Construction of Pairing-Friendly Elliptic Curves

Woo Sug Kang

Department of Mathematics, Korea University
136-701, Seoul, Korea

Abstract

The aim of this paper is to construct pairing friendly elliptic curves. In this paper, we explain a method of finding the polynomials representing $\sqrt{-D}$ and ζ_k over the field containing $\sqrt{-D}$ and ζ_k and how to construct a pairing friendly elliptic curves over the cyclotomic fields containing $\mathbb{Q}(\zeta_k, \sqrt{-D})$ for arbitrary k and D by CP method. By using the factorization of the cyclotomic polynomial combined some polynomial, we extend the construction over cyclotomic fields to the construction over some extensions of the cyclotomic fields containing $\mathbb{Q}(\zeta_k, \sqrt{-D})$. We explain the limitation of finding more families of pairing friendly elliptic curves with embedding degree 10. For all computation, we use the PARI-GP [13].

1 Introduction

We begin by defining some notations. The embedding degree is related to the pairings on elliptic curves. Let E be an elliptic curve defined over a field $\mathbb{F}_q$, where q is prime or prime power. Consider the weil pairing

$$e_n : E[r] \times E[r] \to \mu_r,$$

where $E[r]$ is the r torsion group of $E(\overline{\mathbb{F}}_q)$ and μ_r is the group of r th roots of unity. Some extension of $\mathbb{F}_q$ contains μ_r. The smallest extension degree of $\mathbb{F}_q$ is called the *embedding degree* of E. We can define the embedding degree as the following.

Definition 1.1 *Let E be an elliptic curve defined over $\mathbb{F}_q$, and let r be an order of prime subgroup of E. Then E is said to have an embedding degree k with respect to r if r divides $q^k - 1$, but does not divides $q^i - 1$ for all $0 < i < k$.*

The pairings like the Weil pairing, converts a discrete logarithm problem in $E(\mathbb{F}_q)$(ECDLP) to one in $\mathbb{F}^*_{q^k}$(DLP). The pairing based cryptography uses this fact. To define the pairing friendly elliptic curve, we need one more parameter $\rho = \log q/\log r$, the ratio of the size between the finite field and the order of subgroup of an elliptic curve. An ordinary elliptic curve over $\mathbb{F}_q$ is called a *pairing friendly elliptic curve* if the embedding degree is not too large and its ρ value is close to 1. For the supersingular curves, there is a well known fact that its embedding degrees are less than or equal to 6 [19].

We consider nonsupersingular elliptic curves. There are several methods of constructing elliptic curves with prescribed embedding degree k [2, 3, 5, 9, 10, 11, 18, 21]. All of these construction use the complex multiplication method(CM method). To apply the CM method, we have to solve the following diophantine equation for given a prime or a prime power q and a positive integer D.

$$Dy^2 = 4q - t^2.$$

If we find the solution, an order of the elliptic curve E over $\mathbb{F}_q$ made by CM method is

$$q + 1 - t.$$

Thus to make a pairing friendly elliptic curve by CM method, we need to find (t,r,q) satisfying the following conditions:

Condition 1.2 (pairing friendly elliptic curve)

(1) q is a prime of prime power and r is a prime.

(2) r divides $q + 1 - t$.

(3) r divides $q^k - 1$ but does not divides $q^i - 1$ for $1 < i < k$.

(4) $Dy^2 = 4q - t^2$ for some integer y.

The Condition 1.2.(3) is changed by the following lemma [2].

Lemma 1.3 [2, Lemma 1] *Conditions 1.2.(3) implies that r divides $\Phi_k(t-1)$, where $\Phi_k(t)$ is k the cyclotomic polynomial.*

To obtain families of curves, we can parametrize t, r and q as polynomials $t(x)$, $r(x)$ and $q(x)$.

Definition 1.4 [10, Definition 2.6] *Let $t(x)$, $r(x)$ and $q(x)$ be polynomials with rational coefficients. For a given positive integer k and positive square-free integer D, we say that the triple $(t(x), r(x), q(x))$ represents a family of elliptic curves with embedding degree k and discriminant D if the following conditions are satisfied:*

(1) $q(x)$ represents primes or prime power and $r(x)$ represents primes.

(2) $r(x)$ divides $q(x) + 1 - t(x)$.

(3) $r(x)$ divides $\Phi_k(t(x) - 1)$, where $\Phi_k(x)$ is the k-th cyclotomic polynomial.

(4) $Dy^2 = 4q(x) - t(x)^2 = 4h(x)r(x) - (t(x)-2)^2$ *has infinitely many integer solutions,*

where $h(x)$ *is a cofactor of* $\#E(\mathbb{F}_q) = h(x)r(x) = q(x) + 1 - t(x)$.

Now we define $\rho = \deg q(x)/\deg r(x)$.
The goal of most constructions is to find polynomials $(t(x), r(x), q(x))$ satisfying Definition 1.4.

Brezing and Weng gave the construction based on CP method [5].

Construction 1.5 (Brezing and Weng's method)

1. Fix D, $k \in \mathbb{N}$.
2. Choose an irreducible polynomial $r(x)$ such that ζ_k, $\sqrt{-D} \in K$, where ζ_k is a primitive k-th root of unity and $K = \mathbb{Q}[x]/(r(x))$.
3. Choose $t(x)$ which represents $1 + \zeta_k$ in K.
4. Choose $b(x)$ which represents $\sqrt{-D}$ in K.
5. Compute $y(x) = (t(x) - 2)b(x)/D$ in K.
6. Compute $q(x) = (t(x)^2 + Dy(x)^2)/4 \in \mathbb{Q}[x]$.
7. If $q(x)$ and $r(x)$ represent prime for some x, by the CM method, construct an elliptic curve over $\mathbb{F}_{q(x)}$ with an order $r(x)$ subgroup.

The elliptic curves constructed by this method have ρ less than 2. The difficult point of Construction 1.5 is to find a polynomial $r(x)$ satisfying the following condition:

Condition 1.6

(1) $K = \mathbb{Q}[x]/(r(x))$ *contains* ζ_k *and* $\sqrt{-D}$.

(2) The polynomials represent ζ_k *and* $\sqrt{-D}$ *are easily found.*

(3) $q(x)$ *represent primes or prime power and* $r(x)$ *represents primes.*

The smallest field satisfying Condition 1.6.(1) is $\mathbb{Q}(\zeta_k, \sqrt{-D})$. But if this field is not a cyclotomic field, denominators of coefficients of $t(x)$ and $b(x)$ are very large in generally. We give some example for this in section 3. Most previous results are produced when $\mathbb{Q}(\zeta_k, \sqrt{-D})$ is a cyclotomic field. i.e. D's are 1, 2 or 3 [5].

In this paper, we explain how to construct a pairing friendly elliptic curves over some extension fields of $\mathbb{Q}(\zeta_k, \sqrt{-D})$ for arbitrary k and D. First, we work over cyclotomic field. One of advantages of cyclotomic field is that the ring of algebraic integer of cyclotomic field $\mathbb{Q}(\zeta_l)$ is $\mathbb{Z}[\zeta_l]$.

Lemma 1.7 *If* $\sqrt{-D}$ *is contained in* $\mathbb{Q}(\zeta_l)$ *then* $\sqrt{-D}$ *is represented by* ζ_l *with integer coefficients.*

Proof. The ring of algebraic integer of $\mathbb{Q}(\zeta_l)$ is $\mathbb{Z}[\zeta_l]$ and $\sqrt{-D}$ is an algebraic integer. Thus there is $\sqrt{-D}$ in $\mathbb{Z}[\zeta_l]$. □

Since $\sqrt{-D}$ is represented by ζ_l with integer coefficients, Lemma 1.7 guarantees Condition 1.6.(2) and (3) for many cases of $q(x)$. Another advantage is that $r(x)$ always represent primes. Section 2.4 explains this.

The remaining problem is how to find polynomials representing $\sqrt{-D}$ and ζ_k. In previous works, they found such polynomials with some conditions of k and D. We explain the method of finding the polynomials representing $\sqrt{-D}$ and ζ_k over cyclotomic fields without any conditions. By using this method , we make a general construction over cyclotomic fields.

Barreto and Naehrig proposed the method that applied the idea of Galbraith, McKee and Valença to Brezing and Weng's method, especially in Construction 1.5, they let $r(x)$ be an irreducible factor of $\Phi_k(u(x))$ for some polynomial $u(x)$ [3]. We explain this method in Section 4.

This paper is organized as follows:
In Section 2, we explain the choice of cyclotomic fields containing ζ_k and $\sqrt{-D}$ and the method of computing polynomials representing ζ_k and $\sqrt{-D}$. When $q(x)$ is reducible, we give some results on an extension of finite field. In Section 3, we explain the construction over $\mathbb{Q}(\zeta_k, \sqrt{-D})$ where this is not a cyclotomic field and its problems. In Section 4, we explain the factorization of $\Phi_k(u(x))$ for some $u(x)$ and make a construction on extensions of cyclotomic fields by using Barreto and Naehig's idea. In Section 5, we explain the limitation of find more families of pairing friendly elliptic curves with embedding degree 10. In Section 6, we give the tables of results.

2 Construction on $\mathbb{Q}(\zeta_k, \zeta_d)$

The following is the main construction on cyclotomic field.

Construction 2.1 (Construction on cyclotomic field)

1. [Initialize]

   Fix D, $k \in \mathbb{N}$, where D is a square free integer.

   Let d be D if $D \equiv 3 \bmod 4$, $4D$ if $D \equiv 1$ or $2 \bmod 4$.

   Let $l = \mathrm{lcm}(k, d)$.

   Let $r(x) = \Phi_l(x)$, where $\Phi_l(x)$ is l-th cyclotomic polynomial.

   Let $K = \mathbb{Q}[x]/(r(x)) = \mathbb{Q}(\zeta_l)$.

2. [Find the polynomials representing to ζ_k and $\sqrt{-D}$]

   Let $t(x) = 1 + x^{\alpha}$, where α is multiple of l/k.

   By the Table 3, find $b(x)$ representing to $\sqrt{-D}$ in K.

3 [Compute the family]

Compute $y(x) = (t(x) - 2)b(x)/D$ in K.

Compute $q(x) = (t(x)^2 + Dy(x)^2)/4$ in $\mathbb{Q}[x]$.

4. [Check Definition 1.4.(1)]

Check whether $q(x)$ satisfies Definition 1.4.(1).

5. [Construct an elliptic curve]

If $q(x)$ and $r(x)$ represent primes for some x, by the CM method, construct an elliptic curve over $\mathbb{F}_{q(x)}$ with an order $r(x)$ subgroup.

Since deg $r(x)$ increases as D increases, we can expect that ρ will be more near to 1 for large D. But we almost obtain the best ρ values when D is small. We compute that for deg $r(x) \leq 100$, $k \leq 50$ and $D \leq 50$. When D is equal to 1, 2 or 3, ρ is the minimum value, except $k = 3$, 4 and 6. We give the result table in section 6.

Now we explain each steps.

2.1 Step 1 : Initialize

We have to construct a field K which has ζ_k and $\sqrt{-D}$. For any square free integer D, let d be D if D is equivalent to 3 modulo 4, $4D$ otherwise i.e. $-d$ is the discriminant of $\mathbb{Q}(\sqrt{-D})$. The following lemma gives the method of choice of cyclotomic field containing ζ_k and $\sqrt{-D}$.

Lemma 2.2 *$\mathbb{Q}(\zeta_d)$ is the minimal cyclotomic field containing $\sqrt{-D}$, where $-d$ is the discriminant of $\mathbb{Q}(\sqrt{-D})$.*

Proof. By Conductor-discriminant Formula [25], $-d$ is equal to its conductor. □

Lemma 2.2 shows that $K = \mathbb{Q}(\zeta_l)$ is the minimal l-th cyclotomic field which has ζ_k and $\sqrt{-D}$.

2.2 Step 2 : Polynomials representing ζ_k and $\sqrt{-D}$

There are $\varphi(k)$ numbers of primitive k-th roots of unity and the polynomial $x^{l/k}$ is one of k-th roots of unity in K. If $\gcd(\alpha, k) = 1$, $(x^{l/k})^\alpha$ is also a primitive k-th root of unity. Thus we can choose $\varphi(k)$ numbers of polynomials representing primitive k-th roots of unity.

The polynomial $x^{l/d}$ is corresponding to ζ_d in K. There are $\varphi(d)$ numbers of primitive d-th roots of unity, but a square root of $-D$ has only two possibility, $\pm\sqrt{-D}$. So if we represent $\sqrt{-D}$ by one of primitive d-th roots of unity, we can find the polynomial corresponding to $\sqrt{-D}$ in K. Since $\sqrt{-D}$ is in $\mathbb{Q}(\zeta_d)$

and integral, we can find the solutions of the polynomial $x^2 + D$ in K, moreover $\mathbb{Z}[\zeta_d]$. We compute this equation by **PARI** [13]. There is a function in **PARI** which gives the roots of the polynomial in number field. The following is the Code of finding the representation of $\sqrt{-D}$ in ζ_d.

PARI Code : Find the representation of $\sqrt{-D}$ in ζ_d

Input : D

Output : polynomial corresponding to $\sqrt{-D}$ in $\mathbb{Q}(\zeta_d)$

```
Represent_D(D) = \
{
  local( d,f,nf,sqD ) ; \
  if ( issquarefree(D) , \
       d = -quaddisc(-D) ; \
       f=polcyclo(d,y) ; \
 /* initialize of number field nf */
       nf=nfinit(f) ; \
 /* roots of x^2+D in nf */
       sqD=nfroots(nf,x^2+D) ; \
 /* change the variable y to x */
       sqD=subst(sqD[2].pol,y,x) ; \
 ) ; \
 sqD
}
```

We make a table for the representations of $\sqrt{-D}$ in $\mathbb{Q}(\zeta_d)$ in section 6.

2.3 Step 3 : Compute the family

All computations for polynomials, in Construction 2.1, is worked in K except $q(x)$ i.e. compute them modulo $r(x)$.

Lemma 2.3 *ρ is less that 2.*

Proof. deg$t(x)$ and deg$y(x)$ are less than deg$r(x)$. Thus since $q(x) = (t(x)^2 + Dy(x)^2)/4$, deg$q(x)$ is less than 2deg$r(x)$ and so ρ=deg$q(x)$/deg$r(x)$ is less that 2. □

2.4 Step 4 : Check Definition 1.4.(1)

We have to check whether $q(x)$ and $r(x)$ satisfy Definition 1.4.(1). To do it, we need the following conjecture.([11, 14])

Conjecture 2.4 ([11, 14]) *There are infinitely many $a \in \mathbb{Z}$ such that $f(a)$ is prime if the following three conditions are satisfied:*

(1) The leading coefficient of f is positive.

(2) f is irreducible.

(3) The set of values $f(\mathbb{Z}^+)$ has no common divisor larger than 1.

For any l, $r(x) = \Phi_l(x)$ satisfies this conjecture.

Proposition 2.5 *For any l, the set of values $\Phi_l(\mathbb{Z}^+)$ has no common divisor larger than 1.*

Proof. If l is equal to 1, it is clear. Suppose that l is larger than 1.
Recall that

$$x^l - 1 = \prod_{d|l} \Phi_d(x).$$

Since $\Phi_1(x) = x - 1$, $\Phi_l(x)$ divides

$$\frac{x^l - 1}{x - 1} = x^{l-1} + x^{l-2} + \cdots + 1.$$

Thus $\Phi_l(1)$ divides l and $\Phi_l(l)$ divides $l^{l-1} + l^{l-2} + \cdots + 1$. Since $\gcd(l, l^{l-1} + \cdots + 1) = 1$, $\gcd(\Phi_l(1), \Phi_l(l)) = 1$. □

Thus we only check for $q(x)$ by computing for some values.

2.5 Construct an elliptic curve

Suppose that $r(x)$, $q(x)$, $t(x)$ and $y(x)$ represent some prime r, prime power q and some integers t and y for some $x \in \mathbb{Z}$, where q is not divided by 2. Then

$$4q^2 = t^2 + Dy^2.$$

An order of the elliptic curve constructed from (q, t, y) by CM method is divided by r.

Let $k = \mathbb{Q}(\sqrt{-D})$, $\mathcal{O}_k$ a ring of algebraic integer of k and $\mathcal{O}_k^*$ a unit group of $\mathcal{O}_k$.
First, we have to find a root of the Hilbert class polynomial of D modulo r for given D, say j_0. Then j_0 is the j-invariant of an elliptic curve E_{j_0} of the form

$$\begin{array}{lllllll} E_{j_0} & : & y^2 = x^3 + 3\kappa x + 2\kappa & \textit{with} & \kappa & = \dfrac{j_0}{1728 - j_0} & \textit{if} \;\; D \neq 1, 3 \\ E_{j_0} & : & y^2 = x^3 + ax & \textit{with} & a & \in \mathbb{F}_q{}^* & \textit{if} \;\; D = 1 \\ E_{j_0} & : & y^2 = x^3 + b & \textit{with} & b & \in \mathbb{F}_q{}^* & \textit{if} \;\; D = 3. \end{array}$$

Let

$$\pi = \frac{t + \sqrt{-D}y}{2}.$$

Then

$$\begin{aligned} \#E_{j_0}(\mathbb{F}_q) &= N_k(1-\zeta\pi) \\ q &= N_k(\zeta\pi) \end{aligned}$$

for $\pi \in \mathcal{O}_k$ and $\zeta \in \mathcal{O}_k^*$.
If D =1 or 3 then j_0=1728 or 0 and the corresponding elliptic curves have quartic or sextic twists, respectively. If $D \neq 1$ and 3, the elliptic curve has quadratic twists. Especially, the quadratic twist of E_{j_0} is of the form

$$E'_{j_0} \ : \ y^2 = x^3 + 3\kappa c^2 x + 2\kappa c^3$$

where $\kappa = j_0/(1728 - j_0)$ and $c \in \mathbb{F}_q$.
So we have to choose an elliptic curve with the correct order among the twists. Let m be an integer such that $m = N_k(1-\zeta\pi)$ and it is divided by r. Let $m' = N_k(1-\zeta'\pi)$ for some ζ' not equal to $\zeta \in \mathcal{O}_k^*$. If $[m]P = \infty$ and $[m']P \neq \infty$ for some $P \in E_{j_0}(\mathbb{F}_q)$ then E_{j_0} is the elliptic curve that we want to find.

We explain the CM method in Appendix A.

2.6 Some results when $q(x)$ is reducible

If $q(x)$ is a power of irreducible polynomial, we may construct a pairing friendly elliptic curve over extension of finite field. It is not always possible. The followings are only results in our computation when $q(x)$ is a power of irreducible polynomial.

Some families over extension of prime field :

Example 2.6 $k = 3$, $D = 3$, $\alpha = 1$.

$$\begin{aligned} r(x) &= x^2 + x + 1. \\ t(x) &= x + 1. \\ q(x) &= (x+1)^2. \end{aligned}$$

If $x + 1$ is prime or prime power and $x^2 + x + 1$ is prime, we can construct an elliptic curve over $\mathbb{F}_{(x+1)^2}$ with embedding degree 3 and $\rho = 1$.

Example 2.7 $k = 3$, $D = 3$, $\alpha = 2$.

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

If x is prime or prime power and x^2+x+1 is prime, we can construct an elliptic curve over $\mathbb{F}_{x^2}$ with embedding degree 3 and $\rho = 1$.

Example 2.8 $k = 4,\ D = 1,\ \alpha = 1.$

$$\begin{aligned} r(x) &= x^2 + 1. \\ t(x) &= x + 1. \\ q(x) &= 1/2(x + 1)^2. \end{aligned}$$

If $q(x)$ is prime power, $x + 1$ is a power of 2. Then $x^2 + 1$ is always divided by 2. i.e. $r(x)$ cannot be prime. So the construction is impossible.

Example 2.9 $k = 4,\ D = 1,\ \alpha = 3.$

$$\begin{aligned} r(x) &= x^2 + 1. \\ t(x) &= -x + 1. \\ q(x) &= 1/2(x - 1)^2. \end{aligned}$$

If $q(x)$ is prime power, $x - 1$ is a power of 2. Then $x^2 + 1$ is always divided by 2. i.e. $r(x)$ cannot be prime. So the construction is impossible.

Example 2.10 $k = 6,\ D = 3,\ \alpha = 1.$

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

If $q(x)$ is prime power, $x + 1$ is a power of 3. Then $x^2 - x + 1$ is always divided by 3. i.e. $r(x)$ cannot be prime. So the construction is also impossible.

Example 2.11 $k = 6,\ D = 3,\ \alpha = 5.$

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

If $q(x)$ is prime power, $x - 1$ is a power of 3. Then $x^2 - x + 1$ is always divided by 3. i.e. $r(x)$ cannot be prime. So the construction is also impossible.

Consider the field $\mathbb{F}_q$ with characteristic 2 or 3. Let $q = p^n$, where p=2 or 3.

Lemma 2.12 *Let r be the largest prime factor of an elliptic curve E over $\mathbb{F}_{p^n}$. Then the embedding degree*

$$k = \mid p^n \mid = \frac{\mid p \mid}{\gcd(\mid p \mid, n)}.$$

where $\mid a \mid$ is multiplicative order of a modulo r.

Proof. r divides $q^k - 1 = p^{nk} - 1$ and does not divide $p^{ni} - 1$ for $0 < i < k$. Thus the multiplicative order of p^n modulo r is k. □

If $\mid p \mid$ is small, we expect a small embedding degree k. But for most prime r, 2 and 3 have a large order. Thus most ordinary curves over a finite field with chatacteristic 2 or 3 have a large embedding degree. In Example 2.6, $r(2^i)$ and $r(3^j)$ are prime when i =1, 3 and j =1, 3, 9 for $i, j < 1000$, respectively.
Note that if r divides $2^{nk}-1$, then l is a prime factor of nk-th mersenne number.

3 Construction on $\mathbb{Q}(\zeta_k, \sqrt{-D})$

Let $K = \mathbb{Q}(\zeta_k, \sqrt{-D})$. We also construct pairing friendly elliptic curves over K, where this field is not a cyclotomic field i.e. d does not divide k. The following is the PARI code of finding the representation of ζ_k and $\sqrt{-D}$ in K.

PARI Code : Find the representation of ζ_k and $\sqrt{-D}$ in $\mathbb{Q}(\zeta_k, \sqrt{-D})$

`Input :  k, D`
`Output :  r(x), t(x) and b(x) in` $\mathbb{Q}(\zeta_k, \sqrt{-D})$

```
 Represent_kD(k,D)= \
 {
  local(POLCOMP,r,sq_D,ZETA_k) ; \
  if ( issquarefree(D),\
       POLCOMP=polcompositum(x^2+D,polcyclo(k),1)[1] ; \
       r=POLCOMP[1] ; \
       sq_D=POLCOMP[2].pol ; \
       ZETA_k=POLCOMP[3].pol ; \
  ) ; \
 [r,ZETA_k+1,sq_D]
}
```

We only use the PARI function **polcompositum**. This gives the polynomial $r(x)$, and the roots of $x^2 + D = 0$ and $\Phi_k(x) = 0$ as elements of $\mathbb{Q}[x]/(r(x))$. If K is not a cyclotomic field, the denominator of coefficients of $r(x)$ are growing as D and k increases. **polred** in PARI, makes its coefficient small. But the degree of decrease is only a little and this function is very slow. So this method is not good for large discriminant and large k.

Example 3.1 $k = 8,\ D = 17.$

$$\begin{aligned}
K &= \mathbb{Q}(\zeta_8, \sqrt{-17}). \\
r(x) &= x^8 + 68x^6 + 1736x^4 + 19448x^2 + 84100. \\
t(x) &= -17/267960x^7 - 607/133980x^5 - 17221/133980x^3 - 39268/33495x + 1. \\
b(x) &= -17/267960x^7 - 607/133980x^5 - 17221/133980x^3 - 72763/33495x. \\
q(x) &= 17/15956124800x^{14} - 1/2475950400x^{13} + 186583/1220643547200x^{12} - \\
&\quad \cdots - 41207687/30949380x + 1921757/853776.
\end{aligned}$$

Example 3.2 $k = 7,\ D = 1.$

$$\begin{aligned}
K &= \mathbb{Q}(\zeta_7, \sqrt{-1}) \\
r(x) &= x^{12} + 2x^{11} + 9x^{10} + 14x^9 + 31x^8 + 34x^7 + 41x^6 + 12x^5 - 23x^4 \\
&\quad -28x^3 + 11x^2 + 8x + 1. \\
t(x) &= -114243472/65265341x^{11} - 204769600/65265341x^{10} \\
&\quad -988109696/65265341x^9 - 1398866651/65265341x^8 \\
&\quad -3273455408/65265341x^7 - 3238008452/65265341x^6 \\
&\quad -4092584160/65265341x^5 - 608191962/65265341x^4 \\
&\quad +2627467472/65265341x^3 + 2600701292/65265341x^2 \\
&\quad -1754413800/65265341x - 439258918/65265341. \\
q(x) &= 8021189411500160/4259564735846281x^{22} \\
&\quad +28586727396255616/4259564735846281x^{21} \\
&\quad +163906886117738456/4259564735846281x^{20} \\
&\quad +441581971739245064/4259564735846281x^{19} \\
&\quad +\cdots \\
&\quad +1002227778135310510/4259564735846281x \\
&\quad +124828323194560706/4259564735846281.
\end{aligned}$$

Example 3.3 $k = 7,\ D = 1.$
By the method in section 2,

$$\begin{aligned}
K &= \mathbb{Q}(\zeta_7, \zeta_4). \\
r(x) &= x^{12} - x^{10} + x^8 - x^6 + x^4 - x^2 + 1. \\
t(x) &= x^4 + 1. \\
q(x) &= 1/4(x^{22} - 2x^{18} + x^{14} + x^8 + 2x^4 + 1).
\end{aligned}$$

Remark 3.4 Example 3.1, 3.2 show that the degree of increase of coefficients is more influenced by k than D. Strictly speaking, it is influenced by the degree $\varphi(k) = [\mathbb{Q}(\zeta_k) : \mathbb{Q}]$.

Remark 3.5 Example 3.2, 3.3 are constructed over the same field $\mathbb{Q}(\zeta_7, \sqrt{-1}) = \mathbb{Q}(\zeta_7, \zeta_4)$. These examples show that the results are very different as the choice of $r(x)$.

Remark 3.6 We can apply this method to all extension fields of $\mathbb{Q}(\zeta_k, \sqrt{-D})$. But if that field does not have a special property, this method is not useful.

4 Construction on extensions of $\mathbb{Q}(\zeta_k, \zeta_d)$

4.1 Construction on extensions of $\mathbb{Q}(\zeta_k, \zeta_d)$

We explain a construction on extensions of $\mathbb{Q}(\zeta_k, \zeta_d)$ by using a factorization of $\Phi_l(u(x))$ for some polynomial $u(x)$.

Lemma 4.1 *Let $r(x)$ be an irreducible factor of $\Phi_l(u(x))$ over $\mathbb{Q}$ for some polynomial $u(x)$ and l an integer defined in Construction 2.1. Let $K = \mathbb{Q}[x]/(r(x))$. Then K contains ζ_k and $\sqrt{-D}$.*

Proof. $\Phi_l(u(x))$ divides $(u(x))^l - 1$. Thus $u(x)$ is a l-th root of unity in K. By Lemma 2.2, ζ_k and $\sqrt{-D}$ are in K. □

By substitution ζ_k by $u(x)$, we can use Construction 2.1 for the construction on some extension fields of $\mathbb{Q}(\zeta_k, \zeta_d)$.

Construction 4.2 (Construction on some extension of cyclotomic field)

1. [Initialize]

   Fix D, $k \in \mathbb{N}$, where D is a square free integer.

   Let d be D if $D \equiv 3 \bmod 4$, $4D$ if $D \equiv 1$ or $2 \bmod 4$.

   Let $l = \mathrm{lcm}(k, d)$.

   Choose a polynomial $u(x)$ in $\mathbb{Q}[x]$ such that $\Phi_l(u(x))$ splits.

   Let $r(x)$ be an irreducible factor of $\Phi_l(u(x))$.

   Let $K = \mathbb{Q}[x]/(r(x))$.

2. [Find the polynomials representing to ζ_k and $\sqrt{-D}$]

   Let $t(x) = 1 + u(x)^\alpha$, where α is multiple of l/k.

   By the Table 3, find $b(x)$ representing to $\sqrt{-D}$ in K.

3 [Compute the family]

   Compute $y(x) = (t(x) - 2)b(x)/D$ in K.

   Compute $q(x) = (t(x)^2 + Dy(x)^2)/4$ in $\mathbb{Q}[x]$.

4. [Check Definition 1.4.(1)]

   Check $r(x)$ and $q(x)$ satisfy Definition 1.4.(1).

5. [Construct an elliptic curve]

   If $q(x)$ and $r(x)$ represent prime for some x, by the CM method, construct an elliptic curve over $\mathbb{F}_{q(x)}$ with an order $r(x)$ subgroup.

Remark 4.3 If the degree of $r(x)$ in Construction 4.2 is equal to $\varphi(l)$, $K = \mathbb{Q}[x]/(r(x))$ is equal to $\mathbb{Q}(\zeta_k, \zeta_d)$.

4.2 The factorization of the cyclotomic polynomials

Galbraith, McKee and Valença explained the factorization of the cyclotomic polynomials with its degree 4 combined a quadratic polynomial by converting some equation in the cyclotomic field into an elliptic curve. But if the degree of combining polynomial is larger than 2, the corresponding equation comes from some curves with large genus. It is very difficult to find rational points of such curves.

Lemma 4.4 *Let $u(x)$ be a polynomial of degree larger than 1 over $\mathbb{Q}$ and $k > 1$. Then*

(1) [6, Lemma 3.6.1] *If $u(x) - \zeta_k$ is irreducible over $\mathbb{Q}(\zeta_k)$ then $\Phi_k(u(x))$ is the power of an irreducible polynomial over $\mathbb{Q}$.*

(2) [12, Lemma 1] *If $u(x) - \zeta_k = 0$ has a solution in $\mathbb{Q}(\zeta_k)$ then $\Phi_k(u(x))$ splits.*

(3) The degrees of irreducible factors of $\Phi_k(u(x))$ are multiples of $\varphi(k)$.

Proof. Define the norm of a polynomial $A(x)$ as

$$\mathcal{N}(A) = \prod_{\sigma \in Gal(\mathbb{Q}(\zeta_k)/\mathbb{Q})} \sigma(A)$$

Then by Galois theory $\mathcal{N}(A) \in \mathbb{Q}[x]$.

(1) Let $v(x) = u(x) - \zeta_k$. Suppose that $v(x)$ is irreducible over $\mathbb{Q}(\zeta_k)$. Let $\mathcal{N}(v) = \prod_i v_i$ be a factorization of $\mathcal{N}(v)$. Since $v(x)$ divides $\mathcal{N}(v)$ and $v(x)$ is irreducible over $\mathbb{Q}(\zeta_k)$, $v(x)$ divides $v_i(x)$ in $\mathbb{Q}(\zeta_k)[x]$ for some i. Since $v_i(x)$ is a polynomial over $\mathbb{Q}$, $\sigma(v(x))$ divides v_i in $\mathbb{Q}(\zeta_k)$ for all $\sigma \in Gal(\mathbb{Q}(\zeta_k)/\mathbb{Q})$. Thus $\mathcal{N}(v)$ divides $v_i^{\varphi(k)}$ in $\mathbb{Q}[x]$ and $\mathcal{N}(v)$ is equal to $\Phi_k(u(x))$. So $\Phi_k(u(x)) = v_i^n$ for some $n \geq \varphi(k)$.

(2) Let θ be a solution of $u(x) - \zeta_k$ in $\mathbb{Q}(\zeta_k)$. Then θ is also a solution of $\Phi_k(u(x))$. Since $\theta \in \mathbb{Q}(\zeta_k)$, $\Phi_k(u(x))$ is reducible over $\mathbb{Q}$.

(3) Let $l(x)$ be an irreducible factor of $\Phi_k(u(x))$. Then $l(x)$ divides $u(x)^k - 1$ i.e. $u(x)$ is a k-th root of unity of $\mathbb{Q}[x]/(l(x))$. Since $\mathbb{Q}[x]/(l(x))$ contains $\mathbb{Q}(\zeta_k)$, $\deg l(x) = [\mathbb{Q}[x]/(l(x)) : \mathbb{Q}]$ is divided by $\varphi(x)$. □

Remark 4.5 The converse of Lemma 4.4.(1) is not true. Suppose $v(x) = u(x) - \zeta_k$ is reducible over $\mathbb{Q}(\zeta_k)$. Let $v(x) = v_1(x)v_2(x)$. Then $\Phi_k(u(x)) = \mathcal{N}(v) = \mathcal{N}(v_1)\mathcal{N}(v_2)$. But there is the case that $\mathcal{N}(v_1)$ is equal to $\mathcal{N}(v_2)$. When $\varphi(k) \leq 3$, converse is true by Lemma 4.4.(2).

If $u(x)$ is a quadratic polynomial with integer coefficient, we can solve the equation $u(x) = \zeta_k$ by the following lemma.

Lemma 4.6 *Suppose that $A\zeta_k + B$ is a square in $\mathbb{Q}(\zeta_k)$, where A and B are rational integers and $Ac + B$ is square for some c in $\mathbb{Q}$. Then there exists a quadratic polynomial $u(x)$ such that $\Phi_k(u(x))$ is factored into two irreducible polynomials of degree $\varphi(k)$. $u(x)$ is of the form*

$$A/4x^2 + \sqrt{Ac+B}x + c.$$

Proof. Let

$$x = \frac{-b \pm \sqrt{A\zeta_k + B}}{2a}$$

Then x is a solution of $ax^2+bx+c = \zeta_k$ in $\mathbb{Q}(\zeta_k)$, where $a = A/4$, $b = \sqrt{Ac+B}$. By Lemma 4.4, this is true. □

We find the necessary conditions of a factorization of $\Phi_k(ax^n)$ for $n = 1, 2, 3, 4$.

Lemma 4.7

(1) *Suppose that $\Phi_k(ax^2)$ is reducible over $\mathbb{Q}$, where a is a square free integer. Then a is a divisor of k or $k/2$ if k is odd or even, respectively.*

(2) *Suppose that $\Phi_k(ax^4)$ is reducible over $\mathbb{Q}$, where a is a quartic free integer. Then a squarefree part of a is a divisor of k or $k/2$ if k is odd or even, respectively.*

(3) *If $\Phi_k(x^n)$ splits, it is a product of cyclotomic polynomials.*

(4) *If k is divided by 4 then $\Phi_k(x)$ is an even polinomial.*

Proof. (1) Suppose that $\Phi_k(ax^2)$ is reducible over $\mathbb{Q}$. By Lemma 4.4, $ax^2 - \zeta_k$ has a solution in $\mathbb{Q}(\zeta_k)$. If k is odd, ζ_k is a square in $\mathbb{Q}(\zeta_k)$. So a is also a square. By Lemma 2.2, a divides k. Let k be even. $ax^2 - \zeta_k$ has also a solution in $\mathbb{Q}(\zeta_{2k})$. Since ζ_k is a square in $\mathbb{Q}(\zeta_{2k})$, a is also a square in $\mathbb{Q}(\zeta_{2k})$. By Lemma 2.2, $4a$ divides $2k$.

(2) Suppose that $\Phi_k(ax^4)$ is reducible over $\mathbb{Q}$. By Lemma 4.4, $ax^4 - \zeta_k$ is reducible over $\mathbb{Q}(\zeta_k)$. If k is odd, ζ_k is a square in $\mathbb{Q}(\zeta_k)$. So a is also a square. By Lemma 2.2, a squarefree part of a divides k. Let k be even. $ax^4 - \zeta_k$ is also reducible over $\mathbb{Q}(\zeta_{2k})$. Since ζ_k is a square in $\mathbb{Q}(\zeta_{2k})$, a is also a square in $\mathbb{Q}(\zeta_{2k})$. By Lemma 2.2, a squarefree part of $4a$ divides $2k$.

(3) $\Phi_k(x^n)$ divides $x^{nk}-1$. Since

$$x^m - 1 = \prod_{d|m} \Phi_d(x)$$

an irreducible factor of $\Phi_k(x^n)$ is a cyclotomic polynomial.

(4) Let k=$2k'$ with k' is even.

$$\begin{aligned} \deg\Phi_{k'}(x^2) &= 2\varphi(k') = 2\varphi(k'/2). \\ \deg\Phi_k(x) &= \varphi(k) = 2\varphi(k'/2). \end{aligned}$$

Since ζ_k is a root of $\Phi_{k'}(x^2)$ and $\Phi_k(x)$, $\Phi_{k'}(x^2) = \Phi_k(x)$. □

Remark 4.8 By Lemma 4.7.(4), if 4 divides k then we do not need to consider $\Phi_k(ax^n)$ for a negative a.

Remark 4.9 Let $a = a'b^2$, where a' is a square free integer. If $\Phi_k(ax^2)$ splits, $\Phi_k(ax^4)$ also splits and this is the same result by substitution x to bx^2. Thus we only need to consider ax^4 for square integer a.

Lemma 4.10 *If a not equal to ± 1 is a qubicfree integer and 3 does not divides k then $\Phi(ax^3)$ is irreducible.*

Proof. Suppose that $\Phi(ax^3)$ is reducible. Then by Lemma 4.6, $ax^3 = \zeta_k$ is solvable in $\mathbb{Q}(\zeta_k)$. Since $x^3 = \zeta_k$ is solvable in $\mathbb{Q}(\zeta_k)$ by (1), $x^3 = a$ is also solvable in $\mathbb{Q}(\zeta_k)$. Thus $\mathbb{Q}(\sqrt[3]{a}) \subset \mathbb{Q}(\zeta_k)$. But since the discriminant of $x^3 - a$ is -3^3a^2 i.e. not square, the Galois group of $x^3 - a$ is S_3. Since $\mathbb{Q}(\zeta_k)/\mathbb{Q}$ is an abelian extension, this is a contradiction. □

We factored $\Phi(u(x))$ for degree of $u(x)$ is 3, 4, 5 except above Lemma's and the coefficients of $u(x)$ are less than or equal to 10, and give some results of Construction 4.2 in section 6.

5 The limitation of finding a pairing friendly elliptic curve with embedding degree 10

Theorem 5.1 [12, Theorem 2, 3, 4] *Let $u(x)$ be a quadratic polynomial. Then*

(1) There is no $u(x)$ which splits $\Phi_8(u(x))$.

(2) There is infinitely many $u(x)$ which split $\Phi_k(u(x))$ when k =5, 10.

(3) The only $u(x)$ are $2x^2$ and $6x^2$ which split $\Phi_{12}(u(x))$.

Theorem 5.1 show that there are infinitely many quadratic polynomial $u(x)$ which split $\Phi_k(u(x))$ when $k = 10$. We tried to find another families with embedding degree 10, by using Lemma 4.6.

Theorem 5.2 *For $1 \leq A \leq 4000$ and $-1000 \leq B \leq 1000$,*

(1) There are three integer pair $(A, B) = (40, -55)$, $(44, -32)$ and $(220, -160)$, up to square, satisfying Lemma 4.6 when $k = 10$.

(2) If $(A, B) = (40, -55)$, the CM equation $4r^2(x) - (t(x) - 2)^2$ is a quadratic polynomial, especially, $u(x) = 10x^2 + 5x + 2$. Otherwise the degree of CM equations is 4.

Remark 5.3 If (a, B) satisfies Lemma 4.6, (e^2a, e^2B) also satisfies Lemma 4.6 for any integer e. They represent the same families.

Remark 5.4 In Theorem 5.2.(1), $u(x) = 10x^2 \pm \sqrt{40c - 55}x + c$. For any c which makes $\sqrt{40c - 55}$ square, $u(x)$'s are equal by translation and reflextion.

Example 5.5 (Freeman's family when k = 10)

$$\begin{aligned}
(A, B) &= (40, -55). \\
u(x) &= 10x^2 + 5x + 2. \\
\Phi_{10}(u(x)) &= (25x^4 + 25x^3 + 15x^2 + 5x + 1)(400x^4 + 400x^3 + 240x^2 + 60x + 11) \\
t(x) &= 10x^2 + 5x + 3. \\
r(x) &= 25x^4 + 25x^3 + 15x^2 + 5x + 1. \\
q(x) &= 25x^4 + 25x^3 + 25x^2 + 10x + 3. \\
Dy^2 &= 15x^2 + 10x + 3.
\end{aligned}$$

Example 5.6 *If substitute x by $1 - x$ in example 5.5 then $c = 7$.*

$$u_1(x) = 10x^2 + 15x + 7 = 10(1 - x)^2 + 5(1 - x) + 2.$$

Example 5.7 *If substitute x by $2x$ in example 5.5 then this is the result for $(A, B) = (2^2 \times 10, 2^2 \times (-55))$.*

$$u_2(x) = 40x^2 + 10x + 2 = 10(2x)^2 + 5(2x) + 2.$$

Example 5.8 *Let $(A, B) = (44, -32)$.*

$$\begin{aligned}
u_3(x) &= 11x^2 + 10x + 3. \\
\Phi_{10}(u(x)) &= \quad (11x^4 + 21x^3 + 16x^2 + 6x + 1) \\
&\quad \times (1331x^4 + 2299x^3 + 1606x^2 + 494x + 61).
\end{aligned}$$

Example 5.9 *Let* $(A, B) = (220, -160)$.

$$\begin{aligned} u_3(x) &= 55x^2 + 40x + 8. \\ \Phi_{10}(u(x)) &= \quad (275x^4 + 475x^3 + 315x^2 + 95x + 11) \\ &\quad \times(33275x^4 + 39325x^3 + 18315x^2 + 3945x + 331). \end{aligned}$$

6 Results

Table 1,2 give the best ρ value for our computation.

Table 1 : The best ρ value for k

k	D	ρ	$u(x)$	deg
3	1	1.500	$2x^2, 6x^2$	4
4	3	1.500	$2x^2, 6x^2$	4
	6	1.500	x	8
5	3	1.500	x, x^2	8
6	1	1.500	x	4
	7	1.500	$x, -x^2, 3x^2$	12
7	3	1.333	$x, -3x^2, x^2$	12
8	3	1.250	x	8
9	3	1.333	$x, -3x^2, x^2$	6
10	1	1.500	x, x^3	8
	3	1.500	$3x^2$	8
11	3	1.200	$x, -3x^2, x^2$	20
12	3	1.000	$6x^2$	4
13	3	1.167	$x, -3x^2, x^2$	24
14	3	1.333	$x, -x^2, 3x^2$	12
15	3	1.500	$x, -3x^2, x^2$	8
16	3	1.375	x	16
17	1	1.188	x, x^3	32
18	2	1.583	x	24
19	3	1.111	$x, -3x^2, x^2$	36
20	3	1.375	x	16
21	3	1.333	$x, -3x^2, x^2$	12
22	1	1.300	x, x^3	20
23	3	1.091	$x, -3x^2, x^2$	44
24	3	1.250	x	8
25	3	1.300	$x, -75x^2, -3x^2$ $x^2, 25x^2$	40
26	3	1.167	$x, -x^2, 3x^2$	24
27	3	1.111	x, x^2	18
28	1	1.333	x, x^3	12
29	3	1.071	x, x^2	56
30	3	1.500	$x, -x^2, 3x^2$	8
31	3	1.067	$x, -3x^2, x^2$	60
32	3	1.063	x	32
33	3	1.200	$x, -3x^2, x^2$	20
34	3	1.125	$3x^2$	32
35	3	1.500	$x, -3x^2, x^2$	48
36	2	1.417	x	24
37	3	1.056	$x, -3x^2, x^2$	72
38	3	1.111	$x, -x^2, 3x^2$	36
39	3	1.167	$x, -3x^2, x^2$	24
40	3	1.438	x	32
41	3	1.050	x, x^2	80
42	3	1.333	$x, -x^2, 3x^2$	12
43	3	1.048	$x, -3x^2, x^2$	84
44	3	1.150	x	40
45	3	1.333	$x, -3x^2, x^2$	24
46	3	1.136	$3x^2$	44
47	3	1.043	$x, -3x^2, x^2$	92
48	3	1.125	x	16
49	3	1.190	$x, -147x^2, -3x^2$ $x^2, 49x^2$	84
50	3	1.300	$x, -25x^2, -x^2$ $3x^2, 75x^2$	40

* *deg* means the degree of $r(x)$.

Table 2 : The best ρ value for D

k	D	ρ	$u(x)$	deg
3	**1**	**1.500**	$\mathbf{2x^2, 6x^2}$	**4**
	5	1.875	$6x^2, 10x^2, 30x^2$	16
	7	1.833	$x, -7x^2, -3x^2, x^2, 21x^2$	12
			$-4x^4$	24
	11	1.900	$-11x^2, -3x^2, 33x^2$	20
	13	1.958	$2x^2, 6x^2, 26x^2, 78x^2$	48
	15	1.750	$x, -15x^2, -3x^2, x^2, 5x^2$	8
	19	1.944	$x, -19x^2, -3x^2, x^2, 57x^2$	36
	21	1.917	$2x^2, 14x^2, 42x^2$	24
	23	1.864	$x, -3x^2, x^2$	44
	31	1.967	$x, -31x^2, -3x^2, x^2, 93x^2$	60
	35	1.958	$-35x^2, 21x^2, 105x^2$	48
	39	1.667	x, x^2	24
	43	1.976	$x, -43x^2, -3x^2, x^2, 129x^2$	84
	47	1.935	$x, -3x^2, x^2$	92
4	**3**	**1.500**	$\mathbf{2x^2, 6x^2}$	**4**
	5	1.750	x, x^3	8
	6	**1.500**	$\mathbf{x}$	**8**
	7	1.833	$x, 2x^2, 14x^2, x^3$	12
	11	1.500	$2x^2$	20
	13	1.833	x, x^3	24
	15	1.875	$2x^2, 6x^2, 10x^2, 30x^2$	16
	19	1.944	$x, 2x^2, 38x^2, x^3$	36
	22	1.875	x^3	80
	23	1.864	$2x^2$	44
	29	1.964	x, x^3	56
	30	1.875	x	32
	31	1.967	$2x^2, 62x^2$	60
	35	1.958	$10x^2, 14x^2, 70x^2$	48
	39	1.958	$x, 6x^2, 78x^2$	48
	43	1.976	$86x^2$	84
	47	1.935	$2x^2$	92
5	1	1.750	x, x^3	8
	3	**1.500**	$\mathbf{x, x^2}$	**8**
	5	1.750	x, x^3	8
	7	1.833	x, x^2, x^3	24
	10	1.875	x, x^3	16
	11	1.800	x, x^2, x^3	40
	13	1.979	$2x^2, 26x^2$	96
	15	1.750	$-15x^2, -3x^2, 5x^2$	8
	19	1.833	x, x^2, x^3	72
	21	1.979	$6x^2, 42x^2$	96
	23	1.955	$-23x^2$	88
	35	1.917	$-35x^2, 5x^2$	24
	39	1.979	$-39x^2, -3x^2$	96
6	**1**	**1.500**	$\mathbf{x}$	**4**
	2	1.750	x	8
	5	1.875	$x, 10x^2$	16
	6	1.750	x	8
	7	**1.500**	$\mathbf{x, -x^2, 3x^2}$	**12**
	10	1.938	x	32
	11	1.900	$-33x^2, 3x^2, 11x^2$	20
			$4x^4$	40
	13	1.917	$2x^2$	48
	14	1.958	x	48
	15	1.750	$x, -5x^2, -x^2$	8
	17	1.969	x	64
	19	1.944	$x, -57x^2, -x^2, 3x^2, 19x^2$	36
	21	1.917	$x, 14x^2$	24
	22	1.925	x	80
	23	1.864	$x, -x^2, 3x^2$	44
			$36x^4$	88
	26	1.979	x	96
	30	1.938	x	32
	31	1.700	$x, -x^2$	60
	33	1.850	x	40
	35	1.958	$-105x^2, -5x^2, 3x^2, 7x^2$ $15x^2, 35x^2$	48
	39	1.917	$x, -x^2$	24
	42	1.958	x	48
	43	1.976	$x, -129x^2, -x^2, 3x^2, 43x^2$	84
	47	1.935	$x, -x^2$	92
7	1	1.500	x, x^3	12
	3	**1.333**	$\mathbf{x, -3x^2, x^2}$	**12**
	5	1.958	$x, 2x^2, 10x^2, 14x^2, 70x^2, x^3$	48
	7	1.667	$x, -7x^2, x^2, x^3$	6
	11	1.900	x, x^2, x^3	60
	14	1.750	x, x^3	24
	15	1.958	$x, -35x^2, -15x^2, -7x^2$ $-3x^2, x^2, 5x^2, 21x^2, 105x^2$	48
	35	1.917	$-35x^2, -7x^2, 5x^2$	24
8	1	1.500	$2x^3 + 2x^2 + 4x + 1$ $2x^3 + 4x^2 + 6x + 3$ $9x^3 + 3x^2 + 2x + 1$	4
	2	1.500	$2x^3 + 2x^2 + 4x + 1$ $2x^3 + 4x^2 + 6x + 3$ $9x^3 + 3x^2 + 2x + 1$	4
	3	**1.250**	$\mathbf{x}$	**8**
	7	1.875	x^3	48
	11	1.925	x^3	80
	13	1.875	x, x^3	48
	15	1.938	x	32
	17	1.938	x, x^3	64
	19	1.889	x, x^3	72
	22	1.850	x, x^3	40
	34	1.969	x, x^3	64
9	1	1.833	x	12
	2	1.917	x	24
	3	**1.333**	$\mathbf{x, -3x^2, x^2}$	**6**
	5	1.875	x	48
	6	1.750	x	24
	7	1.833	$x, -3x^2, x^2, 9x^2$	36
	10	1.896	x	96
	11	1.933	$x, -99x^2, -11x^2, x^2$	60
	15	1.833	$x, -15x^2, -3x^2, x^2, 5x^2$ $9x^2, 45x^2$	24
	30	1.938	x	96
	39	1.917	$9x^2$	72

k	D	ρ	$u(x)$	deg
10	**1**	**1.500**	$\mathbf{x, x^3}$	**8**
	2	1.813	x^3	32
	3	**1.500**	$\mathbf{3x^2}$	**8**
	5	1.750	x, x^3	8
	6	1.938	x	32
	7	1.917	$x, -5x^2, -x^2, 7x^2, 35x^2, x^3$	24
	10	1.875	x, x^3	16
	11	1.900	$x, -x^2, x^3$	40
	13	1.938	x, x^3	96
	14	1.938	x, x^3	96
	15	1.500	$15x^2$	8
	19	1.722	$x, -x^2, x^3$	72
	21	1.979	$x, 6x^2, 42x^2, 70x^2, 210x^2$	96
	23	1.932	$x, -5x^2, -x^2, x^3$	88
	30	1.938	x	32
	35	1.917	$x, -5x^2, -x^2, 7x^2, 35x^2, x^3$	24
	39	1.979	$3x^2, 39x^2$	96
11	1	1.300	x, x^3	20
	2	1.975	x^3	80
	3	**1.200**	$\mathbf{x, -3x^2, x^2}$	**20**
	5	1.925	x, x^3	80
	6	1.925	x	80
	7	1.700	x, x^2, x^3	60
	11	1.600	x, x^2, x^3	10
	15	1.925	x, x^2	80
	33	1.950	$6x^2, 22x^2, 66x^2$	40
12	1	1.500	$2x^2$	4
	2	1.750	x	8
	3	**1.000**	$\mathbf{6x^2}$	**4**
	7	1.750	$2x^2$	24
	11	1.850	x	40
	15	1.750	x	16
	17	1.906	$2x^2$	64
	19	1.972	$x, 2x^2, 6x^2, 38x^2, 114x^2$	72
	23	1.932	$x, 2x^2$	88
	33	1.950	$2x^2, 6x^2, 22x^2, 66x^2$	40
	35	1.979	$2x^2, 10x^2, 14x^2, 70x^2$	96
	39	1.917	$2x^2$	48
13	1	1.250	x, x^3	24
	2	1.667	x, x^3	48
	3	**1.167**	$\mathbf{x, -3x^2, x^2}$	**24**
	5	1.896	x, x^3	96
	6	1.896	x	96
	7	1.639	x, x^2, x^3	72
	13	1.750	x, x^3	24
	15	1.896	x, x^2	96
	26	1.875	x, x^3	48
	39	1.833	$x, -3x^2, x^2$	24
14	1	1.500	x, x^3	12
	2	1.750	x, x^3	24
	3	**1.333**	$\mathbf{x, -x^2, 3x^2}$	**12**
	5	1.958	$x, 2x^2, 10x^2, 14x^2, x^3$	48
	6	1.958	x	48
	7	1.583	$x^5 + x^4 + x^3 + x^2 + x + 1$	24
	10	1.979	x, x^3	96
	11	1.867	$x, -x^2, x^3$	60
	14	1.917	x, x^3	24
	15	1.833	$x, -x^2$	48
	21	1.833	x	24
	35	1.917	$x, -5x^2, -x^2, 7x^2, 35x^2, x^3$	24
	42	1.875	x	48
15	1	1.875	$x, 10x^2$	16
	2	1.750	x	32
	3	**1.500**	$\mathbf{x, -3x^2, x^2}$	**8**
	5	1.875	x	16
	6	1.750	x	32
	7	1.917	x, x^2	48
	10	1.938	x	32
	11	1.925	x, x^2	80
	15	1.750	$x, -15x^2, -3x^2, x^2, 5x^2$	8
	21	1.979	$x, 30x^2, 42x^2, 70x^2, 210x^2$	96
	30	1.813	x	32
	35	1.958	$-35x^2, -15x^2, -7x^2, -3x^2$ $5x^2, 21x^2, 105x^2$	48
	39	1.979	$65x^2$	96
16	2	1.625	x^3	16
	3	**1.375**	$\mathbf{x}$	**16**
	5	1.813	x, x^3	32
	7	1.625	x, x^3	48
	10	1.875	x, x^3	32
	11	1.875	x, x^3	80
	14	1.958	x^3	96
	26	1.958	x, x^3	96
17	**1**	**1.188**	$\mathbf{x, x^3}$	**32**
	2	1.750	x, x^3	64
	3	1.125	x, x^2	32
	7	1.563	x, x^2, x^3	96
	17	1.938	x, x^3	32
	34	1.906	x, x^3	64
18	1	1.833	x	12
	2	**1.583**	$\mathbf{x}$	**24**
	3	1.667	$3x^2$	6
			$4x^4, 36x^4$	12
	5	1.875	x	48
	6	1.917	x	24
	7	1.833	$x, -9x^2, -x^2, 3x^2$	36
	11	1.867	$x, -x^2$	60
	15	1.833	$-45x^2, -5x^2, 3x^2, 15x^2$	24
	39	1.944	$39x^2$	72
19	1	1.167	x, x^3	36
	2	1.778	x, x^3	72
	3	**1.111**	$\mathbf{x, -3x^2, x^2}$	**36**
	19	1.667	x, x^2, x^3	18
20	1	1.500	x, x^3	8
	2	1.938	x^3	32
	3	**1.375**	$\mathbf{x}$	**16**
	5	1.750	$2x^2, 10x^2$	8
	6	1.938	x	32
	7	1.792	x^3	96
	11	1.975	$x, 2x^2, 10x^2, 22x^2, 110x^2, x^3$	80
	21	1.979	$2x^2, 6x^2, 10x^2, 14x^2, 30x^2$ $42x^2, 70x^2, 210x^2$	96

k	D	ρ	$u(x)$	deg
	35	1.958	$x, 2x^2, 10x^2, 14x^2, 70x^2, x^3$	48
21	1	1.833	x	24
	2	1.792	x	48
	3	**1.333**	$\mathbf{x, -3x^2, x^2}$	**12**
	5	1.979	$x, 2x^2, 6x^2, 10x^2, 14x^2, 30x^2$ $42x^2, 70x^2, 210x^2$	96
	6	1.833	x	48
	7	1.667	$x, x^2, 21x^2$	12
	14	1.875	x	48
	15	1.958	$x, -15x^2, -7x^2, -3x^2, x^2$ $21x^2, 105x^2$	48
	21	1.833	x	24
	35	1.958	$x, -35x^2, -15x^2, -7x^2$ $-3x^2, x^2, 5x^2, 21x^2, 105x^2$	48
			$-4x^4, -196x^4$	96
	42	1.875	x	48
22	**1**	**1.300**	$\mathbf{x, x^3}$	**20**
	2	1.675	x^3	80
	3	1.300	$3x^2$	20
	5	1.950	x, x^3	80
	6	1.925	x	80
	7	1.700	$x, -x^2, x^3$	60
	11	1.800	$x, -x^2, 11x^2, x^3$	10
			x^3	20
			$484x^4$	20
	15	1.975	$x, -165x^2, -33x^2, -5x^2$ $-x^2, 3x^2, 11x^2, 15x^2, 55x^2$	80
	22	1.850	x, x^3	40
	33	1.950	$x, 2x^2, 6x^2, 66x^2$	40
23	1	1.136	x, x^3	44
	2	1.636	x, x^3	88
	3	**1.091**	$\mathbf{x, -3x^2, x^2}$	**44**
	23	1.727	x, x^2, x^3	22
	46	1.977	x, x^3	88
24	2	1.500	x	8
	3	**1.250**	$\mathbf{x}$	**8**
	10	1.875	x	32
	11	1.775	x	80
	13	1.979	x	96
	15	1.813	x	32
	33	1.925	x	80
	39	1.979	x	96
	42	1.958	x	48
25	1	1.350	x, x^3	40
	3	**1.300**	$\mathbf{x, -75x^2, -3x^2, x^2, 25x^2}$	**40**
	5	1.750	x, x^3	40
	15	1.750	x, x^2	40
26	1	1.250	x, x^3	24
	2	1.604	x^3	96
	3	**1.167**	$\mathbf{x, -x^2, 3x^2}$	**24**
	5	1.958	x, x^3	96
	6	1.917	x	96
	7	1.639	$x, -x^2, x^3$	72
	13	1.833	x, x^3	24
	15	1.958	$x, -x^2$	96
	26	1.875	x, x^3	48
	39	1.917	$x, -13x^2, -x^2, 3x^2, 39x^2$	24
27	1	1.611	x	36
	2	1.472	x	72
	3	**1.111**	$\mathbf{x, x^2}$	**18**
	6	1.806	x	72
	15	1.750	$x, x^2, 9x^2$	72
28	**1**	**1.333**	$\mathbf{x, x^3}$	**12**
	2	1.708	x^3	48
	3	1.417	x	24
	5	1.958	x, x^3	48
	6	1.875	x	48
	7	1.500	x, x^3	12
	10	1.938	x, x^3	96
	15	1.979	$30x^2, 42x^2, 210x^2$	96
	21	1.917	$6x^2, 14x^2, 42x^2$	24
	35	1.958	$2x^2, 10x^2, 14x^2, 70x^2$	48
	42	1.958	x	48
29	1	1.107	x, x^3	56
	3	**1.071**	$\mathbf{x, x^2}$	**56**
	29	1.964	x, x^3	56
30	1	1.875	$x, 2x^2, 6x^2, 10x^2, 30x^2$	16
	2	1.813	x	32
	3	**1.500**	$\mathbf{x, -x^2, 3x^2}$	**8**
	5	1.625	x	16
	6	1.938	x	32
	7	1.917	$x, -x^2$	48
	10	1.813	x	32
	11	1.950	$x, -x^2$	80
	15	1.750	$-5x^2, 3x^2, 15x^2$	8
	21	1.979	$14x^2, 42x^2$	96
	30	1.938	x	32
	35	1.958	$x, -x^2, 7x^2, 35x^2$	48
	39	1.938	$x, -x^2$	96
31	1	1.100	x, x^3	60
	3	**1.067**	$\mathbf{x, -3x^2, x^2}$	**60**
	31	1.667	x, x^2, x^3	30
32	2	1.438	x^3	32
	3	**1.063**	$\mathbf{x}$	**32**
	5	1.750	x, x^3	64
	6	1.750	x	32
	7	1.479	x, x^3	96
	10	1.969	x, x^3	64
	14	1.917	x, x^3	96
33	1	1.750	x	40
	2	1.575	x	80
	3	**1.200**	$\mathbf{x, -3x^2, x^2}$	**20**
	6	1.825	x	80
	11	1.600	x, x^2	20
	15	1.950	x, x^2	80
	22	1.975	x	80
	33	1.950	$x, 22x^2$	40
34	1	1.188	x, x^3	32
	2	1.625	x, x^3	64
	3	**1.125**	$\mathbf{3x^2}$	**32**
	7	1.563	$x, -x^2, x^3$	96
	17	1.938	x, x^3	32

k	D	ρ	$u(x)$	deg
	34	1.906	x, x^3	64
35	1	1.542	x, x^3	48
	2	1.917	x, x^3	96
	3	**1.500**	$\mathbf{x, -3x^2, x^2}$	**48**
	5	1.792	x, x^3	48
	7	1.750	x, x^2, x^3	24
	10	1.917	x, x^3	96
	14	1.979	x, x^3	96
	15	1.917	$x, -3x^2, x^2$	48
	21	1.938	x	96
	35	1.917	$x, -35x^2, -7x^2, x^2, 5x^2, x^3$	24
36	1	1.667	x	12
	2	**1.417**	$\mathbf{x}$	**24**
	3	1.833	$2x^2, 6x^2, 18x^2$	12
	5	1.917	x	48
	6	1.917	x	24
	7	1.972	x	72
	10	1.896	x	96
	15	1.958	x	48
37	1	1.083	x, x^3	72
	3	**1.056**	$\mathbf{x, -3x^2, x^2}$	**72**
	37	1.861	x, x^3	72
38	1	1.167	x, x^3	36
	2	1.667	x, x^3	72
	3	**1.111**	$\mathbf{x, -x^2, 3x^2}$	**36**
	19	1.833	x^3	36
	38	1.917	x, x^3	72
39	1	1.708	x	48
	2	1.521	x	96
	3	**1.167**	$\mathbf{x, -3x^2, x^2}$	**24**
	6	1.917	x	96
	13	1.917	x	48
	15	1.917	$x, -15x^2, -3x^2, x^2, 5x^2$	96
	26	1.938	x	96
	39	1.833	x, x^2	24
40	2	1.750	x^3	32
	3	**1.438**	$\mathbf{x}$	**32**
	5	1.750	x, x^3	16
	7	1.813	x, x^3	96
	10	1.875	x^3	32
	14	1.958	x, x^3	96
	15	1.750	x	32
	30	1.938	x	32
	35	1.938	x, x^3	96
41	1	1.075	x, x^3	80
	3	**1.050**	$\mathbf{x, x^2}$	**80**
	41	1.925	x, x^3	80
42	1	1.917	$x, 2x^2, 6x^2, 14x^2, 42x^2$	24
	2	1.625	x	48
	3	**1.333**	$\mathbf{x, -x^2, 3x^2}$	**12**
	5	1.938	x	96
	6	1.875	x	48
	7	1.667	$3x^2, 7x^2$	12
	14	1.958	x	48
	15	1.958	$-105x^2, -21x^2, 3x^2, 15x^2$ $35x^2$	48
	21	1.917	$x, 2x^2, 6x^2, 42x^2$	24
	35	1.958	$x, -105x^2, -21x^2, -5x^2$ $-x^2, 3x^2, 7x^2, 15x^2, 35x^2$	48
	42	1.958	x	48
43	1	1.071	x, x^3	84
	3	**1.048**	$\mathbf{x, -3x^2, x^2}$	**84**
	43	1.810	x, x^2, x^3	42
44	1	1.200	x, x^3	20
	2	1.525	x^3	80
	3	**1.150**	$\mathbf{x}$	**40**
	5	1.925	x, x^3	80
	6	1.950	x	80
	11	1.750	x^3	40
	22	1.900	x, x^3	40
	33	1.900	x	40
45	1	1.958	x	48
	2	1.729	x	96
	3	**1.333**	$\mathbf{x, -3x^2, x^2}$	**24**
	5	1.958	x	48
	6	1.938	x	96
	10	1.854	x	96
	15	1.750	$x, x^2, 9x^2$	24
	30	1.938	x	96
46	1	1.136	x, x^3	44
	2	1.659	x, x^3	88
	3	**1.136**	$\mathbf{3x^2}$	**44**
	23	1.727	$x, -x^2, x^3$	22
	46	1.909	x, x^3	88
47	1	1.065	x, x^3	92
	3	**1.043**	$\mathbf{x, -3x^2, x^2}$	**92**
	47	1.783	x, x^2, x^3	46
48	2	1.375	x	16
	3	**1.125**	$\mathbf{x}$	**16**
	6	1.750	x	16
	7	1.833	x	96
	10	1.844	x	64
	14	1.958	x	96
	15	1.781	x	64
	30	1.938	x	64
49	1	1.214	x, x^3	84
	3	**1.190**	$\mathbf{x, -147x^2, -3x^2, x^2, 49x^2}$	**84**
	7	1.381	x, x^2, x^3	42
50	1	1.350	x, x^3	40
	2	1.900	x, x^3	80
	3	**1.300**	$\mathbf{x, -25x^2, -x^2, 3x^2, 75x^2}$	**40**
	5	1.850	x, x^3	40
	10	1.875	x, x^3	80
	15	1.800	$x, -5x^2, -x^2, 15x^2$	40

Table 3 : The representation of $\sqrt{-D}$

D	*representation*
2	$x^3 + x$
3	$2x + 1$
5	$2x^7 - x^5 + 2x^3$
6	$2x^7 + x^5 - x^3 + x$
7	$2x^4 + 2x^2 + 2x + 1$
10	$x^{15} + 2x^9 + 2x^7 - x^5 - 2x^3 + 2x$
11	$2x^9 + 2x^5 + 2x^4 + 2x^3 + 2x + 1$
13	$2x^{21} - 2x^{19} - 2x^{15} + x^{13} - 2x^{11} - 2x^7 + 2x^5$
14	$2x^{23} + x^{21} - 2x^{17} + 2x^{15} + 2x^{13} - 2x^{11} + x^7 + 2x^5$
15	$2x^7 - 2x^5 + 4x^4 - 2x^3 + 2x^2 + 4x - 3$
17	$2x^{31} - 2x^{29} + 2x^{27} + 2x^{23} - x^{17} + 2x^{11} + 2x^7 - 2x^5 + 2x^3$
19	$2x^{17} + 2x^{16} + 2x^{11} + 2x^9 + 2x^7 + 2x^6 + 2x^5 + 2x^4 + 2x + 1$
21	$2x^{23} + x^{21} + 2x^{19} + 2x^{17} - 2x^{15} - 2x^{13} + 2x^{11} - 2x^3 + 2x$
22	$2x^{37} - x^{33} - 2x^{31} + 2x^{27} - 2x^{25} - 2x^{23} - 2x^{15} + x^{11} - 2x^9 + 2x^5 + 2x^3 - 2x$
23	$2x^{18} + 2x^{16} + 2x^{13} + 2x^{12} + 2x^9 + 2x^8 + 2x^6 + 2x^4 + 2x^3 + 2x^2 + 2x + 1$
26	$2x^{47} + 2x^{45} - 2x^{41} + x^{39} + 2x^{37} - 2x^{33} + 2x^{31} + 2x^{21} - 2x^{19} + 2x^{15} + x^{13} - 2x^{11} + 2x^7 + 2x^5$
29	$2x^{55} + 2x^{47} + 2x^{43} - 2x^{41} + 2x^{39} - 2x^{37} + 2x^{31} - x^{29} + 2x^{27} - 2x^{21} + 2x^{19} - 2x^{17} + 2x^{15} + 2x^{11} + 2x^3$
30	$2x^{31} + 4x^{29} + 2x^{27} + x^{25} + 2x^{23} - 2x^{21} - 2x^{19} - x^{15} - 2x^9 - 2x^7 + x^5 + 4x$
31	$2x^{28} + 2x^{25} + 2x^{20} + 2x^{19} + 2x^{18} + 2x^{16} + 2x^{14} + 2x^{10} + 2x^9 + 2x^8 + 2x^7 + 2x^5 + 2x^4 + 2x^2 + 2x + 1$
33	$4x^{37} - x^{33} - 4x^{31} + 2x^{27} + 4x^{25} + 2x^{23} - 2x^{15} + 2x^{11} + 2x^9 - 4x^5 - 2x^3 + 2x$
34	$2x^{63} - 2x^{53} - x^{51} + 2x^{49} + 2x^{39} + 2x^{33} + 2x^{31} - 2x^{27} + 2x^{25} + 2x^{23} - 2x^{21} + x^{17} - 2x^{13} - 2x^{11} + 2x^9 + 2x^7 - 2x^3 + 2x$
35	$4x^{22} - 2x^{21} + 2x^{20} - 4x^{16} + 4x^{15} - 2x^{14} - 4x^{11} + 2x^{10} - 4x^9 + 4x^8 + 2x^5 - 4x^4 + 1$
37	$2x^{69} + 2x^{61} - 2x^{59} + 2x^{57} - 2x^{55} - 2x^{51} + 2x^{45} - 2x^{43} - 2x^{39} + x^{37} - 2x^{35} - 2x^{31} + 2x^{29} - 2x^{23} - 2x^{19} + 2x^{17} - 2x^{15} + 2x^{13} + 2x^5$
38	$2x^{69} - 2x^{65} + 2x^{63} - x^{57} + 2x^{55} + 2x^{53} + 2x^{47} - 2x^{43} - 2x^{41} + 2x^{39} + 2x^{37} - 2x^{35} - 2x^{33} + 2x^{29} + 2x^{23} + 2x^{21} - x^{19} + 2x^{13} - 2x^{11} + 2x^7$
39	$2x^{23} + 4x^{20} - 4x^{19} + 2x^{17} + 2x^{14} - 2x^{13} - 2x^{12} + 4x^{11} + 2x^{10} - 2x^9 + 4x^8 - 4x^6 + 4x^5 + 2x^4 - 2x^3 + 4x^2 + 2x - 3$
41	$2x^{79} + 2x^{75} + 2x^{71} - 2x^{69} + 2x^{67} - 2x^{65} + 2x^{63} + 2x^{55} - 2x^{53} + 2x^{47} - x^{41} + 2x^{35} - 2x^{29} + 2x^{27} + 2x^{19} - 2x^{17} + 2x^{15} - 2x^{13} + 2x^{11} + 2x^7 + 2x^3$
42	$2x^{47} + 4x^{43} + 2x^{41} - 2x^{37} - 3x^{35} + 2x^{27} + 2x^{25} + 4x^{23} + x^{21} - 2x^{19} + 2x^{17} - 4x^{15} - 4x^{11} + x^7 - 2x^5 + 2x^3 + 2x$
43	$2x^{41} + 2x^{40} + 2x^{38} + 2x^{36} + 2x^{35} + 2x^{31} + 2x^{25} + 2x^{24} + 2x^{23} + 2x^{21} + 2x^{17} + 2x^{16} + 2x^{15} + 2x^{14} + 2x^{13} + 2x^{11} + 2x^{10} + 2x^9 + 2x^6 + 2x^4 + 2x + 1$
46	$2x^{87} - 2x^{85} + 2x^{81} - 2x^{77} - 2x^{75} + 2x^{73} + 2x^{71} - x^{69} - 2x^{59} + 2x^{55} + 2x^{49} + 2x^{47} + 2x^{41} + 2x^{39} - 2x^{35} + 2x^{31} - 2x^{29} - 2x^{27} + 2x^{25} + x^{23} - 2x^{13} + 2x^9 - 2x^3 + 2x$
47	$2x^{42} + 2x^{37} + 2x^{36} + 2x^{34} + 2x^{32} + 2x^{28} + 2x^{27} + 2x^{25} + 2x^{24} + 2x^{21} + 2x^{18} + 2x^{17} + 2x^{16} + 2x^{14} + 2x^{12} + 2x^9 + 2x^8 + 2x^7 + 2x^6 + 2x^4 + 2x^3 + 2x^2 + 2x + 1$

7 Conclusion

We have proposed a general construction of pairing friendly elliptic curves over an extension field of $K = \mathbb{Q}(\zeta_k, \sqrt{-D})$. We can find a suitable field containing $\mathbb{Q}(\zeta_k, \sqrt{-D})$ for our construction by the method in section 4. But we can not find a suitable field between $K = \mathbb{Q}(\zeta_k, \sqrt{-D})$ and $\mathbb{Q}(\zeta_k, \sqrt{-D})$. Most good ρ value appear when the discriminant 1 and 3. The advantage of elliptic curves with j-invariant 0 or 1728 is that computations of the pairing are reduced. But the security of these curves is also reduced. If a discriminant D is very large, it is difficult to compute the Hilbert class polynomial. Thus if anyone needs a pairing friendly elliptic curves with a discriminant not equal to 1 or 3 and sufficiently small, our method is useful.

APPENDIX

A CM method

Let K be an imaginary quadratic field $\mathbb{Q}(\sqrt{-D})$, $\mathcal{O}_K$ the maximal order of K, $H_{\mathcal{O}}$ the ring class field associated to an order $\mathcal{O}$ in K, $C(\mathcal{O}_K)$ the ideal class group of $\mathcal{O}_K$ and h_K the class number of K.

Theorem A.1 [15, Theorem 4] *Let p be a rational prime which splits completely in K and $\mathfrak{P}$ a prime of $H_{\mathcal{O}}$ above p with residue degree $f = f_{\mathfrak{P}|p}$ and such that $[\mathcal{O}_K : \mathcal{O}] \notin \mathfrak{P}$. Let $\mathcal{E}$ be an elliptic curve over $H_{\mathcal{O}}$ which has complex multiplication by $\mathcal{O}$ and good, ordinary reduction at $\mathfrak{P}$. Then there is an element $\pi \in \mathcal{O} \setminus p\mathcal{O}$ satisfying the system of norm equations*

$$\begin{aligned} q &= N_K(\pi) \\ \#E(\mathbb{F}_q) &= N_K(1-\pi) \end{aligned}$$

for the $\mathfrak{P}$-reduces curve E of $\mathcal{E}$, where $q = p^f$. The endomophism ring of $\mathcal{E}$ is stable under the reduction map $\mathcal{E} \xrightarrow{\mathfrak{P}} E$, i.e. $\mathrm{End}\mathcal{E} = \mathrm{End}E = \mathcal{O}$. *Moreover, every elliptic curve over $\mathbb{F}_q$ with endomophism ring $\mathcal{O}$ arises in this way.*

Proof. See [7, Theorem 14.16]. □

Theorem A.2 [15, Theorem 5] *The imaginary quadratic field K of Theorem A.1 is given by*

$$K = \mathbb{Q}(\sqrt{(q+1-m)^2 - 4q}).$$

Proof. See [7, Section 14] □

Since an elliptic curve $E/\mathbb{C}$ is isomorphic to E/Λ for some lattice $\Lambda \subset \mathbb{C}$, we consider $E/\mathbb{C}$ as E/Λ.

Proposition A.3 [23, Proposition 11.1] *There is a one to one correspondence between $C(\mathcal{O}_K)$ and isomophism classes of elliptic curves $E/\mathbb{C}$ with $\mathrm{End}(E) \cong C(\mathcal{O}_K)$.*

Proof. See [23, Proposition 11.1] and [7, Section 14] □

Theorem A.4 [23, Theorem 11.2]

(1) $j(\Lambda)$ is an algebraic integer.

(2) $[K(j(\Lambda)) : K] = [\mathbb{Q}(j(\Lambda)) : \mathbb{Q}]$.

(3) The field $H_K = K(j(\Lambda))$ is the maximal unramified abelian extension of K (I.e. H_K is the Hilbert class field of K.)

(4) Let $\{\Lambda_1\}, \ldots, \{\Lambda_{h_K}\}$ be a complete set of representatives for $C(\mathcal{O}_K)$. Then $j(\Lambda_1), \ldots, j(\Lambda_{h_K})$ form a complete set of $Gal(H_K/K)$ conjugates for $j(\Lambda)$.

Proof. See [7, Section 14]. □

By (A.4.(4)), the minimal polynomial of H_K is given by

$$H_D(x) = \prod (x - j(\Lambda)).$$

Theorem A.5 *Let $p > 3$ be a prime and j j-invariant of E over $\mathbb{F}_p$. Then E over $\mathbb{F}_p$ is given by*

$$\begin{array}{lllllll} E & : & y^2 = x^3 + 3\kappa x + 2\kappa & with & \kappa = \dfrac{j}{1728 - j} & if & j \neq 0, 1728 \\ E & : & y^2 = x^3 + ax & with & a \in \mathbb{F}_p{}^* & if & j = 1728 \\ E & : & y^2 = x^3 + b & with & b \in \mathbb{F}_p{}^* & if & j = 0. \end{array}$$

Proof. See [23, Proposition 5.4]. □

The reduction of E modulo a prime $\mathfrak{p}$ of H_K is again an elliptic curve. Its j-invariant is a root of $H_D(x)$ modulo p, where p is the integer prime in $\mathfrak{p}$. But by reduction, every isomorphism class of elliptic curves over H_K splits into several isomorphism classes of elliptic curves over $\mathbb{F}_p$. I.e. an isomorphism class of elliptic curves over $\mathbb{F}_p$ is not uniquely determiner by j-invariant. For fixed j-invariant, the number of their isomorphism classes is given by the number of unit in $\mathcal{O}_K$.

Theorem A.6 [15, Theorem 11] *Let E and E' be elliptic curves over $\mathbb{F}_p$. If E is ordinary, then E and E' are isomorphic if and only if $j(E) = j(E')$ and $\#E(\mathbb{F}_p) = \#E'(\mathbb{F}_p)$.*

Proof. See [7, Proposition 14.19]. □

Theorem A.7 *If $D > 4$, all elliptic curves with given j-invariant, $j \neq 0, 1728$, over $\mathbb{F}_p$ are given by*

$$y^2 = x^3 + 3\kappa c^2 x + 2\kappa c^3$$

where $\kappa = j/(1728 - j)$ and $c \in \mathbb{F}_p$

Proof. See [23, Proposition 5.4] and [7, Theorem 14.16]. □

Remark A.8 We must choose p such that p splits in K because $H_D(x)$ has a root modulo p. By Hensel's lemma, if $H_D(x)$ has a root modulo p, $H_D(x)$ has h_k number of roots. Thus we find h_k number of curves with the same orders.

References

[1] D. Boneh and M. Franklin, *Identity-based encryption from thr Weil pairing*, In Advances in Cryptology-Crypto 2001, Lecture Note in Computer Science, vol. 2139, Springer-Verlag, 2002, 213-229.

[2] P.S.L.M. Barreto, B. Lynn, and M. Scott, *Constructing elliptic curves with prescribed embedding degrees*, Security in Communication Networks - SCN'2002, Lecture Note in Computer Science, vol. 2576, Springer-Verlag, 2002, 263-273.

[3] P.S.L.M. Barreto and M. Naehrig, *Pairing-friendly elliptic curves of prime order*, Workshop on Selected Areas in Cryptography - In Proceedings of SAC 2005, Lecture Notes in Computer Science, vol. 3897, Springer-Verlag, 2006, 319-331.

[4] I.F. Balke, G. Seroussi, and N.P. Smart, *Elliptic Curves in Cryptography*, London Mathematical Society Lecture Note Series, **265**, 1999.

[5] F. Brezing and A. Weng. *Elliptic curves sutable for pairing based cryptography*, Designs, Codes and Cryptography, **37**(2005),133-141.

[6] H. Cohen. *A course in Computational Algebraic Number Theory*, Graduate Texts in Mathematics, vol. 138, Springer-Verlag, 2000.

[7] D.A. Cox, *Primes of the form $x^2 + ny^2$*, John Wiley & Sons, New York 1989.

[8] C. Cocks and R.G.E. Pinch, *Identity-based cryptosystems based on the Weil pairing*, unpublished manuscript, (2001).

[9] R. Dupont, A. Enge, and F. Morain. *Building Curves with Arbitrary Small MOV Degree over Finite Prime Fields*, J. Cryptology, **18(2)**(2005), 79-89.

[10] D. Freeman. *Constructing pairing-friendly elliptic curves with embedding degree 10*, In Algorithmic Number Theory Symposium - ANTS-VII, lecture Notes in Computer Science, vol. 4076, Springer-Verlag, 2006, 452-465.

[11] D. Freeman, M. Scott, E. Teske. *A taxonomy of pairing-friendly elliptic curves*, Cryptology ePrint Archive Report 2006/372. Available at:**http://eprint.iacr.org/2006/372/**.

[12] S. Galbraith, J. McKee, and P. Valença. *Ordinary abelian varieties having small embedding degree*, In Proc. Workshop on Mathematical Problems and Techniques in Cryptology, CRM, Barcelona, 2005, 29-45.

[13] The PARI Group, Bordeaux, *PARI-GP Version 2.3.1.*

[14] S. Lang. *Algebra*, Addison-Wesley, Reading, MA, 1993, 3rd ed.

[15] G.-J. Lay and H.G. Zimmer, *Constructing elliptic curves with given group order over large finite fields*, In Algorithmic Number Theory Symposium - ANTS-1, Lecture Notes in Computer Science, vol. 877, Springer-Verlag, 1994, 250-263.

[16] R. Lidl and H. Niederreiter, *Introduction to finite fields and their applicationa*, Cambridge University Press, 1997.

[17] A. Murphy and N. Fitzpatrick, *Elliptic curves for pairing applications*, Cryptology ePrint Archive Report 2005/302. Available at:**http://eprint.iacr.org/2005/302/**.

[18] A. Miyaji, M. Nakabayashi, and S. Takano, *New explicit conditions of elliptic curve traces for FR-reduction*, IEICE Transactions on Fundamentals, **E84-A(5)** (2001), 1234-1243.

[19] A. Menezes, T. Okamoto and S. Vanstone, *Reducing elliptic curve logarithms to logarithms in a finite field*, IEEE Transactions on Information Theory, **39** (1993), 1639-1646.

[20] A. Menezes and S. Vanstone, *Isomorphism classes of elliptic curves over finite fields of characteristic 2*, Utilitas Mathematica. **38** (1990), 135-153.

[21] M. Scott and P.S.L.M. Barreto, *Generating more MNT elliptic curves*, Designs, Codes and Cryptography, **38** (2006), 209-217.

[22] A. Shamir, *Identity based cryptosystems and signature schemes*, In Advances in Cryptology-Crypto 1984, Lecture Note in Computer Science, vol. 196, Springer-Verlag, 1984, 47-53.

[23] J.H. Silverman, *The Arithmetic of Elliptic Curves. Springer*, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, 1986.

[24] V. Miller, *The Weil pairing, and its efficient calculation*, J. Cryptology, **17** (2004), 235-261.

[25] L.C. Washington, *Introduction to Cyclotomic Fields*, Springer-Verlag, 1997.