Constructing Pairing-Friendly Genus 2 Curves with Split Jacobian

Robert Dryło

Institute of Mathematics, Polish Academy of Sciences,
Warsaw School of Economics, Poland
r.drylo@impan.gov.pl

Abstract. Genus 2 curves with simple but not absolutely simple jacobians can be used to construct pairing-based cryptosystems more efficient than for a generic genus 2 curve. We show that there is a full analogy between methods for constructing ordinary pairing-friendly elliptic curves and simple abelian varieties, which are iogenous over some extension to a product of elliptic curves. We extend the notion of complete, complete with variable discriminant, and sparse families introduced in by Freeman, Scott and Teske [11] for elliptic curves, and we generalize the Cocks-Pinch method and the Brezing-Weng method to construct families of each type. To realize abelian surfaces as jacobians we use of genus 2 curves of the form $y^2 = x^5 + ax^3 + bx$ or $y^2 = x^6 + ax^3 + b$, and apply the method of Freeman and Satoh [10]. As applications we find some families of abelian surfaces with recorded ρ-value $\rho = 2$ for embedding degrees $k = 3, 4, 6, 12$, or $\rho = 2.1$ for $k = 27, 54$. We also give variable-discriminant families with best ρ-values.

Keywords: Pairing-friendly hyperelliptic curves, abelian varieties, Weil numbers, CM method.

1 Introduction

Since pairings have been introduced to design cryptographic protocols (see, e.g., [2, 3, 20, 35]), one of the main problems is to construct abelian varieties suitable for these applications. Let $A/\mathbb{F}_q$ be an abelian variety containing an $\mathbb{F}_q$-rational subgroup of prime order r with the embedding degree $k = \min\{l : r \mid (q^l - 1)\}$. To implement pairing-based cryptosystems k should be suitably small so that pairings of r-torsion points with values in the field $\mathbb{F}_{q^k}$ could be efficiently computed, but the discrete logarithm problem in $\mathbb{F}_{q^k}$ remains intractable. Furthermore, in order the arithmetic on A to be more efficient, we would like that the bit size of r to be close to the size of $\#A(\mathbb{F}_q)$. Since $\log(\#A(\mathbb{F}_q)) \approx \dim A \log(q)$, we would like the parameter $\rho = \dim A \log q / \log r$ to be close to one. We can achieve $\rho \approx 1$ using supersigular abelian varieties, which in each dimension have bounded embedding degrees (e.g., $k \leq 6$ or 12 for supersingular elliptic curves or abelian surfaces (see [14, 29, 31])). For higher security levels we use ordinary varieties, which are unlikely to be found by a random choice and require specific constructions. In practice, we mainly use elliptic curves or jacobians of hyperelliptic curves of low genus.

Pairing-friendly elliptic curves. In general, to construct an ordinary elliptic curve E with an embedding degree k we first find parameters (r, t, q) of E, where t is the trace of E, q is the size of the field of definition, and r is the order of a subgroup with the embedding degree k. Then we use the Complex Multiplication (CM) method to find the equation of E, which requires that the CM discriminant d of E is sufficiently small, where d is the square-free part the non-negative integer $4q - t^2$. Parameters (r, t, q) of pairing-friendly elliptic

curves are generated either directly, like in the Cocks-Pinch method (see [11, Theorem 4.1]), or are obtained as values of suitable polynomials $(r(x), t(x), q(x))$ called parametric families. The former method is very flexible and allows one to obtain the subgroup orders r and discriminants d of almost arbitrary size, however with ρ-value only around 2. Using parametric families we can considerably improve ρ-values for more restricted subgroup orders and discriminants.

Miyaji, Nakabayashi and Takano [25] were the first researchers to use parametric families to characterize elliptic curves of prime orders with embedding degrees $k = 3, 4, 6$. Scott and Barreto [32], and Galbraith et al. [15] generalized their idea to describe elliptic curves with prescribed cofactors for $k = 3, 4, 6$. Currently constructions of families with $\rho = 1$ are yet known for $k = 10$ and 12, and were discovered by Freeman [8] and Barreto-Naehrig [1], respectively. Most families used in practice are so-called complete families, and are constructed by the Brezing-Weng method [4]. We now recall the general definition and classification of families introduced by Freeman, Scott and Teske [11].

Definition 1. ([11, Definition 2.7]) Let k and d be positive integers such that d is square-free. We say that a triple of polynomials $(r(x), t(x), q(x))$ in $\mathbb{Q}[x]$ *parametrizes a family of elliptic curves with embedding degree k and discriminant d* if the following conditions are satisfied:

1. $q(x) = p(x)^s$ for some $s \geq 1$ and $p(x)$ that represents primes.
2. $r(x)$ is irreducible, non-constant, 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 $\Phi_k(x)$ is the kth cyclotomic polynomial.
5. The CM equation $4q(x) - t(x)^2 = dy^2$ has infinitely many integer solutions (x, y).

Properties of the CM equation lead us to the classification of families. It is clear that we can write $4q(x) - t(x)^2 = f(x)g(x)^2$, where $f(x) \in \mathbb{Z}[x]$ is square-free and $g(x) \in \mathbb{Q}[x]$. Then condition (5) implies by Siegel's theorem that $\deg f(x) \leq 2$ (see [8, Proposition 2.10] or Lemma 16). We say that a family is *complete* if $f = d$; then the CM equation is satisfied for any $x \in \mathbb{Z}$. We say that a family is *complete with variable discriminant* if $\deg f = 1$; then substituting $x \leftarrow (dx^2 - b)/a$, where $f(x) = ax + b$, yields a complete family with discriminant d if conditions (1) and (2) of Definition 1 are satisfied. A family is called *sparse* if $\deg f = 2$; then the CM equation can be transformed to the generalized Pell equation, whose solutions grow exponentially. We note that the Brezing-Weng method [4] can be generalized to construct families of the latter two types (see [7]). These families can be used to generate elliptic curves with larger discriminant, which may be desired for larger randomness of cryptosystems.

Pairing-friendly genus 2 curves. There is also a great deal of interest in constructing pairing-friendly genus 2 curves. Freeman, Stevenhagen and Streng [12] give a general method to generate pairs (r, π) such that π is a Weil q-number corresponding by the Honda-Tate theory to a simple ordinary abelian variety with embedding degree k with respect to r. In order to realize these varieties as jacobians, we must chose π from a suitable CM field K, where Weil numbers in question are characterized by the condition

$$\mathrm{N}_{K/\mathbb{Q}}(\pi - 1) \equiv \Phi_k(\pi\bar{\pi}) \equiv 0 \pmod{r}.$$

If $[K : \mathbb{Q}] = 2g$, then the corresponding varieties are of dimension g with ρ-value around $2g^2$. Freeman [9] generalized this method to construct parametric families of abelian vari-

eties. In order to obtain pairing-friendly ordinary abelian surfaces, which generically have ρ-value around 4, or less than 4 for parametric families, we use genus 2 curves, whose jacobian is simple but not absolutely simple. Kawazoe and Takahashi [23] use curves of the form $y^2 = x^5 + ax$ and a closed formula for their order [13] (see also Kachisa [21]). Freeman and Satoh [10] give a general method to construct an elliptic curve, whose Weil restriction over some extension contains an abelian surface with a given embedding degree. To realize that surface as a jacobian, they use curves of the form $y^2 = x^5 + ax^3 + bx$ or $y^2 = x^6 + ax^3 + b$. Recently Guillevic and Vergnaud [17] extended their method using closed formulas for the order of these curves.

Contribution. In this paper we show that there is a full analogy between methods for constructing pairing-friendly elliptic curves and simple abelian varieties which are isogenous over some extension to a product of elliptic curves. Now we outline the main idea of our method. Let K be a CM field of degree $2g$, and suppose that we have a polynomial $\pi(x, y) \in K[x, y]$ such that $q(x, y) = \pi(x, y)\bar{\pi}(x, y) \in \mathbb{Q}[x, y]$ and the image $\pi(\mathbb{Z}^2)$ contains "sufficiently many" Weil numbers in K. Then we can use $\pi(x, y)$ to generate pairing-friendly Weil numbers analogously as in the Cooks-Pinch method. If r is a prime such that the system

$$\mathrm{N}_{K/\mathbb{Q}}(\pi(x, y) - 1) = \Phi_k(q(x, y)) = 0, \tag{1}$$

has solutions over $\mathbb{F}_r$, then we check whether $\pi(x, y)$ is a Weil number for lifts $x, y \in \mathbb{Z}$ of these solutions. Since generically solutions over $\mathbb{F}_r$ are of the similar size as r, the resulting varieties have ρ-value $\rho = g \log q(x, y)/ \log r \approx 2g \deg \pi(x, y)$. Thus to obtain ρ-value around $2g$, we need suitable polynomials $\pi(x, y)$ of degree one. If K contains an imaginary quadratic subfield $K_0 = \mathbb{Q}(\sqrt{-d})$, then for any $u \in K$ such that $c = u\bar{u} \in \mathbb{Q}$, the polynomial $\pi(x, y) = u(x + y\sqrt{-d})$ satisfies $q(x, y) = \pi(x, y)\bar{\pi}(x, y) = c(x^2 + dy^2) \in \mathbb{Q}[x, y]$, however, if $c \neq 1$, then the image $\pi(\mathbb{Z}^2)$ does not contain sufficiently many primes. Therefore we will use $\pi(x, y) = \zeta_s(x + y\sqrt{-d})$ to generate Weil numbers in the CM field $K = \mathbb{Q}(\zeta_s, \sqrt{-d})$, where ζ_s is an sth primitive root of unity and $d > 0$ is a square-free integer. We note that Weil q-numbers of the form $\pi = \zeta_s\pi_0$ with $\pi_0 \in \mathbb{Q}(\sqrt{-d})$ correspond to simple abelian varieties which are isogenous over $\mathbb{F}_{q^s}$ to a power of an elliptic curve $E/\mathbb{F}_q$ with the Weil q-number π_0 (see Corollary 4).

To generalize the Cocks-Pinch and the Brezing-Weng methods we describe in Section 3 prime finite fields and number fields, where system (1) has solutions for $\pi(x, y) = \zeta_s(x + y\sqrt{-d})$, and we give explicit formulas on solutions. In Section 4 we focus on constructing genus 2 curves, whose jacobian corresponds to Weil numbers $\pi = \zeta_s\pi_0$ in a quartic CM field $K = \mathbb{Q}(\zeta_s, \sqrt{-d})$. We give an algorithm to construct curves of the form $y^2 = x^6+ax^3+b$ and $y^2 = x^5+ax^3+bx$, which is based on the method of Freeman and Satoh (see [10, Algorithm 5.11]). In Section 5 we generalize on abelian varieties Definition 1 and classification of families of elliptic curves. In Sections 6, 7, 8 we generalize the Brezing-Weng method to construct families of each type.

As applications we give complete families of abelian surfaces $(r(x), \pi(x))$ with variable discriminant and best ρ-values such that $\deg r(x) < 25$. We note that some of these families for fixed discriminants were found in [10] and [17]. Furthermore, some complete families with variable discriminant are given in [10, Section 7], where they are obtained from complete families satisfying certain conditions, but no general method to construct such families is given. We also find some families with recorded ρ-value $\rho = 2$ for $k = 3, 4, 6, 12$, or $\rho \approx 2.1$ for $k = 27, 54$ (see Examples 19, 24, 27).

2 Background

In this section we gather basic facts on abelian varieties, which will be needed in the sequel (for details see [26, 37–40]).

Let $A/\mathbb{F}_q$ be a g-dimensional abelian variety with qth Frobenius endomorphism π_A, and its characteristic polynomial f_A. Then we have $f_A(\pi_A) = 0$, and $\#A(\mathbb{F}_q) = f_A(1)$. Furthermore, all roots of f_A are Weil q-numbers. Recall that an algebraic integer π is called *a Weil q-number* if $|\alpha(\pi)| = \sqrt{q}$ for every embedding $\alpha : \mathbb{Q}(\pi) \to \mathbb{C}$). We say that A is *simple* if it is not isogenous over $\mathbb{F}_q$ to a product of two positive dimensional abelian varieties. By the Honda-Tate theorem the map which associates the Frobenius endomorphism π_A to a simple abelian variety $A/\mathbb{F}_q$ induces a one-to-one correspondence between isogeny classes of simple abelian varieties over $\mathbb{F}_q$ and conjugacy classes of Weil q-numbers. Recall also that a variety A is called *ordinary* if it has the maximum number p^g of all p-torsion points over $\overline{\mathbb{F}}_q$, where $p = \operatorname{char}\mathbb{F}_q$. We have the following.

Theorem 2. ([40]) *Let $A/\mathbb{F}_q$ be a simple abelian variety of dimension g with the endomorphism algebra $K = \operatorname{End}_{\mathbb{F}_q}(A) \otimes \mathbb{Q}$. Then A is ordinary if and only if $K = \mathbb{Q}(\pi_A)$ is a CM field of degree $2g$, and $\pi_A, \overline{\pi}_A$ are relatively prime in $\mathcal{O}_K$. Furthermore, if A is ordinary, then f_A is the minimal polynomial of π_A, and*

$$\#A(\mathbb{F}_q) = f_A(1) = \mathrm{N}_{K/\mathbb{Q}}(\pi_A - 1). \tag{2}$$

Recall that a number field K is called a *CM field* if it is an imaginary quadratic extension of a totally real field. Then K has an automorphism, denoted by a bar, which commutes with every embedding $K \to \mathbb{C}$ and the complex conjugation in $\mathbb{C}$.

In this paper we are interested in simple abelian varieties, which are not absolutely simple (i.e., split over some extension of the base field).

Proposition 3. *A simple ordinary abelian variety $A/\mathbb{F}_q$ with a Weil q-number π splits over $\mathbb{F}_{q^s}$ if and only if $\mathbb{Q}(\pi^s) \subsetneq \mathbb{Q}(\pi)$. Then A is isogenous to B^n over $\mathbb{F}_{q^s}$, where $B/\mathbb{F}_{q^s}$ is a simple abelian variety with the Weil q^s-number π^s.*

Proof. For the sake of completeness we give a proof (see also [18, Lemma 4]). We recall that if $f_{A,q}(x) = \prod_{i=1}^{2g}(x - \pi_i)$, then $f_{A,q^s}(x) = \prod_{i=1}^{2g}(x - \pi_i^s)$. Since A is simple and ordinary, $f_{A,q}(x)$ is irreducible, and hence all π_i are conjugated. If $\mathbb{Q}(\pi^s) \subsetneq \mathbb{Q}(\pi)$, then f_{A,q^s} is not the minimal polynomial of π^s, so A splits over $\mathbb{F}_{q^s}$. Conversely, if $A \sim B_1 \times \cdots \times B_m$ for simple abelian varieties $B_i/\mathbb{F}_{q^s}$, then $f_{A,q^s} = f_{B_1} \cdots f_{B_m}$. Since each B_i is ordinary, f_{B_i} is irreducible. Furthermore, since all the numbers $\pi_1^s, \ldots, \pi_{2g}^s$ are conjugated, it follows that they are exactly roots of each f_{B_i}. Hence all f_{B_i} are equal, and from the Honda-Tate theorem it follows that all B_i are isogenous over $\mathbb{F}_{q^s}$, so $A \sim B_1^n$.

Corollary 4. *Let $A/\mathbb{F}_q$ be an ordinary simple abelian variety with a Weil q-number π, and $E/\mathbb{F}_q$ be an ordinary elliptic curve with a Weil q-number π_0.*

(i) Then A is isogenous to E^g over $\mathbb{F}_{q^n}$ if and only if $\pi = \zeta_s \pi_0$, where ζ_s is an sth primitive root from unity and $s \mid n$.

(ii) If s is even and $\pi = \zeta_s \pi_0$, then A is isogenous to E'^g over $\mathbb{F}_{q^{s/2}}$, where E' is the quadratic twist of E.

(iii) If $\pi = \zeta_s \pi_0$, then $\mathbb{Q}(\pi) = \mathbb{Q}(\zeta_s, \sqrt{-d})$, where $\pi_0 \in \mathbb{Q}(\sqrt{-d})$ and d is a positive square-free integer.

Proof. (i) By Proposition 3 we have $A \sim E^g$ over $\mathbb{F}_{q^n}$ if and only if $\pi^n = \pi_0^n$. So, if s is the minimal integer such that $\pi^s = \pi_0^s$, then $\pi = \zeta_s \pi_0$, and obviously $s \mid n$.

(ii) Since $-\pi_0$ is the Weil q-number of the quadratic twists E' of E, and $\pi = \zeta_{s/2}(-\pi_0)$, it follows from (i) that $A \sim E'^g$ over $\mathbb{F}_{q^{s/2}}$.

(iii) Since E is ordinary, π_0^s and $\bar{\pi}_0^s$ are relatively prime. Hence $\pi^s = \pi_0^s$ generates $\mathbb{Q}(\sqrt{-d})$, which implies that $\zeta_s, \sqrt{-d} \in \mathbb{Q}(\pi)$, so $\mathbb{Q}(\pi) = \mathbb{Q}(\zeta_s, \sqrt{-d})$.

2.1 Weil numbers of pairing-friendly varieties

Recall that *the embedding degree* of an abelian variety $A/\mathbb{F}_q$ with respect to a prime $r \mid \#A(\mathbb{F}_q)$, $r \neq \operatorname{char} \mathbb{F}_q$, is the minimal integer k such that $r \mid (q^k - 1)$. In other words, $q \pmod r$ is a kth primitive root of unity, or equivalently, if $r \nmid k$, it is a root of the kth cyclotomic polynomial $\Phi_k(x)$. By Theorem 2 we have the following.

Lemma 5. ([12, Proposition 2.1]) *Let $K = \mathbb{Q}(\pi)$ be a CM field of degree $2g$, where π is a Weil q-number corresponding to an ordinary abelian variety A. Let k be a positive integer and r be a prime such that $r \nmid kq$. Then A has the embedding degree k with respect to r if and only if*

(1) $r \mid \Phi_k(q)$,
(2) $r \mid \mathrm{N}_{K/\mathbb{Q}}(\pi - 1)$.

3 The generalized Cocks-Pinch method

Let $K = \mathbb{Q}(\zeta_s, \sqrt{-d})$ be a CM field of degree $2g$, where ζ_s is an sth primitive root of unity and $d > 0$ is a square-free integer. To generate as in the Cooks-Pinch method pairing-friendly Weil numbers of the form $\pi = \zeta_s \pi_0$ with $\pi_0 \in \mathbb{Q}(\sqrt{-d})$, we need to find a prime finite field $\mathbb{F}_r$ where the system

$$\mathrm{N}_{K(x,y)/\mathbb{Q}(x,y)} \left(\zeta_s(x + y\sqrt{-d}) - 1\right) = \Phi_k\left(x^2 + dy^2\right) = 0, \tag{3}$$

has solutions, and check whether $\pi(x, y) = \zeta_s(x + y\sqrt{-d})$ is a Weil number for lifts $x, y \in \mathbb{Z}$ of these solutions. We describe below such prime fields $\mathbb{F}_r$, and give explicit formulas on solutions. We also give an analogous result for number fields in order to further generalize the Brezing-Weng.

Lemma 6. *Let $R = \mathbb{Z}$ or $\mathbb{Q}[x]$, and $r \in R$ be a prime such that the residue field $R/(r)$ contains primitive roots of unity ζ_k, ζ_s and $\sqrt{-d}$ (if $R = \mathbb{Z}$, we assume that $r \nmid 2dks$). If $\sqrt{-d} \notin \mathbb{Q}(\zeta_s)$, then solutions in $R/(r)$ of system (3) are of the form*

$$x = \frac{\zeta_s^{-1} + \zeta_k \zeta_s}{2}, \quad y = \pm \frac{\zeta_s^{-1} - \zeta_k \zeta_s}{2\sqrt{-d}}. \tag{4}$$

If $\sqrt{-d} \in \mathbb{Q}(\zeta_s)$, then one of these pairs is a solution of (3).

Proof. We have

$$\mathrm{N}_{K(x,y)/\mathbb{Q}(x,y)}\left(\zeta_s(x+y\sqrt{-d})-1\right)=\prod_{\sigma\in\mathrm{Aut}(K)}\Big(\sigma(\zeta_s)\big(x+y\sigma(\sqrt{-d})\big)-1\Big),$$

and

$$x^2+dy^2=\sigma(\zeta_s)\big(x+y\sigma(\sqrt{-d})\big)\sigma(\zeta_s^{-1})\big(x-y\sigma(\sqrt{-d})\big).$$

Thus (3) has the same solutions over $\mathbb{Q}(\zeta_k,\zeta_s,\sqrt{-d})$ as systems

$$\sigma(\zeta_s)\big(x+y\sigma(\sqrt{-d})\big)=1,$$
$$\sigma(\zeta_s^{-1})\big(x-y\sigma(\sqrt{-d})\big)=\zeta_k,$$

for each ζ_k and $\sigma\in\mathrm{Aut}(K)$. Hence

$$x=\frac{\sigma(\zeta_s^{-1})+\zeta_k\sigma(\zeta_s)}{2},\quad y=\frac{\sigma(\zeta_s^{-1})-\zeta_k\,\sigma(\zeta_s)}{2\sigma(\sqrt{-d})}. \tag{5}$$

If $\sqrt{-d}\notin\mathbb{Q}(\zeta_s)$, then the above solutions are of the form (4), since each automorphism of $\mathbb{Q}(\zeta_s)$ has two extensions on K. If $\sqrt{-d}\in\mathbb{Q}(\zeta_s)$, this solution is equal to one of pairs (4). Now let P be a prime ideal over r in $S=R[\zeta_s,\zeta_k,\sqrt{-d}]$, and S_P be the localization of S at P. It follows from the assumption that $R/(r)=S/P=S_P/PS_P$. Reducing solutions (5) mod PS_P we get solutions in $R/(r)$ of the desired form, sine reduction mod P induces an isomorphism between sth and kth roots of unity in S and $R/(r)$ by the following fact.

Lemma 7. *Let $R=\mathbb{Z}$ or $\mathbb{Q}[x]$, and $r\in R$ be a prime such that the residue field $R/(r)$ contains sth primitive roots of unity (if $R=\mathbb{Z}$, we assume that $r\nmid s$). If P is a prime ideal in $R[\zeta_s]$ over r, then $R/(r)=R[\zeta_s]/P$ and reduction mod P induces an isomorphism between sth roots of unity in $R[\zeta_s]$ and $R/(r)$.*

Proof. We note that $S=R[\zeta_s]$ is the integral closure of R in the field of fractions of S. This is well-known for $R=\mathbb{Z}$; if $R=\mathbb{Q}[x]$, it follows from the fact that $F[x]$ is integrally closed in $F(x)$ for any field F; in particular for $F=\mathbb{Q}(\zeta_s)$. We also note that the sth cyclotomic polynomial $\Phi_s(x)$ is irreducible over $\mathbb{Q}(x)$, because it is irreducible over $\mathbb{Q}$ and coefficients of monic factors of polynomials in $\mathbb{Q}[x]$ are algebraic over $\mathbb{Q}$. Since $R\subset S$ is an integral extension of Dedekind domains, we have $rS=\prod_{i=1}^n P_i^e$, where P_i are prime ideals in S. Let $r_i\mathrm{mod}r$ for $r_i\in R$ be different sth primitive roots of unity in $R/(r)$ for $i=1,\ldots,\varphi(s)$. Since $r_i\mathrm{mod}r$ are roots of $\Phi_s(x)$, after rearranging we have $P_i=(r,\zeta_s-r_i)$ (see [24, Proposition I.8.25]). Thus $\zeta_s^j\equiv r_i^j\mathrm{mod}P_i$ yields an isomorphism between sth roots of unity.

From Lemma 6 we obtain the following generalization of the Cocks-Pinch algorithm.

Algorithm 8. Input: A CM field $K=\mathbb{Q}(\zeta_s,\sqrt{-d})$ of degree $2g$, and a positive integer k. Output: A pair (r,π) such that r is a prime and $\pi=\zeta_s\pi_0$ with $\pi_0\in\mathbb{Q}(\sqrt{-d})$ is a Weil q-number corresponding to a g-dimensional ordinary abelian variety $A/\mathbb{F}_q$ with the embedding degree k with respect to r.

1. Choose a prime r such that $\mathrm{lcm}(s,k)|(r-1)$ and $\sqrt{-d}\in\mathbb{F}_r$.

2. Let $x = \frac{\zeta_s^{-1}+\zeta_k\zeta_s}{2}$ and $y = \frac{\zeta_s^{-1}-\zeta_k\zeta_s}{2\sqrt{-d}}$ for all primitive roots of unity $\zeta_s, \zeta_k \in \mathbb{F}_r$.
3. If $\sqrt{-d} \in \mathbb{Q}(\zeta_s)$ and x, y in the previous step do not satisfy system (3), put $y := -y$.
4. Let $x_1, y_1 \in [0, r)$ be lifts of x, y.
5. Let $\pi = \zeta_s\big(x_1 + ir + (y_1 + jr)\sqrt{-d}\big)$ for $i, j \in [-m, m]$, where m is a small integer.
6. Return (r, π) if $q = \pi\bar{\pi}$ is prime and $x_1 + ir \neq 0$.

We expect that solutions of system (3) behave like random elements in $\mathbb{F}_r$, so we generically obtain ρ-value $\rho = \frac{g\log((x_1+ir)^2+d(y_1+jr)^2)}{\log r} \approx 2g$.

Remark. If $d \equiv 3 \bmod 4$, we obtain Weil numbers $\pi = \zeta_s\pi_0$ such that π_0 is in the proper suborder $\mathbb{Z}[\sqrt{-d}]$. If we want to generate Weil numbers without this restriction, we can modify the above method using $\pi(x, y) = \zeta_s(x + y(1 + \sqrt{-d})/2)$.

4 Freeman-Satoh curves

In this section we focus on constructing genus 2 curves, whose jacobian corresponds to a given Weil number $\pi = \zeta_s\pi_0$ in a quartic CM field $K = \mathbb{Q}(\zeta_s, \sqrt{-d})$, where $\pi_0 \in \mathbb{Q}(\sqrt{-d})$. Since $\varphi(s) = 2$ or 4, we have $s = 3, 4, 6, 8, 12$ (the quartic CM field $\mathbb{Q}(\zeta_5)$ contains no imaginary quadratic subfield). We note that a simple abelian surface which is not absolutely simple, may be not isogenous to the jacobian of any curve (see [28]). Since abelian surfaces corresponding to Weil numbers in question have automorphisms of order s, so of order 3 or 4, first it is natural to consider genus 2 curves which have automorphisms of order 3 or 4. We will use the following families of curves

$$y^2 = x^6 + ax^3 + b, \tag{6}$$

$$y^2 = x^5 + ax^3 + bx, \tag{7}$$

which have automorphisms of order 3 and 4 given by $(x, y) \mapsto (\zeta_3 x, y)$ and $(-x, iy)$, respectively (for more details on genus 2 curves with additional automorphisms see [6, 16, 19, 33]). We will need the following result due to Freeman and Satoh [10].

Lemma 9. ([10, Propositions 4.1 and 4.2]) *A curve C given by* (6) *or* (7) *is isomorphic to the curve $y^2 = x^6 + cx^3 + 1$ or $y^2 = x^5 + cx^3 + x$, respectively, where $c = a/\sqrt{b}$. Furthermore,* $\mathrm{Jac}(C)$ *is isogenous over some extension to E^2, where E is an elliptic curve with the j-invariant*

$$j(E) = 2^8 3^3 \frac{(2c-5)^3}{(c-2)(c+2)^3}, \tag{8}$$

$$j(E) = 2^6 \frac{(3c-10)^3}{(c-2)(c+2)^2}, \tag{9}$$

respectively.

We now describe a method based on [10, Algorithm 5.11]. Suppose that an abelian surface $A/\mathbb{F}_q$ corresponding to a Weil q-number $\pi = \zeta_s\pi_0$ is isogenous to the jacobian of a genus 2 curve C given by (6) or (7). Then A is isogenous over some extension to E^2, where E is an elliptic curve with the j-invariant given by (8) or (9), respectively. By Corollary 4, A is also isogenous to E_0^2 over $\mathbb{F}_{q^s}$, where E_0 is an elliptic curve with the Weil q-number π_0. Hence E and E_0 are isogenous, and so $\mathrm{End}(E)$ is an order in $K_0 = \mathbb{Q}(\sqrt{-d})$.

In particular, if $\mathrm{End}(E) = \mathcal{O}_{K_0}$ is the maximal order, then $j(E)$ is a root of the Hilbert class polynomial $H_{K_0}(x)$. Conversely, if $j \in \mathbb{F}_q$ is a root of $H_{K_0}(x)$, and there exists $c \in \mathbb{F}_q$ satisfying equations (8) or (9) with $j(E) = j$, then we determine isomorphism classes over $\mathbb{F}_q$ of curves $y^2 = x^6 + ax^3 + b$ or $y^2 = x^5 + ax^3 + bx$ with $a, b \in \mathbb{F}_q$ satisfying $c = a/\sqrt{b}$, and verify if jacobians of these curves correspond to π. We recall that to check with high probability if the jacobian of a curve C corresponds to a Weil number π we pick a random point $P \in \mathrm{Jac}(C)$ and check if $nP = 0$, where $n = \mathrm{N}(\pi - 1)$. The above procedure we give below as an algorithm. The only improvement is that we admit *all* twists of the above curves. The following examples show that this improvement is essential.

Example 10. Let $\pi = \zeta_3(3 + 2\sqrt{-5})$ be a Weil q-number with $q = \pi\bar{\pi} = 29$ and $n = \mathrm{N}_{K/\mathbb{Q}}(1-\pi) = 1029$. Using Algorithm 11 below we find that π corresponds to the jacobian of the curve

$$y^2 = 4x^6 + 26x^5 + 7x^4 + 11x^3 + 24x^2 + 27x + 4,$$

which is a twist of the curve $y^2 = x^6 + 5x^3 + 1$. However, checking all $a, b, c \in \mathbb{F}_{29}$, we find that there are no curves $y^2 = ax^6 + bx^3 + c$, whose jacobian corresponds to π.

Algorithm 11. Input: A square-free positive integer d, $s = 3, 4$, and a Weil q-number $\pi = \zeta_s\pi_0$ with π_0 in $K_0 = \mathbb{Q}(\sqrt{-d})$. Output: A genus 2 curve over $\mathbb{F}_q$, whose jacobian corresponds to π, or $\emptyset$.

1. Compute the Hilbert class polynomial $H_{K_0}(x)$.
2. For each root $j \in \mathbb{F}_q$ of $H_{K_0}(x)$ find solutions $c \in \overline{\mathbb{F}}_q$ of equations (8) or (9).
3. For each solution c, let $C : y^2 = x^6 + cx^3 + 1$ or $C : y^2 = x^5 + cx^3 + x$. Remove C if it is not hyperelliptic.
4. If $c \notin \mathbb{F}_q$ and all absolute invariants of C lie in $\mathbb{F}_q$, determine a model $C_1/\mathbb{F}_q$ of C and put $C := C_1$.
5. Determine all twists of C over $\mathbb{F}_q$.
6. For each twist C' choose a random point $P \in \mathrm{Jac}(C')(\mathbb{F}_q)$ and compute nP, where $n = \mathrm{N}_{K/\mathbb{Q}}(\pi - 1)$.
7. Return C' if $nP = 0$.

In this algorithm we need to compute the Hilbert class polynomial $H_{K_0}(x)$, which requires that the discriminant d is sufficiently small (see [36]). We also note that if a genus 2 curve $C/\overline{\mathbb{F}}_q$ has a model over $\mathbb{F}_q$, then all its absolute invariants lie in $\mathbb{F}_q$. The converse property is not always true, but it does hold if C has automorphisms other than the identity and the hyperelliptic involution. Then a model of C over $\mathbb{F}_q$ can be computed using the generalization of the Mestre algorithm [30] due to Cardona and Quer [5].

Remark 12. (i) In the above algorithm it usually suffices to use curves (6) or (7) if $s = 3$ or 4, respectively. However, it may happen for the CM field $K = \mathbb{Q}(\zeta_{12})$ that we need to use curves (6) to realize Weil numbers of the form $i\pi_0$ with $\pi_0 \in \mathbb{Q}(\sqrt{-3})$ (see Example 19).
(ii) For Weil numbers in the CM field $\mathbb{Q}(\zeta_8)$ we can usually use curves $y^2 = x^5 + ax$, which have automorphisms of order 8, $(x, y) \mapsto (\zeta_8^2 x, \zeta_8 y)$. Originally to construct pairing-friendly curves of this form Kawazoe and Takahashi [23] used the closed formula on their order (see [13]).

Example 13. For $K = \mathbb{Q}(\zeta_3, \sqrt{-5})$ and $k = 16$, we find the following parameters of an abelian surface with $\rho = 4.011$, and the corresponding genus 2 curve:

$$
\begin{aligned}
r &= 48(10^{53} + 2085) + 1 \ \text{(181-bits prime)},\\
\pi &= \zeta_3(43052596005393018890282705273195337598678148826092149 84 + 57150806789593855035415547 2517\\
&\quad 64179095237824101815209 3\sqrt{-5}),\\
q &= 20168367586386572810015424271002249732267166683454467732594522539415397151727 6154391831469\\
&\quad 84296058295131523501,\\
y^2 &= x^6 + x^3 + 98153291727173047426466825074438376575740617497151582440282601963384830645758936 2\\
&\quad 32913860543632038045605118 72.
\end{aligned}
$$

Example 14. For $K = \mathbb{Q}(i, \sqrt{-7})$ the following abelian surface has embedding degree $k = 31$ and $\rho = 4.016$:

$$
\begin{aligned}
r &= 124(10^{75} + 3) + 1 \ \text{(256-bits prime)},\\
\pi &= i(96180181687130548086884708381078859138617038963689573425053970665226825986272 + 91558027\\
&\quad 99235777905099734889345646175817336249315015553451165600417834527285 3\sqrt{-7}),\\
q &= 67930734778315036928975166628644947130517387169432242055607030285583182335449420739462127 5\\
&\quad 41092926455433020262880660629280273105153102439936019342663775247,\\
y^2 &= 3x^6 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0,\\
a_4 &= 33598834264919032392606873512053335842744152826695842009617052556638071501840617988369094 09\\
&\quad 29053258439399481704008550987597610050426614764135822532343 4953,\\
a_3 &= 53568375176044744706267570717483438429124514759757339864067900061611934596851330165088783 0\\
&\quad 87061366317277737242870773498865524678821349877901446296718597438,\\
a_2 &= 20883824034068456880580362609611958725293164107308482736332244204650437266984961691635645 71\\
&\quad 71176635445125147016524676328092739235264591714565408500671781 8,\\
a_1 &= 57720778065183501500394160125969638193912223362157928071963646675538960777428029050063274589\\
&\quad 92289332456424150506228 8566242408798365886239297499816304155 07,\\
a_0 &= 40608745286371422614086942885541479059151002533283910337262145107513480124319683073247403806\\
&\quad 51303179475100907083325584702880742764524413028309436228200399 8.
\end{aligned}
$$

5 Parametric Families

Here we generalize Definition 1 and classification of families of elliptic curves on simple abelian varieties over $\mathbb{F}_q$, which are isogenous over some extension to a power of an elliptic curve defined over $\mathbb{F}_q$. Recall that by Corollary 4 Weil q-numbers of such abelian varieties are of the form $\pi = \zeta_s\pi_0$, where π_0 is a Weil q-number of an elliptic curve.

Definition 15. Let $K = \mathbb{Q}(\zeta_s, \sqrt{-d})$ be a CM field of degree $2g$, where ζ_s is an sth primitive root of unity and $d > 0$ is a square-free integer. Let $r(x) \in \mathbb{Q}[x]$ and $\pi(x) = \zeta_s(f_1(x)+f_2(x)\sqrt{-f(x)})$, where $f_1(x), f_2(x), f(x) \in \mathbb{Q}[x]$. We say that the pair $(r(x), \pi(x))$ *parametrizes a family of g-dimensional ordinary abelian varieties with embedding degree k and discriminant d* if the following conditions are satisfied:

1. $q(x) = f_1^2(x) + f_2^2(x)f(x)$ is a power of a polynomial in $\mathbb{Q}[x]$ that represents primes, and $\gcd(f_1(x), q(x)) = 1$.

2. $r(x)$ is irreducible, non-constant, integer valued, and has positive leading coefficient.
3. $r(x)$ divides $N_{K_1/\mathbb{Q}(x)}(\pi(x)-1)$, where $K_1=\mathbb{Q}(x,\zeta_s,\sqrt{-f})$.
4. $r(x)$ divides $\Phi_k(q(x))$.
5. The CM equation $f(x)=dy^2$ has infinitely many integer solutions (x,y).

We note that the ρ-values $g\log q(x)/\log r(x)$ of parametrized abelian varieties tend to the ρ-value of the family

$$\rho=\frac{g\deg q(x)}{\deg r(x)}.$$

The assumption $\gcd(f_1(x),q(x))=1$ is necessary to obtain ordinary varieties. It follows from the fact that an abelian variety with a Weil q-number $\pi=\zeta_s\pi_0$ is ordinary if and only if the corresponding elliptic curve with the Weil q-number π_0 is ordinary, which means that its trace $\pi_0+\bar{\pi}_0$ is relatively prime to q. In the examples below $q(x)$ will always represent primes, then it is sufficient that $f_1\neq 0$. As for elliptic curves to obtain parameters of an abelian variety with the endomorphism algebra $K=\mathbb{Q}(\zeta_s,\sqrt{-d})$ we find integer solutions (x_0,y_0) to the CM equation $f(x)=dy^2$, and check whether $\pi(x_0)$ is a Weil number, and $r(x_0)$ is prime, or almost prime. If this is the case, then $N_{K_1/\mathbb{Q}(x)}(\pi(x)-1)(x_0)$ is the order of an abelian variety corresponding to $\pi(x_0)$, and it is divisible by large prime factors of $r(x_0)$. To generalize classification of families we will need the following fact (see also [8, Proposition 2.10]).

Lemma 16. *In Definition 15 we can assume that $f\in\mathbb{Z}[x]$ is square-free, $\deg f\leq 2$, and the leading coefficient of f is positive.*

Proof. Obviously, condition (5) in Definition 15 implies that the leading coefficient of f is positive. We can write $f=g_1g_2^2$, where $g_1\in\mathbb{Z}[x]$ is square-free and $g_2\in\mathbb{Q}[x]$. By Siegel's theorem (see [34, Theorem IX.4.3]) the curve $dy^2=f(x)$ contains finitely many integer points if $f\in\mathbb{Q}[x]$ is square-free of degree $\deg f\geq 3$. Thus replacing f by g_1 and f_2 by f_2g_2 we have $\deg f\leq 2$.

Definition 17. Let $(r(x),\pi(x))$ be a family satisfying Definition 15 with $f(x)$ as in Lemma 16. We say that the family is

1. *complete with discriminant d* if $f=d$,
2. *complete with variable discriminant* if $\deg f=1$,
3. *sparse* if $\deg f=2$.

The above conditions have the same interpretation as for elliptic curves, and are useful to obtain algorithms to generate families of each type, which generalize the Brezing-Weng method [4].

6 Complete Families

First we generalize the Brezing-Weng method [4] to construct complete families of abelian varieties. Let $K=\mathbb{Q}(\zeta_s,\sqrt{-d})$ be a CM field of degree $2g$. To construct a complete family $(r(x),\pi(x))$ with $\pi(x)=\zeta_s(f_1(x)+f_2(x)\sqrt{-d})$, we need to find a number field $L=\mathbb{Q}[x]/(r(x))$ where the system

$$\mathrm{N}_{K(x,y)/\mathbb{Q}(x,y)}\left(\zeta_s(x+y\sqrt{-d})-1\right)=\Phi_k\left(x^2+dy^2\right)=0 \tag{10}$$

has solutions, and take $f_1, f_2 \in \mathbb{Q}[x]$ to be lifts of these solutions. Such number fields and formulas on solutions have been described in Lemma 6. Hence we have the following algorithm.

Algorithm 18. Input: A CM field $K = \mathbb{Q}(\zeta_s, \sqrt{-d})$ of degree $2g$, a positive integer k, and a number field L containing $\zeta_s, \zeta_k, \sqrt{-d}$.
Output: A complete family $(r(x), \pi(x))$ of g-dimensional ordinary abelian varieties with embedding degree k, or $\emptyset$.

1. Find a polynomial $r(x) \in \mathbb{Q}[x]$ such that $L = \mathbb{Q}[x]/(r(x))$.
2. Let $x_1 = \frac{\zeta_s^{-1}+\zeta_k\zeta_s}{2}$ and $y_1 = \frac{\zeta_s^{-1}-\zeta_k\zeta_s}{2\sqrt{-d}}$ for all $\zeta_s, \zeta_k \in L$.
3. If $\sqrt{-d} \in \mathbb{Q}(\zeta_s)$ and x_1, y_1 do not satisfy system (10), put $y_1 = -y_1$.
4. Let $f_1, f_2 \in \mathbb{Q}[x]$ be lifts of x_1, y_1 with $\deg f_i < \deg r$, $i = 1, 2$.
5. Let $\pi(x) = \zeta_s(f_1(x) + f_2(x)\sqrt{-d})$.
6. Return $(r(x), \pi(x))$ if $f_1 \neq 0$, $2f_1(x) \in \mathbb{Z}$ for some $x \in \mathbb{Z}$, and $q(x) = f_1(x)^2 + df_2^2(x)$ represents primes.

We note that resulting families have ρ-value

$$\rho = \frac{2g \max\{\deg f_1, \deg f_2\}}{\deg r} \leq \frac{2g(\deg r - 1)}{\deg r} < 2g.$$

In the above algorithm we can take as L the cyclotomic field $L = \mathbb{Q}(\zeta_s, \zeta_m, \zeta_k) = \mathbb{Q}(\zeta_l)$, where m is the smallest integer such that $\sqrt{-d} \in \mathbb{Q}(\zeta_m)$ and $l = \mathrm{lcm}(s, m, k)$. We note that such m exists, because $\sqrt{(-1)^{\frac{p-1}{2}}p} \in \mathbb{Q}(\zeta_p)$ for each prime $p > 2$ and $\sqrt{-2} \in \mathbb{Q}(\zeta_8)$ (see [27, Lemma 2.2]). Now we give a few examples; more complete families with variable discriminant will be given in Section 8.

Example 19. Let $s = 4$, $d = 3$, and $K = \mathbb{Q}(\zeta_{12}) = \mathbb{Q}(i, \sqrt{-3})$. Let $k = 12$ and $L = K = \mathbb{Q}[x]/(r_0(x))$, where $r_0(x) = x^4 + 2x^3 + 6x^2 - 4x + 4$ is the minimal polynomial of $\zeta_{12} - \zeta_{12}^2 + \zeta_{12}^3$. Using $\pi(x, y) = i(x + y\sqrt{-3})$ we find the following family of simple ordinary abelian surfaces with embedding degree $k = 12$ and $\rho = 2$:

$$\begin{aligned} r(x) &= \tfrac{1}{36}(x^4 + 2x^3 + 6x^2 - 4x + 4), \\ \pi(x) &= \tfrac{i}{12}\big(x^2(-\sqrt{-3} + 1) - 2x(\sqrt{-3} + 1) - 6\sqrt{-3} - 2\big). \end{aligned}$$

We note that this construction is analogous to the Barreto-Naehrig family of elliptic curves with $k = 12$ and $\rho = 1$ (see [1]). For example, we generate the following parameters of abelian surfaces and the corresponding genus 2 curves using Algorithm 11.

$$
\begin{aligned}
x &= 87960930234340,\\
r &= 166286408606805664482429223743717411451268709008301229 \ \text{(180-bits prime)},\\
\pi &= \tfrac{i}{2}(128952087461504213424246115 3 - 128952087461510077486261738 1\sqrt{-3}),\\
q &= 166286408606805664482429223872669498912781800418 0996723,\\
y^2 &= 3x^6 + 399087380656333594757830137294406797390676321003439214x^3\\
&\quad +840318388709976017122087137087102952585808061504841608
\end{aligned}
$$

$$
\begin{aligned}
x &= 46116860184274347310,\\
r &= 125642457939801322085590357749816450418837410380874526029083415447117270861649 \ \text{(256-bits prime)},\\
\pi &= \tfrac{i}{2}(354460798875984764473015759359659256913 - 354460798875984764503760332815842155121\sqrt{-3}),\\
q &= 125642457939801322085590357749816450419191871179750510793602548066661204465873,\\
y^2 &= 10x^6 + 100513966351841057668472286199853160335353496943800408634882038453328963572700x^3\\
&\quad + 729329339848958714442434908666134531393324973824215765054704071017354959683 50
\end{aligned}
$$

Example 20. Let $s = 8$, $d = 2$, and $K = \mathbb{Q}(\zeta_8)$; we have $\sqrt{-2} = \zeta_8^3 + \zeta_8$. Using $\pi(x, y) = \zeta_8(x + y\sqrt{-2})$ we obtain Kawazoe-Takahashi families [23]. For example, we have the following family with $k = 32$ and $\rho = 3.25$:

$$
\begin{aligned}
r(x) &= \Phi_{32}(x),\\
\pi(x) &= \tfrac{\zeta_8}{4}\big(-2x^{13} + 2x^{12} - \sqrt{-2}(x^9 + x^8 + x + 1)\big).
\end{aligned}
$$

$$
\begin{aligned}
x &= 1011203,\\
r &= r(x)/2 = 59756285640301639937164660348874024804987005781756086983396949367884563171 5 31028321537514119056 1\\
&\quad \text{(318-bits prime)},\\
\pi &= -27636661717843096901242245558493120316710924191467536 2\,\zeta_8^2 - 57792052245650861120797900184955492980142309 75\\
&\quad 89947855348929618296359476697841\,\zeta_8 + 27636661717843096901242245558493120316710924191467536 2,\\
q &= 33399213027640387398202066273490523254329235495826947116565196632094950741 9\ 07470195554624141450877072423 26\\
&\quad 37828784532408999026408517139467788305673313723369,\\
y^2 &= x^5 + 21x.
\end{aligned}
$$

Example 21. We can also give some families of 3-dimensional varieties with $\rho < 6$. Constructing the corresponding genus 3 curves we leave as an open problem. The only sixtic CM fields of the form $K = \mathbb{Q}(\zeta_s, \sqrt{-d})$ are the cyclotomic fields $\mathbb{Q}(\zeta_7)$ and $\mathbb{Q}(\zeta_9)$, which contain $\sqrt{-7}$ and $\sqrt{-3}$, respectively.

(i) Let $K = \mathbb{Q}(\zeta_7)$ and $\alpha = \sqrt{-7} = 2\,\zeta_7^4 + 2\,\zeta_7^2 + 2\,\zeta_7 + 1$.

$$k = 7, \quad \rho = 4,$$
$$r(x) = \Phi_7(x),$$
$$\pi(x) = \tfrac{\zeta_7}{14}(-2\,\alpha\,x^4 + (\alpha+7)x^3 + 2\,\alpha\,x^2 + (\alpha+7)x - 2\,\alpha),$$

$$k = 21, \quad \rho = 4,$$
$$r(x) = \Phi_{21}(x),$$
$$\pi(x) = \tfrac{\zeta_{21}}{14}((-\alpha-7)x^8 + (\alpha-7)x^7 - 2\,\alpha\,x^6 + 2\,\alpha\,x^4 - 2\,\alpha\,x^2 + (\alpha-7)x - \alpha-7).$$

(ii) Let $K = \mathbb{Q}(\zeta_9)$ and $\alpha = \sqrt{-3} = 2\,\zeta_9^3 + 1$.

$$k = 9, \quad \rho = 4,$$
$$r(x) = \Phi_9(x),$$
$$\pi(x) = \tfrac{\zeta_9}{6}((-\alpha-3)x^4 + (\alpha+3)x^3 + (\alpha-3)x + 2\,\alpha).$$

7 Sparse families

In this section we generalize Algorithm 18 to construct sparse families in an analogous way as the Brezing-Weng method was generalized to construct such families of elliptic curves (see [7]). If $(r(x), \pi(x))$ is a family of abelian varieties with $\pi(x) = \zeta_s(f_1(x) + f_2(x)\sqrt{f(x)})$, then $(f_1(x), f_2(x)) \bmod r(x)$ is a solution of the system

$$\mathrm{N}_{K_1/\mathbb{Q}(x)}(\zeta_s(X + Y\sqrt{-f}) - 1) = \Phi_k(X^2 + fY^2) = 0, \tag{11}$$

where $K_1 = \mathbb{Q}(x, \zeta_s, \sqrt{-f})$. Hence to construct sparse families we should find polynomials $r(x) \in \mathbb{Q}[x]$ and $f(x) \in \mathbb{Z}[x]$, where $r(x)$ is irreducible and $f(x)$ satisfies Lemma 16, such that system (11) has solutions in the number field $L = \mathbb{Q}[x]/(r(x))$, and take f_1, f_2 to be lifts of these solutions. Such number fields are described in the following lemma, which generalizes Lemma 3.

Lemma 22. *Let $f \in \mathbb{Z}[x]$ satisfy Lemma 16 and $\deg f = 1, 2$. Let $r(x) \in \mathbb{Q}[x]$ be irreducible such that $\zeta_s, \zeta_k, \sqrt{-\bar{f}} \in L = \mathbb{Q}[x]/(r(x))$, where a bar denotes reduction mod $r(x)$. Then system* (11) *has solutions in L of the form*

$$X = \frac{\zeta_s^{-1} + \zeta_k\zeta_s}{2}, \quad Y = \pm\frac{\zeta_s^{-1} - \zeta_k\zeta_s}{2\sqrt{-\bar{f}}}. \tag{12}$$

Proof. As in the proof of Lemma 6 we first show that solutions in the field of fractions of $S = \mathbb{Q}[x, \zeta_s, \zeta_k, \sqrt{-f}]$ are of the above form. Then for a prime ideal P in S over r reduction mod PS_P yields the desired result by Lemma 7.

Hence we have the following algorithm; in the next section we give a simplified version to construct complete families with variable discriminant.

Algorithm 23. Input: A number field L containing primitive roots of unity ζ_s, ζ_k. Output: A sparse family $(r(x), \pi(x))$ of $\varphi(s)$-dimensional ordinary abelian varieties with embedding degree k, or $\emptyset$.

1. Find $r(x) \in \mathbb{Q}[x]$ such that $L = \mathbb{Q}[x]/(r(x))$.
2. Let $f_1 \in \mathbb{Q}[x]$ be the lift of $X = \frac{\zeta_s^{-1}+\zeta_s\zeta_k}{2}$ with $\deg f_1 < \deg r$.
3. If $f_1 \neq 0$ and $2f_1(x) \in \mathbb{Z}$ for some $x \in \mathbb{Z}$, let $f(x) = a_2x^2 + a_1x + a_0$ for integers $a_0, a_1, a_2 \in [-m, m]$, where $a_2 > 0$ and $m \in \mathbb{Z}$.
4. If f is square-free and $\sqrt{-\bar{f}} \in L$, let $f_2 \in \mathbb{Q}[x]$ be the lift of $Y = \frac{\zeta_s^{-1}-\zeta_s\zeta_k}{2\sqrt{-\bar{f}}}$ with $\deg f_2 < \deg r$.
5. Let $\pi(x) = \zeta_s\big(f_1(x) + f_2(x)\sqrt{-f(x)}\big)$.
6. Return $(r(x), \pi(x))$ if $q(x) = f_1^2(x) + f_2^2(x)f(x)$ represents primes.

Note that the resulting families have ρ-value

$$\rho = \frac{2g \max\{\deg f_1, \deg f_2 + 1\}}{\deg r} \leq 2g.$$

We now show how to construct sparse families of ordinary abelian surfaces with $k = 3, 4, 6$ and $\rho = 2$. These families are analogous to constructions for elliptic curves with $k = 3, 4, 6$ and $\rho = 1$ due to Miyaji et al. [25], Scott and Barreto [32], and Galbraith et al. [15].

Example 24. Let $s = 3, 4$, and $K = \mathbb{Q}(\zeta_s)$. Let $k = 3, 4, 6$, and $\zeta_k \in L = K = \mathbb{Q}[x]/(r(x))$ for $r(x) \in \mathbb{Q}[x]$. In order to construct a family $(r(x), \pi(x))$ with $\pi(x) = \zeta_s(f_1(x) + f_2(x)\sqrt{-f(x)})$ and $\rho = 2$, we must find a polynomial $f(x) \in \mathbb{Z}[x]$ as in step 4 of Algorithm 23 such that f_2 is constant. Since f_2 is the lift of $Y = (\zeta_s^{-1} - \zeta_s\zeta_k)/2\sqrt{-\bar{f}}$, we must have $Y \in \mathbb{Q}$. We can assume $Y = 1$, since $c^2 f$ and Y/c yield the same family for each $c \in \mathbb{Q}^\times$. Then for fixed $\zeta_s, \zeta_k \in L$, $\bar{f}$ is uniquely determined by $\bar{f} = -(\zeta_s^{-1} - \zeta_s\zeta_k)^2/4 = a\bar{x} + b$ for some $a, b \in \mathbb{Q}$. So we can take $f = ax + b + cr(x)$ for $c \in \mathbb{Q}$, $c > 0$. As f_1 we take the lift of $X = (\zeta_s^{-1} - \zeta_s\zeta_k)/2$. If $f_1 \neq 0$, $2f_1(x) \in \mathbb{Z}$ for some $x \in \mathbb{Z}$, and $q(x)$ represents primes, we obtain the desired family. For example, we have the following families with $\rho = 2$:

$$\begin{aligned}
&k = 3,\\
&\quad r(x) = 4x^2 + 2x + 1,\\
&\quad \pi(x) = \tfrac{\zeta_3}{6}\big(6x + 3 + \sqrt{-(12x^2 + 60x + 3)})\big),\\
&k = 4,\\
&\quad r(x) = 4x^2 + 1,\\
&\quad \pi(x) = \tfrac{i}{2}\big(-2x - 1 + \sqrt{-(12x^2 + 4x + 3)}\big),\\
&k = 6,\\
&\quad r(x) = 4x^2 - 2x + 1,\\
&\quad \pi(x) = \tfrac{\zeta_3}{2}\big(-2x - 1 + \sqrt{-(12x^2 - 4x + 3)}\big).
\end{aligned}$$

Example 25. Let $k = 8, s = 4$, and $L = \mathbb{Q}(\zeta_8)$. For $f = 7x^2 - 10x + 7$ we have $f \bmod \Phi_8(x) = -(-2\zeta_8^3 + 2\zeta_8^2 - \zeta_8 - 1)^2$. We have the following family with $\rho = 3$:

$$r(x) = \Phi_8(x),$$
$$\pi(x) = \tfrac{i}{2}\big(-x^2 + x + (2x^2 + 3x + 2)\sqrt{-(7x^2 - 10x + 7)}\big).$$

8 Complete families with variable discriminant

In this section we modify Algorithm 23 to construct complete families with variable discriminant $(r(x), \pi(x))$, where $\pi(x) = \zeta_s(f_1(x) + f_2(x)\sqrt{-f(x)})$ and $f(x) = ax + b$. Substituting $x \leftarrow (x - b)/a$, we can assume that $f = x$. Then by Lemma 22, $L = \mathbb{Q}[x]/(r(x))$ is a number field containing ζ_s, ζ_k, and $\sqrt{-\bar{x}}$. Let us note that a polynomial $r(x) \in \mathbb{Q}[x]$ such that $L = \mathbb{Q}[x]/(r(x))$ and $\sqrt{-\bar{x}} \in L$ can be obtained as the minimal polynomial of a primitive element $z \in L$ such that $\sqrt{-z} \in L$. Hence we have the following variant of Algorithm 23.

Algorithm 26. Input: A number field L such that $\zeta_s, \zeta_k \in L$. Output: A complete family with variable discriminant $(r(x), \pi(x))$ of $\varphi(s)$-dimensional ordinary abelian varieties with embedding degree k, or $\emptyset$.

1. Find a primitive element $z \in L$ such that $\sqrt{-z} \in L$.
2. Let $r(x)$ be the minimal polynomial of z and $L = \mathbb{Q}[x]/(r(x))$.
3. Let $X = \frac{\zeta_s^{-1} + \zeta_s\zeta_k}{2}$ and $Y = \frac{\zeta_s^{-1} - \zeta_s\zeta_k}{2\sqrt{-\bar{x}}}$ for all $\zeta_s, \zeta_k \in L$.
4. Let $f_1(x), f_2(x) \in \mathbb{Q}[x]$ be lifts of X, Y with $\deg f_i < \deg r$, $i = 1, 2$.
5. Let $\pi(x) = \zeta_s(f_1(x) + f_2(x)\sqrt{-x})$.
6. Return $(r(x), \pi(x))$ if $f_1 \neq 0$, $2f_1(x) \in \mathbb{Z}$ for some $x \in \mathbb{Z}$, and $q(x) = f_1^2(x) + xf_2^2(x)$ represents primes.

The resulting families have ρ-value

$$\rho = \frac{g \max\{2\deg f_1, 1 + 2\deg f_2\}}{\deg r} \leq \frac{g(2\deg r - 1)}{\deg r} < 2g.$$

In the examples below we take as L the cyclotomic field $L = \mathbb{Q}(\zeta_s, \zeta_k) = \mathbb{Q}(\zeta_l)$, where $l = \mathrm{lcm}(s, k)$. A crucial step in the above algorithm is to find a primitive element $z \in L$ such that $\sqrt{-z} \in L$, which can be chosen in the following ways:

- If l is odd, then $\sqrt{\zeta_l} = \pm\zeta_l^{(l+1)/2}$, so we can take $z = \zeta_{2l} = -\zeta_l$ and $r(x) = \Phi_{2l}(x)$. Similarly, if $l/2$ is odd, we can take $r(x) = \Phi_l(x)$.
- If $4|l$, then $\sqrt{\pm\zeta_l} \notin \mathbb{Q}(\zeta_l)$, but there may exist $a \in \mathbb{Z}$ such that $\sqrt{-\zeta_l/a} \in \mathbb{Q}(\zeta_l)$. Then we can take $z = \zeta_l/a$ and $r(x) = \Phi_l(ax)$.
- As in the method of Kachisa, Schaefer, Scott [22] we can vary elements $z_0 = a_0 + a_1\zeta_l + \cdots + a_{\varphi(l)-1}\zeta_l^{\varphi(l)-1}$, which have small integer coefficients in the cyclotomic basis, and use $z = -z_0^2$.

In the examples below we will also give a necessary condition on discriminant d so that $q(dx^2)$ could represent primes.

Example 27. (i) Let $k = 27, s = 3$, and $L = \mathbb{Q}(\zeta_{27})$. We obtain the complete family with variable discriminant $d \equiv 3 \pmod 8$ and $\rho = 2.11$

$$r(x) = \Phi_{54}(x),$$
$$\pi(x) = \tfrac{\zeta_3}{2}\big(x^9 - x^5 - 1 - (x^9 - x^4 - 1)\sqrt{-x}\big).$$

For example, we can generate the following parameters:

$d = 987$

$x = 1$

$r = 790148551064734600930099312825768542489884551187609503$ (179-bits prime)

$\pi = \frac{\zeta_3}{2}(888903004305345672187555919 - 888903004306281391354749065\sqrt{-987})$

$q = 19516669211298861382258201587090168045690156924964823659$

$y^2 = x^6 + x^3 + 151105907749622646118621216513432167109227634777454854520$

$\rho = 2.078$

$d = 2091$

$x = 3$

$r = 876471422925486228668169992755608896154428941533110512882066273701054252154 63$ (255-bits prime)

$\pi = \frac{\zeta_3}{2}(29605260055022084110471960720957774487 9 - 888157801650662530394935347022383083571\sqrt{-2091})$

$q = 412379804486441270587675183690854571980192627889184083816045552664656156778750593$

$y^2 = x^6 + x^3 + 565781593297967606888483041245436831680975502419728920009099985777652395651749 52$

$\rho = 2.094$

(ii) Similarly, for $k = 54$, $s = 3$, and $L = \mathbb{Q}(\zeta_{54})$, we obtain the complete family with variable discriminant $d \equiv 3 \pmod 8$ and $\rho = 2.11$

$$r(x) = \Phi_{54}(x),$$
$$\pi(x) = \tfrac{\zeta_3}{2}\big(x^9 + x^5 - 1 + (x^9 + x^4 - 1)\sqrt{-x}\big).$$

Example 28. (i) Let $s = 3$, $k = 12$ and $L = \mathbb{Q}(\zeta_{12})$; then $\sqrt{-\zeta_{12}/2} \in L$. We have the following family with discriminant $d \equiv 3 \pmod 8$ and $\rho = 3.5$:

$$r(x) = \Phi_{12}(2x),$$
$$f_1(x) = \tfrac{\zeta_3}{2}\big(-8x^3 + 4x^2 - 1 + (8x^3 - 4x - 1)\sqrt{-x}\big)$$

Example 29. Let $k = 8$, $s = 4$, and $L = \mathbb{Q}(\zeta_8)$. Let $r(x)$ be the minimal polynomial of $z = -(\zeta_8 - 1)^2$. We have the following family with discriminant $d = 1, 7 \pmod 8$ and $\rho = 7/2$:

$$r(x) = x^4 + 4x^3 + 8x^2 - 8x + 4,$$
$$\pi(x) = \tfrac{i}{24}\big(-3x^3 - 15x^2 - 36x + 6 + (x^3 + 5x^2 + 16x + 2)\sqrt{-x}\big).$$

Table 1. Best ρ-values of complete families with variable discriminant $((r(x), \pi(x))$ such that $\deg r(x) < 25$, which are given in the appendix.

k	ρ	d	$\deg r$	k	ρ	d	$\deg r$
2	3.00	3 (mod 8)	2	22	2.7	3 (mod 8)	10
3	3.00	$1, 3, 7, 9$ (mod 10)	2	24	3.75	$2, 10, 11, 19$ (mod 24)	8
4	3.00	3 (mod 4)	2	26	2.25	3mod8	24
5	3.00	1 (mod 4)	8	27	2.11	3mod8	18
6	3.00	any	2	28	3.08	3mod8	24
7	2.50	3mod8	12	30	2.75	3mod8	8
8	3.50	$1, 7$ (mod 8)	4	33	2.30	3mod8	20
9	2.33	3mod8	6	36	3.50	3mod8	12
10	3.50	any	8	39	2.33	1mod4	24
11	2.40	1 (mod 4)	20	42	2.83	3mod8	12
12	3.50	3mod8	4	45	2.58	3mod8	24
13	2.25	3mod8	24	54	2.11	3mod8	18
14	2.50	3mod8	12	60	3.75	3mod8	14
15	2.75	3mod8	8	66	2.30	3mod8	20
16	3.75	some	8	78	2.42	3mod4	24
18	2.33	3mod8	6	84	3.75	3mod8	24
20	3.75	3mod8	8	90	2.58	3mod8	24
21	2.66	1 (mod 4)	12				

References

1. Barreto, P.S.L.M., Naehrig, M.: Pairing-friendly elliptic curves of prime order. In Selected Areas in Cryptography – SAC 2005. LNCS, vol. 3897, pp. 319-331. Springer, Heidelberg (2006)
2. Boneh, D., Franklin, M.: Identity-based encryption from the Weil pairing. In Advances in Cryptology Crypto 2001. LNCS, vol. 2139, pp. 213-229. Springer, Berlin (2001). Full version: SIAM J. Comput. 32(3), 586-615 (2003).
3. Boneh, D., Lynn, B., Shacham, H.: Short signatures from the Weil pairing. In Advances in Cryptology Asiacrypt 2001. LNCS, vol. 2248, pp. 514-532. Springer, Berlin (2002). Full version: J. Cryptol. 17, 297-319 (2004)
4. Brezing, F., Weng, A.: Elliptic curves suitable for pairing based cryptography. Des. Codes Cryptogr. 37, 133-141 (2005)
5. Cardona, G., Quer, J.: Field of moduli and field of definition for curves of genus 2. Available at: http://arxiv.org/abs/math/0207015.
6. Cardona, G., Quer, J.: Curves of genus 2 with group of automorphisms isomorphic to D_8 or D_{12}. Trans. Amer. Math. Soc. 359, 2831-2849 (2007)
7. On constructing families of pairing-friendly elliptic curves with variable discriminant. INDOCRYPT-2011. LNCS, vol. 7107, pp. 310-319. Springer, Berlin (2011).
8. Freeman, D.: Constructing pairing-friendly elliptic curves with embedding degree 10. In Algorithmic Number Theory Symposium – ANTS-VII. LNCS, vol. 4076, pp. 452-465. Springer, Berlin (2006).
9. Freeman, D.: A generalized Brezing-Weng algorithm for constructing pairing-friendly ordinary abelian varieties. In: Pairing-Based Cryptography – Pairing 2008. LNCS, vol. 5209, pp. 146-163. Springer, Heidelberg (2008)
10. Freeman, D., Satoh, T.: Constructing pairing-friendly hyperelliptic curves using Weil restriction. J. Number Theory 131, 959-983 (2011)
11. Freeman, D., Scott, M., Teske, E.: A taxonomy of pairing-friendly elliptic curves. J. Cryptol. 23, 224-280 (2010)
12. Freeman, D., Stevenhagen, P., Streng, M.: Abelian varieties with prescribed embedding degree. In: Algorithmic Number Theory – ANTS VIII. LNCS, vol. 5011, pp. 60-73. Springer, Heidelberg (2008)
13. Furukawa, E., Kawazoe, M., Takahashi, T.: Counting points for hyperelliptic curves of type $y^2 = x^5 + ax$ over finite prime fields. In Selected Areas in Cryptography – SAC 2003. LNCS, vol. 3006, pp. 26-41. Springer, Heidelberg (2004)
14. Galbraith, S.: Supersingular curves in cryptography. In ASIACRYPT 2001. LNCS, 2248, pp. 495–513. Springer, Berlin (2001).

15. Galbraith, S., McKee, J., Valença, P.: Ordinary abelian varieties having small embedding degree. Finite Fields Appl. 13, 800–814 (2007)
16. Gaudry, P., Schost, E.: On the invariants of the quotients of the Jacobian of a curve of genus 2. In Applied Algebra, Algebraic Algorithms and Error-Correcting Codes — AAECC- 14. LNCS, vol. 2227, pp. 373-386. Springer, Heidelberg (2001)
17. Guillevic, A., Vergnaud, D.: Genus 2 Hyperelliptic Curve Families with Explicit Jacobian Order Evaluation and Pairing-Friendly Constructions. To appear in Pairing-Based Cryptography – Pairing 2012, LNCS.
18. Howe, E., Zhu, H.: On the existence of absolutely simple abelian varieties of a given dimension over an arbitrary field. J. Number Theory 92, 139-163 (2002)
19. Igusa, J.: Arithmetic Variety of Moduli for Genus Two. Ann. Math. 72, 612-649 (1960)
20. Joux A.: A one round protocol for tripartite Diffie–Hellman. In Algorithmic Number Theory Symposium – ANTS-IV. LNCS, vol. 1838, pp. 385-393. Springer, Berlin (2000). Full version: J. Cryptol. 17, 263-276 (2004)
21. Kachisa, E.: Generating More Kawazoe-Takahashi Genus 2 Pairing-Friendly Hyperelliptic Curves. In: Pairing-Based Cryptography – Pairing 2010. LNCS, vol. 6487, pp. 312-326. Springer, Heidelberg (2010).
22. Kachisa, E., Schaefer, E., Scott, M.: Constructing Brezing-Weng pairing friendly elliptic curves using elements in the cyclotomic field, in *Pairing-Based Cryptography–Pairing 2008*. LNCS, vol. 5209, pp. 126-135. Springer, Heidelberg (2008)
23. Kawazoe, M., Takahashi, T.: Pairing-friendly ordinary hyperelliptic curves with ordinary Jacobians of type $y^2 = x^5 + ax$. In: Pairing-Based Cryptography – Pairing 2008. LNCS, vol. 5209, pp. 164-177. Springer, Heidelberg (2008)
24. Lang, S.: Algebraic Number Theory. Graduate Texts in Mathematics, Vol. 110. Springer, Berlin (1994)
25. Miyaji, A., Nakabayashi, M., Takano, S.: New explicit conditions of elliptic curve traces for FR-reduction. IEICE Trans. Fundam. E84-A(5), 1234–1243 (2001)
26. Milne, J.S.: Abelian varieties. In: Cornell, G., Silverman, J. (eds.) Arithmetic Geometry 103-150. Springer, New York (1986)
27. Murphy, A., Fitzpatrick, N.: Elliptic curves for pairing applications. Available at: http://eprint.iacr.org/2005/302
28. Maisner, D., Nart, E.: Abelian surfaces over finite fields as Jacobians. Experimental Mathematics 11, 321-337 (2002). With an appendix by Everett W. Howe.
29. Menezes, A., Okamoto, T., Vanstone, S.: Reducing elliptic curve logarithms to logarithms in a finite field. IEEE Trans. Inf. Theory 39, 1639-1646 (1993)
30. Mestre, J.F.: Construction de courbes de genre 2 à partir de leurs modules. In Effective methods in algebraic geometry (Castiglioncello, 1990), pages 313-334. Birkhäuser, Boston, MA (1991)
31. Rubin, K., Silverberg, A.: Using abelian varieties to improve pairing-based cryptography. J. Cryptol. 22, 330-364 (2009)
32. Scott, M., Barreto, P.S.L.M.: Generating more MNT elliptic curves. Des. Codes Cryptogr. 38, 209–217 (2006)
33. Shaska, T., Voelklein, H.: Elliptic subfields and automorphisms of genus 2 function fields. Algebra, arithmetic and geometry with applications (West Lafayette, IN, 2000), 703–723. Springer, Heidelberg (2004)
34. Silverman, J.: The Arithmetic of Elliptic Curves. Springer, Berlin (1986).
35. Sakai, R., Ohgishi, K., Kasahara, M.: Cryptosystems based on pairings. In 2000 Symposium on Cryptography and Information Security – SCIS 2000, Okinawa, Japan, 2000.
36. Sutherland, A.: Computing Hilbert class polynomials with the Chinese remainder theorem. Math. Comp. 80, 501-538 (2011)
37. Tate, J.: Classes d'isogénie des variétés abéliennes sur un corps fini. (d'aprés T. Honda.) Séminarie Bourbaki 1968/69, exposé 352. Lect. Notes in Math., vol. 179, pp. 95-110. Springer (1971)
38. Tate, J.: Endomorphisms of abelian varieties over finite fields. Inventiones Mathematicae 2 (1966)
39. Waterhouse, W.C.: Abelian varieties over finite fields. Ann. Sci. École Norm. Sup. 2, 521-560 (1969)
40. Waterhouse, W.C., Milne, J.S.: Abelian varieties over finite fields. Proc. Symp. Pure Math. 20, 53-64 (1971)

9 Appendix: Complete families $((r(x), \pi(x))$ with variable discriminant and best ρ-values such that $\deg r(x) < 25$.

$$
\begin{aligned}
k = 2, \quad & \rho = 3 \\
r(x) &= \Phi_6(x) \\
\pi(x) &= \tfrac{\zeta_3}{2}\big(2x - 1 + x\sqrt{-x}\big)
\end{aligned}
$$

$$
\begin{aligned}
k = 3, \quad & \rho = 3 \\
r(x) &= x^2 + 11x + 49 \\
\pi(x) &= \tfrac{\zeta_3}{70}\big(7x + 56 + (x - 17)\sqrt{-x}\big)
\end{aligned}
$$

$$
\begin{aligned}
k = 4, \quad & \rho = 3 \\
r(x) &= x^2 - 6x + 25 \\
\pi(x) &= \tfrac{i}{40}\big(5x + 5 + (x + 9)\sqrt{-x}\big)
\end{aligned}
$$

$$
\begin{aligned}
k = 5, \quad & \rho = 3 \\
r(x) &= \Phi_{30}(x) \\
\pi(x) &= \tfrac{\zeta_3}{2}\big(-x^6 + x^5 + x - 1 - (x^3 + x^2)\sqrt{-x}\big)
\end{aligned}
$$

$$
\begin{aligned}
k = 6, \quad & \rho = 3 \\
r(x) &= \Phi_6(x) \\
\pi(x) &= \tfrac{\zeta_3}{2}\big(x - 2 + (x - 1)\sqrt{-x}\big)
\end{aligned}
$$

$$
\begin{aligned}
k = 7, \quad & \rho = 2.5 \\
r(x) &= \Phi_{42}(x) \\
\pi(x) &= \tfrac{\zeta_3}{2}\big(x^7 + x^4 - 1 + (x^7 + x^3 - 1)\sqrt{-x}\big)
\end{aligned}
$$

$$
\begin{aligned}
k = 8, \quad & \rho = 3.5 \\
r(x) &= x^4 + 4x^3 + 8x^2 - 8x + 4 \\
\pi(x) &= \tfrac{i}{24}\big(-3x^3 - 15x^2 - 36x + 6 + (x^3 + 5x^2 + 16x + 2)\sqrt{-x}\big)
\end{aligned}
$$

$$
\begin{aligned}
k = 9, \quad & \rho = 2.33 \\
r(x) &= \Phi_{18}(x) \\
f_1(x) &= \tfrac{\zeta_3}{2}\big(x^6 - x^3 + 1 + (x^3 + x^2 - 1)\sqrt{-x}\big)
\end{aligned}
$$

$$
\begin{aligned}
k = 10, \quad & \rho = 3.5 \\
r(x) &= \Phi_{30}(5x) \\
\pi(x) &= \tfrac{\zeta_3}{2}\big(-78125x^7 - 15625x^6 + 3125x^5 + 625x^4 + 125x^3 + 25x^2 - 2 \\
&\qquad + (15625x^6 - 6250x^5 - 1250x^4 - 250x^3 + 25x^2)\sqrt{-x}\big)
\end{aligned}
$$

$$k=11,\quad \rho=2.4$$
$$r(x)=\Phi_{66}(x)$$
$$f_1(x)=\tfrac{\zeta_3}{2}\big(-x^{12}+x^{11}+x-1+(x^6+x^5)\sqrt{-x}\big)$$

$$k=12,\quad \rho=3.5$$
$$r(x)=\Phi_{12}(2x)$$
$$f_1(x)=\tfrac{\zeta_3}{2}\big(-8x^3+4x^2-1+(8x^3-4x-1)\sqrt{-x}\big)$$

$$k=13,\quad \rho=2.25$$
$$r(x)=\Phi_{78}(x)$$
$$f_1(x)=\tfrac{\zeta_3}{2}\big(x^{13}-x^7-1+(x^{13}-x^6-1)\sqrt{-x}\big)$$

$$k=14,\quad \rho=2.5$$
$$r(x)=\Phi_{42}(x)$$
$$\pi(x)=\tfrac{\zeta_3}{2}\big(x^7-x^4-1+(-x^7+x^3+1)\sqrt{-x}\big)$$

$$k=15,\quad \rho=2.75$$
$$r(x)=\Phi_{30}(x)$$
$$f_1(x)=\tfrac{\zeta_3}{2}\big(x^5-x^3-1+(x^5-x^2-1)\sqrt{-x}\big)$$

$$k=16,\quad \rho=3.75$$
$$r(x)=x^8+76x^6+678x^4+332x^2+1$$
$$\pi(x)=\tfrac{i}{30464}\big(29x^7-29x^6+2173x^5-2173x^4+17175x^3-17175x^2-21009x+5777$$
$$+(5777x^7-229x^6+439081x^5-17389x^4+3918979x^3-154335x^2+1935139x$$
$$-71215)\sqrt{-x}\big)$$

$$k=18,\quad \rho=2.33$$
$$r(x)=\Phi_{18}(x)$$
$$\pi(x)=\tfrac{\zeta_3}{2}\big(x^3-x^2-1+(-x^3+x+1)\sqrt{-x}\big)$$

$$k=20,\quad \rho=3.75$$
$$r(x)=\Phi_{20}(2x)$$
$$\pi(x)=\tfrac{i}{2}\big(-64x^6+32x^5+16x^4-4x^2+1+(128x^7-32x^5-4x^2-1)\sqrt{-x}\big)$$

$$k=21,\quad \rho=2.66$$
$$r(x)=\Phi_{42}(x)$$
$$\pi(x)=\tfrac{\zeta_3}{2}\big(-x^8+x^7+x-1+(x^4+x^3)\sqrt{-x}\big)$$

$k = 22, \quad \rho = 2.7$

$r(x) = \Phi_{22}(x)$

$\pi(x) = \frac{\zeta_3}{2}\big(x^{11} - x^8 - 1 + (-x^{13} + x^5 + x^2)\sqrt{-x}\big)$

$k = 24, \quad \rho = 3.75$

$r(x) = x^8 + 80x^6 + 456x^4 + 320x^2 + 16$

$\pi(x) = \frac{\zeta_3}{10752}\big(- 176x^7 + 28x^6 - 14040x^5 + 2240x^4 - 77088x^3 + 12656x^2 - 40480x + 1792$
$+(177x^7 + 34x^6 + 14150x^5 + 2704x^4 + 79892x^3 + 14248x^2 + 50552x + 9024)\sqrt{-x}\big).$

$k = 26, \quad \rho = 2.25$

$r(x) = \Phi_{78}(x)$

$\pi(x) = \frac{\zeta_3}{2}\big(x^{13} + x^7 - 1 - (x^{13} + x^6 - 1)\sqrt{-x}\big)$

$k = 27, \quad \rho = 2.11$

$r(x) = \Phi_{54}(x)$

$\pi(x) = \frac{\zeta_3}{2}\big(x^9 - x^5 - 1 + (-x^9 + x^4 + 1)\sqrt{-x}\big)$

$k = 28, \quad \rho = 3.08$

$r(x) = \Phi_{84}(2x)$

$\pi(x) = \frac{\zeta_3}{2}\big(16384x^{14} - 32x^5 - 1 + (262144x^{18} - 131072x^{17} + 65536x^{16} + 32768x^{15}$
$-4096x^{12} - 1024x^{10} + 64x^6 - 4x^2 - 1)\sqrt{-x}\big)$

$k = 30, \quad \rho = 2.75$

$r(x) = \Phi_{30}(x)$

$\pi(x) = \frac{\zeta_3}{2}\big(x^5 + x^3 - 1 + (-x^5 - x^2 + 1)\sqrt{-x}\big)$

$k = 33, \quad \rho = 2.3$

$r(x) = \Phi_{33}(-x)$

$f_1(x) = \frac{\zeta_3}{2}\big(x^{11} + x^6 - 1 + (x^{11} + x^5 - 1)\sqrt{-x}\big)$

$k = 36, \quad \rho = 3.5$

$r(x) = \Phi_{36}(2x)$

$f_1(x) = \frac{\zeta_3}{2}\big(64x^6 - 32x^5 - 1 + (1024x^10 + 512x^9 - 128x^7 - 16x^4 - 1)\sqrt{-x}\big)$

$k = 39, \quad \rho = 2.33$

$r(x) = \Phi_{78}(x)$

$f_1(x) = \frac{\zeta_3}{2}\big(- x^{14} + x^{13} + x - 1 - (x^7 + x^6)\sqrt{-x}\big)$

$$k = 42, \quad \rho = 2.83$$
$$r(x) = \Phi_{42}(x)$$
$$\pi(x) = \tfrac{\zeta_3}{2}\big(x^7 + x^5 - 1x + (x^8 + x^3 - x)\sqrt{-x}\big)$$

$$k = 45, \quad \rho = 2.58$$
$$r(x) = \Phi_{90}(x)$$
$$\pi(x) = \tfrac{\zeta_3}{2}\big(x^{15} + x^8 - 1(x^{15} + x^7 - 1)\sqrt{-x}\big)$$

$$k = 54, \quad \rho = 2.11$$
$$r(x) = \Phi_{54}(x)$$
$$\pi(x) = \tfrac{\zeta_3}{2}\big(x^9 + x^5 - 1 + (x^9 + x^4 - 1)\sqrt{-x}\big)$$

$$k = 60, \quad \rho = 3.75$$
$$r(x) = \Phi_{60}(2x)$$
$$\pi(x) = \tfrac{\zeta_3}{2}\big(32768x^{15} + 16384x^{14} + 4096x^{12} - 256x^8 - 64x^6 - 16x^4 + 1$$
$$+(4096x^{12} + 1024x^{10} - 128x^7 + 32x^5 - 4x^2 - 1)\sqrt{-x}\big)$$

$$k = 66, \quad \rho = 2.3$$
$$r(x) = \Phi_{66}(x)$$
$$\pi(x) = \tfrac{\zeta_3}{2}\big(x^{11} - x^6 - 1 + (-x^{11} + x^5 + 1)\sqrt{-x}\big)$$

$$k = 78, \quad \rho = 2.42$$
$$r(x) = \Phi_{78}(x)$$
$$\pi(x) = \tfrac{\zeta_3}{2}\big(x^{13} - x^8 - 1 + (x^{14} - x^6 - x)\sqrt{-x}\big)$$

$$k = 84, \quad \rho = 3.75$$
$$r(x) = \Phi_{84}(2x)$$
$$\pi(x) = \tfrac{1}{2}\mathrm{i}g(16384x^{14} + 2x - 1 + (-4194304x^{22} - 131072x^{17} + 65536x^{16} - 4096x^{12}$$
$$-2048x^{11} - 1024x^{10} + 256x^8 + 64x^6 + 16x^4 - 4x^2 - 1)\sqrt{-x}\big)$$

$$k = 90, \quad \rho = 2.58$$
$$r(x) = \Phi_{90}(x)$$
$$f_1(x) = \tfrac{1}{2}\big(x^{15} - x^8 - 1 + (-x^{15} + x^7 + 1)\sqrt{-x}\big).$$