}$$

3.3.4 Main Result

Our main result is that Examples 73 and 74 are the only examples of super-isolated surfaces with near-prime order and cryptographic size.

Theorem 75. *Examples 73 and 74 are the only super-isolated abelian surfaces $A/\mathbb{F}_p$ with the property that*

$$\#A(\mathbb{F}_p) = cr \text{ where } c \leq 1000, \ r \text{ is prime, and } 2^{160} \leq r \leq 2^{512}. \tag{3.17}$$

Sketch of proof. We will show that if A is a super-isolated abelian surface satisfying property (3.17), then the roots of the characteristic polynomial of the Frobenius endomorphism of A are super-isolated Weil p-numbers for a quartic CM field K with class number 1, such that $p \leq 2^{261}$. The claim then follows by running the algorithm in Section 3.3.2 long enough to find all such Weil numbers.

Let A be a super-isolated abelian surface over $\mathbb{F}_p$ satisfying property (3.17). We want to apply Corollary 57, but we first must show that the characteristic polynomial f of the Frobenius endomorphism is irreducible. Recall from Section 3.3.1 that $\#A(\mathbb{F}_p) = f(1)$. Using the well-known Hasse bound and property (3.17), it is not difficult to see that A is not the product of two elliptic curves, hence A is simple. Therefore f is a power of an irreducible polynomial (see Section 3.3.1). Because $f(1)$ is almost prime, this implies that f is irreducible. So by Corollary 57, every root π of f is a super-isolated Weil p-number in the quartic CM field $K = \mathbb{Q}(\pi)$ of class number 1.

Next we will show that property 3.17 implies that $p \leq 2^{261}$. This is similar to using the Hasse bound above. Since the roots of f are Weil p-numbers, it follows that $f(x) = x^4 + ax^3 + bx^2 + pax + p^2$ with $|a| \leq 4\sqrt{p}$ and $|b| \leq 6p$. So

$$r \geq \frac{p^2 - 4p^{3/2} - 6p - 4\sqrt{p} - 1}{1000}.$$

A straightforward calculation shows that this inequality, when combined with the bound $r \geq 2^{512}$, implies that $p \leq 2^{261}$.

The next part of the proof is computational. We used `Sage` to compute the implicit constants in Section 3.3.2 that are used to bound the number of steps the algorithm must take in order to enumerate all super-isolated Weil p-numbers with $p \leq 2^{261}$ (see Theorem 72). Some details for the case of $K = \mathbb{Q}(\zeta_5)$ are given in Appendix A. Our results show that there are 282 conjugacy classes of such Weil numbers. Only those given in Examples 73 and 74 satisfy the properties in the claim. The source code is available at https://sites.math.washington.edu/~tscholl2/super-isolated. □

Remark 76. The bound $c \leq 1000$ used above is arbitrary. The smaller c is the more efficient the cryptosystem will be. The three smallest values of c were 31, 521, and 73399.

Remark 77. Note that the surfaces in Examples 73 and 74 provide 113 and 116 bits of security respectively (i.e. half the bitlength of the largest prime dividing the order). Recent standards suggest using between 128 and 256 bits of security [65].

3.4 Generalizations to Arbitrary Finite Fields

In this section, we will briefly summarize how our results extend to arbitrary finite fields.

The main result from Section 3.2 is Corollary 45. This extends directly to arbitrary finite fields by replacing the prime p with any prime power q. This is because the main ingredient, Theorem 4.6 of [73], applies to elliptic curves over $\mathbb{F}_q$. The estimates in Section 3.2.3 can also be modified by allowing the polynomial $p(x)$ to take on prime power values. Because non-prime prime powers are sparse, these changes are not expected to effect the estimates given in Heuristic 52.

The main result from Section 3.3 is Theorem 55. This can be extended to arbitrary finite fields $\mathbb{F}_q$, where q is a power of a prime p, by adding the hypothesis that A is ordinary. Essentially, this means that $\pi + \overline{\pi}$ is prime to p, see [89, Ch. 7] for more details. In order to extend the algorithm in Section 3.3.2, we would want to allow the polynomial $P(x_1, x_2, x_3, x_4)$ in Equation 3.4 to take prime values, and then check that the algebraic integer π has the property that $\pi + \overline{\pi}$ is prime to p.

Chapter 4

SUPER-ISOLATED ABELIAN VARIETIES

4.1 Introduction

The goal of this chapter is to characterize abelian varieties A defined over a finite field $\mathbb{F}_q$ such that the $\mathbb{F}_q$-isogeny class of A contains a single $\mathbb{F}_q$-isomorphism class. In this case, we call A *super-isolated* (see Definition 118 below). The study of super-isolated varieties was originally motivated by elliptic curve cryptography. In the previous chapters, we discussed hypothetical situations in which it is advantageous to choose parameters for cryptosystems that use curves with a small isogeny class. Hyperelliptic cryptosystems which are used today use Jacobians of curves of genus 1 or 2. As noted in the previous chapter, there are fewer isolated curves with genus 2 than with genus 1. The main result of this chapter is that for $g \geq 3$, there are only finitely many super-isolated ordinary simple abelian varieties of dimension g (see Corollary 123 below). This is interesting because it means that most curves whose Jacobian is super-isolated are among the curves that could be used in practice. Essentially, we have an existence result in the practical range, and a non-existence result in the non-practical range.

This chapter is organized as follows. In Section 4.2 we review some standard results in algebraic number theory that will be used in the following sections. This will also serve to set most of our notation. In Section 4.3 we introduce certain algebraic integers called *Weil generators*. In Section 4.4, we outline a simple algorithm to enumerate Weil generators in a given number field. Our main result on Weil generators is Theorem 102 in Section 4.5. In Section 4.7, we apply the results on Weil generators to study super-isolated varieties. The finiteness result mentioned above can be made effective when $g = 3$. Some detailed examples of how to compute the corresponding constants are given in Section 4.6. Examples showing

how Weil generators correspond to super-isolated varieties are given in Section 4.7.

4.2 Background

The goal of this section is to recall some standard facts from algebraic number theory and to set notation.

For an extension of number fields K/F, let $\mathrm{Disc}_{K/F}$ and $\mathrm{Diff}_{K/F}$ denote the relative discriminant and different ideals respectively. If the field F is not given, then it is assumed to be $\mathbb{Q}$. Let h_K denote the class number of K.

For any $\alpha \in K$, let $\mathrm{Disc}_{K/F}(\alpha)$ and $\mathrm{Diff}_{K/F}(\alpha)$ denote the discriminant and different of α respectively. If $f \in F[x]$ is the characteristic polynomial of α over F, then by definition $\mathrm{Diff}_{K/F}(\alpha) = f'(\alpha)$ and $\mathrm{Disc}_{K/F}(\alpha)$ is the discriminant of f.

Example 78. If $K \neq F(\alpha)$, then $\mathrm{Diff}_{K/F}(\alpha) = \mathrm{Disc}_{K/F}(\alpha) = 0$.

Example 79. Suppose K is a CM field and F is the maximal totally real subfield. For any $\alpha \in K$, the characteristic polynomial of α over F is $f(x) = x^2 - (\alpha + \overline{\alpha})x + \alpha\overline{\alpha}$. So $\mathrm{Diff}_{K/F}(\alpha) = \alpha - \overline{\alpha}$ and $\mathrm{Disc}_{K/F}(\alpha) = (\alpha - \overline{\alpha})^2$.

Lemma 80. *Let K/F be an arbitrary extension of number fields and let $\alpha \in K$ such that $K = F(\alpha)$. Then*

$$\mathrm{Disc}_{K/F}(\alpha) = (-1)^{\binom{[K:F]}{2}} \mathrm{Norm}_{K/F}\left(\mathrm{Diff}_{K/F}(\alpha)\right).$$

Proof. The proof is the same as in the special case with $F = \mathbb{Q}$, which appears as Theorem 8 in [57, Pg. 26]. □

Lemma 81. *Let K/F be an arbitrary extension of number fields. Then*

$$\mathcal{O}_K = \mathcal{O}_F[\alpha] \quad \Leftrightarrow \quad (\mathrm{Diff}_{K/F}(\alpha)) = \mathrm{Diff}_{K/F}.$$

Proof. The forwards direction is proved in [66, Prop. 2.4, Pg. 197], so it remains to prove the reverse direction. Suppose that $(\mathrm{Diff}_{K/F}(\alpha)) = \mathrm{Diff}_{K/F}$. Then by Lemma 80 and [66,

Thm. 2.9, Pg. 201],

$$\left(\mathrm{Disc}_{K/F}(\alpha)\right) = \left(\mathrm{Norm}_{K/F}\left(\mathrm{Diff}_{K/F}(\alpha)\right)\right) = \mathrm{Norm}_{K/F}\left(\mathrm{Diff}_{K/F}\right) = \mathrm{Disc}_{K/F}\,.$$

Recall that if $\{\beta_j\}$ is a basis for $\mathcal{O}_F$, then the set $\{\beta_j\alpha^i\}$ spans a $\mathbb{Z}$-submodule of $\mathcal{O}_K$ and has discriminant

$$\mathrm{Norm}_{K/F}\left(\mathrm{Disc}_{K/F}(\alpha)\right)\mathrm{Disc}_F^{[K:F]} = \mathrm{Disc}_{K/F}\,\mathrm{Disc}_F^{[K:F]},$$

see [57, Pg. 43]. This last quantity is Disc_K by [66, Cor. 2.10, Pg. 202]. In particular, $\{\beta_j\alpha^i\}$ is a basis for $\mathcal{O}_K$, so $\mathcal{O}_K = \mathcal{O}_F[\alpha]$. □

Definition 82. Let $\alpha \in \overline{\mathbb{Q}}$. The *height* of α is

$$h(\alpha) = \max_{\sigma:\mathbb{Q}(\alpha)\to\mathbb{C}} |\sigma(\alpha)|\,.$$

4.3 Weil Generators

The goal of this section is to define certain algebraic integers we call *Weil generators*, and to give some of their properties.

Definition 83. Let K be a CM field. We say $\alpha \in \mathcal{O}_K$ is a *Weil number* if $\alpha\overline{\alpha} \in \mathbb{Z}$. If $\alpha\overline{\alpha} = n$, then we say α is a Weil n-number.

Remark 84. If α is a Weil number in K, then $|\sigma(\alpha)|$ is constant for all $\sigma : K \to \mathbb{C}$. This means that $|\,\mathrm{Norm}_{K/\mathbb{Q}}(\alpha)| = h(\alpha)^{[K:\mathbb{Q}]}$.

Definition 85. Let K be a CM field. We say $\alpha \in \mathcal{O}_K$ is a *Weil generator for* K if α is a Weil number and $\mathbb{Z}[\alpha, \overline{\alpha}] = \mathcal{O}_K$.

Example 86. If α is a Weil number in K, then so is $\zeta\alpha$ for any root of unity ζ in K. However, this does not hold for Weil generators. For example, if $K = \mathbb{Q}(i)$, then i is a Weil generator for K, but $i^2 = -1$ is not because it lies in a proper subfield of K. However, if α is a Weil generator, then so are all of the conjugates of α and $-\alpha$.

Example 87. Let $K = \mathbb{Q}(i)$ and $\alpha = i$. Then $\alpha\overline{\alpha} = 1$ and $\mathbb{Z}[\alpha, \overline{\alpha}] = \mathcal{O}_K$, so α is a Weil generator. In fact, if K is any quadratic imaginary field and $\mathcal{O}_K = \mathbb{Z}[\gamma]$, then α is a Weil generator for K if and only if $\alpha = a \pm \gamma$ for some $a \in \mathbb{Z}$.

Remark 88. If α is a Weil generator for K and F is the maximal totally real subfield of K, then $\mathcal{O}_K = \mathcal{O}_F[\alpha]$. By Lemma 81, this implies that $(\mathrm{Diff}_{K/F}(\alpha)) = \mathrm{Diff}_{K/F}$.

Example 89. Let $K = \mathbb{Q}(\sqrt{10}, \sqrt{-13})$. Then $\mathrm{Diff}_{K/F} = (26, 13 + \sqrt{-13})$ is not a principal ideal. Therefore K does not contain a Weil generator by Remark 88.

Example 90. Let $K = \mathbb{Q}(\sqrt{60}, \sqrt{-2})$. We claim that there is no α such that $\mathcal{O}_K = \mathcal{O}_F[\alpha]$, which implies that K does not contain a Weil generator. Suppose for contradiction that such an α exists. Because 2 is totally ramified in K, it follows that $\mathrm{Diff}_{K/F} = (2)$. Therefore $\alpha - \overline{\alpha} = 2u$ for some $u \in \mathcal{O}_K^\times$. But one can show that $\mathcal{O}_K^\times = \mathcal{O}_F^\times$, so any such u actually lies in F. This is a contradiction because conjugation negates $\alpha - \overline{\alpha}$ but fixes $2u$.

Example 91. Let ζ_n be a primitive nth root of unity with $n \geq 3$, and let $K = \mathbb{Q}(\zeta_n)$. Then ζ_n is a Weil generator for K because $\mathcal{O}_K = \mathbb{Z}[\zeta_n]$ and $\zeta_n\overline{\zeta}_n = 1$.

Lemma 92. *Let K be a CM field and F be the maximal totally real subfield of K. If α is a Weil generator for K, then $\mathcal{O}_F = \mathbb{Z}[\alpha + \overline{\alpha}]$.*

Proof. By hypothesis, every element of $\mathcal{O}_K$ can be written as polynomial in $\alpha, \overline{\alpha}$ with coefficients in $\mathbb{Z}$. $\mathcal{O}_F$ is precisely the polynomials which are symmetric in α and $\overline{\alpha}$. Recall that the subring of symmetric polynomials in $\mathbb{Z}[x, y]$ is $\mathbb{Z}[x + y, xy]$. Therefore, $\mathcal{O}_F = \mathbb{Z}[\alpha + \overline{\alpha}, \alpha\overline{\alpha}]$. But $\alpha\overline{\alpha} \in \mathbb{Z}$, so this is the same as $\mathbb{Z}[\alpha + \overline{\alpha}]$. □

Remark 93. If α is a Weil number in K, then the property $\mathcal{O}_F = \mathbb{Z}[\alpha + \overline{\alpha}]$ does not imply α is a Weil generator. For example, if K is a quadratic imaginary field, then every $\alpha \in \mathcal{O}_K$ satisfies $\alpha\overline{\alpha} \in \mathbb{Z}$ and $\mathcal{O}_F = \mathbb{Z}[\alpha + \overline{\alpha}]$. However, not every α will satisfy $\mathcal{O}_K = \mathbb{Z}[\alpha, \overline{\alpha}]$, e.g. $K = \mathbb{Q}(i)$ and $\alpha = 2i$.

Example 94. Let $K = \mathbb{Q}[x]/(x^6 + 12x^4 + 17x^2 + 2)$. Then K is a CM field of degree 6. Moreover, the prime 2 splits completely in F, hence there are 3 maps from $\mathcal{O}_F \to \mathbb{F}_2$. This shows that F is not monogenic as there are only 2 maps $\mathbb{Z}[x] \to \mathbb{F}_2$. Therefore K does not contain any Weil generators.

Lemma 95. *Let K be a CM field and F the maximal totally real subfield of K. Then $\alpha \in \mathcal{O}_K$ is a Weil generator for K if and only if the following hold*

(i) $\alpha\overline{\alpha} \in \mathbb{Z}$

(ii) $\mathbb{Z}[\alpha + \overline{\alpha}] = \mathcal{O}_F$

(iii) $(\mathrm{Diff}_{K/F}(\alpha)) = \mathrm{Diff}_{K/F}$

Proof. Suppose that α is a Weil generator for K. Then α satisfies property (i) by definition, and property (ii) follows from Lemma 92. Note that $\mathcal{O}_K = \mathbb{Z}[\alpha, \overline{\alpha}]$ implies that $\mathcal{O}_K = \mathcal{O}_F[\alpha]$. So by Lemma 81, α satisfies property (iii).

Now suppose that $\alpha \in K$ satisfies properties (i)-(iii). By Lemma 81 and property (iii), $\mathcal{O}_K = \mathcal{O}_F[\alpha]$ and $\mathcal{O}_F = \mathbb{Z}[\alpha + \overline{\alpha}]$. Hence $\mathcal{O}_K = \mathbb{Z}[\alpha, \alpha + \overline{\alpha}] = \mathbb{Z}[\alpha, \overline{\alpha}]$, so α is a Weil generator. □

Remark 96. The properties in Lemma 95 are independent as shown by the following examples:

1. If $K = \mathbb{Q}(i)$ and $\alpha = 2i$, then (i) and (ii) hold, but not (iii).

2. If $K = \mathbb{Q}(\zeta_5)$ and $\alpha = \zeta_5 + 1$, then (ii) and (iii) hold, but not (i).

3. If $K = \mathbb{Q}(\zeta_5)$ and $\alpha = -5\zeta_5^3 - 4\zeta_5^2 + 2\zeta_5 - 2$, then (i) and (iii) hold, but not (ii).

Next we will show that we can always write Weil generators in a certain form. To do this, we first introduce some notation. Let K be a fixed CM field of degree $2g$. Let F be

the maximal totally real subfield of K. Fix $\gamma \in \mathcal{O}_K$ such that $\mathcal{O}_K = \mathcal{O}_F[\gamma]$.[1] Let T denote a set of representatives of the set of $\eta \in \mathcal{O}_F$ such that $\mathbb{Z}[\eta] = \mathcal{O}_F$ modulo integer translation. That is, for every η' such that $\mathbb{Z}[\eta'] = \mathcal{O}_F$, there exists a unique $\eta \in T$ such that $\eta' - \eta \in \mathbb{Z}$.

Lemma 97. *If $\alpha \in K$ is a Weil generator, then*

$$\alpha = \frac{u(\gamma - \overline{\gamma}) + \eta + a}{2} \tag{4.1}$$

for a unique $u \in \mathcal{O}_F^\times$, $\eta \in T$, and $a \in \mathbb{Z}$.

Proof. Let $u = (\alpha - \overline{\alpha})/(\gamma - \overline{\gamma})$. By Lemma 81 and Lemma 95, both $\alpha - \overline{\alpha}$ and $\gamma - \overline{\gamma}$ generate $\mathrm{Diff}_{K/F}$, so $u \in \mathcal{O}_F^\times$. By Lemma 92, $\mathbb{Z}[\alpha + \overline{\alpha}] = \mathcal{O}_F$, so there is a unique $\eta \in T$ such that $a = \alpha + \overline{\alpha} - \eta \in \mathbb{Z}$. Then η, u, and a satisfy the required conditions. □

Next we recall a theorem of György which implies that the set T is finite. This means that the number of possible η (up to integer translation) in equation (4.1) is finite.

Theorem 98 ([37])**.** *For any number field L, the set T of η such that $\mathcal{O}_L = \mathbb{Z}[\eta]$, up to integer translation, is finite. Moreover, representatives for T can be effectively determined.*

Example 99. If $\deg L = 2$, then we may choose $T = \left\{(\mathrm{Disc}_L \pm \sqrt{\mathrm{Disc}_L})/2\right\}$. Hence T has cardinality 2.

Equation (4.1) suggests that one way to search for Weil generators is to fix γ and enumerate over values for η, u, and a. The following lemma gives an optimization: when $g \geq 2$, there is at most one possible value of a.

Lemma 100. *If $g \geq 2$, then for any $u \in \mathcal{O}_F^\times$ and $\eta \in T$, then there is at most one $a \in \mathbb{Z}$ such that the right hand side of equation (4.1) is a Weil generator.*

Proof. Let $u \in \mathcal{O}_F^\times$ and $\eta \in T$. Let $\Omega = (u(\gamma - \overline{\gamma}) + \eta)/2$. It is sufficient to show that there is at most one $a \in \mathbb{Q}$ such that $\alpha = \Omega + a/2$ satisfies $\alpha\overline{\alpha} \in \mathbb{Q}$. This is a necessary condition

[1] It is possible that such a γ does not exist, as in Example 90. However, by Lemma 81 and Lemma 95, if no such γ exists, then K does not contain a Weil generator.

for α to be a Weil generator. A straightforward computation shows that $\alpha\overline{\alpha} \in \mathbb{Q}$ if and only if $\Omega\overline{\Omega} + a\eta/2 \in \mathbb{Q}$. Because $\{1, \eta, \ldots, \eta^g\}$ is a $\mathbb{Q}$-basis for F, we may write $\Omega\overline{\Omega} = \sum a_i\eta^i$ for unique rational numbers $a_0, \ldots, a_g \in \mathbb{Q}$. Then $\Omega\overline{\Omega} + a\eta/2 \in \mathbb{Q}$ if and only if $a = -2a_1$ and $a_i = 0$ for all $i > 1$. □

4.4 Searching for Weil Generators

The goal of this section is to describe an efficient method for searching for Weil generators in a given CM field K. We will use the same notation as in Section 4.3.

A naive approach to finding Weil generators is to directly search over all elements of $\mathcal{O}_K$. Using Lemma 95, one can quickly test whether a given $\alpha \in \mathcal{O}_K$ is a Weil generator. This approach is impractical because Weil generators are sparse, as shown in Theorem 102 below. Instead, we will enumerate units in F and use those to attempt to construct Weil generators.

Recall from Lemma 97 that every Weil generator α can be written as

$$\alpha = \frac{u(\gamma - \overline{\gamma}) + \eta + a}{2},$$

for a unique $u \in \mathcal{O}_F^\times$, $\eta \in T$, and $a \in \mathbb{Z}$. Moreover, a is uniquely determined by u and η (see Lemma 100). Therefore, by searching over all u and η, we will eventually find all Weil generators α.

Algorithm 3 Search Weil Generators

Input: A CM field K of degree $2g$, with $g \geq 2$, and a bound B

Output: All Weil generators in K up to a certain bound.

$F \leftarrow$ the maximal totally real subfield of K
$\gamma \leftarrow$ an element of K such that $\mathcal{O}_K = \mathcal{O}_F[\gamma]$
$T \leftarrow$ a complete set of $\eta \in F$ such that $\mathcal{O}_F = \mathbb{Z}[\eta]$ up integer translation
$U \leftarrow$ all units $u \in \mathcal{O}_F^\times$ with height $h(u) \leq B$
for all $u \in U$ and $\eta \in T$ **do**
    $\Omega \leftarrow (u(\gamma - \overline{\gamma}) + \eta)/2$
    Write $\Omega\overline{\Omega} = \sum_{i=0}^{g-1} a_i \eta^i$.
    $\alpha \leftarrow \Omega - a_1$
    if $a_i = 0$ for $i > 1$ and $\alpha \in \mathcal{O}_K$ **then**
        print α
    end if
end for

Theorem 101. *Every α outputted by the Algorithm 3 is a Weil generator. Moreover, for every Weil generator $\alpha \in K$, if Algorithm 3 is given a sufficiently large set U, then it will eventually print α.*

Proof. Suppose that the algorithm outputs α. Then $\alpha = \Omega - a_1$ where $\Omega = (u(\gamma - \overline{\gamma}) + \eta)/2$ and $a_1 \in \mathbb{Q}$. Because $\Omega\overline{\Omega} - a_1\eta \in \mathbb{Q}$, it follows that $(\Omega - a_1)(\overline{\Omega} - a_1) = \alpha\overline{\alpha} \in \mathbb{Q}$. Recall that $\alpha \in \mathcal{O}_K$ by construction, so $\alpha\overline{\alpha} \in \mathbb{Z}$. This also shows that $a_1 \in \mathbb{Q} \cap \frac{1}{2}\mathcal{O}_K = \frac{1}{2}\mathbb{Z}$. Hence $\alpha + \overline{\alpha} = \eta - 2a_1 \in \eta + \mathbb{Z}$, so $\mathbb{Z}[\alpha + \overline{\alpha}] = \mathcal{O}_F$. Also, $\alpha - \overline{\alpha} = \Omega - \overline{\Omega} = u(\gamma - \overline{\gamma})$ so $(\mathrm{Diff}_{K/F}(\alpha)) = (\mathrm{Diff}_{K/F}(\gamma)) = \mathrm{Diff}_{K/F}$. By Lemma 95, this shows that α is a Weil generator.

Now suppose that α is a Weil generator for K. We want to show that for a large enough bound B, Algorithm 3 will eventually output α. By Lemma 97, $\alpha = (u(\gamma - \overline{\gamma}) + \eta + a)/2$ for unique $u \in \mathcal{O}_F^\times$, $\eta \in T$, and $a \in \mathbb{Z}$. If $B \geq h(u)$, then Algorithm 3 is guaranteed to find α because it enumerates all possible η and a (which corresponds to $-2a_1$ in the notation of

Algorithm 3) such that $(u(\gamma - \overline{\gamma}) + \eta + a)/2$ is a Weil generator. □

4.5 Counting Weil Generators

In this section, we state and prove our main result on the number of Weil generators of bounded height in a given CM field K of degree $2g$.

Theorem 102. *Let W be the set of Weil generators in a CM field K of degree $2g$. Then*

$$\#\{\alpha \in W : h(\alpha) \leq N\} = \begin{cases} 4N + O(1) & g = 1 \\ \rho \log N + O(1) & g = 2 \text{ and } W \neq \emptyset \\ O(1) & g \geq 3, \end{cases}$$

where ρ is a constant depending on K. Moreover, for $g \leq 3$, the constants can be made effective.

To prove Theorem 102, we proceed by cases depending on the degree of K. The case $g = 1$ is given by Proposition 104 in Section 4.5.1. The case $g = 2$ is given by Proposition 105 in Section 4.5.2. Lastly, the result for $g \geq 3$ is given by Proposition 110 in Section 4.5.3.

Throughout this section, we will keep the notation introduced at the end of Section 4.3. Unless otherwise noted,

- K is a fixed CM field of degree $2g$.
- F is the maximal totally real subfield of K.
- γ is a fixed element of K such that $\mathcal{O}_K = \mathcal{O}_F[\gamma]$.
- T is a set of representatives of generators for $\mathcal{O}_F$ up to integer translation. That is, if $\eta \in T$ then $\mathcal{O}_F = \mathbb{Z}[\eta]$.

Remark 103. It is possible that such a γ does not exist, as in Example 90. However, by Lemma 81 and Lemma 95, a necessary condition for K to contain a Weil generator is that such a γ exists.

4.5.1 The Case $g = 1$

The goal of this section is to prove Theorem 102 in the case $g = 1$.

Proposition 104. *If K is a quadratic imaginary field, then*

$$\#\{\alpha \in W : h(\alpha) \leq N\} = 4N + O(1).$$

Proof. Let $-d = \mathrm{Disc}_K$ and let $\omega = (d \pm \sqrt{-d})/2$. Then $\mathcal{O}_K = \mathbb{Z}[\omega]$. Recall from Example 87 that $\alpha \in K$ is a Weil generator if and only if $\alpha = a \pm \omega$ for some $a \in \mathbb{Z}$. The claim follows because $h(a \pm \omega) = |a| + O(1)$. □

4.5.2 The Case $g = 2$

The goal of this section is to prove Theorem 102 in the case $g = 2$.

Proposition 105. *Let K be a quartic CM field. There is a constant ρ that depends only on K such that if $W \neq \emptyset$, then*

$$\#\{\alpha \in W : h(\alpha) \leq N\} = \rho \log N + O(1).$$

Moreover, both ρ and the implied constant in $O(1)$ are effectively computable.

The main idea behind the proof of Proposition 105 is to show that counting Weil numbers reduces to counting solutions to Pell's equation.

We will use the same notation as before. Because F is a real quadratic field, we can take T to be $\{\pm(d + \sqrt{d})/2\}$ where $d = \mathrm{Disc}_F$. However, there is no obvious choice of γ because $\mathcal{O}_K$ is not always a free $\mathcal{O}_F$-module, e.g. Example 89. Some of the implied constants in this section will depend on the choice of γ and T as will the implied constant in the proposition. But the constant ρ in Proposition 105 depends only on the field K.

The outline of the proof of Proposition 105 is as follows. Let $\alpha \in W$. By Lemma 97, we can write $\alpha = (u(\gamma - \overline{\gamma}) + \eta + a)/2$ for a unique $u \in \mathcal{O}_F^\times$, $\eta \in T$, and $a \in \mathbb{Z}$. First we will show that $h(\alpha)$ is approximately $h(u)^2$ (see Lemma 109 below). Next we will count the

number of $u \in \mathcal{O}_F^\times$ which are associated to some $\alpha \in W$. Recall that every such u is of the form $\pm u_0^k$ where u_0 is a fundamental unit for F and k is an integer. We will show that u corresponds to some α if and only if k satisfies a certain congruence condition. Therefore counting the number of α of bounded height essentially reduces to counting the number of k of bounded absolute value in a given congruence class.

Before proving Proposition 105, we describe an example in detail that both motivates and shows how to compute the value of ρ for the field $\mathbb{Q}(\zeta_5)$.

Example 106. We will show how to compute the constant ρ from Proposition 105 for the field $K = \mathbb{Q}(\zeta_5)$. Let[2] $\gamma = \zeta_5$, $\eta_0 = \zeta_5 + \overline{\zeta}_5$, and $T = \{\eta_0, -\eta_0\}$. A fundamental unit for F is $u_0 = \zeta_5 + \overline{\zeta}_5$. For $u \in \mathcal{O}_F^\times$ and $\eta \in T$ we define the following quantities:

$$\begin{aligned}
\Omega(u,\eta) &= \frac{u(\gamma - \overline{\gamma}) + \eta}{2}, \\
a(u,\eta) &= \text{The unique element of } (1/2)\mathbb{Z} \text{ such that } \operatorname{Norm}_{K/F}\left(\Omega(u,\eta) + \frac{a(u,\eta)}{2}\right) \in \mathbb{Q} \\
&\qquad \text{(see the proof of Lemma 100)}, \\
\alpha(u,\eta) &= \Omega(u,\eta) + \frac{a(u,\eta)}{2}.
\end{aligned}$$

Note that it is not always the case that $a(u,\eta) \in \mathbb{Z}$. For example, if $u = \eta_0^2$, then $a(u,\eta_0) = 5/2$. For this reason, $\alpha(u,\eta)$ is not a Weil generator for all possible pairs (u,η).

By Lemma 97, every $\alpha \in W$ is of the form $\alpha(u,\eta)$ for some $u \in \mathcal{O}_F^\times$ and $\eta \in T$. We want to characterize pairs (u,η) for which $\alpha(u,\eta) \in W$. Recall that every $u \in \mathcal{O}_F^\times$ can be written as $u = \pm u_0^k$ for some $k \in \mathbb{Z}$. Our first step is to prove that

$$\alpha(\pm u_0^k, \pm\eta_0) \in W \text{ if and only if } k \text{ satisfies a certain congruence condition.} \tag{4.2}$$

It turns out that $\alpha(u,\eta)$ is a Weil generator if and only if it is integral. To see this, note

[2]It is not always true that T can be chosen as fundamental units of F. For example, the fundamental units for $\mathbb{Q}(\sqrt{6})$ are $\pm(5+2\sqrt{6})^{\pm 1}$ which do not generate the ring of integers $\mathbb{Z}[\sqrt{6}]$. Similarly, $\gamma + \overline{\gamma}$ is not always in T. For example, if $K = \mathbb{Q}(\sqrt{5}, \sqrt{-1})$ then $\mathcal{O}_K = \mathbb{Z}[(1+\sqrt{5})/2, \sqrt{-1}]$ so we may choose $\gamma = \sqrt{-1}$ hence $\gamma + \overline{\gamma} = 0$.

that $\alpha(u,\eta)$ has the following properties:

$$\alpha(u,\eta)\overline{\alpha(u,\eta)} \in \mathbb{Q}, \quad \alpha(u,\eta) + \overline{\alpha(u,\eta)} = \eta + a, \quad \text{and} \quad \alpha(u,\eta) - \overline{\alpha(u,\eta)} = u\,(\gamma - \overline{\gamma})\,.$$

So by Lemma 95, $\alpha(u,\eta) \in W$ if and only if $\alpha(u,\eta) \in \mathcal{O}_K$. By construction, $\alpha(u,\eta) \in (1/4)\mathcal{O}_K$ for all $u \in \mathcal{O}_F^\times$ and $\eta \in T$. Therefore $\alpha(u,\eta) \in W$ if and only if $4\alpha(u,\eta) \equiv 0 \mod 4\mathcal{O}_K$. We want to characterize the values of u and η for which this congruence condition holds.

The equivalence class of $\alpha(u,\eta)$ modulo $4\mathcal{O}_K$ depends only on the equivalence class of u and η modulo $4\mathcal{O}_F$. To see why, we need to show that $\Omega(u,\eta)$ and $a(u,\eta)$ modulo $4\mathcal{O}_K$ depend only on u and η modulo $4\mathcal{O}_F$. The dependence of $\Omega(u,\eta)$ on u and η is clear. Recall that the construction of $a(u,\eta)$ given in Lemma 100 depends only on the coefficients of $\Omega(u,\eta)\overline{\Omega(u,\eta)}$ with respect to the basis $\{1,\eta\}$. Hence $4a(u,\eta)$ modulo 4 depends only on u and η modulo $4\mathcal{O}_F$. Therefore $\alpha(u,\eta) \in W$ if and only if u and η lie in a particular set of equivalence classes of $\mathcal{O}_F/4\mathcal{O}_F$.

Next we will show that we can restrict attention to pairs (u,η) of the form (u_0^k,η_0). Recall that every pair (u,η) is of the form $(\pm u_0^k, \pm\eta_0)$ for some choice of signs and integer $k \in \mathbb{Z}$. It follows from the definition of Weil generator that $\alpha \in W$ if and only if $\pm\alpha, \pm\overline{\alpha} \in W$. This means that $\alpha(\pm u_0^k, \pm\eta_0) \in W$ if and only if $\alpha(u_0^k,\eta_0) \in W$. In particular $\alpha(\pm u_0^k, \pm\eta_0)$ lies in W if and only if u_0^k lies in a particular equivalence class in $\mathcal{O}_F/4\mathcal{O}_F$. The statement in equation (4.2) now follows since u_0 has finite order in $(\mathcal{O}_F/4\mathcal{O}_F)^\times$.

Next we will determine explicitly the condition on k such that $\alpha(u_0^k,\eta_0) \in W$. Because 2 is inert in F, u_0 has order 3 in $(\mathcal{O}_F/2\mathcal{O}_F)^\times$. Table 4.1 gives the values of $4\alpha(u_0^k,\eta_0)$ mod $4\mathcal{O}_K$ for $k = 0,1,2$. It shows that $\alpha(\pm u_0^k, \pm\eta_0) \in W$ if and only if $k \not\equiv 2 \mod 3$.

We have shown that each $k \in \mathbb{Z}$ with $k \not\equiv 2 \mod 3$ corresponds to 4 Weil generators given by $\alpha(\pm u_0^k, \pm\eta_0)$. Lemma 109 below says that $h(\alpha(\pm u_0^k, \pm\eta_0))$ is approximately $h(u_0^k)^2$. Thus we can conclude the following (more details are given in the proof of Proposition 105 below).

k	$4\alpha(u_0^k, \eta_0) \mod 4\mathcal{O}_K$
0	0
1	0
2	$-2\zeta_5^3 - 2\zeta_5^2 + 1$

Table 4.1: Values of $4\alpha(u_0^k, \eta_0)$ modulo $4\mathcal{O}_K$.

$$\begin{aligned}
\#\{\alpha \in W : h(\alpha) \le N\} &= 4 \cdot \#\left\{k \in \mathbb{Z} : k \not\equiv 2 \mod 3 \text{ and } h(u_0^k) \le \sqrt{N}\right\} + O(1) \\
&= 4 \cdot \#\left\{k \in \mathbb{Z} : k \not\equiv 2 \mod 3 \text{ and } |k| \le \frac{\log N}{2 \log h(u_0)}\right\} + O(1) \\
&= \frac{8 \log N}{3 \log h(u_0)} + O(1). \\
&= \frac{8 \log N}{3 \log\left(\frac{1+\sqrt{5}}{2}\right)} + O(1).
\end{aligned}$$

Figure 4.1 below shows the accuracy of this estimate for the number of Weil generators of bounded height.

Next we will proceed with our proof of Proposition 105. We start with some lemmas. Our first goal is to show that $h(\alpha)$ is approximately $h(u)^2$. In order to compare $h(\alpha)$ and $h(u)$, we will need the following lemmas. For a fixed $\eta \in T$, we can write any $\beta \in F$ in the form $\beta = b + c\eta$ for some unique $b, c \in \mathbb{Q}$. The lemmas below compare $h(\beta)$ with $|c|$.

Lemma 107. *Let $\eta \in \overline{\mathbb{Q}} \setminus \mathbb{Q}$ and let $\beta = b + c\eta$ for some $b, c \in \mathbb{Q}$. Then there is a positive constant C_1 that depends only on η such that if $c \neq 0$ then*

$$C_1|c| \le h(\beta).$$

Proof. Let σ and τ be embeddings $\overline{\mathbb{Q}} \to \mathbb{C}$ such that $\sigma(\eta) \neq \tau(\eta)$. Let $C_1 = |\sigma(\eta) - \tau(\eta)|/2$, i.e. C_1 is half the distance from $\sigma(\eta)$ to $\tau(\eta)$. Since $-b/c$ cannot be closer than C_1 to both

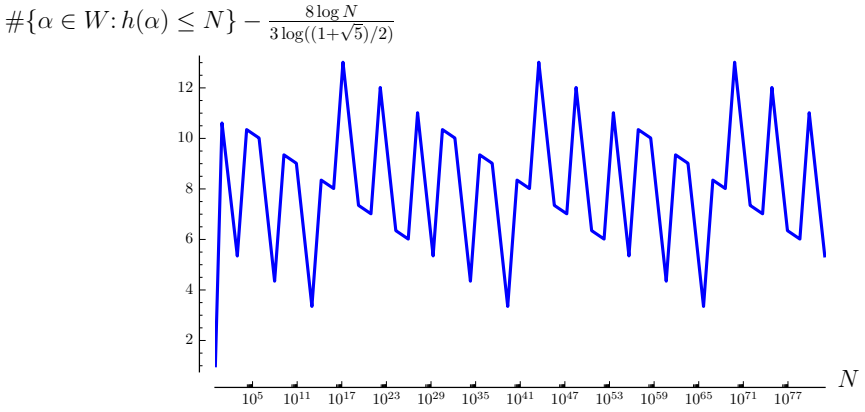

Figure 4.1: A comparison of the number of Weil generators of bounded height as found by Algorithm 3 and the asymptotic value given in Example 106.

$\sigma(\eta)$ and $\tau(\eta)$, we have that

$$C_1 \leq \max\left\{\left|\frac{b}{c}+\sigma(\eta)\right|, \left|\frac{b}{c}+\tau(\eta)\right|\right\} \leq h\left(\frac{b}{c}+\eta\right).$$

Up to replacing b, c with $-b, -c$, we may assume that c is positive. The claim then follows from multiplying this inequality by c and using the fact that h commutes with multiplication by a positive rational number. □

Lemma 108. *Let F be a real quadratic field and let $\eta \in \mathcal{O}_F$. For any $\beta \in \mathbb{Z}[\eta]$, there is a positive constant C_2 depending only on η such that if $\beta = b + c\eta$ with $b, c \in \mathbb{Z}$ and $c \neq 0$, then*

$$h(\beta) \leq C_2|c|\sqrt{\left|\mathrm{Norm}_{F/\mathbb{Q}}\,\beta\right|}.$$

Proof. By the triangle inequality, $h(\beta) \leq |b| + |c|h(\eta)$. Therefore it is enough to bound $|b|$ from above by a constant times $|c|\sqrt{\left|\mathrm{Norm}_{F/\mathbb{Q}}(\beta)\right|}$. Let $t = \mathrm{Trace}_{F/\mathbb{Q}}(\eta)$, $n_\eta = \mathrm{Norm}_{F/\mathbb{Q}}(\eta)$, and $n_\beta = \mathrm{Norm}_{F/\mathbb{Q}}(\beta)$. Then we can write the norm of $b + c\eta = \beta$ as $b^2 + bct + c^2 n_\eta = n_\beta$.

Therefore

$$\begin{aligned}
|b| &= \frac{\left|-ct \pm \sqrt{(ct)^2 - 4\left(c^2 n_\eta - n_\beta\right)}\right|}{2} \\
&\leq |c| \cdot \left(\frac{|t| + \sqrt{t^2 + 4\left(|n_\eta| + |n_\beta|/c^2\right)}}{2} \right) \\
&\leq |c| \cdot \left(\frac{|t| + \sqrt{t^2 + 4\left(|n_\eta| + |n_\beta|\right)}}{2} \right) \\
&\leq |c|\sqrt{|n_\beta|} \cdot \left(\frac{|t| + \sqrt{t^2 + 4\left(|n_\eta| + 1\right)}}{2} \right).
\end{aligned}$$

□

Next we will combine the two previous lemmas to show that if $\alpha \in W$ and $u \in \mathcal{O}_F^\times$ is the associated unit, then $h(\alpha)$ is approximately $h(u)^2$.

Lemma 109. *Let $\alpha \in W$, and let $u \in \mathcal{O}_F^\times$, $\eta \in T$, and $a \in \mathbb{Z}$ satisfy $\alpha = (u(\gamma - \overline{\gamma}) + \eta + a)/2$, as in Lemma 97. Then there exist positive constants C_3, C_4, C_5, depending only on γ and η, such that if $h(u) \geq C_3$ then*

$$C_4 h(u)^2 \leq h(\alpha) \leq C_5 h(u)^2.$$

Proof. Let $\Omega = (u(\gamma - \overline{\gamma}) + \eta)/2$ so that $\alpha = \Omega + a/2$. To prove the claim we will show that if $h(u)$ is sufficiently large, then $h(\Omega)$ is approximately $h(u)$ and $|a|$ is approximately $h(u)^2$.

First we will show that $h(\Omega)$ is approximately $h(u)$. By choosing C_3 large enough, we can assume that

$$\frac{\min_\sigma \{|\sigma(\gamma - \overline{\gamma})|\}}{2} h(u) \leq h(u) \min_\sigma \{|\sigma(\gamma - \overline{\gamma})|\} - h(\eta).$$

Note that the right hand side is

$$\leq h(u(\gamma - \overline{\gamma})) - h(\eta).$$

By the triangle inequality, the last expression is

$$\leq 2h(\Omega) \leq h(u)h(\gamma - \overline{\gamma}) + h(\eta).$$

We may also choose C_3 large enough so that $h(u) \geq h(\eta)$. So the previous expression is

$$\leq (h(\gamma - \overline{\gamma}) + 1)\, h(u).$$

Thus we have shown that

$$\frac{\min_\sigma \{|\sigma(\gamma - \overline{\gamma})|\}}{2} h(u) \leq 2h(\Omega) \leq (h(\gamma - \overline{\gamma}) + 1)\, h(u).$$

Next we will show that $|a|$ is approximately $h(u)^2$. Recall that $\alpha = \Omega + a/2$ for a unique integer a. As seen in the proof of Lemma 100, $-a/2$ is the coefficient of η when $\Omega\overline{\Omega}$ is written with respect to the $\mathbb{Q}$-basis $\{1, \eta\}$ of F. That is, $\Omega\overline{\Omega} = b - a/2\eta$ where b is an integer.

We would like to apply Lemmas 107 and 108 to relate $|a|$ to $h(\Omega\overline{\Omega})$. However, $\mathrm{Norm}_{F/\mathbb{Q}}(\Omega\overline{\Omega})$ may be large, so the bound in Lemma 108 is not useful. To get around this issue, we will consider $\Omega - \eta/2$ instead of Ω. Let $\beta = (\Omega - \eta/2)(\overline{\Omega} - \eta/2)$. Note that

$$\beta = \frac{-u^2(\gamma - \overline{\gamma})^2}{4} \quad \text{and} \quad \beta = b - \frac{a}{2}\eta - \frac{\eta}{2}\left(\Omega + \overline{\Omega}\right) + \frac{\eta^2}{4} = b - \frac{a}{2}\eta - \frac{\eta^2}{4}.$$

The equation on the left shows that $\mathrm{Norm}_{F/\mathbb{Q}}\, \beta$ depends only on γ, and that $h(\beta)$ can be bounded above and below by $h(u)^2$ times constants depending only on γ. The equation on the right shows that the coefficient of η of β written with respect to the basis $\{1, \eta\}$ is $-a/2$ plus a constant depending only on η. Therefore, assuming that $\beta \notin \mathbb{Q}$, we may apply Lemmas 107 and 108 to relate $h(\beta)$ and $|a|$. Up to replacing the constants in the lemmas by some factors that depend only on η and γ, we have

$$C_1|a| \leq h(u)^2 \leq C_2|a|.$$

The final step is to show that there are only finitely many $\alpha \in W$ such that $\beta \in \mathbb{Q}$. This is necessary because the hypothesis of Lemmas 107 and 108 require that $c \neq 0$, where c is the coefficient of η of β written with respect to the basis $\{1, \eta\}$. Note that if $c = 0$, then $\beta \in \mathbb{Q}$ and $h(\beta) = \sqrt{\mathrm{Norm}_{F/\mathbb{Q}}(\beta)}$. The latter which depends only on γ. In particular, this means there are finitely many possible β, hence there are finitely many Weil generators α with this property. $\square$

We are now ready to finish the proof of Proposition 105 by counting the number of $u \in \mathcal{O}_F^\times$ which are associated to some $\alpha \in W$.

Proof. Our proof follows the same argument as in Example 106. Let u_0 be a fundamental unit for F and let η_0 be a generator for $\mathcal{O}_F$, i.e. $\mathcal{O}_F = \mathbb{Z}[\eta_0]$. For any $k \in \mathbb{Z}$ and choice of signs, let $\alpha(\pm u_0^k, \pm\eta_0)$ be defined as in Example 106. Recall that every $\alpha \in W$ is of the form $\alpha = \alpha(\pm u_0^k, \pm\eta_0)$ for some choice of signs and integer k.

Note that the argument given in Example 106 that proves the statement in equation (4.2) holds in general. That is, $\alpha(\pm u_0^k, \pm\eta_0) \in W$ if and only if k satisfies a congruence condition. Let $\mathcal{P}$ denote the set of $k \in \mathbb{Z}$ that satisfy this condition.

By applying Lemma 109 to η_0 and $-\eta_0$, we can find positive constants C_3, C_4, C_5, which depend only on γ, such that if $h(\alpha(\pm u_0^k, \pm\eta_0)) \geq C_3$ then

$$C_4 h(u_0)^{2|k|} \leq h(\alpha(\pm u_0^k, \pm\eta_0)) \leq C_5 h(u_0)^{2|k|}.$$

Let S be the number of Weil generators of height less than C_3. Then

$$4 \cdot \#\left\{k \in \mathcal{P} \colon C_5 h(u_0)^{2|k|} \leq N\right\} - S \leq \#\left\{\alpha \in W \colon h(\alpha) \leq N\right\} \leq 4 \cdot \#\left\{k \in \mathcal{P} \colon C_4 h(u_0)^{2|k|} \leq N\right\} + S. \tag{4.3}$$

As $\mathcal{P}$ is characterized by a congruence condition, there is a constant C_6 such that

$$\#\{k \in \mathcal{P} \colon |k| \leq M\} = C_6 M + O(1).$$

Then both sides of the inequalities in equation (4.3) are equal to

$$\frac{2C_6 \log N}{\log h(u_0)} + O(1).$$

□

4.5.3 The Case $g \geq 3$

The goal of this section is to prove Theorem 102 in the case $g \geq 3$.

Proposition 110. *If K is a CM field of degree $2g$ with $g \geq 3$, then W is finite. Moreover, if $g = 3$ then the there is a computable upper bound for $\#W$.*

Our proof of Proposition 110 is as follows. Recall that every Weil generator α can be written in the form $(u(\gamma - \overline{\gamma}) + \eta + a)/2$ for a unique $u \in \mathcal{O}_F^\times$, $\eta \in T$, and $a \in \mathbb{Z}$. Recall that by definition, $\alpha\overline{\alpha} \in \mathbb{Z}$. This condition places a significant restriction on the possible values of u, η, and a. By Lemma 100, a is uniquely determined by u and η. Therefore it suffices to show that the possible set of pairs (u, η) arising in this way is finite. In fact, we will parameterize pairs (u, η) by integral points on a finite union of absolutely irreducible plane curves of degree g. These curves will have g distinct points at infinity. So by Siegel's theorem, the number of integral points is finite. When $g = 3$, the curves have genus 1 or 0 depending on the singularities. In the genus 0 case, finding integral points reduces to finding solutions to an S-unit equation, which can be effectively determined [39, Thm. D.8.4]. In the genus 1 case, we may use the effective (but impractical) bounds from Baker and Coates [3]. For more details on the effective bounds, see Section 4.6.

We start by proving a lemma which will be used to show that the curves arising in the proof of Proposition 110 are geometrically irreducible.

Lemma 111. *Let $f_1, \ldots, f_g \in \overline{\mathbb{Q}}[x, y, z]$ be homogeneous linear polynomials such that the lines in projective space defined by the vanishing of the f_i intersect the line at infinity (given by $z = 0$) at distinct points. If $t \in \overline{\mathbb{Q}}$ is nonzero, then $tz^g + \prod f_i$ is irreducible.*

Proof. Let $F_t = tz^g + \prod f_i$, and let $h_1, \ldots, h_k$ be the irreducible factors of F_t, i.e.

$$F_t(x, y, z) = tz^g + \prod_{i=1}^{g} f_i(x, y, z) = \prod_{j=1}^{k} h_j(x, y, z).$$

By hypothesis, the line defined by $f_i(x, y, z) = 0$ does not coincide with the line at infinity. So by a change of coordinates, we may assume that $f_1 = x$. Then $F_t(0, y, z) = tz^g = \prod h_j(0, y, z)$. Because $t \neq 0$, it follows $h_j(0, y, z)$ is of the form $a_j z^{n_j}$ for some nonzero a_j and positive integer n_j. This shows that the point $(0 : 1 : 0)$ lies in every irreducible component of the projective variety defined by F_t.

Notice that the projective variety defined by F_0 is a union of lines, all of whose pairwise intersections occur in the affine plane. This means that F_0 has no singularities on the line at infinity. The same property also holds for F_t because

$$\frac{dF_t}{dx} = \frac{dF_0}{dx}, \quad \frac{dF_t}{dy} = \frac{dF_0}{dy}, \quad \frac{dF_t}{dz}(x,y,0) = \frac{dF_0}{dz}(x,y,0), \quad \text{and } F_t(x,y,0) = F_0(x,y,0).$$

Therefore the point $P = (0:1:0)$ must be a smooth point of the variety defined by F_t, and hence lies in a distinct irreducible component. But by the above, P lies in every irreducible component, hence F_t is irreducible. □

We are now ready to prove Proposition 110.

Proof of Proposition 110. Let $\alpha \in W$. Recall that α can be written as $(u(\gamma - \overline{\gamma}) + \eta + a)/2$ for a unique $u \in \mathcal{O}_F^\times$, $\eta \in T$, and $a \in \mathbb{Z}$. Let $\Omega = \alpha - a/2$. By definition,

$$\alpha\overline{\alpha} = \Omega\overline{\Omega} + \frac{\eta a}{2} + \frac{a^2}{4} \in \mathbb{Z}.$$

Let $\delta = (\gamma - \overline{\gamma})(\overline{\gamma} - \gamma)$. Then we have shown that

$$4\Omega\overline{\Omega} = u^2\delta + \eta^2 = A + B\eta \tag{4.4}$$

for some $A, B \in \mathbb{Z}$. It is important that $4\Omega\overline{\Omega}$ lies in the $\mathbb{Z}$-span of $\{1, \eta\}$. This already is a significant restriction on the possible values of u and η since $\mathcal{O}_F$ has rank $g \geq 3$ by hypothesis.

By [66, Cor. 2.10, Pg. 202], $\mathrm{Norm}_{F/\mathbb{Q}}(u^2\delta) = \mathrm{Norm}_{F/\mathbb{Q}}(\delta) = \pm \mathrm{Disc}_K / \mathrm{Disc}_F^2$. So by rearranging equation (4.4) and taking norms, we have that

$$\mathrm{Norm}_{F/\mathbb{Q}}\left(A + B\eta - \eta^2\right) = \frac{|\mathrm{Disc}_K|}{\mathrm{Disc}_F^2}.$$

In particular, $x = A$ and $y = B$ is an integral point on the curve C_η given by the vanishing of the polynomial

$$-\frac{|\mathrm{Disc}_K|}{\mathrm{Disc}_F^2} + \prod_{\sigma : F \to \mathbb{C}} \left(x + y\sigma(\eta) - \sigma(\eta)^2\right). \tag{4.5}$$

By construction, C_η has g distinct points at infinity given by $(-\sigma(\eta) : 1 : 0)$. Because C_η is geometrically irreducible by Lemma 111, it follows from Siegel's theorem [77] (see also [39, Rem. D.9.2.2]) that C_η has finitely many integral points.

To finish the proof, it suffices to show that the map described above sending $\alpha \in W$ to the integral point (A, B) is finite-to-one. Recall that by Theorem 98, the set T is finite, so we may fix some $\eta \in T$. By equation (4.4), u is determined up to sign by the point (A, B) and η. Finally, by Lemma 100, a is determined by the pair (u, η). Hence for each point (A, B) there is a finite number of possible triples (u, η, a) corresponding to Weil generators.

When $g = 3$, we use an effective version of Siegel's theorem. Note that in this case, the curve C_η has genus 1 or 0 depending on its singularities. If C_η has genus 0, then the integral points can be computed by solving an S-unit equation [39, Thm. D.8.4]. If C_η has genus 1, then the main theorem of [2] gives a computable (but impractical) bound on the number of integral points. For more details, see Section 4.6. □

4.6 *Effectiveness With* $g = 3$

The goal of this section is to show how to give a concrete bound for the number of Weil generators in a sextic CM field. We will start by summarizing the relevant results from Section 4.5.

Let K be a CM field with maximal totally real subfield F and let W be the set of all Weil generators in K. Recall from Lemma 97 that every $\alpha \in W$ corresponds to a unique triple (u, η, a) with $u \in \mathcal{O}_F^\times$, $\eta \in T$, and $a \in \mathbb{Z}$. By Lemma 100, a is uniquely determined by η and u. Furthermore, the proof of Proposition 110 showed that all possible values of u for a fixed η are determined up to sign by the integral points of the curve C_η defined by equation (4.5). Therefore,

$$\#W \leq 2 \sum_{\eta \in T} \#C_\eta(\mathbb{Z}).$$

The following lemma shows that if $\deg K = 6$, then it is sufficient to consider a single $\eta \in T$.

Lemma 112. *Suppose that* $\deg K = 6$*, and let* $\eta_1, \eta_2 \in T$*. Then* C_{η_1} *and* C_{η_2} *are isomorphic via an integral linear change of variables. In particular, there is a bijection between* $C_{\eta_1}(\mathbb{Z})$ *and* $C_{\eta_2}(\mathbb{Z})$*.*

Proof. Recall that the curve C_{η_i} is defined by the polynomial $f_{\eta_i}(x, y)$ in equation (4.5). For any embedding $\sigma : F \to \mathbb{R}$, let $L_i^\sigma(x, y) = x + y\sigma(\eta_i) - \sigma(\eta_i)^2$. Then

$$f_{\eta_i}(x, y) = \prod_{\sigma : F \to \mathbb{R}} L_i^\sigma(x, y) - \frac{|\operatorname{Disc}_K|}{\operatorname{Disc}_F^2}.$$

To prove the claim, we will construct an invertible integral change of coordinates $\tilde{v}$ such that $f_{\eta_1} \circ \tilde{v} = f_{\eta_2}$. Our construction of $\tilde{v}$ relies on finding an algebraic integer $v \in \mathcal{O}_F$ with the property that

$$v = A_1 + B_1\eta_1, \quad v\eta_2 = A_2 + B_2\eta_1, \quad v\eta_2^2 = A_3 + B_3\eta_1 + \eta_1^2, \tag{4.6}$$

for some integers $A_i, B_i \in \mathbb{Z}$. First we will show how to construct $\tilde{v}$ given such a v. A construction of v is given at the end of the proof.

We define $\tilde{v} : \mathbb{R}^2 \to \mathbb{R}^2$ by

$$\tilde{v}(x, y) = (A_1x + A_2y - A_3, B_1x + B_2y - B_3).$$

To show that $\tilde{v}$ has the desired property, we will first show that $\tilde{v}$ transforms L_1^σ to a scaled L_2^σ. Note that

$$\begin{aligned}
(L_1^\sigma \circ \tilde{v})(x, y) &= (A_1x + A_2y - A_3) + (B_1x + B_2y - B_3)\sigma(\eta_1) - \sigma(\eta_1^2) \\
&= \sigma(A_1 + B_1\eta_1)x + \sigma(A_2 + B_2\eta_1)y - \sigma(A_3 + B_3\eta_1 + \eta_1^2) \\
&= \sigma(v)\left(x + \sigma(\eta_2)y - \sigma(\eta_2^2)\right) \\
&= \sigma(v)L_2^\sigma(x, y).
\end{aligned}$$

Therefore

$$f_{\eta_1} \circ \tilde{v} = \prod_\sigma (L_1^\sigma \circ \tilde{v}) - \frac{|\operatorname{Disc}_K|}{\operatorname{Disc}_F^2} = \operatorname{Norm}_{F/\mathbb{Q}}(v) \prod_\sigma L_2^\sigma - \frac{|\operatorname{Disc}_K|}{\operatorname{Disc}_F^2}.$$

If $v \in \mathcal{O}_F^\times$, then the right hand side of this equation is f_{η_2} as required.

Next we will show that $v \in \mathcal{O}_F^\times$ by constructing an inverse to $\tilde{v}$. Because $L_1^\sigma \circ \tilde{v} = \sigma(v) L_2^\sigma$ for all σ, it follows that $\tilde{v}$ maps the intersection of the lines defined by $L_2^{\sigma_i}(x,y) = 0$ and $L_2^{\sigma_j}(x,y) = 0$ to the intersection of the lines defined by $L_1^{\sigma_i}(x,y) = 0$ and $L_1^{\sigma_j}(x,y) = 0$, for all pairs (σ_i, σ_j). By swapping η_1 and η_2 in our construction for v, which is given below, we can find an element $v' \in \mathcal{O}_F$ such that the linear map $\tilde{v}'$ acts as an inverse to $\tilde{v}$ on these intersections. The lines defined by the polynomials $\{L_1^\sigma \colon \sigma : F \to \mathbb{R}\}$ are in general position. So it follows that $\tilde{v} \circ \tilde{v}'$ fixes three distinct points. Therefore, $\tilde{v}$ and $\tilde{v}'$ are inverses, and

$$L_1^\sigma = L_1^\sigma \circ \tilde{v} \circ \tilde{v}' = \sigma(v) \left(L_2^\sigma \circ \tilde{v}'\right) = \sigma(vv') L_1^\sigma.$$

This shows that $vv' = 1$, so $v \in \mathcal{O}_F^\times$.

It remains to construct the element v satisfying equation (4.6). Our (rather technical) construction of v is as follows. Consider the two $\mathbb{Z}$-bases for $\mathcal{O}_F$ given by $\mathcal{B}_i = \{1, \eta_i, \eta_i^2\}$ for $i = 1, 2$. Let P be the change of basis matrix from $\mathcal{B}_2$ to $\mathcal{B}_1$. That is, the columns of P are the elements of $\mathcal{B}_2$ written as vectors with respect to the basis $\mathcal{B}_1$. Let $P^{-1}_{i,j}$ denote the i,j-entry of the matrix P^{-1}, and for $\beta \in \mathcal{O}_F$, let $[\beta]_i$ denote the ith component of the vector given by writing β with respect to the basis $\mathcal{B}_1$. Now define

$$v = P^{-1}_{3,3} - P^{-1}_{3,2}[\eta_1^3]_3 + P^{-1}_{3,2}\eta_1.$$

A straightforward but tedious calculation proves that v satisfies the properties given in equation (4.6). □

Remark 113. Lemma 112 fails when $g > 3$. For example, using `Magma`, one can show that if $K = \mathbb{Q}(\zeta_{15})$, $\eta_1 = \zeta_{15}^7 - \zeta_{15}^6 - \zeta_{15}^5 + 2\zeta_{15}^4 - \zeta_{15}^2 - 2$, and $\eta_2 = -\zeta_{15}^7 + \zeta_{15}^5 - \zeta_{15}^4 + \zeta_{15}^2 - \zeta_{15} - 3$; then C_{η_1} and C_{η_2} are not isomorphic.

By Lemma 112, in order to find all Weil generators in a sextic CM field, it suffices to find all integral points on C_η for a single $\eta \in T$. The others can be computed by the change of coordinates from the lemma. Because $g = 3$, C_η is a plane curve of degree 3, so there are two

possible values for the genus. If C_η is singular, then it has genus 0 and the integer points can be enumerated by solving a certain S-unit equation [39, Thm. D.8.4]. If C_η is smooth, then it has genus 1. In this case, one can attempt to find all integer points using the methods of [83].

4.6.1 An Example of Genus 0

In this section, we will find all Weil generators in $\mathbb{Q}(\zeta_9)$. This field was chosen because it was the only sextic CM field with class number 1 such that the resulting curves C_η had genus 0. The class number requirement is not used in this section, but it is relevant for finding super-isolated abelian varieties as described in Section 4.7 below.

Proposition 114. *There are* 36 *Weil generators in* $\mathbb{Q}(\zeta_9)$. *They are:*

$$
\begin{aligned}
&-3\zeta_9^4-2\zeta_9,\ -\zeta_9^5+2\zeta_9^2,\ -2\zeta_9^5-\zeta_9^4+2\zeta_9^3-2\zeta_9+4,\ \zeta_9^5-2\zeta_9^4-2\zeta_9^3+2\zeta_9^2+2,\ -2\zeta_9^5-3\zeta_9^2,\ \zeta_9^4+3\zeta_9,\\
&-2\zeta_9^5+2\zeta_9^4-2\zeta_9^3-\zeta_9^2+2\zeta_9+2,\ -\zeta_9^4+2\zeta_9^3-2\zeta_9^2+\zeta_9+4,\ -\zeta_9,\ \zeta_9^5+\zeta_9^2,\ -\zeta_9^2,\ \zeta_9^4+\zeta_9,\\
&-\zeta_9^4-\zeta_9,\ \zeta_9^2,\ -\zeta_9^5-\zeta_9^2,\ \zeta_9,\ -\zeta_9^5+2\zeta_9^4+2\zeta_9^3-2\zeta_9^2-2,\ 2\zeta_9^5+\zeta_9^4-2\zeta_9^3+2\zeta_9-4,\\
&\zeta_9^5-2\zeta_9^2,\ 3\zeta_9^4+2\zeta_9,\ \zeta_9^4,\ \zeta_9^5,\ -\zeta_9^4-3\zeta_9,\ 2\zeta_9^5+3\zeta_9^2,\ \zeta_9^4-2\zeta_9^3+2\zeta_9^2-\zeta_9-4,\\
&2\zeta_9^5-2\zeta_9^4+2\zeta_9^3+\zeta_9^2-2\zeta_9-2,\ \zeta_9^5-2\zeta_9^3-\zeta_9^2-2\zeta_9+2,\ 2\zeta_9^5+2\zeta_9^4+2\zeta_9^3+2\zeta_9^2+\zeta_9+4,\ 2\zeta_9^4-\zeta_9,\\
&3\zeta_9^5+\zeta_9^2,\ -2\zeta_9^5-2\zeta_9^4-2\zeta_9^3-2\zeta_9^2-\zeta_9-4,\ -\zeta_9^5+2\zeta_9^3+\zeta_9^2+2\zeta_9-2,\ -3\zeta_9^5-\zeta_9^2,\ -2\zeta_9^4+\zeta_9,\ -\zeta_9^5,\ -\zeta_9^4.
\end{aligned}
$$

To prove Proposition 114, we will find all integral points on C_η for some $\eta \in T$. Then we will apply Lemma 112 to find the integral points of $C_{\eta'}$ for all other $\eta' \in T$.

Let $\eta = \zeta_9 + \zeta_9^{-1}$. Then C_η is the curve defined by the polynomial

$$f_\eta(x,y) = x^3 - 3xy^2 - y^3 - 6x^2 - 3xy + 9x + 3y - 4.$$

Lemma 115. *Let* C_η *be the plane curve defined above. Then*

$$C_\eta(\mathbb{Z}) = \{(22,-63),(1,0),(1,-3),(-2,6),(7,-3),(4,0),(-2,-3),(43,21),(-2,3),(-62,42)\}.$$

Proof. Our proof follows the argument of [39, Thm. D.8.4]. The main difference is that we will reduce the problem of finding integral points to solving a unit equation in $\mathcal{O}_K$ instead of a more general S-unit equation.

First we want to find a parameterization $\varphi : \mathbb{P}^1 \to C_\eta$. Note that C_η has a unique singular point $Q = (1 : 0 : 1)$. Every line L through Q intersects C_η at a unique point P. There is a bijection between the set of lines through Q and $\mathbb{P}^1$. This map is given by

$$\varphi(u, v) = (\varphi_x, \varphi_y, \varphi_z) = \left(u^3 - 3uv^2 + 4v^3, -3\left(u^3 - u^2v + uv^2\right), u^3 - 3u^2v + v^3\right).$$

The inverse is

$$\psi(x, y, z) = (\psi_u, \psi_v) = (y, z - x).$$

Over K, φ_y and φ_z factor as

$$\varphi_y = -3\prod_{i=1}^{3} u - \alpha_i v, \quad \varphi_z = \prod_{i=1}^{3} u - \beta_i v$$

where $\alpha_i, \beta_i \in \mathcal{O}_K$ and are all distinct.

Suppose that $(u, v) \in \mathbb{P}^1$ is such that $\varphi(u, v) \in C_\eta(\mathbb{Z})$, i.e. $\varphi_x(u, v)/\varphi_z(u, v)$ and $\varphi_y(u, v)/\varphi_z(u, v)$ lie in $\mathbb{Z}$. We may assume that $u, v \in \mathcal{O}_K$ and are coprime. Note that 3 is totally ramified in K, so there is a unique prime of K lying over 3 which is generated by some $\nu \in \mathcal{O}_K$. Let S be the set containing only this prime. Next we will show that $u - \beta_j v$ is an S-unit. Note that

$$\gcd\left(u - \alpha_i v, u - \beta_j v\right) \mid (\alpha_i - \beta_j) \gcd\left(u, v\right) = \alpha_i - \beta_j.$$

A short computation shows that $\mathrm{Norm}_{K/\mathbb{Q}}(\alpha_i - \beta_j) \in \{1, 9\}$, in particular, they are S-units. By hypothesis,

$$\frac{-3\prod u - \alpha_i v}{\prod u - \beta_j v} = \frac{\varphi_y(u, v)}{\varphi_z(u, v)} \in \mathbb{Z}.$$

By the above, the denominator is relatively prime to the numerator at all primes outside of S. Because the quotient is integral, this implies that the $u - \beta_j v$ are S-units.

Next we claim that $\mathrm{ord}_\nu(u - \beta_j v) \leq 12$ for every j. Note that since $\varphi_y(u, v)/\varphi_z(u, v) \in \mathbb{Z}$, it follows that

$$\sum_j \mathrm{ord}_\nu\left(u - \beta_j v\right) \leq 6 + \sum_i \mathrm{ord}_\nu\left(u - \alpha_i v\right).$$

Moreover, above we saw that for any fixed i, j, we have that $\gcd(u - \alpha_i v, u - \beta_j v) \mid \alpha_i - \beta_j$. A straightforward computation shows that $\max_{i,j}\{\mathrm{ord}_\nu(\alpha_i - \beta_j)\} = 2$, so

$$\min\{\mathrm{ord}_\nu(u - \alpha_i v), \mathrm{ord}_\nu(u - \beta_j v)\} \leq 2.$$

So if $\mathrm{ord}_\nu(u - \beta_j v) > 12$, then by the first inequality, there is some i such that $\mathrm{ord}_\nu(u - \alpha_i v) > 2$, but this contradicts the second inequality.

Now we will show how finding integral points on C_η reduces to solving a unit equation. Let $A = (\beta_2 - \beta_3)/(\beta_2 - \beta_1)$ and $B = (\beta_3 - \beta_1)/(\beta_2 - \beta_1)$. One can show that A, B are units in $\mathcal{O}_K^\times$. Then

$$A\frac{u - \beta_1 v}{u - \beta_3 v} + B\frac{u - \beta_2 v}{u - \beta_3 v} = 1.$$

This is sometimes called Siegel's identity. By the above, each summand in this equation is an S-unit whose valuation at ν is bounded between -12 and 12.

Therefore, we are looking for solutions $X, Y \in \mathcal{O}_{K,S}^\times$ to the S-unit equation

$$X + Y = 1.$$

Given such a solution, we can solve for u, v using the equations

$$X = A\frac{u - \beta_1 v}{u - \beta_3 v}, \quad Y = B\frac{u - \beta_2 v}{u - \beta_3 v}.$$

At this moment, we do not know of a widely available and refereed implementation of an S-unit equation solver over number fields for arbitrary sets S of primes[3]. However, because of the bounds on $\mathrm{ord}_\nu(u - \beta_j v)$, it suffices to find solutions $X, Y \in \mathcal{O}_K^\times$ to the unit equation

$$\nu^i X + \nu^j Y = 1$$

for all pairs i, j with $-12 \leq i, j \leq 12$. Using `Magma`, we found the 10 integral points on C_η listed in the statement. □

[3]One is currently being written for `Sage`, see https://trac.sagemath.org/ticket/22148.

Outline of the Proof of Proposition 114. The proof is computational, so we only outline the steps. For each $\eta' \in T$, we computed the transformation between C_η and $C_{\eta'}$ given in the proof of Lemma 112. By applying these transformations to the points given in Lemma 115, we obtained $C_{\eta'}(\mathbb{Z})$ for all η'. Finally, we used the method outlined in the proof of Proposition 110 to find all Weil generators associated to the integral points of $C_{\eta'}$. □

4.6.2 An Example of Genus 1

Suppose that C_η has genus 1. By construction, C_η contains the F-rational point $(-\eta : 1 : 0)$. Therefore C_η is isomorphic (over F) to an elliptic curve. If the rank of this curve is 0, then we can provably find all Weil generators in K by finding the torsion points of C_η.

Example 116. Let $K = \mathbb{Q}(\beta)$ where β is a root of $x^6 - x^5 + 3x^4 + 5x^2 - 2x + 1$. Let η be a root of $x^3 + x^2 - 2x - 1$ in the maximal totally real subfield F of K. Then C_η is given by the polynomial

$$f_\eta = x^3 + x^2y - 2xy^2 - y^3 - 5x^2 - xy + y^2 + 6x + 2y - 28.$$

Over F, C_η is isomorphic to the elliptic curve E given by the Weirstrass equation

$$y^2 + xy + y = x^3 + 611x + 6416.$$

We used `Sage` to compute that E/F has rank 0. The torsion group $E(F)$ consists of the points $\{(0 : 1 : 0), (4 : 92 : 1), (4 : -97 : 1)\}$. In this case, F is Galois and the images of $E(F)$ in C_η are the points at infinity, i.e. $(-\sigma(\eta) : 1 : 0)$ for each $\sigma \in \mathrm{Gal}(F/\mathbb{Q})$. Therefore $C_\eta(\mathbb{Z}) = \emptyset$. By Lemma 112, the same holds for any $\eta' \in F$ such that $\mathcal{O}_F = \mathbb{Z}[\eta']$, hence K has no Weil generators.

4.6.3 General Bounds for the Genus 1 *Case*

While there are general methods for finding integral points on genus 1 curves [83], they usually require a point of $C_\eta(\mathbb{Q})$ or a basis for the Mordell-Weil group over F. However, we

can give an upper bound on the height of any Weil generator for K using the main result in [3]. This in turn can be used to bound $\#W$. In this section, we will compute this bound explicitly.

Recall from the proof of Proposition 110 that any Weil generator α corresponds to a point on C_η as follows. We write $\alpha = \Omega + a/2$ where $\Omega = (u(\gamma - \overline{\gamma}) + \eta)/2$ and $\eta \in T$, $u \in \mathcal{O}_F^\times$, and $a \in \mathbb{Z}$. Then $4\Omega\overline{\Omega} = (\eta^2 + u^2\delta) = A + B\eta$ and $(A, B) \in C_\eta(\mathbb{Z})$.

Because $\alpha\overline{\alpha} = \Omega\overline{\Omega} + a\eta/2 + a^2/4 \in \mathbb{Z}$, we know that $a = -B/2$. So

$$h(\alpha)^2 = \alpha\overline{\alpha} = \frac{A}{4} + \frac{B^2}{16} \leq h(P)^2,$$

where $h(P) = \max(|A|, |B|)$.

Let H_η denote the maximum absolute value of the coefficients of the defining polynomial of some C_η for some η. By a theorem of Baker and Coates [3], if $P = (A, B)$ is an integral point on C_η, then

$$h(P) \leq \exp\exp\exp\left(2H_\eta\right)^{10^{3^{10}}}.$$

Let $\mathcal{H} = \max_{\eta \in T} H_\eta$. Then for any Weil generator $\alpha \in W$,

$$h(\alpha) \leq \exp\exp\exp\left(2\mathcal{H}\right)^{10^{3^{10}}}. \tag{4.7}$$

Remark 117. One can get a better, but still impractical, upper bound on $h(P)$ using the main result in [72].

We can use equation (4.7) to bound the number $\#W$ of Weil generators in K. Because the bound in equation (4.7) is already impractical, we will not try for an optimal bound. Let κ be the number of roots of unity in K. Then there are at most κ Weil generators which generate the same ideal. This is because if two Weil numbers generate the same idea, then they differ by a root of unity. Moreover, $\mathrm{Norm}_{K/\mathbb{Q}}(\alpha) = h(\alpha)^{\deg K}$. So the bound on $h(\alpha)$ gives a bound on $\mathrm{Norm}_{K/\mathbb{Q}}(\alpha\mathcal{O}_K)$. It remains to count the number of ideals in $\mathcal{O}_K$ of bounded norm. Let ζ_K denote the Dedekind zeta-function of K. If a_n is the number of ideals of $\mathcal{O}_K$ of norm n, then

$$\sum_{n \leq M} a_n \leq M^2 \sum_{n \leq M} \frac{a_n}{n^2} \leq M^2 \zeta_K(2).$$

Therefore

$$\#W \leq \kappa\zeta_K(2)\left(\exp\exp\exp\left(2\mathcal{H}\right)^{10^{3^{10}}}\right)^{2\deg K}.$$

4.7 Super-Isolated Varieties

In this section we are interested in abelian varieties with the following property.

Definition 118. Let q be a prime power. We say that an abelian variety $A/\mathbb{F}_q$ is *super-isolated* if its $\mathbb{F}_q$-rational isogeny class contains no other $\mathbb{F}_q$-isomorphism classes.

The goal of this section is to give examples of super-isolated abelian varieties, as well as to explain their relationship to Weil generators (see Definition 85).

Example 119. There are 5 isomorphism classes of elliptic curves over $\mathbb{F}_2$, and they are given in Table 4.2. Recall that two elliptic curves over a finite field are isogeneous if and only if they share the same number of points. Because each curve in Table 4.2 has a different number of points, they lie in distinct isogeny classes. Hence they are all super-isolated.

E	$\#E(\mathbb{F}_2)$
$y^2+y=x^3$	3
$y^2+y=x^3+x$	5
$y^2+y=x^3+x+1$	1
$y^2+xy=x^3+1$	4
$y^2+xy+y=x^3+1$	2

Table 4.2: Isomorphism classes of elliptic curves over $\mathbb{F}_2$.

First we will explain the connection between super-isolated abelian varieties and Weil generators. A theorem of Honda and Tate says that there is a bijection between conjugacy classes of Weil q-numbers and isogeny classes of simple abelian varieties over $\mathbb{F}_q$, see [90,

Sec. I.6] for references. This bijection works as follows. Let $A/\mathbb{F}_q$ be an abelian variety that is simple over $\mathbb{F}_q$, and let $f(x) \in \mathbb{Z}[x]$ be the characteristic polynomial of the Frobenius endomorphism of A, which has degree $2g$. The Honda-Tate bijection sends the isogeny class of A to the roots of f. Let π be any root of f.

Recall that A is ordinary if π is totally imaginary and $(\pi + q/\pi, q) = 1$ [89, Ch. 7]. In this case, $K = \mathbb{Q}(\pi)$ is a CM field of degree $2g$ (see [89, Thm. 7.2] or [85, Thm. 2]). Theorem 121 below shows that if A is ordinary then A is super-isolated if and only if π is a Weil generator for K and K has class number 1. Example 131 below shows that without the ordinary hypothesis, it is possible for A to be super-isolated and π to not be a Weil generator.

Remark 120. If A is not ordinary, then $f(x)$ may not be irreducible. For example, by [56, Thm. 2.9], $f(x) = (x^2 - 5)^2$ is the characteristic polynomial of the Frobenius endomorphism of a simple abelian surface over $\mathbb{F}_5$.

Theorem 121. *Suppose that A is a simple ordinary abelian variety over $\mathbb{F}_q$. Let π denote a root of the characteristic polynomial of the Frobenius endomorphism of A and $K = \mathbb{Q}(\pi)$. Then A is super-isolated if and only if π is a Weil generator for K and K has class number 1.*

Proof. By [89, Thm. 7.4], the set of endomorphism rings that appear in the isogeny class of A are precisely the orders in K containing $\mathbb{Z}[\pi, \overline{\pi}]$. So there is one endomorphism ring if and only if $\mathbb{Z}[\pi, \overline{\pi}] = \mathcal{O}_K$. The result then follows from [89, Thm. 7.2], which says that the isomorphism classes of abelian varieties in the isogeny class of A whose endomorphism ring is isomorphic to $\mathcal{O}_K$ form a principal homogeneous space for the class group of K. In particular, there is one isomorphism class with endomorphism ring $\mathcal{O}_K$ if and only if K has class number 1. □

Example 122. Let C be the hyperelliptic curve given by $y^2 = x^5 + 4$ over the field $\mathbb{F}_{11}$. The zeta-function $Z(C, t)$ of C is given by

$$Z(C, t) = \frac{121t^4 + 121t^3 + 51t^2 + 11t + 1}{11t^2 - 12t + 1}.$$

Recall that the reverse of the numerator of $Z(C,t)$ is the characteristic polynomial $f(x)$ of the Frobenius endomorphism of the Jacobian J of C [19, Ch. 5.2]. In this case

$$f(x) = x^4 + 11x^3 + 51x^2 + 121x + 121.$$

Because f is irreducible, J is a simple abelian surface. Let π be a root of $f(x)$. A straightforward calculation shows that π is a Weil generator for $K = \mathbb{Q}(\zeta_5)$ and that $\pi + 11/\pi$ is coprime to 11. Therefore J is super-isolated by Theorem 121.

The following is a straightforward corollary of Theorem 121 and Theorem 102.

Corollary 123. *Let $g \geq 3$. There are finitely many super-isolated simple ordinary abelian varieties of dimension g.*

Proof. Let A be a super-isolated simple ordinary abelian variety over a finite field of dimension $g \geq 3$, and let π be a root of the characteristic polynomial of the Frobenius endomorphism of A. By Theorem 121, π is a Weil generator for $K = \mathbb{Q}(\pi)$, which is a CM field of degree $2g$ and class number 1. The Honda-Tate theorem says that the map sending the isogeny class of A (which, because A is super-isolated, is equivalent to the isomorphism class of A) to the conjugacy class of π is injective. Therefore, it is sufficient to count the number of Weil generators in CM fields of degree $2g$ with class number 1. Theorem 125 says that the number of such fields is finite, and Theorem 102 says that the number of Weil generators in each such field is finite. □

Remark 124. If a conjecture of Stark holds, then we do not need to fix g in Corollary 123, see Remark 126 below.

4.7.1 CM Fields With Class Number 1

In this section we will review some of the known results on CM fields with class number 1. These fields are important for finding super-isolated abelian varieties.

An important conjecture by Gauss was that there are 9 quadratic imaginary fields with class number 1 [36]. This was eventually proven simultaneously by Stark and Baker [2, 81].

Moreover, the following theorem of Stark from 1974 shows that the number of CM fields with class number 1 is finite in any degree.

Theorem 125 ([82])**.** *There is a finite number of CM fields with class number* 1 *with a fixed degree.*

Remark 126. It is believed that there is a finite number of CM fields with class number 1 [82].

It is an important problem in number theory to find all CM fields of class number 1 in each degree. For small values of g, all CM fields with class number 1 and degree $2g$ can now be found in the literature. A brief summary of results is given in Table 4.3.

Degree	# of CM fields with class number 1	Reference
2	9	[2, 81]
4	Galois: 54	[75]
	Non-Galois: 37	[54]
6	Galois: 17	[53, 91]
	Non-Galois: 386	[11, 12]

Table 4.3: Summary of the class number 1 problem for CM fields of degree ≤ 6.

Recall that a necessary condition for a CM field K to contain a Weil generator is that $\mathcal{O}_K$ is a free $\mathcal{O}_F$-module. This condition was used in Example 90 to show that $\mathbb{Q}(\sqrt{60}, \sqrt{-2})$ has no Weil generators. However. this condition is always satisfied when K has class number 1 because in that case F also has class number 1 [88, Prop. 4.11]. Hence $\mathcal{O}_F$ is a PID, so by the structure theorem for modules over a PID, $\mathcal{O}_K$ is a free $\mathcal{O}_F$-module.

4.7.2 Examples of Super-Isolated Elliptic Curves

In this section we will give examples of super-isolated elliptic curves, as well as extend Theorem 121 to include the case of supersingular curves.

In [73], Schoof gave a formula for size of the isogeny class of an elliptic curve $E/\mathbb{F}_q$ in terms of $\#E(\mathbb{F}_q)$ and q. The following is a straightforward consequence of that formula.

Proposition 127. *Let $q = p^a$ be a prime power, E be an elliptic curve over $\mathbb{F}_q$, and $t = q + 1 - \#E(\mathbb{F}_q)$. Then $E/\mathbb{F}_q$ is super-isolated if and only if one of the following holds:*

(i) $t \not\equiv 0 \mod p$ *and* $t^2 - 4q \in \{-3, -4, -7, -8, -11, -19, -43, -67, -163\}$.

(ii) $p \in \{2, 3, 5, 7, 13\}$, *and* $t^2 = 4q$.

(iii) $p \in \{2, 3\}$, *and* $t^2 = p^{a+1}$.

(iv) $p = 2$ *and* $t = 0$.

(v) $p = 3$ *and* $t^2 = q$.

Proof. Case (i) corresponds to ordinary elliptic curves and follows from Theorem 121. The set of values for $t^2 - 4q$ are the discriminants of the imaginary quadratic fields with class number 1, see Table 4.3 for references. The rest of the cases follow directly from a special case of [73, Thm. 4.6]. □

Table 4.4 gives examples of curves satisfying each case in Proposition 127.

Case	E	q	t
(i)	$y^2 = x^3 + 4$	7	5
(ii)	$y^2 + y = x^3$	4	-4
(iii)	$y^2 + y = x^3 + x + 1$	2	2
(iv)	$y^2 + y = x^3$	2	0
(v)	$y^2 = x^3 - x + \beta$	9	3

Table 4.4: Examples of super-isolated elliptic curves. Here $\beta \in \mathbb{F}_9$ satisfies $x^2 - x - 1$.

Recall that the property of being super-isolated depends on the base field (see Definition 118). It is often the case that a variety may be super-isolated over $\mathbb{F}_q$, but not over an extension of $\mathbb{F}_q$.

Example 128. Let $E/\mathbb{F}_7$ be the elliptic curve defined by $y^2 = x^3+4$. Note that $\#E(\mathbb{F}_7) = 3$, so E is super-isolated by Proposition 127. However, over the extension field $\mathbb{F}_{49}$, E is isogeneous, but not isomorphic, to the curve given by $y^2 = x^3 + 6\beta x + 4$, where $\beta \in \mathbb{F}_{49}$ is a root of $x^2 + 6x + 3$. Therefore $E/\mathbb{F}_7$ is super-isolated but $E/\mathbb{F}_{49}$ is not.

It is possible for an abelian variety that is not super-isolated over the base field to become super-isolated over an extension field. For elliptic curves, this phenomenon can only occur for supersingular curves. To see why, let $E/\mathbb{F}_q$ be an ordinary elliptic curve and suppose that $E/\mathbb{F}_{q^k}$ is super-isolated for some extension field $\mathbb{F}_{q^k}$. Then any curve $E'/\mathbb{F}_q$ which is isogeneous to $E/\mathbb{F}_q$ must become isomorphic to E over $\mathbb{F}_{q^k}$. This means that $E'/\mathbb{F}_q$ is a twist of $E/\mathbb{F}_q$ (see [78, Ch. X.5]). One can show that for ordinary curves, non-trivial twists are never isogeneous (here a non-trivial twist is one that is not isomorphic over the base field). For example, if $E'/\mathbb{F}_q$ is a quadratic twist of $E/\mathbb{F}_q$, and $t = p + 1 - \#E(\mathbb{F}_q)$, then $\#E'(\mathbb{F}_q) = p + 1 + t$. Since E is ordinary, $t \neq 0$ so E' lies in a different isogeny class (see also [89, Pg. 542]).

Example 129. Let $E/\mathbb{F}_5$ be the supersingular elliptic curve given by $y^2 = x^3 + 2$. Then E is isogeneous, but not isomorphic, to the curve $E'/\mathbb{F}_5$ given by $y^2 = x^3 + 1$. However, by applying Proposition 127, one can check that $E/\mathbb{F}_{25}$ is super-isolated. In this case, $E/\mathbb{F}_5$ and $E'/\mathbb{F}_5$ become isomorphic over $\mathbb{F}_{25}$.

Another possibility is that a super-isolated variety could stay super-isolated in every extension.

Example 130. Let $E/\mathbb{F}_2$ be the curve given by $y^2 + y = x^3$. In this case, one can compute

(see [78, Ex. 5.13]) that

$$t(E/\mathbb{F}_{2^a}) = \begin{cases} 0 & a \text{ odd} \\ 2(-2)^{a/2} & a \text{ even.} \end{cases}$$

By Proposition 127, this shows that $E/\mathbb{F}_{2^a}$ is super-isolated for every $a \geq 1$.

The following example shows that if E is supersingular, then it is possible that E is super-isolated but the Frobenius endomorphism does not correspond to a Weil generator.

Example 131. Let $E/\mathbb{F}_9$ be the supersingular elliptic curve in the last row of Table 4.4. The characteristic polynomial $f(x)$ of the Frobenius endomorphism of E is $f(x) = x^2 - 3x + 9$. Let π be a root of $f(x)$ and $K = \mathbb{Q}(\pi)$. The discriminant of $f(x)$ is -27, so $\mathbb{Z}[\pi]$ has index 3 in $\mathcal{O}_K$. In particular, π is not a Weil generator for K. This shows that the ordinary hypothesis in Theorem 121 is necessary.

One way to construct super-isolated elliptic curves over large prime fields is to use the *complex-multiplication (CM) method*. A detailed summary of the CM method can be found in [19, Ch. 18]. Essentially, using the CM method to generate super-isolated curves works as follows:

1. Choose a quadratic imaginary field K with class number 1.

2. Find an elliptic curve $E/\mathbb{C}$ whose endomorphism ring is isomorphic to $\mathcal{O}_K$.

3. Choose a Weil generator π (with non-zero trace) for K such that $p = \pi\overline{\pi}$ is prime and is ≥ 5. This will ensure that the resulting curve is ordinary.

4. Find a twist of the reduction $E/\mathbb{F}_p$ whose Frobenius endomorphism corresponds to π.

If also the only roots of unity in K are ± 1, then we can always use E as opposed to one of its twists. To see why, recall that in this case there is only a single twist of E: the quadratic twist. If E has $p + 1 - \text{Trace}_{K/\mathbb{Q}}(\pi)$ points, then the quadratic twist of E has

$p + 1 + \text{Trace}_{K/\mathbb{Q}}(\pi)$. It follows from Proposition 127 that if one of them is isolated, then they both are.

Example 132. Let $K = \mathbb{Q}(\sqrt{-2})$. The endomorphism ring (over $\mathbb{C}$) of the elliptic curve $E/\mathbb{Q}$ given by $y^2 = x^3 - x^2 - 3x - 1$ is isomorphic to $\mathcal{O}_K$. Recall that every Weil generator for K is of the form $\pi = b \pm \sqrt{-2}$ for some integer b. Thus searching for primes p such that $E/\mathbb{F}_p$ is super-isolated reduces to finding values of b such that $p = b^2 + 2$ is prime. After a short search, we found that $b = 105, 10041, 1000017, 100000017, 10000000185$ all have the property that $b^2 + 2$ is prime.

The CM method described above can also be used to generate curves with useful properties, such as prime order and a base field with low hamming weight.

Example 133. Let $\pi = 2^{127} + 2^{25} + 2^{12} + 2^6 + (1 - \sqrt{-3})/2$. Then $p = \pi\overline{\pi}$ is a 255 bit prime with Hamming weight 14. Using the CM method, we found a super-isolated curve $E/\mathbb{F}_p$ given by $y^2 = x^3 + 19$ that has $\#E(\mathbb{F}_p) = (\pi - 1)(\overline{\pi} - 1)$ points, which is also prime.

4.7.3 Examples in Higher Dimensions

In this section we will give examples of super-isolated abelian varieties in dimension $g \geq 2$. One way to construct these varieties is to fix a prime p and randomly choose curves over $\mathbb{F}_p$ until the Jacobian is super-isolated. We can check if the Jacobian J of a curve $C/\mathbb{F}_p$ is super-isolated using the zeta-function of C as in Example 122. Some examples of curves found this way are given in Table 4.5. Because super-isolated abelian varieties are rare, this method of search is impractical when p is large.

Another way to construct super-isolated abelian varieties is described in Example 134. This method is based on a generalization of the CM method to higher dimensions, see [19, Ch. 18].

Example 134. Let $\pi \in K = \mathbb{Q}(\zeta_5)$ be a totally imaginary Weil p-number such that p splits in K. Let $C/\mathbb{Q}$ be the curve defined by $y^2 = x^5 - 1$. The endomorphism ring over $\mathbb{C}$ of the

Curve	Genus	Field
$y^2 = x^3 + 5x^2 + x + 1$	1	$\mathbb{F}_7$
$y^2 = x^5 + 2x^4 + 4x^3 + x^2 + x + 4$	2	$\mathbb{F}_5$
$y^2 = x^7 + x^5 + x + 2$	3	$\mathbb{F}_3$
$y^2 + (x^5 + x^3 + 1)y = x^9 + x^6$	4	$\mathbb{F}_2$

Table 4.5: Examples of hyperelliptic curves with super-isolated Jacobians.

Jacobian J of C is isomorphic to $\mathcal{O}_K$. This means that there is a twist $C'/\mathbb{F}_p$ of $C/\mathbb{F}_p$ such that the Frobenius endomorphism of the Jacobian of C' satisfies the minimal polynomial of π. If π is also a Weil generator for K, then the resulting surface will be super-isolated. For example, $\pi = 45\zeta_5^3 - 10\zeta_5^2 + 34\zeta_5 - 2320$ is a Weil generator for K with $p = \pi\overline{\pi} = 5465351$ prime. In this case, the Jacobian of the curve $y^2 = x^5 - 4$ over $\mathbb{F}_p$ is super-isolated.

The CM method is difficult for genus $g > 5$ or fields K of large discriminant or degree. The main difficulty is writing down an appropriate global variety $A/\mathbb{C}$. See [4] for a construction in dimension 3. Moreover, for $g \geq 3$, Theorem 102 suggests that there are few super-isolated abelian varieties of dimension g.

It is sometimes possible to use properties of the field K to construct slightly larger examples than we could find by randomly searching through curves.

Example 135. Suppose that K is a sextic CM field with class number 1 that contains $\sqrt{-1}$, and suppose that $C/\mathbb{F}_p$ is a curve of genus 3 whose Jacobian has an endomorphism ring isomorphic to $\mathcal{O}_K$. Then it follows from [19, Cor. 18.17] that C is isomorphic to a curve of the form $y^2 = x^7 + x^5 + ax^3 + bx$ for some $a, b \in \mathbb{F}_p$. This means that we can search for a super-isolated abelian threefold by first finding a Weil generator π for K such that $p = \pi\overline{\pi}$ is prime. Then we can range over all pairs $(a, b) \in (\mathbb{F}_p)^2$ and check if the Jacobian of the resulting curve is super-isolated. We used this method to find the curve $y^2 = x^7 + x^5 + 160x^3 + 79x$ over the field $\mathbb{F}_{353}$. The characteristic polynomial $f(x)$ of the

Frobenius endomorphism of the Jacobian J of this curve is

$$x^6 - 88x^5 + 3440x^4 - 80400x^3 + 1214320x^2 - 10965592x + 43986977.$$

The roots of this polynomial are Weil generators for the field generated by the root π of f (which is a sextic CM field with class number 1); hence J is a super-isolated abelian threefold.

BIBLIOGRAPHY

[1] Leonard M. Adleman, Jonathan DeMarrais, and Ming-Deh Huang. A subexponential algorithm for discrete logarithms over hyperelliptic curves of large genus over GF(q). *Theoret. Comput. Sci.*, 226(1-2):7–18, 1999.

[2] A. Baker. Linear forms in the logarithms of algebraic numbers. I, II, III. *Mathematika 13 (1966), 204-216; ibid. 14 (1967), 102-107; ibid.*, 14:220–228, 1967.

[3] A. Baker and J. Coates. Integer points on curves of genus 1. *Proc. Cambridge Philos. Soc.*, 67:595–602, 1970.

[4] Jennifer S. Balakrishnan, Sorina Ionica, Kristin Lauter, and Christelle Vincent. Constructing genus-3 hyperelliptic Jacobians with CM. *LMS J. Comput. Math.*, 19(suppl. A):283–300, 2016.

[5] R. Balasubramanian and Neal Koblitz. The improbability that an elliptic curve has subexponential discrete log problem under the Menezes-Okamoto-Vanstone algorithm. *J. Cryptology*, 11(2):141–145, 1998.

[6] Paul T. Bateman and Roger A. Horn. A heuristic asymptotic formula concerning the distribution of prime numbers. *Math. Comp.*, 16:363–367, 1962.

[7] Daniel J. Bernstein, Chitchanok Chuengsatiansup, Tanja Lange, and Peter Schwabe. Kummer strikes back: new DH speed records. In Palash Sarkar and Tetsu Iwata, editors, *Advances in cryptology—ASIACRYPT 2014. Part I*, volume 8873 of *Lecture Notes in Comput. Sci.*, pages 317–337. Springer, Heidelberg, 2014.

[8] Daniel J. Bernstein and Tanja Lange. SafeCurves: choosing safe curves for elliptic-curve cryptography. https://safecurves.cr.yp.to/, accessed 10 April 2018.

[9] Joppe W Bos, Craig Costello, Patrick Longa, and Michael Naehrig. Selecting elliptic curves for cryptography: An efficiency and security analysis. *J. Cryptographic Engineering*, 6(4):259–286, 2016.

[10] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[11] Gérard Boutteaux and Stéphane Louboutin. The class number one problem for some non-normal sextic CM-fields. In *Analytic number theory (Beijing/Kyoto, 1999)*, volume 6 of *Dev. Math.*, pages 27–37. Kluwer Acad. Publ., Dordrecht, 2002.

[12] Gérard Boutteaux and Stéphane Louboutin. The class number one problem for the non-normal sextic CM-fields. II. *Acta Math. Inform. Univ. Ostraviensis*, 10(1):3–23, 2002.

[13] Reinier Bröker, Denis Charles, and Kristin Lauter. Evaluating large degree isogenies and applications to pairing based cryptography. In *Pairing-based cryptography—Pairing 2008*, volume 5209 of *LNCS*, pages 100–112. Springer, Berlin, 2008.

[14] Reinier Bröker, Kristin Lauter, and Andrew V. Sutherland. Modular polynomials via isogeny volcanoes. *Math. Comp.*, 81(278):1201–1231, 2012.

[15] Daniel R. Brown. SEC 2: Recommended Elliptic Curve Domain Parameters, Jan 27 2010. Available at http://www.secg.org/sec2-v2.pdf.

[16] Paul-Jean Cahen and Jean-Luc Chabert. *Integer-valued polynomials*, volume 48 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 1997.

[17] Henri Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, 1993.

[18] Henri Cohen. *Advanced topics in computational number theory*, volume 193 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000.

[19] Henri Cohen, Gerhard Frey, Roberto Avanzi, Christophe Doche, Tanja Lange, Kim Nguyen, and Frederik Vercauteren, editors. *Handbook of elliptic and hyperelliptic curve cryptography*. Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, 2006.

[20] Alina Carmen Cojocaru and Igor E. Shparlinski. On the embedding degree of reductions of an elliptic curve. *Inform. Process. Lett.*, 109(13):652–654, 2009.

[21] David A. Cox. *Primes of the form x^2+ny^2*. Pure and Applied Mathematics (Hoboken). John Wiley & Sons, Inc., Hoboken, NJ, second edition, 2013. Fermat, class field theory, and complex multiplication.

[22] Claus Diem and Emmanuel Thomé. Index calculus in class groups of non-hyperelliptic curves of genus three. *J. Cryptology*, 21(4):593–611, 2008.

[23] Andreas Enge. Computing discrete logarithms in high-genus hyperelliptic Jacobians in provably subexponential time. *Math. Comp.*, 71(238):729–742, 2002.

[24] Alexei Entin. On the Bateman-Horn conjecture for polynomials over large finite fields. *Compos. Math.*, 152(12):2525–2544, 2016.

[25] Etienne Fouvry and Henryk Iwaniec. Gaussian primes. *Acta Arith.*, 79(3):249–287, 1997.

[26] Gerhard Frey and Herbert Gangl. How to disguise an elliptic curve (Weil descent). *Talk at ECC*, 98, September 1998.

[27] Gerhard Frey, Michael Müller, and Hans-Georg Rück. The Tate pairing and the discrete logarithm applied to elliptic curve cryptosystems. *IEEE Trans. Inform. Theory*, 45(5):1717–1719, 1999.

[28] John Friedlander and Andrew Granville. Limitations to the equi-distribution of primes. IV. *Proc. Roy. Soc. London Ser. A*, 435(1893):197–204, 1991.

[29] John Friedlander and Henryk Iwaniec. Using a parity-sensitive sieve to count prime values of a polynomial. *Proc. Nat. Acad. Sci. U.S.A.*, 94(4):1054–1058, 1997.

[30] John Friedlander and Henryk Iwaniec. *Opera de cribro*, volume 57 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, RI, 2010.

[31] Steven D. Galbraith and Nigel P. Smart. A cryptographic application of Weil descent. In *Cryptography and coding (Cirencester, 1999)*, volume 1746 of *LNCS*, pages 191–200. Springer, Berlin, 1999.

[32] P. Gaudry. Fast genus 2 arithmetic based on theta functions. *J. Math. Cryptol.*, 1(3):243–265, 2007.

[33] P. Gaudry, F. Hess, and N. P. Smart. Constructive and destructive facets of Weil descent on elliptic curves. *J. Cryptology*, 15(1):19–46, 2002.

[34] P. Gaudry, E. Thomé, N. Thériault, and C. Diem. A double large prime variation for small genus hyperelliptic index calculus. *Math. Comp.*, 76(257):475–492, 2007.

[35] Pierrick Gaudry. An algorithm for solving the discrete log problem on hyperelliptic curves. In Bart Preneel, editor, *Advances in cryptology—EUROCRYPT 2000 (Bruges)*, volume 1807 of *LNCS*, pages 19–34. Springer, Berlin, 2000.

[36] Carl Friedrich Gauss. *Disquisitiones arithmeticae*. Translated into English by Arthur A. Clarke, S. J. Yale University Press, New Haven, Conn.-London, 1966.

[37] K. Györy. Sur les polynômes à coefficients entiers et de discriminant donné. III. *Publ. Math. Debrecen*, 23(1-2):141–165, 1976.

[38] F. Hess. Generalising the GHS attack on the elliptic curve discrete logarithm problem. *LMS J. Comput. Math.*, 7:167–192, 2004.

[39] Marc Hindry and Joseph H. Silverman. *Diophantine geometry: An Introduction*, volume 201 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000.

[40] Taira Honda. Isogeny classes of abelian varieties over finite fields. *J. Math. Soc. Japan*, 20:83–95, 1968.

[41] David Jao, Stephen D. Miller, and Ramarathnam Venkatesan. Do all elliptic curves of the same order have the same difficulty of discrete log? In *Advances in cryptology—ASIACRYPT 2005*, volume 3788 of *LNCS*, pages 21–40. Springer, Berlin, 2005.

[42] David Jao, Stephen D. Miller, and Ramarathnam Venkatesan. Expander graphs based on GRH with an application to elliptic curve cryptography. *J. Number Theory*, 129(6):1491–1504, 2009.

[43] David Jao and Vladimir Soukharev. A subexponential algorithm for evaluating large degree isogenies. In *Algorithmic number theory*, volume 6197 of *LNCS*, pages 219–233. Springer, Berlin, 2010.

[44] Jonathan Katz and Yehuda Lindell. *Introduction to modern cryptography*. Chapman & Hall/CRC Cryptography and Network Security. CRC Press, Boca Raton, FL, second edition, 2015.

[45] Ann Hibner Koblitz, Neal Koblitz, and Alfred Menezes. Elliptic curve cryptography: the serpentine course of a paradigm shift. *J. Number Theory*, 131(5):781–814, 2011.

[46] Neal Koblitz. Elliptic curve cryptosystems. *Math. Comp.*, 48(177):203–209, 1987.

[47] Neal Koblitz. Hyperelliptic cryptosystems. *J. Cryptology*, 1(3):139–150, 1989.

[48] Neal Koblitz and Alfred Menezes. The brave new world of bodacious assumptions in cryptography. *Notices Amer. Math. Soc.*, 57(3):357–365, 2010.

[49] Neal Koblitz and Alfred Menezes. Intractable problems in cryptography. In *Finite fields: theory and applications*, volume 518 of *Contemp. Math.*, pages 279–300. Amer. Math. Soc., Providence, RI, 2010.

[50] David Kohel. *Endomorphism rings of elliptic curves over finite fields*. PhD thesis, University of California at Berkeley, 1996.

[51] J. C. Lagarias and A. M. Odlyzko. Effective versions of the Chebotarev density theorem. In *Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975)*, pages 409–464. Academic Press, London, 1977.

[52] Manfred Lochter and Johannes Merkle. ECC Brainpool standard curves and curve generation, IETF Internet-Draft, February 18 2010.

[53] Stéphane Louboutin. Minoration au point 1 des fonctions L et détermination des corps sextiques abéliens totalement imaginaires principaux. *Acta Arith.*, 62(2):109–124, 1992.

[54] Stphane Louboutin and Ryotaro Okazaki. Determination of all non-normal quartic CM-fields and of all non-abelian normal octic CM-fields with class number one. *Acta Arith.*, 67(1):47–62, 1994.

[55] Florian Luca, David Jose Mireles, and Igor E. Shparlinski. MOV attack in various subgroups on elliptic curves. *Illinois J. Math.*, 48(3):1041–1052, 2004.

[56] Daniel Maisner and Enric Nart. Abelian surfaces over finite fields as Jacobians. *Experiment. Math.*, 11(3):321–337, 2002. With an appendix by Everett W. Howe.

[57] D.A. Marcus. *Number Fields*. Universitext. Springer New York, 2012.

[58] Alfred Menezes and Edlyn Teske. Cryptographic implications of Hess' generalized GHS attack. *Appl. Algebra Engrg. Comm. Comput.*, 16(6):439–460, 2006.

[59] Alfred Menezes, Edlyn Teske, and Annegret Weng. Weak fields for ECC. In *Topics in cryptology—CT-RSA 2004*, volume 2964 of *LNCS*, pages 366–386. Springer, Berlin, 2004.

[60] Alfred J. Menezes, Tatsuaki Okamoto, and Scott A. Vanstone. Reducing elliptic curve logarithms to logarithms in a finite field. *IEEE Trans. Inform. Theory*, 39(5):1639–1646, 1993.

[61] Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone. *Handbook of applied cryptography*. CRC Press Series on Discrete Mathematics and its Applications. CRC Press, Boca Raton, FL, 1997. With a foreword by Ronald L. Rivest.

[62] Andrea Miele and Arjen K Lenstra. Efficient ephemeral elliptic curve cryptographic keys. In Javier Lopez and Chris J. Mitchell, editors, *Information Security: 18th International Conference, ISC 2015, Trondheim, Norway, September 9-11, 2015, Proceedings*, volume 9290 of *LNCS*, pages 524–547, Cham, 2015. Springer International Publishing.

[63] Stephen D. Miller and Ramarathnam Venkatesan. Spectral analysis of Pollard rho collisions. In *Algorithmic number theory*, volume 4076 of *Lecture Notes in Comput. Sci.*, pages 573–581. Springer, Berlin, 2006.

[64] Victor S. Miller. Use of elliptic curves in cryptography. In *Advances in cryptology—CRYPTO '85 (Santa Barbara, Calif., 1985)*, volume 218 of *Lecture Notes in Comput. Sci.*, pages 417–426. Springer, Berlin, 1986.

[65] National Institute of Standards and Technology. Digital Signature Standard (DSS). Federal Information Processing Standards Publication 186-4, 2013.

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

[67] M. Pandey. On Eisenstein primes. *ArXiv e-prints*, July 2016. https://arxiv.org/abs/1607.00469v3.

[68] Stephen C. Pohlig and Martin E. Hellman. An improved algorithm for computing logarithms over GF(p) and its cryptographic significance. *IEEE Trans. Information Theory*, IT-24(1):106–110, 1978.

[69] Karl Rubin and Alice Silverberg. Choosing the correct elliptic curve in the CM method. *Mathematics of Computation*, 79(269):545–561, 2010.

[70] Takakazu Satoh and Kiyomichi Araki. Fermat quotients and the polynomial time discrete log algorithm for anomalous elliptic curves. *Comment. Math. Univ. St. Paul.*, 47(1):81–92, 1998.

[71] A. Schinzel and W. Sierpiński. Sur certaines hypothèses concernant les nombres premiers. *Acta Arith.*, 4:185–208; erratum 5 (1958), 259, 1958.

[72] Wolfgang M. Schmidt. Integer points on curves of genus 1. *Compositio Math.*, 81(1):33–59, 1992.

[73] René Schoof. Nonsingular plane cubic curves over finite fields. *J. Combin. Theory Ser. A*, 46(2):183–211, 1987.

[74] I. A. Semaev. Evaluation of discrete logarithms in a group of p-torsion points of an elliptic curve in characteristic p. *Math. Comp.*, 67(221):353–356, 1998.

[75] Bennett Setzer. The determination of all imaginary, quartic, abelian number fields with class number 1. *Math. Comp.*, 35(152):1383–1386, 1980.

[76] Victor Shoup. *A computational introduction to number theory and algebra*. Cambridge University Press, Cambridge, second edition, 2009.

[77] Carl L. Siegel. über einige Anwendungen diophantischer Approximationen [reprint of Abhandlungen der Preußischen Akademie der Wissenschaften. Physikalisch-mathematische Klasse 1929, Nr. 1]. In *On some applications of Diophantine approximations*, volume 2 of *Quad./Monogr.*, pages 81–138. Ed. Norm., Pisa, 2014.

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

[79] Nigel P. Smart. The discrete logarithm problem on elliptic curves of trace one. *J. Cryptology*, 12(3):193–196, 1999.

[80] Benjamin Smith. Isogenies and the discrete logarithm problem in Jacobians of genus 3 hyperelliptic curves. *J. Cryptology*, 22(4):505–529, 2009.

[81] H. M. Stark. A complete determination of the complex quadratic fields of class-number one. *Michigan Math. J.*, 14:1–27, 1967.

[82] H. M. Stark. Some effective cases of the Brauer-Siegel theorem. *Invent. Math.*, 23:135–152, 1974.

[83] Roel J. Stroeker and Nikolaos Tzanakis. Computing all integer solutions of a genus 1 equation. *Math. Comp.*, 72(244):1917–1933, 2003.

[84] Andrew V. Sutherland. Isogeny volcanoes. In *ANTS X—Proceedings of the Tenth Algorithmic Number Theory Symposium*, volume 1 of *Open Book Ser.*, pages 507–530. Math. Sci. Publ., Berkeley, CA, 2013.

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

[86] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 7.5)*, 2017. `http://www.sagemath.org`.

[87] Wenhan Wang. *Isolated Curves for Hyperelliptic Curve Cryptography.* PhD thesis, University of Washington, 2012.

[88] Lawrence C. Washington. *Introduction to Cyclotomic Fields.* Graduate Texts in Mathematics. Springer New York, 1997.

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

[90] William C. Waterhouse and J. S. Milne. Abelian varieties over finite fields. In *1969 Number Theory Institute (Proc. Sympos. Pure Math., Vol. XX, State Univ. New York, Stony Brook, N.Y., 1969)*, pages 53–64. Amer. Math. Soc., Providence, R.I., 1971.

[91] Ken Yamamura. The determination of the imaginary abelian number fields with class number one. *Math. Comp.*, 62(206):899–921, 1994.

Appendix A

DETAILS FOR $\mathbb{Q}(\zeta_5)$

In this section, we provide a detailed example of the algorithm in Section 3.3.2, for the field $\mathbb{Q}(\zeta_5)$. We also show how long the algorithm must run in order to enumerate all super-isolated Weil p-numbers with $p \leq 2^{261}$. We will use the notation from Section 3.3.2 and the methods from Section 3.3.2.

Let $K = \mathbb{Q}(\zeta_5)$. Recall that step 2 of the algorithm chooses a basis $\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$ for $\mathcal{O}_K$ such that $\{\alpha_1, \alpha_2\}$ form a basis for $\mathcal{O}_F$ where F is the maximal real subfield of K. In this case, $F = \mathbb{Q}(\sqrt{5})$. We choose

$$\alpha_1 = 1, \quad \alpha_2 = -\zeta_5^3 - \zeta_5^2 + 2, \quad \alpha_3 = -3\zeta_5^2 - 2\zeta_5^2 - 2, \quad \alpha_4 = -2\zeta_5^3 + 3\zeta_5^2 - \zeta_5 - 1.$$

Let ϕ_1, ϕ_2 be the embeddings $K \hookrightarrow \mathbb{C}$ defined by

$$\phi_1(\zeta_5) = e^{2\pi i/5}, \quad \phi_2(\zeta_5) = e^{4\pi i/5}.$$

For reference, $\phi_1(\alpha_2) = \frac{5+\sqrt{5}}{2}$ and $\phi_2(\alpha_2) = \frac{5-\sqrt{5}}{2}$.

Next we compute the polynomials defined in Equations (3.2)-(3.5):

$$\begin{aligned}
f_1 &= 2x_2 + 5x_3 - 2x_4, \\
f_2 &= x_3^2 + 9x_3x_4 + 19x_4^2, \\
P &= x_1^2 + 5x_1x_2 + \frac{15}{2}x_2^2 - \frac{3}{2}x_1x_3 + \frac{5}{2}x_2x_3 + 9x_3^2 - 2x_1x_4 - \frac{15}{2}x_2x_4 + \frac{3}{2}x_3x_4 + \frac{37}{2}x_4^2, \\
P_0 &= x_1x_2 + \frac{5}{2}x_2^2 + \frac{5}{2}x_1x_3 + \frac{11}{2}x_2x_3 - 2x_3^2 - x_1x_4 - \frac{7}{2}x_2x_4 - \frac{7}{2}x_3x_4 - \frac{9}{2}x_4^2.
\end{aligned}$$

The next step is to enumerate all solutions to the equation $f_2(x_3, x_4) = \pm 1$. We do this following the method laid out in step 5.

Write $f_2 = ax_3^2 + bx_3x_4 + cx_4^2$, and then choose a generator γ for the ideal $I = a\mathbb{Z} + ((b + \sqrt{\Delta_F})/2)\mathbb{Z}$. Because in this case $I = \mathcal{O}_F$, we will choose $\gamma = 1$. A fundamental unit for $\mathcal{O}_F$ is

$$\epsilon = -\zeta_5^3 - \zeta_5^2 - 1.$$

Now for each choice of sign and value of i we compute $\sigma = \pm\epsilon^i\gamma$ and write

$$\sigma = a_3 a + a_4 \frac{b + \sqrt{\Delta_F}}{2}$$

as in step 5.3.

The remaining steps of the algorithm are straightforward, so we will skip ahead to compute the bound on i in order to find all super-isolated Weil p-numbers with $p \leq 2^{261}$. We first compute the constants from Section 3.3.2.

Notice that $f_2(a_3, a_4) = \pm 1$ implies that

$$\begin{aligned} a_3 &= \frac{-ba_4 \pm \sqrt{(ba_4)^2 - 4a(ca_4^2 \pm 1)}}{2a} \\ &= \frac{-ba_4 \pm |a_4|\sqrt{\Delta_F \pm 4a/a_4^2}}{2a}. \end{aligned}$$

Therefore we can bound $|a_3|$ from above by

$$\begin{aligned} |a_3| &\leq \frac{|b| + \sqrt{\Delta_F + 4|a|}}{2|a|}|a_4| \\ &= 6|a_4|. \end{aligned}$$

Next we want to bound $|a_4|$ from below by an exponential function in i. Following the proof of Lemma 70,

$$\begin{aligned} \min(|\phi_1(\gamma)|, |\phi_2(\gamma|) \max(|\phi_1(\epsilon)|, |\phi_2(\epsilon)|)^{|i|} &\leq \max\left(|\phi_1(\gamma\epsilon^i)|, |\phi_2(\gamma\epsilon^i)|\right) \\ &\leq |a_3||a| + |a_4|\frac{|b| + \sqrt{\Delta_F}}{2} \\ &= |a_3| + \frac{9 + \sqrt{5}}{2}|a_4| \\ &\leq 6|a_4| + \frac{9 + \sqrt{5}}{2}|a_4| \\ &\leq 12|a_4|. \end{aligned}$$

Since $\gamma = 1$ and $\max(|\phi_1(\epsilon)|, |\phi_2(\epsilon)|) = \frac{1+\sqrt{5}}{2} \geq 3/2$, we have

$$|a_4| \geq \frac{1}{12}\left(\frac{3}{2}\right)^{|i|}.$$

Next we want to bound $P(a_1, a_2, a_3, a_4)$ from below in terms of $|a_4|$. We follow the same steps as in the proof of Lemma 71. For simplicity, we will assume that (a_1, a_2, a_3, a_4) is a solution to Equations (3.14)-(3.16). In our case, these equations are

$$\begin{aligned}
1 &= 2x_2 + 5x_3 - 2x_4, \\
0 &= x_1 + 5x_2^2 + 11x_2x_3 - 4x_3^2 - 7x_2x_4 - 7x_3x_4 - 9x_4^2, \\
x_3 &= \frac{-9 + \sqrt{5 + 4/x_4^2}}{2} x_4.
\end{aligned}$$

Note that integral solutions to these equations exist, for example, $x_1 = 115, x_2 = -45, x_3 = 17, x_4 = -3$. This solution comes from setting $i = 7$.

By solving each of these constraints in terms of x_4, we have

$$\begin{aligned}
x_1 &= \frac{5}{8}\,x_4^2 + \frac{1}{8}\left(5\,x_4^2 + 28\,x_4\right)\sqrt{5 + \frac{4}{x_4^2}} - 33\,x_4 - 1, \\
x_2 &= -\frac{5}{4}\,x_4\sqrt{5 + \frac{4}{x_4^2}} + \frac{49}{4}\,x_4 + \frac{1}{2}, \\
x_3 &= \frac{1}{2}\,x_4\sqrt{5 + \frac{4}{x_4^2}} - \frac{9}{2}\,x_4.
\end{aligned}$$

Substituting these into the polynomial $P(x_1, x_2, x_3, x_4)$ as in the proof of Lemma 71, we have

$$P_4(x_4) = \frac{75}{32}\,x_4^4 + \frac{55}{16}\,x_4^2 + \frac{5}{32}\left(5\,x_4^4 + 4\,x_4^2\right)\sqrt{5 + \frac{4}{x_4^2}} + 1.$$

In particular,

$$P_4(x_4) \geq \frac{75}{32}x_4^4$$

for all $x_4 > 0$.

We saw above that for each integer i, any associated pair (a_3, a_4) (as computed in step 5 of the algorithm in Section 3.3.2) satisfies

$$|a_4| \geq \frac{1}{12}\left(\frac{3}{2}\right)^{|i|}.$$

If the tuple happens to satisfy Equations (3.14)-(3.16), then

$$P(a_1, a_2, a_3, a_4) \geq \frac{75}{32}\left(\frac{1}{12}\left(\frac{3}{2}\right)^{|i|}\right)^4.$$

So in order to capture all super-isolated Weil p-numbers with $p \leq 2^{261}$ which satisfy the constraints above, we have to check all i with $|i| \leq 118$. The bound for other choices of signs in Equations (3.14)-(3.16) can be computed similarly.

VITA

Travis Scholl earned a B.S. from the University of Oregon in 2013, and is expected to earn a Ph.D. from the University of Washington in 2018. His research interests include computational algebraic number theory and elliptic curve cryptography. He has published papers in the Journal of Mathematical Cryptology and Experimental Mathematics. He has also given several research talks at the Center for Communications Research, the University of Pennsylvania, the University of Oregon, and the University of Washington. Travis is also interested in mathematics education, and has taught several math courses at the University of Washington.