Constructing Abelian Varieties for Pairing-Based Cryptography

by

David Stephen Freeman

A.B. (Harvard University) 2002

A dissertation submitted in partial satisfaction of the
requirements for the degree of
Doctor of Philosophy

in

Mathematics

in the

GRADUATE DIVISION
of the
UNIVERSITY OF CALIFORNIA, BERKELEY

Committee in charge:
Professor Kenneth A. Ribet, Co-chair
Professor Edward F. Schaefer, Co-chair
Professor Bjorn Poonen
Professor David A. Wagner

Spring 2008

The dissertation of David Stephen Freeman is approved:

Co-chair Date

Co-chair Date

Date

Date

University of California, Berkeley

Spring 2008

Constructing Abelian Varieties for Pairing-Based Cryptography

Abstract

Constructing Abelian Varieties for Pairing-Based Cryptography

by

David Stephen Freeman
Doctor of Philosophy in Mathematics

University of California, Berkeley

Professor Kenneth A. Ribet and Professor Edward F. Schaefer, Co-chairs

Abelian varieties that have small embedding degree with respect to a large prime-order subgroup are key ingredients for implementing pairing-based cryptographic systems. Such "pairing-friendly" abelian varieties are rare and thus require specific constructions.

We begin by giving a single coherent framework that classifies the known constructions of pairing-friendly ordinary elliptic curves. This abstract framework leads us to discover several new constructions of such curves. Our most important contribution in this regard is the construction of elliptic curves of prime order with embedding degree 10, which solves an open problem posed by Boneh, Lynn, and Shacham. We also describe a procedure for generating families of pairing-friendly elliptic curves with variable CM discriminant, which can be used to increase the degree of randomness in cryptosystem parameters.

We then consider higher-dimensional abelian varieties. We provide two algorithms that, given a CM field K, construct Frobenius elements π of pairing-friendly ordinary abelian varieties with complex multiplication by K. Both algorithms generalize existing constructions of pairing-friendly ordinary elliptic curves. The first generalizes the method of Cocks and Pinch, while the second generalizes that of Brezing and Weng and leads to varieties over smaller fields than the first. Given the output π of either algorithm, one can then use complex multiplication methods to construct explicitly an abelian variety with Frobenius element π.

Finally, we turn to the question of the complex multiplication methods used to construct explicit examples of pairing-friendly abelian varieties. We focus on the Chinese remainder theorem algorithm of Eisenträger and Lauter for computing Igusa class polyno-

mials of quartic CM fields. One of the steps of this algorithm requires determining whether endomorphism rings of Jacobians of genus 2 curves over small prime fields are isomorphic to the ring of integers in a given quartic CM field. We provide an efficient probabilistic algorithm that carries out this computation. Using our algorithm to determine endomorphism rings, we have implemented a probabilistic version of the full Eisenträger-Lauter algorithm in MAGMA and used it to compute Igusa class polynomials for several quartic CM fields K.

For Torrey, my mathematical muse.

Contents

List of Figures

List of Tables

Acknowledgments

My research on pairing-friendly elliptic curves began during a summer internship at Hewlett-Packard Laboratories, Palo Alto, in 2005. I thank Vinay Deolalikar for suggesting this topic and for providing advice and support. I also thank Gadiel Seroussi for bringing me to HP Labs and for supporting my research.

Chapters 2 and 3 include material from [41] and [37], the former of which is joint work with Mike Scott of Dublin City University (Ireland) and Edlyn Teske of the University of Waterloo (Canada), and the latter of which grew out of my work at HP Labs. I thank Paulo Barreto, Florian Hess, Ezekiel Kachisa, Ben Lynn, Michael Naehrig, Igor Shparlinski, Alice Silverberg, and Frederik Vercauteren for helpful discussions and feedback on earlier versions of the material in [41]. I thank Paulo Barreto, Steven Galbraith, and Mike Scott for their valuable feedback on earlier versions of the material in [37]. I am especially indebted to Mike Scott, who used the algorithm presented in Section 3.1 to compute examples of elliptic curves of cryptographic size with embedding degree 10. Two of these curves now appear in this dissertation as Examples 3.1.5 and 3.1.6, and further examples appear in Appendix A.1.

Chapter 4 includes material from [42] and [39], the former of which is joint work with Peter Stevenhagen and Marco Streng of Universiteit Leiden (the Netherlands). The problem of constructing pairing-friendly genus 2 curves was first suggested to me by Kristin Lauter. My initial work on the subject, presented in [38], was inspired by discussions with Dan Boneh and Edward Schaefer in the winter of 2006-07. The material in [42] grew out of a visit to the Centrum voor Wiskunde en Informatica (CWI), Amsterdam, and Universiteit Leiden in the fall of 2007. I thank Ronald Cramer, Peter Stevenhagen, and the DIAMANT project for inviting me to the Netherlands. I thank Tanja Lange, Michael Naehrig, Edward Schaefer, and Marco Streng for helpful feedback on earlier drafts of the material in [39].

Chapter 5 includes material from [40], which is joint work with Kristin Lauter of Microsoft Research (USA). This line of research began as part of an internship at Microsoft Research, Redmond, during the summer of 2006. I thank Microsoft for its hospitality; Denis Charles and Jean-Marc Couveignes for helpful discussions; and Reinier Bröker, David Kohel, and Christophe Ritzenthaler for their feedback on previous versions of [40].

My dissertation research at UC Berkeley has been supported by a National Defense Science and Engineering Graduate Fellowship. I was previously supported by a National

Science Foundation Graduate Research Fellowship. I thank Everett Howe for help with background information on abelian varieties, and Bjorn Poonen for providing detailed and timely responses to a large number of questions.

Special thanks go to Kenneth Ribet and Edward Schaefer, not only for guiding my research mathematically but also for providing invaluable advice and support regarding life in general. You are advisors in the best sense of the word.

Thanks go also to friends and family for being generous with their love and support, to Stuart and Emerson for being furry, and to Torrey for being.

Chapter 1

Introduction

1.1 Pairings in cryptography

The use of abelian varieties in public-key cryptography goes back to the mid-1980s, when Victor Miller [89] and Neal Koblitz [65] independently proposed using groups of points on elliptic curves in discrete logarithm-based cryptosystems. The discrete logarithm problem on elliptic curves has now been studied extensively for more than twenty years, and it appears that the initial claim that the problem is computationally infeasible is still sound — to this day, there is no algorithm that solves the problem in less than exponential time.

Higher-dimensional abelian varieties first appeared on the scene when Koblitz [66] proposed that the discrete logarithm problem is also infeasible on Jacobians of hyperelliptic curves over finite fields. The supposed advantage of g-dimensional abelian varieties over elliptic curves is that one can work over a field that is a factor of g smaller while retaining the same level of security, thus leading to potential speed advantages. However, it is only recently that the arithmetic operations on these varieties have been optimized to the point where, for certain applications, Jacobians of hyperelliptic curves are now competitive with elliptic curves in terms of performance at a given security level [11].

In the early days of elliptic curve cryptography, supersingular elliptic curves were often proposed for use in cryptosystems. Supersingular curves E over finite fields $\mathbb{F}_q$ have the feature that their number of $\mathbb{F}_q$-rational points is easy to count, which was important in the days before fast point-counting algorithms were developed. However, in 1993 Menezes, Okamoto, and Vanstone [86] showed that the Weil pairing can be used to reduce the discrete logarithm problem on a supersingular elliptic curve E over $\mathbb{F}_q$ to the same problem in the

multiplicative group of some extension field $\mathbb{F}_{q^k}$ with $k \leq 6$. Shortly thereafter, Frey and Rück [43] devised a similar reduction using the Tate pairing, which also applies to higher-dimensional abelian varieties. Since there exist subexponential-time algorithms for discrete logarithms in multiplicative groups of finite fields, the discrete logarithm can usually be computed faster in $\mathbb{F}_{q^k}^{\times}$ than in $E(\mathbb{F}_q)$, and thus these reductions were interpreted as attacks on the discrete logarithm problem on elliptic curves.

After the publication of the MOV and Frey-Rück attacks, supersingular elliptic curves were commonly perceived as "weak" and thus unsuitable for cryptography. This attitude reigned until 2000, when Antoine Joux [60] proposed a one-round protocol for three-party key agreement using the Weil or Tate pairings on supersingular elliptic curves. Joux's key observation was that the curve parameters can be chosen so that the discrete logarithm problem is still infeasible even after the MOV or Frey-Rück reduction, and that the bilinear property of the pairing allows one to perform computations in the "target group" $\mathbb{F}_{q^k}^{\times}$ that previously appeared to require a discrete logarithm.

Joux's discovery opened the floodgates, and in the next few years many important cryptosystems were constructed that made use of bilinear maps. The greatest success was the development of identity-based encryption, which was discovered independently by Sakai, Ohgishi, and Kasahara [109] and Boneh and Franklin [14], and which solved a problem first posed by Shamir in 1984 [114]. Other notable accomplishments include short signature schemes [17], broadcast encryption with small ciphertexts [15], and applications to private information retrieval and zero-knowledge proofs [16]. The subject has now expanded to the point where the First International Conference in Pairing-Based Cryptography was held in Tokyo in 2007; 86 papers were submitted and 18 were presented at the conference [121]. This work is no longer completely theoretical, either — at least one company, Voltage, Inc. [126], has brought pairing-based cryptography to market.

All of the pairing-based cryptographic constructions use the pairing as a "black box"; that is, they can be implemented using any groups on which there is a nondegenerate bilinear map, or pairing. While the security proofs of these systems usually make use of assumptions such as the "bilinear Diffie-Hellman assumption" [14], in the most general sense the security level of the system is determined by the complexity of the discrete logarithm problems in the domain ("source group") and codomain ("target group") of the pairing.

At present, the only known pairings between groups in which the discrete logarithm problems are computationally infeasible are the Weil and Tate pairings on abelian varieties

over finite fields, and their variants such as the Eta [7] and Ate [56] pairings. If A is a abelian variety defined over the field $\mathbb{F}_q$ of q elements, these pairings in general take as input a point P defined over $\mathbb{F}_q$ and a point Q defined over some extension field $\mathbb{F}_{q^k}$, and produce as output an element $e(P,Q)$ of the multiplicative group $\mathbb{F}_{q^k}^\times$.

For a pairing-based system using A to be secure, the discrete logarithm problems in $A(\mathbb{F}_q)$ and $\mathbb{F}_{q^k}^\times$ must both be infeasible. The best known generic discrete logarithm algorithm on abelian varieties (in both theory and practice) is the parallelized Pollard rho algorithm [104, 123]. This algorithm has heuristic running time $O(\sqrt{r}/m)$, where r is the size of largest prime-order subgroup of $A(\mathbb{F}_q)$ and m is the number of processors used. In dimensions $g \geq 3$ index calculus methods have been developed that can solve the discrete logarithm problem in time $\tilde{O}(q^{2-2/g})$, where the implied constant depends on g [1, 49, 53, 48]. For fixed g these methods are still exponential in the field size q; however if the size of the group $A(\mathbb{F}_q)$ is held constant, index calculus methods are subexponential in the dimension g. Thus abelian varieties of high dimension are usually considered to be unsuitable for cryptographic applications.

On the other side of things, the best algorithm for discrete logarithm computation in finite fields is the index calculus attack (e.g., [99]), which has running time subexponential in the field size. Thus to achieve the same level of security on both sides of the pairing, the size q^k of the extension field must be significantly larger than r. The ratio of these sizes is computed from three parameters: the *embedding degree*, which is the degree k of the extension field required by the pairing; the dimension g of the abelian variety; and a parameter ρ, which is defined to be $g \log q / \log r$ and which roughly measures the size of the entire group $A(\mathbb{F}_q)$ relative to the size of the prime-order subgroup that provides input points to the pairing. The ratio of the number of bits in the extension field size to the number of bits in the subgroup order is thus given by $\rho \cdot k/g$.

There has been much speculation about the exact sizes of r and q^k required to match standard sizes of keys for symmetric encryption, using for example the Advanced Encryption Standard (AES) [74, 101]. We outline in Table 1.1 one view of the matter for $g = 1$ or 2, distilled by Mike Scott from material taken from various authoritative sources, in particular [47] and [74]. The listed bit sizes are those matching the security levels of the SKIPJACK, Triple-DES, AES-Small, AES-Medium, and AES-Large symmetric key encryption schemes. By a "b-bit security level," we mean the minimum number of bit operations necessary to break the system is (conjecturally) 2^b. In dimensions $g \geq 3$ the subgroup size r should be

Table 1.1: Bit sizes of parameters for one- and two-dimensional abelian varieties and corresponding embedding degrees to obtain commonly desired levels of security.

Security level (in bits)	Subgroup size r (in bits)	Extension field size q^k (in bits)	$\rho \cdot k$	
			$g = 1$	$g = 2$
80	160	960 – 1280	6 – 8	12 – 16
112	224	2200 – 3600	10 – 16	20 – 32
128	256	3000 – 5000	12 – 20	24 – 40
192	384	8000 – 10000	20 – 26	40 – 52
256	512	14000 – 18000	28 – 36	56 – 72

increased to take into account the existence of index calculus attacks, and the embedding degree k adjusted to take into account both r and g.

As we can see from the table, to achieve varied levels of security it is necessary to construct curves with varying embedding degree. However, in their paper on the Weil pairing reduction, Menezes, Okamoto and Vanstone [86] showed that supersingular elliptic curves always have embedding degree $k \leq 6$. Rubin and Silverberg [108] generalized this work to show that for $g \leq 6$, supersingular abelian varieties always have embedding degree $k \leq 7.5g$. Since these values are at the low end of the security spectrum (as Table 1.1 shows for the case where $g = 1$ or 2 and $\rho \approx 1$), to obtain efficient performance at higher security levels we must construct non-supersingular varieties that have larger embedding degrees. As we will see in Section 1.2.3 below, this is in general a hard problem. We thus have the following

Motivating Problem. Given positive integers b, k, and g, construct a g-dimensional abelian variety over a finite field that has a b-bit prime-order subgroup and embedding degree k.

Any solution to this problem must be feasible for b of cryptographic size, i.e., large enough so that the discrete logarithm problem in a group whose order is a b-bit prime number is computationally infeasible. For current technology this means $b \geq 160$. By "construct," we mean that we wish to describe the given abelian variety explicitly in a way such that both arithmetic on the abelian variety and pairings can be computed in a reasonable amount of time with current hardware and software.

The statement of the Motivating Problem refers to the size of the subgroup on the abelian variety and the embedding degree, but does not address directly the third parameter

needed to compute the security level in the finite field, namely the ρ-value. In general, varieties with small ρ-values are desirable in order to speed up arithmetic on the abelian variety. For example, an elliptic curve with a 160-bit subgroup and $\rho = 1$ is defined over a 160-bit field, while a curve with a 160-bit subgroup and $\rho = 2$ is defined over a 320-bit field, and group operations and pairings can be computed much more quickly on the first curve. In addition, the cryptographic elements of a pairing-based protocol (such as keys and ciphertexts) usually consist of points on the abelian variety and are described in terms of coordinates in $\mathbb{F}_q$, so systems using abelian varieties with smaller ρ-values require less bandwidth for the same security level. Thus in our attempts to solve the motivating problem, we prefer abelian varieties with smaller ρ-values, with our ultimate goal being varieties with a prime number of points, which have $\rho \approx 1$.

1.2 Pairing-friendly abelian varieties

Before we discuss our contribution to the solution of the Motivating Problem, we give some relevant background on elliptic curves and abelian varieties and define the technical terminology we will use throughout this dissertation.

For further background, Silverman [117] provides an excellent exposition of elliptic curves; information on abelian varieties can be found in the article of Waterhouse and Milne [129], which focuses on varieties over finite fields, and those of Milne [90, 92], which treat varieties over arbitrary fields. Lang's book [72] is a standard reference for basic algebra, while Hartshorne's [55] is the same for algebraic geometry.

An *abelian variety* A is a smooth, projective, absolutely irreducible algebraic variety with a group structure whose operations are given by algebraic morphisms. An *elliptic curve* is a one-dimensional abelian variety, and an *abelian surface* is a two-dimensional abelian variety. If A is an abelian variety defined over a field F (written A/F), we denote by $A(F)$ the group of F-rational points of A. If r is an integer, then $A[r]$ denotes the group of all r-torsion points of A defined over an algebraic closure $\overline{F}$ of F. We denote by $A(F)[r]$ the group of r-torsion points of A defined over F. If A has dimension g and r is prime to the characteristic of F, then $A[r] \cong (\mathbb{Z}/r\mathbb{Z})^{2g}$.

A positive-dimensional abelian variety A/F is *simple* (or *F-simple*) if it is not isogenous over F to a product of lower-dimensional abelian varieties. We say that A is *absolutely simple* if it not isogenous over $\overline{F}$ to a product of lower-dimensional abelian varieties.

1.2.1 Frobenius endomorphism and CM fields

Let $\mathbb{F}_q$ denote the finite field of q elements. Every abelian variety A defined over $\mathbb{F}_q$ has an endomorphism called the *Frobenius endomorphism*, which is denoted by π and which operates by raising the coordinates of a point to the qth power. The Frobenius endomorphism satisfies a monic, integer polynomial h_A known as the *characteristic polynomial of Frobenius*, which is the characteristic polynomial of the action of π on the Tate module T_ℓ for any prime $\ell \nmid q$ [90, §12]. By a theorem of Weil [90, Theorem 19.1], all of the complex roots of h_A have absolute value $\sqrt{q}$; a monic, irreducible polynomial in $\mathbb{Z}[x]$ with this property is called a *q-Weil polynomial*, and any root is called a *q-Weil number*. By Honda-Tate theory [122], q-Weil polynomials are in one-to-one correspondence with isogeny classes of simple abelian varieties over $\mathbb{F}_q$.

If A is simple, then h_A is a power of an irreducible polynomial and we can view π as an element of a number field K. The field K is either a *CM field*, which is an imaginary quadratic extension of a totally real field, or the field $\mathbb{Q}(\sqrt{q})$ [122]. We call a CM field K *primitive* if it contains no proper CM subfields. The full endomorphism algebra $E = \mathrm{End}_F(A) \otimes \mathbb{Q}$ is a central simple algebra over $K = \mathbb{Q}(\pi)$, and by a theorem of Tate [122] it satisfies

$$2 \cdot \dim(A) = [E : K]^{1/2}[K : \mathbb{Q}]. \tag{1.1}$$

Since $A(\mathbb{F}_q)$ is the kernel of the endomorphism $\pi - 1$, we have

$$\#A(\mathbb{F}_q) = h_A(1). \tag{1.2}$$

If $E = K = \mathbb{Q}(\pi)$, then we also have

$$\#A(\mathbb{F}_q) = \mathrm{Norm}_{K/\mathbb{Q}}(\pi - 1). \tag{1.3}$$

A g-dimensional abelian variety A defined over a field F of characteristic p is *ordinary* if $\dim_{\mathbb{F}_p} A[p] = g$, or equivalently, if the middle coefficient of h_A is prime to p. We say that A is *supersingular* if A is $\overline{F}$-isogenous to a product of supersingular elliptic curves. Silverman [117, Theorem 3.1] characterizes supersingular elliptic curves, while Galbraith [44, Theorem 1] gives several equivalent conditions for an abelian variety to be supersingular. We call a q-Weil number π ordinary or supersingular if the corresponding abelian variety (in the sense of Honda-Tate theory [122]) is the same. If $g \geq 2$ then there are g-dimensional abelian varieties that are neither ordinary nor supersingular.

If A is ordinary and simple then the endomorphism ring $\mathrm{End}(A)$ is commutative. It then follows from (1.1) that $E = K = \mathbb{Q}(\pi)$ and K has degree $2g$, where $g = \dim A$. In this case, $\mathrm{End}(A)$ is an order $\mathcal{O}$ in the ring of integers of K (denoted $\mathcal{O}_K$). We take the statement *A has complex multiplication by K* or *CM by K* to mean that $\mathrm{End}(A) \otimes \mathbb{Q} \cong K$, and we take the statement *A has CM by $\mathcal{O}$* to mean that $\mathrm{End}(A) \cong \mathcal{O} \subset \mathcal{O}_K$. We will discuss the theory of complex multiplication further in Chapter 4.

In the case of elliptic curves, we will often work with the *trace* of the Frobenius endomorphism, which is defined to be the integer $t = \pi + \overline{\pi}$. Equation (1.2) then tells us that

$$\#E(\mathbb{F}_q) = q + 1 - t. \tag{1.4}$$

The trace satisfies the *Hasse bound* $|t| \leq 2\sqrt{q}$ [117, §5.1], which leads to upper and lower bounds on the number of $\mathbb{F}_q$-rational points of E:

$$q - 2\sqrt{q} + 1 \leq \#E(\mathbb{F}_q) \leq q + 2\sqrt{q} + 1.$$

If $E/\mathbb{F}_q$ is an elliptic curve with trace t, then t is relatively prime to q if and only if E is ordinary.

1.2.2 Curves and Jacobians

Throughout this dissertation, a *curve* will refer to a smooth, projective, absolutely irreducible algebraic variety of dimension one. We will often describe curves by equations in two variables, possibly with a singularity at infinity, such as $C : y^2 = f(x)$. In this case we take the curve C to be the normalization of the projective closure of the affine plane curve defined by this equation. The *genus* of a curve C is the dimension of the space of regular differentials on C.

A *hyperelliptic curve* over a field F is a curve C/F of genus $g \geq 2$ for which there exists a two-to-one map, defined over $\overline{F}$, from C to the projective line $\mathbb{P}^1$. If the characteristic of F is not 2, any hyperelliptic curve of genus g can be represented by an affine model of the form $y^2 = f(x)$, where f is a polynomial in $\overline{F}[x]$ of degree $2g+1$ or $2g+2$ with no multiple roots. All curves of genus 2 are hyperelliptic (see [55, Exercise IV.1.7]).

If C is a curve over F, the *Jacobian* of C, denoted $\mathrm{Jac}(C)$, is a principally polarized abelian variety over F of dimension g, where g is the genus of C. The group $\mathrm{Jac}(C)(\overline{F})$ is isomorphic to the group $\mathrm{Pic}^0(\overline{C})$ given by linear equivalence classes of degree-zero divisors

on $\overline{C}$, the base extension of C to $\overline{F}$. (For more information on Jacobians, see [91].) We will denote by O the trivial divisor class, which is the identity in the group $\mathrm{Jac}(C)(\overline{F})$. When we say that a curve C has complex multiplication by a field K or an order $\mathcal{O}$, we mean that $\mathrm{Jac}(C)$ has this property.

If C is a genus 1 curve given by a Weierstrass equation of the form $y^2 = f(x)$ with $\deg f = 3$, we denote by O the single point at infinity in the projective closure of this affine curve. We then have an isomorphism of varieties $C \to \mathrm{Jac}(C)$ given by $\phi : P \mapsto [P - O]$. We will identify C with $\mathrm{Jac}(C)$ by this isomorphism, and call C an elliptic curve.

1.2.3 Pairings and embedding degrees

Let A be an abelian variety defined over a field F, and let r be a positive integer relatively prime to $\mathrm{char}\, F$. Let μ_r be the group of rth roots of unity in an algebraic closure of F. The *Weil pairing* is a nondegenerate, bilinear, Galois-equivariant map

$$e_{weil,r} : A[r] \times \hat{A}[r] \to \mu_r,$$

where $\hat{A}$ is the dual of A. (If A is principally polarized, as is the case when A is a Jacobian, then $\hat{A} \cong A$.) For definitions of the Weil pairing and proofs of its properties, see [117, §3.8] for elliptic curves and [90, §16] for general abelian varieties.

If F is a finite field, the *Tate pairing* is a nondegenerate, bilinear, Galois-equivariant map

$$e_{tate,r} : A(F)[r] \times \hat{A}(F)/r\hat{A}(F) \to F^\times/(F^\times)^r.$$

If $\mu_r \subset F$, then the target group $F^\times/(F^\times)^r$ is isomorphic to μ_r; otherwise it is isomorphic to μ_s for some $s \mid r$. For a definition of the Tate pairing and proofs of its properties, see [33].

From these descriptions it is apparent that if F is finite, then to obtain Weil or Tate pairing values of order r we must work over a field containing the rth roots of unity.

Definition 1.2.1. Let A be an abelian variety defined over a field F, and let r be a positive integer relatively prime to $\mathrm{char}(F)$. We say that A has *embedding degree k with respect to r* if

1. A has a F-rational point of order r, and
2. $[F(\mu_r) : F] = k$.

If C is a curve, then we say that C has embedding degree k with respect to r if and only if the Jacobian of C does.

We often ignore r when stating the embedding degree, as it is usually clear from the context.

The embedding degree gets its name because we can use a pairing to embed a cyclic subgroup of $A(F)$ of order r into the multiplicative group of the degree-k extension of F. The Menezes-Okamoto-Vanstone attack on the discrete logarithm problem on supersingular elliptic curves [86] makes use of such an embedding. If A is a g-dimensional abelian variety defined over $\mathbb{F}_q$ with $q = p^d$ and m is the multiplicative order of p modulo r, then the quantity m/dg is a good measure of the security of cryptosystems based on A [58]. If $\mathbb{F}_q$ is a prime field (i.e., $d = 1$) then this quantity is equal to k/g.

For constructive applications of pairings, the embedding degree of A needs to be small enough so that the pairing is easy to compute, but large enough so that the discrete logarithm in $\mathbb{F}_{q^k}^{\times}$ is computationally infeasible. Balasubramanian and Koblitz [5] showed that for a random elliptic curve E over a random field $\mathbb{F}_q$ and a prime $r \approx q$, the probability that E has embedding degree less than $\log^2 q$ with respect to r is vanishingly small, and in general the embedding degree can be expected to be around r. Luca, Mireles, and Shparlinski [79] have obtained similar results for fixed values of q, and we expect analogous results to hold in higher dimensions. We conclude that if r is around 2^{160} (the smallest value currently acceptable for security in implementations) pairings on a random abelian variety will take values in a field of roughly 2^{160} *bits*, so the computation is completely hopeless.

To avoid the Pohlig-Hellman attack [103], the points on A used in cryptographic protocols should have prime order. Thus we wish to construct abelian varieties over finite fields that have points of large prime order r and small embedding degree with respect to r. Such varieties are (informally) called "pairing-friendly."

Constructions of pairing-friendly abelian varieties make substantial use of the theory of cyclotomic polynomials and cyclotomic fields. We recall a few basic facts here; for a deeper discussion, see Lidl and Niederreiter's book [77]. For every positive integer k, we let ζ_k denote a primitive kth root of unity in $\overline{\mathbb{Q}}$, i.e., an algebraic number such that $(\zeta_k)^k = 1$ and $(\zeta_k)^\ell \neq 1$ for any positive $\ell < k$. The minimal polynomial of ζ_k over $\mathbb{Q}$ is called the *kth cyclotomic polynomial* and is denoted $\Phi_k(x)$. These polynomials have integer coefficients

and can be defined recursively by setting $\Phi_1(x) = x - 1$ and using the formula

$$x^k - 1 = \prod_{d|k} \Phi_d(x) \tag{1.5}$$

for $k > 1$. The degree of $\Phi_k(x)$ is denoted $\varphi(k)$ and is also called *Euler's phi function*; it gives the number of positive integers less than or equal to k that are relatively prime to k.

Lemma 1.2.2. *Let A be an abelian variety over a finite field $\mathbb{F}_q$ with an $\mathbb{F}_q$-rational point of order r. If r is relatively prime to q then the following conditions are equivalent:*

1. *A has embedding degree k with respect to r.*
2. *k is the smallest integer such that r divides $q^k - 1$.*
3. *k is the multiplicative order of q modulo r.*

Furthermore, if r is a prime not dividing k then these conditions are equivalent to

4. *$\Phi_k(q) \equiv 0 \pmod{r}$, where Φ_k is the kth cyclotomic polynomial.*

Proof. The equivalence of (1) and (2) follows from the fact that the multiplicative group of a finite field is cyclic, and the equivalence of (2) and (3) follows trivially from the definitions.

Now suppose r is prime and (2) holds, so $r \mid q^k - 1$ but $r \nmid q^i - 1$ for any $1 \leq i < k$. By (1.5) and since r is prime, this means $r \mid \Phi_k(q)$. Conversely, if (4) holds, then (1.5) implies that $r \mid q^k - 1$. It remains to show that $r \nmid q^i - 1$ for any $1 \leq i < k$. We follow Menezes' proof [85, Lemma 6.3]. Let $f(x) = x^k - 1$ and $\mathbb{F} = \mathbb{Z}/r\mathbb{Z}$. Then $\mathbb{F}$ is a field. Since $r \nmid k$, we have $\gcd(f(x), f'(x)) = 1$ in $\mathbb{F}[x]$. Thus, f has only single roots in $\mathbb{F}$. Using (1.5) and the fact that q is a root of $\Phi_k(x)$ over $\mathbb{F}$, we obtain $\Phi_d(q) \not\equiv 0 \pmod{r}$ for any $d \mid k$, $1 \leq d < k$. Therefore, $r \nmid q^d - 1$ for any $d \mid k$, $1 \leq d < k$. Finally, we note that $r \nmid q^i - 1$ for any positive i that does not divide k, since in this case we would have $r \mid q^{\gcd(i,k)} - 1$. □

We can also give a characterization of the embedding degree in terms of the Frobenius endomorphism π.

Corollary 1.2.3. *Let $A/\mathbb{F}_q$ be a simple abelian variety with Frobenius endomorphism π, and suppose that $K = \mathbb{Q}(\pi)$ equals $\mathrm{End}(A) \otimes \mathbb{Q}$. Let k be a positive integer, Φ_k the kth cyclotomic polynomial, and r a square-free integer not dividing kq. If*

$$\begin{aligned} \mathrm{Norm}_{K/\mathbb{Q}}(\pi - 1) &\equiv 0 \pmod{r}, \\ \Phi_k(\pi\overline{\pi}) &\equiv 0 \pmod{r}, \end{aligned}$$

then A has embedding degree k with respect to r.

Proof. Since r is square-free, the first condition tells us that $A(\mathbb{F}_q)$ has a cyclic subgroup of order r, while the second tells us that condition (4) of Lemma 1.2.2 holds for each prime dividing r. □

We also observe that in the case of an elliptic curve $E/\mathbb{F}_q$ with trace of Frobenius t and a cyclic subgroup of order r, the formula for the number of points (1.4) implies that $q \equiv t - 1 \pmod{r}$, and thus we can rephrase Lemma 1.2.2 in terms of $t - 1$:

Corollary 1.2.4. *Let E be an elliptic curve over a finite field $\mathbb{F}_q$ with trace of Frobenius t and an $\mathbb{F}_q$-rational point of order r. If r is relatively prime to q then the following conditions are equivalent:*

1. *E has embedding degree k with respect to r.*
2. *k is the smallest integer such that r divides $(t-1)^k - 1$.*
3. *k is the multiplicative order of $t - 1$ modulo r.*

Furthermore, if r is a prime not dividing k then these conditions are equivalent to

4. *$\Phi_k(t-1) \equiv 0 \pmod{r}$, where Φ_k is the kth cyclotomic polynomial.* □

For implementation purposes, the subgroup of prime order r should be close as possible to the full group $A(\mathbb{F}_q)$, with the "ideal" case being that r is actually the full group order. Since this ideal is difficult to achieve in practice, we define a parameter ρ that represents how close to this ideal a given g-dimensional abelian variety is. Using the fact that $\#A(\mathbb{F}_q) \approx q^g$ [90, Theorem 19.1], we can approximate the ratio of the size (in bits) of this group order to the size (in bits) of the subgroup order r by the parameter

$$\rho = \frac{g \log q}{\log r}. \tag{1.6}$$

We can interpret the ρ-value of an abelian variety as the ratio of the abelian variety's required bandwidth to its security level. As we discussed in Section 1.1, abelian varieties with ρ-values close to 1 usually provide the best performance in implementations. However, such varieties are often limited to specific, small embedding degrees k, and thus to achieve comparable security levels in $A[r]$ and $\mathbb{F}_{q^k}^\times$ it is not uncommon to use varieties with larger ρ-values.

1.2.4 Complex multiplication methods

From the discussion above, we see that the problem of constructing a pairing-friendly abelian variety essentially reduces to determining a q-Weil number π and a subgroup size r that have the relationship specified by Corollary 1.2.3, and then constructing an explicit abelian variety over $\mathbb{F}_q$ with Frobenius element π. The bulk of this dissertation is dedicated to solving the first problem. The latter task is achieved by *complex multiplication methods*, or *CM methods*, which we now discuss.

The key idea underlying CM methods is the following: by the Serre-Tate theory of canonical liftings [78], every ordinary abelian variety A over $\mathbb{F}_q$ is the reduction modulo a suitable prime $\mathfrak{p}$ over q of an abelian variety A_0 over $\overline{\mathbb{Q}}$ with $\mathrm{End}(A_0) \cong \mathrm{End}(A)$. Furthermore, if A is a simple, principally polarized abelian variety of dimension $g \leq 3$, then A_0 is the Jacobian of a genus g curve $C_0/\overline{\mathbb{Q}}$.

At present, CM methods have only been developed in dimension $g \leq 3$. In these cases, we have the following:

Proposition 1.2.5. *Let π be an ordinary q-Weil number, and suppose that the number field $K = \mathbb{Q}(\pi)$ is a primitive CM field of degree $2g$ with $g \leq 3$. Then there is a genus g curve $C/\mathbb{F}_q$ such that $\mathrm{End}(\mathrm{Jac}(C)) \cong \mathcal{O}_K$, the ring of integers of K, and either*

1. *C is elliptic or hyperelliptic and $\mathrm{Jac}(C)$ has Frobenius element π, or*
2. *C is a smooth plane quartic and $\mathrm{Jac}(C)$ has Frobenius element π or $-\pi$.*

Proof. The result is well-known for $g = 1$, so we consider the cases $g = 2$ or 3. Let $\mathcal{A}$ be the isogeny class of abelian varieties over $\mathbb{F}_q$ with Frobenius element π. Since K is primitive and π is ordinary, it follows from the Honda-Tate theorem [122, Théorème 1] that any abelian variety $A \in \mathcal{A}$ is absolutely simple.

Suppose there is an $A \in \mathcal{A}$ that is principally polarized and has endomorphism ring isomorphic to $\mathcal{O}_K$. Then by theorems of Weil (for $g = 2$) and Oort and Ueno (for $g = 3$) [100], A is $\overline{\mathbb{F}}_q$-isomorphic to the Jacobian of a genus g curve $\overline{C}$. If $\overline{C}$ is hyperelliptic, then there is a hyperelliptic curve $C/\mathbb{F}_q$ such that $\mathrm{Jac}(C)$ is $\mathbb{F}_q$-isomorphic to A (see e.g. [73, Appendix, §7]), proving statement (1). If $\overline{C}$ is not hyperelliptic then there is a curve $C/\mathbb{F}_q$ such that $\mathrm{Jac}(C)$ is $\mathbb{F}_q$-isomorphic to either A or its quadratic twist A' (again, see e.g. [73, Appendix, §7]). Any nonhyperelliptic curve of genus 2 or 3 is a smooth plane quartic, so

statement (2) now follows from the facts that $\mathrm{End}(A') \cong \mathrm{End}(A)$ and A' has Frobenius element $-\pi$.

It remains to show that there is an $A \in \mathcal{A}$ that is principally polarized and has endomorphism ring isomorphic to $\mathcal{O}_K$. Let K_0 be the maximal totally real subfield of K. By the work of Howe [59, Propositions 5.7 and 10.1], it suffices to show that there is a finite prime $\mathfrak{p}$ of K_0 that ramifies in K. For $g = 2$, a variation of Howe's proof of [59, Lemma 12.1] shows that if there is no finite prime $\mathfrak{p}$ of K_0 that ramifies in K, then K contains an imaginary quadratic subfield, contradicting the assumption that K is primitive. For $g = 3$, the result follows directly from [59, Corollary 10.3]. □

Proposition 1.2.5 has as an immediate consequence that given a primitive CM field K and an ordinary Weil number $\pi \in \mathcal{O}_K$, we can solve the construction problem by compiling the finite list of $\overline{\mathbb{Q}}$-isomorphism classes of curves in characteristic zero whose Jacobians have CM by $\mathcal{O}_K$. From representatives of this list, we obtain a list $\mathcal{C}$ of curves over $\mathbb{F}_q$ whose Jacobians have CM by $\mathcal{O}_K$ by reducing at some fixed prime $\mathfrak{p}$ over q. Changing the choice of the prime $\mathfrak{p}$ amounts to taking the reduction at $\mathfrak{p}$ of conjugate curves, which also have Jacobians with CM by $\mathcal{O}_K$.

For every curve $C \in \mathcal{C}$, we compute the set of its twists, i.e., all the curves up to $\mathbb{F}_q$-isomorphism that become isomorphic to C over $\overline{\mathbb{F}}_q$. If C is elliptic or hyperelliptic (which is always the case when $g \leq 2$), then there is at least one twist C' of a curve $C \in \mathcal{C}$ whose Jacobian has the specified Frobenius element π. This curve can be selected from the list of twists using the fact that $\#\operatorname{Jac}(C)(\mathbb{F}_q) = \operatorname{Norm}_{K/\mathbb{Q}}(\pi - 1)$. (Note that while efficient point-counting algorithms do not exist for varieties of dimension $g > 1$, if $q \gg g$ we can determine probabilistically whether an abelian variety over $\mathbb{F}_q$ has a given order by choosing a few random points, multiplying by the expected order, and seeing if the result is always the identity.) If C is not hyperelliptic, then it may happen that we can only find a curve C' such that $\operatorname{Jac}(C')$ has Frobenius element $-\pi$; in this case the desired abelian variety is the quadratic twist of $\operatorname{Jac}(C')$, which cannot be described as the Jacobian of a curve over $\mathbb{F}_q$.

It now remains only to construct the list of curves over $\overline{\mathbb{Q}}$ with CM by $\mathcal{O}_K$.

In genus 1, where we are dealing with elliptic curves, the problem has been studied extensively. The j-invariants of elliptic curves over $\overline{\mathbb{Q}}$ with CM by the ring of integers $\mathcal{O}_K$ of a quadratic imaginary field K are the roots of the *Hilbert class polynomial* of K, which is a monic, square-free polynomial with integer coefficients. There are three different approaches

to computing the Hilbert class polynomial: a complex-analytic algorithm [3, 35], a Chinese remainder theorem algorithm [23, 2], and a p-adic algorithm [29, 20]. The best running time for these algorithms is $\tilde{O}(h_K^2)$, where h_K is the class number of K [35, 20]. Since the degree of the Hilbert class polynomial is h_K and the bit size of the coefficients grows roughly linearly in h_K, this running time is essentially the best possible. At present, the largest class number for which the elliptic curve CM method is feasible is $h_K = 10^5$ [35].

Analogous methods exist for constructing genus 2 curves over $\overline{\mathbb{Q}}$ with CM by the ring of integers $\mathcal{O}_K$ of a given quartic CM field K. In this case, the solutions rely on computing the curves' absolute Igusa invariants via the computation of the *Igusa class polynomials* for K, which lie in $\mathbb{Q}[x]$. (A precise definition of the Igusa class polynomials appears on page 96.) Again there are three different approaches to computing the class polynomials: a complex-analytic algorithm [119, 124, 131, 27], a Chinese remainder theorem algorithm [34], and a p-adic algorithm [51]. These algorithms are less extensively developed than their elliptic curve analogues; at present they can handle only very small quartic CM fields, and there is no running time analysis for any of them. We discuss the genus 2 CM method in more detail in Chapter 5, focusing on the Chinese remainder approach.

In genus 3, the invariant theory and the corresponding theory of class polynomials have been developed only in two special cases. The first, due to Weng [130], is the case of hyperelliptic curves with CM by a degree-6 field K containing $\mathbb{Q}(i)$. The second, due to Koike and Weng [70], is the case of Picard curves (curves of the form $y^3 = f(x)$ with $\deg f = 4$) with CM by a degree-6 field K containing $\mathbb{Q}(\zeta_3)$. In both cases the class polynomials are computed via a complex-analytic algorithm, and the algorithms are again limited to very small CM fields K.

In each of these cases the correspondence between curves and absolute invariants commutes with reduction at p. It follows that we can find the invariants of curves $C/\mathbb{F}_q$ that have CM by $\mathcal{O}_K$ by computing roots of the class polynomials in $\mathbb{F}_q$. (See [34, Theorem 2], reproduced as Theorem 5.1.2 below, for a precise statement of this result in the case $g = 2$.) An explicit equation for the curve C can then be computed from the invariants using well-known formulas for $g = 1$, using Mestre's algorithm [88] for $g = 2$, and using the appropriate algorithms in the two tractable cases with $g = 3$ [130, 70]. The requirement that $\mathrm{Jac}(C)$ be ordinary is essential, and ensures that $p = \mathrm{char}(\mathbb{F}_q)$ does not divide the denominator of any coefficient of the class polynomial; see [54, Section 4] for further details in the case $g = 2$.

Explicit CM theory has not been developed for dimensions $g \geq 4$, save for a few specific examples. Moreover, "most" principally polarized abelian varieties of dimension $g \geq 4$ are not Jacobians, as the moduli space of Jacobians has dimension $3g - 3$, while the moduli space of abelian varieties has dimension $g(g+1)/2$. For implementation purposes we prefer Jacobians or even hyperelliptic Jacobians, as these are the only abelian varieties on which group operations and pairings can be computed efficiently over finite fields of cryptographic size.

1.2.5 Algorithms

Many of the results in this dissertation are presented in the form of algorithms. We define an *algorithm* to be a sequence of computations that can be implemented on a Turing machine and is guaranteed to terminate after a finite amount of time. A *probabilistic algorithm* is an algorithm that has access to an external source of input from which truly random bits can be generated. When we say that a probabilistic algorithm terminates in a finite amount of time, we mean that for any valid input the expected running time

$$\int_0^\infty tP(t)dt,$$

where $P(t)$ is the probability of terminating at time t, is finite.

Our definition does not take into account whether an algorithm produces correct output; an algorithm's proof of correctness is separate from its statement. When we say that a probabilistic algorithm is correct, we mean that for any valid input it produces correct output with probability greater than $1/2$. We also make no *a priori* claims about the running time of our algorithms. Indeed, showing that our algorithms can run in polynomial time with negligible error probability will often be an essential part of our discussion.

In general we will not distinguish between probabilistic and deterministic algorithms. Indeed, some of our algorithms contain steps such as "choose element x from set Y" that can be implemented either deterministically or probabilistically. Obviously, any algorithm that makes explicit reference to randomness in its description will be probabilistic.

1.2.6 Miscellaneous notation

We denote by $\mathbb{Z}$ the ring of integers, and by $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ the fields of rational, real, and complex numbers respectively. If F is a field we denote by $\overline{F}$ an algebraic closure of F. Unless otherwise stated, all fields are assumed to be separable.

The "big-O" notation $f(x) = O(g(x))$ means that there exist positive constants C and N such that for any $x > N$, $|f(x)| \leq C\,|g(x)|$. If $g(x) > 1$ for x sufficiently large, the "soft-O" notation $f(x) = \tilde{O}(g(x))$ means that there is some positive integer k such that $f(x) = O(g(x)\log^k g(x))$. Note that $f(x) = \tilde{O}(g(x))$ implies that $f(x) = O(g(x)^{1+\epsilon})$ for any $\epsilon > 0$. Analogous definitions hold for functions of several variables.

1.3 Scope of this dissertation

In this dissertation we present several new contributions to the solution of the Motivating Problem of page 4. We focus on the case where the abelian variety in question is ordinary, as supersingular varieties of low dimension have already been classified by Rubin and Silverberg and been shown to have bounded embedding degree k in any dimension g, and varieties of intermediate type are poorly understood in the context of pairing-friendly abelian varieties.[†]

In Chapter 2 we give an abstract and general framework that classifies the known constructions of pairing-friendly ordinary elliptic curves. Our framework allows the practitioner to quickly determine the various attributes of any such construction, making it easy to select a construction for any specified set of performance and security requirements.

More importantly, our framework leads us to discover new constructions of pairing-friendly ordinary elliptic curves. We describe these new constructions in Chapter 3. Our most important contribution in this regard is the construction of elliptic curves of prime order with embedding degree 10, which solves an open problem posed by Boneh, Lynn, and Shacham [17]. We also describe a procedure for generating families of pairing-friendly elliptic curves with variable CM discriminant, which will be useful for those who desire the maximum possible degree of randomness in cryptosystem parameters.

In Chapter 4 we study higher-dimensional abelian varieties. We provide two algorithms that, given a CM field K, construct Frobenius elements π of pairing-friendly ordinary abelian varieties with CM by K. Both algorithms generalize existing constructions of pairing-friendly ordinary elliptic curves. The first method generalizes the construction of Cocks and Pinch [25] and works for (nearly) arbitrary subgroup sizes r. The second generalizes the method of Brezing and Weng [19] and leads to varieties with better ρ-values than the

[†]There is one discussion in the literature of such intermediate varieties, due to Hitt [57], which gives existence results for pairing-friendly abelian surfaces of intermediate type in characteristic 2. Explicit construction of pairing-friendly varieties of this type remains an entirely open problem.

first. Given the output π of either algorithm, one can then use complex multiplication methods to construct explicitly an abelian variety with Frobenius element π.

Finally, in Chapter 5 we turn to the question of the CM methods used to construct explicit examples of pairing-friendly abelian varieties. We focus on implementation aspects of Eisenträger and Lauter's Chinese remainder theorem algorithm [34] for computing Igusa class polynomials of quartic CM fields. One of the steps of this algorithm requires determining whether endomorphism rings of Jacobians of genus 2 curves over small prime fields are isomorphic to the full ring of integers in a given quartic CM field. Our contribution is to provide an efficient probabilistic algorithm that carries out this computation. Using our algorithm to determine endomorphism rings, we have implemented a probabilistic version of the full Eisenträger-Lauter CRT algorithm in MAGMA [18] and used it to compute Igusa class polynomials for several quartic CM fields K with small discriminant. We find that in practice the running time of the CRT algorithm is dominated not by the endomorphism ring computation but rather by the need to compute p^3 curves for many small primes p.

Chapter 2

A Taxonomy of Pairing-Friendly Elliptic Curves

2.1 Introduction

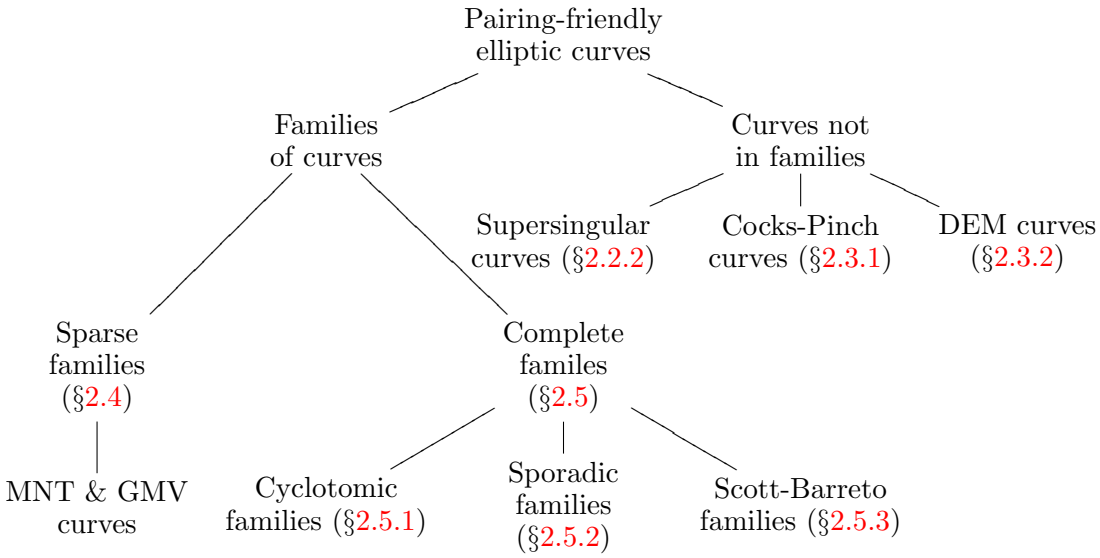
During the time that pairing-based cryptography has been studied in earnest, numerous researchers have worked on the Motivating Problem of page 4 in the case of elliptic curves, i.e., $g = 1$, and there now exist many methods for constructing pairing-friendly elliptic curves. In this chapter we gather these constructions into a single coherent framework. A diagram outlining our classification is given in Figure 2.1.

Our framework will aid the practitioner by allowing him or her to select elliptic curves for any desired combination of performance and security requirements. More importantly, by determining the abstract properties that make the existing constructions work, we can use these properties to produce new constructions that improve on the known ones. These new constructions appear in Chapter 3.

The designers of the first pairing-based protocols proposed the use of supersingular elliptic curves [14]; we discuss these curves in Section 2.2.2. However, supersingular curves are limited to embedding degree $k = 2$ for prime fields and $k \leq 6$ in general [86], so for higher embedding degrees we must turn to ordinary curves.

There are a large number of constructions of ordinary elliptic curves with prescribed embedding degree. All of these constructions are based on the complex multiplication (CM) method of curve construction (see Section 1.2.4), and all construct curves over prime fields.

Figure 2.1: Classification of pairing-friendly elliptic curves



The highest-level distinction we make in our framework is between methods that construct individual curves and those that construct families of curves. The former type are methods that give integers q and r such that there is an elliptic curve E over $\mathbb{F}_q$ with a subgroup of order r and embedding degree k with respect to r. The latter type are methods that give polynomials $q(x)$ and $r(x)$ such that if $q(x_0)$ is prime for some value of x_0, there is an elliptic curve E over $\mathbb{F}_{q(x_0)}$ with a subgroup of order $r(x_0)$ and embedding degree k with respect to $r(x_0)$. Families of curves have the advantage that the sizes of the finite field and the prime-order subgroup can be varied simply by specifying x_0.

There are two constructions in the literature that produce ordinary elliptic curves with small embedding degree that are not given in terms of families: the method of Cocks and Pinch [25] and that of Dupont, Enge, and Morain [32]. In Section 2.3 we describe these two methods and discuss their merits and drawbacks.

The remaining constructions of ordinary elliptic curves with small embedding degree fall into the category of families of curves. Here we make another distinction. The construction of such curves depends on our being able to find integers x, y satisfying an equation of the form

$$Dy^2 = 4q(x) - t(x)^2$$

for some fixed positive integer D and polynomials $q(x)$ and $t(x)$. The parameter D is the "CM discriminant" (which we often call simply the "discriminant"), which we will define formally in Section 2.2. In some cases, this equation will only have solutions for some set of (x, y) that grows exponentially; we call such families *sparse*. In others, this equation may be satisfied for any x, i.e., we can write y as a polynomial in x and the equation gives an equality of polynomials; we call such families *complete*.

Sparse families, discussed in Section 2.4, are primarily based on the ideas of Miyaji, Nakabayashi, and Takano [93]. These families give most of the known constructions of curves of prime order, but are limited to small embedding degrees k. Complete families, discussed in Section 2.5, exist for arbitrary k but usually give curves with $\rho > 1$. All of the constructions of complete families can be viewed as choosing a polynomial $r(x)$ parametrizing the pairing-friendly subgroup size and computing polynomials in $\mathbb{Q}[x]$ that map to certain elements of the number field $K = \mathbb{Q}[x]/(r(x))$. We can further classify the complete families according to properties of the number field K. We briefly list the families and the corresponding type of number field.

- Cyclotomic families (§2.5.1): K is a cyclotomic field, r is a cyclotomic polynomial, and K contains $\sqrt{-D}$ for some small D. Constructions given in [8, 19].
- "Sporadic" families (§2.5.2): K is a (perhaps trivial) extension of a cyclotomic field, r is not a cyclotomic polynomial, and K contains $\sqrt{-D}$ for some small D. Constructions given in [9, 62].
- Scott-Barreto families (§2.5.3): K is a (perhaps trivial) extension of a cyclotomic field, and K contains no $\sqrt{-D}$ for any small D. Constructions given in [113].

Much of the material in this chapter is joint work with Michael Scott of Dublin City University (Ireland) and Edlyn Teske of the University of Waterloo (Canada). A more comprehensive exposition of these topics appears in [41].

2.2 How to generate pairing-friendly elliptic curves

In this section we discuss the common properties of the various constructions of pairing-friendly elliptic curves. As we saw in Section 1.2.3, it is unlikely that a "random" elliptic curve over a finite field will have small embedding degree with respect to a large prime-order subgroup, and thus construction of curves with these properties requires specialized

algorithms. All such algorithms currently in the literature follow essentially the same high-level structure:

1. Fix k, and compute integers t, r, q such that there is an elliptic curve $E/\mathbb{F}_q$ that has trace t, a subgroup of prime order r, and embedding degree k.
2. Use the complex multiplication method to find the equation of the curve E over $\mathbb{F}_q$.

The difficult part of such algorithms is finding t, r, q as in Step (1) while ensuring that Step (2) remains feasible.

We now specialize to the case where E is ordinary; a discussion of supersingular curves can be found in Section 2.2.2. An ordinary elliptic curve with the properties described in Step (1) exists if and only if the following conditions hold:

1. q is prime or a prime power.
2. r is prime.
3. t is relatively prime to q.
4. r divides $q + 1 - t$.
5. r divides $\Phi_k(q)$, where Φ_k is the kth cyclotomic polynomial.
6. $4q - t^2 = Dy^2$ for some square-free positive integer D and some integer y.

Condition (1) ensures that there is a finite field with q elements. Since the proportion of prime powers to primes is virtually zero, we will in general take q to be a prime number. Condition (6) implies that $t \leq 2\sqrt{q}$; together with condition (3) this implies that there exists an ordinary elliptic curve E defined over $\mathbb{F}_q$ with $\#E(\mathbb{F}_q) = q + 1 - t$ (cf. [128, Theorem 4.1]). Conditions (2) and (4) combine to tell us that $E(\mathbb{F}_q)$ has a subgroup of prime order r. By Lemma 1.2.2, condition (5) is equivalent to E having embedding degree k with respect to r.

We now know that if such t, r, q can be constructed, then there exists an ordinary elliptic curve $E/\mathbb{F}_q$ with embedding degree k and an order-r subgroup. The characteristic polynomial of Frobenius for E is $x^2 - tx + q$, and thus condition (6) implies that $\mathrm{End}(E) \otimes \mathbb{Q} \cong \mathbb{Q}(\sqrt{-D})$. By Proposition 1.2.5, we may assume that $\mathrm{End}(E)$ is isomorphic to the ring of integers of $K = \mathbb{Q}(\sqrt{-D})$. We may thus compute the j-invariant of E as a root of the

Hilbert class polynomial for $\mathcal{O}_K$, modulo a prime over q. If the class number h_K of K is sufficiently small then this class polynomial can be constructed in a reasonable amount of time; in practice we can take $h_K < 10^5$ [35].

The equation in condition (6) is called the *CM equation*. We call the integer D the *CM discriminant* of $E/\mathbb{F}_q$; it is defined to be the square-free part of the nonnegative integer $4q - t^2$. (Other authors may define the CM discriminant to be negative, or to be the discriminant of the quadratic imaginary field $\mathbb{Q}(\sqrt{-D})$.) If we use condition (4) to write $q + 1 - t = hr$ for some positive integer h, then the CM equation is equivalent to

$$Dy^2 = 4hr - (t-2)^2. \tag{2.1}$$

We call h the *cofactor* of the pairing-friendly curve.

2.2.1 Families of pairing-friendly curves

For applications, we would like to be able to construct curves of specified bit size. To this end, we describe "families" of pairing-friendly curves for which the curve parameters t, r, q are given as polynomials $t(x), r(x), q(x)$ in terms of a parameter x. The idea of parametrizing t, r, q as polynomials has been used by several different authors in their constructions, including Miyaji, Nakabayashi, and Takano [93]; Barreto, Lynn, and Scott [8]; Scott and Barreto [113]; and Brezing and Weng [19]. Our definition of a family of pairing-friendly curves is a formalization of ideas implicit in these works. The definition provides a concise description of many existing constructions and gives us a framework that we can use to discover previously unknown pairing-friendly curves.

Since the values of $q(x)$ and $r(x)$ will be the sizes of a field and a group in which we wish to do cryptography, respectively, the polynomials we construct will need to have the property that for many values of x, $q(x)$ is a prime power (which in general we will take to be a prime) and $r(x)$ is prime or a small cofactor times a prime. However, one drawback to the description of q and r as polynomials is that very little is known about prime values of polynomials. For example, it is not even known that $x^2 + 1$ takes an infinite number of prime values. Thus when describing the polynomials that we wish to take prime values, we must impose conditions that make it likely that they will do so.

Our definition is motivated by the following fact: if $f(x) \in \mathbb{Z}[x]$, then a famous conjecture of Buniakowski and Schinzel (see [72, p. 323]) says that a non-constant $f(x)$ takes an infinite number of prime values if and only if f has positive leading coefficient, f is

irreducible, and $\gcd(\{f(x) : x \in \mathbb{Z}\}) = 1$. Furthermore, a conjecture of Bateman and Horn [10] vastly generalizes the prime number theorem to give the expected density of such prime values. For our purposes we must also consider polynomials with rational coefficients; our definition incorporates the natural generalization of these conjectures to such polynomials.

Definition 2.2.1. Let $f(x)$ be a polynomial with rational coefficients. We say f *represents primes* if the following conditions are satisfied:

1. $f(x)$ is non-constant.
2. $f(x)$ has positive leading coefficient.
3. $f(x)$ is irreducible.
4. $f(x) \in \mathbb{Z}$ for some $x \in \mathbb{Z}$ (equivalently, for an infinite number of $x \in \mathbb{Z}$).
5. $\gcd(\{f(x) : x, f(x) \in \mathbb{Z}\}) = 1$.

For future reference, we note that if there is some x such that $f(x) = \pm 1$, then conditions (4) and (5) are both satisfied. We need one more definition before we can define families of pairing-friendly curves.

Definition 2.2.2. A polynomial $f(x) \in \mathbb{Q}[x]$ is *integer-valued* if $f(x) \in \mathbb{Z}$ for every $x \in \mathbb{Z}$.

For example, $f(x) = \frac{1}{2}(x^2 + x + 2)$ is integer-valued and represents primes.

Definition 2.2.3. Let $t(x), q(x), r(x) \in \mathbb{Q}[x]$ be nonzero polynomials.

(i) For a given positive integer k and positive square-free integer D, the triple (t, r, q) *represents a family of elliptic curves with embedding degree k and discriminant D* if the following conditions are satisfied:

1. $q(x) = p(x)^d$ for some $d \geq 1$ and $p(x)$ that represents primes.
2. $r(x)$ is non-constant, irreducible, and integer-valued, and has positive leading coefficient.
3. $r(x)$ divides $q(x) + 1 - t(x)$.
4. $r(x)$ divides $\Phi_k(t(x) - 1)$, where Φ_k is the kth cyclotomic polynomial.
5. The equation $Dy^2 = 4q(x) - t(x)^2$ has infinitely many integer solutions (x, y).

If these conditions are satisfied, we often simply call (t, r, q) a *family*.

(ii) We say that a family (t, r, q) is *ordinary* if $\gcd(t(x), q(x)) = 1$.

(iii) We say that a family (t, r, q) is *complete* if for every integer x there is some integer y that satisfies the equation $Dy^2 = 4q(x) - t(x)^2$; otherwise we say that the family is *sparse*.

(iv) We say that (t, r, q) represents a *potential* family of curves if conditions (2)–(5) of (i) are satisfied; in this case $q(x)$ may or may not be a power of a $p(x)$ that represents primes.

Part (i) of Definition 2.2.3 is designed so that if (t, r, q) represents a family of curves with embedding degree k, and (x_0, y_0) is a solution to the equation of condition (5) such that $p(x_0)$ is prime, then there exists an elliptic curve $E/\mathbb{F}_{q(x_0)}$ with a subgroup of order $r(x_0)$ and embedding degree k. If the class number of $\mathbb{Q}(\sqrt{-D})$ is less than 10^5 then E can be constructed via the CM method. In practice we will usually have $d = 1$ in condition (1), so $q(x)$ will represent primes and the curves we construct will be defined over prime fields.

For cryptographic applications, we also need $r(x_0)$ to be prime or very nearly prime; the conditions (2) on $r(x)$ suggest that this will often be the case. We can then use the following algorithm to search for an x_0 with the desired properties.

Algorithm 2.2.4.

Input: polynomials $q(x)$ and $r(x) \in \mathbb{Q}[x]$ satisfying conditions (1) and (2) of Definition 2.2.3 (i), respectively, and a positive integer y_0.

Output: positive integers x_0 and h such that $q(x_0)$ is prime and $r(x_0)$ is h times a prime.

1. Compute integers a, b such that $q(ax + b)$ is integer-valued and represents primes.
2. Set $h \leftarrow \gcd(\{q(ax + b)r(ax + b) : x \in \mathbb{Z}\})$.
3. Set $\widetilde{r}(x) \leftarrow r(x)/h$.
4. Set $x_1 \leftarrow y_0$.
5. Repeat $x_1 \leftarrow x_1 + 1$ until $q(ax_1 + b)$ and $\widetilde{r}(ax_1 + b)$ are prime integers.
6. Set $x_0 \leftarrow ax_1 + b$. Return h and x_0.

The input y_0 is the starting point for the search, and should be chosen so that $r(y_0)/h$ is at least the minimum size desired for security. Since h does not depend on the input y_o, if the h output by the algorithm is too large we can try again with a larger y_0.

Proposition 2.2.5. *Suppose the $q(x)$ and $r(x)$ input into Algorithm 2.2.4 have degrees d_1 and d_2 respectively. If the Bateman-Horn conjecture [10] is true, then the expected running time of the algorithm is $O(d_1 d_2 (\log \alpha\delta y_0)^2)$, where δ is the smallest integer such that $\delta q(x) \in \mathbb{Z}[x]$ and $\alpha = \max\{q(x)r(x) : |x| \leq \delta/2\}$.*

Proof. We first show that integers a, b as in Step (1) always exist. Write $q(x) = \widetilde{q}(x)/\delta$; then $\widetilde{q}(x) \in \mathbb{Z}[x]$. Write the factorization of δ as

$$\delta = \prod_{p \text{ prime}} p^{e_p}.$$

Since $q(x)$ represents primes, for each p there exists a b_p such that $q(b_p)$ is an integer not divisible by p, and thus p^{e_p} divides $\widetilde{q}(b_p)$ exactly. Let a and b be integers such that

$$a = \prod_{p|\delta} p^{e_p+1}, \qquad b \equiv b_p \pmod{p^{e_p+1}} \text{ for all } p \mid \delta.$$

Then $q(ax+b)$ is integer-valued and is nonzero mod p for every p dividing δ. For every p not dividing δ, $ax+b$ ranges through all residue classes mod p, so there is some residue class of x mod p for which p does not divide $\widetilde{q}(ax+b)$. Thus there is no prime p dividing $q(ax+b)$ for all x, which is equivalent to $q(ax+b)$ representing primes.

Let h be as in Step (2). Since $q(ax+b)$ and $r(ax+b)$ are integer-valued and $q(ax+b)$ represents primes, there is some c such that

$$\begin{aligned} \gcd\left(\{q(ax+b) : x \equiv c \bmod h\}\right) &= 1, \\ \gcd\left(\{r(ax+b) : x \equiv c \bmod h\}\right) &= h. \end{aligned}$$

It follows that the values of the polynomials $q(ahx+ac+b)$ and $\widetilde{r}(ahx+ac+b)$ are integers with no common divisor. The Bateman-Horn conjecture implies that we should expect to test roughly $d_1 d_2 (\log ahy_0)^2$ values of x_1 before we find one for which $q(ax_1+b)$ is prime and $r(ax_1+b)$ is h times a prime. Since $\log a = O(\log \delta)$ and $h \leq \alpha$, the result follows. □

Proposition 2.2.5 shows that heuristically, the expected number of executions of Step (5) is linear in the degrees of q and r, and quadratic in the number of bits in y_0. We note

(and find in practice) that the a computed in Step (1) can be smaller than the a produced in the proof of the proposition, and that there may be multiple valid choices of b for a given a. In addition, the α of the statement is usually a gross overestimate.

Condition (3) of Definition 2.2.3 (i) ensures that for a given value x_0 for which $q(x_0)$ is prime, $r(x_0)$ divides $\#E(\mathbb{F}_{q(x_0)})$. If in fact $r(x_0) = q(x_0) + 1 - t(x_0)$, then for values of x for which $r(x_0)$ and $q(x_0)$ are both prime, $\#E(\mathbb{F}_q)$ will be prime. This is the "ideal" case, but it is difficult to achieve in practice. We therefore extend our definition of the parameter ρ (1.6) to indicate how close to this ideal a given family of curves is.

Recall that the ρ-value of a g-dimensional abelian variety over $\mathbb{F}_q$ with respect to a subgroup of order r is $\rho = g \log q / \log r$. If $q = q(x)$ and $r = r(x)$ are parametrized as polynomials, then for large x the ρ-value approaches $g \deg q / \deg r$. This analysis leads to the following definition of ρ-value for a family of elliptic curves:

Definition 2.2.6. Let $t(x), r(x), q(x) \in \mathbb{Q}[x]$, and suppose (t, r, q) represents a family of elliptic curves with embedding degree k. The *ρ-value of the family represented by* (t, r, q), denoted $\rho(t, r, q)$, is

$$\rho(t, r, q) = \lim_{x \to \infty} \frac{\log q(x)}{\log r(x)} = \frac{\deg q(x)}{\deg r(x)}.$$

The Hasse bound $|\#E(\mathbb{F}_q) - q + 1| \leq 2\sqrt{q}$ implies that $\rho(t, r, q)$ is always at least 1. (For individual curves, $\rho(E) \geq 1 - \frac{2 \log 2}{\log r}$.) If (t, r, q) represents curves of prime order, then $\deg r = \deg q$ and $\rho = 1$. Note, however, that the converse may not be true: if $\rho(t, r, q) = 1$, then we may find that for any curve E in this family $\#E(\mathbb{F}_q) = hr(x)$ where h is a constant-size cofactor. (For examples of such families, see [46, §3].)

We conclude this section by demonstrating some properties of ρ for ordinary elliptic curves with embedding degree 1 or 2.

Proposition 2.2.7. *Suppose (t, r, q) represents a family of ordinary elliptic curves with embedding degree $k \leq 2$ and discriminant D.*

1. *If $k = 1$, then $\rho(t, r, q) \geq 2$ if either of the following conditions holds:*
   - *(a)* $\deg t(x) \geq 1$, *or*
   - *(b) there are an infinite number of integer solutions (x, y) to the CM equation (2.1) for which $r(x)$ is square free and relatively prime to D.*
2. *If $k = 2$, then $\rho(t, r, q) \geq 2$.*

Proof. Since $r(x)$ divides $\Phi_k(t(x)-1)$ and $\deg \Phi_k = 1$, if $\Phi_k(t(x)-1) \neq 0$ then we must have $\deg t(x) \geq \deg r(x)$. Thus by the Hasse bound $\rho(t, r, q) \geq 2$. It remains to consider the cases $k = 1$, $t(x) = 2$ and $k = 2$, $t(x) = 0$. If $t(x) = 0$ then the family of curves is not ordinary, a contradiction. Now suppose $k = 1$ and $t(x) = 2$; then the CM equation (2.1) becomes $Dy^2 = 4h(x)r(x)$. The hypothesis (1b) implies that there are an infinite number of x for which $h(x) \geq r(x)$, and therefore $\deg h(x) \geq \deg r(x)$. Since $\deg q(x) = \deg h(x) + \deg r(x)$, we conclude that $\rho \geq 2$. □

Remark 2.2.8. Let $E/\mathbb{F}_q$ be an ordinary elliptic curve that has embedding degree $k \leq 2$ with respect to r, and let D be the CM discriminant of E. Using the same reasoning as in the proof of Proposition 2.2.7, one can show that if either

1. $k = 1$, r is square free, and $\gcd(r, D) = 1$, or
2. $k = 2$, and q and r are prime,

then $\rho(E) \geq 2(1 - \varepsilon)$, with $\varepsilon \to 0$ as $r \to \infty$.

2.2.2 Supersingular curves

Recall that an elliptic curve $E/\mathbb{F}_q$ with $\#E(\mathbb{F}_q) = q+1-t$ is *supersingular* if and only if $\gcd(t, q) > 1$. Supersingular curves have embedding degrees $k \in \{1, 2, 3, 4, 6\}$ [86], and furthermore $k = 2$ is the only possible embedding degree over prime fields $\mathbb{F}_q$ with $q \geq 5$. By the Hasse bound, group orders of supersingular curves are of the form $q + 1 - t$ with $t^2 \in \{0, q, 2q, 3q, 4q\}$.

The only known general method to construct supersingular curves is reduction of CM curves in characteristic zero. In particular, the CM curves $y^2 = x^3 + ax$ and $y^2 = x^3 + b$ defined over $\mathbb{Q}$ reduce to supersingular curves over $\mathbb{F}_p$ for all primes $p \equiv 3 \pmod 4$ and $p \equiv 2 \pmod 3$ respectively. These two curves will suffice for most applications; Algorithm 2.2.11 gives an explicit procedure for constructing a supersingular curve over any given prime field.

For fields of characteristic 2 and 3, representatives for each $\mathbb{F}_q$-isomorphism class of supersingular curves have been determined by Menezes and Vanstone [87] and Morain [95], respectively. Supersingular curves with $k = 4$ or 6 exist only in characteristic 2 and 3, respectively, and Menezes [84] has characterized prime-order supersingular curves in these cases. Thus we limit our discussion in this section to curves with $k \leq 3$.

Remark 2.2.9. Supersingular curves are commonly perceived as "weak" curves, and thus as not desirable for cryptographic applications. However, Koblitz and Menezes [68] argue:

> There is no known reason why a nonsupersingular curve with small embedding degree k would have any security advantage over a supersingular curve with the same embedding degree.

On the other hand, as opposed to ordinary curves with embedding degree $k > 1$, supersingular curves have the added advantage that they have distortion maps (in the sense of Verheul [125]), which is a desirable feature in some pairing-based applications [24].

Embedding degree $k = 1$

Supersingular curves with embedding degree $k = 1$ exist only over finite fields $\mathbb{F}_q$ where $q = p^s$ with s even. Then we can write $q - 1 = (\sqrt{q} + 1)(\sqrt{q} - 1)$, so $r \mid q - 1$ if $r \mid (\sqrt{q} + 1)$ or $r \mid (\sqrt{q} - 1)$. For a supersingular curve with $k = 1$ over $\mathbb{F}_q$, this requires $\#E(\mathbb{F}_q) = q \pm 2\sqrt{q} + 1$, that is, $t = \pm 2\sqrt{q}$ [45], and we see that such curves must have $\rho \geq 2$.

To construct supersingular curves with embedding degree 1, we let $q' = \sqrt{q}$ and let $E/\mathbb{F}_{q'}$ be a curve with trace zero, i.e., $\#E(\mathbb{F}_{q'}) = q' + 1$. Then the characteristic polynomial of the q'-power Frobenius endomorphism is $x^2 + q'$, which factors as $(x + i\sqrt{q'})(x - i\sqrt{q'})$. The Weil conjectures [117, Theorem V.2.2] then tell us that the characteristic polynomial of the q-power Frobenius map is $(x - q')^2$, so $\#E(\mathbb{F}_q) = (q' - 1)^2 = q - 2\sqrt{q} + 1$. Thus even though $E/\mathbb{F}_{q'}$ has embedding degree 2, if we consider E as a curve over $\mathbb{F}_q$ then E has embedding degree 1 with respect to r.

We will see in Section 2.2.2 how to construct a trace-zero curve over $\mathbb{F}_{q'}$ with an order-r subgroup for arbitrary r. Since we may take $\log q' / \log r$ arbitrarily close to 1 for such curves, the ρ-value for $E/\mathbb{F}_q$ with embedding degree 1 can be made arbitrarily close to 2, and we see from the discussion above that this is the best possible ρ-value. If for some reason we want our curve to have $q + 2\sqrt{q} + 1$ points, we may simply take a quadratic twist (over $\mathbb{F}_q$) of the curve with $q - 2\sqrt{q} + 1$ points.

We conclude that in any case where a supersingular curve $E/\mathbb{F}_q$ with $k = 1$ and $\rho(E) = \rho_0$ is desired, we may obtain an entirely equivalent setup by choosing a supersingular curve $E'/\mathbb{F}_{\sqrt{q}}$ with $k = 2$ and $\rho(E') = \rho_0/2$.

Embedding degree $k = 2$

The case of embedding degree 2 offers the most flexibility; in fact, we can construct curves over prime fields with arbitrary subgroup size and ρ-value. For embedding degree $k = 2$ we require $r \mid q + 1$. This is certainly the case if $t = 0$, and such supersingular curves can be defined over both prime and non-prime fields.

Construction of supersingular curves in characteristic greater than 3 makes use of the following theorem:

Theorem 2.2.10 ([71, Theorem 13.12])**.** *Let L be a number field, and E/L be an elliptic curve with complex multiplication. Suppose* $\mathrm{End}(E) \otimes \mathbb{Q} = \mathbb{Q}(\sqrt{-D})$*. Let $\mathfrak{p} \mid p$ be a prime of L where E has good reduction. Then the reduction of $E \mod \mathfrak{p}$ is supersingular if and only if $\mathfrak{p}$ does not split in $\mathbb{Q}(\sqrt{-D})$, i.e., $\left(\frac{-D}{p}\right) \neq 1$.*

Given a subgroup size r, if we choose any even h such that $q = hr - 1$ is prime, then we have the following algorithm (combining the constructions of Koblitz and Menezes [68, §7] and Bröker [21, §3.4]) for constructing a curve over $\mathbb{F}_q$ with embedding degree 2 with respect to r.

Algorithm 2.2.11.

Input: a prime $q \geq 5$.

Output: a supersingular elliptic curve $E/\mathbb{F}_q$.

1. If $q \equiv 3 \pmod 4$, return $y^2 = x^3 + ax$ for any $a \in \mathbb{F}_q^\times$.
2. If $q \equiv 5 \pmod 6$, return $y^2 = x^3 + b$ for any $b \in \mathbb{F}_q^\times$.
3. If $q \equiv 1 \pmod{12}$, do the following:
   (a) Let D be the smallest prime such that $D \equiv 3 \pmod 4$ and $\left(\frac{-D}{q}\right) = -1$.
   (b) Compute the Hilbert class polynomial H_D of $\mathbb{Q}(\sqrt{-D})$.
   (c) Compute a root $j \in \mathbb{F}_q$ of $H_D \pmod q$.
   (d) Let $m = j/(1728 - j)$, and return $y^2 = x^3 + 3mc^2x + 2mc^3$ for any $c \in \mathbb{F}_q^\times$. □

The condition $D \equiv 3 \pmod 4$ in Step (3a) guarantees that the Hilbert class polynomial H_D has a root in $\mathbb{F}_q$ [21, §3.4]. Note that this construction allows us to choose r and h almost completely arbitrarily, so we may make our choices so that r has low Hamming

weight or some other special form. In particular, Boneh, Goh, and Nissim [16] observe that we may choose r to be a large composite number such as an RSA modulus; curves with such group orders are used in some recent pairing-based protocols.

We see from Theorem 2.2.10 that the popular supersingular curves $y^2 = x^3 + ax$ and $y^2 = x^3 + b$ are simply special cases of the general construction method, for the two equations define CM curves over $\mathbb{Q}$ with CM discriminant 1 and 3, respectively. However, these two cases have the additional nice property that the distortion maps are easy to compute, as both curves have automorphisms defined over $\mathbb{F}_{q^2}$. Koblitz and Menezes [68] give explicit determinations of the distortion maps in both cases.

Embedding degree $k = 3$

A supersingular curve over $\mathbb{F}_q$ of prime order has embedding degree $k = 3$ if and only if $q = p^s$ with s even, and $t = \pm\sqrt{q}$ [93]. In characteristic $p > 3$, the only such curves are those of the form

$$y^2 = x^3 + \gamma,$$

where γ is a non-cube in $\mathbb{F}_q^\times$ [95]. If we specialize to the case $q = p^2$ where $p \equiv 2 \pmod 3$ is a large prime, then we have $\#E(\mathbb{F}_{p^2}) = p^2 \pm p + 1$. If the sign of the middle term is positive (i.e., $t = -p$), then for certain $p = 3x - 1$ we may find curves of prime order, since $r(x) = (3x-1)^2 + (3x-1) + 1$ represents primes in the sense of Definition 2.2.1. In the case where $t = p$ we find that $\#E(\mathbb{F}_q)$ must be a multiple of 3 and can be equal to 3 times a prime.

We can recast these results in our language of "families" (Definition 2.2.3). Depending on the sign of t we have one of

$$\begin{aligned} t(x) &= -3x + 1, \quad r(x) = 9x^2 - 3x + 1, \quad q(x) = (3x-1)^2; \\ t(x) &= 3x - 1, \quad r(x) = 9x^2 - 9x + 3, \quad q(x) = (3x-1)^2. \end{aligned}$$

Since $4q(x) - t(x)^2 = 3(3x-1)^2$, the triple (t, r, q) represents a family of elliptic curves with embedding degree 3 and discriminant 3. The ρ-value for this family is 1; in particular, if $r(x)$ and $3x - 1$ are prime then we may construct a curve over $\mathbb{F}_{q(x)}$ with embedding degree 3 and prime order.

Since arithmetic in $\mathbb{F}_{p^2}$ for suitably chosen p can be as fast as arithmetic in $\mathbb{F}_{p'}$ with $p' \approx p^2$, this is a good method for generating useful curves with embedding degree 3 and

small ρ-value. Note that particularly fast $\mathbb{F}_{p^2}$ arithmetic results when optimal extension fields [4] are used; Duan, Cui and Chan [31] give sample families and curves for this setup.

2.3 Generating ordinary elliptic curves with arbitrary embedding degree

We begin our survey of methods for constructing pairing-friendly ordinary elliptic curves with the two most general methods in the literature, the Cocks-Pinch method and the Dupont-Enge-Morain method. Both methods can be used to construct curves with arbitrary embedding degree; however, both methods produce curves with $\rho \approx 2$, which may not be suitable for certain applications. Neither method produces families of curves in the sense of Definition 2.2.3, but we will see in Section 2.5 that the Cocks-Pinch method does generalize to produce families with $\rho < 2$. Furthermore, the Cocks-Pinch method has the advantage that it can produce curves with prime-order subgroups of nearly arbitrary size. The subgroups of Dupont-Enge-Morain curves, on the other hand, must have an order r that divides a value of a certain polynomial, which results in the value of r being more difficult to specify precisely.

2.3.1 The Cocks-Pinch method

In an unpublished manuscript [25], Cocks and Pinch gave a procedure for constructing pairing-friendly curves with arbitrary embedding degree k. The Cocks-Pinch method fixes a subgroup size r and a CM discriminant D and computes t such that the CM equation must be satisfied.

Theorem 2.3.1 ([25]). *Fix a positive integer k and a positive square-free integer D. Execute the following steps.*

1. *Let r be an odd prime such that $k \mid r-1$ and $\left(\frac{-D}{r}\right) = 1$.*
2. *Let z be a kth root of unity in $(\mathbb{Z}/r\mathbb{Z})^\times$. (Such a z exists because $k \mid r-1$.) Let $t' = z + 1$.*
3. *Let $y' = (t'-2)/\sqrt{-D} \pmod{r}$.*
4. *Let t be the unique lift of t' to $(0, r]$, and let y be the unique lift of y' to $(0, r]$. Let $q = (t^2 + Dy^2)/4$.*

If q is an integer and prime, then there exists an elliptic curve E over $\mathbb{F}_q$ with an order-r subgroup and embedding degree k. If the class number of $\mathbb{Q}(\sqrt{-D})$ is less than 10^5 then E can be constructed via the CM method.

The key feature of this algorithm is that y is constructed so that $Dy^2 + (t-2)^2$ is divisible by r. With q chosen such that the CM equation $4q - t^2 = Dy^2$ is satisfied, this yields $4(q+1-t) \equiv 0 \mod r$. Lastly, the choice of t ensures that $\Phi_k(t-1) \equiv 0 \mod r$.

We observe that there is no reason to believe *a priori* that we can find a t or y that is much smaller than r, and thus in general we find that $q \approx r^2$. We conclude that the curves produced by this method tend to have ρ-values around 2. However, these curves are easy to generate, and in particular we can take r to be (nearly) arbitrary, so r can have low Hamming weight or other desirable features.

The Cocks-Pinch method is important not only because it is the most flexible algorithm for constructing ordinary pairing-friendly curves, but also because it can be generalized to produce families of elliptic curves with $\rho < 2$ (Section 2.5) and higher-dimensional pairing-friendly abelian varieties (Chapter 4).

Remark 2.3.2. In Step (4) we could in fact choose t and y to be *any* integers congruent to t' and y' modulo r. In particular, if we wish to generate a curve with a given ρ-value $\rho_0 \geq 2$, we could add to t and y an integer divisible by r and of size roughly $r^{\rho_0/2}$.

Remark 2.3.3. Rubin and Silverberg [107] have observed that the Cocks-Pinch method can be used to construct curves with embedding degree k with respect to r when r is a large composite number, such as an RSA modulus. As in the case where r is prime, these curves have ρ-value around 2.

2.3.2 The Dupont-Enge-Morain method

Whereas the Cocks-Pinch method fixes an r and then computes t and q such that the CM equation is satisfied, the approach of Dupont, Enge, and Morain [32] is to compute t and r simultaneously using resultants. The theory of resultants is discussed in [72, §IV.8].

Theorem 2.3.4 ([32])**.** *Fix a positive integer k, and execute the following steps.*

1. *Compute the resultant*

$$R(a) = \mathrm{Res}_x(\Phi_k(x-1), a + (x-2)^2).$$

2. *Choose a such that $a = Dy^2$ with D square-free, and let r be the largest prime factor of $R(a)$.*

3. *Compute $g(x) = \gcd(\Phi_k(x-1), a + (x-2)^2)$ in $\mathbb{F}_r[x]$.*

4. *Let $t' \in \mathbb{F}_r$ be a root of the polynomial g. If there is no such root, go to Step (2) and choose a different a.*

5. *Let t be the unique lift of t' to $(0, r]$. Let $q = (t^2 + a)/4$.*

If q is an integer and prime, then there exists an elliptic curve E over $\mathbb{F}_q$ with an order-r subgroup and embedding degree k. If the class number of $\mathbb{Q}(\sqrt{-D})$ is less than 10^5 then E can be constructed via the CM method.

The key idea of the Dupont-Enge-Morain method is to use the following property of resultants [72, Corollary IV.8.4]: if $f(x)$ and $g(x)$ are polynomials over a field K, then $\mathrm{Res}_x(f(x), g(x)) = 0$ if and only if $f(x)$ and $g(x)$ have a common root in $\overline{K}$. If we consider $\Phi_k(x-1)$ and $a + (x-2)^2$ to be polynomials in the two variables a, x, then the resultant R is a single-variable polynomial in a of degree $\varphi(k)$. If we fix a and take r to be a prime factor of $R(a)$, then $R(a) \equiv 0 \pmod{r}$, and thus $\Phi_k(x-1)$ and $a + (x-2)^2$ have a common factor $g(x)$ when considered as polynomials mod r, i.e., in $\mathbb{F}_r[x]$. In practice we find that if k is small and r is of cryptographic size then the factor $g(x)$ is linear, so we can find a root $t' \in \mathbb{F}_r$ that lifts to an integer t. The values of t and r computed thus satisfy $r \mid \Phi_k(t-1)$ and $r \mid Dy^2 + (t-2)^2$. By construction of q, the CM equation holds, which then yields $q + 1 - t \equiv 0 \pmod{r}$.

We observe that there is again no reason to believe *a priori* that t is much smaller than r, and thus in general we find that $q \approx r^2$. We conclude that the curves produced by this method also tend to have ρ values around 2.

Like the Cocks-Pinch method, the Dupont-Enge-Morain method is effective for computing curves for arbitrary embedding degree k. However, whereas in the former method we could choose the subgroup size r nearly arbitrarily, in this method r is a factor of a value of the polynomial $R(a)$. Since r must be of cryptographic size, it will usually only be computationally feasible to find such an r if the remaining factors of $R(a)$ are small, so in general r will be roughly the size of $R(a)$. Since $R(a)$ has degree $\varphi(k)$ and is irreducible (because it is the resultant of two irreducible polynomials), the factors r we find will grow roughly like $a^{\varphi(k)}$. Thus the possible subgroup orders r are more restricted in the Dupont-Enge-Morain

method than in the Cocks-Pinch method. This is the only significant difference between the two methods, and thus we recommend using the Cocks-Pinch method for applications where a curve with arbitrary embedding degree and $\rho \approx 2$ is desired.

2.4 Sparse families of pairing-friendly curves

Recall that to construct families of pairing-friendly curves, we search for polynomials $t(x), r(x), q(x)$ that satisfy certain divisibility conditions modulo $r(x)$, and for which the CM equation

$$Dy^2 = 4q(x) - t(x)^2 = 4h(x)r(x) - (t(x) - 2)^2 \tag{2.2}$$

has infinitely many solutions (x, y). Here, $h(x)$ is the "cofactor" satisfying

$$h(x)r(x) = q(x) + 1 - t(x).$$

In practice, for any $t(x)$ we can easily find $r(x)$ and $q(x)$ satisfying the divisibility conditions modulo $r(x)$; the difficulty arises in choosing the polynomials so that $Dy^2 = 4q(x) - t(x)^2$ has infinitely many integer solutions. In general, if $f(x)$ is a square-free polynomial of degree at least 3, then there will be only a finite number of integer solutions to the equation $Dy^2 = f(x)$ (cf. Proposition 2.4.5 below). Thus we conclude that (t, r, q) can represent a family of curves only if $f(x)$ has some kind of special form.

We now consider one of these special forms: namely, the case where $f(x)$ is quadratic. We show that in this case, one integral solution to the equation $Dy^2 = f(x)$ will give us infinitely many solutions. This is the technique that Miyaji, Nakabayashi and Takano [93] use to produce curves with embedding degree 3, 4, or 6, and we will use the same technique in Section 3.1 to construct curves with embedding degree 10.

The idea is as follows: since $f(x)$ is quadratic, we complete the square to write the equation $Dy^2 = f(x)$ as $u^2 - D'v^2 = T$ for some constants D' and T, and observe that (u, v) is a solution to this equation if and only if $u + v\sqrt{D'}$ has norm T in the real quadratic field $\mathbb{Q}(\sqrt{D'})$. By Dirichlet's unit theorem, there is a one-dimensional set of norm-one integral elements of this field; multiplying each of these units by our element of norm T gives an infinite family of elements of norm T. We then show that a certain fraction of these elements can be converted back to solutions of the original equation.

Theorem 2.4.1. *Fix an integer $k > 0$, and suppose the polynomials $t(x)$, $r(x)$, $q(x) \in \mathbb{Q}[x]$ satisfy conditions (1)–(4) of Definition 2.2.3 (i). Let $f(x) = 4q(x) - t(x)^2$. Suppose $f(x) =$*

$ax^2 + bx + c$, with $a, b, c \in \mathbb{Z}$, $a > 0$, and $b^2 - 4ac \neq 0$. Let D be a square-free integer such that aD is not a square. If the equation $Dy^2 = f(x)$ has an integer solution (x_0, y_0), then (t, r, q) represents a family of curves with embedding degree k.

Proof. Completing the square in the equation $Dy^2 = f(x)$ and multiplying by $4a$ gives

$$aD(2y)^2 = (2ax + b)^2 - (b^2 - 4ac).$$

If we write $aD = D'w^2$ with D' square-free and make the substitutions $u = 2ax+b$, $v = 2wy$, $T = b^2 - 4ac$, the equation becomes

$$u^2 - D'v^2 = T. \tag{2.3}$$

Note that since aD is not a square, we have $D' > 1$.

Under the above substitution, a solution (x_0, y_0) to the original equation $Dy^2 = f(x)$ gives an element $u_0 + v_0\sqrt{D'}$ of the real quadratic field $\mathbb{Q}(\sqrt{D'})$ with norm T. Furthermore, this solution satisfies the congruence conditions

$$\begin{aligned} u_0 &\equiv b \pmod{2a} \\ v_0 &\equiv 0 \pmod{2w}. \end{aligned} \tag{2.4}$$

We wish to find an infinite set of solutions (u, v) satisfying the same congruence conditions, for we can transform such a solution into an integer solution to the original equation. To find such solutions we employ Dirichlet's unit theorem [98, §1.7], which tells us that the integer solutions to the equation $\alpha^2 - D'\beta^2 = 1$ are in one-to-one correspondence with the real numbers

$$\alpha + \beta\sqrt{D'} = \pm(\alpha_0 + \beta_0\sqrt{D'})^n$$

for some fixed (α_0, β_0) and any integer n. The real number $\alpha_0 + \beta_0\sqrt{D'}$ is either a fundamental unit of the real quadratic field $\mathbb{Q}(\sqrt{D'})$ or (if the norm of the fundamental unit is -1) the square of a fundamental unit.

Reducing the coefficients of $\alpha_0 + \beta_0\sqrt{D'}$ modulo $2a$ gives an element z of the ring

$$R = \frac{\mathbb{Z}[x]}{(2a, x^2 - D')}.$$

Furthermore, since $(\alpha_0 + \beta_0\sqrt{D'})(\alpha_0 - \beta_0\sqrt{D'}) = 1$, z is invertible in R, i.e., $z \in R^\times$. Since $R^\times$ is a finite group of size less than $4a^2$, there is an integer $m < 4a^2$ such that $z^m = 1$ in

$R^\times$.[†] Lifting back up to the full ring $\mathbb{Z}[\sqrt{D'}]$, we see that $(\alpha_0 + \beta_0\sqrt{D'})^m = \alpha_1 + \beta_1\sqrt{D'}$ for integers α_1, β_1 satisfying

$$\begin{aligned} \alpha_1 &\equiv 1 \pmod{2a}, \\ \beta_1 &\equiv 0 \pmod{2a}. \end{aligned} \tag{2.5}$$

Now for any integer n we can compute integers (u, v) such that

$$u + v\sqrt{D'} = (u_0 + v_0\sqrt{D'})(\alpha_1 + \beta_1\sqrt{D'})^n. \tag{2.6}$$

We claim that (u, v) satisfy the congruence conditions (2.4). To see this, let $\alpha_n + \beta_n\sqrt{D'} = (\alpha_1 + \beta_1\sqrt{D'})^n$. The conditions (2.5) imply that $\alpha_n \equiv 1 \pmod{2a}$ and $\beta_n \equiv 0 \pmod{2a}$. Combining this observation with the formulas

$$\begin{aligned} u &= \alpha_n u_0 + \beta_n v_0 D' \\ v &= \alpha_n v_0 + \beta_n u_0, \end{aligned}$$

we see that $u \equiv u_0 \equiv b \pmod{2a}$ and $v \equiv v_0 \pmod{2a}$. Furthermore, $v_0 \equiv 0 \pmod{2w}$ and $2w$ divides $2a$ (since $aD = D'w^2$ and D is square free), so we conclude that $v \equiv 0 \pmod{2w}$.

The new solution (u, v) thus satisfies the congruence conditions (2.4). Any integer n gives such a solution, so by setting $x = (u - b)/2a$ and $y = v/2w$ for each such (u, v), we have generated an infinite number of integer solutions to the equation $Dy^2 = f(x)$. This is condition (5) of Definition 2.2.3 (i); by hypothesis (t, r, q) satisfy conditions (1)–(4), so we conclude that (t, r, q) represents a family of curves with embedding degree k. □

Remark 2.4.2. More generally, we may find an infinite family of curves in the case where $f(x) = g(x)^2 h(x)$, with $h(x)$ quadratic. Specifically, if we let $y = y'g(x)$, then given one integral solution (x, y') to the equation $Dy'^2 = h(x)$ we may use the method of Theorem 2.4.1 to find an infinite number of solutions. However, we currently know of no examples for which $f(x)$ is of this form.

Remark 2.4.3. We see from (2.6) that solutions to the Pell equation (2.3) grow exponentially, and thus only very few values of x satisfy our original equation $Dy^2 = f(x)$. (Indeed, even the smallest solution will be exponential in the bit size of D [75].) Thus the families of Theorem 2.4.1 will be sparse (in the sense of Definition 2.2.3).

[†]In fact, since z is an element of the norm-one subgroup of $R^\times$, m is bounded above by $2^s a$, where s is the number of distinct primes dividing $2a$. A more detailed study of the group $R^\times$ appears in [36].

Remark 2.4.4. The argument in the proof of Theorem 2.4.1 can easily be made into an algorithm for finding x and y, using for example using one of the techniques described by Matthews [83] or Robertson [105] to find a fundamental solution to the equation (2.3), and using the continued fraction expansion of $\sqrt{D'}$ to find the fundamental unit (or its square) $\alpha_0 + \beta_0\sqrt{D'}$ [75].

Theorem 2.4.1 tells us that if $f(x)$ is quadratic and square free, we obtain a family of curves of the prescribed embedding degree for *each* D. If $f(x)$ is instead a linear or constant function times a square, then we obtain a family of curves for a single D. In this case the family is complete (in the sense of Definition 2.2.3), and such examples belong in the discussion of Section 2.5.

We conclude this section with a partial converse to Theorem 2.4.1; namely, if the degree of $f(x)$ is at least 3, then we are unlikely to find an infinite family of curves.

Proposition 2.4.5. *Let (t, r, q) be polynomials with integer coefficients satisfying conditions (1)–(4) of Definition 2.2.3, and let $f(x) = 4q(x) - t(x)^2$. Suppose $f(x)$ is square free and $\deg f(x) \geq 3$. Then (t, r, q) does not represent a family of elliptic curves with embedding degree k.*

Proof. Since $f(x)$ is square free (i.e., has no double roots) and has degree at least 3, the equation $Dy^2 = f(x)$ defines a smooth affine plane curve of genus $g \geq 1$. By Siegel's Theorem [117, Theorem IX.4.3] such curves have a finite number of integral points, so condition (5) of Definition 2.2.3 is not satisfied. □

2.4.1 MNT curves

Miyaji, Nakabayashi and Takano [93] were the first to propose ordinary pairing-friendly curves, for embedding degrees $k = 3$, 4, and 6. In fact, ordinary curves of prime order with embedding degrees 3, 4, or 6 have been fully characterized as follows:

Theorem 2.4.6 ([93])**.** *Let q be a prime and $E/\mathbb{F}_q$ be an ordinary elliptic curve such that $r = \#E(\mathbb{F}_q)$ is prime. Let $t = q + 1 - r$.*

1. *Assume $q > 64$. E has embedding degree $k = 3$ if and only if there exists $x \in \mathbb{Z}$ such that $t = -1 \pm 6x$ and $q = 12x^2 - 1$.*

2. *Assume $q > 36$. E has embedding degree $k = 4$ if and only if there exists $x \in \mathbb{Z}$ such that $t = -x$ or $t = x + 1$, and $q = x^2 + x + 1$.*

3. *Assume $q > 64$. E has embedding degree $k = 6$ if and only if there exists $x \in \mathbb{Z}$ such that $t = 1 \pm 2x$ and $q = 4x^2 + 1$.*

In all three cases, the proof (of the "only if" part) of Theorem 2.4.6 starts out with the condition $r \mid \Phi_k(q)$ and exploits the primality of the group order. All of the proofs are entirely elementary.

Remark 2.4.7. It is easy to show (see [63]) that if both r and q are primes greater than 64 then there is an elliptic curve $E/\mathbb{F}_q$ with embedding degree 6, discriminant D, and $\#E(\mathbb{F}_q) = r$ if and only if there is an elliptic curve $E'/\mathbb{F}_r$ with embedding degree 4, discriminant D, and $\#E'(\mathbb{F}_r) = q$.

In all three cases of Theorem 2.4.6, the CM equation $Dy^2 = 4q(x) - t(x)^2$ defines a curve of genus zero, with the right-hand side being quadratic in x. In each case, by a linear change of variables, the CM equation can be transformed into a generalized Pell equation of the form (2.3). Specifically,

1. for $k = 3$, setting $u = 6x \pm 3$ and $v = y$ yields $u^2 - 3Dv^2 = 24$,
2. for $k = 4$, setting $u = 3x + 2$ (if $t = -x$) or $u = 3x + 1$ (if $t = x + 1$), and $v = y$ yields $u^2 - 3Dv^2 = -8$, and
3. for $k = 6$, setting $u = 6x \mp 1$ and $v = y$ yields $u^2 - 3Dv^2 = -8$.

(The signs in (1) and (3) are to match those in Theorem 2.4.6.) We can then find solutions (x, y) (if any exist) using the procedure of Theorem 2.4.1 (cf. Remark 2.4.4).

Now, the *MNT strategy* for generating ordinary elliptic curves of prime order with embedding degree $k = 3$, 4, or 6 is the following: repeatedly select small discriminants D and compute solutions (u, v) to equation (2.3) (with $T = 24$ or $T = -8$) until the corresponding $q = q(x)$ and $r = q(x) + 1 - t(x)$ are primes of the desired bit length. Then there exists an elliptic curve over $\mathbb{F}_q$ with r points and embedding degree 3, 4, or 6, respectively, which can be constructed via the CM method.

The search for MNT curves can be sped up slightly by noting that if $k = 3$, it is necessary that $D \equiv 19 \pmod{24}$ [93], and if $k = 4$ or 6 then necessarily $D \equiv 3 \pmod 8$ and $D \not\equiv 5 \pmod{10}$. Also, T must be a quadratic residue modulo $3D$ in all cases.

The major downside of MNT curves is that (as noted in Remark 2.4.3) the families obtained are sparse. In fact, Luca and Shparlinski [80, 81] give a heuristic argument that

for any upper bound $\overline{D}$, there exist only a finite number of MNT curves with discriminant $D \leq \overline{D}$, with no bound on the field size! On the other hand, specific sample curves of cryptographic interest have been found, such as MNT curves of 160-bit, 192-bit, or 256-bit prime order (see, for example, [101] and [112]).

2.4.2 Extensions of the MNT strategy

The MNT strategy has been extended by Scott and Barreto [113], and by Galbraith, McKee and Valença [46], by allowing a small constant-size cofactor h.

Starting out with (2.2), Scott and Barreto [113] fix small integers h and d and substitute $r = \Phi_k(t-1)/d$ and $t = x+1$, to obtain the equation

$$Dy^2 = 4h\frac{\Phi_k(x)}{d} - (x-1)^2. \tag{2.7}$$

As the right-hand side is quadratic in x for $k = 3$, 4, or 6, just as with MNT curves we can transform (2.7) into a generalized Pell equation of the form (2.3) by an appropriate linear substitution of x. Subsequently, the MNT strategy can be applied to find curves with embedding degrees $k = 3$, 4, or 6 of almost-prime order.

Galbraith, McKee and Valença [46] give a complete characterization of curves with embedding degree $3, 4$ and 6 with cofactors $2 \leq h \leq 5$. This is achieved by mimicking the Miyaji-Nakabayashi-Takano proof of Theorem 2.4.6, but substituting hr for $\#E(\mathbb{F}_q)$, followed by an explicit (but tedious) analysis for $h = 2, 3, 4, 5$. Just as in the prime-order case, all resulting parametrizations for t are linear in x, and all resulting parametrizations for q are quadratic in x, so that the resulting CM equations $Dy^2 = 4q(x) - t(x)^2$ are quadratic in x and allow for a transformation into generalized Pell equations.

Given the nature of the solutions of Pell equations, we once again obtain sparse families.

2.5 Complete families of pairing-friendly curves

Once again, we start out with the CM equation

$$Dy^2 = 4q(x) - t(x)^2 = 4h(x)r(x) - (t(x)-2)^2 \tag{2.8}$$

and search for polynomials $t(x), r(x), q(x)$ that satisfy certain divisibility conditions and for which the CM equation has infinitely many solutions (x, y). The constructions in this section work by choosing the parameters $D, t(x), r(x), q(x)$ such that the right-hand side of

the CM equation is always D times a perfect square, and thus the equation is satisfied for every integer x. These constructions thus give complete families of curves in the sense of Definition 2.2.3.

There are two principal strategies for constructing complete families, one due to Scott and Barreto [113] and the other due originally to Barreto, Lynn, and Scott [8], and in its fullest generality to Brezing and Weng [19]. Both start in the same way: fix an embedding degree k, choose an irreducible polynomial $r(x) \in \mathbb{Z}[x]$ such that $K = \mathbb{Q}[x]/(r(x))$ is a number field containing the kth roots of unity, and then choose $t(x)$ to be a polynomial mapping to $1 + \zeta_k$, where ζ_k is a primitive kth root of unity in K.

At this point the two strategies diverge. Brezing and Weng use the fact that if K contains a square root of $-D$, then since $r(x) = 0$ in K, we can factor the CM equation (2.8) in K as

$$\left(t(x) - 2 + y\sqrt{-D}\right)\left(t(x) - 2 - y\sqrt{-D}\right) \equiv 0 \mod r(x).$$

Since $t(x) \mapsto \zeta_k + 1 \in K$, it now becomes clear that if we choose $y(x)$ to be a polynomial mapping to $(\zeta_k - 1)/\sqrt{-D}$ in K, then the CM equation is automatically satisfied for any x.

If we do not know that K contains an element of the form $\sqrt{-D}$ for some D, then we may apply the Scott-Barreto strategy. This strategy is to take the $t(x)$ and $r(x)$ from above and search (usually via computer) for cofactors $h(x)$ that make the right-hand side of the CM equation (2.8) either a perfect square or a linear factor times a perfect square. The CM equation then becomes

$$Dy^2 = (ax + b)g(x)^2.$$

If $a = 0$ then we take $D = b$ and $y = g(x)$. If $a > 0$, we may choose any D and make the substitution $x \mapsto \frac{Dz^2 - b}{a}$. If we then set $y = zg(x)$, the CM equation is automatically satisfied for any z.

In both cases we finish by constructing $q(x)$ as

$$q(x) = \frac{1}{4}\left(t(x)^2 + Dy(x)^2\right).$$

If $q(x)$ represents primes and $r(x)$ has positive leading coefficient, then (t, r, q) represents a complete family of pairing-friendly curves.

The success of either strategy depends heavily on the choice of number field K. The obvious choice is to set K to be a cyclotomic field $\mathbb{Q}(\zeta_\ell)$ for some ℓ that is a multiple of

k, and define $r(x)$ to be the ℓth cyclotomic polynomial $\Phi_\ell(x)$. Then K contains the kth roots of unity. Furthermore, it is a standard result of the theory of cyclotomic fields that K contains $\sqrt{-1}$ if $4 \mid \ell$, K contains $\sqrt{-2}$ if $8 \mid \ell$, and K contains $\sqrt{(\frac{-1}{p})p}$ for any odd prime p dividing ℓ. Thus, for any k and D we can use a cyclotomic field in the Brezing-Weng construction; see Murphy and Fitzpatrick's work [96] for more details. We call families constructed in this manner "cyclotomic families," and we discuss some of the most efficient constructions in Section 2.5.1 below.

We may achieve even better success by choosing K to be a (perhaps trivial) extension of a cyclotomic field, with $r(x)$ not a cyclotomic polynomial. There are two ways of creating such an extension. The first is to make the substitution $x \mapsto u(x)$ for some polynomial u. If $\Phi_\ell(u(x))$ is irreducible we have gained nothing, but if $\Phi_\ell(u(x))$ factors as $r_1(x)r_2(x)$ with r_1 irreducible, then we may set $K = \mathbb{Q}[x]/(r_1(x))$. Then K is a field containing the ℓth roots of unity, and $u(x)$ maps to an ℓth root of unity in K. If we know that $\sqrt{-D} \in \mathbb{Q}(\zeta_\ell)$, then $\sqrt{-D} \in K$ as well, and we may use the Brezing-Weng construction; otherwise we may apply the Scott-Barreto construction.

The second method, due to Kachisa, Schaefer, and Scott [62] is to find a non-cyclotomic polynomial $r(x)$ such that $K = \mathbb{Q}[x]/(r(x))$ is isomorphic to the cyclotomic field $\mathbb{Q}(\zeta_\ell)$. Such a polynomial $r(x)$ can be computed as the minimal polynomial of a random element of $\mathbb{Q}(\zeta_\ell)$. Given this $r(x)$, we can find a polynomial $t(x)$ mapping to $1 + \zeta_k$ in K and proceed as in the Brezing-Weng method.

Since nontrivial factorizations of $\Phi_\ell(u(x))$ are rare for random $u(x)$ and, furthermore, the $q(x)$ produced by the Kachisa-Schaefer-Scott technique do not usually represent primes, we will call families of curves obtained by either of these techniques "sporadic" families; they are discussed in Section 2.5.2 below. Although such families are rare, they may have better ρ-values than curves constructed using a cyclotomic field. This was most spectacularly demonstrated by Barreto and Naehrig [9], who used this method to construct curves of prime order with embedding degree 12 (Example 2.5.7 below).

2.5.1 Cyclotomic families

Barreto, Lynn, and Scott [8], and independently, Brezing and Weng [19], both observed that if we apply the Cocks-Pinch method but parametrize t, r, q as polynomials, then we can improve on this value of ρ. Brezing and Weng stated the construction in greatest generality;

their theorem is below.

Theorem 2.5.1 ([19]). *Fix a positive integer k and a positive square-free integer D. Execute the following steps.*

1. *Find an irreducible polynomial $r(x) \in \mathbb{Z}[x]$ with positive leading coefficient such that $K = \mathbb{Q}[x]/(r(x))$ is a number field containing $\sqrt{-D}$ and the cyclotomic field $\mathbb{Q}(\zeta_k)$.*
2. *Choose a primitive kth root of unity $\zeta_k \in K$.*
3. *Let $t(x) \in \mathbb{Q}[x]$ be a polynomial mapping to $\zeta_k + 1$ in L.*
4. *Let $y(x) \in \mathbb{Q}[x]$ be a polynomial mapping to $(\zeta_k - 1)/\sqrt{-D}$ in L. (So, if $s(x)$ maps to $\sqrt{-D}$ then $y(x) \equiv (2 - t(x))s(x)/D \bmod r(x)$.)*
5. *Let $q(x) \in \mathbb{Q}[x]$ be given by $(t(x)^2 + Dy(x)^2)/4$.*

If $q(x)$ represents primes, then the triple $(t(x), r(x), q(x))$ represents a family of curves with embedding degree k and discriminant D.

The ρ-value for this family (Definition 2.2.6) is

$$\rho(t, r, q) = \frac{2 \max\{\deg t(x), \deg y(x)\}}{\deg r(x)}.$$

Since we can always choose $t(x)$ and $y(x)$ to have degree strictly less than $r(x)$, we see that this method can produce families with ρ-values strictly less than 2. In general, we expect the smallest possible degree for $t(x)$ and $y(x)$ to be $\deg(r) - 1$, so ρ will not be much less than 2. However, for certain clever choices of the number field K, we may construct polynomials t and y with smaller degree, thus improving the ρ-value. We will now examine in detail some constructions for certain sets of k.

Barreto, Lynn, and Scott [8] gave the first construction along the lines of Theorem 2.5.1. They construct families by taking the polynomial $r(x)$ defining the number field K to be the kth cyclotomic polynomial, choosing $\zeta_k \mapsto x$ in K (so $t(x) = 1 + x$),[†] and using the fact that if k is divisible by 3 then $\sqrt{-3} \in K$. Brezing and Weng [19] set $r(x)$ to be a cyclotomic polynomial $\Phi_\ell(x)$ for some ℓ that is a multiple of the desired embedding degree k and choosing various representatives for ζ_k in $\mathbb{Q}[x]/(r(x))$. The discriminants D in these

[†]Here and in the following examples, for $\alpha \in K$ and $f(x) \in \mathbb{Q}[x]$ we use the notation $\alpha \mapsto f(x)$ to mean that $f(x)$ represents α in $K = \mathbb{Q}[x]/(r(x))$.

constructions are often taken to be 1 or 3. The tricky part of most of these constructions is ensuring that the resulting $q(x)$ represents primes.

The constructions we present in this section are generalizations of constructions already existing in the literature. Construction 2.5.2 is based on an example of Brezing and Weng [19, §3, Example 3], while Constructions 2.5.3 and 2.5.4 adapt this example to even embedding degrees k. Construction 2.5.5 generalizes examples of Brezing and Weng [19, §3, Example 4] and Barreto, Lynn, and Scott [8, §3.1]. Finally, Construction 2.5.6 generalizes examples of Brezing and Weng [19, §3, Example 5] and Murphy and Fitzpatrick [96, Example 2.2.2 and §4.4].

We begin with a construction given by Brezing and Weng, who state the construction for prime embedding degrees k; we observe that the construction extends readily to all odd k. We choose K to be a cyclotomic field containing a fourth root of unity $\sqrt{-1}$, so we may choose $D = 1$.

Construction 2.5.2 ([19])**.** Let k be odd, and let $r(x) = \Phi_{4k}(x)$, so $K = \mathbb{Q}[x]/(r(x)) \cong \mathbb{Q}(\zeta_{4k})$. We choose $\zeta_k \mapsto -x^2$ (so $t(x) = 1 - x^2$) and $\sqrt{-1} \mapsto x^k$. The Brezing-Weng method (Theorem 2.5.1) then gives

$$\begin{aligned} q(x) &= \frac{1}{4}\left((-x^2+1)^2 + (x^2+1)^2 x^{2k}\right) \\ &= \frac{1}{4}\left(x^{2k+4} + 2x^{2k+2} + x^{2k} + x^4 - 2x^2 + 1\right). \end{aligned} \tag{2.9}$$

Since $q(1) = 1$, if q is irreducible then it represents primes. Computations with PARI [102] show that $q(x)$ is irreducible for odd $k < 200$, and we conjecture that $q(x)$ is irreducible for all odd k. We conclude that for odd $k < 200$ (and conjecturally for all odd k), (t, r, q) represents a complete family of curves with embedding degree k and discriminant 1. The ρ-value for this family is $\deg q / \deg \Phi_{4k} = (k+2)/\varphi(k)$. □

We next observe that if k is odd, then $\zeta_{2k} = -\zeta_k$. Thus if we change the sign of the polynomials representing ζ_k in Construction 2.5.2, the same construction can be used to create families with embedding degree $2k$ and the same ρ-values.

Construction 2.5.3. Let k be odd. Changing the sign of ζ_k in Construction 2.5.2 gives

$$\begin{aligned} r(x) &= \Phi_{4k}(x), \\ t(x) &= x^2 + 1, \\ q(x) &= \frac{1}{4}\left(x^{2k+4} - 2x^{2k+2} + x^{2k} + x^4 + 2x^2 + 1\right). \end{aligned}$$

Then (t, r, q) represents a potential family of pairing-friendly elliptic curves with embedding degree $2k$ and discriminant 1. If x is odd, then $q(x)$ is an integer. Since $q(x)$ is the reverse of the polynomial given in (2.9), $q(x)$ is irreducible if and only if (2.9) is. Thus (t, r, q) represents a family of curves for odd $k < 200$, and we conjecture for all k. The ρ-value for this family is $(k+2)/\varphi(k)$; in terms of the embedding degree $k' = 2k$ the ρ-value is $(k'/2+2)/\varphi(k')$. □

With the same setup, using $\zeta_{4k} = \sqrt{\zeta_{2k}}$ gives the following construction.

Construction 2.5.4. Let k be odd. Using $\zeta_{4k} \mapsto x$ in Construction 2.5.2 gives

$$\begin{aligned} r(x) &= \Phi_{4k}(x), \\ t(x) &= x + 1, \\ q(x) &= \frac{1}{4}\left(x^{2k+2} - 2x^{2k+1} + x^{2k} + x^2 + 2x + 1\right). \end{aligned}$$

Then (t, r, q) represents a potential family of pairing-friendly elliptic curves with embedding degree $4k$ and discriminant 1. Since $q(1) = 1$, if q is irreducible then it represents primes. Computations with PARI [102] show that $q(x)$ is irreducible for odd $k < 200$, and we conjecture that $q(x)$ is irreducible for all odd k. Thus (t, r, q) represents a family of curves for odd $k < 200$, and we conjecture for all k. The ρ-value for this family is $(k+1)/\varphi(k)$; in terms of the embedding degree $k' = 4k$ the ρ-value is $(k'/2+2)/\varphi(k')$. □

We now consider families constructed by choosing K to be a cyclotomic field containing a cube root of unity. Such fields contain $\sqrt{-3}$, so we may choose $D = 3$. Some constructions of this form have been given by Barreto, Lynn, and Scott [8] and Brezing and Weng [19] for certain values of k; we consider the construction for all k, and discover families in all cases where k is not divisible by 18.

Construction 2.5.5. Let k be any positive integer, let $\ell = \mathrm{lcm}(6, k)$, and let $r(x) = \Phi_\ell(x)$. We work in the field $\mathbb{Q}(\zeta_k, \zeta_6)$, defined as $K \cong \mathbb{Q}[x]/(\Phi_\ell(x))$. In this field we have $\sqrt{-3} \mapsto 2x^{\ell/6} - 1$. Our goal is to use the relation $x^{\ell/3} = x^{\ell/6} - 1 \mod r(x)$ to minimize the degree of $y(x) = (\zeta_k - 1)/\sqrt{-3}$. The obvious choice is $\zeta_k \mapsto x^{\ell/k}$; however, in many cases we can do better by choosing $\zeta_k \mapsto x^a$ with a only slightly larger than $\ell/6$. Since x is a primitive ℓth root of unity, for x^a to be a primitive kth root of unity we need $\gcd(a, \ell) = \ell/k$. The exact choice depends on the congruence class of x modulo 6:

- $k \equiv 1 \pmod 6$, $\ell = 6k$: Since $2k+1 \equiv 3 \pmod 6$, x^{2k+1} is a primitive $2k$th root of unity. Since k is odd, $-x^{2k+1}$ is a primitive kth root of unity. Thus we choose $\zeta_k \mapsto -x^{2k+1} \equiv -x^{k+1} + x \mod r(x)$.

- $k \equiv 2 \pmod 6$, $\ell = 3k$: We have $k+1 \equiv 3 \pmod 6$, so we choose $\zeta_k \mapsto x^{k+1} \equiv x^{k/2+1} - x \mod r(x)$.

- $k \equiv 3 \pmod 6$, $\ell = 2k$: Since $x^{2k/3}$ is a cube root of unity and $3 \mid k$, we need to multiply $x^{2k/3}$ by a primitive kth root of unity. Since k is odd and x is a $2k$th root of unity, $-x$ is a kth root of unity. Thus we choose $\zeta_k \mapsto -x^{2k/3+1} \equiv -x^{k/3+1} + x \mod r(x)$.

- $k \equiv 4 \pmod 6$, $\ell = 3k$: Choose $\zeta_k \mapsto x^3$.

- $k \equiv 5 \pmod 6$, $\ell = 6k$: We have $k+1 \equiv 0 \pmod 6$, so we choose $\zeta_k \mapsto x^{k+1}$.

- $k \equiv 0 \pmod 6$, $\ell = k$: Choose $\zeta_k \mapsto x$.

If $z(x)$ is the polynomial mapping to ζ_k, we compute $y(x)$ by taking $\frac{1}{3}z(x)(1 - 2x^{\ell/6})$ and adding $\pm 2xr(x)$ to cancel out the leading term if $k \pmod 6 \in \{1, 2, 3, 5\}$. We note that for small values of k the resulting $t(x)$ and $y(x)$ are not completely reduced modulo $r(x)$; however, we find that further reduction leads to a $q(x)$ that does not represent primes. Our choices for ζ_k and $y(x)$ give the following formulas for $q(x)$, which are valid for all positive k:

- $k \equiv 1 \pmod 6$: $q(x) = \frac{1}{3}(x+1)^2(x^{2k} - x^k + 1) - x^{2k+1}$.

- $k \equiv 2 \pmod 6$: $q(x) = \frac{1}{3}(x-1)^2(x^k - x^{k/2} + 1) + x^{k+1}$.

- $k \equiv 3 \pmod 6$: $q(x) = \frac{1}{3}(x+1)^2(x^{2k/3} - x^{k/3} + 1) - x^{2k/3+1}$.

- $k \equiv 4 \pmod 6$: $q(x) = \frac{1}{3}(x^3-1)^2(x^k - x^{k/2} + 1) + x^3$.

- $k \equiv 5 \pmod 6$: $q(x) = \frac{1}{3}(x^2 - x + 1)(x^{2k} - x^k + 1) + x^{k+1}$.

- $k \equiv 0 \pmod 6$: $q(x) = \frac{1}{3}(x-1)^2(x^{k/3} - x^{k/6} + 1) + x$. □

We see that we have $\deg q = \ell/3 + 2$ in all cases except $k \equiv 4 \pmod 6$, in which case $\deg q = \ell/3 + 6$. Thus for any k, we have constructed a potential family of pairing-friendly

curves with embedding degree k and discriminant 3. The ρ-values of these families are $\rho = (\ell/3+6)/\varphi(\ell)$ if $k \equiv 4 \pmod 6$, and $(\ell/3+2)/\varphi(\ell)$ otherwise.

It remains to consider whether $q(x)$ represents primes. We can check conditions (4) and (5) of Definition 2.2.1 simultaneously: If k is even then $q(1) = 1$, if $k \equiv 1$ or $3 \pmod 6$ then $q(-1) = 1$, and if $k \equiv 5 \pmod 6$ then $q(-1) = 4$ and $q(2)$ is an odd integer. Finally, computations with PARI [102] indicate that the appropriate $q(x)$ is irreducible for all $k < 300$, except when k is divisible by 18. We conjecture that these polynomials are irreducible for all k not divisible by 18.

Next, we consider families obtained by choosing K to be a cyclotomic field containing an eighth root of unity. Such fields contain $\sqrt{-2}$, so we may choose $D = 2$. Brezing and Weng give an example of the construction with $k = 18$, while Murphy and Fitzpatrick [96] give an example with $k = 24$. We describe the construction for any k divisible by 3.

Construction 2.5.6. Let k be a positive integer divisible by 3. We work in the field $\mathbb{Q}(\zeta_k, \zeta_8)$, defined as $K \cong \mathbb{Q}[x]/(\Phi_\ell(x))$, where $\ell = \operatorname{lcm}(8, k)$. In this field, we have $\zeta_k \mapsto x^{\ell/k}$ (so $t(x) = x^{\ell/k} + 1$), and $\sqrt{-2} = \zeta_8 + \zeta_8^3 \mapsto x^{\ell/8} + x^{3\ell/8}$. We choose $y(x)$ to be a polynomial mapping to $(\zeta_k - 1)/\sqrt{-2}$ and compute the reduction of $y(x)$ modulo $\Phi_\ell(x)$. Since k is a multiple of 3, we can use the relation $x^{\ell/3} = x^{\ell/6} - 1$ to compute $y(x)$ modulo $\Phi_\ell(x)$ explicitly, for we have

$$\begin{aligned} \frac{\zeta_k - 1}{\sqrt{-2}} &\mapsto \frac{1}{2}(1 - x^{\ell/k})(x^{3\ell/8} + x^{\ell/8}) \\ &\equiv \frac{1}{2}(1 - x^{\ell/k})(x^{5\ell/24} + x^{\ell/8} - x^{\ell/24}) \mod \Phi_\ell(x). \end{aligned}$$

We set $y(x)$ equal to this last polynomial. If $\frac{\ell}{k} + \frac{5\ell}{24} < \varphi(\ell)$ (a condition which holds whenever $3 \mid k$, $k \geq 18$, and k has at most two prime factors greater than 3), then $y(x)$ is the minimal-degree representative of $(\zeta_k - 1)/\sqrt{-2}$ modulo $\Phi_\ell(x)$, and we may set

$$q(x) = \frac{1}{8}\left(2(x^{\ell/k} + 1)^2 + (1 - x^{\ell/k})^2(x^{5\ell/24} + x^{\ell/8} - x^{\ell/24})^2\right).$$

The degree of q is thus $\left(\frac{2\ell}{k} + \frac{5\ell}{12}\right)$. We observe that $q(1) = 1$ for any k; computations with PARI show that $q(x)$ is irreducible when $3 \mid k$ and $k < 200$, and we conjecture that $q(x)$ is irreducible for all such k. Thus for these values of k, $(x^{\ell/k} + 1, \Phi_\ell(x), q(x))$ represents a family of curves with embedding degree k. The ρ-value of this family is $(\frac{5k}{6} + 4)/\varphi(k)$ if k is odd, and $(\frac{5k}{12} + 2)/\varphi(k)$ if k is even. □

Table 2.1: Families of pairing-friendly elliptic curves with $k \in \{15, 28, 44\}$ and $D = 2$.

k	ℓ	$t(x), q(x)$	ρ
15	120	$t(x) = x^{28}+x^{24}-x^{16}-x^{12}-x^8+1$ $q(x) = \frac{1}{8}(2x^{56}+4x^{52}+x^{50}+2x^{48}+2x^{46}-4x^{44}+x^{42}-6x^{40}-4x^{36}-x^{30}$ $+12x^{28}-2x^{26}+14x^{24}-x^{22}+2x^{20}-10x^{16}-10x^{12}+x^{10}-8x^8+2x^6+x^2+8)$	7/4
28	56	$t(x) = -x^2$ $q(x) = \frac{1}{8}(2(x^2-1)^2+x^{14}(x^2+1)^2(x^{14}+1)^2)$	23/12
44	88	$t(x) = -x^2$ $q(x) = \frac{1}{8}(2(x^2-1)^2+x^{22}(x^2+1)^2(x^{22}+1)^2)$	7/4

Construction 2.5.6, while stated only for k divisible by 3, can be carried out for any positive integer k, setting $y(x)$ to be the minimal-degree representative for $(\zeta_k - 1)/\sqrt{-2}$ in K. However, unlike the case of Construction 2.5.5, the expressions for $q(x)$ when k is not divisible by 3 or when $\frac{\ell}{k} + \frac{5\ell}{24} \geq \varphi(\ell)$ become too complicated to enumerate explicitly in general. Furthermore, in some cases the construction may not give a family of curves; for example, if $k = 20$ the $q(x)$ given by the construction never takes integer values. Potential families for a few selected values of k are given in Table 2.1.

2.5.2 Sporadic families of Brezing-Weng curves

Brezing and Weng only consider cyclotomic polynomials $r(x)$ for their constructions, but in some cases using non-cyclotomic polynomials $r(x)$ that define (perhaps trivial) extensions of cyclotomic fields may turn out to be even more effective. One method for constructing such extensions is to substitute $x \mapsto u(x)$ in the cyclotomic polynomial $\Phi_\ell(x)$, where $u(x)$ is some polynomial. If $\Phi_\ell(u(x))$ is irreducible, as is usually the case, going to the extension field will give us no advantage, as we will just be substituting $x \mapsto u(x)$ in t, r, and q. However, if $\Phi_\ell(u(x))$ factors, we may gain some advantage.

Galbraith, McKee and Valença [46] have analyzed the factorizations of $\Phi_\ell(u(x))$ when u is quadratic and Φ_ℓ has degree 4. For $\ell = 8$ there are no quadratic u such that $\Phi_8(u(x))$ factors. For $\ell = 5, 10$, there is a one-dimensional family of such u, parametrized be the rational points of a rank-one elliptic curve over $\mathbb{Q}$. However, since $\mathbb{Q}(\zeta_5) = \mathbb{Q}(\zeta_{10})$ has no quadratic imaginary subfields, we cannot use Theorem 2.5.1 to construct a complete family

using such a factorization.

Finally, for $\ell = 12$ there are two such $u(x)$. Barreto and Naehrig constructed pairing-friendly curves of prime order using one such factorization.

Example 2.5.7 (Barreto-Naehrig curves [9])**.** Galbraith, McKee and Valença [46] discovered that if $u(x) = 6x^2$, then $\Phi_{12}(u(x)) = r(x)r(-x)$, where $r(x) = 36x^4 + 36x^3 + 18x^2 + 6x + 1$. If we set $K = \mathbb{Q}[x]/(r(x))$, then $\zeta_{12} \mapsto 6x^2$ in K, and using $\sqrt{-3} = 2\zeta_{12}^2 - 1$ we compute $y(x) = 6x^2 + 4x + 1$ and $q(x) = 36x^4 + 36x^3 + 24x^2 + 6x + 1$. Since $q(x)$ and $r(x)$ have the same degree and leading coefficient, $r(x)$ is actually the number of points on the elliptic curve to be constructed. Thus if $q(x)$ and $r(x)$ are both prime for some value of x, then the elliptic curve constructed will have prime order. □

A computer search for further factorizations of $\Phi_k(u(x))$ for various values of k and degrees of u found the following example.

Example 2.5.8. Let $k = 8$. If $u(x) = 9x^3 + 3x^2 + 2x + 1$, then $\Phi_8(u(x))$ has an irreducible factor $r(x) = 9x^4 + 12x^3 + 8x^2 + 4x + 1$. Setting $D = 1$ and $K = \mathbb{Q}[x]/(r(x))$, we choose $\zeta_8 \mapsto -u(x)$ and $\sqrt{-1} = \zeta_8^2 \mapsto -18x^3 - 15x^2 - 10x - 4 \mod r(x)$. Applying Theorem 2.5.1, we compute

$$\begin{aligned} t(x) &= -9x^3 - 3x^2 - 2x \\ q(x) &= \frac{1}{4}\left(81x^6 + 54x^5 + 45x^4 + 12x^3 + 13x^2 + 6x + 1\right). \end{aligned}$$

Since $q(1) = 53$ and $q(-1) = 17$ are distinct primes, $q(x)$ represents primes. We conclude that (t, r, q) represents a family of curves with embedding degree 8. The ρ-value for this family is $3/2$, which is worse than $\rho = 5/4$ given by Construction 2.5.5. However, curves with $D = 1$ have an automorphism of order 4, and since k is a multiple of 4 we may take advantage of this "quartic twist" to map points $P \in E(\mathbb{F}_{q^8})$ down to the field $\mathbb{F}_{q^2}$, thus speeding up the pairing computation (see [56, §5]). □

Kachisa, Schaefer, and Scott [62], building on the work of Kachisa [61], give a different strategy for constructing non-cyclotomic polynomials that define a cyclotomic field. Their strategy is to choose elements $\beta \in \mathbb{Q}(\zeta_\ell)$ that can be written as an integer linear combination of a power basis with small coefficients, and let $r(x)$ be the minimal polynomial of β. Since most elements of $\mathbb{Q}(\zeta_\ell)$ do not lie in a proper subfield, in most cases we have $\mathbb{Q}[x]/(r(x)) \cong \mathbb{Q}(\zeta_\ell)$. We can then proceed as in the Brezing-Weng method.

Which β and which kth root of unity modulo $r(x)$ to choose are determined by computer search; the resulting polynomial $q(x)$ should have a degree low enough such that we obtain an attractive ρ-value. In practice we find that most polynomials $q(x)$ generated by the construction have large denominators, so it is rare for these polynomials to take integer values. Yet favorable polynomials do exist, as the following examples show. We give one example below; others can be found in [62].

Example 2.5.9 ([62])**.** Let $k = \ell = 16$. We set $\beta = -2z^5+z$, which has minimal polynomial

$$r(x) = x^8 + 48x^4 + 625.$$

In $\mathbb{Q}[x]/(r(x))$, we use $\zeta_{16} \mapsto \frac{1}{35}(2x^5 + 41x)$, so

$$t(x) = \frac{1}{35}\left(2x^5 + 41x + 35\right).$$

We use $\sqrt{-1} \mapsto -\frac{1}{7}(x^4 + 24)$. We get $y(x) = -\frac{1}{35}(x^5 + 5x^4 + 38x + 120)$ and

$$q(x) = \frac{1}{980}\left(x^{10} + 2x^9 + 5x^8 + 48x^6 + 152x^5 + 240x^4 + 625x^2 + 2398x + 3125\right).$$

The polynomial $q(x)$ is irreducible. We find that both $q(x)$ and $t(x)$ are integers if and only if $x \equiv \pm 25 \pmod{70}$. In addition, $\gcd(\{q(\pm 25 + 70n) : n \in \mathbb{Z}\}) = 1$, so q represents primes. Thus (t, r, q) represents a family of curves with embedding degree 16. The ρ-value of this family is 5/4. □

2.5.3 Scott-Barreto families

To employ the strategy of Scott and Barreto [113], we again take K to be an extension of a cyclotomic field, but this time we do not assume that K contains an element $\sqrt{-D}$. If we choose $t(x)$ to be any polynomial and $r(x)$ to be an irreducible factor of $\Phi_k(t(x) - 1)$, then $\mathbb{Q}[x]/(r(x))$ defines an extension of a cyclotomic field. We then search for an $h(x)$ that makes the right hand side of the CM equation

$$Dy^2 = 4h(x)r(x) - (t(x) - 2)^2$$

take the form of a linear factor times a perfect square. Below we give some examples of this method that achieve ρ-values less than 2 with (nearly) arbitrary D. These examples are due to Mike Scott, who found them by fixing k and executing a computer search through the space of possible $t(x)$ and $h(x)$.

Example 2.5.10. Let $k = 4$. Take $t(x) = x+1$, $r(x) = \Phi_4(x) = x^2+1$, $h(x) = (x+13)/25$. Then the CM equation becomes

$$\begin{aligned} Dy^2 &= \frac{4}{25}(x+13)(x^2+1) - (x-1)^2 \\ &= \frac{1}{25}(4x+3)(x+3)^2. \end{aligned}$$

If we substitute $x = (Dz^2 - 3)/4$, the right hand side becomes D times a square, and we find

$$q(x) = \frac{1}{25}\left(x^3 + 13x^2 + 26x + 13\right).$$

The ρ-value for this family is $3/2$. We observe that $q(x)$ is an integer if and only if $x \equiv 2 \pmod 5$, and since $x = (Dz^2 - 3)/4$ we conclude that $D \equiv 11$ or $19 \pmod{20}$. □

Example 2.5.11. Let $k = 6$. Take $t(x) = -4x^2 + 4x + 2$, $r(x) = \Phi_6(t(x) - 1) = 16x^4 - 32x^3 + 12x^2 + 4x + 1$, $h(x) = x/4$. Then the CM equation becomes

$$Dy^2 = x(4x^2 - 6x + 1)^2.$$

If we substitute $x = Dz^2$, the right hand side becomes D times a square, and we find

$$q(x) = 4x^5 - 8x^4 + 3x^3 - 3x^2 + \frac{17}{4}x + 1.$$

The ρ-value for this family is $5/4$. □

Setting $D = 3$ in Example 2.5.11 would be ideal in terms of performance, for curves with $D = 3$ have sextic twists [9] that would allow both inputs to the pairing to be given over $\mathbb{F}_q$. Unfortunately, the polynomial $r(3z^2)$ factors into two degree-four polynomials in z, so $r(3z^2)$ can never be prime. However, the construction does produce curves with $\rho \approx 5/4$ for many other values of D.

Chapter 3

New Constructions of Pairing-Friendly Elliptic Curves

3.1 Elliptic curves with embedding degree 10.

In this section we use the framework of Chapter 2, and in particular the theory of "sparse families" described in Section 2.4, to construct elliptic curves of prime order with embedding degree 10. This result also appears in [37].

As in Chapter 2, we are looking for polynomials $t(x), r(x), q(x)$ that parametrize the trace, subgroup size, and field size (respectively) of elliptic curves with prescribed embedding degree. Since we want the curves to have prime order, $r(x)$ must be the full group size of the curve, and the three polynomials must satisfy $r(x) = q(x) + 1 - t(x)$. Furthermore, the CM equation

$$Dy^2 = 4q(x) - (t(x))^2 = 4r(x) - (t(x) - 2)^2$$

must have an infinite number of solutions. As we showed in Proposition 2.4.5, this can only happen if the right hand side $f(x) = 4r(x) - (t(x) - 2)^2$ is quadratic or has a multiple root. Since $r(x)$ must be an irreducible factor of $\Phi_k(t(x) - 1)$, where Φ_k is the kth cyclotomic polynomial, the following lemma suggests that a quadratic $f(x)$ occurs naturally only in the cases $k = 3$, 4, or 6.

Lemma 3.1.1. *Fix k, let $t(x)$ be a polynomial, and let $r(x)$ be an irreducible factor of $\Phi_k(t(x) - 1)$. Then the degree of r is a multiple of $\varphi(k)$, where φ is the Euler phi function.*

Proof. Suppose $t(x)$ has degree d, so $\deg \Phi_k(t(x)-1) = d\varphi(k)$. Let θ be a root of $r(x)$ in $\overline{\mathbb{Q}}$, and let $\omega = t(\theta)-1$. Then $\Phi_k(\omega) = 0$, so ω is a primitive kth root of unity. We thus have the inclusion of fields $\mathbb{Q}(\theta) \supset \mathbb{Q}(\omega) \supset \mathbb{Q}$. Since $[\mathbb{Q}(\theta) : \mathbb{Q}] = \deg r(x)$ and $[\mathbb{Q}(\omega) : \mathbb{Q}] = \varphi(k)$, we conclude that $\varphi(k)$ divides $\deg r(x)$. □

Our key observation is that since construction of a sparse family requires $f(x) = 4r(x) - (t(x)-2)^2$ to be quadratic (see Theorem 2.4.1) and Lemma 3.1.1 implies that $\deg r(x) \geq \varphi(k)$, if $k > 6$ we must choose $r(x)$ and $t(x)$ in such a way that the high-degree terms of $t(x)^2$ cancel out those of $4r(x)$. In particular, the degree of $t(x)$ must be half the degree of $r(x)$. We have discovered that for $k = 10$ there is a choice of $r(x)$ and $t(x)$ such that this is possible. The resulting construction of elliptic curves with embedding degree 10 solves an open problem posed by Boneh, Lynn, and Shacham [17, §4.5].

We begin by noting that in the case $k = 10$, Lemma 3.1.1 tells us that the smallest possible degree of $r(x)$ is $\varphi(10) = 4$. Thus to get the high-degree terms of $t(x)^2$ to cancel out those of $4r(x)$ in this smallest case we must choose $t(x)$ to be quadratic, and furthermore $\Phi_{10}(t(x)-1)$ must have a degree-4 factor.

It happens that for $k \in \{5, 8, 10, 12\}$, Galbraith, McKee, and Valença [46] have characterized all quadratic $t(x)$ such that $\Phi_k(t(x)-1)$ factors into two irreducible quartic polynomials. In the case $k = 10$ they show that there is an infinite set of $t(x)$ such that this factorization occurs, and that these $t(x)$ are parametrized by the rational points of a certain rank-1 elliptic curve. By experimenting with some of the examples given by Galbraith, McKee, and Valença, we discovered that $t(x) = 10x^2 + 5x + 3$ leads to a quadratic $f(x)$.

Theorem 3.1.2. *Fix a positive square-free integer D relatively prime to 15. Define $t(x)$, $r(x)$, and $q(x)$ by*

$$\begin{aligned} t(x) &= 10x^2 + 5x + 3 \\ r(x) &= 25x^4 + 25x^3 + 15x^2 + 5x + 1 \\ q(x) &= 25x^4 + 25x^3 + 25x^2 + 10x + 3. \end{aligned}$$

If the equation $u^2 - 15Dv^2 = -20$ has a solution with $u \equiv 5 \pmod{15}$, then (t, r, q) represents a sparse family of curves with embedding degree 10.

Proof. It is easy to verify that conditions (1)–(4) of Definition 2.2.3 (i) hold. Condition (5) requires an infinite number of integer solutions to $Dy^2 = f(x)$, where $f(x) = 4q(x) - t(x)^2$.

The key observation is that for this choice of t and n,

$$f(x) = 4q(x) - t(x)^2 = 15x^2 + 10x + 3.$$

Multiplying by 15 and completing the square transforms the equation we wish to solve into

$$D'y^2 = (15x + 5)^2 + 20,$$

where $D' = 15D$. Integer solutions to this equation correspond to integer solutions to $u^2 - D'v^2 = -20$ with $u \equiv 5 \pmod{15}$. By Theorem 2.4.1, if one such solution exists then an infinite number exist, so (t, r, q) represents a family of curves with embedding degree 10. Since the solutions grow exponentially, this family is sparse (cf. Remark 2.4.3). □

To use Theorem 3.1.2 to construct curves with embedding degree 10, we choose a D and search for solutions to the equation $u^2 - 15Dv^2 = -20$ that give prime values for q and r. The following lemma, proposed by Mike Scott, speeds up this process by restricting the values of D that we can use.

Lemma 3.1.3. *Let $q(x)$ be as in Theorem 3.1.2. If (x, y) is an integer solution to $Dy^2 = 15x^2 + 10x + 3$ such that $q(x)$ is prime, then $D \equiv 43$ or $67 \pmod{120}$.*

Proof. If $x \equiv 0$ or $2 \pmod 3$ then $q(x)$ is divisible by 3, while if x is odd then $q(x)$ is even. Thus if $q(x)$ is prime, then $x \equiv 4 \pmod 6$.

To deduce the stated congruence for D, we consider the equation $Dy^2 = 15x^2+10x+3$ modulo 3, 5, and 8. To begin, we have $Dy^2 \equiv x \equiv 1 \pmod 3$, so $D \equiv 1 \pmod 3$. Next, we have $Dy^2 \equiv 3 \pmod 5$, so $y^2 \equiv 1$ or $4 \pmod 5$ and $D \equiv 2$ or $3 \pmod 5$. Finally, since x is even we see that $Dy^2 \equiv 3 \pmod 8$, and thus $y^2 \equiv 1 \pmod 8$ and $D \equiv 3 \pmod 8$. Combining these results via the Chinese remainder theorem, we conclude that $D \equiv 43$ or $67 \pmod{120}$. □

After reading an earlier version of this work [36], Mike Scott used Theorem 3.1.2 and Lemma 3.1.3 to find examples of elliptic curves with embedding degree 10 via the following algorithm.

Algorithm 3.1.4. Let (t, r, q) be as in Theorem 3.1.2. The following algorithm takes inputs `MaxD`, `MinBits`, and `MaxBits`, and outputs pairs (D, x_0) such that $D <$ `MaxD`, the number of bits in $q(x_0)$ is between `MinBits` and `MaxBits`, and $q(x_0)$ and $r(x_0)$ are both prime.

1. Set D to be a positive integer such that $D \equiv 43$ or $67 \pmod{120}$ and $15D$ is square free.

2. Use the continued fraction algorithm [75] to compute a fundamental unit γ of the ring of integers in $\mathbb{Q}(\sqrt{15D})$. Set $\delta \leftarrow \gamma^2$ if γ has norm -1, $\delta \leftarrow \gamma$ otherwise.

3. Use the algorithm of Lagrange, Matthews [83], and Mollin [94, Chapter 5] to find fundamental solutions (u, v) to the equation $u^2 - 15Dv^2 = -20$. (See also [105].)

4. For each fundamental solution (u, v) found in (3):

   (a) If $\log_2 u > (\texttt{MaxBits} + 11)/4$, go to the next fundamental solution.

   (b) If $u \equiv \pm 5 \pmod{15}$ and $\log_2 u > (\texttt{MinBits} + 11)/4$, then:

      i. Set $x_0 \leftarrow (-5 \pm u)/15$.

      ii. If $q(x_0)$ and $r(x_0)$ are prime, output (D, x_0).

   (c) Write $\delta(u + v\sqrt{15D}) = u' + v'\sqrt{15D}$. Set $u \leftarrow u'$, $v \leftarrow v'$, and return to step (a).

5. Increase D. If $D < \texttt{MaxD}$, return to step (1); otherwise terminate.

The bounds on $\log_2 u$ in Step (4) can be explained as follows: since $q(x) = 25x^4 + O(x^3)$ and $x = (-5 \pm u)/15$, $q(x)$ grows roughly like $u^4/2025$. We conclude that $\log_2 q(x) \approx 4 \log_2 u - 11$, so we require u in the algorithm to satisfy

$$\frac{\texttt{MinBits} + 11}{4} < \log_2 u < \frac{\texttt{MaxBits} + 11}{4}. \tag{3.1}$$

In our description of Algorithm 3.1.4, the specific parameters of Theorem 3.1.2 have allowed us to simplify the procedure described in the proof of Theorem 2.4.1. The requirement that $15D$ be square free implies that $w = 1$, and the fact that $b = 10$ is even allows us to remove the factors of 2 in the congruence moduli of equations (2.4). Thus in Step (4) we need only to find (u, v) with $u^2 - 15Dv^2 = -20$ and $u \equiv \pm 5 \pmod{15}$. Given this requirement, we see that the only restriction on the unit $\delta = \alpha + \beta\sqrt{15D}$ in Step (4c) is that $\alpha \not\equiv 0 \pmod{3}$, which must be true since $\alpha^2 - 15D\beta^2 = 1$. Thus our choice of $\delta = \gamma$ or γ^2 will always give new solutions (u, v) with $u \equiv \pm 5 \pmod{15}$; i.e., the parameter m of Theorem 2.4.1 is equal to 1.

In practice the fundamental unit γ computed in Step 2 will usually be very large, in which case we may skip Step (4c) altogether. For example, computations with PARI

indicate that when $D \approx 10^9$, γ has at least 100 bits 99.5% of the time and at least 200 bits 98.9% of the time.

Mike Scott ran Algorithm 3.1.4 with inputs `MaxD` $= 2 \cdot 10^9$, `MinBits` $= 148$, and `MaxBits` $= 512$; some sample output appears in Appendix A.1. For each (D, x_0) output by the algorithm, one may then use the CM method (see Section 1.2.4) to construct an elliptic curve over $\mathbb{F}_{q(x_0)}$ whose number of points is $r(x_0)$. Since $r(x_0)$ is prime, by Lemma 1.2.2 this curve has embedding degree 10.

Below are two examples of elliptic curves that Scott constructed in this manner.

Example 3.1.5. (A 234-bit curve.) Running Algorithm 3.1.4 with $D = 1227652867$ produces the output $x_0 = -164286669864814370$, from which we compute the 234-bit primes

$$\begin{aligned} q &= 182116508039694720644932643473759500459342546966570904207262300432038 03 \\ r &= 182116508039694720644932643473759497760331557439520307504500337823066 51. \end{aligned}$$

The class number of $\mathbb{Q}(\sqrt{-D})$ is 5328. The CM method produces the curve E over $\mathbb{F}_q$ given by

$$y^2 = x^3 - 3x + 15748668094913401184777964473522859086900831274922948973320684995903275.$$

Then $E/\mathbb{F}_q$ has r points and embedding degree 10. □

Example 3.1.6. (A 252-bit curve.) Running Algorithm 3.1.4 with $D = 1039452307$ produces the output $x_0 = -4009700747060840276$, from which we compute the 252-bit primes

$$\begin{aligned} q &= 64623109973488169622031249105052520826733388469664312016352626944028254616 43 \\ r &= 64623109973488169622031249105052520825125618461566285955627764593062921012 61. \end{aligned}$$

The class number of $\mathbb{Q}(\sqrt{-D})$ is 4548. The CM method produces the curve E over $\mathbb{F}_q$ given by

$$y^2 = x^3 - 3x + 4946538166640251374274628820269694144249181776013154863288086212076808528141.$$

Then $E/\mathbb{F}_q$ has r points and embedding degree 10. □

Ideally, the bit size of curves with embedding degree 10 should be chosen so that the discrete logarithm in the finite field $\mathbb{F}_{q^{10}}$ is approximately of the same difficulty as the discrete logarithm problem on an elliptic curve of prime order over $\mathbb{F}_q$. Using the best known discrete logarithm algorithms, this happens when q has between 220 and 250 bits (see Table 1.1 and [13, Chapter 1]). The curves in Examples 3.1.5 and 3.1.6 have been

selected so that their bit sizes are close to this range and the class numbers of $\mathbb{Q}(\sqrt{-D})$ are small enough for the CM method to be effective.

In practice, it appears that curves with small embedding degree, prime order, and small CM discriminant D are quite rare. Luca and Shparlinski [80, 81] come to this conclusion for curves with embedding degree 3, 4, or 6 (the MNT curves) through a heuristic analysis of the MNT construction. Since our construction of curves with embedding degree 10 is similar to the MNT construction (cf. Section 2.4.1), a similar analysis should hold for our $k = 10$ curves. The experimental evidence supports this reasoning: Scott's execution of Algorithm 3.1.4 with $\texttt{MaxD} = 2 \cdot 10^9$ found only 23 curves with prime orders between 148 and 512 bits [111]. Parameters for these curves can be found in Appendix A.1.

If we relax the condition on $r(x_0)$ in Step 4(b)ii of Algorithm 3.1.4 and allow $r(x_0) = hr_0$ with r_0 a large prime and h a small cofactor, then we may find a larger number of suitable curves. Scott also ran this version of the algorithm and found 101 curves with r_0 between 148 and 512 bits, h at most 16 bits, and $D < 2 \cdot 10^9$ [111]. Some examples can be found in Appendix A.1.

3.1.1 Comparison with prior state of the art

The problem that motivated Boneh, Lynn, and Shacham to seek prime-order elliptic curves with embedding degree 10 is that of producing short digital signatures using their algorithm [17] at a security level equivalent to the Digital Signature Algorithm (DSA) over a 2048-bit prime field. The standards for DSA [6, 30] require DSA signatures over a 2048-bit field $\mathbb{F}_q$ to use a 224-bit prime-order subgroup of $\mathbb{F}_q^\times$. It follows that to obtain Boneh-Lynn-Shacham (BLS) signatures at this security level we should work in an elliptic curve subgroup whose order is a prime of at least 224 bits, and the Weil pairing should map this subgroup to a finite field of at least 2048 bits. (This is also the recommended equivalence between DSA and elliptic curve signatures [6, §5.6].) Since the ratio 2048/224 is between 9 and 10, for the most efficient implementation of BLS signatures at this security level we should use curves of prime order with embedding degree 9 or 10.

Before our discovery of the family in Theorem 3.1.2, the smallest known ρ-value for a family of elliptic curves with embedding degree 10 was 3/2. This family, which is due to

Table 3.1: Elliptic curve parameters for Boneh-Lynn-Shacham signatures with security equivalent to 2048-bit DSA.

Family	Embedding degree k	Field size q (bits)	Subgroup size r (bits)	Extension field q^k (bits)
Miyaji-Nakabayashi-Takano (Theorem 2.4.6)	6	342	342	2052
Barreto-Lynn-Scott (Construction 2.5.5)	7	299	224	2091
Brezing-Weng (Construction 2.5.5)	8	280	224	2240
Brezing-Weng (Construction 2.5.5)	9	299	224	2688
Brezing-Weng (Equation (3.2), page 57)	10	336	224	3360
Barreto-Lynn-Scott (Construction 2.5.5)	11	269	224	2957
Barreto-Naehrig (Example 2.5.7)	12	224	224	2688
Freeman (Example 3.1.5)	**10**	**234**	**234**	**2340**

Brezing and Weng [19, §3, Example 2], has CM discriminant 1 and (t, r, q) given by

$$t(x) = -x^6 + x^4 - x^2 + 2, \quad r(x) = \Phi_{20}(x), \quad q(x) = \frac{1}{4}(x^{12} - x^{10} + x^8 - 5x^6 + 5x^4 - 4x^2 + 4). \tag{3.2}$$

An elliptic curve in this family with a 224-bit prime-order subgroup would be defined over a 336-bit field $\mathbb{F}_q$, and the pairing would map to a 3360-bit field. A BLS signature using such a curve would attain the level of security equivalent to 2048-bit DSA, but the signatures would be 336 bits long.

On the other hand, if we implement BLS signatures using the 234-bit prime-order curve of Example 3.1.5, then the pairing maps to a 2340-bit field and signatures are 234 bits long, so the desired security is obtained with a shorter signature.

Table 3.1 shows these and several other possibilities for families of elliptic curves with subgroups of at least 224 bits for which the pairing maps to a field of at least 2048 bits. The size of a BLS signature using a curve from this table is the size of the finite field $\mathbb{F}_q$. Note that all of the choices in the table would provide shorter signatures than 2048-bit DSA, which produces signatures of 448 bits.

We observe that Barreto-Naehrig curves of prime order with embedding degree 12 can also produce short BLS signatures at this security level. Since the pairing on a 224-bit Barreto-Naehrig curve maps to a larger field than does the pairing on the curve in Example 3.1.5, the public and private keys will be larger and the signature verification may take longer if the Barreto-Naehrig curve is used. However, compression techniques such as those of [9, §3] may be used to reduce these sizes and the complexity of the pairing computation.

3.2 More discriminants in cyclotomic families

In this section we describe an extension to the constructions of "complete families" that we described in Section 2.5. The "cyclotomic" and "sporadic" constructions we described in that section have in common that we first fix a (small) square-free CM discriminant, and then compute the corresponding complete family of curves, all with the same discriminant. We refer to such constructions as *basic constructions*.

Some users, however, might prefer more flexibility with regard to the CM discriminant D. For example, one might view curves with $D = 3$ suspiciously, as these curves have the unusual property of having an automorphism group of order 6, and the extra structure may be used to aid a future (as yet unknown) discrete logarithm attack. This is an example of the "hard-line" position on security articulated by Koblitz [67]:

> All parameters for a cryptosystem must always be chosen with the maximal possible degree of randomness, because any extra structure or deviation from randomness might some day be used to attack the system.

Users taking this viewpoint will want families of pairing-friendly elliptic curves with variable CM discriminant D.

Our main result in this section is Theorem 3.2.1, which, given a family of curves with fixed discriminant, allows us to build a family of curves with variable CM discriminant and the same ρ-value. Thus, combining a basic construction with Theorem 3.2.1 yields a general method for constructing families of curves with variable CM discriminant and $\rho < 2$. Previous constructions with variable discriminant required either $\rho \geq 2$ (cf. Section 2.3) or $k \leq 6$ (cf. Section 2.5.3). Note that D is by definition square free, so curves with different CM discriminants D are not isogenous.

After presenting our main result, we give examples of variable-discriminant families for any embedding degree k satisfying $\gcd(k, 24) \in \{1, 2, 3, 6, 12\}$. In particular, Constructions

3.2.2 and 3.2.6 combine Theorem 3.2.1 with the method of Brezing and Weng to give new families of curves for $k \equiv 3 \pmod 4$ and $k \equiv 2 \pmod 8$, respectively. When k is not divisible by 3, these families have ρ-value smaller than that of any other known variable-discriminant complete family. Furthermore, the families with $k \equiv 10 \pmod{24}$ have ρ-value smaller than any other known complete family, with fixed (in advance) or variable discriminant.

Recall that a triple of polynomials (t, r, q) is said to represent a *potential* family of elliptic curves with embedding degree k if it satisfies conditions (2)–(5) of Definition 2.2.3 (i); in particular, q may not represent primes (or be a power of a $p(x)$ that represents primes). Our result says that if the polynomials in a potential family have a certain form, we may obtain families with (nearly) arbitrary discriminant. In particular, this allows us to make D a parameter input at the time of curve construction rather than at the time the polynomials t, r, q are computed. We will then see that in many cases the potential families are actual families in the sense of Definition 2.2.3.

Theorem 3.2.1. *Suppose (t, r, q) represents a potential family of elliptic curves with embedding degree k and discriminant D. Let $K \cong \mathbb{Q}[x]/(r(x))$, and let $y(x) \mapsto (\zeta_k - 1)/\sqrt{-D}$ in K as in Theorem 2.5.1. Suppose t, r, and q are even polynomials and y is an odd polynomial. Define r', q' to be the polynomials such that $r(x) = r'(x^2)$ and $q(x) = q'(x^2)$. Then for any integer α such that $r'(\alpha x^2)$ is irreducible, there exists a potential family of curves with embedding degree k, discriminant αD, and ρ-value equal to $\rho(t, r, q)$.*

Proof. We begin by defining polynomials t', y' such that $t(x) = t'(x^2)$ and $y(x) = x \cdot y'(x^2)$. Let σ be a root of $r(x)$, so $K = \mathbb{Q}(\sigma)$. Let $\tau = \sigma/\sqrt{\alpha}$, so τ is a root of $r'(\alpha x^2)$. If $r'(\alpha x^2)$ is irreducible, we may define L to be the number field $\mathbb{Q}(\tau) \cong \mathbb{Q}[x]/(r'(\alpha x^2))$. Then any element of K that can be expressed as an even polynomial $g(\sigma^2)$ is also an element of L. In particular, since $t(x)$ is even and $t'(\sigma^2) - 1 = \zeta_k$ in K, we have $\zeta_k = t'(\alpha\tau^2) - 1$ in L.

Now let β be the element $y'(\sigma^2) \in K$; then $\beta = y'(\alpha\tau^2)$ in L. From the definition of $y(x)$ we have $-Dy(\sigma)^2 = -D\sigma^2 y'(\sigma^2)^2 = (\zeta_k - 1)^2$ in K, so

$$-D\sigma^2 y'(\alpha\tau^2)^2 = (\zeta_k - 1)^2$$

in L. Substituting $\sigma^2 = \alpha\tau^2$ gives

$$-D\alpha\tau^2 y'(\alpha\tau^2)^2 = (\zeta_k - 1)^2,$$

so we conclude that

$$\tau y'(\alpha\tau^2) = \frac{\zeta_k - 1}{\sqrt{-\alpha D}}$$

in L.

A straightforward computation now shows that

$$q'(\alpha x^2) = \frac{1}{4}\left(t'(\alpha x^2)^2 + \alpha D(xy'(\alpha x^2))^2\right).$$

Since $r'(\alpha x^2)$ is irreducible by hypothesis, it satisfies condition (2) of Definition 2.2.3 (i). Thus by Theorem 2.5.1, the triple

$$(t'(\alpha x^2), r'(\alpha x^2), q'(\alpha x^2))$$

represents a potential family of curves with embedding degree k and discriminant αD. The ρ-value for this family is $2\deg q'/2\deg r' = \deg q/\deg r$. □

Theorem 3.2.1 tells us that if t, r, q are even polynomials and $\sqrt{-D} \mod r(x)$ is an odd polynomial, then the substitution $x^2 \mapsto \alpha x^2$ usually gives a potential family of curves with discriminant αD. In practice, if $r(x)$ is irreducible then $r'(\alpha x^2)$ is nearly always irreducible, and the difficult part in obtaining true families is ensuring that $q'(\alpha x^2)$ represents primes.

Our first application of Theorem 3.2.1 is to the following construction, which improves on Construction 2.5.2 for certain odd values of k.

Construction 3.2.2. Let k be odd, $D = 1$, and $K = \mathbb{Q}[x]/(\Phi_{4k}(x))$. If we take $\zeta_k \mapsto (-1)^{(k+1)/2}x^{k+1}$, so $t(x) = 1 + (-1)^{(k+1)/2}x^{k+1}$, then using $\sqrt{-1} \mapsto x^k$ we have

$$\frac{\zeta_k - 1}{\sqrt{-1}} \mapsto (1 - (-1)^{(k+1)/2}x^{k+1})x^k \equiv (-1)^{(k+1)/2}x + x^k \mod \Phi_{4k}(x)$$

(since $x^{2k} \equiv -1 \mod \Phi_{4k}(x)$). We may then compute

$$q(x) = \frac{1}{4}\left(x^{2k+2} + x^{2k} + 4(-1)^{(k+1)/2}x^{k+1} + x^2 + 1\right).$$

Then $(t(x), \Phi_{4k}(x), q(x))$ represents a complete potential family of curves with embedding degree k and discriminant 1. The ρ-value for this family is $\deg q/\deg \Phi_{4k} = (k+1)/\varphi(k)$. □

When $k \equiv 1 \pmod 4$ (i.e., when the middle term of $q(x)$ is negative), $q(x)$ has a factor $(x^2-1)^2$, and thus we do not have a family of curves. We conjecture that $q(x)$ is irreducible whenever $k \equiv 3 \pmod 4$, and computations show that the conjecture holds for $k < 200$. In

addition, $q(x)$ is an integer whenever x is odd. Unfortunately, we find that $q(x)$ is always even when x is odd, so q fails condition (5) of Definition 2.2.1 and thus does not represent primes.

But all is not lost! We note that t, r, q of Construction 3.2.2 are even polynomials and $\sqrt{-1}$ is an odd polynomial, so we may apply Theorem 3.2.1 to make the substitution $x^2 \mapsto \alpha x^2$ in t, r, q. After making this substitution, we may find that the new $q(x)$ does indeed represent primes and thus we get a true family of curves. However, to get even a potential family, we must first show that $r(x)$ is irreducible. We will first need an algebraic lemma.

Lemma 3.2.3. *Let $K = \mathbb{Q}(\theta)$ be a number field, and let $r(x)$ be the minimal polynomial of θ. Then for $\alpha \in K$, the polynomial $r(\alpha x^2)$ is irreducible if and only if $\alpha\theta$ is not a square in K.*

Proof. The proof follows exactly the proof of [46, Lemma 1]. We observe that the argument holds regardless of whether K is Galois. □

Corollary 3.2.4. *Let k be odd, and let α be an non-square integer not dividing k. Then $\Phi_k(\alpha x^2)$ is irreducible.*

Proof. Since ζ_k is a square in $\mathbb{Q}(\zeta_k)$, by Lemma 3.2.3 $\Phi_k(\alpha x^2)$ is irreducible if and only if α is not a square in $\mathbb{Q}(\zeta_k)$; a sufficient condition for this to occur is α is a non-square integer not dividing k. □

Theorem 3.2.1 and Corollary 3.2.4 combine to tell us that Construction 3.2.2 leads to potential families of curves with discriminant α for any non-square $\alpha \nmid k$, and it remains only to check that the new q, which we denote as

$$q_\alpha(x) = \frac{1}{4}\left(\alpha^{k+1}x^{2k+2} + \alpha^k x^{2k} + 4(-\alpha)^{(k+1)/2}x^{k+1} + \alpha x^2 + 1\right),$$

represents primes. If $k \equiv 1 \pmod 4$ then $q_\alpha(x)$ always factors, but for $k \equiv 3 \pmod 4$ $q_\alpha(x)$ is likely to be irreducible.

Other than by checking each value of α and k individually, we have no way of showing that $q_\alpha(x)$ represents primes. However, if $\alpha \equiv 3 \pmod 4$ and x is odd, $q_\alpha(x)$ is an odd integer, so q_α may represent primes. In practice it appears that, for various k and α both congruent to 3 (mod 4), $q_\alpha(x)$ does indeed represent primes. We cannot prove this result, but we give one such example below.

Example 3.2.5. Let $k = 11$, $\alpha = 19$. Applying Theorem 3.2.1 to Construction 3.2.2 with these parameters gives the family

$$\begin{aligned} t(x) &= 19^6 x^{12} + 1, \\ r(x) &= \Phi_{11}(-19x^2), \\ q(x) &= \frac{1}{4}\left(19^{12}x^{24} + 19^{11}x^{22} + 4 \cdot 19^6 x^{12} + 19x^2 + 1\right). \end{aligned}$$

This family has embedding degree 11. When $x_0 = 14593$ we find that $q(x_0)$ is a 265-bit prime and $r(x_0)$ is a 222-bit prime. The unique curve with CM by the ring of integers in $\mathbb{Q}(\sqrt{-19})$ has j-invariant -884736 [118, §A.3]; an equation over $\mathbb{F}_{q(x_0)}$ is given by

$$y^2 = x^3 + 12x + 66248813315465742379993088433739283151123356836790321937028949722975746927398287\backslash \\ 5\backslash \\ 94920383080570557692937273510793 9.$$

□

As in the derivation of Construction 2.5.3 from Construction 2.5.2, we may use the fact that if k is odd then $\zeta_{2k} = -\zeta_k$ to derive an analogous construction for embedding degrees that are twice an odd number.

Construction 3.2.6. Let k be odd. Changing the sign of ζ_k in Construction 3.2.2 gives

$$\begin{aligned} t(x) &= 1 - (-1)^{(k+1)/2}x^{k+1}, \\ r(x) &= \Phi_{4k}(x), \\ q(x) &= \frac{1}{4}\left(x^{2k+2} + x^{2k} - 4(-1)^{(k+1)/2}x^{k+1} + x^2 + 1\right). \end{aligned}$$

Then (t, r, q) represents a potential family of pairing-friendly elliptic curves with embedding degree $2k$, discriminant 1, and ρ-value $(k+1)/\varphi(k)$. In terms of the embedding degree $k' = 2k$, the ρ-value is thus $(k'/2 + 1)/\varphi(k')$. □

If $k \equiv 3 \pmod 4$ then $q(x)$ has a factor of $(x^2 - 1)^2$, and if $k \equiv 1 \pmod 4$ then $q(x)$ takes integer values when x is odd, and these values are always even. Substituting $x^2 \mapsto \alpha x^2$, we get

$$q_\alpha(x) = \frac{1}{4}\left(\alpha^{k+1}x^{2k+2} + \alpha^k x^{2k} - 4(-\alpha)^{(k+1)/2}x^{k+1} + \alpha x^2 + 1\right).$$

As in Construction 3.2.2, $q_\alpha(x)$ is even for $\alpha \equiv 1 \pmod 4$, so we must choose $\alpha \equiv 3 \pmod 4$ if we want $q_\alpha(x)$ to represent primes. We illustrate with an example.

Example 3.2.7. Let $k = 13$ and $\alpha = 251$ (the largest prime factor of 2008). Applying Theorem 3.2.1 to Construction 3.2.6 with these parameters gives the family

$$\begin{aligned} t(x) &= 251^7 x^{14} + 1, \\ r(x) &= \Phi_{13}(-251x^2), \\ q(x) &= \frac{1}{4}\left(251^{14}x^{28} + 251^{13}x^{26} + 4 \cdot 251^7 x^{14} + 251x^2 + 1\right). \end{aligned}$$

This family has embedding degree 26. When $x_0 = 3255$ we find that $q(x_0)$ is a 437-bit prime and $r(x_0)$ is a 376-bit prime. We computed the Hilbert class polynomial for the ring of integers of $\mathbb{Q}(\sqrt{-251})$ in MAGMA [18] and found a root $j_0 \in \mathbb{F}_{q(x_0)}$. The curve with j-invariant j_0 is given by

$$y^2 = x^3 + x + 87716541112078391814612991346308451257991698160348998116463089502545341174699\backslash$$
$$69\backslash 458312266776406054404171478315795953474442753849998.$$

□

To conclude this section, we note that Constructions 2.5.2 and 2.5.3 satisfy the conditions of Theorem 3.2.1. We make the substitution $x^2 \mapsto \alpha x^2$, where α is odd, and obtain a potential family of pairing-friendly curves. The discriminant of a curve in this family is α.

We also note that Construction 2.5.6 satisfies the conditions of Theorem 3.2.1 when k is not divisible by 8. If k is not divisible by 4 we may choose any odd α; if k is divisible by 4 we must choose $\alpha \equiv 1 \pmod 4$. Since $D = 2$ in Construction 2.5.6, the discriminant of a curve in the resulting potential family can be any square-free positive integer congruent to 2 mod 4 (if $4 \nmid k$) or 2 mod 8 (if $4 \mid k$). We can do the same for the cases presented in Table 2.1; an analysis shows that we can take any α for $k = 15$ and $\alpha \equiv 3 \pmod 4$ for $k = 28$ or 44.

3.2.1 Algorithm for generating variable-discriminant families

By combining the substitution $x^2 \mapsto \alpha x^2$ from Theorem 3.2.1 (for some appropriate α) with one of the basic constructions 2.5.2, 2.5.3, 2.5.6, 3.2.2 or 3.2.6, we can generate a family of pairing-friendly curves with variable discriminant D for any k satisfying $\gcd(k, 24) \in \{1, 2, 3, 6, 12\}$. We now give step-by-step instructions for this procedure.

1. Select an embedding degree k with $\gcd(k, 24) \in \{1, 2, 3, 6, 12\}$.

2. Select a basic construction from the following list. (Some values of k may offer more than one possibility.)

   - Construction 2.5.2, if k is odd.
   - Construction 2.5.3, if $k \equiv 2 \pmod 4$.
   - Construction 2.5.6, if $3 \mid k$.
   - Construction 3.2.2, if $k \equiv 3 \pmod 4$.
   - Construction 3.2.6, if $k \equiv 2 \pmod 8$.

3. Use the selected basic construction to compute polynomials $t(x)$, $r(x)$, $q(x)$ that represent a family of elliptic curves with embedding degree k.

4. Let t', r', q' be polynomials such that $t(x) = t'(x^2)$, $r(x) = r'(x^2)$, and $q(x) = q'(x^2)$.

5. Select a square-free positive integer $\alpha \nmid k$ such that after the substitution $x^2 \mapsto \alpha x^2$, the resulting polynomial $q'(\alpha x^2)$ represents primes. This condition requires α to have the following form:

   - α odd for Constructions 2.5.2, 2.5.3, and 2.5.6 with $4 \nmid k$.
   - $\alpha \equiv 1 \pmod 4$ for Construction 2.5.6 with $4 \mid k$.
   - $\alpha \equiv 3 \pmod 4$ for Constructions 3.2.2 and 3.2.6.

6. Let $D = 2\alpha$ if Construction 2.5.6 was used, and let $D = \alpha$ otherwise.

Then $(t'(\alpha x^2), r'(\alpha x^2), q'(\alpha x^2))$ represents a family of elliptic curves with embedding degree k and discriminant D. In particular, for values of α and x such that $q'(\alpha x^2)$ is prime, there is an elliptic curve over $\mathbb{F}_{q'(\alpha x^2)}$ with a subgroup of order $r'(\alpha x^2)$ and embedding degree k. If the class number of $\mathbb{Q}(\sqrt{-D})$ is less than 10^5, the equation for this curve can be computed by the CM method.

One setting where this procedure may be useful is if some degree of randomness is desired in the CM discriminant of a pairing-friendly elliptic curve. One can carry out Steps (1)–(4), compute an integer a such that $r'(a)$ has slightly fewer than the minimum number of bits necessary for the desired security level in the elliptic curve subgroup, and then choose α randomly in $[1, a]$ subject to the constraints of Step (5). One then expects that there should be values of x such that $q'(\alpha x^2)$ is prime and $r'(\alpha x^2)$ is a (near-)prime of the desired

bit length. These values of x and α can then be used to generate a pairing-friendly curve via the CM method.

Note that the Cocks-Pinch method (Theorem 2.3.1) can be used to generate elliptic curves with arbitrary CM discriminant for any embedding degree k. However, the ρ-values of such curves will always be around 2. The advantage of the procedure outlined in this section is that we can vary the CM discriminant *and* obtain ρ-values strictly less than 2, for many values of k.

Chapter 4

Constructing Pairing-Friendly Abelian Varieties

4.1 Introduction

In Chapters 2 and 3 we addressed the Motivating Problem of page 4 in the case $g = 1$ by describing constructions of pairing-friendly elliptic curves. In this chapter we consider the same problem for arbitrary g, and give two methods that produce pairing-friendly abelian varieties of arbitrary dimension.

In contrast to the case of elliptic curves, very little is known about pairing-friendly ordinary abelian varieties of dimension $g \geq 2$. While there are several existence results [46, 57], until very recently there were no explicit constructions of such varieties. In [38] we presented a method for constructing ordinary, absolutely simple abelian surfaces ($g = 2$), and there is a construction due to Kawazoe and Takahashi [64] that produces pairing-friendly ordinary abelian surfaces that are simple over $\mathbb{F}_q$ but are $\overline{\mathbb{F}}_q$-isogenous to a product of two isomorphic elliptic curves.

Our first main result, Algorithm 4.2.6, generalizes to arbitrary dimension the method of Cocks and Pinch (Theorem 2.3.1) for producing pairing-friendly elliptic curves. The algorithm produces q-Weil numbers π that correspond (in the sense of Honda-Tate theory [122]) to ordinary, absolutely simple abelian varieties having arbitrary embedding degree with respect to a subgroup of (nearly) arbitrary order r. The method works by fixing a CM field K of degree $2g$ and a primitive CM type Φ on K and using a *type norm* to construct

a q-Weil number $\pi \in K$ that satisfies the conditions of Corollary 1.2.3. It follows that the q-Weil number π is the Frobenius element of a pairing-friendly ordinary abelian variety A of dimension g. If the CM field K is suitably small, CM methods can then be used to produce A explicitly (see Section 1.2.4). In the case $g = 2$ this method supersedes our result of [38]. This work is joint with Peter Stevenhagen and Marco Streng of Universiteit Leiden (the Netherlands) and appears in [42].

Section 4.3 provides some explicit examples of pairing-friendly abelian varieties constructed by Algorithm 4.2.6. We find that on inputs of cryptographic size, the ρ-values of the varieties produced are very close to $2g\widehat{g}$, where $2\widehat{g}$ is the degree of the reflex field of K. (If K is Galois then $\widehat{g} = g$, but in general we expect $\widehat{g}$ to be much larger than g.) This experimental observation agrees with a heuristic analysis of the algorithm's output.

In dimension $g = 2$ the construction of [38] and that of Algorithm 4.2.6 both lead to ordinary, absolutely simple abelian varieties with $\rho \approx 8$. The construction of Kawazoe and Takahashi produces ordinary abelian surfaces with ρ-values between 3 and 4; however, these varieties are not absolutely simple, and thus the construction can be interpreted as producing pairing-friendly elliptic curves over some extension field of $\mathbb{F}_q$. Since all of the constructions of pairing-friendly elliptic curves can produce curves with $\rho \leq 2$, in order to make higher-dimensional pairing-friendly abelian varieties appealing to the practitioner we must produce examples with smaller ρ-values.

In Section 4.4 we demonstrate the first constructions of pairing-friendly ordinary abelian varieties of dimension $g \geq 2$ that are absolutely simple and have ρ-values significantly less than $2g\widehat{g}$. Our second main result, Algorithm 4.4.9, uses the techniques of Section 4.2 to abstract and generalize the method of Brezing and Weng (Theorem 2.5.1) for constructing pairing-friendly elliptic curves. The key idea is to parametrize the subgroup order r and the Frobenius element π as polynomials of a single variable $r(x) \in \mathbb{Q}[x]$ and $\pi(x) \in K[x]$. We then extend the type norm to polynomials and construct the polynomial $\pi(x)$ as the extended type norm of an element $\xi \in \widehat{K}[x]$ that is chosen to have specified residues modulo factors of $r(x)$ in $\widehat{K}[x]$. As in the Brezing-Weng method, we compute parameters for individual varieties by finding an x_0 for which $q(x_0) = \pi(x_0)\overline{\pi}(x_0)$ is prime and $r(x_0)$ has a large prime factor. Once such an x_0 is found, we can use CM methods to construct the abelian variety whose Frobenius element is given by $\pi(x_0)$.

In Section 4.5 we discuss how to select the parameters in this algorithm to produce the optimal output, and we provide a number of examples of families of ordinary abelian

varieties produced by our method. These include several families of abelian surfaces ($g = 2$) with $\rho \leq 7$, including one with embedding degree 5 and $\rho \approx 4$, which could be a practical choice for certain security levels. We also demonstrate a family of three-dimensional abelian varieties with $\rho \approx 12$. We conclude by discussing avenues for further research in this area.

4.2 Weil numbers yielding prescribed embedding degrees

Let $\mathbb{F}_q$ be the field of q elements, A a g-dimensional simple abelian variety over $\mathbb{F}_q$, and $K = \mathbb{Q}(\pi) \subset \mathrm{End}_{\mathbb{F}_q}(A) \otimes \mathbb{Q}$ the number field generated by the Frobenius endomorphism π of A. As we described in Section 1.2.1, π is a *q-Weil number* in K: an algebraic integer with the property that all of its embeddings in $\overline{\mathbb{Q}}$ have complex absolute value $\sqrt{q}$. By Honda-Tate theory [122], all q-Weil numbers arise as Frobenius elements of abelian varieties over $\mathbb{F}_q$.

The q-Weil number π determines the embedding degree of A with respect to a subgroup of prime order r. As we saw in Corollary 1.2.3, if $K = \mathbb{Q}(\pi)$ equals $\mathrm{End}_{\mathbb{F}_q}(A) \otimes \mathbb{Q}$ and there is an integer k for which $r \nmid qk$ and

$$N_{K/\mathbb{Q}}(\pi - 1) \equiv 0 \pmod{r}, \tag{4.1}$$

$$\Phi_k(\pi\overline{\pi}) \equiv 0 \pmod{r}, \tag{4.2}$$

then A has embedding degree k with respect to r. Thus, we can prove the *existence* of an abelian variety A with embedding degree k by exhibiting a q-Weil number $\pi \in K$ with these properties. The following lemma states what we need.

Lemma 4.2.1. *Let π be a q-Weil number and $\mathbb{F}_q$ be the field of q elements. Then there exists a unique isogeny class of simple abelian varieties $A/\mathbb{F}_q$ with Frobenius π. If $K = \mathbb{Q}(\pi)$ is totally imaginary of degree $2g$ and q is prime, then such A have dimension g, and K is the full endomorphism algebra $\mathrm{End}_{\mathbb{F}_q}(A) \otimes \mathbb{Q}$. If furthermore q is unramified in K, then A is ordinary.*

Proof. The main theorem of [122] yields existence and uniqueness, and shows that $E = \mathrm{End}_{\mathbb{F}_q}(A) \otimes \mathbb{Q}$ is a central simple algebra over $K = \mathbb{Q}(\pi)$ satisfying

$$2 \cdot \dim(A) = [E : K]^{\frac{1}{2}}[K : \mathbb{Q}].$$

For K totally imaginary of degree $2g$ and q prime, Waterhouse [128, Theorem 6.1] shows that we have $E = K$ and $\dim(A) = g$. By [128, Proposition 7.1], A is ordinary if and only

if $\pi + \overline{\pi}$ is prime to $q = \pi\overline{\pi}$ in $\mathcal{O}_K$. Thus if A is not ordinary, the ideals (π) and $(\overline{\pi})$ have a common divisor $\mathfrak{p} \subset \mathcal{O}_K$ with $\mathfrak{p}^2 \mid q$, so q ramifies in K. □

Example 4.2.2. Our general construction is motivated by the case where K is a Galois CM field of degree $2g$, with cyclic Galois group generated by σ. Here σ^g is complex conjugation, so we can construct an element $\pi \in \mathcal{O}_K$ satisfying $\pi\sigma^g(\pi) = \pi\overline{\pi} \in \mathbb{Z}$ by choosing any $\xi \in \mathcal{O}_K$ and letting

$$\pi = \prod_{i=1}^{g} \sigma^i(\xi).$$

For such π, we have $\pi\overline{\pi} = N_{K/\mathbb{Q}}(\xi) \in \mathbb{Z}$. If $N_{K/\mathbb{Q}}(\xi)$ is a prime q, then π is a q-Weil number in K.

Now we wish to impose the conditions (4.1) and (4.2) on π. Let r be a rational prime that splits completely in K, and $\mathfrak{r}$ a prime of $\mathcal{O}_K$ over r. For $i = 1, \ldots, 2g$, put $\mathfrak{r}_i = \sigma^{-i}(\mathfrak{r})$; then the factorization of r in $\mathcal{O}_K$ is $r\mathcal{O}_K = \prod_{i=1}^{2g} \mathfrak{r}_i$. If $\alpha_i \in \mathbb{F}_r = \mathcal{O}_K/\mathfrak{r}_i$ is the residue class of ξ modulo $\mathfrak{r}_i$, then $\sigma^i(\xi)$ modulo $\mathfrak{r}$ is also α_i, so the residue class of π modulo $\mathfrak{r}$ is $\prod_{i=1}^{g} \alpha_i$. Furthermore, the residue class of $\pi\overline{\pi}$ modulo $\mathfrak{r}$ is $\prod_{i=1}^{2g} \alpha_i$. If we choose ξ to satisfy

$$\prod_{i=1}^{g} \alpha_i = 1 \in \mathbb{F}_r, \tag{4.3}$$

we find $\pi \equiv 1 \pmod{\mathfrak{r}}$ and thus $N_{K/\mathbb{Q}}(\pi - 1) \equiv 0 \pmod{r}$. By choosing ξ such that in addition

$$\zeta = \prod_{i=1}^{2g} \alpha_i = \prod_{i=g+1}^{2g} \alpha_i \tag{4.4}$$

is a primitive k-th root of unity in $\mathbb{F}_r^\times$, we guarantee that $\pi\overline{\pi} = N_{K/\mathbb{Q}}(\xi)$ is a primitive k-th root of unity modulo r. Thus we can try to find a suitable Weil number π by picking residue classes $\alpha_i \in \mathbb{F}_r^\times$ for $i = 1, \ldots, 2g$ meeting the two conditions (4.3) and (4.4), computing some "small" lift $\xi \in \mathcal{O}_K$ with $(\xi \bmod \mathfrak{r}_i) = \alpha_i$, and testing whether ξ has prime norm. As numbers of moderate size have a high probability of being prime by the prime number theorem, a small number of choices $(\alpha_i)_i$ should suffice. There are $(r-1)^{2g-2}\varphi(k)$ possible choices for $(\alpha_i)_{i=1}^{2g}$, where φ is the Euler phi function, so for $g > 1$ and large r we are very likely to succeed. For $g = 1$, there are only a few choices $(\alpha_1, \alpha_2) = (1, \zeta)$, but one can try various lifts and thus recover the Cocks-Pinch algorithm (Theorem 2.3.1) for finding pairing-friendly elliptic curves. □

For arbitrary CM fields K, the appropriate generalization of the map

$$\xi \mapsto \prod_{i=1}^{g} \sigma^i(\xi)$$

in Example 4.2.2 is provided by the *type norm*. A *CM type* of a CM field K of degree $2g$ is a set $\Phi = \{\phi_1, \ldots, \phi_g\}$ of embeddings of K into its normal closure L such that $\Phi \cup \overline{\Phi} = \{\phi_1, \ldots, \phi_g, \overline{\phi_1}, \ldots, \overline{\phi_g}\}$ is the complete set of embeddings of K into L. The *type norm* $N_\Phi : K \to L$ with respect to Φ is the map

$$N_\Phi : x \mapsto \prod_{i=1}^{g} \phi_i(x),$$

which clearly satisfies

$$N_\Phi(x)\overline{N_\Phi(x)} = N_{K/\mathbb{Q}}(x) \in \mathbb{Q}. \tag{4.5}$$

If K is not Galois, the type norm N_Φ does not map K to itself, but to its *reflex field* $\widehat{K}$ with respect to Φ. To end up in K, we can however take the type norm with respect to the *reflex type* Ψ, which we will define now (cf. [115, Section 8]).

Let G be the Galois group of $L/\mathbb{Q}$, and H the subgroup fixing K. Then the $2g$ left cosets of H in G can be viewed as the embeddings of K in L, and this makes the CM type Φ into a set of g left cosets of H for which we have $G/H = \Phi \cup \overline{\Phi}$. Let S be the union of the left cosets in Φ, and put $\widehat{S} = \{\sigma^{-1} : \sigma \in S\}$. Let $\widehat{H} = \{\gamma \in G : \gamma S = S\}$ be the stabilizer of S in G. Then $\widehat{H}$ defines a subfield $\widehat{K}$ of L, and as we have $\widehat{H} = \{\gamma \in G : \widehat{S}\gamma = \widehat{S}\}$ we can interpret $\widehat{S}$ as a union of left cosets of $\widehat{H}$ inside G. These cosets define a set of embeddings Ψ of $\widehat{K}$ into L. We call $\widehat{K}$ the *reflex field* of (K, Φ) and we call Ψ the *reflex type*.

Lemma 4.2.3. *The field $\widehat{K}$ is a CM field, and Ψ is a CM type of $\widehat{K}$. The field $\widehat{K}$ is generated over $\mathbb{Q}$ by the sums $\sum_{\phi\in\Phi} \phi(x)$ for $x \in K$. The type norm N_Φ maps K to $\widehat{K}$.*

Proof. The first two statements are proved in [115, Chapter II, Proposition 28] (though the definition of $\widehat{H}$ differs from ours, because Shimura lets G act from the right). For the last statement, notice that for $\gamma \in \widehat{H}$, we have $\gamma S = S$, so $\gamma \prod_{\phi\in\Phi} \phi(x) = \prod_{\phi\in\Phi} \phi(x)$. □

A CM type Φ of K is *induced* from a CM subfield $K' \subset K$ if it is of the form $\Phi = \{\phi : \phi|_{K'} \in \Phi'\}$ for some CM type Φ' of K'. In other words, Φ is induced from K' if and only if S as above is a union of left cosets of $\mathrm{Gal}(L/K')$. We call Φ *primitive* if it is not induced from a strict subfield of K. Notice that the reflex type Ψ is primitive by definition

of $\widehat{K}$, and that (K,Φ) is induced from the reflex of its reflex. In particular, if Φ is primitive, then the reflex of its reflex is (K,Φ) itself. For K Galois and Φ primitive we have $\widehat{K}=K$, and the reflex type of Φ is $\Psi=\{\phi^{-1}:\phi\in\Phi\}$.

For CM fields K of degree 2 or 4 with primitive CM types, the reflex field $\widehat{K}$ has the same degree as K. This fails to be so for $g\geq 3$; a proof of this fact appears in [42]. For a "generic" CM field K the degree of L is $2^g g!$, and $\widehat{K}$ is a field of degree 2^g generated by $\sum_\sigma \sqrt{\sigma(\eta)}$, with σ ranging over $\mathrm{Gal}(K_0/\mathbb{Q})$.

From (4.5) and Lemma 4.2.3, we see that for every $\xi\in\mathcal{O}_{\widehat{K}}$, the element $\pi=N_\Psi(\xi)$ is an element of $\mathcal{O}_K$ that satisfies $\pi\overline{\pi}\in\mathbb{Z}$. To make π satisfy the conditions of Corollary 1.2.3, we need to impose conditions modulo r on ξ in $\widehat{K}$. The following proposition allows us to index the factors of r in $\widehat{K}$ in a way that will be useful for our construction.

Proposition 4.2.4. *Let (K,Φ) be a CM type, and let r be a prime that splits completely in K, and therefore in its normal closure L and in the reflex field $\widehat{K}$ with respect to Φ. Pick a prime $\mathfrak{R}$ over r in L, and for each $\psi\in\Psi$ write $\mathfrak{r}_\psi=\psi^{-1}(\mathfrak{R})$, i.e., the inverse image of $\mathfrak{R}$ under the embedding $\psi:\widehat{K}\to L$. Then the complete factorization of r in $\mathcal{O}_{\widehat{K}}$ is*

$$r\mathcal{O}_{\widehat{K}}=\prod_{\psi\in\Psi}\mathfrak{r}_\psi\overline{\mathfrak{r}_\psi}.$$

Proof. Let $G=\mathrm{Gal}(L/\mathbb{Q})$ and $H=\mathrm{Gal}(L/\widehat{K})$. For each $\psi\in\Psi$, let $\psi'\in G$ be a representative of the left coset of H in G that induces the embedding ψ on $\widehat{K}$. Then for each $\psi\in\Psi$ we have $\mathfrak{r}_\psi=\psi'^{-1}(\mathfrak{R})\cap\mathcal{O}_{\widehat{K}}$. Since H fixes $\widehat{K}$, it follows that $\sigma\psi'^{-1}(\mathfrak{R})$ is a prime of L over $\mathfrak{r}_\psi$ for every $\sigma\in H$, and thus

$$\mathfrak{r}_\psi\mathcal{O}_L=\prod_{\sigma\in H}\sigma\psi'^{-1}(\mathfrak{R}).$$

If we denote by $\overline{\Psi}$ the set $\{\overline{\psi}:\psi\in\Psi\}$, then $\Psi\cup\overline{\Psi}$ is a complete set of coset representatives of H in G. It follows that $G=\{\sigma\psi',\sigma\overline{\psi'}:\psi\in\Psi,\sigma\in H\}$, and thus

$$r\mathcal{O}_L=\prod_{\psi\in\Psi}\prod_{\sigma\in H}\sigma\psi'^{-1}(\mathfrak{R})\sigma\overline{\psi'}^{-1}(\mathfrak{R})=\prod_{\psi\in\Psi}(\mathfrak{r}_\psi\mathcal{O}_L)(\overline{\mathfrak{r}_\psi}\mathcal{O}_L).$$

The statement follows by taking the intersection of both sides with $\mathcal{O}_{\widehat{K}}$. □

We can now generalize the argument of Example 4.2.2 to arbitrary CM fields K.

Theorem 4.2.5. *Let (K, Φ) be a CM type and $(\widehat{K}, \Psi)$ its reflex. Let $r \equiv 1 \pmod{k}$ be a prime that splits completely in K, and write its factorization in $\mathcal{O}_{\widehat{K}}$ as in Proposition 4.2.4. Given $\xi \in \mathcal{O}_{\widehat{K}}$, write $(\xi \bmod \mathfrak{r}_\psi) = \alpha_\psi \in \mathbb{F}_r$ and $(\xi \bmod \overline{\mathfrak{r}_\psi}) = \beta_\psi \in \mathbb{F}_r$ for $\psi \in \Psi$. Suppose that*

$$\prod_{\psi \in \Psi} \alpha_\psi = 1 \qquad \text{and} \qquad \prod_{\psi \in \Psi} \beta_\psi = \zeta \tag{4.6}$$

for some primitive k-th root of unity $\zeta \in \mathbb{F}_r^\times$. Let $\pi = N_\Psi(\xi) \in \mathcal{O}_K$. Then

1. $\pi\overline{\pi} \in \mathbb{Z}$,
2. $N_{K/\mathbb{Q}}(\pi - 1) \equiv 0 \pmod{r}$, *and*
3. $\Phi_k(\pi\overline{\pi}) \equiv 0 \pmod{r}$.

Proof. Statement (1) follows from the fact that $\pi\overline{\pi} = N_{\widehat{K}/\mathbb{Q}}(\xi)$. Next, let $\mathfrak{R} \subset \mathcal{O}_L$ be the prime over r underlying the factorization of Proposition 4.2.4. Since $\psi(\mathfrak{r}_\psi) \subset \mathfrak{R}$ for all $\psi \in \Psi$, the conditions (4.6) imply that $\pi - 1 \in \mathcal{O}_K$ and $\Phi_k(\pi\overline{\pi}) \in \mathbb{Z}$ are both elements of $\mathfrak{R}$. Statements (2) and (3) now follow. □

If the element π in Theorem 4.2.5 generates K and $N_{K/\mathbb{Q}}(\pi)$ is a prime q that is unramified in K, then by Lemma 4.2.1 π is a q-Weil number corresponding to an g-dimensional ordinary abelian variety A over $\mathbb{F}_q$ with endomorphism algebra K and Frobenius element π. By Corollary 1.2.3, A has embedding degree k with respect to r. This leads to the following algorithm.

Algorithm 4.2.6.

Input: a CM field K of degree $2g \geq 4$, a primitive CM type Φ of K, a positive integer k, and a prime $r \equiv 1 \pmod{k}$ that splits completely in K.

Output: a prime q and a q-Weil number $\pi \in K$ corresponding to a g-dimensional ordinary, simple abelian variety $A/\mathbb{F}_q$ that has embedding degree k with respect to r.

1. Compute a Galois closure L of K and the reflex $(\widehat{K}, \Psi)$ of (K, Φ). Set $\widehat{g} \leftarrow \frac{1}{2} \deg \widehat{K}$ and write $\Psi = \{\psi_1, \psi_2, \ldots, \psi_{\widehat{g}}\}$.
2. Fix a prime $\mathfrak{R} \mid r$ of $\mathcal{O}_L$, and compute the factorization of r in $\mathcal{O}_{\widehat{K}}$ as in Proposition 4.2.4.
3. Compute a primitive k-th root of unity $\zeta \in \mathbb{F}_r^\times$.

4. Choose random $\alpha_1, \ldots, \alpha_{\widehat{g}-1}, \beta_1, \ldots, \beta_{\widehat{g}-1} \in \mathbb{F}_r^\times$.

5. Set $\alpha_{\widehat{g}} \leftarrow \prod_{i=1}^{\widehat{g}-1} \alpha_i^{-1} \in \mathbb{F}_r^\times$ and $\beta_{\widehat{g}} \leftarrow \zeta \prod_{i=1}^{\widehat{g}-1} \beta_i^{-1} \in \mathbb{F}_r^\times$.

6. Compute $\xi \in \mathcal{O}_{\widehat{K}}$ such that $(\xi \mod \mathfrak{r}_{\psi_i}) = \alpha_i$ and $(\xi \mod \overline{\mathfrak{r}_{\psi_i}}) = \beta_i$ for $i = 1, 2, \ldots, \widehat{g}$.

7. Set $q \leftarrow N_{\widehat{K}/\mathbb{Q}}(\xi)$. If q is not prime, go to Step (4).

8. Set $\pi \leftarrow N_\Psi(\xi)$. If q is not unramified in K, or π does not generate K, go to Step (4).

9. Return q and π.

Remark 4.2.7. We require $g \geq 2$ in Algorithm 4.2.6, as the case $g = 1$ is already covered by Example 4.2.2, and requires a slight adaptation.

The condition that r be prime is for simplicity of presentation only; the algorithm easily extends to square-free values of r that are given as products of splitting primes. Such r are required, for example, by the cryptosystem of Boneh, Goh, and Nissim [16]. An example with an r of this form appears as Example 4.3.9 below.

Theorem 4.2.8. *If the field K is fixed, then the heuristic expected run time of Algorithm 4.2.6 is polynomial in $\log r$.*

Proof. The algorithm consists of a precomputation for the field K in Steps (1)–(3), followed by a loop in Steps (4)–(7) that is performed until an element $\xi \in \widehat{K}$ is found that has prime norm q, and we also find in Step (8) that q is unramified in K and the type norm $\pi = N_\Psi(\xi)$ generates K.

The primality condition in Step (7) is the "true" condition that becomes harder to achieve with increasing r, whereas the conditions in Step (8), which are necessary to guarantee correctness of the output, are so extremely likely to be fulfilled (especially in cryptographic applications where K is small and r is large) that they will hardly ever fail in practice and only influence the run time by a constant factor.

As ξ is computed in Step (6) as the lift to $\mathcal{O}_{\widehat{K}}$ of an element $\overline{\xi} \in \mathcal{O}_{\widehat{K}}/r\mathcal{O}_{\widehat{K}} \cong (\mathbb{F}_r)^{2\widehat{g}}$, its norm can be bounded by a constant multiple of $r^{2\widehat{g}}$. Heuristically, $q = N_{\widehat{K}/\mathbb{Q}}(\xi)$ behaves as a random number, so by the prime number theorem it will be prime with probability at least $(2\widehat{g} \log r)^{-1}$, and we expect that we need to repeat the loop in Steps (4)–(7) about $2\widehat{g} \log r$ times before finding an element ξ with prime norm q. As each of the steps is polynomial in $\log r$, so is the expected run time up to Step (7), and we are done if we show

that the conditions in Step (8) are met with some positive probability if K is fixed and r is sufficiently large.

For q being unramified in K, one simply notes that only finitely many primes ramify in the field K (which is fixed) and that q tends to infinity with r, since r divides $N_{K/\mathbb{Q}}(\pi-1) \leq (\sqrt{q}+1)^{2g}$.

Finally, we show that π generates K with probability tending to 1 as r tends to infinity. To show that $K = \mathbb{Q}(\pi)$, it suffices to show that any automorphism ϕ of L that fixes π also fixes K. Let ϕ be an automorphism of L. Then the set $\phi \circ \Psi$ is a CM type of $\widehat{K}$. Suppose that the following condition holds:

$$\textit{for every vector } \vec{v} \in \{0,1\}^{\widehat{g}} \textit{ that is not all 0 or 1, we have } \prod_{i=1}^{\widehat{g}} (\alpha_i/\beta_i)^{v_i} \neq 1. \tag{4.7}$$

Choose $\vec{v} \in \{0,1\}^{\widehat{g}}$ such that $v_i = 0$ if $\phi \circ \Psi$ contains ψ_i and $v_i = 1$ otherwise. Since α_i is $(\psi_i(\xi) \bmod \mathfrak{R})$ and β_i is $(\overline{\psi_i(\xi)} \bmod \mathfrak{R})$, it follows that $(\pi/\phi(\pi) \bmod \mathfrak{R})$ is equal to $\prod_{i=1}^{\widehat{g}} (\alpha_i/\beta_i)^{v_i}$. By the assumption (4.7), if this expression is 1 then $\vec{v} = \vec{0}$ or $\vec{v} = \vec{1}$, so $\phi \circ \Psi = \Psi$ or $\overline{\phi} \circ \Psi = \Psi$. By definition of the reflex, these conditions imply that either ϕ or $\overline{\phi}$ is trivial on K, which is equivalent to ϕ acting trivially on the maximal real subfield K_0. It follows that ϕ either is trivial on K or acts on K by complex conjugation. If the latter holds, then $\phi(\pi) = \pi$ implies that π is real and $q = \pi^2$, so q ramifies in K.

We conclude that if (4.7) holds and q is unramified in K, then $\phi(\pi) = \pi$ implies that ϕ is trivial on K, and thus $K = \mathbb{Q}(\pi)$. The set of $2^{\widehat{g}} - 2$ (dependent) conditions in (4.7) on the $2\widehat{g} - 2$ independent random variables α_i, β_i, $1 \leq i \leq \widehat{g} - 1$, is satisfied with probability at least $1 - (2^{\widehat{g}} - 2)/(r-1)$. Since the probability that q is unramified tends to 1 as r tends to infinity, it follows that $K = \mathbb{Q}(\pi)$ with probability tending to 1 as r tends to infinity. □

4.3 Performance of Algorithm 4.2.6 and examples

Step (6) of Algorithm 4.2.6 uses the Chinese remainder theorem to determine an element $\xi \in \mathcal{O}_{\widehat{K}}$ with the specified residues α_i and β_i modulo primes over r. In practice, for given r, one lifts a standard basis of $\mathcal{O}_{\widehat{K}}/r\mathcal{O}_{\widehat{K}} \cong (\mathbb{F}_r)^{2\widehat{g}}$ to $\mathcal{O}_{\widehat{K}}$. Multiplying those lifts by integer representatives for the elements α_i and β_i of $\mathbb{F}_r$, one quickly obtains lifts ξ. We also choose, independently of r, a $\mathbb{Z}$-basis of $\mathcal{O}_{\widehat{K}}$ consisting of elements that are "small" with respect to all absolute values of $\widehat{K}$. We translate ξ by multiples of r to lie in rF, where F is

the fundamental parallelotope in $\widehat{K} \otimes \mathbb{R}$ consisting of those elements that have coordinates in $(-\frac{1}{2}, \frac{1}{2}]$ with respect to our chosen basis.

If we denote the maximum on $F \cap \widehat{K}$ of all complex absolute values of $\widehat{K}$ by $M_{\widehat{K}}$, we have $q = N_{\widehat{K}/\mathbb{Q}}(\xi) \leq (rM_{\widehat{K}})^{2\widehat{g}}$. For the ρ-value $\rho = g \log q / \log r$ (see page 11), we find

$$\rho \leq 2g\widehat{g}(1 + \log M_{\widehat{K}} / \log r), \tag{4.8}$$

which is approximately $2g\widehat{g}$ if r gets large with respect to $M_{\widehat{K}}$. We would like ρ to be small, but this is not what one obtains by lifting random admissible choices of $\overline{\xi}$.

Theorem 4.3.1. *If the field K is fixed and r is large, we expect that*

1. *the output q of Algorithm 4.2.6 yields $\rho \approx 2g\widehat{g}$, and*
2. *an optimal choice of $\xi \in \mathcal{O}_{\widehat{K}}$ satisfying the conditions of Theorem 4.2.5 yields $\rho \approx 2g$.*

The proof of Theorem 4.3.1 is due to Peter Stevenhagen and Marco Streng, and appears in [42]. The idea is as follows: let $H_{r,k}$ be the subset of the parallelotope $rF \subset \widehat{K} \otimes \mathbb{R}$ consisting of those $\xi \in rF \cap \mathcal{O}_{\widehat{K}}$ that satisfy the two congruence conditions (4.6) for a given embedding degree k. To prove (1), one shows heuristically that a random $\xi \in H_{r,k}$ has $N_{\widehat{K}/\mathbb{Q}}(\xi) \approx r^{2\widehat{g}}$. To prove (2), one shows that the smallest value of M for which the expected number of $\xi \in H_{r,k}$ with $N_{\widehat{K}/\mathbb{Q}}(\xi) \leq M$ is at least 1 is $M \approx r^2$.

Open Problem 4.3.2. Find an efficient algorithm to compute an element $\xi \in \mathcal{O}_{\widehat{K}}$ satisfying the conditions of Theorem 4.2.5 for which $\rho \approx 2g$.

4.3.1 Examples demonstrating the distribution of ρ-values

For very small values of r we are able to do a brute-force search for the smallest q by testing all possible values of $\alpha_1, \ldots, \alpha_{\widehat{g}-1}, \beta_1, \ldots, \beta_{\widehat{g}-1}$ in Step (4) of Algorithm 4.2.6. We performed two such searches, one in dimension 2 and one in dimension 3. The experimental results support the conclusions of Theorem 4.3.1, that $\rho \approx 2g$ is possible with a smart choice in the algorithm, and that $\rho \approx 2g\widehat{g}$ is achieved with a randomized algorithm.

Example 4.3.3. Take $K = \mathbb{Q}(\zeta_5)$, and let $\Phi = \{\phi_1, \phi_2\}$ be the CM type of K defined by $\phi_n(\zeta_5) = e^{2\pi i n/5}$. We ran Algorithm 4.2.6 with $r = 1021$ and $k = 2$, and tested all possible values of α_1, β_1. The total number of primes q found was 125578, and the distribution of the corresponding ρ-values appears in Figure 4.1. The smallest q found was $q = 2023621$, giving

Figure 4.1: Distribution of ρ-values for pairing-friendly abelian surfaces with CM field $\mathbb{Q}(\zeta_5)$ and embedding degree 2 with respect to $r = 1021$.

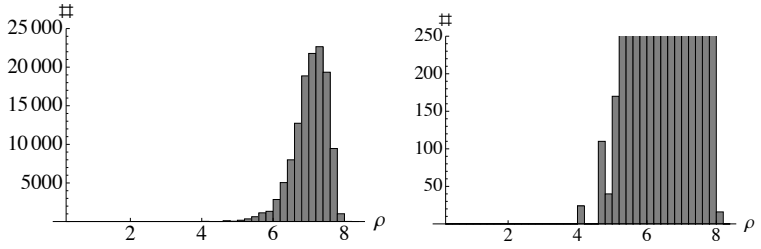
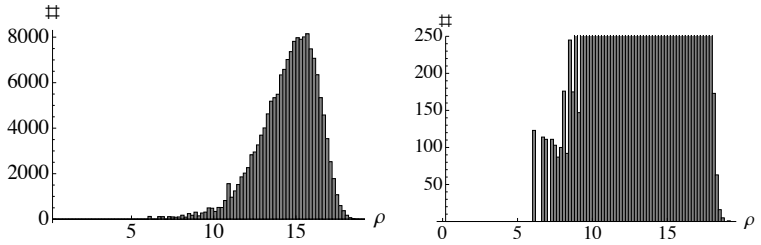


Figure 4.2: Distribution of ρ-values for pairing-friendly abelian surfaces with CM field $\mathbb{Q}(\zeta_7)$ and embedding degree 4 with respect to $r = 29$.



a ρ-value of 4.19. The curve over $\mathbb{F}_q$ for which the Jacobian has this ρ-value is $y^2 = x^5 + 18$, and the number of points on its Jacobian is 4092747290896. □

Example 4.3.4. Take $K = \mathbb{Q}(\zeta_7)$, and let $\Phi = \{\phi_1, \phi_2, \phi_3\}$ be the CM type of K defined by $\phi_i(\zeta_7) = e^{2\pi i/7}$. We ran Algorithm 4.2.6 with $r = 29$ and $k = 4$, and tested all possible values of $\alpha_1, \alpha_2, \beta_1, \beta_2$. The total number of primes q found was 162643, and the distribution of the corresponding ρ-values appears in Figure 4.2. The smallest q found was $q = 911$, giving a ρ-value of 6.07. The curve over $\mathbb{F}_q$ for which the Jacobian has this ρ-value is $y^2 = x^7 + 34$, and the number of points on its Jacobian is 778417333. □

Example 4.3.5. Take $K = \mathbb{Q}(\zeta_5)$, and let $\Phi = \{\phi_1, \phi_2\}$ be the CM type of K defined by $\phi_i(\zeta_5) = e^{2\pi i/5}$. We ran Algorithm 4.2.6 with $r = 2^{160} + 685$ and $k = 10$, and tested 2^{20} random values of α_1, β_1. The total number of primes q found was 7108. Of these primes, 6509 (91.6%) produced ρ-values between 7.9 and 8.0, while 592 (8.3%) had ρ-values between 7.8 and 7.9. The smallest q found had 623 binary digits, giving a ρ-value of 7.78. □

4.3.2 Examples of cryptographic size

We implemented Algorithm 4.2.6 in MAGMA [18] and used it to compute examples of q-Weil numbers π corresponding to pairing-friendly abelian varieties of dimension 2 and 3. We then used CM methods (Section 1.2.4) to find curves whose Jacobians are in the specified isogeny class. We chose the subgroup size r so that the discrete logarithm problem in $A[r]$ is expected to take roughly 2^{80} steps. The embedding degree k is chosen so that $r^{k/g} \approx 1024$; this would be the ideal embedding degree for the 80-bit security level if we could construct varieties over $\mathbb{F}_q$ with $\#A(\mathbb{F}_q) \approx r$.

Example 4.3.6. Let $\eta = \sqrt{-2+\sqrt{2}}$ and let K be the degree-4 Galois CM field $\mathbb{Q}(\eta)$. Let $\Phi = \{\phi_1, \phi_2\}$ be the CM type of K such that $\mathrm{Im}(\phi_i(\eta)) > 0$. We ran Algorithm 4.2.6 with CM type (K, Φ), $r = 2^{160} - 1679$, and $k = 13$. The algorithm output the following field size:

$$\begin{aligned} q \;=\; & 3134605780829315791376234453100527571554468021964133849744950023887230035061716 5 \setminus \\ & 4089253085397320557815144528570696358820481879419873926412384900210489039945980 7 \setminus \\ & 4631327324771546515176667557021 67 \quad (640 \text{ bits}) \end{aligned}$$

There is a single $\overline{\mathbb{F}}_q$-isomorphism class of curves over $\mathbb{F}_q$ whose Jacobians have CM by $\mathcal{O}_K$. It has been computed in [124], and the desired twist turns out to be

$$C : y^2 = x^5 + 3x^4 - 2x^3 - 6x^2 + 3x + 1.$$

The number of points on $\mathrm{Jac}(C)$ is

$$\begin{aligned} n \;=\; & 9825753401208564546874202024474095320978583307689740411447658880380289884172176555206 3 \setminus \\ & 9218115436181878893905499309007254607493882359752609523797673099037195770065660097304 0 \setminus \\ & 0439477737685984674972298678000258590772033253331684046018749228661140581967158173043 5 \setminus \\ & 1402518165256511999250281116458991019215724287409920692464855942170056346859949692288 2 \setminus \\ & 4842521586998633255894544870557038879938 8. \end{aligned}$$

The ρ-value of $\mathrm{Jac}(C)$ is 7.99. □

Example 4.3.7. Let $\eta = \sqrt{-30+2\sqrt{5}}$ and let K be the degree-4 non-Galois CM field $\mathbb{Q}(\eta)$. The reflex field $\widehat{K}$ is $\mathbb{Q}(\omega)$ where $\omega = \sqrt{-15+2\sqrt{55}}$. Let Φ be the CM type of K such that $\mathrm{Im}(\phi_i(\eta)) > 0$. We ran Algorithm 4.2.6 with the CM type (K, Φ), subgroup size $r = 2^{160} - 1445$, and embedding degree $k = 13$. The algorithm output the following field size:

$$q = 1109165488716951297136540704029359957997637815897340518163508137915707830213092 7 \backslash$$
$$5165200362378619253107712738894445330358409133449245275269309408919298654153381 9 \backslash$$
$$3551886616778340023118130834598146 1 \quad (645 \text{ bits})$$

The Igusa class polynomials for K can be found in the preprint version of [131]. We used the roots of the Igusa class polynomials mod q to construct curves over $\mathbb{F}_q$ with CM by $\mathcal{O}_K$. As K is non-Galois with class number 4 and the real quadratic subfield $\mathbb{Q}(\sqrt{5})$ has class number 1, there are 8 isomorphism classes of curves in 2 isogeny classes [132, Theorem 3.1]. We found a curve C in the correct isogeny class with equation $y^2 = x^5 + a_3x^3 + a_2x^2 + a_1x + a_0$, with

$$a_3 = 3790982736104090243439033807275491870596956662286524459834078537949206229349302 3 \backslash$$
$$0788722063247159195346026151591518950319957405579197595583440787957848421270026 3 \backslash$$
$$2600401437108457032108586548189769$$
$$a_2 = 1896035099273106614161944712168106284395182234121698008963211029490098526734892 7 \backslash$$
$$5670043511443169778547909878272180632727907470820642926375198310935125083185373 5 \backslash$$
$$1901282000421070182572671506056432$$
$$a_1 = 6933748814292402291021949990743247017433118324822672111253519992965066326048728 1 \backslash$$
$$5017735143296725120703741619661425566879680804661264176792227374912536654153444 0 \backslash$$
$$5882465731376523304907041006464504$$
$$a_0 = 3167814256193959689564602175360701234227765838416988096109570182577670412620481 8 \backslash$$
$$4823068777891679060396975757144988041786168947127416701638860871296694117812042 4 \backslash$$
$$3813332617272038494020178561119564.$$

The number of points on $\mathrm{Jac}(C)$ is

$$n = 1230248081360713415235387507698945486993147761623432892219369544435366780728356799124 5 \backslash$$
$$5228936193387735906879245870018629052950468479680456894408068173015760260457214712702 2 \backslash$$
$$3128852331785639221267111450226768728390111556759189165029845899332188712400366504852 3 \backslash$$
$$3867065075141962056038803248062466015214703652012681808971683243430757262414852500815 2 \backslash$$
$$0145786633766490530099470665256217052140496 8 0.$$

The ρ-value of $\mathrm{Jac}(C)$ is 8.06. □

Example 4.3.8. Let K be the degree-6 Galois CM field $\mathbb{Q}(\zeta_7)$, and let $\Phi = \{\phi_1, \phi_2, \phi_3\}$ be the CM type of K such that $\phi_n(\zeta_7) = e^{2\pi in/7}$. We used the CM type (K, Φ) to construct a curve C whose Jacobian has embedding degree 17 with respect to $r = 2^{180} - 7427$. There is

a unique isomorphism class of curves in characteristic zero whose Jacobians are absolutely simple and have CM by K; these curves are given by $y^2 = x^7 + a$. Algorithm 4.2.6 output the following field size:

$$\begin{aligned} q \;=\; & 157558413811977153591787802014368793057776946867137463955067876140250081217597497263 49 \backslash \\ & 377162542168169176007186988081292604570406371468028127020440686127726925907718896620 51 \backslash \\ & 561078068230000961208749156120171849242068432046217592329462633576371925167987740263 8 \backslash \\ & 911689714410855314811092763287402991115312604840826985712143103349 9 \quad (1077 \text{ bits}) \end{aligned}$$

The equation of the curve C is $y^2 = x^7 + 10$. The number of points on $\mathrm{Jac}(C)$ is

$$\begin{aligned} n \;=\; & 391133307032133839032918991654978467072996402822880103712828134881479536921539476626 64 \backslash \\ & 872524859749361422647231083217148421036859164002887161826333889351145328351666933300 40 \backslash \\ & 955459433590125617747713055265006666049243295531881776994530045554057264335215616276 22 \backslash \\ & 610741291090131272644122359302349147688870708662754957253695235892901596480172868253 32 \backslash \\ & 133981197564383412203831309616970540127395313628179550566955449237032604021015581621 69 \backslash \\ & 273342914872860734984590484470378399389176648640683324366435063591365016666836695077 326 \backslash \\ & 305374336097087031291086788083075176511319710761182651175244697173028052742019673491 44 \backslash \\ & 384260641591065197212058116419617612276846051832819190013539357982975203110786387114 48 \backslash \\ & 723792084641282895044011321854622409087777321950112922310199243279463508408749296918 01 \backslash \\ & 702424011720903833528138647998882488130471345394700260936891679701349438008058990224 27 \backslash \\ & 485861350771588528520014968332821323490400899073063482489197936356279119510106570550 98 \backslash \\ & 159756792889062169576019083. \end{aligned}$$

The ρ-value of $\mathrm{Jac}(C)$ is 17.95. □

We now give an example of an abelian surface that is pairing-friendly with respect to a subgroup whose order is a composite number that is presumed to be infeasible to factor, such as an RSA modulus. Such abelian varieties are required by a number of recent protocols, such as that of Boneh, Goh, and Nissim [16].

Example 4.3.9. Let $K = \mathbb{Q}(\zeta_5)$. We chose two random 512-bit primes congruent to 1 mod 5,

$$\begin{aligned} r_1 \;=\; & 118566889331223067125318070661222383966664655888377495575065704906841443039028138258 73 \backslash \\ & 551794459259674597557027194217311490745735797836341219374437395610371, \\ r_2 \;=\; & 127209537040249968517150097878529705000577836983364794731442746226324611249456989732 58 \backslash \\ & 268824071286151997260549018351088484741838683144715708710336086192081, \end{aligned}$$

and set $r = r_1 r_2$. Let $\Phi = \{\phi_1, \phi_2\}$ be the CM type of K defined by $\phi_i(\zeta_5) = e^{2\pi i/5}$. We used the CM type (K, Φ) to construct a curve C whose Jacobian has embedding degree 1

with respect to both r_1 and r_2. We ran Steps (4) and (5) of Algorithm 4.2.6 for each of r_1 and r_2, and combined the results modulo r in Step (6). This modified algorithm output the field size

$$
\begin{aligned}
q \;=\; & 153058705774098518762891130285803298360786599300304292405120423433011928347991491444 42 \setminus \\
& 053067273712044563056522501678500210839236585343566831942262311827808313266341878794 16 \setminus \\
& 144951840312677789641092794489218677405525366161290703543048977836593587395950107189 15 \setminus \\
& 111467563715473304979817343827134269843160283828058978399624962283201012279735558546 47 \setminus \\
& 045544744695417250820423749352378026516095186367150186411227475242915216442335911463 78 \setminus \\
& 218599011767900376600283898328314328990976705909962230276863155690967153147366562239 31 \setminus \\
& 388487954033285848859537678304634667076300168170384988356833490616618456138597388521 34 \setminus \\
& 276035879848749051026137613713397976761532454306453563584433764494838004034382044393 84 \setminus \\
& 979997479996429237170472867449735922758213821248629603297867309777120641926996961399 14 \setminus \\
& 726118145805685128921811874333998357210514186475094306570627584558011390955650290076 35 \setminus \\
& 616549553662766451200270002225145707454050774372527349795468118371185640703846138234 16 \setminus \\
& 733738923122130008828401017479357495064340090931899861944159208123918194159992632207 59 \setminus \\
& 883443700567808229154222198510648716563824287104739856320134685970370082677171539556 43 \setminus \\
& 030777315495863430977475198347574260720732948577234857306864058903304364720561175984 60 \setminus \\
& 965761440398702915841156471.
\end{aligned}
$$

The equation of the curve C is $y^2 = x^5 + 28$. The number of points on $\mathrm{Jac}(C)$ is

$$
\begin{aligned}
n \;=\; & 234269674132420592477611536659647767448346154104609364382477123711391767792621099023 43 \backslash \\
& 741992286699462595735808286300394610862390817585759726955145135018809382937596557710 00 \backslash \\
& 635577481353520309588174980751843619765159965324755455980138593662394881240514904169 08 \backslash \\
& 071977016317951070939556587743427867957482516152674291579914981554962140840451917164 69 \backslash \\
& 769704795402381086994039598316789608511755821256010821397176264778262234948600153676 25 \backslash \\
& 510180600021930334863452285333045411815430730800600022570001189247719175226686995068 52 \backslash \\
& 802119714433903911337095275488865267819820405779816928227145398322894471648517028445 18 \backslash \\
& 436753945261662929515498723244535445928873101250139120813187347876876117053794039533 81 \backslash \\
& 271910455226038467603579313457508476637440061419175595777764872608104466991431208516 73 \backslash \\
& 676504441754414392487394172584053080714779921582695690640509181958068311317366113340 68 \backslash \\
& 267935054130049143025054001876942848364312675572569059371248803337504251620924609390 49 \backslash \\
& 048236309584254170167045307000210384757171724067959564788480175606773717564052800838 27 \backslash \\
& 870705377890393676755431101552256254328131067077918168367626963927164704683869828390 56 \backslash \\
& 394407689105212991087130337057393369456238221304942253193878195078846876287085665977 08 \backslash \\
& 234525162775009635611461870471542205502641580949113892552643159348115551922116538838 71 \backslash \\
& 472023807991843274426482239629810172467852018867599728362107736194391906354988401773 50 \backslash \\
& 732591571565900914014059732217684476871604941862958051363439791955039505582306757360 28 \backslash \\
& 874934676317059073465261366616813265395967529644873434698593794524069097512607943192 84 \backslash \\
& 506092218636992333363189853746820677999845965822229816287661808303223291200655405910 7 \backslash \\
& 862348464067643781196801904994569443553301818930971945482991896181011497162832028931 73 \backslash \\
& 588076096353364992828581698883456215470482912199056641607558278210208705441350248399 27 \backslash \\
& 351977664994060806154091501655412920392092886644925531285733554714204639121347900162 37 \backslash \\
& 890458062975125668415799644971562284031753629624602083696930513982010364309680710924 61 \backslash \\
& 548535571624477307064640119759329849740338456293295892492693549596815685065447935141 23 \backslash \\
& 310928423893715798484753409846026972569291552078769189493199991830718203078759318574 39 \backslash \\
& 791822357108500900484514671521597078109972001196775384313618798634776701866606947861 25 \backslash \\
& 401804492124075891967759289239924918277648407040786504460010375623276098206745221226 52 \backslash \\
& 067691767468834613657657606844256253261719547310060961300923901856079708430246748696 57 \backslash \\
& 771457887513649049469267920704101690966911336139252 96.
\end{aligned}
$$

The ρ-value of $\mathrm{Jac}(C)$ with respect to $r = r_1 r_2$ is 7.98. □

We conclude with an example of an 8-dimensional pairing-friendly abelian variety found using our algorithms. Since CM methods are not developed in dimension 8, we started with a single CM abelian variety A in characteristic zero and applied our algorithm to different CM types until we found a prime q for which the reduction has the specified embedding degree. To speed up the search, we used a small (i.e., non-cryptographic) subgroup

size r.

Example 4.3.10. Let $K = \mathbb{Q}(\zeta_{17})$. We set $r = 1021$ and $k = 10$ and ran Algorithm 4.2.6 repeatedly with different CM types for K. Given the output, we tested the Jacobians of twists of $y^2 = x^{17} + 1$ for the specified number of points. We found that the curve $y^2 = x^{17} + 30$ has embedding degree 10 with respect to r over the field $\mathbb{F}_q$ of order

$$q = 68696035083224346148549085355452089780388194 37.$$

The CM type producing this q was

$$\Phi = \{\phi_1, \phi_3, \phi_5, \phi_6, \phi_8, \phi_{10}, \phi_{13}, \phi_{15}\},$$

where $\phi_n(\zeta_{17}) = e^{2\pi i n/17}$. The number of points on $\mathrm{Jac}(C)$ is

$$\begin{aligned} n = {} & 4959676766973469039648329429724204926413799125988399146632581536947358335287835707841 5 \backslash \\ & 3372224025654657688763275686875873746786074362633967094166430826747352178946505866939 0 \backslash \\ & 7824139700993964762873646390760785141177020876658189602580569351531287393407123029282 1 \backslash \\ & 3486779830713205432998663323320181918282811733968897715273624369010587353095444941361 3 \backslash \\ & 0889813139420191020723 7. \end{aligned}$$

The ρ-value of $\mathrm{Jac}(C)$ is 121.9. □

Even if we could improve on the ρ-value of Example 4.3.10, abelian varieties of dimension 8 would be of limited use in cryptographic applications, as index calculus attacks can solve the discrete logarithm problem in time $O(q^{16/9})$ [49]. If $\rho \approx 1$ then this is equivalent to $O(r^{2/9})$, which is much faster than the best time of $O(r^{1/2})$ in dimensions 1 and 2.

4.4 A generalized Brezing-Weng method

Algorithm 4.2.6 can be viewed as a generalization to arbitrary dimension of the Cocks-Pinch method (Theorem 2.3.1) for constructing pairing-friendly ordinary elliptic curves. In the elliptic curve case, the Brezing-Weng method (Theorem 2.5.1) generalizes the Cocks-Pinch method by parametrizing the trace t, subgroup size r, and field size q as polynomials $t(x)$, $r(x)$, $q(x)$ that produce valid curve parameters for many different inputs x. The advantage of such "families" is that the ρ-values produced are often smaller than those produced by the Cocks-Pinch method.

In this section, we show how the techniques of Section 4.2 can be used to view the Brezing-Weng construction from a new perspective that admits a generalization to higher dimensions. In dimension g the resulting abelian varieties have ρ-values strictly less than $2g\widehat{g}$, which is the best value we expect to obtain from Algorithm 4.2.6.

For convenience, we reproduce the Brezing-Weng algorithm here.

Algorithm 4.4.1 ([19])**.**

Input: a positive integer k and a positive square-free integer D.

Output: polynomials $r(x)$, and $q(x)$ such that for any x_0 for which $q(x_0)$ is prime, there is an ordinary elliptic curve E over $\mathbb{F}_{q(x_0)}$ such that $\mathrm{End}(E) \otimes \mathbb{Q} \cong \mathbb{Q}(\sqrt{-D})$ and E has embedding degree k with respect to $r(x_0)$.

1. Find an irreducible polynomial $r(x) \in \mathbb{Z}[x]$ such that $L = \mathbb{Q}[x]/(r(x))$ is a number field containing $\sqrt{-D}$ and the cyclotomic field $\mathbb{Q}(\zeta_k)$.
2. Choose a primitive kth root of unity $\zeta \in L$.
3. Let $t(x) \in \mathbb{Q}[x]$ be a polynomial mapping to $\zeta + 1$ in L.
4. Let $y(x) \in \mathbb{Q}[x]$ be a polynomial mapping to $(\zeta - 1)/\sqrt{-D}$ in L.
5. Set $q(x) \leftarrow (t(x)^2 + Dy(x)^2)/4$. Return $r(x)$ and $q(x)$. □

Remark 4.4.2. In this chapter we will always use K to denote a CM field, and L to denote a field containing K and some primitive kth root of unity. This notation differs slightly from that of Chapter 2.

Our new perspective on the Brezing-Weng method starts with the fact that since $L = \mathbb{Q}[x]/(r(x))$ contains $K = \mathbb{Q}(\sqrt{-D})$, the polynomial $r(x)$ splits into two irreducible factors when viewed as an element of $K[x]$. We thus have $r(x) = r_1(x)\overline{r_1}(x)$ in $K[x]$, and $L \cong K[x]/(r_1(x)) \cong K[x]/(\overline{r_1}(x))$. Without loss of generality, we may assume that the map implied in Steps (3) and (4) of Algorithm 4.4.1 sends x to a root of $r_1(x)$.

If we compute $t(x)$ and $y(x)$ as in Theorem 4.4.1 and let $\pi(x) = \frac{1}{2}(t(x) + y(x)\sqrt{-D})$, then $\pi(x) \equiv \zeta \bmod r_1(x)$. In addition, we see that $\overline{\pi}(x) = \frac{1}{2}(t(x) - y(x)\sqrt{-D}) \equiv 1 \bmod r_1(x)$, or equivalently, $\pi(x) \equiv 1 \bmod \overline{r}_1(x)$. We thus see that $\pi(x)$ satisfies conditions analogous to those of Corollary 1.2.3:

$$\begin{aligned} (\pi(x) - 1)(\overline{\pi}(x) - 1) &\equiv 0 \bmod r(x), \\ \Phi_k(\pi(x)\overline{\pi}(x)) &\equiv 0 \bmod r(x). \end{aligned}$$

The expression $\pi(x)\overline{\pi}(x)$ gives the $q(x)$ of the algorithm, so we conclude that for any $x_0 \in \mathbb{Q}$ for which $q(x_0)$ is a prime integer, $\pi(x_0) \in K$ is the Frobenius endomorphism of the elliptic curve E specified in the algorithm's description.

Algorithm 4.2.6 fixes a prime subgroup size r and uses the type norm from $\widehat{K}$ to construct a Frobenius element $\pi \in K$ that has specified residues modulo certain primes over r in $\mathcal{O}_K$. To apply these ideas to the Brezing-Weng construction, we extend the type norm to a multiplicative map $\mathcal{N}_\phi$ on polynomials in $K[x]$.

Definition 4.4.3. Let K be a CM field and Φ be a CM type of K, and let L be the normal closure of K. Define the *extended type norm* $\mathcal{N}_\phi : K[x] \to L[x]$ by

$$\mathcal{N}_\Phi(\xi) = \prod_{\phi \in \Phi} \phi(\xi),$$

where $\phi(\xi)$ is obtained by applying ϕ to the coefficients of ξ.

If $\deg K = 2g$, then $\mathcal{N}_\Phi(\xi)$ is a polynomial of degree g times the degree of ξ.

Lemma 4.4.4. *Let $\xi \in K[x]$, and let Φ be a CM type of K. Then $\mathcal{N}_\Phi(\xi) \in \widehat{K}[x]$, where $\widehat{K}$ is the reflex field of (K, Φ).*

Proof. Let L be the normal closure of K, and let $\sigma \in \mathrm{Gal}(L/\widehat{K})$. Then by definition of the reflex type, σ permutes the elements of Φ, so $\sigma(\prod_{\phi\in\Phi} \phi(\xi)) = \prod_{\phi\in\Phi} \phi(\xi)$. (Cf. Lemma 4.2.3.) □

Remark 4.4.5. In a similar manner, for any extension of number fields L/K we can extend the norm $N_{L/K}$ to polynomials $f \in L[x]$ by setting $\mathcal{N}_{L/K}(f) = \prod_\phi \phi(f)$, where ϕ ranges over the set of embeddings of L in its normal closure that fix K. An argument analogous to the proof of Lemma 4.4.4 then shows that the image of $\mathcal{N}_{L/K}$ is contained in $K[x]$.

To generalize the Brezing-Weng construction, we let K be a CM field of degree $2g$ with primitive CM type Φ. Let $(\widehat{K}, \Psi)$ be the reflex CM type, and let $\deg \widehat{K} = 2\widehat{g}$. Let $L = \mathbb{Q}[x]/(r(x))$ be a number field containing $\widehat{K}$ and $\mathbb{Q}(\zeta_k)$. In the case where $K = \widehat{K}$ is a quadratic imaginary field, the Brezing-Weng method constructs directly a polynomial $\pi(x)$ parametrizing Frobenius elements by prescribing the residues of $\pi(x)$ modulo each factor of $r(x)$ in $K[x]$. To generalize this construction along the lines of Algorithm 4.2.6, we construct $\pi(x)$ as the extended type norm $\mathcal{N}_\Psi$ of an element $\xi \in \widehat{K}[x]$ with prescribed residues modulo factors of $r(x)$ in $\widehat{K}[x]$. The following proposition is an analogue of Proposition 4.2.4 that allows us to index the factors of $r(x)$ in $\widehat{K}[x]$ in a way that will be useful for our construction.

Proposition 4.4.6. *Let $\widehat{K}$ be a CM field and Ψ be a CM type on $\widehat{K}$. Let $r(x) \in \mathbb{Q}[x]$ be irreducible, and assume that $L = \mathbb{Q}[x]/(r(x))$ is Galois and contains $\widehat{K}$. Let $G = \mathrm{Gal}(L/\mathbb{Q})$ and $H = \mathrm{Gal}(L/\widehat{K})$. For each $\psi \in \Psi$ let $\psi' \in G$ be a representative of the left coset of H that induces the embedding ψ on $\widehat{K}$.*

Fix a root $\gamma \in L$ of $r(x)$. For each $\psi \in \Psi$, define

$$r_\psi(x) = \mathcal{N}_{L/\widehat{K}}(x - \psi'^{-1}(\gamma)), \qquad \overline{r_\psi}(x) = \mathcal{N}_{L/\widehat{K}}(x - \overline{\psi'}^{-1}(\gamma)).$$

Then for each $\psi \in \Psi$, r_ψ and $\overline{r_\psi}$ are irreducible elements of $\widehat{K}[x]$, and the complete factorization of $r(x)$ in $\widehat{K}[x]$ is given by

$$r(x) = \prod_{\psi \in \Psi} r_\psi(x)\overline{r_\psi}(x). \tag{4.9}$$

Proof. The fact that r_ψ and $\overline{r_\psi}$ are in $\widehat{K}[x]$ follows from Remark 4.4.5. Since L is Galois, any root $\delta \in L$ of $r_\psi(x)$ is also a root of $r(x)$, and thus $L = \mathbb{Q}(\delta) = \widehat{K}(\delta)$. It follows that the minimal polynomial of δ over $\widehat{K}$ has degree $[L : \widehat{K}]$, which by construction is the degree of $r_\psi(x)$. Therefore $r_\psi(x)$ is the minimal polynomial of δ over $\widehat{K}$ and is thus irreducible. The proof for $\overline{\psi}$ is analogous.

Since the elements of H induce the complete set of embeddings of $\widehat{K}$ in L, we have

$$r_\psi(x) = \prod_{\sigma \in H} (x - \sigma\psi'^{-1}(\gamma)), \qquad \overline{r_\psi}(x) = \prod_{\sigma \in H} (x - \sigma\overline{\psi'}^{-1}(\gamma)).$$

If we let $\Psi' = \{\psi' : \psi \in \Psi\}$ and $\overline{\Psi'} = \{\overline{\psi'} : \psi \in \Psi\}$, then the set of roots of the right hand side of (4.9) is exactly $\{\tau(\gamma) : \tau \in H(\Psi' \cup \overline{\Psi'})^{-1}\}$. Since $\Psi' \cup \overline{\Psi'}$ is a complete set of left coset representatives of H in G, its inverse is a complete set of *right* coset representatives of H in G, and thus $H(\Psi' \cup \overline{\Psi'})^{-1} = G$. We conclude that $\{\tau(\gamma) : \tau \in H(\Psi' \cup \overline{\Psi'})^{-1}\}$ consists of precisely the roots of $r(x)$ in L. □

We now obtain an analogue of Theorem 4.2.5:

Theorem 4.4.7. *Let (K, Φ) be a CM type and $(\widehat{K}, \Psi)$ its reflex. Let $r(x) \in \mathbb{Q}[x]$ be an irreducible (not necessarily monic) polynomial such that $L = \mathbb{Q}[x]/(r(x))$ is a Galois extension of $\mathbb{Q}$ containing $\widehat{K}$ and the cyclotomic field $\mathbb{Q}(\zeta_k)$.*

Let $\gamma \in L$ be a root of $r(x)$, and write the factorization of $r(x)$ in $\widehat{K}[x]$ as in Proposition 4.4.6. Given $\xi \in \widehat{K}[x]$, for each $\psi \in \Psi$ suppose $\alpha_\psi, \beta_\psi \in \mathbb{Q}[x]$ satisfy

$$\xi \equiv \alpha_\psi \bmod r_\psi(x) \qquad \text{and} \qquad \xi \equiv \beta_\psi \bmod \overline{r_\psi}(x). \tag{4.10}$$

Suppose that

$$\prod_{\psi\in\Psi}\alpha_\psi(\gamma)=1 \qquad \text{and} \qquad \prod_{\psi\in\Psi}\beta_\psi(\gamma)=\zeta, \tag{4.11}$$

where $\zeta\in L$ is a primitive kth root of unity. Then $\pi(x)=\mathcal{N}_\Psi(\xi)\in K[x]$ satisfies

1. $\pi(x)\overline{\pi}(x)\in\mathbb{Q}[x]$,
2. $\mathcal{N}_{K/\mathbb{Q}}(\pi(x)-1)\equiv 0 \bmod r(x)$, *and*
3. $\Phi_k(\pi(x)\overline{\pi}(x))\equiv 0 \bmod r(x)$.

Proof. Statement (1) follows from Remark 4.4.5 and the fact that $\pi(x)\overline{\pi}(x)=\mathcal{N}_{\widehat{K}/\mathbb{Q}}\xi$. Next, (4.10) implies that $\xi-\alpha_\psi=fr_\psi$ for some $f\in\widehat{K}[x]$, so $\psi'^{-1}(\gamma)\in L$ is a root of $\xi-\alpha_\psi\in\widehat{K}[x]$. Applying ψ' to this expression and using the fact that $\alpha_\psi\in\mathbb{Q}[x]$, we see that γ is a root of $\psi(\xi)-\alpha_\psi\in L[x]$. It follows that $(\psi(\xi))(\gamma)=\alpha_\psi(\gamma)$, and by the same reasoning, $(\overline{\psi}(\xi))(\gamma)=\beta_\psi(\gamma)$. Now since $\pi(\gamma)=\prod_{\psi\in\Psi}(\psi(\xi))(\gamma)$ by definition of the extended type norm, we conclude from (4.11) that $\pi(\gamma)=1$ and $\overline{\pi}(\gamma)=\zeta$, from which statements (2) and (3) follow. □

If $\pi(x)$ and $r(x)$ are as in Theorem 4.4.7, then by Corollary 1.2.3 for any $x_0\in\mathbb{Q}$ for which $q=\pi(x_0)\overline{\pi}(x_0)$ is a prime, the algebraic integer $\pi(x_0)\in\mathcal{O}_K$ is the Frobenius element of an abelian variety over $\mathbb{F}_q$ that has embedding degree k with respect to $r(x_0)$. We can thus view $\pi(x)$ as defining a one-parameter "family" of pairing-friendly Frobenius elements. The following definition formalizes this concept, generalizing Definition 2.2.3.

Definition 4.4.8. Let K be a CM field of degree $2g$, let $\pi(x)\in K[x]$, and let $r(x)\in\mathbb{Q}[x]$. We say that (π,r) *represents a family of g-dimensional abelian varieties with embedding degree k* if:

1. $q(x)=\pi(x)\overline{\pi}(x)$ is in $\mathbb{Q}[x]$.
2. $q(x)$ represents primes (in the sense of Definition 2.2.1).
3. $r(x)$ is non-constant, irreducible, and integer-valued, and has positive leading coefficient.
4. $\mathcal{N}_{K/\mathbb{Q}}(\pi(x)-1)\equiv 0 \bmod r(x)$.
5. $\Phi_k(q(x))\equiv 0 \bmod r(x)$, where Φ_k is the kth cyclotomic polynomial.

With our setup, we can now adapt Algorithm 4.2.6 to our new context.

Algorithm 4.4.9.

Input: a primitive CM type (K, Φ); its reflex type $(\widehat{K}, \Psi)$; a positive integer k; a polynomial $r(x) \in \mathbb{Q}[x]$, satisfying condition (3) of Definition 4.4.8, such that $\mathbb{Q}[x]/(r(x))$ is a Galois number field containing K and the cyclotomic field $\mathbb{Q}(\zeta_k)$; and a non-empty set $\Sigma \subset \mathbb{Q}[x]$.

Output: a polynomial $\pi(x) \in K[x]$ such that if $q(x) = \pi(x)\overline{\pi}(x)$ represents primes (in the sense of Definition 2.2.1), then (π, r) represents a family of abelian varieties with embedding degree k (in the sense of Definition 4.4.8).

1. Set $\widehat{g} \leftarrow \frac{1}{2} \deg \widehat{K}$ and write $\Psi = \{\psi_1, \psi_2, \ldots, \psi_{\widehat{g}}\}$. Set $L \leftarrow \mathbb{Q}[x]/(r(x))$.

2. Let $\gamma \in L$ be a root of $r(x)$. Compute the factorization of $r(x)$ in $\widehat{K}[x]$ as in Proposition 4.4.6.

3. Choose a primitive kth root of unity $\zeta \in L$.

4. Choose polynomials $\alpha_1, \ldots, \alpha_{\widehat{g}-1}, \beta_1, \ldots, \beta_{\widehat{g}-1} \in \mathbb{Q}[x]$ from Σ.

5. Compute $\alpha_{\widehat{g}} \in \mathbb{Q}[x]$ such that $\prod_{i=1}^{\widehat{g}} \alpha_i(\gamma) = 1$, and compute $\beta_{\widehat{g}} \in \mathbb{Q}[x]$ such that $\prod_{i=1}^{\widehat{g}} \beta_i(\gamma) = \zeta$.

6. Use the Chinese remainder theorem to compute $\xi \in \widehat{K}[x]$ such that $\xi \equiv \alpha_i \bmod r_{\psi_i}(x)$ and $\xi \equiv \beta_i \bmod \overline{r_{\psi_i}}(x)$ for $i = 1, 2, \ldots, \widehat{g}$.

7. Set $\pi(x) \leftarrow \mathcal{N}_{\Psi}(\xi)$, and return $\pi(x)$. □

We note that if K is a quadratic imaginary field, then Step (4) is empty and setting $q(x) = \pi(x)\overline{\pi}(x)$ and $t(x) = \pi(x) + \overline{\pi}(x)$ recovers the Brezing-Weng algorithm. In this case the polynomial $r(x)$ splits into two factors in $K[x]$ regardless of whether L is Galois, so we do not need the Galois hypothesis on L.

Given the output $\pi(x)$ of Algorithm 4.4.9, we can use Algorithm 2.2.4 to find an x_0 for which $q(x_0) = \pi(x_0)\overline{\pi}(x_0)$ is prime and $r(x_0)$ has a large prime factor. By Proposition 2.2.5, we expect that such an x_0 can be found in time that is linear in the degrees of π and r and quadratic in the desired bit size of x_0. By Lemma 4.2.1, in order for $\pi(x_0)$ to be the Frobenius element of an ordinary, simple abelian variety of dimension g, we need to confirm

that $\pi(x_0)$ generates K over $\mathbb{Q}$ and $q(x_0)$ is unramified in K. An analysis along the lines of Theorem 4.2.8 shows that these two conditions are satisfied with very high probability. Once the conditions are checked, we can then use the CM methods described in Section 1.2.4 to construct an explicit abelian variety A over $\mathbb{F}_{q(x_0)}$ with embedding degree k.

4.5 Parameter selection in Algorithm 4.4.9 and examples

The primary advantage of Algorithm 4.4.9 over Algorithm 4.2.6 is that the former leads to pairing-friendly abelian varieties with smaller ρ-values than the latter. Recall that the ρ-value of a g-dimensional abelian variety over $\mathbb{F}_q$ with respect to a subgroup of order r is $\rho = g \log q / \log r$. If $q = q(x)$ and $r = r(x)$ are parametrized as polynomials, then for large x the ρ-value approaches $g \deg q / \deg r$. This motivates the definition of a ρ-value for a family of pairing-friendly abelian varieties.

Definition 4.5.1. Suppose (π, r) represents a family of g-dimensional abelian varieties with embedding degree k, and let $q(x) = \pi(x)\overline{\pi}(x)$. The *$\rho$-value of the family represented by* (π, r), denoted $\rho(\pi, r)$, is

$$\rho(\pi, r) = \lim_{x \to \infty} \frac{g \log q(x)}{\log r(x)} = \frac{g \deg q(x)}{\deg r(x)}.$$

The key feature of Algorithm 4.4.9 is that the polynomial ξ constructed by the Chinese remainder theorem in Step (6) can always be chosen to have degree strictly less than $\deg r$, and thus $\deg \pi \leq \widehat{g}(\deg r - 1)$. We thus obtain

$$\rho(\pi, r) = 2g\widehat{g}\frac{\deg \xi}{\deg r} \leq 2g\widehat{g}\frac{\deg r - 1}{\deg r}.$$

This asymptotic ρ-value is an improvement over the ρ-values produced by Algorithm 4.2.6, which by Theorem 4.3.1 gives expected ρ-values very close to $\rho \approx 2g\widehat{g}$ for varieties of cryptographic size.

To improve the ρ-values further one would try to choose the inputs to Algorithm 4.4.9 in some clever manner so that the π produced has degree significantly less than $\widehat{g} \deg r$. These choices include the ζ of Step (3), the α_i and β_i of Step (4) (which are chosen from the input Σ), and the input polynomial $r(x)$.

In Section 2.5 we saw a number of methods for computing an optimal π in the case of elliptic curves, where there are only ζ and $r(x)$ to consider. In higher dimensions we search

for a $\pi(x)$ of low degree by following the model of Brezing and Weng described in Section 2.5.1. We let $r(x)$ be a cyclotomic polynomial Φ_ℓ such that $k \mid \ell$ and $L \cong \mathbb{Q}(\zeta_\ell)$ contains the specified CM field K. Since L is abelian, in this case the CM field K must also be abelian, and thus equal to the reflex field $\widehat{K}$. We choose the α_i, β_i all to be polynomials that reduce to roots of unity (of any order) in L. Since $r(x)$ is the ℓth cyclotomic polynomial, x is a primitive ℓth root of unity in $\mathbb{Q}[x]/(r_\psi(x))$ for all $\psi \in \Psi$. Thus if we choose α_i, β_i as

$$(\alpha_1, \ldots, \alpha_g) \in \{(x^{a_1}, \ldots, x^{a_g}) : 0 \le a_i < \ell,\ \textstyle\sum_{i=1}^g a_i = 0\}, \tag{4.12}$$

$$(\beta_1, \ldots, \beta_g) \in \left\{(x^{b_1}, \ldots, x^{b_g}) : 0 \le b_i < \ell,\ \gcd(\ell, \textstyle\sum_{i=1}^g b_i) = \ell/k\right\}, \tag{4.13}$$

then $\prod \alpha_i = x^{\sum a_i} \equiv 1 \bmod r(x)$, and $\prod \beta_i = x^{\sum b_i}$ is a primitive kth root of unity mod $r(x)$.

4.5.1 Dimension 2

For given CM type (K, Φ), embedding degree k, and cyclotomic polynomial $r(x) = \Phi_\ell(x)$, our implementation of Algorithm 4.4.9 searches through all α_i, β_i satisfying (4.12) and (4.13) and returns the ξ of smallest degree. We illustrate with a detailed example for $g = 2$ that produces ρ-values around 4, thus answering (in one case) Open Problem 4.3.2.

Example 4.5.2 ($g = 2, k = 5, \rho = 4$)**.** Let $K = \mathbb{Q}(\zeta_5)$, $k = 5$, and

$$r(x) = \Phi_5(x) = x^4 + x^3 + x^2 + x + 1.$$

We choose the CM type $\Phi = \{\phi_1, \phi_2\}$ where ϕ_1 is the identity and $\phi_2 : \zeta_5 \mapsto \zeta_5^3$. Then $\Psi = \{\psi_1, \psi_2\}$, where ψ_1 is the identity and $\psi_2 : \zeta_5 \mapsto \zeta_5^2$. If we use the root $\gamma = \zeta_5$ to factor $r(x)$ in $K[x]$ as in Proposition 4.4.6, we obtain

$$r(x) = r_1(x) r_2(x) \overline{r_1}(x) \overline{r_2}(x) = (x - \zeta_5)(x - \zeta_5^3)(x - \zeta_5^4)(x - \zeta_5^2).$$

We choose

$$\alpha_1 = x, \quad \alpha_2 = x^3, \quad \beta_1 = x, \quad \beta_2 = x^4$$

and use the Chinese remainder theorem to compute

$$\begin{aligned}\xi(x) = {} & \tfrac{1}{5}(-2\zeta_5^3 - 4\zeta_5^2 - \zeta_5 - 3)x^2 + \tfrac{1}{5}(-\zeta_5^3 - 2\zeta_5^2 + 2\zeta_5 + 1)x \\ & + \tfrac{1}{5}(-2\zeta_5^3 - 4\zeta_5^2 - \zeta_5 - 3).\end{aligned}$$

Taking the extended type norm $\mathcal{N}_\Phi(\xi)$ gives

$$\pi(x) = \tfrac{1}{5}(-\zeta_5^3 + \zeta_5^2 + \zeta_5 - 1)x^4 + \tfrac{1}{5}(\zeta_5^3 + 2\zeta_5 - 3)x^3 + \tfrac{1}{5}(3\zeta_5^2 + 4\zeta_5 - 2)x^2 + \tfrac{1}{5}(\zeta_5^3 + 2\zeta_5 - 3)x + \tfrac{1}{5}(-\zeta_5^3 + \zeta_5^2 + \zeta_5 - 1), \tag{4.14}$$

and we compute

$$q(x) = \pi(x)\overline{\pi}(x) = \tfrac{1}{5}\left(x^8 + 2x^7 + 8x^6 + 9x^5 + 15x^4 + 9x^3 + 8x^2 + 2x + 1\right).$$

Since $q(x)$ is irreducible and $q(1) = 11$ and $q(-4) = 11941$ are distinct primes, $q(x)$ represents primes as in Definition 2.2.1, and thus (π, r) represents a family of abelian surfaces with embedding degree 5.

Let us construct an example abelian surface in this family. We input $y_0 = 2^{54}$ to Algorithm 2.2.4. Using $a = 5$ and $b = 1$ in Step (1), the algorithm outputs $h = 5$ and $x_0 = 90071992547410826$. We then compute

$$\begin{aligned} r(x_0) &= 5 \cdot 131640364585701781315832859207623600506738373421858387002808795266 51 \\ q(x_0) &= 866459279412824385938792486752217637176780280467936882241506648125593297263812468035 9 \backslash \\ &\quad 567670957526027076700398139345585675165846688475 61 \quad \text{(449 bits)}. \end{aligned}$$

Then $r(x_0)$ is 5 times a 224-bit prime r_0. The Frobenius element $\pi(x_0) \in \mathbb{Q}(\zeta_5)$ can be computed from (4.14), and the number of points n is

$$\begin{aligned} N_{K/\mathbb{Q}}(\pi(x_0) - 1) &= 75075168288059088075871172602962817897209439480106038613987715530997005372 4 \backslash \\ &\quad 325739795315304263728043006622715158418852616320709984510863881685818554792 \backslash \\ &\quad 291764148781436936054052813749689440867929088179317241437357723407745744526 \backslash \\ &\quad 071772162827435691962393142167332744537571805. \end{aligned}$$

Over any field $\mathbb{F}$ there is a single $\overline{\mathbb{F}}$-isomorphism class of abelian surfaces whose ring of $\overline{\mathbb{F}}$-endomorphisms is isomorphic to $\mathbb{Z}[\zeta_5]$. If $\operatorname{char}\mathbb{F}$ is prime to 10, then this abelian surface is isomorphic (over $\overline{\mathbb{F}}$) to the Jacobian of $C : y^2 = x^5 + 1$. Over $\mathbb{F}$ we must find the twist of C that is in the correct $\mathbb{F}$-isogeny class; i.e., has a Jacobian with the correct number of $\mathbb{F}$-rational points. By choosing a random point P on each twist and seeing whether $[n]P = O$, we find that the correct curve over $\mathbb{F} = \mathbb{F}_{q(x_0)}$ is

$$C : y^2 = x^5 + 5.$$

The ρ-value of $\operatorname{Jac}(C)$ with respect to the subgroup of order r_0 is 4.02. □

Table 4.1: Quartic CM fields K contained in cyclotomic fields $\mathbb{Q}(\zeta_\ell)$ with $\varphi(\ell) \leq 16$.

K	ℓ
$\mathbb{Q}(\zeta_5)$	$5, 10, 15, 20, 30, 40, 60$
$\mathbb{Q}(\sqrt{-13+2\sqrt{13}})$	$13, 26$
$\mathbb{Q}(\sqrt{-2+\sqrt{2}})$	$16, 32, 48$
$\mathbb{Q}(\sqrt{-5+\sqrt{5}})$	40
$\mathbb{Q}(\sqrt{-6+3\sqrt{2}})$	48
$\mathbb{Q}(\sqrt{-30+6\sqrt{5}})$	60

Remark 4.5.3. The abelian surface $A = \mathrm{Jac}(C)$ computed in Example 4.5.2 has the property that the bit size of the field $\mathbb{F}_{q^k}$ in which pairings on A take their values is roughly $\rho k/g = 10$ times the bit size of the prime-order subgroup $A[r]$. It follows that A is suitable for applications with security level equivalent to a 112-bit symmetric-key system (cf. Table 1.1 and Section 3.1.1). In addition, since the curve C has a degree-10 twist, we expect that twisting methods such as those developed for elliptic curves [97] can be used to increase the speed of pairing computation on the Jacobian and reduce the size of the input.

We ran Algorithm 4.4.9 for all degree-4 CM fields K that are primitive (i.e., do not contain a quadratic imaginary subfield) and are contained in a cyclotomic field $\mathbb{Q}(\zeta_\ell)$ with $\varphi(\ell) \leq 16$. Such fields are necessarily Galois cyclic. These fields, and the corresponding values of ℓ, appear in Table 4.1. We let the inputs to the algorithm range over all such K and ℓ and embedding degrees k dividing ℓ. Given an η such that $K = \mathbb{Q}(\eta)$, we let Φ be the CM type that consists of embeddings ϕ_i such that $\phi_i(\eta)$ all have positive imaginary part. We tested all choices of α_i, β_i satisfying (4.12) and (4.13), and computed the ξ of smallest degree that produces a $q(x)$ that represents primes in the sense of Definition 2.2.1. Some examples appear below.

Example 4.5.4 ($g = 2, k = 10, \rho = 6$)**.** Let $K = \mathbb{Q}(\zeta_5)$, $k = 10$, $r(x) = \Phi_{10}(x) = x^4 - x^3 + x^2 - x + 1$. Algorithm 4.2.6 outputs

$$\begin{aligned}\pi(x) =& \tfrac{1}{25}(\zeta_5^3 - \zeta_5^2 - \zeta_5 + 1)x^6 + \tfrac{1}{25}(-6\zeta_5^3 + 5\zeta_5^2 + 3\zeta_5 - 2)x^5 + \tfrac{1}{5}(2\zeta_5^3 - \zeta_5^2 - 2)x^4 + \tfrac{1}{5}(-2\zeta_5^3 \\ & - \zeta_5 + 4)x^3 + \tfrac{1}{5}(3\zeta_5^3 - 2\zeta_5^2 - 2)x^2 + \tfrac{1}{25}(-4\zeta_5^3 - \zeta_5^2 - \zeta_5 + 11)x + \tfrac{1}{25}(4\zeta_5^3 - 5\zeta_5^2 - 2\zeta_5 - 2).\end{aligned}$$

The ρ-value of this family is 6. On input $y_0 = 2^{40}$, Algorithm 2.2.4 outputs $h = 5$ and

$x_0 = 5497558154509$. We find that A is the Jacobian of the genus 2 curve

$$C : y^2 = x^5 + 15.$$

Then $r(x_0)$ is 5 times a 168-bit prime r_0. The ρ-value of A with respect to r_0 is within 10^{-10} of 6. □

Example 4.5.5 $(g = 2, k = 16, \rho = 7)$**.** Let $K = \mathbb{Q}(\eta)$, where $\eta = \sqrt{-2+\sqrt{2}}$. Let $k = 16$ and $r(x) = \Phi_{16}(x) = x^8 + 1$. Algorithm 4.4.9 outputs

$$\begin{aligned}\pi(x) = &\tfrac{1}{64}(-\eta^2-2)x^{14} + \tfrac{1}{32}(-\eta^2-3\eta-2)x^{13} + \tfrac{1}{64}(\eta^2-4\eta-16)x^{12} + \tfrac{1}{16}(-2\eta^3+\eta^2-6\eta\\ &+5)x^{11} + \tfrac{1}{64}(-8\eta^3+\eta^2-28\eta)x^{10} + \tfrac{1}{32}(4\eta^3-\eta^2+7\eta-2)x^9 + \tfrac{1}{64}(8\eta^3-\eta^2+16\eta\\ &-34)x^8 + \tfrac{1}{8}(-\eta^3-2\eta+4)x^7 + \tfrac{1}{64}(-8\eta^3-\eta^2-16\eta-2)x^6 + \tfrac{1}{32}(4\eta^3-\eta^2+13\eta-2)x^5\\ &+\tfrac{1}{64}(8\eta^3+\eta^2+28\eta-16)x^4 + \tfrac{1}{16}(\eta^2+2\eta+5)x^3 + \tfrac{1}{64}(\eta^2+4\eta)x^2 + \tfrac{1}{32}(-\eta^2-\eta-2)x\\ &+\tfrac{1}{64}(-\eta^2-2).\end{aligned}$$

The ρ-value of this family is 7. The single $\overline{\mathbb{Q}}$-isomorphism class of genus 2 curves whose Jacobians have CM by $\mathcal{O}_K$ is given by van Wamelen [124]. On input $y_0 = 2^{18}$, Algorithm 2.2.4 outputs $h = 2$ and $x_0 = 1083939$. We find A to be the Jacobian of the genus 2 curve

$$C : y^2 = x^5 + 3x^4 - 2x^3 - 6x^2 + 3x + 1.$$

Then $r(x_0)$ is 2 times a 160-bit prime r_0. The ρ-value of A with respect to r_0 is 6.91. □

Example 4.5.6 $(g = 2, k = 13, \rho = 20/3)$**.** Let $K = \mathbb{Q}(\eta)$, where $\eta = \sqrt{-13+2\sqrt{13}}$. Let $k = 13$ and let

$$r(x) = \Phi_{13}(x) = x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1.$$

Algorithm 4.4.9 outputs

$$\begin{aligned}\pi(x) = &\tfrac{1}{4056}(-19\eta^3+183\eta^2-377\eta+2301)x^{20} + \tfrac{1}{338}(-2\eta^3+7\eta^2-39\eta+78)x^{19} + \tfrac{1}{4056}(23\eta^3\\ &+177\eta^2+481\eta+2535)x^{18} + \tfrac{1}{1352}(7\eta^3+49\eta^2+65\eta+767)x^{17} + \tfrac{1}{2028}(19\eta^3+141\eta^2\\ &+221\eta+1755)x^{16} + \tfrac{1}{1352}(\eta^3+97\eta^2-65\eta+1183)x^{15} + \tfrac{1}{2028}(31\eta^3+192\eta^2+377\eta\\ &+2496)x^{14} + \tfrac{1}{1352}(13\eta^3+173\eta^2+195\eta+2587)x^{13} + \tfrac{1}{26}(3\eta^2-2\eta+39)x^{12} + \tfrac{1}{52}(\eta^3+8\eta^2\\ &+11\eta+104)x^{11} + \tfrac{1}{312}(5\eta^3+33\eta^2+55\eta+507)x^{10} + \tfrac{1}{78}(2\eta^3+9\eta^2+28\eta+117)x^9\\ &+\tfrac{1}{312}(5\eta^3+33\eta^2+55\eta+507)x^8 + \tfrac{1}{4056}(97\eta^3+441\eta^2+1235\eta+5811)x^7 + \tfrac{1}{338}(2\eta^3\\ &+32\eta^2+13\eta+429)x^6 + \tfrac{1}{2028}(8\eta^3+165\eta^2+52\eta+2535)x^5 + \tfrac{1}{1352}(19\eta^3+81\eta^2+273\eta\\ &+923)x^4 + \tfrac{1}{338}(-\eta^3+9\eta^2-26\eta+130)x^3 + \tfrac{1}{4056}(23\eta^3+99\eta^2+325\eta+1521)x^2\\ &+\tfrac{1}{2028}(8\eta^3+3\eta^2+130\eta+39)x + \tfrac{1}{338}(-\eta^2-13).\end{aligned}$$

Table 4.2: Best ρ-values for families of abelian surfaces.

k	CM field K	$r(x)$	ρ-value	k	CM field K	$r(x)$	ρ-value
6	$\mathbb{Q}(\sqrt{-6+3\sqrt{2}})$	$\Phi_{48}(x)$	7.5	30	$\mathbb{Q}(\zeta_5)$	$\Phi_{60}(x)$	7
8	$\mathbb{Q}(\sqrt{-5+\sqrt{5}})$	$\Phi_{40}(x)$	7.5	32	$\mathbb{Q}(\sqrt{-2+\sqrt{2}})$	$\Phi_{32}(x)$	7.5
15	$\mathbb{Q}(\zeta_5)$	$\Phi_{15}(x)$	7	40	$\mathbb{Q}(\zeta_5)$	$\Phi_{40}(x)$	6.5
20	$\mathbb{Q}(\zeta_5)$	$\Phi_{20}(x)$	6	60	$\mathbb{Q}(\zeta_5)$	$\Phi_{60}(x)$	7

The ρ-value of this family is 20/3. The single $\overline{\mathbb{Q}}$-isomorphism class of genus 2 curves whose Jacobians have CM by $\mathcal{O}_K$ is given by van Wamelen [124]. On input $y_0 = 7 \cdot 2^{15}$, Algorithm 2.2.4 outputs $h = 13$ and $x_0 = 3127658$. We find A to be the Jacobian of the genus 2 curve

$$C : y^2 = x^5 + 104x^4 + 5408x^3 + 140608x^2 + 1687296x + 7311616.$$

Then $r(x_0)$ is 13 times a 256-bit prime r_0. The ρ-value of A with respect to r_0 is 6.74. □

Some additional families we obtained for $g = 2$ are summarized in Table 4.2. The $\pi(x)$ produced by Algorithm 4.4.9 and example varieties of cryptographic size can be found in Appendix A.2.

We restrict to $r(x)$ of degree at most 16 because as the degree of $r(x)$ grows it becomes increasingly unlikely that we will find families with ρ-values significantly less than 8. For the same reason, we expect that non-Galois quartic CM fields K will not provide greatly improved ρ-values, as we must work in a field L that contains the compositum of the Galois closure of K and the cyclotomic field $\mathbb{Q}(\zeta_k)$, so if $k \geq 3$ then L must have degree at least 16 over $\mathbb{Q}$.

4.5.2 Dimension 3

In dimension $g = 3$, we applied the procedure described in Section 4.5.1 to the degree-6 Galois CM field $\mathbb{Q}(\zeta_7)$. The family we discovered produces three-dimensional ordinary abelian varieties with ρ-values better than the best examples produced by Algorithm 4.2.6, which have $\rho \approx 18$.

Example 4.5.7 $(g = 3, k = 7, \rho = 12)$**.** Let $K = \mathbb{Q}(\zeta_7)$, $k = 7$, and

$$r(x) = \Phi_7(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1.$$

Algorithm 4.4.9 outputs

$$\begin{aligned}\pi(x) =& \tfrac{1}{49}(-2\zeta_7^5 - 2\zeta_7^3 - 2\zeta_7^2 + 6\zeta_7)x^{12} + \tfrac{1}{49}(-7\zeta_7^5 + 4\zeta_7^4 - 4\zeta_7^3 + 2\zeta_7^2 + 13\zeta_7 - 1)x^{11} + \tfrac{1}{49}(-9\zeta_7^5 \\ &+ 10\zeta_7^4 - 2\zeta_7^3 + \zeta_7^2 + 23\zeta_7 + 5)x^{10} + \tfrac{1}{49}(-16\zeta_7^5 + 9\zeta_7^4 - 13\zeta_7^3 - 2\zeta_7^2 + 45\zeta_7 - 2)x^9 \\ &+ \tfrac{1}{49}(-22\zeta_7^5 + 6\zeta_7^4 - 19\zeta_7^3 + 3\zeta_7^2 + 39\zeta_7 - 7)x^8 + \tfrac{1}{49}(-7\zeta_7^5 + 13\zeta_7^4 - 2\zeta_7^3 - 2\zeta_7^2 + 28\zeta_7 \\ &+ 12)x^7 + \tfrac{1}{7}(-2\zeta_7^5 + \zeta_7^4 - 2\zeta_7^3 + \zeta_7^2 + 3\zeta_7 - 1)x^6 + \tfrac{1}{49}(-12\zeta_7^5 - 7\zeta_7^4 - 26\zeta_7^3 - 12\zeta_7^2 + 8\zeta_7)x^5 \\ &+ \tfrac{1}{49}(-7\zeta_7^5 + 3\zeta_7^4 - 10\zeta_7^3 + 5\zeta_7^2 + 8\zeta_7 - 6)x^4 + \tfrac{1}{49}(2\zeta_7^5 + 4\zeta_7^4 + 2\zeta_7^3 - \zeta_7^2 + 5\zeta_7 + 9)x^3 \\ &+ \tfrac{1}{49}(-5\zeta_7^5 - 2\zeta_7^4 - 8\zeta_7^3 + 2\zeta_7^2 - 3\zeta_7 - 5)x^2 + \tfrac{1}{49}(\zeta_7^5 + \zeta_7^4 - 2\zeta_7^3 - 3\zeta_7^2 + 3\zeta_7)x + \tfrac{1}{49}(\zeta_7^4 \\ &+ 2\zeta_7^3 + 2\zeta_7^2 + 2)\end{aligned}$$

The ρ-value of this family is 12. The single $\overline{\mathbb{Q}}$-isomorphism class of genus 3 curves whose Jacobians have CM by $\mathcal{O}_K$ is given by $y^2 = x^7 + 1$. On input $y_0 = 2^{28}$, Algorithm 2.2.4 outputs $h = 7$ and $x_0 = 1879056152$. We find A to be the Jacobian of the genus 3 curve

$$C : y^2 = x^7 + 16.$$

Then $r(x_0)$ is 7 times a 183-bit prime r_0. The ρ-value of A with respect to r_0 is 12.10. □

We also ran our algorithm for the degree-6 CM field $\mathbb{Q}(\zeta_9)$ and found families with ρ-values of 15 for $k = 9$ and $k = 18$. The $\pi(x)$ output by the algorithm and example varieties of cryptographic size can be found in Appendix A.3. Abelian varieties with CM by $\mathbb{Q}(\zeta_9)$ are Jacobians of Picard curves of the form $y^3 = x^4 + ax$ [70]. Since these curves are not hyperelliptic, by Proposition 1.2.5 for any q-Weil number $\pi \in \mathbb{Z}[\zeta_9]$ there is a curve $C/\mathbb{F}_q$ whose Jacobian has Frobenius element either π or $-\pi$. In the second case the abelian variety over $\mathbb{F}_q$ with Frobenius element π is the quadratic twist of $\mathrm{Jac}(C)$, and is not isomorphic over $\mathbb{F}_q$ to a Jacobian.

Future Directions

Algorithm 4.4.9 improves on the best known ρ-values of pairing-friendly ordinary abelian varieties of dimension $g \geq 2$ for many different choices of CM field K and embedding degree k. However, to make ordinary abelian varieties of dimension $g \geq 2$ competitive with elliptic curves in terms of performance, we must construct varieties with $\rho \leq 2$, with the ultimate goal of producing ρ-values close to 1. Achieving this goal is the most important problem for further work.

Our construction leaves a great deal of room for searching for better parameters. One direction would be to choose various Galois CM fields K and let $L = K(\zeta_k)$. Another approach would be to fix K and L and use the approach of Kachisa, Schaefer, and Scott

[62] to search systematically through polynomials $r(x)$ such that $L \cong \mathbb{Q}[x]/(r(x))$. In the case where $g \geq 2$, one could also increase the size of the input Σ, which is the set from which we choose the residues α_i, β_i of ξ modulo factors of $r(x)$ in $\widehat{K}[x]$. In practice we find that when we use elements of Σ with large coefficients, the $q(x)$ computed have coefficients with large denominators and are thus unlikely to take integer values. However, even restricting Σ to contain only polynomials with small coefficients leaves many possible choices for α_i and β_i, and a program that searches systematically through these choices should have a good chance of finding improved ρ-values.

Chapter 5

Implementing the Genus 2 CM Method via the Chinese Remainder Theorem

5.1 Introduction

In this chapter we study the genus 2 case of the complex multiplication methods discussed in Section 1.2.4. These methods are used not only to construct the pairing-friendly abelian varieties discussed in previous chapters, but also to construct abelian varieties in any situation where a specified number of points is desired. CM methods are especially relevant in genus 2, as Schoof-like point-counting methods are currently too slow to be applicable to abelian surfaces over prime fields of 128 bits or larger [11], and thus Jacobians of random curves cannot be used for applications requiring medium to high security levels.

The genus 2 CM method constructs genus 2 curves whose Jacobians have CM by the ring of integers $\mathcal{O}_K$ of a given quartic CM field K. The central part of the procedure is computing the Igusa class polynomials for K. These polynomials are defined as follows.

Definition 5.1.1. Given a genus 2 curve C over any field, let $(j_1(C), j_2(C), j_3(C))$ be the absolute Igusa invariants of C (see [124, p. 313] or [54, §5.2] for definitions[†]). For a given primitive quartic CM field K, let $\mathcal{C}_K$ be a set consisting of one representative from each $\mathbb{C}$-

[†]We observe that Goren and Lauter's definition of the third invariant in terms of modular forms [54, p. 472] is incorrect: the coefficient of $\psi_4\chi_{10}^{-4}\chi_{12}^3$ should be $2^{-3}\cdot 3^2$ instead of $2^2\cdot 3$.

isomorphism class of genus 2 curves $C/\mathbb{C}$ such that $\mathrm{End}(\mathrm{Jac}(C)) \cong \mathcal{O}_K$. Then for $i = 1, 2, 3$, the ith *Igusa class polynomial* for K is

$$H_i(x) = \prod_{C \in \mathcal{C}_K} (x - j_i(C)).$$

The fact that $\mathcal{C}_K$ is finite follows from [115, Chapter II, Proposition 17]. It follows from Definition 5.1.1 that given the Igusa class polynomials for K, we can construct genus 2 curves with CM by $\mathcal{O}_K$ by applying Mestre's algorithm [88] to triples of roots of the polynomials. We also note that since any CM abelian variety in characteristic zero is defined over $\overline{\mathbb{Q}}$ [115, Chapter III, Proposition 26], the group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ permutes the set of triples $(j_1(C), j_2(C), j_3(C))$ and thus the $H_i(x)$ have rational coefficients.

In this chapter we study the implementation of Eisenträger and Lauter's Chinese remainder theorem algorithm for computing the Igusa class polynomials [34]. The fundamental theorem underlying the algorithm is the following:

Theorem 5.1.2 ([34, Theorem 2])**.** *Let K be a primitive quartic CM field. Let p be a rational prime that splits completely in K and splits completely into principal ideals in $\widehat{K}$, the reflex field of K. For $i = 1, 2, 3$, let $H_{i,p}(x)$ be the reduction mod p of the Igusa class polynomial $H_i(x)$. Let $\mathcal{C}_{p,K}$ be a set consisting of one representative from each $\overline{\mathbb{F}}_p$-isomorphism class of genus 2 curves $C/\overline{\mathbb{F}}_p$ such that $\mathrm{End}(\mathrm{Jac}(C)) \cong \mathcal{O}_K$. Then $H_{i,p}(x)$ is well-defined (i.e., p does not divide the denominator of any coefficient of $H_i(x)$), and*

$$H_{i,p}(x) = \prod_{C \in \mathcal{C}_{p,K}} (x - j_i(C)). \tag{5.1}$$

□

Eisenträger and Lauter used this theorem to give an algorithm that takes as input a primitive quartic CM field K and an integer λ that is a multiple of the denominators of all coefficients of the $H_i(x)$, and produces the Igusa class polynomials of K. The basic outline of the algorithm is as follows:

1. Define S to be a set of small primes with splitting behavior as in Theorem 5.1.2, such that the product of all the primes is larger than λ times any coefficient of $H_i(x)$.

2. For each prime p in S:

(a) For each triple $(j_1, j_2, j_3) \in \mathbb{F}_p^3$ of Igusa invariants, construct a genus 2 curve C over $\mathbb{F}_p$ corresponding to that triple.

(b) Find the subset of curves C from (2a) for which the endomorphism ring of $\mathrm{Jac}(C)$ is the full ring of integers $\mathcal{O}_K$.

(c) Use equation (5.1) to construct the Igusa class polynomials mod p from the triples collected in Step (2b).

3. Use the bound λ on denominators and either the Chinese remainder theorem or the Explicit CRT [12] to construct the Igusa polynomials either with rational coefficients or modulo a prime of cryptographic size, respectively.

It is a result of Igusa (see [22, §1]) that the set of curves computed in Step (1) consists of one curve from each $\overline{\mathbb{F}}_p$-isomorphism class of genus 2 curves over $\mathbb{F}_p$. We note that at present there is no effective way of computing the bounds on the coefficients of Step (1), and thus we cannot prove that the output is correct. However, heuristically we expect the case where the output is incorrect to be exceedingly rare.

Our main contribution is to provide an efficient probabilistic algorithm for Step (2b) of the Eisenträger-Lauter CRT algorithm: determining whether the endomorphism ring of a Jacobian of a genus 2 curve over a small prime field is the ring of integers in a given quartic CM field K. Using this algorithm, we have implemented a probabilistic version of the full CRT algorithm (Algorithm 5.7.1) in MAGMA [18] and used it to compute Igusa class polynomials for several fields K with small discriminant.

It was previously believed that determining endomorphism rings would be the bottleneck in the genus 2 CRT algorithm. Our results are surprising in the sense that we find that the time taken to determine the endomorphism rings using our probabilistic algorithms is negligible compared with the time needed to compute p^3 genus 2 curves via Mestre's algorithm for each small prime p. For example, for $K = \mathbb{Q}(i\sqrt{13 + 2\sqrt{13}})$ and $p = 157$, the largest prime for which endomorphism rings are computed for this K, our (unoptimized) MAGMA program takes about 52 minutes to loop through 157^3 curves and find 243 curves whose Jacobians have Frobenius element in $\mathcal{O}_K$. Our probabilistic algorithm (also implemented in MAGMA) applied to these 243 curves then takes 16.5 *seconds* to find the single curve whose Jacobian has endomorphism ring isomorphic to $\mathcal{O}_K$.

In Step (2) of the Eisenträger-Lauter algorithm we have fixed a small prime p and a CM field K. We compute a representative of each $\overline{\mathbb{F}}_p$-isomorphism class of genus 2 curves

over $\mathbb{F}_p$, and we wish to determine which of these p^3 curves have $\mathrm{End}(\mathrm{Jac}(C))$ isomorphic to $\mathcal{O}_K$. At a high level, our algorithm that determines endomorphism rings works as follows. Let C be a genus 2 curve over a finite field $\mathbb{F}_p$, and let J be its Jacobian; we assume J is ordinary. Let K be a primitive quartic CM field. The first test is whether $\mathrm{End}(J)$, the endomorphism ring of J, is some order in $\mathcal{O}_K$. This computation is outlined in [34, Section 5] and described in more detail in Section 5.2 below. If $\mathrm{End}(J)$ is an order in $\mathcal{O}_K$, we compute a set of possible elements $\pi \in \mathcal{O}_K$ that could represent the Frobenius endomorphism of J. If π represents the Frobenius endomorphism, then its complex conjugate $\overline{\pi}$ represents the Verschiebung endomorphism (i.e., the dual of the Frobenius endomorphism).

We next determine a set $\{\alpha_i\}$ of elements of $\mathcal{O}_K$ such that $\mathbb{Z}[\pi, \overline{\pi}, \{\alpha_i\}] = \mathcal{O}_K$. It follows that $\mathrm{End}(J) = \mathcal{O}_K$ if and only if each α_i is an endomorphism of J. In Section 5.3 we describe such a set $\{\alpha_i\}$ in which each element has one of two forms: either $\alpha_i = \frac{\pi^k - 1}{\ell}$ for some positive integer k and prime ℓ, or $\alpha_i = \frac{h_i(\pi)}{\ell^d}$ for some cubic polynomial h_i with integer coefficients and some prime power ℓ^d. In Section 5.4 we show how to determine whether an element of the first form is an endomorphism; this is equivalent to determining the field of definition of the ℓ-torsion points of J. In Section 5.5 we show how to determine whether an element of the second form is an endomorphism; this is equivalent to computing the action of Frobenius on a basis of $J[\ell^d]$. The main results are Algorithms 5.4.3 and 5.5.1, two very efficient probabilistic algorithms which check fields of definition and compute the action of Frobenius, respectively. The running times of these algorithms depend primarily on the sizes of the fields over which the points of $J[\ell^d]$ are defined. Section 5.6 provides upper bounds for these sizes in terms of the prime ℓ and the size of the base field p.

A detailed statement of the Eisenträger-Lauter CRT algorithm, incorporating the algorithms of Sections 5.2, 5.4, and 5.5, appears in Section 5.7. Section 5.8 describes various ways in which we have modified our MAGMA implementation to improve the algorithm's performance. Finally, in Section 5.9 we give examples of our algorithm run on several small quartic CM fields.

The material in this chapter is joint work with Kristin Lauter of Microsoft Research (USA) and has also appeared in [40].

5.2 Computing zeta functions and the Frobenius element

To execute the Eisenträger-Lauter CRT algorithm, we fix a primitive quartic CM field K and choose various small primes p. We compute a representative of each $\overline{\mathbb{F}}_p$-isomorphism class of genus 2 curves over $\mathbb{F}_p$, and we wish to determine which of these p^3 curves have $\mathrm{End}(\mathrm{Jac}(C))$ isomorphic to $\mathcal{O}_K$. To make this determination, the first step is to determine whether the endomorphism ring is even an order in $\mathcal{O}_K$. Our hypotheses on p (see Theorem 5.1.2) imply that this can be accomplished by computing the characteristic polynomial of Frobenius, to see if the Frobenius element corresponds to an algebraic integer $\pi \in K$. This in turn is equivalent to determining the zeta function of C, which can be computed by finding the number of points on the curve and its Jacobian, $n = \#C(\mathbb{F}_p)$ and $m = \#J(\mathbb{F}_p)$. For a given field K there are several possibilities for the pairs (n, m), as described in [34, Proposition 4].

In this section we give an explicit algorithm that determines whether $\mathrm{End}(J)$ is an order in $\mathcal{O}_K$ and if so, gives a set $S \subset \mathcal{O}_K$ of possibilities for the Frobenius endomorphism of J. The main point is to find the possible Frobenius elements by finding generators of certain principal ideals (Step (2) below) with absolute value equal to $\sqrt{p}$ (Step (4a) below). We will assume throughout that J is ordinary.

Recall that a number field K is a *CM field* if it is an imaginary quadratic extension of a totally real field. We denote by K_0 the real quadratic subfield of K. A CM field is *primitive* if it has no proper CM subfields. We will assume unless otherwise noted that K is a primitive quartic CM field not isomorphic to $\mathbb{Q}(\zeta_5)$. This implies that K is either Galois cyclic or non-Galois, and that the only roots of unity in K are ± 1. We denote by $\widehat{K}$ the reflex field of K (see page 70 for a definition, and observe that the reflex field is the same for all CM types Φ on K). If K is Galois cyclic, then $\widehat{K} = K$; if K is non-Galois, then $\widehat{K}$ is another primitive quartic CM field [115, p. 64].

Algorithm 5.2.1. Let K be a primitive quartic CM field not isomorphic to $\mathbb{Q}(\zeta_5)$ and let $\widehat{K}$ be the reflex field of K. The following algorithm takes as input the field K, a prime p that splits completely in K and splits completely into principal ideals in $\widehat{K}$, and a curve C defined over the finite field $\mathbb{F}_p$. The algorithm returns `true` or `false` according to whether $\mathrm{End}(J)$ is an order in $\mathcal{O}_K$, where $J = \mathrm{Jac}(C)$. If the answer is `true`, the algorithm also outputs a set $S \subset \mathcal{O}_K$ that consists of the $\mathrm{Aut}(K/\mathbb{Q})$-orbit of the Frobenius endomorphism of J.

1. Compute the decomposition $p = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$ in $\mathcal{O}_K$, using e.g. [26, Algorithm 6.2.9]. Renumber so that $\mathfrak{p}_2 = \overline{\mathfrak{p}_1}$ and $\mathfrak{p}_3 = \overline{\mathfrak{p}_4}$.

2. Compute generators α_1 and α_2 for the principal ideals $\mathfrak{p}_1\mathfrak{p}_3$ and $\mathfrak{p}_2\mathfrak{p}_3$, respectively, using e.g. [26, Algorithm 6.5.10].

3. Compute a fundamental unit u of K_0 with $|u| > 1$, using e.g. [26, Algorithm 5.7.1].

4. For $i \leftarrow 1, 2$, do the following:

   (a) If $|\alpha_i| < \sqrt{p}$, set $\alpha_i \leftarrow \alpha_i u$ until $|\alpha_i| = \sqrt{p}$. If $|\alpha_i| > \sqrt{p}$, set $\alpha_i \leftarrow \alpha_i u^{-1}$ until $|\alpha_i| = \sqrt{p}$.

   (b) Compute the characteristic polynomial $h_i(x)$ of α_i over $\mathbb{Q}$, using e.g. [26, Proposition 4.3.4].

   (c) If K is Galois and $h_1(x) = h_2(-x)$, set $\alpha_2 \leftarrow -\alpha_2$ and $h_2(x) \leftarrow h_2(-x)$.

   (d) Set $(n_{i,+1}, m_{i,+1}) \leftarrow (p + 1 - \frac{h_i'(0)}{p}, h_i(1))$.

   (e) Set $(n_{i,-1}, m_{i,-1}) \leftarrow (p + 1 + \frac{h_i'(0)}{p}, h_i(-1))$.

5. Determine whether the Frobenius endomorphism of J has characteristic polynomial equal to $h_i(\pm x)$ for some i:

   (a) Choose a random point $P \in J(\mathbb{F}_p)$ and compute $Q_{j,\tau} = [m_{i,\tau}]P$ for $i \in \{1, 2\}$, $\tau \in \{\pm 1\}$. If none of $Q_{i,\tau}$ is the identity, return `false`. Otherwise, optionally repeat with another random point P.

   (b) If J passes a certain fixed number of trials of Step (5a), compute $\#C(\mathbb{F}_p)$. If $\#C(\mathbb{F}_p) \neq n_{i,\tau}$ for all $i \in \{1, 2\}$, $\tau \in \{\pm 1\}$, return `false`.

   (c) If $\#C(\mathbb{F}_p) = n_{i,\tau}$, compute $\#J(\mathbb{F}_p)$, using e.g. Baby-Step Giant-Step [26, Algorithm 5.4.1]. If $\#J \neq m_{i,\tau}$ for the same i, τ, return `false`.

6. If K is Galois, output $S = \{\tau\alpha_1, \tau\overline{\alpha_1}, \tau\alpha_2, \tau\overline{\alpha_2}\}$. If K is not Galois, output $S = \{\tau\alpha_i, \tau\overline{\alpha_i}\}$, using the i determined in Step (5c).

7. Return `true`.

Proof. The proof of [34, Proposition 4] shows that the ideals $\mathfrak{p}_1\mathfrak{p}_3$ and $\mathfrak{p}_2\mathfrak{p}_3$ are principal and the Frobenius endomorphism of J corresponds to a generator of one of these ideals or their

complex conjugates. Furthermore, this generator must have complex absolute value $\sqrt{p}$. The generators determined in Step (2) are unique up to unit multiple, so Step (4a) ensures that the absolute values are $\sqrt{p}$, thus making each α_i unique up to complex conjugation and sign. (Here we use the fact that the only roots of unity in K are ± 1.)

If the Frobenius element corresponds to α_i or $\overline{\alpha_i}$, then $h_i(x)$ is the characteristic polynomial of Frobenius, so we can determine this case by checking whether $\#C(\mathbb{F}_p) = n_{i,+1}$ and $\#J(\mathbb{F}_p) = m_{i,+1}$. Similarly, if the Frobenius element corresponds to $-\alpha_i$ or $-\overline{\alpha_i}$, then $h_i(-x)$ is the characteristic polynomial of Frobenius, so we can determine this case by checking whether $\#C(\mathbb{F}_p) = n_{i,-1}$ and $\#J(\mathbb{F}_p) = m_{i,-1}$.

If K is Galois (with Galois group C_4), then the ideal (α_2) is equal to $(\alpha_1)^\sigma$ for some σ generating the Galois group. Since complex absolute value squared is the same as the norm from K to its real quadratic subfield K_0, $|\alpha_1| = \sqrt{p}$ implies that $|\alpha_1^\sigma| = \sqrt{p}$. Since α_1^σ and α_2 both generate (α_2) and have absolute value $\sqrt{p}$, we deduce that $\alpha_1^\sigma = \pm\alpha_2$ or $\pm\overline{\alpha_2}$. Step (4c) ensures that this sign is positive, so α_1 and α_2 have the same characteristic polynomial $h_i(x)$, and thus the Frobenius element could be any of the elements output by Step (6). Since $\mathrm{Aut}(K/\mathbb{Q})$ is generated by σ and σ^2 is complex conjugation, we have output the $\mathrm{Aut}(K/\mathbb{Q})$-orbit of the Frobenius element.

If K is not Galois, then the Frobenius element must be either α_i or $\overline{\alpha_i}$. Since $\mathrm{Aut}(K/\mathbb{Q})$ in this case consists of only the identity and complex conjugation, Step (6) outputs the $\mathrm{Aut}(K/\mathbb{Q})$-orbit of the Frobenius element. □

5.3 Constructing a generating set for $\mathcal{O}_K$

Given the Jacobian J of a genus 2 curve over $\mathbb{F}_p$ and a primitive quartic CM field K, Algorithm 5.2.1 allows us to determine whether there is some $\pi \in \mathcal{O}_K$ that represents the Frobenius endomorphism of J. Since the complex conjugate $\overline{\pi}$ represents the Verschiebung endomorphism, if Algorithm 5.2.1 outputs `true` then we have

$$\mathbb{Z}[\pi, \overline{\pi}] \subseteq \mathrm{End}(J) \subseteq \mathcal{O}_K. \tag{5.2}$$

From this point on we assume we are given an ordinary Jacobian $J/\mathbb{F}_p$ and its Frobenius element $\pi \in \mathcal{O}_K$. Then we know that (5.2) holds, and we wish to determine whether $\mathrm{End}(J) = \mathcal{O}_K$.

Let $\mathcal{B}$ be a $\mathbb{Z}$-module basis for $\mathcal{O}_K$, and consider the collection of elements $\{\alpha \in \mathcal{B} \setminus \mathbb{Z}\}$.

Since this collection generates $\mathcal{O}_K$ over $\mathbb{Z}[\pi, \overline{\pi}]$, it suffices to determine whether or not each element of the collection is an endomorphism of J. Assuming K satisfies some mild hypotheses, Eisenträger and Lauter give one example of a basis $\mathcal{B}$ that suffices to determine the endomorphism ring [34, Lemma 6]. However, the method given in [34] lacks an efficient procedure for testing whether a given $\alpha \in \mathcal{B}$ is an endomorphism of J.

In this section, we derive from an arbitrary basis $\mathcal{B}$ a set of generators for $\mathcal{O}_K$ over $\mathbb{Z}[\pi, \overline{\pi}]$ that are convenient in the sense that there is an efficient probabilistic algorithm (Algorithm 5.4.3 or Algorithm 5.5.1) for determining whether an element of the set is an endomorphism of J. Our findings are summarized in Proposition 5.3.7.

We begin by observing that since $K = \mathbb{Q}(\pi)$, any $\alpha \in \mathcal{O}_K$ can be expressed as a polynomial $f \in \mathbb{Q}[\pi]$. Since π satisfies a polynomial of degree 4 (the characteristic polynomial of Frobenius), f can be taken to have degree 3. Using linear algebra, we may thus write

$$\alpha = \frac{a_0 + a_1\pi + a_2\pi^2 + a_3\pi^3}{n} \tag{5.3}$$

for some integers a_0, a_1, a_2, a_3, n. We assume that a_0, a_1, a_2, a_3 have no common factor with n, so that n is the smallest positive integer such that $n\alpha \in \mathbb{Z}[\pi]$.

The following lemma shows that each $\alpha \in \mathcal{B} \setminus \mathbb{Z}$ can be replaced with a collection of elements that generate the same ring, each with a power of a single prime in the denominator of the expression (5.3).

Lemma 5.3.1. *Let $A \subset B$ be commutative rings with 1, with $[B : A]$ finite. Suppose $\alpha \in B$, and let n be the smallest positive integer such that $n\alpha \in A$. Suppose n factors into primes as $\ell_1^{d_1} \cdots \ell_r^{d_r}$. Then*

$$A[\alpha] = A\left[\tfrac{n}{\ell_1^{d_1}}\alpha, \ldots, \tfrac{n}{\ell_r^{d_r}}\alpha\right].$$

Proof. Clearly the ring on the right is contained in the ring on the left, so we must show that α is contained in the ring on the right. Since the set of integers $\frac{n}{\ell_1^{d_1}}, \ldots, \frac{n}{\ell_r^{d_r}}$ has greatest common divisor 1, there exist integers c_i such that

$$c_1\frac{n}{\ell_1^{d_1}} + \cdots + c_r\frac{n}{\ell_r^{d_r}} = 1. \tag{5.4}$$

Multiplying this identity by α gives the desired result. □

The next lemma shows that only primes dividing the index $[\mathcal{O}_K : \mathbb{Z}[\pi]]$ appear in the denominators.

Lemma 5.3.2. *Let α be an element of $\mathcal{O}_K$, and suppose n is the smallest positive integer such that $n\alpha \in \mathbb{Z}[\pi]$. Then n divides the index $[\mathcal{O}_K : \mathbb{Z}[\pi]]$.*

Proof. Let $N = [\mathcal{O}_K : \mathbb{Z}[\pi]]$. By definition, N is the size of the abelian group $\mathcal{O}_K/\mathbb{Z}[\pi]$. Thus we can write any $\alpha \in \mathcal{O}_K$ as $\alpha = a + b$ with $b \in \mathbb{Z}[\pi]$ and $N \cdot a \in \mathbb{Z}[\pi]$. This shows that $\mathcal{O}_K$ is contained in $\frac{1}{N}\mathbb{Z}[\pi]$. We may thus write $\alpha = f(\pi)/N$ for a unique polynomial f with integer coefficients and degree at most 3. Furthermore, since $n\alpha$ is the smallest positive multiple of α in $\mathbb{Z}[\pi]$, we may write $\alpha = g(\pi)/n$ for a unique polynomial g with integer coefficients and degree at most 3, such that n has no factor in common with all the coefficients of g. We thus have $n \cdot f(\pi) = N \cdot g(\pi)$. If we let d be the gcd of the coefficients of f and e be the gcd of the coefficients of g, then we have $n \cdot d = N \cdot e$. Since $\gcd(n, e) = 1$, we conclude that n divides N. □

We now know that each $\alpha \in \mathcal{B} \setminus \mathbb{Z}$ can be replaced with a collection of elements $\{\frac{n}{\ell_i^{d_i}}\alpha\}$, and the only ℓ_i appearing are divisors of the index $[\mathcal{O}_K : \mathbb{Z}[\pi]]$. The following lemma and corollary show that for any ℓ which divides $[\mathcal{O}_K : \mathbb{Z}[\pi]]$ exactly (i.e., $\ell \mid [\mathcal{O}_K : \mathbb{Z}[\pi]]$ and $\ell^2 \nmid [\mathcal{O}_K : \mathbb{Z}[\pi]]$), the element $\frac{n}{\ell}\alpha$ can be replaced by an element of the form $\frac{\pi^k - 1}{\ell}$. This replacement is useful since by [34, Fact 10], determining whether an element of the form $\frac{\pi^k - 1}{\ell}$ is an endomorphism is equivalent to testing the field of definition of the ℓ-torsion.

Lemma 5.3.3. *Let $A \subset B \subset C$ be abelian groups, with $[C : A]$ finite. Let ℓ be a prime, and suppose ℓ divides $[C : A]$ exactly. Suppose there is some $\beta \in B$ such that $\beta \notin A$ and $\ell\beta \in A$. Then for any $\alpha \in C$ such that $\ell\alpha \in A$, $\alpha \in B$.*

Proof. The hypotheses on $[C : A]$ imply that the ℓ-primary part of C/A (denoted $(C/A)_\ell$) is isomorphic to $\mathbb{Z}/\ell\mathbb{Z}$, so $(B/A)_\ell$ is either trivial or $\mathbb{Z}/\ell\mathbb{Z}$. The conditions on β imply that β has order ℓ in B/A, so $(B/A)_\ell \cong \mathbb{Z}/\ell\mathbb{Z} \cong (C/A)_\ell$, with the isomorphism induced by the inclusion map $B \hookrightarrow C$. Since α is in the ℓ-primary part of C/A, α must also be in the ℓ-primary part of B/A, so $\alpha \in B$. □

Corollary 5.3.4. *Let k be a positive integer. Suppose ℓ divides $[\mathcal{O}_K : \mathbb{Z}[\pi]]$ exactly and $\beta = \frac{\pi^k - 1}{\ell} \notin \mathbb{Z}[\pi]$. Then $\frac{\pi^k - 1}{\ell}$ is an endomorphism of J if and only if every $\alpha \in \mathcal{O}_K \setminus \mathbb{Z}[\pi]$ with $\ell\alpha \in \mathbb{Z}[\pi]$ is also an endomorphism.*

Proof. The result follows directly from Lemma 5.3.3, with $A = \mathbb{Z}[\pi]$, $B = \mathrm{End}(J)$, and $C = \mathcal{O}_K$. □

Furthermore, if $p = \pi\overline{\pi}$ does not divide $[\mathcal{O}_K : \mathbb{Z}[\pi, \overline{\pi}]]$, then any element α_i with denominator $\ell_i = p$ may be ignored due to the following corollary.

Corollary 5.3.5. *Let $\pi \in \mathcal{O}_K$ correspond to the Frobenius endomorphism of an ordinary abelian surface over $\mathbb{F}_p$, and suppose $p \nmid [\mathcal{O}_K : \mathbb{Z}[\pi, \overline{\pi}]]$. Then for any $\alpha \in \mathcal{O}_K$ such that $p\alpha \in \mathbb{Z}[\pi]$, $\alpha \in \mathbb{Z}[\pi, \overline{\pi}]$.*

Proof. Since π is a Frobenius element, it satisfies a characteristic polynomial of the form

$$\pi^4 + s_1\pi^3 + s_2\pi^2 + s_1 p\pi + p^2 = 0.$$

Using $\pi\overline{\pi} = p$ and dividing this equation by π gives

$$\pi^3 + s_1\pi^2 + s_2\pi + s_1 p + p\overline{\pi} = 0. \tag{5.5}$$

From this equation we see that $p\overline{\pi} \in \mathbb{Z}[\pi]$, so either $[\mathbb{Z}[\pi, \overline{\pi}] : \mathbb{Z}[\pi]] = p$ or $\overline{\pi} \in \mathbb{Z}[\pi]$. If $\overline{\pi} \in \mathbb{Z}[\pi]$ then p divides the coefficients of all the terms on the left hand side of (5.5), which it does not, so we deduce that $\overline{\pi} \notin \mathbb{Z}[\pi]$ and $[\mathbb{Z}[\pi, \overline{\pi}] : \mathbb{Z}[\pi]] = p$. The hypothesis $p \nmid [\mathcal{O}_K : \mathbb{Z}[\pi, \overline{\pi}]]$ now implies that p divides $[\mathcal{O}_K : \mathbb{Z}[\pi]]$ exactly, so we may apply Lemma 5.3.3 with $\ell = p$, $A = \mathbb{Z}[\pi]$, $B = \mathbb{Z}[\pi, \overline{\pi}]$, $C = \mathcal{O}_K$, and $\beta = \overline{\pi}$. □

Thus any α satisfying the conditions of the corollary is automatically an endomorphism. We now show that if $p > 3$, then the condition $p \nmid [\mathcal{O}_K : \mathbb{Z}[\pi, \overline{\pi}]]$ is automatically satisfied.

Proposition 5.3.6. *Suppose $p > 3$ and that $\pi \in \mathcal{O}_K$ corresponds to the Frobenius endomorphism of an ordinary abelian surface A over $\mathbb{F}_p$. Then $p \nmid [\mathcal{O}_K : \mathbb{Z}[\pi, \overline{\pi}]]$.*

Proof. Let $\Delta(R)$ denote the discriminant of a $\mathbb{Z}$-module R. Christophe Ritzenthaler pointed out to us that this proposition follows from [59, Proposition 9.4], which shows that

$$\Delta(\mathbb{Z}[\pi, \overline{\pi}]) = \pm \operatorname{Norm}_{K/\mathbb{Q}}(\pi - \overline{\pi})\, \Delta(\mathbb{Z}[\pi + \overline{\pi}]).$$

Alternatively, it is shown in [76, Proposition 7.4] that any prime that divides the index $[\mathcal{O}_K : \mathbb{Z}[\pi, \overline{\pi}]]$ must divide either $[\mathcal{O}_{K_0} : \mathbb{Z}[\pi + \overline{\pi}]]$ or $\frac{\Delta(\mathcal{O}_{K_0}[\pi])}{\Delta(\mathcal{O}_K)}$, and, using [59, Theorem 1.3], that the second quantity is prime to p if the abelian surface is ordinary. The same proposition also shows that $\Delta(\mathbb{Z}[\pi + \overline{\pi}]) < 16p$, and since

$$\frac{\Delta(\mathbb{Z}[\pi + \overline{\pi}])}{\Delta(\mathcal{O}_{K_0})} = [\mathcal{O}_{K_0} : \mathbb{Z}[\pi + \overline{\pi}]]^2,$$

we conclude that if p divides $[\mathcal{O}_K : \mathbb{Z}[\pi, \overline{\pi}]]$ then p^2 divides $[\mathcal{O}_{K_0} : \mathbb{Z}[\pi + \overline{\pi}]]^2$, and thus

$$p^2 \leq \frac{\Delta(\mathbb{Z}[\pi + \overline{\pi}])}{\Delta(\mathcal{O}_{K_0})} < \frac{16p}{5}$$

(since a real quadratic field has discriminant at least 5), which implies $p \leq 3$. □

The following proposition summarizes the results of this section.

Proposition 5.3.7. *Suppose $\{\alpha_i\}$ generates $\mathcal{O}_K$ as a $\mathbb{Z}$-algebra. Let n_i be the smallest positive integer such that $n_i\alpha_i \in \mathbb{Z}[\pi]$, and write the prime factorization of n_i as $n_i = \prod_j \ell_{ij}^{d_{ij}}$. For each (i,j) with $\ell_{ij} \neq p$, let k_{ij} be the smallest integer such that $\pi^{k_{ij}} - 1 \in \ell_{ij}\mathcal{O}_K$. Suppose $p > 3$. Then the following set generates $\mathcal{O}_K$ over $\mathbb{Z}[\pi, \overline{\pi}]$:*

$$\left\{ \frac{n_i}{\ell_{ij}^{d_{ij}}}\alpha_i : \ell_{ij}^2 \mid [\mathcal{O}_K : \mathbb{Z}[\pi]] \text{ or } \frac{\pi^{k_{ij}} - 1}{\ell_{ij}} \in \mathbb{Z}[\pi] \right\} \bigcup$$
$$\left\{ \frac{\pi^{k_{ij}} - 1}{\ell_{ij}} : \ell_{ij}^2 \nmid [\mathcal{O}_K : \mathbb{Z}[\pi]], \ell_{ij} \neq p, \text{ and } \frac{\pi^{k_{ij}} - 1}{\ell_{ij}} \notin \mathbb{Z}[\pi] \right\}.$$

The test of whether $\frac{\pi^{k_{ij}}-1}{\ell_{ij}}$ is in $\mathbb{Z}[\pi]$ is required to apply Corollary 5.3.4. In practice we find that this condition always holds, even for small primes ℓ_{ij}, and thus the second set in the union has one element for each ℓ_{ij} dividing $[\mathcal{O}_K : \mathbb{Z}[\pi]]$ exactly.

Remark 5.3.8. Proposition 5.3.7 shows that if $p > 3$ and the index $[\mathcal{O}_K : \mathbb{Z}[\pi, \overline{\pi}]]$ is square-free, then $\mathcal{O}_K$ can be generated over $\mathbb{Z}[\pi, \overline{\pi}]$ by a collection of elements of the form $\frac{\pi^k - 1}{\ell}$. This answers a question raised by Eisenträger and Lauter [34, Remark 5].

In our application, $\pi \in \mathcal{O}_K$ is only determined up to an automorphism of K, but Proposition 5.3.7 can still be used to determine a generating set for $\mathcal{O}_K$.

Corollary 5.3.9. *Let $\mathcal{S} \subset \mathcal{O}_K$ be the set given in Proposition 5.3.7. Let σ be an element of $\mathrm{Aut}(K/\mathbb{Q})$. Then the set $\{\beta^\sigma : \beta \in \mathcal{S}\}$ generates $\mathcal{O}_K$ over $\mathbb{Z}[\pi^\sigma, \overline{\pi}^\sigma]$.*

Proof. By Proposition 5.3.7, the set $\{\pi, \overline{\pi}\} \cup \mathcal{S}$ generates $\mathcal{O}_K$ as a $\mathbb{Z}$-algebra. Since $\mathcal{O}_K$ is mapped to itself by $\mathrm{Aut}(K/\mathbb{Q})$, the set $\{\pi^\sigma, \overline{\pi}^\sigma\} \cup \{\beta^\sigma : \beta \in \mathcal{S}\}$ also generates $\mathcal{O}_K$ as a $\mathbb{Z}$-algebra. The statement follows immediately. □

5.4 Determining fields of definition

In this section, we consider the problem of determining the field of definition of the n-torsion points of the Jacobian J of a genus 2 curve over $\mathbb{F}_p$. By [34, Fact 10], the n-torsion points of J are defined over $\mathbb{F}_{p^k}$ if and only if $(\pi^k - 1)/n$ is an endomorphism of J, where π is the Frobenius endomorphism of J. Thus determining the field of definition of the ℓ-torsion points allows us to determine whether some of the elements given by Proposition 5.3.7 are endomorphisms.

Algorithm 5.4.1. The following algorithm takes as input a primitive quartic CM field K, an element $\pi \in \mathcal{O}_K$ with $\pi\overline{\pi} = p$, and an integer n with $\gcd(n, p) = 1$, and outputs the smallest integer k such that $\pi^k - 1 \in n\mathcal{O}_K$. If J is the Jacobian of a genus 2 curve over $\mathbb{F}_p$ with Frobenius π^σ for some $\sigma \in \mathrm{Aut}(K/\mathbb{Q})$ and $\mathrm{End}(J) = \mathcal{O}_K$, this integer k is such that the n-torsion points of J are defined over $\mathbb{F}_{p^k}$.

1. Compute a $\mathbb{Z}$-basis $\mathcal{B} = (1, \delta, \gamma, \kappa)$ of $\mathcal{O}_K$, using [120] or [26, Algorithm 6.1.8], and write $\pi = (a, b, c, d)$ in this basis. Set $k \leftarrow 1$.

2. Let $\bar{\mathcal{B}}$ be the reduction of the elements of $\mathcal{B}$ modulo n. Let $(a_1, b_1, c_1, d_1) = (a, b, c, d) \pmod{n}$.

3. Compute $\pi^k \equiv (a_k, b_k, c_k, d_k) \pmod{n}$ with respect to $\bar{\mathcal{B}}$.

4. If $(a_k, b_k, c_k, d_k) \equiv (1, 0, 0, 0) \pmod{n}$, output k. Otherwise set $k \leftarrow k + 1$ and go to Step (3).

Proof. The set $\bar{\mathcal{B}}$ is a $\mathbb{Z}/n\mathbb{Z}$-basis of $\mathcal{O}_K/n\mathcal{O}_K$, so if $\pi^k \equiv (1, 0, 0, 0) \pmod{n}$, then $\pi^k - 1 \in n\mathcal{O}_K$ (since the first element of $\bar{\mathcal{B}}$ is 1). Since $n\mathcal{O}_K$ is mapped to itself by $\mathrm{Aut}(K/\mathbb{Q})$, we have $(\pi^\sigma)^k - 1 \in n\mathcal{O}_K$. If $\mathrm{End}(J) = \mathcal{O}_K$, then $\frac{(\pi^\sigma)^k - 1}{n} \in \mathcal{O}_K = \mathrm{End}(J)$, so by [34, Fact 10], $J[n] \subset J(\mathbb{F}_{p^k})$. □

Remark 5.4.2. Since $J[n] = \bigoplus J[\ell^d]$ for prime powers ℓ^d dividing n, we may speed up Algorithm 5.4.1 by factoring n and computing $k(\ell^d)$ for each prime power factor ℓ^d; then $k(n) = \mathrm{lcm}(k(\ell^d))$. Furthermore, we will see in Propositions 5.6.2 and 5.6.3 below that for a fixed ℓ^d, the possible values of k are very limited. Thus we may speed up the algorithm even further by precomputing these possible values and testing each one, rather than increasing the value of k by 1 until the correct value is found.

Eisenträger and Lauter [34] computed endomorphism rings in several examples by determining the group structure of $J(\mathbb{F}_{p^k})$ to decide whether $J[n] \subset J(\mathbb{F}_{p^k})$. This is an exponential-time algorithm that is efficient only for very small k. Eisenträger and Lauter also suggested that the algorithm of Gaudry and Harley [50] could be used to determine the field of definition of the n-torsion points. One of the primary purposes of this chapter is to present an efficient probabilistic algorithm to test the field of definition of $J[n]$. Below we describe the various methods of testing the field of definition of the n-torsion of J. Since $J[n] = \bigoplus J[\ell^d]$ as ℓ^d ranges over maximal prime-power divisors of n, it suffices to consider each prime-power factor separately. We thus assume in what follows that $n = \ell^d$ is a prime power.

5.4.1 The brute force method

The simplest method of determining the field of definition of the n-torsion is to compute the abelian group structure of $J(\mathbb{F}_{p^k})$. The MAGMA syntax for this computation is straightforward, and the program returns a group structure of the form

$$J(\mathbb{F}_{p^k}) \cong \frac{\mathbb{Z}}{a_1\mathbb{Z}} \times \cdots \times \frac{\mathbb{Z}}{a_j\mathbb{Z}},$$

with $j \leq 4$ and $a_1 \mid \cdots \mid a_j$. The n-torsion of J is contained in $J(\mathbb{F}_{p^k})$ if and only if $j = 4$ and n divides a_1.

While this method is easy to implement, if k is too large it may take too long to compute the group structure (via Baby-Step Giant-Step or similar algorithms), or even worse we may not even be able to factor $\#\operatorname{Jac}(C)(\mathbb{F}_{p^k})$. In practice, computing group structure in MAGMA seems to be feasible for group sizes up to roughly 2^{200}, which means p^k should be no more than roughly 2^{100}, and thus k will have to be very small. Thus the brute force method is very limited in scope; however, it has the advantage that in the small cases it can handle it runs fairly quickly and always outputs the right answer.

5.4.2 The Gaudry-Harley-Schost method

Gaudry and Harley [50] define a Schoof-Pila-like algorithm for counting points on genus 2 curves. The curves input to this algorithm are assumed to have a degree 5 model over $\mathbb{F}_p$, so we can write elements of the Jacobian as pairs of affine points minus twice the Weierstrass point at infinity. An intermediate step in the algorithm is to construct a

polynomial $R(x) \in \mathbb{F}_p[x]$ with the following property: if P_1 and P_2 are points on C such that $D = [P_1] + [P_2] - 2[\infty]$ is an n-torsion point of J, then the x-coordinates of P_1 and P_2 are roots of R. The field of definition of the x-coordinates is at most a degree-two extension of the field of definition of D. Thus in many cases the field of definition of the n-torsion points can be determined from the factorization of $R(x)$.

Gaudry has implemented the algorithm in MAGMA [18] and NTL [116]; the algorithm involves taking two resultants of pairs of two-variable polynomials of degree roughly n^2. The algorithm uses the clever trick of computing a two-variable resultant by computing many single-variable resultants and interpolating the result. The interpolation only works if the field of definition of J has at least $4n^2 - 8n + 4$ elements, so we must base-extend J until the field of definition is large enough. Since $R(x)$ has coefficients in $\mathbb{F}_p$, this base extension has no effect on the result of the computation.

Gaudry and Harley's analysis of the algorithm gives a running time of $\tilde{O}(n^6)$ field multiplications if fast polynomial arithmetic is used, and $O(n^8)$ otherwise. Due to its large space requirements, the algorithm has only succeeded at handling inputs of size $n \leq 19$ [52].

5.4.3 A probabilistic method

As usual, we let J be the Jacobian of a genus 2 curve over $\mathbb{F}_p$, and $\ell \neq p$ be a prime. Let H be the ℓ-primary part of $J(\mathbb{F}_{p^k})$. Then H has the structure

$$H \cong \frac{\mathbb{Z}}{\ell^{\alpha_1}\mathbb{Z}} \times \frac{\mathbb{Z}}{\ell^{\alpha_2}\mathbb{Z}} \times \frac{\mathbb{Z}}{\ell^{\alpha_3}\mathbb{Z}} \times \frac{\mathbb{Z}}{\ell^{\alpha_4}\mathbb{Z}},$$

with $\alpha_1 \leq \alpha_2 \leq \alpha_3 \leq \alpha_4$. Our test rests on the following observations:

- If the ℓ^d-torsion points of J are defined over $\mathbb{F}_{p^k}$, then $\alpha_1 \geq d$, and the number of ℓ^d-torsion points in H is ℓ^{4d}.
- If the ℓ^d-torsion points of J are not defined over $\mathbb{F}_{p^k}$, then $\alpha_1 < d$, and the number of ℓ^d-torsion points in H is at most ℓ^{4d-1}.

We thus make the following calculation: write $\#J(\mathbb{F}_{p^k}) = \ell^s m$ with $\ell \nmid m$. Choose a random point $P \in J$. Then $[m]P \in H$, and we test whether $[\ell^d m]P = O$ in J. If the ℓ^d-torsion points of J are defined over $\mathbb{F}_{p^k}$, then $[\ell^d m]P = O$ with probability $\rho = \ell^{4d-s}$, while if the ℓ^d-torsion points of J are not defined over $\mathbb{F}_{p^k}$ then $[\ell^d m]P = O$ with probability at most ρ/ℓ. If we perform the test enough times, we can determine which probability distribution

we are observing and thus conclude, with a high degree of certainty, whether the ℓ^d-torsion points are defined over $\mathbb{F}_{p^k}$.

This method is very effective in practice, and can be implemented for large k: while computing the group structure of $J(\mathbb{F}_{p^k})$ for large k may be infeasible, it is much easier to compute *points* on $J(\mathbb{F}_{p^k})$ and to do arithmetic on those points. We now give a formal description of the algorithm and determine its probability of success.

Algorithm 5.4.3. The following algorithm takes as input the Jacobian J of a genus 2 curve defined over a finite field $\mathbb{F}_q$, a prime power ℓ^d with $\gcd(\ell, q) = 1$, and a real number $\epsilon \in (0, 1)$. If $J[\ell^d] \subset J(\mathbb{F}_q)$, then the algorithm outputs `true` with probability at least $1 - \epsilon$. If $J[\ell^d] \not\subset J(\mathbb{F}_q)$, then the algorithm outputs `false` with probability at least $1 - \epsilon$.

1. Compute $\#J(\mathbb{F}_q) = \ell^s m$, where $\ell \nmid m$. If $s < 4d$ output `false`.
2. Set $\rho \leftarrow \ell^{4d-s}$, $N \leftarrow \lceil \frac{\sqrt{-2\log\epsilon}}{\rho}(\frac{2\ell}{\ell-1})\rceil$, $B \leftarrow \rho N\left(\frac{\ell+1}{2\ell}\right)$.
3. Repeat N times:
   (a) Choose a random point $P_i \in J(\mathbb{F}_q)$.
   (b) Compute $Q_i \leftarrow [\ell^d m]P_i$
4. If at least B of the Q_i are the identity element O of J, output `true`; otherwise output `false`.

Proof. As observed above, if $J[\ell^d] \subset J(\mathbb{F}_q)$, then $Q_i = O$ with probability ρ, while if $J[\ell^d] \not\subset J(\mathbb{F}_q)$, then $Q_i = O$ with probability at most ρ/ℓ. Thus all we have to do is compute enough Q_i to distinguish the two probability distributions. To figure out how many "enough" is, we use the Chernoff bound [106, Chapter 8, Proposition 5.3]. The version of the bound we use is as follows: If N weighted coins are flipped and μ is the expected number of heads, then for any $\delta \in (0, 1]$ we have

$$\begin{aligned} \Pr[\#\text{heads} < (1-\delta)\mu] &< e^{-\mu^2\delta^2/2} \\ \Pr[\#\text{heads} > (1+\delta)\mu] &< e^{-\mu^2\delta^2/2}. \end{aligned} \tag{5.6}$$

In our case we are given two different probability distributions for the coin flip and wish to tell them apart. If the ℓ^d-torsion points of J are defined over $\mathbb{F}_q$, then the probability that $Q_i = O$ is $\rho = \ell^{4d}/\ell^s$. Thus the expected number of Q_i equal to O is $\mu_1 = \rho N$. If

the ℓ^d-torsion points are not defined over $\mathbb{F}_q$, then the expected number of Q_i equal to O is at most $\mu_2 = \rho N/\ell$. Thus if we set $B = \rho N(\frac{\ell+1}{2\ell})$ to be the midpoint of $[\mu_2, \mu_1]$, we will deduce that $J[\ell^d] \subset J(\mathbb{F}_q)$ if the number of Q_i equal to O is at least B, and $J[\ell^d] \not\subset J(\mathbb{F}_q)$ otherwise.

We thus wish to find an N such that this deduction is correct with probability at least $1-\epsilon$, i.e., an N such that

$$\begin{aligned}\Pr[\#\{Q_i : Q_i = O\} < B] &< \epsilon \quad \text{if } J[\ell^d] \subset J(\mathbb{F}_q),\\ \Pr[\#\{Q_i : Q_i = O\} > B] &< \epsilon \quad \text{if } J[\ell^d] \not\subset J(\mathbb{F}_q).\end{aligned}$$

Substituting our choice of B into the Chernoff bound (5.6) gives

$$\begin{aligned}\Pr[\#\{Q_i : Q_i = O\} < B] &< e^{-2\mu_1^2(\frac{\ell-1}{4\ell})^2} \quad \text{if } J[\ell^d] \subset J(\mathbb{F}_q),\\ \Pr[\#\{Q_i : Q_i = O\} > B] &< e^{-2\mu_2^2(\frac{\ell-1}{4})^2} \quad \text{if } J[\ell^d] \not\subset J(\mathbb{F}_q).\end{aligned}$$

From these equations, we see that we wish to have $2\mu_1^2(\frac{\ell-1}{4\ell})^2 > -\log\epsilon$ and $2\mu_2^2(\frac{\ell-1}{4})^2 > -\log\epsilon$. The two left sides are equal since $\mu_2 = \mu_1/\ell$. We thus substitute $\mu_1 = \rho N$ into the relation $2\mu_1^2(\frac{\ell-1}{4\ell})^2 > -\log\epsilon$, and find that

$$N > \frac{\sqrt{-2\log\epsilon}}{\rho}\left(\frac{2\ell}{\ell-1}\right).$$

Thus this value of N suffices to give the desired success probabilities. □

Remark 5.4.4. If $s = 4d$ the algorithm can be simplified considerably. In this case, if $J[\ell^d] \subset J(\mathbb{F}_q)$ then the ℓ-primary part H of $J(\mathbb{F}_q)$ is isomorphic to $(\mathbb{Z}/\ell^d\mathbb{Z})^4$, and if not then it contains a point of order greater than ℓ^d. Thus if $J[\ell^d] \subset J(F)$ then Q_i will always be the identity, and the algorithm will always return `true`. On the other hand, if $J[\ell^d] \not\subset J(\mathbb{F}_q)$, we may abort the algorithm and return `false` as soon as we find a point $Q_i \neq O$, for in this case we have found a point in H of too large order, and thus the ℓ^d-torsion points are not defined over $\mathbb{F}_q$. If $J[\ell^d] \not\subset J(\mathbb{F}_q)$, then the probability that a random point in H has order $\leq \ell^d$ is at most $1/\ell$, so we must conduct at least $N = \lceil \frac{-\log\epsilon}{\log\ell} \rceil$ trials to ensure a success probability of at least $1-\epsilon$. Thus in this case the method may require many fewer trials.

Remark 5.4.5. Note that while $\#J(\mathbb{F}_q)$ may be very large, in our application where J is defined over a small prime field it is easy to compute $\#J(\mathbb{F}_q)$ from the zeta function of the curve of which J is the Jacobian. Furthermore, while it is probably impossible to factor $\#J(\mathbb{F}_q)$ completely in a reasonable amount of time, it is easy to determine the highest power of ℓ that divides $\#J(\mathbb{F}_q)$.

Proposition 5.4.6. *Let J be the Jacobian of a genus 2 curve over $\mathbb{F}_p$. Assume that the zeta function of $J/\mathbb{F}_p$ is known, so that the cost to compute $\#J(\mathbb{F}_{p^k}) = \ell^s m$ is negligible. Then the expected number of operations in $\mathbb{F}_p$ necessary to execute Algorithm 5.4.3 on inputs $J/\mathbb{F}_{p^k}$, ℓ^d, and ϵ (ignoring $\log\log p$ factors) is*

$$O(k^2 \log k (\log^2 p) \ell^{s-4d} (-\log \epsilon)^{1/2}).$$

Proof. We must compare the cost of the two actions of Step (3), repeated N times. Choosing a random point on $J(\mathbb{F}_q)$ is equivalent to computing a constant number of square roots in $\mathbb{F}_q$, and taking a square root requires $O(\log q)$ field operations in $\mathbb{F}_q$ (see [127, Algorithm 14.15 and Corollary 14.16]). The order of $J(\mathbb{F}_q)$ is roughly q^2, so multiplying a point on $J(\mathbb{F}_q)$ by an integer using a binary expansion takes $O(\log q)$ point additions on $J(\mathbb{F}_q)$. Each point addition takes a constant number of field operations in $\mathbb{F}_q$, so we see that the each trial requires $O(\log q) = O(k \log p)$ field operations in $\mathbb{F}_q$. If fast multiplication techniques are used, then the number of field operations in $\mathbb{F}_p$ needed to perform one field operation in $\mathbb{F}_q$ (ignoring $\log\log p$ factors) is

$$O(\log q \log\log q) = O(k \log k \log p),$$

so each trial takes $O(k^2 \log k \log^2 p)$ field operations in $\mathbb{F}_p$. The number of trials is

$$O(\ell^{s-4d} \sqrt{-\log \epsilon}),$$

which gives a total of

$$O(k^2 \log k (\log^2 p) \ell^{s-4d} (-\log \epsilon)^{1/2})$$

field operations in $\mathbb{F}_p$. □

5.5 Computing the action of Frobenius

As in the previous section, we consider a genus 2 curve C over $\mathbb{F}_p$ with Jacobian J, and assume that the endomorphism ring of J is an order in the ring of integers $\mathcal{O}_K$ of a primitive quartic CM field K. We let π represent the Frobenius endomorphism, and we look at elements $\alpha \in \mathcal{O}_K$ such that $\ell^d \alpha \in \mathbb{Z}[\pi]$ for some prime power ℓ^d. We wish to devise a test that, given such an α, determines whether α is an endomorphism of J.

Since π satisfies a quartic polynomial with integer coefficients, we can write α as

$$\alpha = \frac{a_0 + a_1\pi + a_2\pi^2 + a_3\pi^3}{\ell^d} \tag{5.7}$$

for some integers a_0, a_1, a_2, a_3. Expressing α in this form is useful because of the following fact proved by Eisenträger and Lauter [34, Corollary 9]: α is an endomorphism if and only if $T = a_0 + a_1\pi + a_2\pi^2 + a_3\pi^3$ acts as zero on the ℓ^d-torsion. Thus we need a method for determining whether T acts as zero on the ℓ^d-torsion. Since T is a linear operator, it suffices to check whether $T(Q_i)$ is zero for each Q_i in some set whose points span the full ℓ^d-torsion. Below we describe three different ways to compute such a spanning set.

5.5.1 The brute force method

The most straightforward way to compute a spanning set for the ℓ^d-torsion is to use group structure algorithms to compute a basis of $J[\ell^d]$. This method was used in [34] to compute the class polynomials in one example. The methods of Section 5.4 determine a k for which $J[\ell^d] \subset J(\mathbb{F}_{p^k})$. The computation of the group structure of $J(\mathbb{F}_{p^k})$ gives generators for the group; multiplying these generators by appropriate integers gives generators for the ℓ^d-torsion. It is then straightforward to compute the action of T on each generator g_i for $1 \leq i \leq 4$. If $T(g_i) = O$ for all i, then α is an endomorphism; otherwise α is not an endomorphism.

This method of computing a spanning set has the same drawback as the brute-force method of computing fields of definition: since the best algorithm for computing group structure runs in time exponential in $k \log p$, the method becomes prohibitively slow as k increases. Thus the method is only effective when ℓ^d is very small.

5.5.2 A probabilistic method

The method of Section 5.5.1 for computing generators of $J[\ell^d]$ becomes prohibitively slow as the field of definition of the ℓ^d-torsion points becomes large. However, we can get around this obstacle by randomly choosing many points Q_i of exact order ℓ^d, so that it is highly probable that the set $\{Q_i\}$ spans $J[\ell^d]$.

Recall that we wish to test whether the operator $T = a_0 + a_1\pi + a_2\pi^2 + a_3\pi^3$ acts as zero on the ℓ^d-torsion. To perform the test, we determine the field $\mathbb{F}_{p^k}$ over which we expect the ℓ^d-torsion to be defined. (See Section 5.4.) We pick a random point $P \in J(\mathbb{F}_{p^k})$ and multiply P by an appropriate integer to get a point Q whose order is a power of ℓ. If Q has order ℓ^d, we act on Q by the operator T and test whether we get the identity of J; otherwise we try again with a new P. (See Section 5.5.3 for another method of randomly choosing

ℓ^d-torsion points.) We repeat the test until it is overwhelmingly likely that the points Q span the ℓ^d-torsion. If the set of Q spans the ℓ^d-torsion, then α is an endomorphism if and only if T acts as zero on all the Q.

Algorithm 5.5.1. The following algorithm takes as input the Jacobian J of a genus 2 curve over $\mathbb{F}_p$ with CM by K; a prime power $q = p^k$; a prime power ℓ^d with $\ell \neq p$; an element $\alpha \in \mathcal{O}_K$ such that $\ell^d\alpha \in \mathbb{Z}[\pi]$, where $\pi \in \mathcal{O}_K$ corresponds to the p-power Frobenius endomorphism of J; and a real number $\epsilon > 0$. The algorithm outputs `true` or `false`.

Suppose $J[\ell^d] \subset J(\mathbb{F}_q)$. If α is an endomorphism of J, then the algorithm outputs `true`. If α is not an endomorphism of J, then the algorithm outputs `false` with probability at least $1 - \epsilon$.

1. Compute a_0, a_1, a_2, a_3 such that α satisfies equation (5.7).
2. Set N to be
$$N \leftarrow \begin{cases} \lceil \frac{1}{d - \log_\ell 2} (-\log_\ell \epsilon + 3d) \rceil & \text{if } \ell^d > 2 \\ \max\{\lceil -2\log_2 \epsilon \rceil + 6, 16\} & \text{if } \ell^d = 2. \end{cases}$$
3. Compute $\#J(\mathbb{F}_q) = \ell^s m$, where $\ell \nmid m$.
4. Set $i \leftarrow 1$.
5. Choose a random point $P_i \in J(\mathbb{F}_q)$. Set $Q_i \leftarrow [m]P_i$. Repeat until $[\ell^d]Q_i = O$ and $[\ell^{d-1}]Q_i \neq O$.
6. Compute
$$[a_0]Q_i + [a_1]\,\mathrm{Frob}_p(Q_i) + [a_2]\,\mathrm{Frob}_{p^2}(Q_i) + [a_3]\,\mathrm{Frob}_{p^3}(Q_i) \tag{5.8}$$
in $J(\mathbb{F}_q)$. If the result is nonzero output `false`.
7. If $i < N$, set $i \leftarrow i + 1$ and go to Step (5).
8. Output `true`.

Proof. By [34, Corollary 9], α is an endomorphism of J if and only if the expression (5.8) is O for all ℓ^d-torsion points Q. Furthermore, it suffices to check this expression only on a basis of the ℓ^d-torsion. Step (5) repeats until we find a point Q_i of exact order ℓ^d; the assumption $J[\ell^d] \subset J(\mathbb{F}_q)$ guarantees that we can find such a point. The algorithm computes a total of N such points Q_i. Thus if the set of Q_i span $J[\ell^d]$, then the algorithm will output `true`

or `false` correctly, according to whether $\alpha \in \mathrm{End}(J)$. We must therefore compute a lower bound for the probability that the set of Q_i computed span $J[\ell^d]$.

To compute this bound, we will compute an upper bound for the probability that N points of exact order ℓ^d do not span $J[\ell^d]$. We will make repeated use of the following inequality, which can be proved easily: if ℓ, d, n, and m are positive integers with $\ell > 1$ and $n > m$, then

$$\frac{\ell^{md} - \ell^{m(d-1)}}{\ell^{nd} - \ell^{n(d-1)}} < \frac{1}{\ell^{(n-m)d}}.$$

Next we observe that in any group of the form $(\mathbb{Z}/\ell^d\mathbb{Z})^r$, there are $\ell^{rd} - \ell^{r(d-1)}$ elements of exact order ℓ^d. The probability that a set of N elements does not span a 4-dimensional space is the sum of the probabilities that all the elements span a j-dimensional subspace, for $j = 1, 2, 3$. We consider each case:

- $j = 1$: All of the Q_i are in the space spanned by Q_1, and Q_1 can be any element. The probability of this happening is

$$\left(\frac{\ell^d - \ell^{d-1}}{\ell^{4d} - \ell^{4(d-1)}}\right)^{N-1} < \left(\frac{1}{\ell^{3d}}\right)^{N-1}.$$

- $j = 2$: Q_1 can be any element, one of the Q_i must be independent of Q_1, and the remaining $N - 2$ elements must be in the same 2-dimensional subspace. There are $N - 1$ ways to choose the second element, so the total probability is

$$(N-1)\left(1 - \frac{\ell^d - \ell^{d-1}}{\ell^{4d} - \ell^{4(d-1)}}\right)\left(\frac{\ell^{2d} - \ell^{2(d-1)}}{\ell^{4d} - \ell^{4(d-1)}}\right)^{N-2} < N\left(\frac{1}{\ell^{2d}}\right)^{N-2}.$$

- $j = 3$: Q_1 can be any element, and there must be two more linearly independent elements; there are $\binom{N-1}{2}$ ways of choosing these elements. The remaining $N - 3$ elements must all be in the same 3-dimensional subspace, so the total probability is

$$\frac{(N-1)(N-2)}{2}\left(1 - \frac{\ell^d - \ell^{d-1}}{\ell^{4d} - \ell^{4(d-1)}}\right)\left(1 - \frac{\ell^{2d} - \ell^{2(d-1)}}{\ell^{4d} - \ell^{4(d-1)}}\right)\left(\frac{\ell^{3d} - \ell^{3(d-1)}}{\ell^{4d} - \ell^{4(d-1)}}\right)^{N-3} < \frac{N^2}{2}\left(\frac{1}{\ell^d}\right)^{N-3}.$$

Summing these three cases, we see that the total probability that the Q_i do not span $J[\ell^d]$ is bounded above by

$$N^2\left(\frac{1}{\ell^d}\right)^{N-3}. \tag{5.9}$$

Since $2^N \geq N^2$ for $N \geq 4$, we have

$$N^2 \left(\frac{1}{\ell^d}\right)^{N-3} \leq \ell^{-dN+3d+N\log_\ell 2}.$$

(Note that $N \geq 4$ must always hold if we want to have a spanning set of $J[\ell]$.) Setting this last expression less than ϵ and taking logs, we find

$$N \geq \frac{1}{d - \log_\ell 2}\left(-\log_\ell \epsilon + 3d\right). \tag{5.10}$$

Thus if the number of trials N is greater than or equal to the right hand side of (5.10), then the probability of success is at least $1 - \epsilon$.

The right hand side of expression (5.10) is undefined if $\ell = 2$, $d = 1$, so we must make a different estimate. Since $2^{N/2} \geq N^2$ for $N \geq 16$, the estimate (5.9) bounds the probability of Q_i not spanning $J[\ell^d]$ by

$$\frac{N^2}{2^{N-3}} \leq \frac{1}{2^{N/2-3}}.$$

Setting the right hand side less than ϵ and taking logs gives

$$N \geq -2\log_2 \epsilon + 6. \tag{5.11}$$

Thus if the number of trials N is greater than or equal to the maximum of 16 and the right hand side of (5.11), then the probability of success is at least $1 - \epsilon$. □

Corollary 5.5.2. *Let J, q, ℓ^d, α, and ϵ be as in Algorithm 5.5.1. Suppose $\pi \in \mathcal{O}_K$ is such that π^σ corresponds to the Frobenius endomorphism of J for some $\sigma \in \mathrm{Aut}(K/\mathbb{Q})$. Suppose $J[\ell^d] \subset J(\mathbb{F}_q)$, and suppose Algorithm 5.5.1 is run with inputs J, q, ℓ^d, α, ϵ. If α^σ is an endomorphism of J, then the algorithm outputs* `true`*. If α^σ is not an endomorphism of J, then the algorithm outputs* `false` *with probability at least $1 - \epsilon$.*

Proof. If we write α in the form (5.7), then we have

$$\alpha^\sigma = \frac{a_0 + a_1\pi^\sigma + a_2(\pi^\sigma)^2 + a_3(\pi^\sigma)^3}{\ell^d}.$$

Step (6) of the algorithm determines whether the numerator of this expression acts as zero on ℓ^d-torsion points. By [34, Corollary 9], this action is identically zero if and only if α^σ is an endomorphism of J. The statement now follows from the correctness of Algorithm 5.5.1. □

Remark 5.5.3. Since Q_i is an ℓ^d-torsion point in Step (6), we may speed up the computation of the expression (5.8) by replacing each a_j with a small representative of a_j modulo ℓ^d. We may also rewrite the expression (5.8) as

$$[a_0]Q_i + \mathrm{Frob}_p([a_1]Q_i + \mathrm{Frob}_p([a_2]Q_i + \mathrm{Frob}_p([a_3]Q_i)))$$

to reduce the number of Frob_p operations from 6 to 3.

Remark 5.5.4. Algorithm 5.5.1 assumes that the ℓ^d-torsion points of J are defined over $\mathbb{F}_q$, so with enough trials we are almost certain to get a spanning set of points Q_i. However, if the ℓ^d-torsion points are not defined over $\mathbb{F}_q$, then the points Q_i will span a proper subspace of $J[\ell^d]$. If α is an endomorphism then T will act as zero on all of the Q_i and Algorithm 5.5.1 will output `true`. However, if α is not an endomorphism then T may still act as zero on all of the Q_i (in which case it must have nonzero action on the ℓ^d-torsion points that are not defined over $\mathbb{F}_q$), and the algorithm will incorrectly output `true`. Thus to test whether α is an endomorphism, we must combine Algorithm 5.5.1 with a method of checking the field of definition of the ℓ^d-torsion points, such as the probabilistic method of Algorithm 5.4.3.

Proposition 5.5.5. *Let J be the Jacobian of a genus 2 curve over $\mathbb{F}_p$. Assume that the zeta function of $J/\mathbb{F}_p$ is known, so that the cost to compute $\#J(\mathbb{F}_{p^k}) = \ell^s m$ is negligible. Then the expected number of operations in $\mathbb{F}_p$ necessary to execute Algorithm 5.5.1 on inputs J, $q = p^k$, ℓ^d, and ϵ (ignoring $\log\log p$ factors) is*

$$O(k^2 \log k (\log^2 p) \ell^{s-4d}(-\log \epsilon)).$$

Proof. Let $q = p^k$. In the proof of Proposition 5.4.6, we computed that the cost of computing a random point on $J(\mathbb{F}_q)$ is $O(\log q)$ operations in $\mathbb{F}_q$, and the cost of a point multiplication on $J(\mathbb{F}_q)$ is $O(\log q)$ operations in $\mathbb{F}_q$. The chance that a random point in the ℓ-primary part of $J(\mathbb{F}_q)$ has exact order ℓ is $\frac{\ell^{4d} - \ell^{4d-4}}{\ell^s}$, so the expected number of random points necessary to find one point of exact order ℓ^d is $O(\ell^{s-4d})$. The cost of computing the p-power Frobenius action is proportional to the cost of raising an element of $\mathbb{F}_q$ to the pth power, which is $O(\log p)$ $\mathbb{F}_q$-operations.

We conclude that the expected cost of a single trial with a random point is

$$O(\log q + \log q + \log p)\ell^{s-4d} M(q)$$

operations in $\mathbb{F}_p$, where $M(q)$ is the number of field operations in $\mathbb{F}_p$ needed to perform one field operation in $\mathbb{F}_q$. If fast multiplication techniques are used, then

$$M(q) = O(\log q \log\log q) = O(k \log k \log p)$$

(ignoring $\log\log p$ factors), so each trial takes

$$O(k^2 \log k (\log^2 p) \ell^{s-4d})$$

field operations in $\mathbb{F}_p$. The number of points of exact order ℓ^d computed is $O(-\log \epsilon)$. Putting this all together gives a total of

$$O(k^2 \log k (\log^2 p) \ell^{s-4d} (-\log \epsilon))$$

field operations in $\mathbb{F}_p$. □

5.5.3 The Couveignes method

Recall that to test whether an element $\alpha \in \mathcal{O}_K$ of the form (5.7) is an endomorphism of J, we determine whether the operator $T = a_0 + a_1\pi + a_2\pi^2 + a_3\pi^3$ acts as zero on all elements of a set $\{Q_i\}$ that spans $J[\ell^d]$. Algorithm 5.5.1 computes a spanning set by choosing random points P_i in $J(\mathbb{F}_{p^k})$, multiplying by an appropriate m to get points Q_i in the ℓ-primary part of $J(\mathbb{F}_{p^k})$ (denoted $J(\mathbb{F}_{p^k})_\ell$), and keeping only those Q_i whose order is exactly ℓ^d. If $J(\mathbb{F}_{p^k})_\ell$ is much larger than $J[\ell]$, the orders of most of the Q_i will be too large, and it will take many trials to find the required number of points of order exactly ℓ^d. To reduce the number of trials required, we would like to find a function from $J(\mathbb{F}_{p^k})_\ell$ to $J[\ell^d]$ that sends most of the Q_i to points of exact order ℓ^d.

One way to compute such a function is as follows: compute the order ℓ^{t_i} of each Q_i; if $t_i \geq d$ send $Q_i \mapsto [\ell^{t_i-d}]Q_i$, otherwise send $Q_i \mapsto O$. In most cases the image has order ℓ^d. However, since the multiplier ℓ^{t_i-d} will be different for each Q_i, this function does not define a group homomorphism, and thus the image of a set of points uniformly distributed in $J(\mathbb{F}_{p^k})_\ell$ will not be uniformly distributed in $J[\ell^d]$.

Couveignes [28] has described a map that has the properties we want and is a group homomorphism. The idea is the following: if $\pi^k - 1 \in \ell^d \operatorname{End}(J)$, then there is an endomorphism ϕ such that $\ell^d\phi = \pi^k - 1$. Since $\pi^k - 1$ acts as zero on $J(\mathbb{F}_{p^k})$, the image of ϕ on $J(\mathbb{F}_{p^k})$ must consist of ℓ^d-torsion points. Furthermore, the kernel of ϕ contains $\ell^d J(\mathbb{F}_{p^k})$,

since $\phi(\ell^d P) = (\pi^k - 1)(P) = 0$ if P is defined over $\mathbb{F}_{p^k}$. Thus we have a map

$$\phi : J(\mathbb{F}_{p^k})/\ell^d J(\mathbb{F}_{p^k}) \to J[\ell^d].$$

Couveignes then uses the non-degeneracy of the Frey-Rück pairing (see [110]) to show that ϕ is a bijection. Thus for any Q_i not in $\ell J(\mathbb{F}_{p^k})$, $\phi(Q_i)$ has order exactly ℓ^d. Since ϕ is a surjective group homomorphism, the image of a set of points uniformly distributed in $J(\mathbb{F}_{p^k})$ will be uniformly distributed in $J[\ell^d]$. The chance that $Q_i \in \ell J(\mathbb{F}_{p^k})$ is $1/\ell^4$, so applying ϕ to the Q_i will very quickly give a spanning set of $J[\ell^d]$.

However, there is one important caveat: we may not be able to compute ϕ. The only endomorphisms we can compute are those involving the action of Frobenius and scalar multiplication; namely, endomorphisms in $\mathbb{Z}[\pi]$. Thus we need to take k to be the smallest integer such that $\pi^k - 1 \in \ell^d \mathbb{Z}[\pi]$. We can then use the characteristic polynomial of Frobenius to write $\phi = \frac{\pi^k - 1}{\ell^d} = M(\pi)$, where M is a polynomial of degree 3. Furthermore, since we are applying ϕ only to points $Q_i \in J(\mathbb{F}_{p^k})_\ell$, we may reduce the coefficients of M modulo ℓ^s and get the same action on the Q_i.

We have implemented the map ϕ in MAGMA and tested it on the examples that appear in Section 5.9. In our examples, the smallest k for which $\pi^k - 1 \in \ell^d \mathbb{Z}[\pi]$ is usually equal to ℓk_0, where k_0 is the integer output by Algorithm 5.4.1. We found that the cost of choosing random points over a field of degree ℓ times as large far outweighs the benefit of having to reject fewer of the points Q_i, so this technique does not help to speed up Algorithm 5.5.1.

5.6 Bounding the field of definition of the ℓ^d-torsion points

The running times of Algorithms 5.4.3 and 5.5.1 depend primarily on the size of the field $\mathbb{F}_{p^k}$ over which the ℓ^d-torsion points of J are defined. In this section, we bound the size of k in terms of ℓ^d and p. We also show that to determine the field of definition of the ℓ^d-torsion points of J for $d > 1$, it suffices to determine the field of definition of the ℓ-torsion points of J. This result allows us to work over much smaller fields in Algorithm 5.4.3, thus saving us a great deal of computation.

By Lemma 5.3.2, the prime powers ℓ^d input to Algorithms 5.4.3 and 5.5.1 divide the index $[\mathcal{O}_K : \mathbb{Z}[\pi, \overline{\pi}]]$. Thus a bound on this index gives a bound on the ℓ^d that appear.

Proposition 5.6.1. *Let K be a primitive quartic CM field with discriminant $\Delta = \Delta(\mathcal{O}_K)$. Suppose $\pi \in \mathcal{O}_K$ corresponds to the Frobenius endomorphism of the Jacobian of a genus 2 curve defined over $\mathbb{F}_p$. Then*

$$[\mathcal{O}_K : \mathbb{Z}[\pi, \overline{\pi}]] \leq \frac{16p^2}{\sqrt{\Delta}}.$$

Proof. We showed in the proof of Corollary 5.3.5 that $[\mathbb{Z}[\pi, \overline{\pi}] : \mathbb{Z}[\pi]] = p$. Combining this result with the formula

$$[\mathcal{O}_K : \mathbb{Z}[\pi]] = [\mathcal{O}_K : \mathbb{Z}[\pi, \overline{\pi}]][\mathbb{Z}[\pi, \overline{\pi}] : \mathbb{Z}[\pi]],$$

we see that it suffices to show that $[\mathcal{O}_K : \mathbb{Z}[\pi]] \leq 16p^3/\sqrt{\Delta}$. (Note that $\Delta > 0$ by [59, Proposition 9.4].) Next, recall that

$$[\mathcal{O}_K : \mathbb{Z}[\pi]] = \sqrt{\frac{\Delta(\mathbb{Z}[\pi])}{\Delta(\mathcal{O}_K)}}.$$

It thus suffices to show that $\sqrt{\Delta(\mathbb{Z}[\pi])} \leq 16p^3$. By definition,

$$\sqrt{\Delta(\mathbb{Z}[\pi])} = \prod_{i<j} |\alpha_i - \alpha_j|, \tag{5.12}$$

where α_i are the possible embeddings of π into $\mathbb{C}$. Since π represents an action of Frobenius, it is a p-Weil number, and thus all of the α_i lie on the circle $|z| = \sqrt{p}$. The product (5.12) takes its maximum value subject to this constraint when the α_i are equally spaced around the circle, which happens when the α_i are $\sqrt{p}$ times primitive eighth roots of unity. The maximum product is thus $p^3\sqrt{\Delta(\mathbb{Q}(\zeta_8))} = 16p^3$. □

Proposition 5.6.1 also follows directly from [76, Proposition 7.4], where it is proved in a different manner that $\sqrt{\Delta(\mathbb{Z}[\pi, \overline{\pi}])} \leq 16p^2$.

The next two propositions give tight bounds on the degree k of the extension field of $\mathbb{F}_p$ over which the ℓ^d-torsion points of J are defined. The first considers the case $d = 1$, and the second shows that as d is increased to $d + 1$, k grows by a factor of ℓ.

Proposition 5.6.2. *Let J be the Jacobian of a genus 2 curve over $\mathbb{F}_p$, and suppose that $\mathrm{End}(J)$ is isomorphic to the ring of integers $\mathcal{O}_K$ of a primitive quartic CM field K. Let $\ell \neq p$ be a prime number, and suppose $\mathbb{F}_{p^k}$ is the smallest field over which the points of $J[\ell]$ are defined. If ℓ is unramified in K, then k divides one of the following:*

- *$\ell - 1$, if ℓ splits completely in K;*

- $\ell^2 - 1$, *if* ℓ *splits into two or three prime ideals in* K*;*
- $\ell^3 - \ell^2 + \ell - 1$, *if* ℓ *is inert in* K*.*

If ℓ *ramifies in* K*, then* k *divides one of the following:*

- $\ell^3 - \ell^2$*, if there is a prime over* ℓ *of ramification degree* 3*, or if* ℓ *is totally ramified in* K *and* $\ell \leq 3$*;*
- $\ell^2 - \ell$*, in all other cases where* ℓ *factors into four prime ideals in* K *(counting multiplicities);*
- $\ell^3 - \ell$*, if* ℓ *factors into two or three prime ideals in* K *(counting multiplicities).*

Proof. Let $\pi \in \mathcal{O}_K$ correspond to the Frobenius endomorphism. By [34, Fact 10], the ℓ-torsion points of J are defined over $\mathbb{F}_{p^k}$ if and only if $\pi^k - 1 \in \ell\mathcal{O}_K$. We observe that by the Chinese remainder theorem, this condition is satisfied if and only if $\pi^k \equiv 1 \pmod{\mathfrak{p}_i^{e_i}}$ for all primes $\mathfrak{p}_i \mid \ell\mathcal{O}_K$, where e_i is the ramification degree of $\mathfrak{p}_i$. Next, we note that the condition $\ell \neq p$ implies that $\pi \notin \mathfrak{p}_i$ for all i. To see why this is true, suppose the contrary: $\pi \in \mathfrak{p}_i$. Since $\pi\overline{\pi} = p$, we have $p \in \mathfrak{p}_i$, contradicting the fact that $\mathfrak{p}_i$ is a prime over $\ell \neq p$.

From these observations we deduce that k is the least common multiple of the multiplicative orders of π mod each $\mathfrak{p}_i^{e_i}$, and thus k must divide the least common multiple of

$$\#(\mathcal{O}_K/\mathfrak{p}_i^{e_i}\mathcal{O}_K)^\times = \ell^{f_i(e_i-1)}(\ell^{f_i} - 1),$$

where f_i is the inertia degree of $\mathfrak{p}_i$. We now consider the various possibilities for the splitting of ℓ in $\mathcal{O}_K$.

First, suppose ℓ is unramified, so $e_i = 1$ for all i.

- If ℓ splits completely, then the inertia degrees of all the $\mathfrak{p}_i$ are 1, so $k \mid \ell - 1$.
- If ℓ splits into two or three ideals, then at least one $\mathfrak{p}_i$ has $f_i = 2$ and all have $f_i \leq 2$, so $k \mid \ell^2 - 1$.
- If ℓ is inert, then there is a single $\mathfrak{p}_i$ with $f_i = 4$, and k divides $\ell^4 - 1$. We will return to this case below to get a better bound.

Now suppose ℓ ramifies; there are six possibilities for the splitting of ℓ in $\mathcal{O}_K$.

- If $\ell\mathcal{O}_K = \mathfrak{p}^3\mathfrak{q}$, then $\mathfrak{p}$ and $\mathfrak{q}$ have inertia degree 1, so k divides $\ell^2(\ell - 1)$.

- If $\ell\mathcal{O}_K = \mathfrak{p}^4$, then $\mathcal{O}_K/\mathfrak{p} \cong \mathbb{F}_\ell$, and thus we have $\pi^{\ell-1} = 1+\tau$ for some $\tau \in \mathfrak{p}$. There are now two subcases:
  - If $\ell \geq 5$, then $(1+\tau)^\ell \in 1+\mathfrak{p}^4$, so $\pi^{\ell(\ell-1)} \equiv 1 \pmod{\mathfrak{p}^4}$. Thus k divides $\ell(\ell-1)$.
  - If $\ell = 2$ or 3, then $(1+\tau)^\ell \equiv 1+\tau^\ell \pmod{\mathfrak{p}^4}$, so we must raise the expression to the ℓth power again to get rid of the τ^ℓ term. Thus $\pi^{\ell^2(\ell-1)} \equiv 1 \pmod{\mathfrak{p}^4}$, and k divides $\ell^2(\ell-1)$.
- If $\ell\mathcal{O}_K = \mathfrak{p}^2\mathfrak{q}^2$ or $\mathfrak{p}^2\mathfrak{q}\mathfrak{r}$, then all of the primes in question have inertia degree 1, so k divides $\ell(\ell-1)$.
- If $\ell\mathcal{O}_K = \mathfrak{p}^2\mathfrak{q}$, then $\mathfrak{p}$ has inertia degree 1 and $\mathfrak{q}$ has inertia degree 2, so k divides $\operatorname{lcm}(\ell(\ell-1), \ell^2-1) = \ell(\ell^2-1)$.
- If $\ell\mathcal{O}_K = \mathfrak{p}^2$, then $\mathcal{O}_K/\mathfrak{p} \cong \mathbb{F}_{\ell^2}$, and thus we have $\pi^{\ell^2-1} = 1+\tau$ for some $\tau \in \mathfrak{p}$. Then $(1+\tau)^\ell \in 1+\mathfrak{p}^2$, so $\pi^{\ell(\ell^2-1)} \equiv 1 \pmod{\mathfrak{p}^2}$. Thus k divides $\ell(\ell^2-1)$.

Thus far we have used only the fact that π is an algebraic integer, and we have not used the property that it represents the action of Frobenius. To get a better bound in the case where ℓ is inert in K, we recall that since π is the Frobenius endomorphism, we have $\pi\overline{\pi} = p$, and $K = \mathbb{Q}(\pi)$. Since ℓ is inert, reduction modulo ℓ gives an injective group homomorphism

$$\phi\colon \operatorname{Aut}\left(K/\mathbb{Q}\right) \to \operatorname{Aut}\left((\mathcal{O}_K/\ell\mathcal{O}_K)/(\mathbb{Z}/\ell\mathbb{Z})\right).$$

Furthermore, the target group is isomorphic to $\operatorname{Gal}(\mathbb{F}_{\ell^4}/\mathbb{F}_\ell)$. This group is cyclic of order 4 and is generated by the ℓth-power Frobenius automorphism. Since complex conjugation has order 2 in $\operatorname{Aut}(K/\mathbb{Q})$, its image under ϕ must be the map $\alpha \mapsto \alpha^{\ell^2}$. Thus $\overline{\pi} \equiv \pi^{\ell^2} \pmod{\ell}$, and $\pi^{\ell^2+1} \equiv p \pmod{\ell}$. Since p must reduce to an element of $\mathbb{F}_\ell^\times$, p has order dividing $\ell-1$, so π must have order dividing $(\ell^2+1)(\ell-1)$. □

The following proposition shows that in the cases we need for our application, the field of definition of the ℓ^d-torsion points is determined completely by the field of definition of the ℓ-torsion points.

Proposition 5.6.3. *Let A be an ordinary abelian variety defined over a finite field F, and let ℓ be a prime number not equal to the characteristic of F. Let d be a positive integer, and let F' be the extension field of F of degree ℓ^{d-1}. If the ℓ-torsion points of A are defined*

over F, then the ℓ^d-torsion points of A are defined over F'. If $\mathrm{End}(A)$ *is integrally closed, then the converse also holds.*

Proof. Let $R = \mathrm{End}(A)$, and let $\pi \in R$ be the Frobenius endomorphism of F. By [34, Fact 10], for any positive integers t and k, the ℓ^t-torsion points of A are defined over the degree-k extension of F if and only if $\frac{\pi^k - 1}{\ell^t} \in R$, i.e., $\pi^k \equiv 1 \pmod{\ell^t R}$. To prove the proposition, it suffices to show that

$$\pi \equiv 1 \pmod{\ell R} \quad \Leftrightarrow \quad \pi^{\ell^{d-1}} \equiv 1 \pmod{\ell^d R},$$

with ($\Leftarrow$) holding when R is integrally closed.

First suppose that $\pi^k \equiv 1 \pmod{\ell^t R}$, with $t \geq 1$. Then we can write $\pi^k = 1 + \ell^t y$ for some $y \in R$. Then

$$\pi^{k\ell} = 1 + \ell(\ell^t y) + \binom{\ell}{2}(\ell^t y)^2 + \cdots + (\ell^t y)^\ell,$$

so $\pi^{k\ell} \equiv 1 \pmod{\ell^{t+1} R}$. We conclude that if the points of $A[\ell^t]$ are defined over the degree-k extension of F, then the points of $A[\ell^{t+1}]$ are defined over the degree-$k\ell$ extension of F. If $A[\ell] \subset A(F)$, then by induction $A[\ell^d] \subset A(F')$.

Now suppose that $\pi^{k\ell} \equiv 1 \pmod{\ell^t R}$, with $t \geq 2$. Since A is ordinary, R is an order in a number ring. Thus if R is integrally closed then it is a Dedekind domain, and we may write $\ell R = \prod \mathfrak{p}_i^{e_i}$ uniquely for prime ideals $\mathfrak{p}_i \subset R$. By the Chinese remainder theorem, $\pi^k \equiv 1 \pmod{\ell^t R}$ if and only if $\pi^k \equiv 1 \pmod{\mathfrak{p}_i^{e_i t}}$ for each i, so we may consider the problem locally at each $\mathfrak{p}_i$. Localizing and completing the ring R at the prime $\mathfrak{p}_i$ gives a complete local ring R_v with maximal ideal $\mathfrak{p}_i$ and valuation v satisfying $v(\ell) = e_i$.

By hypothesis, we may write $\pi^{k\ell} = 1 + y$ for some $y \in \mathfrak{p}_i^{e_i t}$. We can define the ℓth-root function on R_v to be

$$(1+y)^{1/\ell} = \exp\left(\frac{1}{\ell}\log(1+y)\right).$$

By [98, Proposition II.5.5], if $y \in \mathfrak{p}_i^{e_i t}$ then $\log(1+y) \in \mathfrak{p}_i^{e_i t}$. Since $v(\ell) = e_i$, we have $v(\frac{1}{\ell}\log(1+y)) \geq e_i(t-1)$, so by the same proposition $(1+y)^{1/\ell}$ converges and is in $1+\mathfrak{p}_i^{e_i(t-1)}$ whenever $(t-1)(\ell-1) > 1$. Thus if $(t-1)(\ell-1) > 1$ then $\pi^k \equiv 1 \pmod{\mathfrak{p}_i^{e_i(t-1)}}$. We conclude that if $t > 2$ or $\ell > 2$ and the points of $A[\ell^t]$ are defined over the degree-$k\ell$ extension of F, then the points of $A[\ell^{t-1}]$ are defined over the degree-k extension of F. If $A[\ell^d] \subset A(F')$, then by descending induction $A[\ell] \subset A(F)$ if ℓ is odd, and $A[4] \subset A(F_2)$ if $\ell = 2$, where F_2 is the quadratic extension of F.

It remains to show that if $A[4] \subset A(F_2)$, then $A[2] \subset A(F)$. This is equivalent to showing that if $\pi^2 - 1 \in 4R$ then $\pi - 1 \in 2R$. We prove the contrapositive: suppose $\pi - 1 \notin 2R$. Then there is some prime $\mathfrak{p}$ over 2 such that $v_\mathfrak{p}(\pi - 1) < v_\mathfrak{p}(2)$. Since $\pi + 1 = (\pi - 1) + 2$ and $v_\mathfrak{p}(\pi - 1) < v_\mathfrak{p}(2)$, we must also have $v_\mathfrak{p}(\pi + 1) < v_\mathfrak{p}(2)$. Multiplying the two expressions gives $v_\mathfrak{p}(\pi^2 - 1) < v_\mathfrak{p}(4)$, so $\pi^2 - 1$ cannot be contained in $4R$. We conclude that $\pi^2 - 1 \in 4R$ implies $\pi - 1 \in 2R$. □

Corollary 5.6.4. *Let J be the Jacobian of a genus 2 curve over $\mathbb{F}_p$, with $p > 3$, and suppose that $\mathrm{End}(J)$ is isomorphic to the ring of integers $\mathcal{O}_K$ of the primitive quartic CM field K. Let $\pi \in \mathcal{O}_K$ correspond to the Frobenius endomorphism of J, and let ℓ^d be a prime power dividing $[\mathcal{O}_K : \mathbb{Z}[\pi, \overline{\pi}]]$. Suppose $\mathbb{F}_{p^k}$ is the smallest field over which the points of $J[\ell^d]$ are defined. Then $k < 3p^6$.*

Proof. We have $\ell \neq p$ by Proposition 5.3.6. By Proposition 5.6.2, the points of $J[\ell]$ are defined over a field F of degree less than ℓ^3 over $\mathbb{F}_p$. By Proposition 5.6.3, the points of $J[\ell^d]$ are defined over a field L of degree ℓ^{d-1} over F. Since degrees of extensions multiply, we get

$$k = [L : \mathbb{F}_p] < \ell^{d+2} \leq \ell^{3d}.$$

By Proposition 5.6.1, $\ell^d \leq \frac{16}{\sqrt{\Delta}} p^2$, where Δ is the discriminant of the quartic CM field K. Lemma 5.6.5 below shows that any primitive quartic CM field has $\Delta \geq 125$, so $\ell^d \leq \frac{16}{\sqrt{125}} p^2$. Since $k < \ell^{3d}$, we conclude that $k < 3p^6$. □

Lemma 5.6.5. *Suppose K is a primitive quartic CM field. Then $\Delta(K) \geq 125$.*

Proof. Since $\Delta(\mathbb{Q}(\zeta_5)) = 125$, it suffices to show that no smaller discriminant can occur. The fact that $\Delta(K) > 0$ follows from [59, Proposition 9.4]. Now suppose $\Delta(K) < 125$. Since $\Delta(K_0)^2 \mid \Delta(K)$, we must have $K_0 = \mathbb{Q}(\sqrt{2})$ or $\mathbb{Q}(\sqrt{5})$, as these are the only two real quadratic fields with discriminant less than 12. Since $\mathbb{Q}(\sqrt{2})$ has class number 1, by [98, Proposition VI.6.9] $\mathbb{Q}(\sqrt{2})$ has no unramified quadratic extensions, so $\Delta(K)$ is strictly greater than $\Delta(K_0)^2$. Thus if $K_0 = \mathbb{Q}(\sqrt{2})$ then $\Delta(K) \geq 128$.

We deduce that $K_0 = \mathbb{Q}(\sqrt{5})$ and K must be of the form $\mathbb{Q}(i\sqrt{a + b\sqrt{5}})$, with a, b, and $a^2 - 5b^2$ positive integers. Since K is primitive, $a^2 - 5b^2$ is not a square in $\mathbb{Q}$ and its square-free part divides $\Delta(K)/\Delta(K_0)^2$. It thus suffices to show that the square-free part of $a^2 - 5b^2$ is at least 5; this follows from the fact that 2 and 3 are inert in $\mathbb{Q}(\sqrt{5})$, so there are no integer solutions to $a^2 - 5b^2 = 2$ or 3. □

5.7 Computing Igusa class polynomials

This section combines the results of all of the previous sections into a full-fledged probabilistic version of Eisenträger and Lauter's CRT algorithm to compute Igusa class polynomials for primitive quartic CM fields [34, Theorem 1].

Algorithm 5.7.1. The following algorithm takes as input a primitive quartic CM field K not isomorphic to $\mathbb{Q}(\zeta_5)$, three integers $\lambda_1, \lambda_2, \lambda_3$ which are multiples of the denominators of the three Igusa class polynomials for K, and a real number $\epsilon > 0$, and outputs three polynomials $H_1, H_2, H_3 \in \mathbb{Q}[x]$. Heuristically, the polynomials $H_i(x)$ output by the algorithm are with high probability the Igusa class polynomials for K.

1. (Initialization.)

   (a) Let D be the degree of the Igusa class polynomials for K. (See [132, Theorem 3.1] for the case where the real quadratic subfield K_0 has class number 1, and [51, preprint version, Corollary 3.1] for the general case.)

   (b) Compute an integral basis $\mathcal{B}$ for $\mathcal{O}_K$, using e.g. [26, Algorithm 6.1.8].

   (c) Set $p \leftarrow 3$, $B \leftarrow 1$, $H_1, H_2, H_3 \leftarrow 0$, $F_1, F_2, F_3 \leftarrow 0$.

2. Set $p \leftarrow \texttt{NextPrime}(p)$ until p splits completely in K and p splits into principal ideals in $\widehat{K}$ (the reflex field of K).

3. (Finding the curves.) Set $T_1, T_2, T_3 \leftarrow \{\}$. For each $(j_1, j_2, j_3) \in \mathbb{F}_p^3$, do the following:

   (a) Compute a curve $C/\mathbb{F}_p$ with Igusa invariants (j_1, j_2, j_3), using the algorithms of Mestre [88] and Cardona-Quer [22].

   (b) Run Algorithm 5.2.1 with inputs K, p, C.

      i. If the algorithm outputs `false`, go to the next triple (j_1, j_2, j_3).

      ii. If the algorithm outputs `true`, let π be one of the possible Frobenius elements it outputs.

   (c) For each prime ℓ dividing $[\mathcal{O}_K : \mathbb{Z}[\pi, \overline{\pi}]]$, do the following:

      i. Run Algorithm 5.4.1 with inputs K, ℓ, π. Let the output be k.

      ii. Run Algorithm 5.4.3 with inputs $\mathrm{Jac}(C)$, $\mathbb{F}_{p^k}$, ℓ, and ϵ. If the output is `false`, go to the next triple (j_1, j_2, j_3).

iii. If ℓ^2 divides $[\mathcal{O}_K : \mathbb{Z}[\pi, \overline{\pi}]]$ or $\frac{\pi^k - 1}{\ell} \in \mathbb{Z}[\pi]$, then for each $\alpha \in \mathcal{B} \setminus \mathbb{Z}$ written in the form (5.3) with denominator n, do the following:

A. Let d be the largest integer such that $\ell^d \mid n$. If $d = 0$, go to the next α.

B. Set $k' \leftarrow k\ell^{d-1}$.

C. Run Algorithm 5.5.1 with inputs $\mathrm{Jac}(C), p^{k'}, \ell^d, \frac{n}{\ell^d}\alpha, \epsilon$.

D. If Algorithm 5.5.1 outputs `false`, go to the next triple (j_1, j_2, j_3). Otherwise go to the next α.

(d) Adjoin j_1, j_2, j_3 to the sets T_1, T_2, T_3, respectively (counting multiplicities).

4. If the size of each set T_1, T_2, T_3 is not equal to D, go to Step (2).

5. (Computing the Igusa class polynomials.) For $i \in \{1, 2, 3\}$, do the following:

(a) Compute $F_{i,p}(x) = \lambda_i \prod_{j \in T_i}(x - j)$ in $\mathbb{F}_p[x]$.

(b) Use the Chinese remainder theorem to compute $F_i'(x) \in \mathbb{Z}[x]$ such that $F_i'(x) \equiv F_i(x) \pmod{B}$, $F_i'(x) \equiv F_{i,p}(x) \pmod{p}$, and the coefficients of $F_i'(x)$ are in the interval $[-pB/2, pB/2]$.

(c) If $F_i'(x) = F_i(x)$, output $H_i(x) = \lambda_i^{-1} F_i(x)$. If $H_i(x)$ has been output for all i, terminate the algorithm.

(d) Set $F_i(x) \leftarrow F_i'(x)$.

6. Set $B \leftarrow pB$, and return to Step (2).

Proof. In view of [34, Theorem 1], it suffices to prove that Step (3c) correctly determines the set of curves with $\mathrm{End}(\mathrm{Jac}(C)) = \mathcal{O}_K$. It follows from Section 5.3 that $\mathrm{End}(\mathrm{Jac}(C)) = \mathcal{O}_K$ if and only if each of the elements of the generating set listed in Proposition 5.3.7 is an endomorphism.

By Algorithm 5.2.1, the π computed in Step (3b) is such that π^σ is the Frobenius element of $\mathrm{Jac}(C)$ for some $\sigma \in \mathrm{Aut}(K/\mathbb{Q})$. By Corollary 5.3.9, $\mathrm{End}(\mathrm{Jac}(C)) = \mathcal{O}_K$ if and only if β^σ is an endomorphism for each β in the generating set of Proposition 5.3.7. Since elements of $\mathrm{Aut}(K/\mathbb{Q})$ preserve $\mathcal{O}_K$ as a set, $[\mathcal{O}_K : \mathbb{Z}[\pi^\sigma, \overline{\pi}^\sigma]] = [\mathcal{O}_K : \mathbb{Z}[\pi, \overline{\pi}]]$.

For each ℓ dividing $[\mathcal{O}_K : \mathbb{Z}[\pi, \overline{\pi}]]$, Steps (3(c)i) and (3(c)ii) test probabilistically whether $\frac{(\pi^\sigma)^k - 1}{\ell}$ is an endomorphism for an appropriate k. By Corollary 5.3.4, for any such ℓ dividing $[\mathcal{O}_K : \mathbb{Z}[\pi, \overline{\pi}]]$ exactly, this suffices to determine whether $\frac{n}{\ell}\alpha^\sigma$ is an endomorphism for each $\alpha \in \mathcal{B} \setminus \mathbb{Z}$.

By Corollary 5.5.2, if ℓ^2 divides $[\mathcal{O}_K : \mathbb{Z}[\pi, \overline{\pi}]]$ then Step (3(c)iii) tests probabilistically whether $\frac{n}{\ell^d}\alpha^\sigma$ is an endomorphism. The input uses the field $\mathbb{F}_{p^{k'}}$ because Proposition 5.6.3 implies that if the ℓ-torsion points are defined over $\mathbb{F}_{p^k}$, then the ℓ^d-torsion points are defined over $\mathbb{F}_{p^{k'}}$.

The "heuristic" part of the statement refers to the termination procedure in Step (5), which differs from the corresponding step in [34, Theorem 1]. After the nth prime p_n we use the Chinese remainder theorem to compute integer polynomials $F_i(x)$ that, by Theorem 5.1.2, are the Igusa class polynomials for K modulo $B_n = \prod_{j=1}^{n} p_j$. If for some i the $F_i(x)$ agree for the nth and $(n+1)$th primes, then with high probability the coefficients of $\lambda_i H_i(x) \in \mathbb{Z}[x]$ are less than B_{n+1}, and thus $F_i(x)$ is equal to $H_i(x)$ itself. This conclusion is justified by the fact that if an integer m has the property that it is the same modulo B_n and modulo B_{n+1}, then $m = a_n + r_n B_n = a_{n+1} + r_{n+1} B_{n+1}$, with $a_n = a_{n+1} < B_n$. It follows that p_{n+1} divides r_n. Since the probability of this happening for a random number r_n is $1/p_{n+1}$, the probability that all coefficients would simultaneously satisfy this congruence is $(1/p_{n+1})^D$, so heuristically we expect that r_{i+1} is actually zero for each coefficient. □

Remark 5.7.2. The λ_i input into the algorithm can be taken to be products of primes bounded in [54], raised to a power that will be made explicit in forthcoming work. In practice, the power can be taken to be a small multiple of 6.

Our version of the algorithm minimizes the amount of computation by terminating the algorithm in Step (5c) as soon as the polynomials agree modulo two consecutive primes. Since we check after every prime p_i whether the algorithm is finished, we do not need to know in advance the number of primes p_i that we will need to use. Thus the only bounds that need to be computed in advance are the bounds λ_i on the denominators of the coefficients of the Igusa class polynomials. In particular, we do not need to have a bound on either the numerators or the absolute values of the coefficients.

5.8 Implementation notes

Our most significant observation is that in practice, the running time of the probabilistic CRT algorithm is dominated by generating p^3 curves for each small p. Steps (3a) and (3b) of Algorithm 5.7.1 generate a list of curves C for which $\mathrm{End}(\mathrm{Jac}(C))$ is an order in $\mathcal{O}_K$. Algorithms 5.4.3 and 5.5.1 determine which endomorphism rings are equal to $\mathcal{O}_K$. Data

comparing the relative speeds of these two parts of the algorithm appear in Section 5.9. This section describes a number of ways to speed up Algorithm 5.7.1, which are reflected in the running times that appear in Section 5.9.

1. If p and k are large, then the extra time required to do arithmetic on $J(\mathbb{F}_{p^k})$ can slow down Algorithms 5.4.3 and 5.5.1 considerably. Since for various ℓ dividing the index $[\mathcal{O}_K : \mathbb{Z}[\pi, \overline{\pi}]]$, the extension degrees k depend only on the prime p and the CM field K and not on the curve C, these extension degrees may be computed in advance (via Algorithm 5.4.1) before generating any curves. We set some bound N and tell the program that if the extension degree k for some ℓ is such that $p^k > N$, we should skip that p and go on to the next prime. For example, if $K = \mathbb{Q}(i\sqrt{13 + 2\sqrt{13}})$ and $p = 53$ (see Example 5.9.2), we have $[\mathcal{O}_K : \mathbb{Z}[\pi, \overline{\pi}]] = 3^2 \cdot 43$, and the 43-torsion of a Jacobian J with $\mathrm{End}(J) = \mathcal{O}_K$ will be defined over $\mathbb{F}_{p^{924}}$, a field of over 5000 bits that is far too large for our current implementation to handle efficiently.

2. In a similar vein, since the speed of Algorithms 5.4.3 and 5.5.1 is determined by the size of the fields $\mathbb{F}_{p^k}$, for optimum performance one should perform these calculations in order of increasing k, so that as the fields get larger there are fewer curves to check.

3. Algorithms 5.4.3 and 5.5.1 take a single curve as input. In Algorithm 5.7.1 those algorithms are executed with the same field K and many different curves, so any parameter that only depends on the field K and the prime p can be precomputed and stored for repeated reference. For example, the representation $\alpha = (a_0 + a_1\pi + a_2\pi^2 + a_3\pi^3)/n$ and the extension degrees k in Step (3(c)i) can be computed only once. In addition, all of the curves that pass Step (3b) have one of a small number of given zeta functions. Since $\#J(\mathbb{F}_{p^k})$ is determined by the zeta function, this number can also be computed in advance.

4. If $\mathbb{F}_{p^k}$ is small enough, it may be faster to check fields of definition using the brute force method of Section 5.4.1, rather than Algorithm 5.4.3. If ℓ is small (as must be the case for k to be small), then we often find that $\#J(\mathbb{F}_{p^k}) = \ell^s m$ with $s \gg 4d$, and thus the number of random points needed in Algorithms 5.4.3 and 5.5.1 will be very large. While computing the group structure is an exponential-time computation, we find that if the group has size at most 2^{200}, MAGMA can compute the group structure fairly quickly.

5. If Step (5c) has already output $H_i(x)$ for some i, the roots of this polynomial mod p can be used as the possible values of j_i in Step (3). This will greatly speed up the calculation of the $F_{i,p}$ for the remaining primes: if one H_i has been output then only p^2D curves need to be computed (instead of p^3), and if two H_i have been output then only pD^2 curves need to be computed.

6. In practice, for small primes p ($p < 800$ in our MAGMA implementation), computing $\#C(\mathbb{F}_p)$ (Step (5b) of Algorithm 5.2.1) is more efficient than choosing a random point on $J(\mathbb{F}_p)$ and determining whether it is killed by one of the potential group orders (Step (5a) of Algorithm 5.2.1), so these two steps should be switched for maximum speed. However, as p grows, the order of the steps as presented will be the fastest.

7. Finally, we note that Algorithm 5.7.1 can easily be parallelized. One could assign to each processor a different prime p for which to compute curves, with a central processor combining the results via the Chinese remainder theorem. Or some processors could compute curves, some could run Algorithm 5.4.3, and some could run Algorithm 5.5.1. These two algorithms could even themselves be parallelized, with each processor computing a different random point on the Jacobian, and the central processor tallying which ones pass or fail the appropriate test.

5.9 Examples

This section describes the performance of Algorithm 5.7.1 on three quartic CM fields: $\mathbb{Q}(i\sqrt{2+\sqrt{2}})$, $\mathbb{Q}(i\sqrt{13+2\sqrt{13}})$, and $\mathbb{Q}(i\sqrt{29+2\sqrt{29}})$. These fields are all Galois and have class number 1, so the density of primes with the desired splitting behavior is maximal. The Igusa polynomials are linear; they have integral coefficients for the first two fields, and have denominators dividing 5^{12} for the last. In all three examples, as p grows the running time of the algorithm becomes dominated by the computation of p^3 curves for each p, whereas it was previously suspected that the endomorphism ring computation would be the slow step in the CRT algorithm. A fast implementation in C to produce the curves from their Igusa invariants and to test the numbers of points would thus significantly improve the running time of the CRT algorithm.

Details of the algorithms' execution are given below. The algorithms were run on a 2.39 GHz AMD Opteron with 4 GB of RAM. The table headings have the following

meaning:

- p: Size of prime field over which curves were generated.
- ℓ^d: Prime powers appearing in the denominators n of elements α input into Algorithms 5.4.3 and 5.5.1, when written in the form (5.3).
- k: Degrees of extension fields over which ℓ^d-torsion points are expected to be defined. These are listed in the same order as the corresponding ℓ^d.
- Curves: Time taken to generate p^3 curves and determine which have CM by K (cf. Algorithm 5.2.1).
- #Curves: Number of curves computed with CM by K.
- 5.4.3 & 5.5.1: Time taken to run Algorithms 5.4.3 and 5.5.1 to find the single curve whose Jacobian has endomorphism ring equal to $\mathcal{O}_K$.

Example 5.9.1. We ran Algorithm 5.7.1 with $K = \mathbb{Q}(i\sqrt{2+\sqrt{2}})$ and $\lambda_1, \lambda_2, \lambda_3 = 1$. The results appear in Table 5.1. The last column of the table shows the intermediate polynomials $F_i(x)$ computed via the Chinese remainder theorem in Step (5b). The algorithm output the $F_i(x)$ listed for $p = 151$ as the Igusa class polynomials of K.

The total time of this run was 3162 seconds, or about 53 minutes. We observe that the polynomials F_2 and F_3 agree for $p = 103$ and $p = 113$. We deduce that these polynomials are the correct Igusa polynomials, and following note (5) of Section 5.8, we use their roots for the values of j_2 and j_3 for $p = 151$. Thus instead of computing $151^3 \approx 2^{22}$ curves, we need to compute only 151 curves, out of which we can easily choose the right one. As a result, the computation for $p = 151$ takes practically no time at all. The same phenomenon also appears for the last prime in Examples 5.9.2 and 5.9.3. □

Example 5.9.2. We ran Algorithm 5.7.1 with $K = \mathbb{Q}(i\sqrt{13+2\sqrt{13}})$ and $\lambda_1, \lambda_2, \lambda_3 = 1$. The results appear in Table 5.2. The algorithm output the following Igusa class polynomials:

$$x - 1836660096, \quad x - 28343520 \quad x - 9762768.$$

The total time of this run was 6969 seconds, or about 116 minutes. In this example we skip some primes because Algorithms 5.4.3 and 5.5.1 would need to compute in fields which are too large to be practical. In particular, for $p = 29, 53, 107, 139$, the algorithms

Table 5.1: Results for Algorithm 5.7.1 run with $K = \mathbb{Q}(i\sqrt{2+\sqrt{2}})$ and $\lambda_1, \lambda_2, \lambda_3 = 1$.

p	ℓ^d	k	Curves	#Curves	5.4.3 & 5.5.1	$F_i(x)$
7	2,4	2,4	0.5 sec	7	0.3 sec	$x+2$ $x+5$ $x+6$ (mod 7)
17	4,8	2,4	4 sec	39	0.2 sec	$x-54$ $x+19$ $x-8$ (mod 119)
23	2,4,7	2,4,3	9 sec	49	2.3 sec	$x+1017$ $x+852$ $x+111$ (mod 2737)
71	2,4	2,4	255 sec	7	0.7 sec	$x-75619$ $x+28222$ $x-46418$ (mod 194327)
97	4,8	2,4	680 sec	39	0.3 sec	$x-8237353$ $x+9355918$ $x+9086951$ (mod 18849719)
103	2,4,17	2,4,16	829 sec	119	17.6 sec	$x+104860961$ $x-28343520$ $x-9762768$ (mod 1941521057)
113	7,8,32	6,4,16	1334 sec	1281	28.8 sec	$x-1836660096$ $x-28343520$ $x-9762768$ (mod 219391879441)
151	2,4,7,17	2,4,6,16	0.2 sec	1	–	$x-1836660096$ $x-28343520$ $x-9762768$ (mod 33128173795591)

would run over extension fields of degree $264, 924, 308, 162$, all of which have well over 1000 bits. Skipping these primes has no effect on the ultimate outcome of the algorithm. □

Example 5.9.3. We ran Algorithm 5.7.1 with $K = \mathbb{Q}(i\sqrt{29+2\sqrt{29}})$ and $\lambda_1, \lambda_2, \lambda_3 = 5^{12}$. The results appear in Table 5.3. The algorithm output the following Igusa class polynomials:

$$x - \frac{2614061544410821165056}{5^{12}}, \quad x + \frac{586040972673024}{5^6}, \quad x + \frac{203047103102976}{5^6}.$$

The total time of this run was 56585 seconds, or about 15 hours, 43 minutes. In this example we again skip some primes because the fields input to Algorithms 5.4.3 and 5.5.1 would be too large. We also note that for $p = 7$, $\mathcal{O}_K = \mathbb{Z}[\pi, \overline{\pi}]$, so any curve over $\mathbb{F}_7$ that has a correct zeta function already has CM by all of $\mathcal{O}_K$, and we do not need to run Algorithms 5.4.3 and 5.5.1. □

Table 5.2: Results for Algorithm 5.7.1 with $K = \mathbb{Q}(i\sqrt{13+2\sqrt{13}})$ and $\lambda_1, \lambda_2, \lambda_3 = 1$.

p	ℓ^d	k	Curves	#Curves	5.4.3 & 5.5.1
29	3,23	2,264	–	–	–
53	3,43	2,924	–	–	–
61	3	2	167 sec	9	0.2 sec
79	27	18	376 sec	81	8.1 sec
107	9,43	6,308	–	–	–
113	3,53	1,52	1118 sec	159	137.2 sec
131	9,53	6,52	1872 sec	477	127.4 sec
139	9,243	6,162	–	–	–
157	9,81	6,54	3147 sec	243	16.5 sec
191	3,4,8	2,2,4	0.2 sec	1	–

Remark 5.9.4. The data in Examples 5.9.1, 5.9.2, and 5.9.3 suggest that odd primes dividing the index $[\mathcal{O}_K : \mathbb{Z}[\pi, \overline{\pi}]]$ always split in $\mathcal{O}_{K_0}$, the ring of integers of K_0. In fact the factorization of the index $[\mathcal{O}_K : \mathbb{Z}[\pi, \overline{\pi}]]$ was given in [34, Proposition 5] for primitive quartic CM fields K when K_0 has class number 1. We write $\pi = c_1 + c_2\sqrt{d} + (c_3 + c_4\sqrt{d})\eta$, where the c_i are rational numbers with only powers of 2 in the denominators and $\eta = i\sqrt{a + b\sqrt{d}}$ with $a, b, d \in \mathbb{Z}$, $d > 0$ and square-free. Then the index is, up to powers of 2, the product of c_2 with $(c_3^2 - c_4^2 d)$, where c_2 is the index of $\mathbb{Z}[\pi + \overline{\pi}]$ in $\mathcal{O}_{K_0}$ up to a power of 2. If a prime divides $(c_3^2 - c_4^2 d)$ exactly, then the prime splits in K_0. Thus primes different from 2 dividing the index $[\mathcal{O}_K : \mathbb{Z}[\pi, \overline{\pi}]]$ exactly either split in K_0 or divide the index $[\mathcal{O}_{K_0} : \mathbb{Z}[\pi + \overline{\pi}]]$. So except possibly for primes dividing c_2, no odd primes dividing the index $[\mathcal{O}_K : \mathbb{Z}[\pi, \overline{\pi}]]$ exactly are inert or totally ramified in K. If K is Galois, then this is enough to ensure that the extension degree k determined by Proposition 5.6.2 is at most ℓ^2. This agrees with the data in our examples, all of which considered Galois fields.

In practice, if a prime ℓ is inert or totally ramified in K, it would almost certainly be skipped anyway, since Proposition 5.6.2 shows that the ℓ-torsion may be defined over an extension field of degree $k \sim \ell^3$, which is too large to be practical (cf. Note (1) of Section 5.8). The theoretical running times of Algorithms 5.4.3 and 5.5.1, given by Propositions 5.4.6 and 5.5.5 respectively, improve if inert or ramified primes ℓ are not considered. The slow step of both algorithms is computing a random point on $J(\mathbb{F}_{p^k})$, which takes roughly $O(k^2 \log k (\log p)^2)$ operations in $\mathbb{F}_p$. Since the bound on ℓ given by Proposition 5.6.1 is p^2, if k is bounded by ℓ^2 instead of ℓ^3, this step would run in $O(p^8 \log^3 p)$ instead of $O(p^{12} \log^3 p)$

Table 5.3: Results for Algorithm 5.7.1 with $K = \mathbb{Q}(i\sqrt{29+2\sqrt{29}})$ and $\lambda_1, \lambda_2, \lambda_3 = 5^{12}$.

p	ℓ^d	k	Curves	#Curves	5.4.3 & 5.5.1
7	–	–	0.3 sec	1	–
23	13	84	9 sec	15	70.7 sec
53	7	6	105 sec	7	0.5 sec
59	4,5,8	2,12,4	164 sec	322	6.4 sec
83	3,5	4,24	431 sec	77	9.8 sec
103	67	1122	–	–	–
107	7,13	6,42	963 sec	105	69.3 sec
139	7,25	2,60	2189 sec	259	62.1 sec
181	9,27	6,18	84 min	161	3.6 sec
197	5,109	24,5940	–	–	–
199	25	60	106 min	37	1355.3 sec
223	4,8,23	2,4,22	174 min	1058	35.1 sec
227	109	1485	–	–	–
233	5,7,13	8,3,28	193 min	735	141.6 sec
239	7,109	6,297	–	–	–
257	3,7,13	4,6,84	286 min	1155	382.8 sec
277	5,7,23	24,6,22	0.3 sec	1	–

time.

Appendix A

Parameters for Pairing-Friendly Abelian Varieties

A.1 Elliptic curves with embedding degree 10

In this section we give results of the execution of Algorithm 3.1.4 with inputs

$$\texttt{MinBits} = 148, \quad \texttt{MaxBits} = 512, \quad \texttt{MaxD} = 2 \cdot 10^9.$$

Mike Scott implemented the computations in C++/NTL [116] and recorded the data [111].

A.1.1 Curves of prime order

Scott's search found 23 curves of prime order over fields of size between 149 and 491 bits. Below we give the field size p, the group size r, and the CM discriminant D for each curve. A curve equation can be determined by computing the Hilbert class polynomial for the ring of integers of $\mathbb{Q}(\sqrt{-D})$ and finding a curve $E/\mathbb{F}_p$ whose j-invariant is a root of the class polynomial mod p.

```
p = 149 bits, r = 149 bits,
D = 1666603
p = 503189899097385532598615948567975432740967203
r = 503189899097385532598571084778608176410973351

p = 167 bits, r = 167 bits,
D = 1744734787
p = 122422753977607994982409086499580592436601185116163
r = 122422753977607994982409064370617311016660704117271
```

```
p = 171 bits, r = 171 bits,
D = 185395987
p = 208332635780340073250223056873601747847583259083020 3
r = 208332635780340073250223047744907738727985799855985 1

p = 171 bits, r = 171 bits,
D = 190795843
p = 288783459370564703358074204145978499714156295998468 3
r = 288783459370564703358074193398263219328939404437805 1

p = 172 bits, r = 172 bits,
D = 1141200763
p = 359076370297381250436079655430433412985633590447104 3
r = 359076370297381250436079643445837127797195914200576 1

p = 180 bits, r = 180 bits,
D = 990757243
p = 112229353097636239352327267681527245278107269334283872 3
r = 112229353097636239352327267469650532921476400874928767 1

p = 188 bits, r = 188 bits,
D = 648666907
p = 284980960902604464050497768248655074807567725439635139163
r = 284980960902604464050497768214892316572932660953073087771

p = 193 bits, r = 193 bits,
D = 1649528323
p = 102764571924850529265158016601185411362042194475393072237 23
r = 102764571924850529265158016599157954117858233596124222151 71

p = 196 bits, r = 196 bits,
D = 579003643
p = 610999632710831287460737695679448703542701616461509147946 03
r = 610999632710831287460737695674505022190871459164348396263 01

p = 234 bits, r = 234 bits,
D = 1227652867
p = 182116508039694720644932643473759500459342546966570904207262300432038 03
r = 182116508039694720644932643473759497760331557439520307504500337823066 51

p = 252 bits, r = 252 bits,
D = 1039452307
p = 646231099734881696220312491050525208267333884696643120163526269440282546 1643
r = 646231099734881696220312491050525208251256184615662859556277645930629210 1261

p = 264 bits, r = 264 bits,
D = 838990723
p = 226658387733617424895482877886636691504567765051420712623670782263702135 79241
243
```

```
r = 2266583877336174248954828778866366915044725477446464465443703904128748041224
6011

p = 273 bits, r = 273 bits,
D = 1683538387
p = 994794232666423237609928058426429521447069688546648293074214122573541834135 2
714723
r = 994794232666423237609928058426429521447049740672248583984030461536583196340 7
761671

p = 291 bits, r = 291 bits,
D = 296281483
p = 379990392681977058452495476314208006476310062395438907088580360605203330085 7
169141842683
r = 379990392681977058452495476314208006476310050066766753414007796539749330763 4
688343579051

p = 301 bits, r = 301 bits,
D = 126139963
p = 229590661297133079381948076027760211454827228448580626683530669594586944720 4
270532747317643
r = 229590661297133079381948076027760211454827228145535639068072439998480149471 6
906367418265011

p = 309 bits, r = 309 bits,
D = 944184187
p = 522119709937996126778166390348868678648374232380302554854977677880618542177 0
49221041059499163
r = 522119709937996126778166390348868678648374232334602676958510771597044173916 1
39398869610147771

p = 315 bits, r = 315 bits,
D = 1487526043
p = 386699228441871904134798367413371755952371867879791941205084116645573455134 6
5115369973641873883
r = 386699228441871904134798367413371755952371867875859007295434111331185978125 5
8823488880436227701

p = 331 bits, r = 331 bits,
D = 1431850363
p = 319419242308641760143653994515271261819878117271962244810429743137095534509 7
650741456242416736232203
r = 319419242308641760143653994515271261819878117271950941373035593660759104630 0
070761686891259023380851

p = 366 bits, r = 366 bits,
D = 33555283
p = 135476856029879968413909316283726176964624775041228997254413116437013327021 7
657630134608449835299087929646177 63
r = 135476856029879968413909316283726176964624775041228997231134211305553216325 5
```

```
39360593097745238140316627358904871

p = 380 bits, r = 380 bits,
D = 267410467
p = 233920494357954205615177947036887029576387192438271304204657640513376829939147781701738559228387684474384024084288
3
r = 233920494357954205615177947036887029576387192438271304204351751321440956398637139900428831172252519889465110851695
1

p = 404 bits, r = 404 bits,
D = 426205003
p = 259770659159119840599603256351585995837138902343320263588846416137970095208080776696742398947011709129254226147343609958
83
r = 259770659159119840599603256351585995837138902343320263588846314202567185498670907430126619209764638521653302590744400004
51

p = 415 bits, r = 415 bits,
D = 79434787
p = 551492409027707600613723061859746139256401933904382504912541909578396770026691474564488025217362585051737222114516029056349
63
r = 551492409027707600613723061859746139256401933904382504912541904881621667777457311799288968162259009200990653394037402370
43071

p = 491 bits, r = 491 bits,
D = 20056963
p = 342267073014074561106300839098488619908315313811302701601680802903448903628158983843044447505214731904468573943727521722811772416183057806409471652358983843044447505214731904468573943727521722811772416183057806409471652
3
r = 342267073014074561106300839098488619908315313811302701601680802903448903616458264668325748854478111469755079073946216087816105859530275605037923462158264668325748854478111469755079073946216087816105859530275605037923462
1
```

A.1.2 Curves with small cofactors

If we relax the condition of r being prime in Algorithm 3.1.4 and allow a "cofactor" h such that $\#E(\mathbb{F}_q) = hr$, we find many more suitable curves. Below we give parameters for all curves found by Scott with subgroup sizes between 148 and 512 bits and cofactors less than 100. In addition to the field size p, the subgroup size r, and the CM discriminant D, we give the cofactor h as well as the ρ-value $\log q / \log r$. Equations for the curves can again be constructed via the CM method.

```
p = 156 bits,
r = 152 bits
D = 1163411323
p = 464917992790652812629498455653723774780960056643
r = 422652720718775284208631039329372091930414375 1
h = 11
rho = 1.022824553
```

```
p = 173 bits,
r = 168 bits
D = 26906587
p = 10138978787899014979556710182668437938887966202371323
r = 32706383186771016063086161229946598611469640931634 1
h = 31
rho = 1.02952336

p = 178 bits,
r = 174 bits
D = 776358547
p = 249780845441118230976458804143017684580147331902502683
r = 22707349585556202816041709376677826345225287399591391
h = 11
rho = 1.019890545

p = 191 bits,
r = 188 bits
D = 125434987
p = 230278639654570064026713021344288581276458952245103671112 3
r = 20934421786779096729701183757699191813638133679731333766 1
h = 11
rho = 1.018490355

p = 198 bits,
r = 193 bits
D = 1464898147
p = 207996980122469265501634927384037072390157655791953255691043
r = 67095800039506214677946750768749980216652223738841145370 81
h = 31
rho = 1.025790194

p = 200 bits,
r = 195 bits
D = 119064067
p = 92457000003773987912963391843876146286797738844152969715844 3
r = 29824838710894834810633352207639947471175907455080071883331
h = 31
rho = 1.025504446

p = 202 bits,
r = 198 bits
D = 744549043
p = 34493571940622236799485901209415159537385706886144836184285 23
r = 31357792673292942544987182917616376951868859171269835992751 1
h = 11
rho = 1.017503473

p = 207 bits,
r = 202 bits
```

```
D = 448871083
p = 13703101785567581738777823237136303275298871528399133297795220 3
r = 44203554146992199157347816893980522807510646400286929830142 21
h = 31
rho = 1.024591482

p = 206 bits,
r = 203 bits
D = 164930707
p = 85329001180125284730411332555603275938544233454665921565241803
r = 77571819254659349754919393232349819271732235526603343565132 41
h = 11
rho = 1.017102936

p = 219 bits,
r = 216 bits
D = 40319947
p = 83756088155309460165689812633529380174531498853120140775892059 6923
r = 76141898323008600150627102394117451943478921237940702343764319 361
h = 11
rho = 1.016050657

p = 233 bits,
r = 227 bits
D = 1651027
p = 98640542846717342665471487697472260538327683361804153558211515023 76483
r = 16170580794543826666470735688110206319994881104609006892443713147 5941
h = 61
rho = 1.026174508

p = 239 bits,
r = 235 bits
D = 1600012003
p = 44717155905549750238504876914826670333870182701004607298256714363 1364283
r = 40651959914136136580458979013478791091025825243672251775637104184 579841
h = 11
rho = 1.014748707

p = 257 bits,
r = 254 bits
D = 546540763
p = 20627881217133872970696893677762700076025506981705135617495174766 76130997847
63
r = 18752619288303520882451721525238818250849701024611302388942433344 39547141051
1
h = 11
rho = 1.013653479

p = 261 bits,
r = 258 bits
```

```
D = 1874162947
p = 309170185227473146406128491657330251422750524639865621139130357333995721324256
3
r = 2810638047522483149146622651430275012930898726559765394195428324625634832050
61
h = 11
rho = 1.013446207

p = 288 bits,
r = 283 bits
D = 131545147
p = 250559957259021962953732187017315563100407812701611327704176736402417732164386
483115483
r = 808257926642006332108813506507469558388412196914321703237435763238084919716428
3969771
h = 31
rho = 1.017564536

p = 292 bits,
r = 286 bits
D = 646182403
p = 740470756986551430806132375561554085357736891433678047531669544304113904707397
1836925163
r = 121388648686319906689529897633041653337333913807140318802109889576792176957393
361142111
h = 61
rho = 1.020739349

p = 303 bits,
r = 299 bits
D = 46195603
p = 161723616736655438164236551795390524707155883602624210511030250328302007134734
22635764905483
r = 521689086247275606981408231598033950668244785555466001961245744217709665899947
504458831021
h = 31
rho = 1.016622879

p = 350 bits,
r = 346 bits
D = 1073269963
p = 150235002338363972338535752935498276647110295684572461544882573742071896499247
2747493168392511848802347723
r = 136577274853058156671396139032271160588282086985974957993500474304509388063499
0770770924961922570988565431 1
h = 11
rho = 1.010000374

p = 423 bits,
r = 420 bits
```

```
D = 57667387
p = 19539026190390247999449803189114514355064936310465740062191618458454620170979645740800898070801638548999046997998642389239186443
r = 17762751082172952726772548353740467595513578464059763692901471317830932754749196939544380619199545485898189174679786019086557 51
h = 11
rho = 1.008248687

p = 444 bits,
r = 440 bits
D = 1607123107
p = 285501601141536926997874855824477618142873554206575395267401440519107031704025289520469259262124301407470615405367521857560071205007 23
r = 259546910128669933634431687113161471038975958369613995697637673199091060913007293917347678893918525720019093315048923041632759075006 1
h = 11
rho = 1.007864659

p = 447 bits,
r = 441 bits
D = 1817751043
p = 25391840424023344337621076529099331218397449997447474312375186502960467874501621225375959681647921598576021242155452498480583035545288 3
r = 35763155526793442729043769759294832701968239433024611707570685215432790015535175619576480980091006422986968730786392162016812700022 81
h = 71
rho = 1.013966129

p = 475 bits,
r = 471 bits
D = 979125307
p = 56336589223407741481417209518418931436608105607497032295951858203778181419660975778630631263022704709935860464465151482184559035892069814412243
r = 51215081112188855892197463198562664942371005097724574814501689276161982677231249932179384877641614825920532824296371364436123562856307779922 51
h = 11
rho = 1.007348791

p = 476 bits,
r = 473 bits
D = 65006443
p = 16904816908064197633782754263562148197644438254478115708980287103174413289113870764770770019072755183280405603559860180696104438311107061542760 3
r = 15368015370967452394347958421420134725131307504071014280891170093794921097166304730765126839016510565041656664336961206271812456711656513850141
h = 11
rho = 1.007324126
```

A.2 Families of pairing-friendly abelian surfaces

Below we give data and example curves for all of the families of abelian surfaces with $\rho < 8$ that we found using Algorithm 4.4.9. For each family we give the following data:

- the embedding degree k,
- the CM field K and polynomial $r(x)$ input into Algorithm 4.4.9,
- the $\pi(x)$ output by the algorithm, and
- the ρ-value of the family (π, r).

We also give an example curve in each family. We used Algorithm 2.2.4 to find a value x_0 for which $q(x_0) = \pi(x_0)\overline{\pi}(x_0)$ is prime and $r(x_0)$ has a large prime factor. Since we are looking for varieties with prime-order subgroups of at least 160 bits, we input the value $y_0 = 2^{\lfloor 160/\deg r \rfloor + 1}$ into Algorithm 2.2.4. Given the output, we then used CM methods to construct a curve over $\mathbb{F}_{q(x_0)}$ whose Jacobian has the specified number of points. We give our results in the following format:

- The values x_0 and h output by Algorithm 2.2.4, as well as the values of a and b used in Step (1) of that algorithm,
- a genus 2 curve C over $\mathbb{F}_{q(x_0)}$ whose Jacobian has CM by K,
- the number of $\mathbb{F}_{q(x_0)}$-rational points on $\mathrm{Jac}(C)$,
- the bit size of the prime-order subgroup of $\mathrm{Jac}(C)$ (i.e., of $r(x_0)/h$), and
- the ρ-value of $\mathrm{Jac}(C)$ with respect to $r(x_0)/h$.

In all cases except the $k = 6$ example, we started with a curve defined over $\mathbb{Q}$ whose Jacobian has CM by K and found the appropriate twist of the curve's reduction modulo $q(x_0)$. Equations for these curves are given by van Wamelen [124]. The remaining case uses a CM field K for which there are no curves over $\mathbb{Q}$ with CM by K. In this case we used the database maintained by David Kohel [69] to compute the absolute Igusa invariants of C, and then constructed C via Mestre's algorithm [88].

We note that some of van Wamelen's curve equations are non-monic and/or of degree 6. Monic, degree-5 models of these curves can easily be obtained by a change of variables; we chose to keep van Wamelen's equations in order to minimize the size of the coefficients.

For completeness, we repeat here the examples that appear in Section 4.5. Note that the values of $\pi(x)$ below may differ from those in the examples of Section 4.5 due to different choices of α_i and β_i in Algorithm 4.4.9. In most cases these will be a permutation of the earlier choices and the $q(x)$ obtained will be the same.

The MAGMA notation `K.1` indicates a root of the polynomial defining the number field K.

```
Embedding degree 5
CM field K = Number Field with defining polynomial x^4 + x^3 + x^2 + x + 1 over
the Rational Field
r(x) = x^4 + x^3 + x^2 + x + 1
pi(x) = 1/5*(-2*zeta_5^2 - zeta_5 - 2)*x^4 + 1/5*(-2*zeta_5^3 - zeta_5^2 -
    2*zeta_5 - 5)*x^3 + 1/5*(-zeta_5^3 - 4*zeta_5^2 - 4*zeta_5 - 6)*x^2 +
    1/5*(-2*zeta_5^3 - zeta_5^2 - 2*zeta_5 - 5)*x + 1/5*(-2*zeta_5^2 - zeta_5 -
    2)
rho-value 4

a = 5  b = 1  h =  5
x0 = 10995116291056
C = Hyperelliptic Curve defined by y^2 = x^5 + 5 over
GF(427197411317015835292256542952348016116227499525880876838258914389443782174\
1235024539485772476069737758 1)
#Jac(C) = 1824976282359596092662078868201538667935951557467364150670631028592 15\
786583932821554695038061279424631206240049911989700333107029550058170604128 4897\
362019684550729676049506454942440045788093700846840308060655
172 bit subgroup
rho = 4.027

*     *     *     *     *     *     *     *     *     *     *     *     *

Embedding degree 6
CM field K = Number Field with defining polynomial x^4 + 12*x^2 + 18 over the
Rational Field
r(x) = x^16 - x^8 + 1
pi(x) = 1/576*(-K.1^2 - 6)*x^30 + 1/96*K.1*x^29 + 1/288*(-2*K.1^2 -
    21)*x^28 + 1/144*(-K.1^3 - 9*K.1)*x^27 + 1/288*(K.1^2 + 6)*x^26 +
    1/288*(-K.1^3 - 9*K.1)*x^25 + 1/96*(K.1^2 + 6)*x^24 + 1/288*(K.1^3 +
    9*K.1)*x^23 + 1/192*(K.1^2 + 6)*x^22 + 1/288*(2*K.1^3 + 15*K.1)*x^21
    + 1/288*(2*K.1^3 + 15*K.1)*x^19 + 1/192*(-K.1^2 - 6)*x^18 +
    1/288*(K.1^3 + 9*K.1)*x^17 + 1/96*(-K.1^2 - 6)*x^16 +
    1/288*(-5*K.1^3 - 57*K.1)*x^15 + 1/192*(-K.1^2 - 6)*x^14 +
    1/288*(-10*K.1^3 - 63*K.1)*x^13 + 1/96*(-2*K.1^3 - 13*K.1)*x^11 +
    1/192*(K.1^2 + 6)*x^10 + 1/96*(K.1^3 + 13*K.1)*x^9 + 1/96*(K.1^2 -
    42)*x^8 + 1/96*(-K.1^3 - 13*K.1)*x^7 + 1/288*(K.1^2 + 6)*x^6 +
    1/48*(K.1^3 + 7*K.1)*x^5 + 1/288*(-2*K.1^2 - 21)*x^4 +
    1/288*(8*K.1^3 + 45*K.1)*x^3 + 1/576*(-K.1^2 - 6)*x^2 + 1/72*(K.1^3
    + 12*K.1)*x + 1
rho-value 15/2
```

```
a = 8  b = 0  h = 1
x0 = 19728
C = Hyperelliptic Curve defined by y^2 = x^5 +
    1044765610978970426841741787779137571274806118741401259517621196950053470 22\
    6890376157569638989576128312522261868300211163233033988496071185386552784 05\
    7240721525332412200324607724240082862641579035697674958761757837267059830 01\
    5720942326026555236316335797 3*x^3 + 24666818822802803889328186987703209200 6\
    8976329534274957124215444789721798578194071461280387958847959212011679325 09\
    6776506961985937652006795754917984624068973413898317873487997799214284371 63\
    5670476101706125922779887699705773430910299688378827593038289892 1*x^2 +
    2564711444580301344744033653685091129605239396257234331977848654006046696 87\
    2436481425954538586921925766627748196030499157630538173581134777079210959 69\
    7960118189105527514362364879834795461999896715342066370332765490512017457 90\
    7248383852440209394972627801 8*x + 747305606561454743203783921227089750555 49\
    9043249253636570227291520186205069968354694972965541722884671057298632328 39\
    7943887031312836094522235707899757049468109223525378198761742537355296744 19\
    1836342733453409624629372551230250952172588868318563614315380 3 over
GF(2750496620499129720252485580903561684169489374849236519442995528958496591300\
1692113042934991731677065609567131389847124725576638776032113179784371373115571\
9997218945562572182640487393890532391901547290863755778060103508644734195363 29\
42051315952537054161)
#Jac(C) = 7565231659377133617241144751387290431203989214706176433643040305802 12\
5674249871678278460099412586036105471111615849908291730698624635883286149262 350\
3504229880398287175019406123330510484765806412871017125490685774246737404684 064\
8923655212225775355386138903636080508237406221645557917136992466421582893883 191\
0611259968114190007806904634847252361780147182309951438188841814605596231171 265\
6769589180406640514598547662799973240478472462918895939601394504360891236694 788\
8389519721703413476765061113255768898325632
229 bit subgroup
rho = 7.376

*     *     *     *     *     *     *     *     *     *     *     *     *

Embedding degree 8
CM field K = Number Field with defining polynomial x^4 + 10*x^2 + 20 over the
Rational Field
r(x) = x^16 - x^12 + x^8 - x^4 + 1
pi(x) = 1/200*(-K.1^3 - K.1^2 - 10*K.1 + 5)*x^30 + 1/400*(-5*K.1^3 -
    6*K.1^2 - 20*K.1 + 10)*x^29 + 1/200*(-9*K.1^3 - 11*K.1^2 - 60*K.1
    - 95)*x^28 + 1/200*(-9*K.1^3 - 7*K.1^2 - 30*K.1 - 25)*x^27 +
    1/100*(2*K.1^3 - 7*K.1^2 + 15*K.1 - 55)*x^26 + 1/200*(-2*K.1^3 +
    17*K.1^2 - 20*K.1 + 75)*x^25 + 1/400*(19*K.1^3 + 46*K.1^2 +
    100*K.1 + 290)*x^24 + 1/200*(16*K.1^3 - 7*K.1^2 + 70*K.1 - 45)*x^23
    + 1/400*(7*K.1^3 + 4*K.1^2 + 40*K.1 + 120)*x^22 + 1/80*(5*K.1^3 -
    6*K.1^2 + 36*K.1 - 6)*x^21 + 1/100*(-3*K.1^3 - 8*K.1^2 - 25*K.1 -
    75)*x^20 + 1/20*(-2*K.1^3 + 2*K.1^2 - 7*K.1 + 12)*x^19 + 1/80*(K.1^3
    - 2*K.1^2 - 30)*x^18 + 1/40*(-K.1^3 + 8*K.1^2 - 10*K.1 + 28)*x^17 +
    1/80*(K.1^3 + 10*K.1^2 + 16*K.1 + 62)*x^16 + 1/40*(3*K.1^3 -
    2*K.1^2 + 10*K.1 - 24)*x^15 + 1/80*(3*K.1^3 + 10*K.1^2 + 24*K.1 +
```

```
    70)*x^14 + 1/40*(3*K.1^3 - 8*K.1^2 + 18*K.1 - 28)*x^13 +
    1/80*(-K.1^3 - 2*K.1^2 - 8*K.1 - 22)*x^12 + 1/20*(-K.1^3 + 2*K.1^2
    - 3*K.1 + 12)*x^11 + 1/400*(-7*K.1^3 - 32*K.1^2 - 60*K.1 - 140)*x^10
    + 1/400*(-15*K.1^3 + 34*K.1^2 - 80*K.1 + 90)*x^9 + 1/400*(7*K.1^3 -
    12*K.1^2 + 80*K.1 - 80)*x^8 + 1/200*(K.1^3 - 7*K.1^2 - 20*K.1 -
    45)*x^7 + 1/400*(3*K.1^3 + 22*K.1^2 + 20*K.1 + 130)*x^6 +
    1/200*(8*K.1^3 - 13*K.1^2 + 50*K.1 - 65)*x^5 + 1/200*(-3*K.1^3 -
    2*K.1^2 - 30*K.1 - 10)*x^4 + 1/200*(-4*K.1^3 - 7*K.1^2 - 20*K.1 -
    25)*x^3 + 1/200*(-4*K.1^3 - 3*K.1^2 - 20*K.1 - 15)*x^2 +
    1/80*(-K.1^3 + 2*K.1^2 - 8*K.1 + 10)*x + 1/400*(3*K.1^3 - 2*K.1^2
    + 20*K.1 + 10)
rho-value 15/2

a = 20  b = 17  h = 1
x0 = 53197
C = Hyperelliptic Curve defined by y^2 = -4*x^5 + 30*x^3 - 45*x + 22 over
    GF(183204227400473854636631436072536959205840312075941767966633188337034061\
09946449593452755107912195460491349615312391361712592227696554747659241442835 16\
60769848218508960135928911793267376005018418288553051700123173025169604569539 47\
90394319799718693840147718859096666852456532617932 71)
#Jac(C) = 335637889374045351052081645066599050488196011356113649757477564960257\
93131598882385623934185589258938297426143110800038441526661720288678637975982 24\
62331327197272866907994352736643829831190151781226115701450012068547925842713 1\
76263960286542626440926678627860910295190332115416362339943079421357046975815 30\
67949242133842558340284982101090727634038991734147992056033816030000620823452763\
68359288248028212188421772531410911100527925554655024075977195793596588102653 52\
00404595728498877808403787380390417915710930675281247464498135652099060840279 24\
0610470086800466779 6
252 bit subgroup
rho = 7.439

*     *     *     *     *     *     *     *     *     *     *     *     *

Embedding degree 10
CM field K = Number Field with defining polynomial x^4 + x^3 + x^2 + x + 1 over
the Rational Field
r(x) = x^4 - x^3 + x^2 - x + 1
pi(x) = 1/25*(2*zeta_5^2 + zeta_5 + 2)*x^6 + 1/25*(2*zeta_5^3 - 9*zeta_5^2 -
    3*zeta_5 - 5)*x^5 + 1/5*(-zeta_5^3 + 2*zeta_5^2 - 2)*x^4 + 1/5*(zeta_5^3 -
    zeta_5^2 + zeta_5 + 5)*x^3 + 1/5*(-2*zeta_5^3 + 3*zeta_5^2 - 2)*x^2 +
    1/25*(-3*zeta_5^2 + zeta_5 + 12)*x + 1/25*(-3*zeta_5^3 + 6*zeta_5^2 +
    2*zeta_5)
rho-value 6

a = 5  b = -1  h =  5
x0 = 10995116288754
C = Hyperelliptic Curve defined by y^2 = x^5 + 2 over
GF(24973988702167203589665436011954256754236654027117675891100744532334294033 52\
14587822425798821832464445139992042000965620720845902590965697576251327730957 01\
)
```

```
#Jac(C) = 623700111695975125922504842885296097742566778967316583412995008821862\
319122032445334898002908383413012552526727147160029812936234959301534761852664 7\
308561356899747148702776090831970493425519397224176542753671207462742993663108 4\
182667387668844270907164563363850638089159444074412136225964523339088088077443 9\
221
172 bit subgroup
rho = 6.000

*     *     *     *     *     *     *     *     *     *     *     *     *

Embedding degree 13
CM field K = Number Field with defining polynomial x^4 + 26*x^2 + 117 over the
Rational Field
r(x) = x^12 + x^11 + x^10 + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x +
    1
pi(x) = 1/4056*(-19*K.1^3 + 183*K.1^2 - 377*K.1 + 2301)*x^20 +
    1/338*(-2*K.1^3 + 7*K.1^2 - 39*K.1 + 78)*x^19 + 1/4056*(23*K.1^3 +
    177*K.1^2 + 481*K.1 + 2535)*x^18 + 1/1352*(7*K.1^3 + 49*K.1^2 +
    65*K.1 + 767)*x^17 + 1/2028*(19*K.1^3 + 141*K.1^2 + 221*K.1 +
    1755)*x^16 + 1/1352*(K.1^3 + 97*K.1^2 - 65*K.1 + 1183)*x^15 +
    1/2028*(31*K.1^3 + 192*K.1^2 + 377*K.1 + 2496)*x^14 +
    1/1352*(13*K.1^3 + 173*K.1^2 + 195*K.1 + 2587)*x^13 + 1/26*(3*K.1^2
    - 2*K.1 + 39)*x^12 + 1/52*(K.1^3 + 8*K.1^2 + 11*K.1 + 104)*x^11 +
    1/312*(5*K.1^3 + 33*K.1^2 + 55*K.1 + 507)*x^10 + 1/78*(2*K.1^3 +
    9*K.1^2 + 28*K.1 + 117)*x^9 + 1/312*(5*K.1^3 + 33*K.1^2 + 55*K.1 +
    507)*x^8 + 1/4056*(97*K.1^3 + 441*K.1^2 + 1235*K.1 + 5811)*x^7 +
    1/338*(2*K.1^3 + 32*K.1^2 + 13*K.1 + 429)*x^6 + 1/2028*(8*K.1^3 +
    165*K.1^2 + 52*K.1 + 2535)*x^5 + 1/1352*(19*K.1^3 + 81*K.1^2 +
    273*K.1 + 923)*x^4 + 1/338*(-K.1^3 + 9*K.1^2 - 26*K.1 + 130)*x^3 +
    1/4056*(23*K.1^3 + 99*K.1^2 + 325*K.1 + 1521)*x^2 + 1/2028*(8*K.1^3
    + 3*K.1^2 + 130*K.1 + 39)*x + 1/338*(-K.1^2 - 13)
rho-value 20/3

a = 13  b = 1  h = 13
x0 = 240254
C = Hyperelliptic Curve defined by y^2 = -11*x^6 - 2*x^5 - x^4 + 4*x^3 + 7*x^2 -
    6*x + 1 over
GF(200279963641204983716498184555510619737021830324502815583346468613663585922 6\
168595996856818699184652243374309856870539091951692210939558534937730150624670 1\
850103759541416747667085567685515616608822513018723014744943)
#Jac(C) = 401120638361223902394555489275643787423393512561030549417337796317288\
875871919664538450695144634617278429677556181873881102089113609698437362866324 8\
199430232645475915633119176055773352243340243869888962789247279923515999897216 0\
658576364963547406247977593016192700456241588701016454613713202149985669375708 1\
434987768824454578329446025231590925195539571520365201627878892954686939657639 5\
212344056138398087335192876468173570406364 64
212 bit subgroup
rho = 6.754

*     *     *     *     *     *     *     *     *     *     *     *     *
```

```
Embedding degree 15
CM field K = Number Field with defining polynomial x^4 + x^3 + x^2 + x + 1 over
the Rational Field
r(x) = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1
pi(x) = 1/25*(zeta_5^3 - zeta_5^2 - zeta_5 + 1)*x^14 + 1/25*(-zeta_5^3 -
    zeta_5^2 + 2)*x^13 + 1/25*(-4*zeta_5^3 + 5*zeta_5^2 + 7*zeta_5 - 3)*x^12 +
    1/25*(4*zeta_5^3 + 4*zeta_5^2 + 5*zeta_5 - 8)*x^11 + 1/25*(6*zeta_5^3 -
    6*zeta_5^2 - 6*zeta_5 + 1)*x^10 + 1/25*(-4*zeta_5^3 + 4*zeta_5^2 + 4*zeta_5
    - 4)*x^9 + 1/25*(-11*zeta_5^3 + 4*zeta_5^2 - 5*zeta_5 - 8)*x^8 +
    1/25*(zeta_5^3 - 5*zeta_5^2 - 3*zeta_5 + 7)*x^7 + 1/25*(4*zeta_5^3 +
    4*zeta_5^2 + 10*zeta_5 - 13)*x^6 + 1/25*(zeta_5^3 + 4*zeta_5^2 - zeta_5 -
    4)*x^5 + 1/25*(6*zeta_5^3 - zeta_5^2 + 4*zeta_5 + 11)*x^4 +
    1/25*(-6*zeta_5^3 - zeta_5^2 - 13)*x^3 + 1/25*(-4*zeta_5^3 - 3*zeta_5 +
    12)*x^2 + 1/25*(4*zeta_5^3 - zeta_5^2 - 3)*x + 1/25*(zeta_5^3 - zeta_5^2 -
    zeta_5 + 1)
rho-value 7

a = 5  b = -1  h =  1
x0 = 10486759
C = Hyperelliptic Curve defined by y^2 = x^5 + 1 over
GF(3027234587378952134543882421765560418784985527734675952435585748958972474354\
247327014206633534366996468338898310245427923624264269501199458903628265938998\
3068954820877181053781299029288485982281)
#Jac(C) = 9164149247023414586161041393135416975410327837220296460255873783012\
569831979274921598247094934151697766822759123326689273868196995452949118550868\
049182399693898026022432603112194235640207527652977099752131402805539189123756\
160926526375943480456507777622886949497024937943256657261166782646822256065286\
411125946937083242821653565760490770079444599917989654513719666744905021787531\
6880
188 bit subgroup
rho = 6.925

*     *     *     *     *     *     *     *     *     *     *     *     *

Embedding degree 16
CM field K = Number Field with defining polynomial x^4 + 4*x^2 + 2 over the
Rational Field
r(x) = x^8 + 1
pi(x) = 1/64*(-K.1^2 - 2)*x^14 + 1/32*(-K.1^2 + 3*K.1 - 2)*x^13 +
    1/64*(K.1^2 + 4*K.1 - 16)*x^12 + 1/16*(2*K.1^3 + K.1^2 + 6*K.1 +
    5)*x^11 + 1/64*(8*K.1^3 + K.1^2 + 28*K.1)*x^10 + 1/32*(-4*K.1^3 - K.1^2
    - 7*K.1 - 2)*x^9 + 1/64*(-8*K.1^3 - K.1^2 - 16*K.1 - 34)*x^8 +
    1/8*(K.1^3 + 2*K.1 + 4)*x^7 + 1/64*(8*K.1^3 - K.1^2 + 16*K.1 - 2)*x^6 +
    1/32*(-4*K.1^3 - K.1^2 - 13*K.1 - 2)*x^5 + 1/64*(-8*K.1^3 + K.1^2 -
    28*K.1 - 16)*x^4 + 1/16*(K.1^2 - 2*K.1 + 5)*x^3 + 1/64*(K.1^2 -
    4*K.1)*x^2 + 1/32*(-K.1^2 + K.1 - 2)*x + 1/64*(-K.1^2 - 2)
rho-value 7

a = 4  b = 3  h = 2
```

```
x0 = 8392747
C = Hyperelliptic Curve defined by y^2 = -x^5 + 3*x^4 + 2*x^3 - 6*x^2 - 3*x + 1
    over
GF(36139815896240802935471276299138341156883199970952529477810273985901656442911\
23886428742211687851041922556081291748931106065270028399425949307651045416589931\
29850257819539624614124167109857632 1)
#Jac(C) = 13060862930141794303263545729477473293464760026445009973953969298143 3\
20028551936321911438867845916215943153525185119748172811760525636611959068349321\
04634474940223871610450373385082951139169556395536081619028323629720587882739891\
37865563410855513110555380064745564464525096560795660042408820489333763257782341\
46430836146192911718624943944342164283090368645559860772407172521164548423 68
184 bit subgroup
rho = 6.918

*     *     *     *     *     *     *     *     *     *     *     *     *

Embedding degree 20
CM field K = Number Field with defining polynomial x^4 + x^3 + x^2 + x + 1 over
the Rational Field
r(x) = x^8 - x^6 + x^4 - x^2 + 1
pi(x) = 1/25*(2*zeta_5^3 + 2*zeta_5^2 + 1)*x^12 + 1/25*(-2*zeta_5^3 - 9*zeta_5^2
    - zeta_5 - 3)*x^11 + 1/25*(-5*zeta_5^3 + 3*zeta_5^2 - zeta_5 - 2)*x^10 +
    1/5*(zeta_5 + 1)*x^9 + 1/5*(zeta_5^3 + zeta_5^2 - zeta_5 - 1)*x^8 +
    1/5*(-zeta_5^2 - zeta_5)*x^7 + 1/5*(zeta_5^2 + zeta_5 + 3)*x^6 +
    1/5*(zeta_5^3 + 2*zeta_5^2 + 3*zeta_5 + 1)*x^5 + 1/5*(2*zeta_5^3 + zeta_5^2
    + 2*zeta_5)*x^4 + 1/5*(zeta_5^3 + 2)*x^3 + 1/25*(-3*zeta_5^3 + 2*zeta_5^2 +
    6)*x^2 + 1/25*(-2*zeta_5^3 + zeta_5^2 - zeta_5 - 3)*x + 1/25*(-2*zeta_5^2 -
    zeta_5 - 2)
rho-value 6

a = 5  b = 2  h = 5
x0 = 10490607
C = Hyperelliptic Curve defined by y^2 = x^5 + 10 over
GF(25252513164005421832503256050659486488764524266558504384377747585073222078 01\
01805172267927279158777943363123016480543140858274493034125643384409883028989 60\
757875722701)
#Jac(C) = 63768942109826712068932298238055036024178515937735423979273091069324 5\
94101403502138543371056982410100038999209511393407422503662341908083591515564 93\
31328205892183335539857190709802387126545382403014847115884192893468379098218 41\
55014989214132036287117677489909438443736257360658431791142299090588046243216 99\
10494875504663931575403958 1
185 bit subgroup
rho = 6.000

*     *     *     *     *     *     *     *     *     *     *     *     *

Embedding degree 30
CM field K = Number Field with defining polynomial x^4 + x^3 + x^2 + x + 1 over
the Rational Field
r(x) = x^16 + x^14 - x^10 - x^8 - x^6 + x^2 + 1
```

```
pi(x) = 1/25*(-4*zeta_5^3 - 6*zeta_5^2 - 6*zeta_5 - 9)*x^28 + 1/25*(-8*zeta_5^3
    - 4*zeta_5^2 - 8*zeta_5 - 5)*x^26 + 1/5*(zeta_5^3 + 2*zeta_5^2 + zeta_5 +
    2)*x^24 + 1/25*(13*zeta_5^3 + 13*zeta_5^2 + 10*zeta_5 + 9)*x^22 +
    1/25*(-zeta_5^3 - 5*zeta_5^2 - 7*zeta_5 - 12)*x^20 + 1/25*(-11*zeta_5^3 -
    4*zeta_5^2 - 9*zeta_5 - 1)*x^18 + 1/25*(-2*zeta_5^3 - zeta_5^2 -
    2*zeta_5)*x^16 + 1/5*(-2*zeta_5^3 - 3*zeta_5^2 - 3*zeta_5 - 4)*x^14 +
    1/25*(2*zeta_5^3 + 2*zeta_5^2 + 1)*x^12 + 1/25*(11*zeta_5^3 + 15*zeta_5^2 +
    12*zeta_5 + 17)*x^10 + 1/25*(zeta_5^3 + 4*zeta_5^2 - zeta_5 + 1)*x^8 +
    1/25*(-8*zeta_5^3 - 9*zeta_5^2 - 13*zeta_5 - 15)*x^6 + 1/5*(zeta_5^3 +
    2*zeta_5^2 + zeta_5 + 2)*x^4 + 1/25*(-7*zeta_5^3 - 7*zeta_5^2 - 10*zeta_5 -
    11)*x^2 + 1/25*(-zeta_5^3 - 2*zeta_5 - 2)
rho-value 7

a = 5  b = 2  h = 1
x0 = 56837
C = Hyperelliptic Curve defined by y^2 = x^5 + 34 over
GF(159892056261540529025757899908608320395832846134131457083124104933722259123\0\
65227239127495294969205837926954090700250116412122825786616123350067217448181\79\
68840307770956913665409130321019836561143668868497574503547786068982089954710\85\
87653569060420961792532978607961)
#Jac(C) = 25565469655543641894915663472332503430309308149392969361785729399894\7\
74101064660027228123773363800429587939714603755373292626688511949035186098419\89\
60836660194280056804046838972626664851954997538850695574002268764012411061198\93\
92890124785476897780455693359852601950453753117472448030366229315956617681649\90\
90308256659567695456231193427519686346476652018019542118120374759228023535447\30\
19835750724015869031593872765772832057576681798154163441418325206728244614586\74\
39023741231081143932312317434049507400132420567235289847649865270 51
254 bit subgroup
rho = 6.972

*     *     *     *     *     *     *     *     *     *     *     *     *

Embedding degree 32
CM field K = Number Field with defining polynomial x^4 + 4*x^2 + 2 over the
Rational Field
r(x) = x^16 + 1
pi(x) = 1/64*(-K.1^2 - 4*K.1 - 10)*x^26 + 1/32*(-K.1^2 - 2*K.1 - 2)*x^25 +
    1/64*(-K.1^2 - 2*K.1 - 10)*x^24 + 1/8*x^23 + 1/32*(-4*K.1^3 + K.1^2 -
    13*K.1 + 1)*x^22 + 1/16*(-2*K.1^3 + K.1^2 - 7*K.1 + 3)*x^21 +
    1/32*(K.1^2 + K.1 + 1)*x^20 + 1/64*(8*K.1^3 - K.1^2 + 14*K.1 - 2)*x^18
    + 1/32*(4*K.1^3 - K.1^2 + 8*K.1 - 2)*x^17 + 1/64*(-K.1^2 - 34)*x^16 +
    1/2*x^15 + 1/8*(-K.1^3 - 2*K.1)*x^14 + 1/8*(-K.1^3 - 2*K.1)*x^13 +
    1/64*(8*K.1^3 - K.1^2 + 28*K.1 - 10)*x^10 + 1/32*(4*K.1^3 - K.1^2 +
    14*K.1 - 2)*x^9 + 1/64*(-K.1^2 - 2*K.1 - 10)*x^8 + 1/8*x^7 + 1/32*(K.1^2
    + 3*K.1 + 1)*x^6 + 1/16*(K.1^2 + K.1 + 3)*x^5 + 1/32*(K.1^2 + K.1 +
    1)*x^4 + 1/64*(-K.1^2 - 2*K.1 - 2)*x^2 + 1/32*(-K.1^2 - 2)*x +
    1/64*(-K.1^2 - 2)
rho-value 13/2

a = 4  b = 3  h = 2
```

```
x0 = 31403
C = Hyperelliptic Curve defined by y^2 = -x^5 + 3*x^4 + 2*x^3 - 6*x^2 - 3*x + 1
    over GF(166485159776374378580956718564217090839469176563770859164433057488 9\
42300401707613463428047773270197776275031785252729123008896286870431733757041 86\
93158083854285796033171486654911277540957755714854534442593152549002844626620 17\
92234849)
#Jac(C) = 27717308425764905325910723041530574535793841431464632850406726631085 5\
13393780740891198991685166375774518261786998561399022944018999527347162913838 07\
17106173017093291786888410855801906030546486712191750847249911720358933843102 97\
45022840892132502173413467449898105670632683775900761110569031974027201023732 72\
00391999807795046057737733226134517179203118234738930876860722256266369798073 73\
92527515578101564560305909684442605128724602548236038772873319893363278158954 49\
6
239 bit subgroup
rho = 6.482

*     *     *     *     *     *     *     *     *     *     *     *     *

Embedding degree 40
CM field K = Number Field with defining polynomial x^4 + x^3 + x^2 + x + 1 over
the Rational Field
r(x) = x^16 - x^12 + x^8 - x^4 + 1
pi(x) = 1/25*(-2*zeta_5^2 - zeta_5 - 2)*x^26 + 1/25*(10*zeta_5^3 - zeta_5^2 +
    2*zeta_5 - 1)*x^25 + 1/25*(15*zeta_5^3 + 3*zeta_5^2 - zeta_5 + 3)*x^24 +
    1/25*(3*zeta_5^3 + 4*zeta_5^2 + 3*zeta_5 + 5)*x^22 + 1/25*(-zeta_5^3 +
    2*zeta_5^2 - 6*zeta_5)*x^21 + 1/25*(-2*zeta_5^3 - 6*zeta_5^2 + 3*zeta_5 -
    5)*x^20 + 1/5*(-zeta_5^3 - zeta_5^2 - zeta_5 - 1)*x^18 + 1/5*(zeta_5^3 +
    zeta_5 + 1)*x^17 + 1/5*zeta_5^2*x^16 + 1/5*(zeta_5^3 + zeta_5^2 + zeta_5 +
    1)*x^14 + 1/5*(-2*zeta_5^3 - 2*zeta_5^2 - 3*zeta_5 - 1)*x^13 + 1/5*(zeta_5^3
    + zeta_5^2 + 2*zeta_5)*x^12 + 1/5*(-zeta_5^3 - zeta_5^2 - zeta_5 - 1)*x^10 +
    1/5*(2*zeta_5^3 + 2*zeta_5^2 + 2*zeta_5 + 2)*x^9 + 1/5*(-zeta_5^3 - zeta_5^2
    - zeta_5 - 1)*x^8 + 1/25*(5*zeta_5^3 + 3*zeta_5^2 + 4*zeta_5 + 3)*x^6 +
    1/25*(-10*zeta_5^3 - 6*zeta_5^2 - 8*zeta_5 - 6)*x^5 + 1/25*(5*zeta_5^3 +
    3*zeta_5^2 + 4*zeta_5 + 3)*x^4 + 1/25*(-2*zeta_5^3 - zeta_5^2 -
    2*zeta_5)*x^2 + 1/25*(4*zeta_5^3 + 2*zeta_5^2 + 4*zeta_5)*x +
    1/25*(-2*zeta_5^3 - zeta_5^2 - 2*zeta_5)
rho-value 13/2

a = 5  b = 1  h = 1
x0 = 16041
C = Hyperelliptic Curve defined by y^2 = x^5 + 2 over
GF(37608608349403431693648579357799717721246918009894942422472869411505743521 89\
48818826367825585113806821703673588828976040144105924966004529002814053035446 54\
72887517962485279348704094722957573064729660661552378055407081)
#Jac(C) = 14144074219788175149251691009469112055084048316486801790733983093742 0\
98729096743878163103974356809161375830364712088318430089411375804946451931303 77\
97337627372690369570454058657121103880434233807966017143637991825626096840671 28\
35224856043461797085119925889394425684860558655275853974590638839738809668681 05\
47084511113092301092069092142480931264430385486562084565028121902901964573288 51\
36936830185002728751058321698693418971651601738 05
```

```
225 bit subgroup
rho = 6.438

*     *     *     *     *     *     *     *     *     *     *     *     *

Embedding degree 60
CM field K = Number Field with defining polynomial x^4 + x^3 + x^2 + x + 1 over
the Rational Field
r(x) = x^16 + x^14 - x^10 - x^8 - x^6 + x^2 + 1
pi(x) = 1/25*(2*zeta_5^3 + zeta_5^2 + 2*zeta_5)*x^28 + 1/25*(2*zeta_5^2 +
    6*zeta_5 + 2)*x^27 + 1/25*(-8*zeta_5^3 - 7*zeta_5^2 + 3*zeta_5 - 3)*x^26 +
    1/25*(-11*zeta_5^3 - 10*zeta_5^2 - 2*zeta_5 - 7)*x^25 + 1/25*(-8*zeta_5^3 -
    2*zeta_5^2 - 2*zeta_5 - 3)*x^24 + 1/25*(-zeta_5^3 + zeta_5^2 + zeta_5 -
    1)*x^23 + 1/25*(10*zeta_5^3 + 8*zeta_5^2 + 9*zeta_5 + 8)*x^22 +
    1/25*(4*zeta_5^3 + 2*zeta_5^2 + 4*zeta_5)*x^21 + 1/25*(6*zeta_5^3 +
    5*zeta_5^2 + 2*zeta_5 + 2)*x^20 + 1/5*(zeta_5^3 + zeta_5^2)*x^19 +
    1/25*(-7*zeta_5^3 - zeta_5^2 - 2*zeta_5)*x^18 + 1/25*(-7*zeta_5^2 - 6*zeta_5
    - 2)*x^17 + 1/25*(3*zeta_5^3 + 7*zeta_5^2 - 8*zeta_5 - 2)*x^16 +
    1/25*(zeta_5^3 + 5*zeta_5^2 + 2*zeta_5 + 7)*x^15 + 1/25*(-2*zeta_5^3 -
    8*zeta_5^2 - 3*zeta_5 - 7)*x^14 + 1/25*(-4*zeta_5^3 - 11*zeta_5^2 + 4*zeta_5
    + 1)*x^13 + 1/25*(-5*zeta_5^3 + 2*zeta_5^2 + zeta_5 - 3)*x^12 +
    1/25*(zeta_5^3 - 2*zeta_5^2 - 4*zeta_5)*x^11 + 1/25*(-zeta_5^3 + 3*zeta_5 -
    2)*x^10 + 1/5*x^9 + 1/25*(7*zeta_5^3 + 6*zeta_5^2 + 2*zeta_5 + 5)*x^8 +
    1/25*(2*zeta_5^2 + zeta_5 - 3)*x^7 + 1/25*(-3*zeta_5^3 - 2*zeta_5^2 -
    2*zeta_5 + 2)*x^6 + 1/25*(4*zeta_5^3 + 3*zeta_5 - 2)*x^5 + 1/25*(2*zeta_5^3
    + 3*zeta_5^2 - 2*zeta_5 + 2)*x^4 + 1/25*(-zeta_5^3 + zeta_5^2 - 4*zeta_5 -
    1)*x^3 + 1/25*(-2*zeta_5^2 - zeta_5 - 2)*x^2 + 1/25*(-zeta_5^3 - 3*zeta_5^2
    - zeta_5)*x + 1/25*(zeta_5^3 + 2*zeta_5 + 2)
rho-value 7

a = 5  b = -1  h = 1
x0 = 26384
C = Hyperelliptic Curve defined by y^2 = x^5 + 19 over
GF(3149188484721621964796486022253819821139243385693502691124803449486277615940\
854766586620610645764879775531405853329419118154924655995390751840535919069074 1\
822500099602758784616277168344884395729671215195304689309797914708606737959964 6\
879100194341)
#Jac(C) = 991738811230326541919783262997413512347437837670926947929510933411367\
127984463935896556963420430822351074543204777123766482700593016433378031122538 2\
170939819857952878885594266347329364628813613064662949046745013825342799159631 9\
427388812907148201938241708539959820622539052079618548171067122543162412520976 3\
707808202417915911136011673816726191956111188525691515301732112757885424432538 1\
334929777903836473342445434758889592740923281502545509815021457977303684717766 7\
277282977807292132420696955
236 bit subgroup
rho = 6.941
```

A.3 Families of three-dimensional pairing-friendly abelian varieties

Below we give data for two families of 3-dimensional abelian varieties with CM by $\mathbb{Q}(\zeta_9)$ and ρ-values of 15. The output of Algorithms 4.4.9 and 2.2.4 are given in the same format as in Appendix A.2; see page 142 for details.

By [70, Lemma 1], if q is prime to 6 an abelian variety over $\mathbb{F}_q$ with CM by $K = \mathbb{Q}(\zeta_9)$ is isomorphic over $\overline{\mathbb{F}}_q$ to the Jacobian of the curve $y^3 = x^4 + x$. By Proposition 1.2.5, given a q-Weil number $\pi \in \mathbb{Z}[\zeta_9]$, there is a curve $C/\mathbb{F}_q$ of the form $y^3 = x^4 + ax$ such that either π or $-\pi$ is the Frobenius element of $\mathrm{Jac}(C)$. Since $[(0,0) - (\infty)]$ is a point of order 3 in $\mathrm{Jac}(C)$, we can easily determine which case occurs in the examples below by checking the values mod 3 of $n_\pm = N_{K/\mathbb{Q}}(\pm\pi - 1)$. In the first example ($k = 9$) we find that $n_+ \equiv 0 \pmod 3$ and $n_- \equiv 1 \pmod 3$ so the Frobenius element is π; in the second example ($k = 18$) we find that $n_+ \equiv 1 \pmod 3$ and $n_- \equiv 0 \pmod 3$ so the Frobenius element is $-\pi$. We can then determine which twist of $y^3 = x^4 + x$ over $\mathbb{F}_q$ has $\#\,\mathrm{Jac}(C) = n_+$ or n_-, respectively.

```
Embedding degree 9
CM field K = Cyclotomic Field of order 9 and degree 6
r(x) = x^6 + x^3 + 1
pi(x) = 1/81*(zeta_9^5 - 2*zeta_9^4 - 2*zeta_9^3 - zeta_9^2 - 4)*x^15 +
    1/81*(-3*zeta_9^5 + zeta_9^4 - zeta_9 - 3)*x^14 + 1/81*(-6*zeta_9^5 +
    zeta_9^4 - 3*zeta_9^3 - 3*zeta_9^2 - zeta_9 - 3)*x^13 + 1/81*(2*zeta_9^5 -
    9*zeta_9^4 - 10*zeta_9^3 - 5*zeta_9^2 - 5*zeta_9 - 14)*x^12 +
    1/81*(-15*zeta_9^5 + 5*zeta_9^4 - 3*zeta_9^3 - 8*zeta_9 - 18)*x^11 +
    1/81*(-12*zeta_9^5 + 2*zeta_9^4 - 15*zeta_9^3 - 12*zeta_9^2 - 5*zeta_9 -
    33)*x^10 + 1/81*(-27*zeta_9^5 - 10*zeta_9^4 - 18*zeta_9^3 - 9*zeta_9^2 -
    28*zeta_9 - 18)*x^9 + 1/9*(-2*zeta_9^5 + zeta_9^4 - 3*zeta_9^3 - 2*zeta_9^2
    - 3*zeta_9 - 4)*x^8 + 1/9*(-3*zeta_9^5 - 2*zeta_9^3 - zeta_9^2 - 3*zeta_9 -
    5)*x^7 + 1/81*(-28*zeta_9^5 - 7*zeta_9^4 - 16*zeta_9^3 - 8*zeta_9^2 -
    27*zeta_9 - 41)*x^6 + 1/81*(-15*zeta_9^5 + 8*zeta_9^4 - 27*zeta_9^3 -
    18*zeta_9^2 - 26*zeta_9 - 33)*x^5 + 1/81*(-21*zeta_9^5 - zeta_9^4 -
    15*zeta_9^3 - 6*zeta_9^2 - 26*zeta_9 - 15)*x^4 + 1/81*(-2*zeta_9^5 -
    8*zeta_9^3 - 4*zeta_9^2 + 5*zeta_9 - 31)*x^3 + 1/81*(-3*zeta_9^5 +
    4*zeta_9^4 + 3*zeta_9^3 + 9*zeta_9^2 + 8*zeta_9 - 18)*x^2 +
    1/81*(12*zeta_9^5 - 2*zeta_9^4 - 3*zeta_9^3 + 3*zeta_9^2 + 5*zeta_9 - 12)*x
    + 1/81*(zeta_9^4 + zeta_9)
rho-value 15

a = 3  b = 1  h = 3
x0 = 6442469677
C = Curve over GF(5411965965472066839922072740950229859614601820299652310481643\
98075931183623872874222094596163802872952918577498305633427808578465571252794857\
66365226820099380328188642823461424903721573345767124939978774377704556843811257
```

```
186752802858156723736945393831722318228774218485623779491127187833459795 9)
defined by y^3 = x^4 + 2*x
#Jac(C) = 158513103958975947104509214404450115776805031373143139657494070947164\
435887926033170449453005950863129023215881820612901067390810176256116330815048 1\
717252529355546349292836424310703437373419005713209766143558318929340535792252 5\
323526381960959205504697590623964470828442476242956502886082875108718547327961 0\
018961242433303787286543326186216373667389175717553083151048827714262228741188 6\
070664717483957970456263773238781087523244057971781160107960538228330866754708 3\
526819604821038042421521466880905961424944162219796652961893437303530334597236 4\
382304729345968446312110615194094366123829403771083199787798454975010177883508 6\
689660478179843599547247342614759433072306187578169955336989160973457039320828 9\
632547727244742939525681762706589474305007863158446640624090158534330858510822 1\
567745195318097757595118957021447889346026185075543906725128674596472435912519 0\
17131238207054459
195 bit subgroup
rho = 14.99

*     *     *     *     *     *     *     *     *     *     *     *     *

Embedding degree 18
CM field K = Cyclotomic Field of order 9 and degree 6
r(x) = x^6 - x^3 + 1
pi(x) = 1/243*(4*zeta_9^5 + 3*zeta_9^4 + 6*zeta_9^3 + 2*zeta_9^2 + 6)*x^15 +
    1/81*(3*zeta_9^5 + 2*zeta_9^4 + 6*zeta_9^3 + zeta_9^2 + 5)*x^14 +
    1/81*(-7*zeta_9^5 - 7*zeta_9^4 - 6*zeta_9^2 + 8*zeta_9 - 2)*x^13 +
    1/243*(-28*zeta_9^5 + 9*zeta_9^4 + 9*zeta_9^3 - 5*zeta_9^2 + 18*zeta_9 +
    18)*x^12 + 1/81*(2*zeta_9^5 + 8*zeta_9^4 - 8*zeta_9^3 - 4*zeta_9^2 -
    3*zeta_9 + 10)*x^11 + 1/81*(-35*zeta_9^4 - 3*zeta_9^3 - 19*zeta_9^2 +
    4)*x^10 + 1/243*(31*zeta_9^5 + 57*zeta_9^4 + 36*zeta_9^3 - 61*zeta_9^2 -
    24*zeta_9 + 33)*x^9 + 1/27*(-8*zeta_9^5 + 2*zeta_9^4 + 8*zeta_9^3 -
    6*zeta_9^2 + 2*zeta_9 - 1)*x^8 + 1/27*(-2*zeta_9^5 + zeta_9^4 + zeta_9^3 +
    zeta_9^2 - 2*zeta_9 - 2)*x^7 + 1/243*(58*zeta_9^5 - 87*zeta_9^4 -
    57*zeta_9^3 + 65*zeta_9^2 - 36*zeta_9 - 3)*x^6 + 1/81*(5*zeta_9^4 -
    9*zeta_9^3 + 19*zeta_9^2 + 12*zeta_9 - 1)*x^5 + 1/81*(8*zeta_9^5 +
    17*zeta_9^4 - 3*zeta_9^3 + 9*zeta_9^2 + 14*zeta_9 + 4)*x^4 +
    1/243*(-zeta_9^5 + 45*zeta_9^4 + 18*zeta_9^3 + 13*zeta_9^2 + 27*zeta_9)*x^3
    + 1/81*(5*zeta_9^5 - 4*zeta_9^4 - 2*zeta_9^3 + 5*zeta_9^2 - 6*zeta_9 -
    2)*x^2 + 1/81*(3*zeta_9^5 - 5*zeta_9^4 + 2*zeta_9^2 - 6*zeta_9 - 2)*x +
    1/243*(4*zeta_9^5 - 6*zeta_9^4 + 2*zeta_9^2 - 6*zeta_9 - 3)
rho-value 15

a = 3  b = 2  h = 3
x0 = 6442452833
C = Curve over GF(1803847164672279252116736628206644909012632819172715343440478\
962968051683350756979430471940046168260994531111771152933749675534207931201119 1\
297795465895087297436158217662347772784528705847684896815303799627173910882232 3\
924536529052617687336188706769071851214910336212993407870581353000835858 9)
defined by y^3 = x^4 + x
#twist(Jac(C)) =
          5869474421205676644807655917689317933426911726337030925106248226144 03\
```

```
455537541949749102152235341553767902937593982170974007780701342035808122176645 4\
556583711863580746184349733941935802869871947793010696211669961554858123345443 0\
801917635288415952994005929450956976808987102977685032868502833002752580746330 9\
060797913913425676924681044681989295008206427682097203020540739213420465208350 3\
076288747701005676232837810595844781674455169684642759182896701464359573649143 9\
340506358479049410313178232403759263374241805864476269119481205869481368775479 8\
179384379074607696550668275668797038077689258081622528493977502171442329923227 2\
439407940215512381687516638639156696847834153536165054755482393988988351467523 9\
211939860994112679168447534112482812962389971398154555748065241249340274049899 3\
469684251897011544152121752458904507464966603881145623529447115223881376540693 5\
140676645411723
195 bit subgroup
rho = 14.97
```

Bibliography

[1] L. Adleman, J. DeMarrais, and M.-D. Huang. "A subexponential algorithm for discrete logarithms over the rational subgroup of the Jacobians of large genus hyperelliptic curves over finite fields." In *Algorithmic Number Theory — ANTS-I*, Springer LNCS **877** (1994), 28–40.

[2] A. Agashe, K. Lauter, and R. Venkatesan. "Constructing elliptic curves with a known number of points over a prime field." In *High Primes and Misdemeanours: Lectures in Honour of the 60th Birthday of Hugh Cowie Williams*, Fields Institute Communincations **41**. American Mathematical Society, Providence, RI (2004), 1–17.

[3] A. Atkin and F. Morain. "Elliptic curves and primality proving." *Mathematics of Computation* **61** (1993), 29–68.

[4] D. Bailey and C. Paar. "Efficient arithmetic in finite field extensions with application in elliptic curve cryptography." *Journal of Cryptology* **14** (2001), 153–176.

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

[6] E. Barker, W. Barker, W. Burr, W. Polk, and M. Smid. "Recommendation for key management — Part 1: General (revised)." National Institute of Standards and Technology (2006). Available at http://csrc.nist.gov/publications/nistpubs/800-57/SP800-57-Part1.pdf.

[7] P. Barreto, S. Galbraith, C. Ó'hÉigeartaigh, and M. Scott. "Efficient pairing computation on supersingular abelian varieties." *Designs, Codes and Cryptography* **42** (2007), 239–271.

[8] P. Barreto, B. Lynn, and M. Scott. "Constructing elliptic curves with prescribed embedding degrees." In *Security in Communication Networks — SCN 2002*, Springer LNCS **2576** (2002), 263–273.

[9] P. Barreto and M. Naehrig. "Pairing-friendly elliptic curves of prime order." In *Selected Areas in Cryptography — SAC 2005*, Springer LNCS **3897** (2006), 319–331.

[10] P. Bateman and R. Horn. "A heuristic asymptotic formula concerning the distribution of prime numbers." *Mathematics of Computation* **16** (1962), 363–367.

[11] D. Bernstein. "Elliptic vs. hyperelliptic, part 1." Talk at ECC 2006, Toronto, Canada (20 September 2006). Available at http://cr.yp.to/talks/2006.09.20/slides.pdf.

[12] D. Bernstein and J. Sorenson. "Modular exponentiation via the explicit Chinese remainder theorem." *Mathematics of Computation* **76** (2007), 443–454.

[13] I. Blake, G. Seroussi, and N. Smart. *Elliptic Curves in Cryptography*, London Mathematical Society Lecture Note Series **265**. Cambridge University Press, Cambridge (2000).

[14] D. Boneh and M. Franklin. "Identity-based encryption from the Weil pairing." In *Advances in Cryptology — CRYPTO 2001*, Springer LNCS **2139** (2001), 213–229. Full version: *SIAM Journal on Computing* **32** (2003), 586–615.

[15] D. Boneh, C. Gentry, and B. Waters. "Collusion resistant broadcast encryption with short ciphertexts and private keys." In *Advances in Cryptology — CRYPTO 2005*, Springer LNCS **3621** (2005), 258–275.

[16] D. Boneh, E.-J. Goh, and K. Nissim. "Evaluating 2-DNF formulas on ciphertexts." In *Theory of Cryptography — TCC 2005*, Springer LNCS **3378** (2005), 325–341.

[17] D. Boneh, B. Lynn, and H. Shacham. "Short signatures from the Weil pairing." In *Advances in Cryptology — ASIACRYPT 2001*, Springer LNCS **2248** (2001), 514–532. Full version: *Journal of Cryptology* **17** (2004), 297–319.

[18] W. Bosma, J. Cannon, and C. Playoust. "The Magma algebra system. I. The user language." *Journal of Symbolic Computation* **24** (1997), 235–265. See also [82].

[19] F. Brezing and A. Weng. "Elliptic curves suitable for pairing based cryptography." *Designs, Codes and Cryptography* **37** (2005), 133–141.

[20] R. Bröker. "A p-adic algorithm to compute the Hilbert class polynomial." To appear in *Mathematics of Computation*. Available at http://research.microsoft.com/~reinierb/padicj.pdf.

[21] R. Bröker. *Constructing elliptic curves of prescribed order*. Ph.D. dissertation, Universiteit Leiden (2006). Available at http://math.leidenuniv.nl/~reinier/thesis.pdf.

[22] G. Cardona and J. Quer. "Field of moduli and field of definition for curves of genus 2." In *Computational Aspects of Algebraic Curves*, Lecture Notes Ser. Comput. **13**. World Scientific, Hackensack, NJ (2005), 71–83.

[23] J. Chao, O. Nakamura, K. Sobataka, and S. Tsujii. "Construction of secure elliptic cryptosystems using CM tests and liftings." In *Advances in Cryptology — ASIACRYPT 1998*, Springer LNCS **1514** (1998), 95–109.

[24] L. Chen, Z. Cheng, and N. Smart. "Identity-based key agreement protocols from pairings." *International Journal of Information Security* **6** (2007), 213–241.

[25] C. Cocks and R. Pinch. "Identity-based cryptosystems based on the Weil pairing." Unpublished manuscript (2001). While this manuscript is generally unavailable, the main result appears as Theorem 2.3.1 above.

[26] H. Cohen. *A Course in Computational Algebraic Number Theory*, Graduate Texts in Mathematics **138**. Springer-Verlag, Berlin (1993).

[27] H. Cohn and K. Lauter. "Generating genus 2 curves with complex multiplication." Technical report, Microsoft Research (2001).

[28] J.-M. Couveignes. "Linearizing torsion classes in the Picard group of algebraic curves over finite fields." Preprint (2007). Available at http://arxiv.org/abs/0706.0272.

[29] J.-M. Couveignes and T. Henocq. "Action of modular correspondences around CM points." In *Algorithmic Number Theory — ANTS-V*, Springer LNCS **2369** (2002), 234–243.

[30] "Digital signature standard (DSS)." Federal Information Processing Standards Publication 186-3 (Draft) (2006). Available at http://csrc.nist.gov/publications/drafts/fips_186-3/Draft-FIPS-186-3%20_March2006.pdf.

[31] P. Duan, S. Cui, and C.-W. Chan. "Effective polynomial families for generating more pairing-friendly elliptic curves." Cryptology ePrint Archive, Report 2005/236 (2005). Available at http://eprint.iacr.org/2005/236.

[32] R. Dupont, A. Enge, and F. Morain. "Building curves with arbitrary small MOV degree over finite prime fields." *Journal of Cryptology* **18** (2005), 79–89.

[33] S. Duquesne and G. Frey. "Background on pairings." In *Handbook of Elliptic and Hyperelliptic Curve Cryptography*. Chapman & Hall/CRC, Boca Raton, FL (2006), 115–124.

[34] K. Eisenträger and K. Lauter. "A CRT algorithm for constructing genus 2 curves over finite fields." To appear in *Algebraic Geometry and Coding Theory 2007*. Available at http://arxiv.org/abs/math.NT/0405305.

[35] A. Enge. "The complexity of class polynomial computation via floating point approximations." To appear in *Mathematics of Computation*. Available at http://fr.arxiv.org/abs/cs.CC/0601104.

[36] D. Freeman. "Constructing families of pairing-friendly elliptic curves." Technical Report HPL-2005-155, Hewlett-Packard Labs (2005). Available at http://www.hpl.hp.com/techreports/2005/HPL-2005-155.html.

[37] D. Freeman. "Constructing pairing-friendly elliptic curves with embedding degree 10." In *Algorithmic Number Theory — ANTS-VII*, Springer LNCS **4076** (2006), 452–465.

[38] D. Freeman. "Constructing pairing-friendly genus 2 curves with ordinary Jacobians." In *Pairing-Based Cryptography — Pairing 2007*, Springer LNCS **4575** (2007), 152–176.

[39] D. Freeman. "A generalized Brezing-Weng algorithm for constructing pairing-friendly ordinary abelian varieties." Cryptology ePrint Archive, Report 2008/155 (2008). Available at http://eprint.iacr.org/2008/155.

[40] D. Freeman and K. Lauter. "Computing endomorphism rings of Jacobians of genus 2 curves over finite fields." In *Algebraic Geometry and its Applications*, ed. J. Chaumine, J. Hirschfeld, and R. Rolland, Number Theory and Its Applications **5**. World Scientific (2008), 29–66.

[41] D. Freeman, M. Scott, and E. Teske. "A taxonomy of pairing-friendly elliptic curves." Cryptology ePrint Archive, Report 2006/372 (2006). Available at http://eprint.iacr.org/2006/372.

[42] D. Freeman, P. Stevenhagen, and M. Streng. "Abelian varieties with prescribed embedding degree." In *Algorithmic Number Theory — ANTS-VIII*, Springer LNCS **5011** (2008), 60–73.

[43] G. Frey and H.-G. Rück. "A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves." *Mathematics of Computation* **62** (1994), 865–874.

[44] S. Galbraith. "Supersingular curves in cryptography." In *Advances in Cryptology — ASIACRYPT 2001*, Springer LNCS **2248** (2001), 495–513.

[45] S. Galbraith. "Pairings." In *Advances in Elliptic Curve Cryptography*, London Math. Soc. Lecture Note Ser. **317**. Cambridge University Press, Cambridge (2005), 183–213.

[46] S. Galbraith, J. McKee, and P. Valença. "Ordinary abelian varieties having small embedding degree." *Finite Fields and their Applications* **13** (2007), 800–814.

[47] S. Galbraith, K. Paterson, and N. Smart. "Pairings for cryptographers." Cryptology ePrint Archive, Report 2006/165 (2006). Available at http://eprint.iacr.org/2006/165.

[48] P. Gaudry. "Index calculus for abelian varieties and the elliptic curve discrete logarithm problem." To appear in *Journal of Symbolic Computation*. Available at http://eprint.iacr.org/2004/073.

[49] P. Gaudry. "An algorithm for solving the discrete log problem on hyperelliptic curves." In *Advances in Cryptology — EUROCRYPT 2000*, Springer LNCS **1807** (2000), 19–34.

[50] P. Gaudry and R. Harley. "Counting points on hyperelliptic curves over finite fields." In *Algorithmic Number Theory — ANTS-IV*, Springer LNCS **1838** (2000), 313–332.

[51] P. Gaudry, T. Houtmann, D. Kohel, C. Ritzenthaler, and A. Weng. "The 2-adic CM method for genus 2 curves with application to cryptography." In *Advances in Cryptology — ASIACRYPT 2006*, Springer LNCS **4284** (2006), 114–129. Preprint version available at http://arxiv.org/abs/math/0503148.

[52] P. Gaudry and É. Schost. "Construction of secure random curves of genus 2 over prime fields." In *Advances in Cryptology — EUROCRYPT 2004*, Springer LNCS **3027** (2004), 239–256.

[53] P. Gaudry, E. Thomé, N. Thériault, and C. Diem. "A double large prime variation for small genus hyperelliptic index calculus." *Mathematics of Computation* **76** (2007), 475–492.

[54] E. Goren and K. Lauter. "Class invariants for quartic CM fields." *Annales de l'Institut Fourier* **57** (2007), 457–480.

[55] R. Hartshorne. *Algebraic Geometry*, Graduate Texts in Mathematics **52**. Springer-Verlag, New York (1977).

[56] F. Hess, N. Smart, and F. Vercauteren. "The eta pairing revisited." *IEEE Transactions on Information Theory* **52** (2006), 4595–4602.

[57] L. Hitt. "Families of genus 2 curves with small embedding degree." Cryptology ePrint Archive, Report 2007/001 (2007). Available at http://eprint.iacr.org/2007/001.

[58] L. Hitt. "On the minimal embedding field." In *Pairing-Based Cryptography — Pairing 2007*, Springer LNCS **4575** (2007), 294–301.

[59] E. Howe. "Principally polarized ordinary abelian varieties over finite fields." *Transactions of the American Mathematical Society* **347** (1995), 2361–2401.

[60] A. Joux. "A one round protocol for tripartite Diffie-Hellman." In *Algorithmic Number Theory — ANTS-IV*, Springer LNCS **1838** (2000), 385–393. Full version: *Journal of Cryptology* **17** (2004), 263–276.

[61] E. Kachisa. *Constructing Brezing-Weng pairing friendly elliptic curves using elements in the cyclotomic field*. Master's thesis, Mzuzu University (2007). Some results appear in [62].

[62] E. Kachisa, E. Schaefer, and M. Scott. "Constructing Brezing-Weng pairing friendly elliptic curves using elements in the cyclotomic field." Cryptology ePrint Archive, Report 2007/452 (2007). Available at http://eprint.iacr.org/2007/452.

[63] K. Karabina. *On prime-order elliptic curves with embedding degrees* 3, 4 *and* 6. Master's thesis, University of Waterloo (2006).

[64] M. Kawazoe and T. Takahashi. "Pairing-friendly hyperelliptic curves of type $y^2 = x^5 + ax$." Cryptology ePrint Archive, Report 2008/026 (2008). Available at http://eprint.iacr.org/2008/026.

[65] N. Koblitz. "Elliptic curve cryptosystems." *Mathematics of Computation* **48** (1987), 203–209.

[66] N. Koblitz. "Hyperelliptic cryptosystems." *Journal of Cryptology* **1** (1989), 139–150.

[67] N. Koblitz. "Good and bad uses of elliptic curves in cryptography." *Moscow Mathematical Journal* **2** (2002), 693–715, 805–806.

[68] N. Koblitz and A. Menezes. "Pairing-based cryptography at high security levels." In *Cryptography and Coding*, Springer LNCS **3796** (2005), 13–36.

[69] D. Kohel. "Quartic CM fields database." Available at http://echidna.maths.usyd.edu.au/kohel/dbs/complex_multiplication2.html.

[70] K. Koike and A. Weng. "Construction of CM Picard curves." *Mathematics of Computation* **74** (2005), 499–518.

[71] S. Lang. *Elliptic Functions*, Graduate Texts in Mathematics **112**. Second edition. Springer-Verlag, New York (1987).

[72] S. Lang. *Algebra*, Graduate Texts in Mathematics **211**. Revised third edition. Springer-Verlag, New York (2002).

[73] K. Lauter. "The maximum or minimum number of rational points on genus three curves over finite fields." *Compositio Mathematica* **134** (2002), 87–111. With an appendix by Jean-Pierre Serre.

[74] A. K. Lenstra. "Unbelievable security (Matching AES security using public key systems)." In *Advances in Cryptology — ASIACRYPT 2001*, Springer LNCS **2248** (2001), 67–86.

[75] H. W. Lenstra, Jr. "Solving the Pell equation." *Notices of the American Mathematical Society* **49** (2002), 182–192.

[76] H. W. Lenstra, Jr., J. Pila, and C. Pomerance. "A hyperelliptic smoothness test. II." *Proceedings of the London Mathematical Society (3)* **84** (2002), 105–146.

[77] R. Lidl and H. Niederreiter. *Finite Fields*, Encyclopedia of Mathematics and its Applications **20**. Second edition. Cambridge University Press, Cambridge (1997).

[78] J. Lubin, J.-P. Serre, and J. Tate. "Elliptic curves and formal groups." Lecture notes from Summer Institute on Algebraic Geometry, Woods Hole, Massachusetts, July 1964. Available at http://www.ma.utexas.edu/users/voloch/lst.html.

[79] F. Luca, D. Mireles, and I. Shparlinski. "MOV attack in various subgroups on elliptic curves." *Illinois Journal of Mathematics* **48** (2004), 1041–1052.

[80] F. Luca and I. Shparlinski. "Elliptic curves with low embedding degree." *Journal of Cryptology* **19** (2006), 553–562.

[81] F. Luca and I. Shparlinski. "On finite fields for pairing based cryptography." *Advances in Mathematics of Communications* **1** (2007), 281–286.

[82] "MAGMA Computational Algebra System." Computational Algebra Group, School of Mathematics and Statistics, University of Sydney. Available at http://magma.maths.usyd.edu.au.

[83] K. Matthews. "The Diophantine equation $x^2 - Dy^2 = N$, $D > 0$." *Expositiones Mathematicae* **18** (2000), 323–331.

[84] A. Menezes. *Elliptic Curve Public Key Cryptosystems*, Kluwer International Series in Engineering and Computer Science **234**. Kluwer Academic, Boston (1993).

[85] A. Menezes. "Introduction to pairing-based cryptography." Notes from lectures given in Santander, Spain (2005). Available at http://www.cacr.math.uwaterloo.ca/~ajmeneze/publications/pairings.pdf.

[86] A. Menezes, T. Okamoto, and S. Vanstone. "Reducing elliptic curve logarithms to logarithms in a finite field." *IEEE Transactions on Information Theory* **39** (1993), 1639–1646.

[87] A. Menezes and S. Vanstone. "Isomorphism classes of elliptic curves over finite fields of characteristic 2." *Utilitas Mathematica* **38** (1990), 135–153.

[88] J.-F. Mestre. "Construction de courbes de genre 2 à partir de leurs modules." In *Effective Methods in Algebraic Geometry*, Progress in Mathematics **94**. Birkhäuser, Boston, MA (1991), 313–334.

[89] V. Miller. "Use of elliptic curves in cryptography." In *Advances in Cryptology — CRYPTO 1985*, Springer LNCS **218** (1986), 417–426.

[90] J. S. Milne. "Abelian varieties." In *Arithmetic Geometry*, ed. G. Gornell and J. Silverman. Springer, New York (1986), 103–150.

[91] J. S. Milne. "Jacobian varieties." In *Arithmetic Geometry*, ed. G. Gornell and J. Silverman. Springer, New York (1986), 167–212.

[92] J. S. Milne. "Abelian varieties." Version 2.00 (2008). Available at www.jmilne.org/math.

[93] A. Miyaji, M. Nakabayashi, and S. Takano. "Characterization of elliptic curve traces under FR-reduction." In *Information Security and Cryptology — ICISC 2000*, Springer LNCS **2015** (2001), 90–108.

[94] R. Mollin. *Fundamental Number Theory with Applications*. CRC Press, Boca Raton, FL (1998).

[95] F. Morain. "Classes d'isomorphismes des courbes elliptiques supersingulières en caractéristique ≥ 3." *Utilitas Mathematica* **52** (1997), 241–253.

[96] A. Murphy and N. Fitzpatrick. "Elliptic curves for pairing applications." Cryptology ePrint Archive, Report 2005/302 (2005). Available at http://eprint.iacr.org/2005/302.

[97] M. Naehrig, P. Barreto, and P. Schwabe. "On compressible pairings and their computation." Cryptology ePrint Archive, Report 2007/429 (2007). Available at http://eprint.iacr.org/2007/429.

[98] J. Neukirch. *Algebraic Number Theory*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences] **322**. Springer-Verlag, Berlin (1999). Translated from the German by N. Schappacher.

[99] A. Odlyzko. "Discrete logarithms in finite fields and their cryptographic significance." In *Advances in Cryptology — EUROCRYPT 1984*, Springer LNCS **209** (1985), 224–314.

[100] F. Oort and K. Ueno. "Principally polarized abelian varieties of dimension two or three are Jacobian varieties." *Journal of the Faculty of Science, University of Tokyo, Section IA: Mathematics* **20** (1973), 377–381.

[101] D. Page, N. Smart, and F. Vercauteren. "A comparison of MNT curves and supersingular curves." *Applicable Algebra in Engineering, Communication and Computing* **17** (2006), 379–392.

[102] *PARI/GP, version* `2.3.0`. Bordeaux (2006). Available at http://pari.math.u-bordeaux.fr.

[103] S. Pohlig and M. Hellman. "An improved algorithm for computing logarithms over G$F(p)$ and its cryptographic significance." *IEEE Transactions on Information Theory* **IT-24** (1978), 106–110.

[104] J. M. Pollard. "Monte Carlo methods for index computation (mod p)." *Mathematics of Computation* **32** (1978), 918–924.

[105] J. Robertson. "Solving the generalized Pell equation." Unpublished manuscript (2004). Available at http://hometown.aol.com/jpr2718/pell.pdf.

[106] S. Ross. *A First Course in Probability*. Fifth edition. Prentice-Hall, Upper Saddle River, NJ (1998).

[107] K. Rubin and A. Silverberg. "Finding composite order ordinary elliptic curves using the Cocks-Pinch method." In preparation.

[108] K. Rubin and A. Silverberg. "Supersingular abelian varieties in cryptology." In *Advances in Cryptology — CRYPTO 2002*, Springer LNCS **2442** (2002), 336–353.

[109] R. Sakai, K. Ohgishi, and M. Kasahara. "Cryptosystems based on pairings." Symposium on Cryptography and Information Security — SCIS 2000, Okinawa, Japan (2000).

[110] E. Schaefer. "A new proof for the non-degeneracy of the Frey-Rück pairing and a connection to isogenies over the base field." In *Computational Aspects of Algebraic Curves*, Lecture Notes Ser. Comput. **13**. World Scientific, Hackensack, NJ (2005), 1–12.

[111] M. Scott. Personal communication (7 November 2005).

[112] M. Scott and P. Barreto. "Compressed pairings." In *Advances in Cryptology — CRYPTO 2004*, Springer LNCS **3152** (2004), 140–156.

[113] M. Scott and P. Barreto. "Generating more MNT elliptic curves." *Designs, Codes and Cryptography* **38** (2006), 209–217.

[114] A. Shamir. "Identity-based cryptosystems and signature schemes." In *Advances in Cryptology — CRYPTO 1984*, Springer LNCS **196** (1985), 47–53.

[115] G. Shimura. *Abelian Varieties with Complex Multiplication and Modular Functions*, Princeton Mathematical Series **46**. Princeton University Press, Princeton, NJ (1998).

[116] V. Shoup. "NTL: a library for doing number theory." Available at http://www.shoup.net/ntl/.

[117] J. Silverman. *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics **106**. Springer-Verlag, New York (1986).

[118] J. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics **151**. Springer-Verlag, New York (1994).

[119] A.-M. Spallek. *Kurven vom Geschlecht 2 und ihre Anwendung in Public-Key-Kryptosystemen*. Ph.D. dissertation, Institut für Experimentelle Mathematik, Universität GH Essen (1994).

[120] B. Spearman and K. Williams. "Relative integral bases for quartic fields over quadratic subfields." *Acta Mathematica Hungarica* **70** (1996), 185–192.

[121] T. Takagi, T. Okamoto, E. Okamoto, and T. Okamoto, eds. *Pairing-Based Cryptography — Pairing 2007*, Springer LNCS **4575** (2007).

[122] J. Tate. "Classes d'isogénie des variétés abéliennes sur un corps fini (d'après T. Honda)." In *Séminaire Bourbaki 1968/69*, Springer Lect. Notes in Math. **179** (1971), 95–110.

[123] P. van Oorschot and M. Wiener. "Parallel collision search with cryptanalytic applications." *Journal of Cryptology* **12** (1999), 1–28.

[124] P. van Wamelen. "Examples of genus two CM curves defined over the rationals." *Mathematics of Computation* **68** (1999), 307–320.

[125] E. Verheul. "Evidence that XTR is more secure than supersingular elliptic curve cryptosystems." *Journal of Cryptology* **17** (2004), 277–296.

[126] Voltage Security Inc. http://voltage.com.

[127] J. von zur Gathen and J. Gerhard. *Modern Computer Algebra*. Second edition. Cambridge University Press, Cambridge (2003).

[128] W. C. Waterhouse. "Abelian varieties over finite fields." *Annales Scientifiques de l'École Normale Supérieure. Quatrième Série* **2** (1969), 521–560.

[129] W. 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)*. American Mathematical Society, Providence, RI (1971), 53–64.

[130] A. Weng. "A class of hyperelliptic CM-curves of genus three." *Journal of the Ramanujan Mathematical Society* **16** (2001), 339–372.

[131] A. Weng. "Constructing hyperelliptic curves of genus 2 suitable for cryptography." *Mathematics of Computation* **72** (2003), 435–458.

[132] A. Weng. "Extensions and improvements for the CM method for genus two." In *High Primes and Misdemeanours: Lectures in Honour of the 60th Birthday of Hugh Cowie Williams*, Fields Institute Communications **41**. American Mathematical Society, Providence, RI (2004), 379–389.