A new method of choosing primitive elements for Brezing-Weng families of pairing friendly elliptic curves

Kisoon Yoon*

Abstract

In this paper we present a new method of choosing primitive elements for Brezing-Weng families of pairing friendly elliptic curves with small rho-value, and we improve on previously-known best rho-values of families [10] for the cases $k = 16$, 22, 28 and 46. Our construction uses fixed discriminants.

1 Introduction

1.1 Pairing friendly elliptic curves

Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$ and let r be a prime number. Let $k \geq 1$ be the smallest positive integer such that the group $E[r]$ of r-torsion points of E is contained in $E(\mathbb{F}_{q^k})$. Then the group μ_r of r^{th} roots of unity lies in $\mathbb{F}_{q^k}$ and there exist non-degenerate bilinear pairings $e : G_1 \times G_2 \to \mu_r$, where G_1 and G_2 are suitable subgroups of $E[r]$ of order r. The existence of such pairings makes it possible to reduce the Elliptic Curve Discrete Logarithm Problem (ECDLP) [16], [11] on E to the Discrete Logarithm Problem (DLP) on $\mu_r \subset \mathbb{F}_{q^k}^{\times}$ for which there exist sub-exponential time algorithms [1].

*Laboratoire de Mathématiques Nicolas Oresme, CNRS UM3 6139, Université de Caen Basse-Normandie, 14032 Caen cedex, France. kisoon.yoon@unicaen.fr This paper was written while the author was a Ph. D. student at the Université de Caen Basse-Normandie funded by NSHC Co., Ltd., Korea. I would like to thank professor John Boxall for his advice and attention to my work.

Date: March 9, 2013

Key words and phrases. Elliptic curves, finite fields, pairing-based cryptography.

On the other hand, on the constructive side, cryptographic protocols based on pairings were first proposed in [13], [21], [5] and many other protocols have been proposed and implementations need high speed algorithms and elliptic curves having prescribed properties. Generally, the Tate pairing is preferred to the Weil pairing for the reason of efficiency. Other pairings are introduced more recently, many of which are special cases of optimal pairings introduced by Vercauteren [22] and Hess [12].

To avoid the known attacks mentioned above, the integer k must be sufficiently large in order that the DLP in $\mathbb{F}_{q^k}^{\times}$ is infeasible, but not so large that the computations in $\mathbb{F}_{q^k}$ become too slow.

We define the *embedding degree* of an elliptic curve E the least positive integer $k \geq 1$ such that r divides $q^k - 1$. From [2], we know that $E[r] \subset E(\mathbb{F}_{q^k})$ for $k \geq 2$ and that elliptic curves having of low embedding degree are very rare. There exists the heuristic asymptotic formula for the number of pairing friendly elliptic curves, which explain concretely about the rareness of such curves along the rho-values [6].

An elliptic curve is called *pairing-friendly* if r is suitable for cryptography and if k is small. The following more precise definition suggested by Freeman, Scott et Teske [10].

Definition 1.1. An elliptic curve E over $\mathbb{F}_q$ is said to be *pairing friendly* if following two conditions are satisfied:

(1) There exists a prime number r such that $r \geq \sqrt{q}$ and r divides $\sharp E(\mathbb{F}_q)$, and

(2) The embedding degree of E is bounded by $\log_2(r)/8$.

Because the embedding degree of a supersingular curve belongs to $\{1, 2, 3, 4, 6\}$ [17], [20], any supersingular curve having a subgroup of sufficiently large prime order is pairing friendly. It is easy to construct examples of super-singular elliptic curves (See § 3 of [10] for details). But for higher security levels higher embedding degrees are more appropriate so ordinary elliptic curves must be used. The existence of an ordinary elliptic curve E of embedding degree k over a finite field $\mathbb{F}_q$ with q elements such that $E(\mathbb{F}_q)$ contains a subgroup of order r implies existence of integers t, D and y such that

(1) q is a prime or a power of prime.

(2) r is a prime.

(3) t is relatively prime to q.

(4) $(t-1)^2 + Dy^2 \equiv 0 \pmod{r}$.

(5) $\Phi_k(t-1) \equiv 0 \pmod{r}$ where $\Phi_k(x)$ is the k-th cyclotomic polynomial.

(6) $4q - t^2 = Dy^2$ where $D \geq 1$ is a square-free integer, and y is an integer.

The integer t is the trace of the Frobenius endomorphism of E over $\mathbb{F}_q$ so that $\#E(\mathbb{F}_q) = q + 1 - t$. Deuring [8] showed that, if t is an integer satisfying the condition (3), then there exists an ordinary elliptic curve over $\mathbb{F}_q$ the number of points of which equals to $q+1-t$. The condition (6) means that the endomorphism ring of E is an order in the imaginary quadratic field $\mathbb{Q}(\sqrt{-D})$. Because the difficulty of explicit construction of E increases rapidly with the size $|D|$, in practice $|D|$ has to be small enough. So, it is desirable to consider D as constant. Therefore we can formulate the problem of the construction of pairing friendly ordinary elliptic curves as follows.

Given k and D, find the integers q, t, r and y that satisfy the conditions from (1) *to* (6).

For efficiency, it is preferable that the field size q is as small as possible with respect to r. So, as a measure of estimating elliptic curves, we define *rho-value* of an elliptic curve as follows

$$\rho = \frac{\log q}{\log r}. \tag{1}$$

Since $|t| \leq 2\sqrt{q}$, a rho-value is at least one. Naturally, the nearer to one is the rho-value, the better is an elliptic curve estimated.

Fix an integer $k \geq 2$ and a positive square-free integer D. A *parametrized family* of pairing friendly elliptic curve is a system of polynomials having rational coefficients $r(x)$, $t(x)$, $q(x)$ that represent simultaneously integers r, t, q that satisfy the conditions from (1) to (6). If there exist infinitely many solutions of the equation $t(x)^2 - 4q(x) = Dy^2$, we call the family a *sparse family*, and furthermore if y can be parametrized as $y(x)$ a polynomial of x, we call the family a *complete family*. With the polynomials $r(x)$ and $q(x)$ of a family, we define the *rho-value of the family* by

$$\rho_x = \frac{\deg q(x)}{\deg r(x)}. \tag{2}$$

A number of different constructions of sparse families and complete families can be found in the literature. A very detailed survey of results obtained up to about 2010 is in [10].

1.2 The Brezing-Weng method

In [7], Brezing and Weng proposed a general method of constructing complete families by means of algebraic extension of $\mathbb{Q}$. We recall a mild generalization of the algorithm. Fix an embedding degree k and a square-free positive integer D. A primitive k-th root of unity is denoted by ζ_k. The following is a brief description of the Brezing-Weng algorithm. Note that the output contains $y(x)$ because it produces complete families.

Algorithm 1.2. Brezing-Weng method.

INPUT: k: positive integer, D: a square-free positive integer
OUTPUT: A complete family of elliptic curves $(r(x), t(x), y(x), q(x))$

---

1. Choose an irreducible polynomial $r(x)$ such that $\sqrt{-D}$, $\zeta_k \in \mathbb{Q}[x]/(r(x))$.
   Let α be the image of x in $\mathbb{Q}[x]/(r(x))$ under the canonical isomorphism.

2. Calculate polynomials $t(x)$ and $y(x) \in \mathbb{Q}[x]$ such that $t(\alpha) = \zeta_k + 1$ and $y(\alpha) = \frac{(t(\alpha)-2)\sqrt{-D}}{-D}$.

3. Let $q(x) = \frac{1}{4}(t(x)^2 + Dy(x)^2) \in \mathbb{Q}[x]$.

4. If $t(x)$ and $y(x)$ represent integers, $q(x)$ represents prime numbers, and $r(x)$ represents almost prime numbers, then OUTPUT$((r(x), t(x), y(x), q(x)))$.
   Otherwise go to 1.

The element α in the algorithm is a primitive element of the field $K = \mathbb{Q}[x]/(r(x))$. We say that the polynomials $r(x)$, $t(x)$, $y(x)$ and $q(x)$ are *associated* to α.

The polynomial $r(x)$ is often taken to be a cyclotomic polynomial, i. e. a root of unity is taken as the primitive element of the field extension $K/\mathbb{Q}$ where $K = \mathbb{Q}(\zeta_k, \sqrt{-D})$. Kachisa, Schaefer and Scott [14] have used primitive elements other than roots of unity to construct some Brezing-Weng families having smaller rho-values. The article of Freeman, Scott and Teske [10] propose various constructions of complete families based on the method of Brezing-Weng. The table 5 of [10] presents the best rho-values of existing families for $k \leq 50$ known before about 2010. Improvements in rho-values arising from so-called variable discriminant families have recently been obtained in [9].

2 Primitive elements of the proposed form

2.1 Introduction

Fix an embedding degree k and let D be a square-free positive integer. Let ζ_k be a primitive k-th root of unity. Let $\sqrt{-D}$ a square root of $-D$. From now on K always denotes the extension field $\mathbb{Q}(\zeta_k, \sqrt{-D})$. Note that $K = \mathbb{Q}(\zeta_k)$ when $\sqrt{-D} \in \mathbb{Q}(\zeta_k)$. The conditions that $\sqrt{-D} \in \mathbb{Q}(\zeta_k)$ are discussed in [18]. We consider an element of the form

$$\alpha = \alpha(a, b, D, k) = (a + b\sqrt{-D})\zeta_k \in K \tag{3}$$

where a and b are rational numbers. We first study the conditions α to be a primitive element of the extension $K/\mathbb{Q}$.

Remark 2.1. In some cases, α is a primitive element of K for some chances of ζ_k and $\sqrt{-D}$, but not for others. This can only happen when $\sqrt{-D} \in \mathbb{Q}(\zeta_k)$. See the proof of the Theorem 2.6 for details of the cases when this happens.

Proposition 2.2. *Let α be as in (3). We can write the k-th power of the equality as*

$$\alpha^k = A + B\sqrt{-D}, \tag{4}$$

where A, $B \in \mathbb{Q}$. If $B \neq 0$, then α is a primitive element of the extension $K/\mathbb{Q}$.

Proof. Let $r(x)$ be the minimal polynomial of α such that $\mathbb{Q}(\alpha) \cong \mathbb{Q}[x]/(r(x))$. From (4), we know that α is a root of the polynomial $r_0(x) = x^{2k} - 2Ax + A^2 + DB^2$. If $B \neq 0$, then from (4) we obtain $\sqrt{-D} = \frac{x^k - A}{B}$ in $\mathbb{Q}[x]/(r(x))$. From (3) and using the fact that $r(x)$ divides $r_0(x)$, we obtain a representation $\zeta_k = \frac{-bx^{k+1} + (aB + Ab)x}{B(a^2 + b^2 D)}$ in $\mathbb{Q}[x]/(r(x))$. As a consequence, because both $\sqrt{-D}$ and ζ_k are in $\mathbb{Q}(\alpha)$, we have $K = \mathbb{Q}(\zeta_k, \sqrt{-D}) \subseteq \mathbb{Q}(\alpha)$. By the definition of α, clearly $\mathbb{Q}(\alpha) \subseteq K$. Therefore $K = \mathbb{Q}(\alpha)$. □

Remark 2.3. In the proof of the Proposition 2.2, we obtain the representations of ζ_k and $\sqrt{-D}$ in $\mathbb{Q}[x]/(r(x))$ under the condition that $B \neq 0$, from which we obtain immediately the polynomial representations $t(x) = \zeta_k + 1$, $y(x) = \frac{\sqrt{-D}(\zeta_k - 1)}{-D}$ and can compute $q(x) = \frac{1}{4}\left(t(x)^2 + Dy(x)^2\right)$. This procedure gives an outline of our construction, which is detailed in §2.2. In the cases where $B = 0$, there are triplets (a, b, D) such that $\alpha(a, b, D)$ is not a primitive element. We shall discuss this in Theorem 2.6.

Lemma 2.4. *Let $\xi = a + b\sqrt{-D}$ where $a, b \in \mathbb{Q}$, $b \neq 0$ and D is a square-free positive integer. Let k be a positive integer. Then ξ^k is a rational number if and only if one of followings holds.*

(i) $2|k$ *and* $\xi = r\sqrt{-D}$, *or*

(ii) $4|k$ *and* $\xi = r(1 \pm \sqrt{-1})$, *or*

(iii) $3|k$ *and* $\xi = r(1 \pm \sqrt{-3})$, *or*

(iv) $6|k$ *and* $\xi = r(3 \pm \sqrt{-3})$,

for a nonzero rational number r.

Proof. Note that we have $b \neq 0$ and $k > 0$ in the assumption. Define $T(a, b, D) = \{k \in \mathbb{Z} | \xi^k \in \mathbb{Q}\}$. We have $|\xi| = |\bar{\xi}|$ where $\bar{\xi}$ is the complex conjugation of ξ, so $\left|\frac{\bar{\xi}}{\xi}\right| = 1$. If $k \in T(a, b, D)$, then $k \in T(a, -b, D)$ also, and $\left(\frac{\bar{\xi}}{\xi}\right)^k \in \{-1, 1\}$, because the quotient is a rational number of absolute value 1. Therefore $\frac{\bar{\xi}}{\xi}$ is a $2k$-th root of unity contained in the quadratic field $\mathbb{Q}(\sqrt{-D})$.

(a) Suppose that $D \neq 1, 3$, then the only roots of unity contained in $\mathbb{Q}(\sqrt{-D})$ are 1 and -1. We have then $a - b\sqrt{-D} = a + b\sqrt{-D}$ or $a - b\sqrt{-D} = -(a + b\sqrt{-D})$. In the first case, $b = 0$ which contradicts the assumption. In the second case, $a = 0$ and $T(a, b, D) = 2\mathbb{Z}$ with $\xi = b\sqrt{-D}$.

(b) Suppose that $D = 1$. Let us write i for $\sqrt{-1}$. The roots of unities in $\mathbb{Q}(i)$ are ± 1 and $\pm i$. If $a - bi = a + bi$, then we have $b = 0$, a contradiction. If $a - bi = -(a + bi)$, then we have $T(a, b, D) = 2\mathbb{Z}$ with $\xi = bi$. If $a - bi = \pm i(a + bi)$, then we have $T(a, b, D) = 4\mathbb{Z}$ with $\xi = a(1 \mp i)$.

(c) Suppose that $D = 3$. Let us write j for $\frac{1+\sqrt{-3}}{2}$. The roots of unities in $\mathbb{Q}(\sqrt{-3})$ are $j, j^2, j^3 = -1, j^4 = -j, j^5 = -j^2, j^6 = 1$. In the cases of ± 1, we obtain again $T(a, b, D) = 2\mathbb{Z}$ with $\xi = b\sqrt{-3}$. If $a - b\sqrt{-3} = j^{\pm 2}(a + b\sqrt{-3})$, then $T(a, b, D) = 3\mathbb{Z}$ with $\xi = a(1 \mp \sqrt{-3})$. If $a - bi = j^{\pm 1}(a + b\sqrt{-3})$, then $T(a, b, D) = 6\mathbb{Z}$ with $\xi = \frac{a}{3}(3 \mp \sqrt{-3})$. □

Before discussing the main theorem, we recall some facts that will be used in the proof. Let $K = \mathbb{Q}(\zeta_k, \sqrt{-D})$. Note that the extension $K/\mathbb{Q}$ is Galois because the extensions $\mathbb{Q}(\zeta_k)/\mathbb{Q}$ and $\mathbb{Q}(\sqrt{-D})/\mathbb{Q}$ are both Galois [15]. Recall that an element $\alpha \in K$ is a primitive element if and only if the only group element of $Gal(K/\mathbb{Q})$ which fixes α is the identity. Consider the action of $Gal(K/\mathbb{Q})$ on $\alpha = (a + b\sqrt{-D})\zeta_k$. There exists an injective

homomorphism $\psi : Gal(K/\mathbb{Q}) \to Gal(\mathbb{Q}(\sqrt{-D})/\mathbb{Q}) \times Gal(\mathbb{Q}(\zeta_k)/\mathbb{Q}) \cong \{ \pm 1\} \times (\mathbb{Z}/k\mathbb{Z})^\times$ via. $\sigma \mapsto (\epsilon(\sigma), u(\sigma))$ which acts as $\sigma((a+b\sqrt{-D})\zeta_k) = (a+b\epsilon(\sigma)\sqrt{-D})\zeta_k^{u(\sigma)}$. If $\sqrt{-D} \notin \mathbb{Q}(\zeta_k)$ then ψ is surjective and is therefore an isomorphism, in which case for all $\sigma \in Gal(K/\mathbb{Q})$ there exists $\widetilde{\sigma}$ such that $\epsilon(\widetilde{\sigma}) = -\epsilon(\sigma)$ and $u(\widetilde{\sigma}) = u(\sigma)$. But if $\sqrt{-D} \in \mathbb{Q}(\zeta_k)$, the sign $\epsilon(\sigma)$ is no longer independent from $u(\sigma)$.

To study the values of $\epsilon(\sigma)$ where $\sqrt{-D} \in \mathbb{Q}(\zeta_k)$, we can use representation of $\sqrt{-D}$ in ζ_k. For an odd prime p who divides k, $\zeta_k^{\frac{k}{p}}$ as a primitive p-th root of unity satisfies the equality of the p-th cyclotomic polynomial $\Phi_p(x) = x^{p-1}+x^{p-2}+\cdots+x+1 = \prod_{i=1}^{p-1}(x-\zeta_k^{\frac{ik}{p}})$, from which we obtain $p = \Phi_p(1) = \prod_{i=1}^{p-1}(1-\zeta_k^{\frac{ik}{p}}) = (-1)^{\frac{p-1}{2}} \prod_{i=1}^{\frac{p-1}{2}}(\zeta_k^{\frac{ik}{p}} - \zeta_k^{-\frac{ik}{p}})^2$. Therefore $(\prod_{i=1}^{\frac{p-1}{2}}(\zeta_k^{\frac{ik}{p}} - \zeta_k^{\frac{-ik}{p}}))^2 = (-1)^{\frac{p-1}{2}}p$ in $\mathbb{Q}(\zeta_k)$. If $4|k$ then $(\zeta_k^{\frac{k}{4}})^2 = -1$, and if $8|k$ then, $(\zeta_k^{\frac{k}{8}}\zeta_k^{\frac{k}{4}}(1+\zeta_k^{\frac{k}{4}}))^2 = 2$. Like this we can represent the square roots of $\pm p$, -1 and 2 in terms of a primitive root of unity ζ_k. For more detailed description about this procedure, refer to [18].

Lemma 2.5. *Suppose that $4|k$ and $\sqrt{-D} \in \mathbb{Q}(\zeta_k)$. Then the map $\sigma : \zeta_k \mapsto \zeta_k^{\frac{k}{2}+1}$ belongs to $Gal(K/\mathbb{Q})$ and $\sigma(\sqrt{-D}) = (-1)^{\frac{k(D+1)}{8}}\sqrt{-D}$.*

Proof. Since $4|k$, we have $\gcd(\frac{k}{2}+1, k) = 1$, so the map $\sigma : \zeta_k \mapsto \zeta_k^{\frac{k}{2}+1}$ belongs to $Gal(\mathbb{Q}(\zeta_k)/\zeta_k)$. If $D \equiv 3 \pmod 4$, then by above procedure we can choose ζ_k such that $\sqrt{-D} = \prod_{p|D}\prod_{j=0}^{\frac{p-1}{2}}(\zeta_k^{\frac{k}{p}j} - \zeta_k^{-\frac{k}{p}j})$ and, because $\frac{k}{p}$ are all even because $k \equiv 0 \pmod 4$, so $\sqrt{-D}$ is invariant under σ, therefore $\epsilon(\sigma) = 1$. If $D \equiv 1 \pmod 4$, then we choose ζ_k such that $\sqrt{-D} = \zeta_k^{\frac{k}{4}}\prod_{p|D}\prod_{j=0}^{\frac{p-1}{2}}(\zeta_k^{\frac{k}{p}j} - \zeta_k^{-\frac{k}{p}j})$ and see that the exponent $\frac{k}{4}$ is even, if $k \equiv 0 \pmod 8$, and is odd if $k \equiv 4 \pmod 8$ while the exponent $\frac{k}{p}$ is always even, therefore $\epsilon(\sigma) = (-1)^{\frac{k}{4}}$. If $D \equiv 2 \pmod 4$, then we must have $8|k$ and we choose ζ_k such that $\sqrt{-D} = \zeta_k^{\frac{k}{8}}\zeta_k^{\frac{k}{4}}(1+\zeta_k^{\frac{k}{4}})(\zeta_k^{\frac{k}{4}})^r\prod_{p|D}\prod_{j=0}^{\frac{p-1}{2}}(\zeta_k^{\frac{k}{p}j} - \zeta_k^{-\frac{k}{p}j})$ and, because the exponent $\frac{k}{8}$ is even, if $k \equiv 0 \pmod{16}$ and is odd, if $k \equiv 8 \pmod{16}$ while the exponent $\frac{k}{p}$ and $\frac{k}{4}$ are always even, therefore $\epsilon(\sigma) = (-1)^{\frac{k}{8}}$. We can summarize all the results in one formula as $\epsilon(\sigma) = (-1)^{\frac{k(D+1)}{8}}$. Note that $\epsilon(\sigma)$ takes always on integers even if D is even because in such a case $8|k$. □

Theorem 2.6. *Let $a, b \in \mathbb{Q}$ and D is a square-free positive integer and suppose $b \neq 0$. There always exists a choice of ζ_k and $\sqrt{-d}$ that $\alpha = (a+b\sqrt{-D})\zeta_k$ is a primitive element of the field extension $\mathbb{Q}(\zeta_k, \sqrt{-D})/\mathbb{Q}$, except in the following cases:*

(*i*) *$D = 1$, $|a| = |b|$ and $k \equiv 8 \pmod{16}$.*

(*ii*) $\sqrt{-D} \notin \mathbb{Q}(\zeta_k)$, $a = 0$ *and* $k \equiv 0 \pmod 4$.

(*iii*) $\sqrt{-D} \in \mathbb{Q}(\zeta_k)$, $a = 0$, $4|k$ *and* $k(D+1) \equiv 8 \pmod{16}$.

Proof. If we take k-th power of the equality $\alpha = (a + b\sqrt{-D})\zeta_k$, we obtain $\alpha^k = A + B\sqrt{-D}$ where $A, B \in \mathbb{Q}$. If $B \neq 0$, by the proposition 2.2, α is a primitive element.

Now suppose $B = 0$. By the lemma 2.4 this occurs if and only if one of the followings holds : (*a*) $|a| = |b|$ and $D = 1$ with $4|k$, or (*b*) $|a| = |b|$ and $D = 3$ with $3|k$, or (*c*) $|a| = 3|b|$ and $D = 3$ with $6|k$, or (*d*) $a = 0$ and $2|k$. We now study the conditions in order for α to be a primitive element in each of these cases.

(*a*) In this case we can write $\alpha = b(1+\epsilon_0\sqrt{-1})\zeta_k$ with ϵ_0 fixed as 1 or -1. If we choose ζ_k such that $\zeta_k^{\frac{k}{4}} = \sqrt{-1}$, then $\alpha = b(\zeta_k + \zeta_k^{\frac{k}{4}+1})$, and the only non-trivial automorphism which fixes α is $\zeta_k \mapsto \zeta_k^{\frac{k}{4}+1}$ with $(\frac{k}{4}+1)^2 \equiv 1 \pmod k$, which is possible only when $k \equiv 8 \pmod{16}$. If we choose ζ_k such that $\zeta_k^{\frac{3k}{4}} = \sqrt{-1}$, then $\alpha = b(\zeta_k + \zeta_k^{\frac{3k}{4}+1})$ can be fixed by the automorphism $\zeta_k \mapsto \zeta_k^{\frac{3k}{4}+1}$ with $(\frac{3k}{4}+1)^2 \equiv 1 \pmod k$, and is possible when $k \equiv 8 \pmod{16}$ again. Therefore $\alpha = b(1 \pm \sqrt{-1})\zeta_k$ cannot be a primitive element when $k \equiv 8 \pmod{16}$.

(*b*) We can write, up to the sign of b, $\alpha = b(-1 + \epsilon_0\sqrt{-3})\zeta_k$ with ϵ_0 fixed as 1 or -1. When $k \not\equiv 6 \pmod 9$, we choose ζ_k such that $\zeta_k^{\frac{k}{3}} = \frac{-1+\epsilon_0\sqrt{-3}}{2}$, then $\alpha = b(-1+\epsilon_0\sqrt{-3})\zeta_k = 2b\zeta_k^{\frac{k}{3}+1}$ is primitive because $\gcd(\frac{k}{3}+1, k) = 1$. When $k \not\equiv 3 \pmod 9$, we choose ζ_k such that $\zeta_k^{\frac{2k}{3}} = \frac{-1+\epsilon_0\sqrt{-3}}{2}$, then $\alpha = b(-1 + \epsilon_0\sqrt{-3})\zeta_k = 2b\zeta_k^{\frac{2k}{3}+1}$ is primitive because $\gcd(\frac{2k}{3}+1, k) = 1$.

(*c*) We can write, up to the sign of b, $\alpha = b(3 + \epsilon_0\sqrt{-3})\zeta_k$ with ϵ_0 fixed as 1 or -1. When $k \not\equiv 24 \pmod{36}$, we choose ζ_k such that $\zeta_k^{\frac{k}{6}} = \frac{1+\epsilon_0\sqrt{-3}}{2}$, then $\alpha = b(3 + \sqrt{-3})\zeta_k = 2b(\zeta_k^{\frac{k}{6}+1} + \zeta_k)$ is primitive. Indeed the only non-trivial automorphism which fixes α is $\zeta_k \mapsto \zeta_k^{\frac{k}{6}+1}$ with $(\frac{k}{6}+1)^2 = 1 \pmod k$, which exists only when $k \equiv 24 \pmod{36}$. When $k \not\equiv 12 \pmod{36}$, we choose ζ_k such that $\zeta_k^{\frac{5k}{6}} = \frac{1+\epsilon_0\sqrt{-3}}{2}$, then $\alpha = b(3+\sqrt{-3})\zeta_k = 2b(\zeta_k^{\frac{5k}{6}+1} + \zeta_k)$ is primitive by the similar reason.

(*d*) Suppose at first that $4 \nmid k$. Then we can take $\frac{k}{2}$-th power of $\alpha = b\sqrt{-D}\zeta_k$ to obtain $\alpha^{\frac{k}{2}} = B\sqrt{-D}\zeta_k$ with $B \neq 0 \in \mathbb{Q}$ because $\frac{k}{2}$ is odd, so that we have $\sqrt{-D} = \frac{\alpha^{\frac{k}{2}}}{B}$ and $\zeta_k = -\frac{\alpha^{\frac{k}{2}+1}}{bBD}$, which shows that α is a primitive element.

Next we suppose that $4|k$. Then we know that $Gal(\mathbb{Q}(\zeta_k, \sqrt{-D})/\mathbb{Q})$ contains an element σ such that $\sigma(\zeta_k) = \zeta_k^{\frac{k}{2}+1} = -\zeta_k$ because $\gcd(\frac{k}{2}+1, k) = 1$. Moreover, if σ satisfies the condition $\sigma(\sqrt{-D}) = -\sqrt{-D}$, then σ will be a non-trivial automorphism satisfying

$\sigma(\sqrt{-D}\zeta_k) = (-\sqrt{-D})(-\zeta_k) = \sqrt{-D}\zeta_k$. When $\sqrt{-D} \notin \mathbb{Q}(\zeta_k)$, we have $Gal(\mathbb{Q}(\sqrt{-D})/\mathbb{Q}) \cong \{\pm 1\} \times (\mathbb{Z}/k\mathbb{Z})^*$, so such an element σ always exists and therefore α cannot be primitive. When $\sqrt{-D} \in \mathbb{Q}(\zeta_k)$, we know by Lemma 2.5 that α is *not* primitive if and only if $\sigma(\sqrt{-D}) = (-1)^{\frac{k(D+1)}{8}}\sqrt{-D} = -\sqrt{-D}$, from which we obtain $k(D+1) \equiv 8 \pmod{16}$. □

2.2 The main strategy

In the remark 2.3, we mentioned the idea to find the polynomial representations of $\sqrt{-D}$ and ζ_k in $\mathbb{Q}[x]/(r(x))$. We now discuss the method of construction more precisely.

For an embedding degree k and a square-free positive integer D, we define

$$n = n(k, D) := \textit{the least positive divisor of } k \textit{ such that } \zeta_k^n \in \mathbb{Q}(\sqrt{-D}).$$

Then, taking the n-th power of the equality $\alpha = (a + b\sqrt{-D})\zeta_k$, we obtain $\alpha^n = (a + b\sqrt{-D})^n\zeta_k^n = A + B\sqrt{-D} \in \mathbb{Q}(\sqrt{-D})$ for $A, B \in \mathbb{Q}$. Then α is a root of the polynomial $r_0(x) = x^{2n} - 2Ax^n + A^2 + DB^2$. The minimal polynomial $r(x)$ of α is a factor of $r_0(x)$. Assume that we have chosen a, b, D and k such that B does not vanish. Then we obtain the representations $\sqrt{-D} = \frac{\alpha^n - A}{B}$ and $\zeta_k = \frac{-b\alpha^{n+1} + (aB + Ab)\alpha}{B(a^2 + b^2D)}$ in $\mathbb{Q}(\alpha)$ as in Proposition 2.2. It follows the polynomial representations in $\mathbb{Q}[x]/(r(x))$,

$$t(x) = \zeta_k + 1 = \frac{-bx^{n+1} + (aB + Ab)x}{B(a^2 + b^2D)} + 1. \tag{5}$$

$$y(x) = -\frac{\sqrt{-D}(t(x) - 2)}{D} = -\frac{ax^{n+1} + (bDB - aA)x}{DB(a^2 + Db^2)} + \frac{x^n - A}{DB} \tag{6}$$

These polynomials give a candidate for a Brezing-Weng family together with the minimal polynomial $r(x)$ and the prime representing polynomial $q(x) = \frac{1}{4}\left(t(x)^2 + Dy(x)^2\right)$. If $t(x)$ and $y(x)$ represent integers, $q(x)$ represents prime numbers and $r(x)$ represent almost prime numbers, then the polynomials give a Brezing-Weng family of rho-value

$$\rho_x = \frac{\deg q(x)}{\deg r(x)} = \frac{2\max\left\{\deg t(x), \deg y(x)\right\}}{\deg r(x)} = \frac{2(n+1)}{e(k, D)\varphi(k)}, \tag{7}$$

where φ is the Euler totient function and $e(k, D)$ is 1 or 2 according to whether $\sqrt{-D}$ belongs to $\mathbb{Q}(\zeta_k)$ or not.

Note that above representations are the results of reduction modulo $r_0(x)$ in the place of reduction modulo $r(x)$, so that the degrees of the polynomials $t(x)$ and $y(x)$ are both

equal to $n+1$, greater by one than the degree of the second most significant term of $r_0(x)$. Because the rho-value is given by (7), the formula is interesting only when $n+1 < \deg r(x) = e(k,D)\phi(k)$. Otherwise we can reduce (5) and (6) modulo $r(x)$ which results in a smaller rho-value, although the resulting $t(x)$ and $y(x)$ may no longer represent integers.

We present rho-values obtained by this construction in some interesting cases in §3, and treat the problem of the representability of integers of the polynomials in §4.

2.3 Some alternatives

On the other hand the analysis of the case (a) in the proof of the Theorem 2.6 suggests an alternative construction where $4|k$ and $D=1$. Suppose $k \not\equiv 8 \pmod{16}$, then by the theorem α is a primitive element. Since $k \equiv 4 \pmod 8$, we have $\gcd(\frac{k}{4}+2, k) = 1$. Let u be an integer such that $u(\frac{k}{4}+2) \equiv 1 \pmod k$. Because $\gcd(u,k)=1$, ζ_k^u is also a primitive root of unity, so we can let $\sqrt{-1} = \zeta_k^{u\frac{k}{4}}$. Let $\alpha = b(1+\sqrt{-1})\zeta_k^u$. Taking the square of this equality we obtain $\alpha^2 = 2b^2\sqrt{-1}\zeta_k^{2u} = 2b^2\zeta_k^{u(\frac{k}{4}+2)} = 2b^2\zeta_k$, and $\sqrt{-1} = (-1)^{\frac{k+4}{8}}\zeta_k^{\frac{k}{4}} = (-1)^{\frac{k+4}{8}}\frac{x^{\frac{k}{2}}}{2^{\frac{k}{4}}b^{\frac{k}{2}}}$, from which we have

$$t(x) \equiv \frac{x^2}{2b^2}+1, \quad y(x) \equiv \frac{x^{\frac{k}{2}+2}}{2^{\frac{k}{4}+1}b^{\frac{k}{2}+2}} - \frac{x^{\frac{k}{2}}}{2^{\frac{k}{4}}b^{\frac{k}{2}}} \pmod{r(x)}, \tag{8}$$

where $r(x)$ is the minimal polynomial of α. Note that $y(x)$ is determined up to sign. Because α is in $\mathbb{Q}(\zeta_k)$, the minimal polynomial $r(x)$ will be a polynomial factor of degree $\varphi(k)$ of $\Phi_k(\frac{x^2}{2b^2})$ where Φ_k is the k-th cyclotomic polynomial. Because $4|k$ and $\deg(t(x)) = 2$, to have a good rho-value, we need that $y(x)$ is of degree near $\frac{\varphi(k)}{2}$, which is generally not likely to happen. The simplest case where $k=4$ and $a=b=1$ gives the polynomials $t(x) = y(x) = x, q(x) = \frac{x^2}{2}$, $r(x) = x^2-2x+2$ that make a family having $\rho_x = 1$. This is a supersingular family over a field of characteristic two. The case where $k=12$ and $a=b=1$ gives another example of $\rho_x = 1$, $t(x) = \frac{x^2}{2}+1$, $y(x) = -\frac{1}{2}x^2+x-1$, $q(x) = \frac{1}{8}x^4 - \frac{1}{4}x^3 + \frac{3}{4}x^2 - \frac{1}{2}x + \frac{1}{2}$, $r(x) = x^4-2x^3+2x^2-4x+4$. But in this case $q(x)$ does not take integer values, so it does not make a family.

On the other hand, because all the exponents of b in the polynomials in (8) are even, if we take $b = \sqrt{C}$ for some square-free $C \in \mathbb{Z}$, the polynomials $t(x)$ and $y(x)$ still remain in $\mathbb{Q}[x]$. If we take $C = D$ for another $D \neq 1$ such that $\sqrt{-D} \in \mathbb{Q}(\zeta_k)$, then $\alpha = (\sqrt{D}+\sqrt{-D})\zeta_k$. By the similar reason as above, the families constructed are not expected to have good rho-values generally. But if we apply this primitive element to the case where $k=12$ and $D=3$ we obtain a family of $\rho_x = 1$, which is found in [3].

If we take C such that $\sqrt{-C} \notin \mathbb{Q}(\zeta_k)$, then $\Phi_k(\frac{x^2}{2C})$ will remain irreducible therefore as the minimal polynomial of α of degree $2\varphi(k)$. This alternative can give acceptable families of $\rho_x = \frac{k+4}{2\varphi(k)}$. For example, if we choose $k = 4p$ for a prime p, we have $\rho_x = 1 + \frac{2}{p-1}$.

3 Application of the main strategy to some interesting cases

3.1 The cases where k is odd and $\sqrt{-D} \notin \mathbb{Q}(\zeta_k)$

We continue using the symbols defined in §2. Fix D such that $\sqrt{-D} \notin \mathbb{Q}(\zeta_k)$. Because k is odd and $\sqrt{-D} \notin \mathbb{Q}(\zeta_k)$, we have $n = k$. By the process described in §2.2, we obtain

$$\begin{aligned} t(x) &= \frac{-bx^{k+1} + (aB + bA)x}{B(a^2 + Db^2)} + 1, \\ y(x) &= -\frac{ax^{k+1} + (bDB - aA)x}{DB(a^2 + Db^2)} + \frac{x^k - A}{DB} \in \mathbb{Q}[x]. \end{aligned} \tag{9}$$

Because $\sqrt{-D} \notin \mathbb{Q}(\zeta_k)$, we have $\deg r(x) = 2\varphi(k)$ and $\deg q(x) = 2k + 2$. So we have

$$\rho_x = \frac{\deg q(x)}{\deg r(x)} = \frac{k+1}{\phi(k)}. \tag{10}$$

From this formula we observe that the bigger the size of each prime factor and the smaller the number of the prime factors, the nearer the approaches rho-value to 1. For example, for $k = p^\ell$ a power of a prime, we have $\rho_x \approx 1 + \frac{1}{p-1}$. In particular, when $k = p$ a prime, the rho-value is $1 + \frac{2}{p-1}$, from which come the best results. We see that the rho-value depends much on the least size prime factor of k. For example, if k is even, then the prime factor $p = 2$ makes rho-value bigger than 2 without exception, so this method is useless for even k. Table 1 shows the rho-values obtained by the construction for odd embedding degrees ≤ 60. In the table, we see also that the cases where k contains prime factors 3, 5 give relatively large rho-values.

k	1	3	5	7	9	11	13	15	17	19	21	23	25	27	29
ρ_x	2.000	2.000	1.500	1.333	1.667	1.200	1.167	2.000	1.125	1.111	1.833	1.090	1.300	1.556	1.071
k	31	33	35	37	39	41	43	45	47	49	51	53	55	57	59
ρ_x	1.067	1.700	1.500	1.056	1.667	1.050	1.048	1.917	1.044	1.191	1.625	1.039	1.400	1.611	1.035

Table 1: ρ_x obtained for k odd < 60, $\sqrt{-D} \notin \mathbb{Q}(\zeta_k)$, $n = k$

Remark 3.1. In the table 1, we can see that the ρ_x are the same as those given in [10] when $k = 1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35, 37, 41, 43, 47, 49$. Our results are worse in the cases where k contains 3 as we have predicted, for which cases we have to use another powering exponent n. See §3.3 for the cases where 3 divides k.

3.2 The cases where k is even and $\sqrt{-D} \notin \mathbb{Q}(\zeta_k)$

Note that these cases contain all of our improved results. Fix D such that $\sqrt{-D} \notin \mathbb{Q}(\zeta_k)$. Because k is even and $\sqrt{-D} \notin \mathbb{Q}(\zeta_k)$, we have $n = \frac{k}{2}$. By the process described in §2.2, we obtain

$$\begin{aligned} t(x) &= \frac{-bx^{\frac{k}{2}+1} + (aB + bA)x}{B(a^2 + Db^2)} + 1, \\ y(x) &= -\frac{ax^{\frac{k}{2}+1} + (bDB - aA)x}{DB(a^2 + Db^2)} + \frac{x^{\frac{k}{2}} - A}{DB} \in \mathbb{Q}[x]. \end{aligned} \tag{11}$$

Because $\deg r(x) = 2\varphi(k)$ and $\deg q(x) = k + 2$, we have

$$\rho_x = \frac{k+2}{2\phi(k)}. \tag{12}$$

In this case two cases are particularly interesting. For $k = 2^\ell p$ $(\ell \geq 1)$ where p is a prime ≥ 3, we have $\rho_x = 1 + \frac{1}{p-1}\left(1 + \frac{1}{2^{\ell-1}}\right)$. For $k = 2^\ell (\ell \geq 1)$, we have $\rho_x = 1 + \frac{1}{2^{\ell-1}}$. Table 2 shows the rho-values that can be obtained by our construction §3.2 for even embedding degrees ≤ 60.

k	2	4	6	8	10	12	14	**16** †	18	20	**22** †	24	26	**28** †	30
ρ_x	2.000	1.500	2.000	1.250	1.500	1.750	1.333	**1.125**	1.667	1.375	**1.200**	1.625	1.167	**1.250**	2.000
k	32	34	36	38	**40** †	42	44	**46** †	48	50	52	54	56	58	60
ρ_x	1.063	1.125	1.583	1.111	**1.313**	1.833	1.150	**1.091**	1.563	1.300	1.125	1.556	1.208	1.071	1.938

Table 2: ρ_x obtained for k even, $\sqrt{-D} \notin \mathbb{Q}(\zeta_k)$, $n = \frac{k}{2}$

Remark 3.2. In the table 2, the † marked entries mean that they are the ρ_x smaller than those of previously known families. We see that $k = 16, 22, 28, 40$ and 46 are such cases. We offer some examples for these cases in §5 except for $k = 40$.

Remark 3.3. For the other cases $k = 4, 8, 10, 14, 20, 26, 32, 34, 38, 44, 50$, the ρ_x are the same as those given in [10]

3.3 The cases where $3|k$, $4|k$ or $6|k$ and $\sqrt{-D} \in \mathbb{Q}(\zeta_k)$

From the previous constructions §3.1 and §3.2, resulting rho-values are relatively large where the k contains small prime factors like 2, 3 or 5. But we can still improve the result by taking n less than k for certain cases. Indeed, the improvements of §3.3 were for the cases where we can take $n = \frac{k}{2}$, i.e where k is even. To lower n, we need that $\mathbb{Q}(\zeta_k^n) \subset \mathbb{Q}(\sqrt{-D})$. The only cases except $n = k, \frac{k}{2}$ are the cases, (a) $3|k$, $D = 3$, $n = \frac{k}{3}$, (b) $4|k$, $D = 1$, $n = \frac{k}{4}$, (c) $6|k$, $D = 3$, $n = \frac{k}{6}$. These are possible because the cyclotomic fields $\mathbb{Q}(\zeta_3) = \mathbb{Q}(\zeta_6)$ and $\mathbb{Q}(\zeta_4)$ are quadratic fields $\mathbb{Q}(\sqrt{-3})$ and $\mathbb{Q}(\sqrt{-1})$ respectively. Therefore, this kind of trial does not work for the case where $5|k$.

We construct families along the method described in §2.2, and have

$$\rho_x = \begin{cases} \frac{2k+6}{3\phi(k)} & \text{if } 3|k \\ \frac{k+4}{2\phi(k)} & \text{if } 4|k \\ \frac{k+6}{3\phi(k)} & \text{if } 6|k \end{cases} \tag{13}$$

Table 3, table 4 and table 5 shows the rho-values for $k \leq 60$ when $n = \frac{k}{3}$, $\frac{k}{4}$ and $\frac{k}{6}$ for the cases where $3|k$, $4|k$ and $6|k$, respectively. We put the rho-values less than 2 in the tables. We can verify that the rho-values are relatively large when $n = \frac{k}{3}$ and $2|k$, and also when $n = \frac{k}{2}$ and $3|k$ by the small factor effects that we have mentioned in the analysis in §3.1. This effect does not appear when $n = \frac{k}{6}$.

k	9	15	21	27	33	39	45	51	57
ρ_x	1.333	1.500	1.333	1.111	1.200	1.167	1.333	1.125	1.111

Table 3: ρ_x obtained when $3|k$, $\sqrt{-D} = \sqrt{-3} \in \mathbb{Q}(\zeta_k)$, $n = \frac{k}{3}$

Remark 3.4. In the table 3, we can see that the ρ_x are the same as those given in [10] when $k = 9, 15, 21, 27, 33, 39, 45$.

k	8	16	20	24	28	32	36	40	44	48	52	56
ρ_x	1.500	1.250	1.500	1.750	1.333	1.125	1.666	1.375	1.200	1.625	1.167	1.250

Table 4: ρ_x obtained when $4|k$, $\sqrt{-D} = \sqrt{-1} \in \mathbb{Q}(\zeta_k)$, $n = \frac{k}{4}$

Remark 3.5. In the table 4, we can see that the ρ_x are the same as those given in [10] when $k = 16, 28, 40$. Note that all these cases are contained in the cases of §3.2 and better results are shown in the table 2.

k	6	12	18	24	30	36	42	48	54	60
ρ_x	2.000	1.500	1.333	1.250	1.500	1.167	1.333	1.125	1.111	1.375

Table 5: ρ_x obtained when $6|k$, $\sqrt{-D} = \sqrt{-3} \in \mathbb{Q}(\zeta_k)$, $n = \frac{k}{6}$

Remark 3.6. In the table 5, we can see that the ρ_x are the same as those given in [10] when $k = 18, 24, 30, 36, 42, 48$. Note that in these cases, these results are better than those of §3.2.

Remark 3.7. In the case where $8|k$, because $\sqrt{-2} \in \mathbb{Q}(\zeta_k)$, we can also take $\alpha = (a + b\sqrt{-2})\zeta_k$ using $n = \frac{k}{8}$.

4 Evaluation of the polynomials and the algorithm

In this section, we discuss the structure and calculation of the set of rational numbers x_0 for which $f(x_0)$ is an integer, f being a polynomial with rational coefficients. Then we apply this to the polynomials $r(x)$, $t(x)$, $y(x)$ and $q(x)$ appearing in the polynomial families. We also recall the situation in which r and q represent primes, as predicted by the Bateman-Horn heuristics [4] (see also [10], §2.1).

Numerical examples will be given in §5.

4.1 Study of polynomials representing integers

The problems of the representations of integers and prime numbers when the variable x takes on integer values are well treated in [10] in practical points of view. In our construction, all variables are defined as rational variables. So we discuss briefly how to reduce this case to that of integral variables. We begin with a definition.

Definition 4.1. Let $f(x) \in \mathbb{Q}[x]$. We say that f *represents integers*, if $f(\mathbb{Q}) \cap \mathbb{Z} \neq \emptyset$.

Define

$$\begin{aligned} V_{\mathbb{Z}}(f) &= f(\mathbb{Q}) \cap \mathbb{Z}, \\ D_{\mathbb{Q}}(f) &= f^{-1}(V_{\mathbb{Z}}(f)) = \{x \in \mathbb{Q} | f(x) \in \mathbb{Z}\}. \end{aligned}$$

If $f(x_0) \in \mathbb{Z}$ then $f(x_1) \in \mathbb{Z}$ for every rational number x_1 congruent to x_0 modulo the common denominator of the coefficients of $f(x)$. We deduce that if f represents integers, then $|f(\mathbb{Q}) \cap \mathbb{Z}| = \infty$.

Definition 4.2. Let $m \geq 1$. Two m-tuples of polynomials $(f_1, \cdots, f_m)$ and $(g_1, \cdots, g_m)$ are said to be *affinely equivalent* if there exists $\lambda, \mu \in \mathbb{Q}$ with $\lambda \neq 0$ such that $g_i(x) = f_i(\lambda x + \mu)$ for all $i \in \{1, \ldots, m\}$. When this is the case, we write $(f_1, \ldots, f_m) \sim (g_1, \ldots, g_m)$.

Note that if $f(x) \sim g(x)$, then we have $V_{\mathbb{Z}}(f) = V_{\mathbb{Z}}(g)$ clearly.

Let $f(x)$ a polynomial of degree ≥ 2 in $\mathbb{Q}[x]$ and write

$$\begin{aligned} &f(x) = \frac{g(x)}{m} \quad \text{where} \quad g(x) = g_n x^n + g_{n-1}x^{n-1} + \cdots + g_1 x + g_0 \in \mathbb{Z}[x], \\ &\gcd(m, g_n, \cdots, g_0) = 1 \text{ and } m \geq 1 \text{ is an integer.} \end{aligned} \tag{14}$$

We want to find $D_{\mathbb{Q}}(f)$.

For a rational number $\frac{u}{v}$, where u, $v \in \mathbb{Z}$ and $\gcd(u, v) = 1$, if $f(\frac{u}{v}) \in \mathbb{Z}$, then we need that $g_n u^n + g_{n-1}u^{n-1}v + \cdots + g_1 uv^{n-1} + g_0 v^n \equiv 0 \pmod{mv^n}$. Since $\gcd(u, v) = 1$, v must divide g_n.

Consequently, for every element $x_1 \in D_{\mathbb{Q}}(f)$, we can let $x_1 = \frac{w}{g_n}$ where $w \in \mathbb{Z}$ and $\gcd(w, g_n) \geq 1$. Substituting this x_1 into (14), we obtain

$$w^n + g_{n-1}w^{n-1} + \cdots + g_0 g_n^{n-1} \equiv 0 \pmod{mg_n^{n-1}}. \tag{15}$$

If an integer $w = w_1$ is a solution of the congruence (15), then the rational numbers $x_1 = \frac{w_1}{g_n} \pmod{mg_n^{n-2}}$ satisfies $f(x_1) \in \mathbb{Z}$. This process gives the set $D_{\mathbb{Q}}(f)$.

Proposition 4.3. *(i) If a polynomial $f(x) \in \mathbb{Q}[x]$ is of the form $f(x) = \frac{g(x)}{m}$ where $m \in \mathbb{Z}$ and $g(x) \in \mathbb{Z}[x]$ has a leading coefficient 1 or -1, then $D_{\mathbb{Q}}(f) \subset \mathbb{Z}$.*

(ii) For a given polynomial $f(x) \in \mathbb{Q}[x]$, we can determine explicitly a polynomial $h(x) \in \mathbb{Q}[x]$ such that $V_{\mathbb{Z}}(f) = V_{\mathbb{Z}}(h)$ and $D_{\mathbb{Q}}(h) \subset \mathbb{Z}$.

Proof. (i) By the above discussion, the denominator of an element of $D_{\mathbb{Q}}(f)$ should divides the leading coefficient of $g(x)$. So, if the leading coefficient of $g(x)$ is 1 or -1, then we have $D_{\mathbb{Q}}(f) \subset \mathbb{Z}$.

(ii) Suppose that $f(x)$ is of the form (14). By the change of variable $x \mapsto \frac{x}{g_n}$, we obtain a polynomial $h(x) = \frac{x^n + g_{n-1}x^{n-1} + g_{n-2}g_n x^{n-2} + \cdots + g_1 g_n^{n-2} x + g_0 g_n^{n-1}}{g_n^{n-1} m}$. We have $V_{\mathbb{Z}}(h) = V_{\mathbb{Z}}(f)$ because $h(x) = f(\frac{x}{g_n}) \sim f(x)$, and $D_{\mathbb{Q}}(h) \subset \mathbb{Z}$ because $h(x)$ satisfies the conditions of (i). □

Definition 4.4. Let us we write a polynomial $f(x) \in \mathbb{Q}$ in the form (14). Then $f(x)$ is called *normalized* if the leading coefficient of $g(x)$ is 1 or -1. If a normalized polynomial $h(x)$ is affinely equivalent to a polynomial $f(x)$, we say that $h(x)$ is a *normalization* of $f(x)$, and the polynomial $f(\frac{x}{g_n})$ is called the *standard normalization* of $f(x)$.

In view of the Proposition 4.3, to find $V_{\mathbb{Z}}(f)$ for a polynomial $f(x)$ in $\mathbb{Q}[x]$, we can work with its standard normalization.

4.2 Application to the polynomials $t(x)$, $y(x)$, $r(x)$, $q(x)$.

In our construction, we assumed that x, a, b take rational values, using § 4.1, we now see that they can be assumed to be integers.

Proposition 4.5. *Let $r_\alpha(x)$, $t_\alpha(x)$, $y_\alpha(x)$, $q_\alpha(x)$ be the polynomials associated to $\alpha = (a + b\sqrt{-D})\zeta_k$ where a, $b \in \mathbb{Q}$ and $b \neq 0$ as in §2.2. Then there exists $\alpha^* = (a^* + b^*\sqrt{-D})\zeta_k$, where a^*, $b^* \in \mathbb{Z}$ and $b^* > 0$ such that the associated polynomials $r_{\alpha^*}(x)$, $t_{\alpha^*}(x)$, $y_{\alpha^*}(x)$ and $q_{\alpha^*}(x)$ satisfy $(r_\alpha(x), t_\alpha(x), y_\alpha(x), q_\alpha(x)) \sim (r_{\alpha^*}(x), t_{\alpha^*}(x), y_{\alpha^*}(x), q_{\alpha^*}(x))$.*

Proof. Let $\alpha = (a + b\sqrt{-D})\zeta_k$, where a, $b \in \mathbb{Q}$, be a primitive element. Let $c \in \mathbb{Z}$, $c > 0$ be such that ac and bc are integers. It suffices to take $\alpha^* = c\alpha$ choosing the sign of c so that $bc > 0$. □

In view of Proposition 4.5, we assume from now on that a, $b \in \mathbb{Z}$ and that $b > 0$. Then the problem of finding $D_{\mathbb{Q}}(t) \cap D_{\mathbb{Q}}(y) \cap D_{\mathbb{Q}}(q) \cap D_{\mathbb{Q}}(r)$ is related to the solvability of a system of polynomial congruences modulo each denominator. The main problem is to solve the system of two congruences corresponding (5) and (6) as follows.

$$\begin{aligned} &-bx^{n+1} + (aB + Ab)x \equiv 0 \pmod{B(a^2 + b^2 D)}, \\ &ax^{n+1} - (a^2 + Db^2)x^n + (bDB - aA)x + A(a^2 + Db^2) \equiv 0 \pmod{DB(a^2 + Db^2)}. \end{aligned} \tag{16}$$

In order to determine $D_{\mathbb{Q}}(t) \cap D_{\mathbb{Q}}(y) \cap D_{\mathbb{Q}}(q) \cap D_{\mathbb{Q}}(r) \subset \mathbb{Z}$, it suffices that one of $t(x)$, $y(x)$, $r(x)$ and $q(x)$ is normalized. So we can replace the congruences (16) by those associated to a normalized tuples of polynomials. Note that the change of variable for the normalization should be simultaneous for multiple congruences.

Proposition 4.6. *In the cases of §3.1 and §3.2, i.e. when $n = k$ or $\frac{k}{2}$, the polynomial $t(x)$ is normalized.*

Proof. In these cases we have $(a + b\sqrt{-D})^n = \pm(A + B\sqrt{-D})$ with $A, B \in \mathbb{Z}$. From the binomial expansion of the left hand side we obtain $B = b\sum_{r=0}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{2r+1} a^{n-2r-1} b^{2r} (-D)^r$, from which we find that b always divide B. Hence, (5) changes to $t(x) = \frac{-x^{n+1} + (aB' + A)x}{B'(a^2 + Db^2)} + 1$ where $B' = \frac{B}{b} \in \mathbb{Z}$, which is a normalized polynomial. □

So for the constructions of §3.1 and §3.2, we need not a normalization process separately. Note that for other constructions §3.3, this proposition is not true.

We obtain the solutions of the congruences (16) in the form $x = x_0 + NX$ where x_0 and N are fixed integers and X is a integer variable. We substitute this into $t(x)$, $y(x)$ and $r(x)$ to obtain polynomials $T(X) = t(x_0 + NX), Y(X) = y(x_0 + NX), R(X) = r(x_0 + NX) \in \mathbb{Z}[X]$. Then the divisibility conditions $\Phi_k(t(x) - 1) \equiv 0 \pmod{r(x)}$ and $(t(x) - 1)^2 + Dy(x)^2 \equiv 0 \pmod{r(x)}$ that hold in the ring $\mathbb{Q}[x]$ become

$$\Phi_k(T(X) - 1) = G(X)R(X), \text{ and } (T(X) - 1)^2 + DY(X)^2 = H(X)R(X), \tag{17}$$

for some polynomials $G(X), H(X) \in \mathbb{Q}[X]$. Note that $R(X) \in \mathbb{Z}[X]$ automatically because $r(x) \in \mathbb{Z}[x]$. Because $\Phi_k(T(X) - 1), (T(X) - 1)^2 + DY(X)^2, R(X)$ are all in $\mathbb{Z}[X]$, we can write, by an application of the Gauss' lemma on polynomial [15], that $G(X)R(X) = c(G)c(R)G_1(X)R_1(X)$ and $H(X)R(X) = c(H)c(R)H_1(X)R_1(X)$ where $G_1(X), H_1(X)$ and $R_1(X)$ are primitive polynomials $\in \mathbb{Z}[x]$, and $c(G)c(R), c(H)c(R) \in \mathbb{Z}$. Here $c(F)$ means the content of the polynomial $F(X)$. Therefore we can write

$$\Phi_k(T(X) - 1) = G_2(X)R_1(X), \text{ and } (T(X) - 1)^2 + DY(X)^2 = H_2(X)R_1(X), \tag{18}$$

for $G_2(X), H_2(X), R_1(x) \in \mathbb{Z}[x]$. So if we replace $R(X)$ by $R_1(x)$, the divisibility conditions hold in the ring $\mathbb{Z}[X]$, so that the divisibility conditions also hold among the integers represented by the corresponding polynomials.

Lastly, if $Q(X) = q(x_0 + NX) = \frac{1}{4}\{T(X)^2 + DY(X)^2\}$ represents primes we obtain a family. Note that for a pair of integers t and y randomly obtained, the probability that $t^2 + Dy^2 \equiv 0 \pmod 4$ is $\frac{1}{2}$ when $D \equiv 3 \mod 4$, and is $\frac{1}{4}$ when $D \equiv 1 \mod 4$.

4.3 Algorithmic and computational aspects

The following algorithm describes the method of finding families of pairing friendly elliptic curves by the main strategy (§2.2). We assume that the inputs are chosen so that one of the exceptional cases in the Theorem 2.6 does not occur.

Algorithm 4.7. Constructing families of pairing-friendly elliptic curves - The main strategy.

INPUT: k, n: positive integers, D: a square-free positive integer, L, M: positive integers
OUTPUT: A list of complete families of elliptic curves $(r(x), t(x), y(x), q(x))$
or an empty list $\emptyset$
VARIABLES: a, b, n, X, $LIST$.

---

1. If $2 \nmid k$ then

   If $3 \nmid k$ then let $n = k$, otherwise let $n = \frac{k}{3}$.

   Else if $2|k$ then

   If $3 \nmid k$ then let $n = \frac{k}{2}$, otherwise let $n = \frac{k}{6}$.

   (Optional: If $4|k$ and $3 \nmid k$ then we can let $n = \frac{k}{4}$)

2. Set $LIST = \emptyset$.

3. For a from $-L$ to L, b from 1 to M do

   3.1. Let $\alpha = (a + b\sqrt{-D})\zeta_k$.

   3.2. Find A and B such that $A + B\sqrt{-D} = \alpha^n$.

   3.3. Let $t(x) = \frac{-bx^{n+1}+(aB+Ab)x}{B(a^2+b^2D)} + 1$,
   $y(x) = -\frac{ax^{n+1}+(bDB-aA)x}{DB(a^2+Db^2)} + \frac{x^n-A}{DB}$,
   $r_0(x) = x^{2n} - 2Ax^n + A^2 + DB^2$.

   3.4. Find the minimal polynomial $r(x)$ of α from the factors of $r_0(x)$.

   3.5. Replace the polynomials $r(x), t(x), y(x)$ by their normalizations.
   Let $t(x) = \frac{g_1(x)}{m_1}$, $y(x) = \frac{g_2(x)}{m_2}$ for $g_1, g_2 \in \mathbb{Z}[x]$, $m_1, m_2 \in \mathbb{Z}$.

3.6. Find the integer solutions of the congruences.
$g_1(x) \equiv 0 \pmod{m_1}$, $g_2(x) \equiv 0 \pmod{m_2}$.
Let the solutions $x = x_i + N_i X$ $(i = 1, \cdots, \ell)$.

3.7. For i from 1 to ℓ do

3.7.1 Let $T(X) = t(x_i + N_i X)$, $Y(X) = y(x_i + N_i X)$,
$Q(X) = \frac{T(X)^2 + DY(X)^2}{4}$, $R(X) = r(x_i + N_i X)$.

3.7.2 If $Q(X)$ represent prime numbers then let $R_1(X) = \frac{R(X)}{c(R(X))}$, and add $(R_1(x), T(x), Y(x), Q(x))$ to $LIST$.

4. OUTPUT($LIST$).

---

5 Examples

In this section, we give some example families constructed by the proposed method. First four examples where $n = \frac{k}{2}$ break the records of ρ_x values when $k = 16, 22, 28$ and 46. The other three examples for the cases where $3|k$, $4|k$ and $6|k$ respectively, are offered to show that our method is useful for another k. The computations are performed by codes of GP/PARI calculator version 2.3.4 in a computer of 4 GHz CPU and 6 GB memory.

Example 5.1. $k = 16,\ D = 19,\ n = \frac{k}{2},\ a = 1,\ b = -9,$

$r(x) = x^{16} + 11015986347776x^8 + 31634849063620633600000000,$

$t(x) = \frac{1}{44704166510080}(-x^9 - 5478964494336x + 44704166510080),$

$y(x) = \frac{1}{7644412473223680}(x^9 - 1540x^8 + 50183131004416x - 8482309487787520),$

$q(x) = \frac{1}{798865920174679153697488896 0}(x^{18} - 2x^{17} + 1540x^{16} + 11015986347776x^{10} - 200732524017664x^9$
$+ 16964618975575040x^8 + 31634849063620633600000000x^2 - 104236367393936105753555763 2x$
$+ 48717667557975775744000000000).$

We see that $\rho_x = 1.125$, and $t(x)$, $y(x)$ represent integers and $q(x)$ represents primes and $r(x)$ represents almost primes where $x = 53516500134953086 0+7988659201746791536974888960X$, etc. for $X \in \mathbb{Z}$. For example, we obtain a numerical example when $X = 88$,

$r_0 = 218728147929748106011356890353 \cdots 101277903139234516363115960577$ (1447-bit),

$t_0 = -938125837401756790742311747438 \cdots 417955118448094516057864297727,$

$q_0 = 220162984677250004436664961339 \cdots 994584081041965620905462655397$ (1692-bit), with $\rho = 1.170$.

For $k = 16$, another parameters $D = 83, n = \frac{k}{2}, a = 1,\ b = 9$ also gives an example.

Example 5.2. $k = 22$, $D = 3$, $n = \frac{k}{2}$, $a = -3$, $b = 2$

$r(x) = x^{20} + 6x^{19} + 15x^{18} - 36x^{17} - 531x^{16} - 2430x^{15} - 3429x^{14} + 30456x^{13} + 254745x^{12}$
$+ 888894x^{11} - 16281x^{10} + 18666774x^9 + 112342545x^8 + 282053016x^7 - 666875349x^6 - 9924365430x^5$
$- 45541810251x^4 - 64839187476x^3 + 567342890415x^2 + 4765680279486x + 16679880978201,$

$t(x) = -\frac{1}{341901}x^{12} - \frac{25740}{469}x + 1,$

$y(x) = \frac{1}{683802}x^{12} + \frac{1}{97686}x^{11} + \frac{76751}{2814}x + \frac{25673}{134},$

$q(x) = \frac{1}{267191528688}x^{24} + \frac{1}{44531921448}x^{23} + \frac{1}{12723406128}x^{22} + \frac{25673}{183258936}x^{13} + \frac{76751}{91629468}x^{12} + \frac{25673}{8726616}x^{11}$
$+ \frac{282475249}{215472}x^2 + \frac{1963530103}{251384}x + \frac{1977326743}{71824}.$

We see that $\rho_x = 1.200$, and $t(x)$, $y(x)$ represent integers and $q(x)$ represents primes and $r(x)$ represents almost primes when $x = 17937045 + 267191528688X$, etc. for $X \in \mathbb{Z}$. For example, we obtain a numerical example when $X = 99$,

$r_0 = 375682463649294937725331452708 \cdots 67254111696251583189463259322 1$ (835-bit),

$t_0 = -343239858738915685119553839795 \cdots 765440417453761981253691221920,$

$q_0 = 515434502743726638701574169825 \cdots 673432678427415474854085670147$ (1032-bit), with $\rho = 1.235$.

For $k = 22$, another parameters $D = 1, n = \frac{k}{2}, a = 1,\ b = 2$ also gives an example.

Example 5.3. $k = 28,\ D = 11,\ n = \frac{k}{2},\ a = -1,\ b = 1,$

$r(x) = x^{24} + 20x^{22} + 256x^{20} + 2240x^{18} + 7936x^{16} - 163840x^{14} - 4419584x^{12} - 23592960x^{10} + 164560896x^8 +$
$6688604160x^6 + 110075314176x^4 + 1238347284480x^2 + 8916100448256$

$t(x) = \frac{1}{106070016}(x^{15} + 11763712x + 106070016)$

$y(x) = \frac{1}{1166770176}(-x^{15} - 12x^{14} - 117833728x - 247234560)$

$q(x) = \frac{1}{41253110412214272}(x^{30} + 2x^{29} + 12x^{28} + 41205760x^{16} + 471334912x^{15} + 494469120x^{14} + 1283918464548864x^2 +$
$7143019702648832x + 15407021574586368)$

We see that $\rho_x = 1.250$ and $t(x)$, $y(x)$ represent integers and $q(x)$ represents primes and $r(x)$ represents almost primes where $x = 40836966312 + 41253110412214272X$, etc. for $X \in \mathbb{Z}$. For example, we obtain a numerical example when $X = 0$,

$r_0 = 44572344868846171690463985 3900...40368310958685725972305030 7457$ (738-bit),

$t_0 = 13810501302700183418917110 3639...10075828263210930000465808 79033,$

$q_0 = 52017258065788501930744249 5391...62544051781664862935481269 6407,$ (1003-bit), with $\rho = 1.280$.

Example 5.4. $k = 46$, $D = 1$, $m = 2$, $a = -3$, $b = -2$,

$r(x) = x^{44} + 6x^{43} + 23x^{42} + 60x^{41} + 61x^{40} - 414x^{39} - 3277x^{38} - 14280x^{37} - 43079x^{36} - 72834x^{35} +$
$123023x^{34} + 1684980x^{33} + 8510581x^{32} + 29158746x^{31} + 64314923x^{30} + 6825840x^{29} - 795138959x^{28} -$
$4859569674x^{27} - 18820611577x^{26} - 49749263700x^{25} - 53827631699x^{24} + 323774637906x^{23} +$

$2642407039523x^{22}+4209070292778x^{21}-9096869757131x^{20}-109299132348900x^{19}-537535487250697x^{18}-1804324202968482x^{17}-3837983883551831x^{16}+428311337279280x^{15}+52463658509849483x^{14}+309213903674466258x^{13}+1173255861418754269x^{12}+3019754420744464260x^{11}+2866200326022980063x^{10}-2205960551354015500 2x^9-1696182373195396708 31x^8-730934552241216009960x^7-2180570228293280338957x^6-3581272190623873904262x^5+685977982406940098 0869x^4+8771521742252676664 0620x^3+4371141668222583870 92423x^2+1482387174440702356226478x+3211838877954855105157369,$

$t(x)=\frac{1}{34351291513799}(x^{24}-11645371944360x+34351291513799),$

$y(x)=\frac{1}{68702583027598}(3x^{24}+13x^{23}-584824319281x-48335960735283),$

$q(x)=\frac{1}{14523215122043066990860460 32}(x^{48}+6x^{47}+13x^{46}-7436301651582x^{25}-2339297277124x^{24}-96671921470566x^{23}+4175390541341311636704 5797x^2-2418255723777694598287 69698x+5428007703743705127715953 61).$

We see that $\rho_x=1.090$ and $t(x)$, $y(x)$ represent integers and $q(x)$ represents primes and $r(x)$ represents almost primes when $x=960188679654379+145232151220430669908604603 2X$, etc. for $X\in\mathbb{Z}$. For example, we obtain a numerical example when $n=26$,

$r_0=3512285159820783753003125843 94\cdots 9725461697719995666729105464 53$ (4094-bit),

$t_0=2055529758631704681968038433 44\cdots 3657320613394543291574554375 20$,

$y_0=3083294637947557022952057650 51\cdots 5772370192725463587745847066 74$,

$q_0=3432977103254167713160725912 62\cdots 9234334978184293404653109731 69$ (4466-bit), with $\rho=1.090$.

Example 5.5. For $k=27$, $D=3$, $n=\frac{k}{3}$, $a=-2$, $b=1$,

$r(x)=x^{18}-4751x^9+40353607,$

$t(x)=\frac{2}{47621}x^{10}-\frac{18357}{47621}x+1,$

$y(x)=-\frac{4}{142863}x^{10}-\frac{2}{20409}x^9-\frac{10907}{142863}x+\frac{4751}{20409},$

$q(x)=\frac{1}{971896989}x^{20}+\frac{4}{971896989}x^{19}+\frac{1}{138842427}x^{18}-4751/971896989x^{11}+\frac{21814}{971896989}x^{10}-\frac{4751}{138842427}x^9+\frac{5764801}{138842427}x^2-\frac{213233585}{971896989}x+\frac{40353607}{138842427}$

This family has $\rho_x=1.111$, and $t(x)$, $y(x)$ represent integers and $q(x)$ represents primes and $r(x)$ represents almost primes where $x=51457+142863X$, etc. for $X\in\mathbb{Z}$.

Example 5.6. For $k=8$, $D=7$, $n=\frac{k}{4}$, $a=-1$, $b=1$,

$r(x)=x^8-16x^4+4096,$

$t(x)=\frac{1}{192}(x^5-16x+192),$

$y(x)=\frac{1}{1344}(-x^5-8x^4-176x-64),$

$q(x)=\frac{1}{129024}(x^{10}+2x^9+8x^8+16x^6+704x^5+128x^4+4096x^2-2560x+32768)$

This family has $\rho_x=1.250$. $t(x)$, $y(x)$ represent integers and $q(x)$ represents primes and $r(x)$ represents almost primes where $x=5396+129024X$, etc. for $X\in\mathbb{Z}$. Note that

we take $D = 7$ which is different from that of table 8.2 of [10].

Example 5.7. For $k = 36$, $D = 3$, $n = \frac{k}{6}$, $a = -2$, $b = 1$,

$r(x) = x^{12} + 683x^6 + 117649$,

$t(x) = -\frac{2}{259}x^7 - \frac{757}{259}x + 1$,

$y(x) = \frac{4}{777}x^7 + \frac{2}{111}x^6 + \frac{1255}{777}x + \frac{683}{111}$,

$q(x) = \frac{1}{28749}x^{14} + \frac{4}{28749}x^{13} + \frac{1}{4107}x^{12} + \frac{683}{28749}x^8 + \frac{2510}{28749}x^7 + \frac{683}{4107}x^6 + \frac{16807}{4107}x^2 + \frac{386569}{28749}x + \frac{117649}{4107}$

This family has $\rho_x = 1.167$, and $t(x)$, $y(x)$ represent integers and $q(x)$ represents primes and $r(x)$ represents almost primes where $x = 490 + 777X$, etc. for $X \in \mathbb{Z}$.

6 Conclusion and perspectives

We have proposed a new method of choosing primitive elements for Brezing-Weng families of pairing friendly elliptic curves. The proposed method improves the rho-values of the families for the case where embedding degrees $k = 16, 22, 28$ and 46. We have summarized the improved results in table 6.

k	ρ_x	D	$\deg r(x)$	Constr.
16	1.125	Some fixed (eg. $19, 83$)	16	§3.2
22	1.200	Some fixed (eg. $1, 3$)	20	§3.2
28	1.250	Some fixed (eg. 11)	24	§3.2
46	1.091	Some fixed (eg. 1)	44	§3.2

Table 6: Improved rho-values of families obtained by the proposed method

Indeed, the method can be considered a kind of generalization of the the methods proposed in [10], [14] and [3]. This explains why our method arrives at the existing records of rho-values for the remaining embedding degrees.

Note that the choice of D in our method is relatively free compared to another methods that use fixed discriminants. In fact, this provides a cause of the improvement in the rho-values by increasing the degree of polynomials concerned. We can see in the table several example D values for each k, and another many choices are possible.

The table 2 of §3.2 shows that the rho-value of a family obtained by our method can be improved also for the case of $k = 40$. We give no example for this case at present, because of some implementation problem. However, we conjecture that a little improvement of strategy will give examples.

References

[1] Leonard Adleman and Jonathan DeMarrais, *A subexponential algorithm for discrete logarithms over all finite fields*, Algorithmic Number Theory. LNCS **877** (1994), 147-158.

[2] Ramachandran Balasubramanian, Neal Koblitz, *The Improbability That an Elliptic Curve Has Subexponential Discrete Log Problem under the Menezes - Okamoto - Vanstone Algorithm*, J. Cryptology **11** (1998), 141-145.

[3] Paulo Barreto and Michael Naehrig, *Pairing-friendly elliptic curves of prime order*, Selected Areas in Cryptography, LNCS **3897** (2006), 319-331.

[4] Paul Bateman, Roger Horn, *A heuristic asymptotic formula concerning the distribution of prime numbers*, Mathematics of Computation **16** (1962), 363-367.

[5] Dan Boneh and Matt Franklin, *Identity-based encryption from the Weil pairing*, Advances in Cryptology, LNCS **2139** (2001), 213 - 229.

[6] John Boxall, *Heuristics on pairing-friendly elliptic curves*, J. Mathematical Cryptology **6(2)** (2012), 81-104.

[7] Friederike Brezing, Annegret Weng, *Elliptic curves suitable for pairing based cryptography*, Designs, Codes and Cryptography **37** (2005), 133-141.

[8] Max Deuring, *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper.* Abh. Math. Sem. Hansischen Univ. **14** (1941), 197-272.

[9] Robert Dryło, *On constructing families of pairing-friendly curves with variable discriminant*, Progress in Cryptology - INDOCRYPT 2011, LNCS **7107** (2011), 310-319.

[10] David Freeman, Michael Scott, Edlyn Teske, *A taxonomy of pairing-friendly elliptic curves*, J. Cryptology **23** (2010), 224-280.

[11] Gerhard Frey, Michael Müller and Hans-Georg Rück, *The Tate pairing and the discrete logarithm applied to elliptic curve cryptosystems*, IEEE Trans. Inform. Theory **45(5)** (1999), 1717-1719.

[12] Florian Hess, *Pairing lattices*, Pairing-Based Cryprography - Pairing 2008, LNCS **5209** (2008), 18-38.

[13] Antoine Joux, *A one round protocol for tripartite Diffie-Hellman*, Algorithmic Number Theory - ANTS-IV, LNCS **1838** (2000), 385-393.

[14] Ezekiel Kachisa, Edward Schaefer, Michael Scott, *Constructing Brezing-Weng Pairing-Friendly Elliptic Curves Using Elements in the Cyclotomic Field*, Pairing-Based Cryptography - Pairing 2008, LNCS **5209** (2008), 126-135.

[15] Serge Lang. *Algebra* Springer, 3rd edition (2002).

[16] Alfred Menezes, T. Okamoto, Scott Vanstone, *Reducing elliptic curve logarithms to logarithms in a finite field*, IEEE Transactions on Information Theory, **39(5)** (1993), 1639-1646.

[17] Alfred Menezes, *Elliptic Curve Public Key Cryptosystems*, Kluwer Academic Publishers (1993).

[18] Angela Murphy, Noel Fitzpatrick, *Elliptic Curves for Pairing Applications*, Cryptology ePring Archive Report 2005/302.

[19] A. Miyaji, M. Nakabayashi and S. Takano, *New explicit conditions of elliptic curve traces for FR-reduction*, IEICE Trans. Fundamentals **E84** (2001), 1234-1243.

[20] François Morain, *Classes d'isomorphismes des courbes elliptiques supersingulières en caracteristique* ≥ 3, Utilitas Mathematica **52** (1997), 241-253, .

[21] R. Sakai, K. Ohgishi, and M. Kasahara, *Cryptosystems based on pairing*, The 2000 Symposium on Cryptography and Information Security - SCIS 2000, 26-28.

[22] Frederik Vercauteren, *Optimal pairings*, IEEE Transactions on Information Theory **56** (2010), 455-461.