Barreto-Naehrig Curve With Fixed Coefficient

– Efficiently Constructing Pairing-Friendly Curves –

Masaaki Shirase

School of Systems Information, Future University Hakodate,
116-2 Kamedanakano, Hakodate, Hokkaido 041-8655, Japan
shirase@fun.ac.jp

Abstract. This paper describes a method for constructing Barreto-Naehrig (BN) curves and twists of BN curves that are pairing-friendly and have the embedding degree 12 by using just primality tests without a complex multiplication (CM) method. Specifically, this paper explains that the number of points of elliptic curves $y^2 = x^3 \pm 16$ and $y^2 = x^3 \pm 2$ over $\mathbb{F}_{p(z)}$ is given by 6 polynomials in z, $n_0(z), \cdots, n_5(z)$, two of which are irreducible, classified by the value of $z \bmod 12$ for a prime $p(z) = 36z^4 + 36z^3 + 24z^2 + 6z + 1$ with z an integer. For example, elliptic curve $y^2 = x^3 + 2$ over $\mathbb{F}_{p(z)}$ always becomes a BN curve for any z with $z \equiv 2, 11 \pmod{12}$. Let $n_i(z)$ be irreducible. Then, to construct a pairing-friendly elliptic curve, it is enough to find an integer z of appropriate size such that $p(z)$ and $n_i(z)$ are primes.

Key words: Pairing-friendly elliptic curve, Barreto-Naehrig curve, twist, Gauss' theorem, Euler's conjecture.

1 Introduction

Pairings that are bilinear mappings have achieved many cryptographic protocols (pairing-based cryptosystems) such as ID based key agreement [26], ID based encryption [6], ID based signature [16], ring signature [31], certificateless public key encryption [1], keyword search encryption [5], efficient broadcast encryption [8], and aggregate signature [7]. Pairings are generally defined on (hyper-)elliptic curves, and elliptic curves suitable for pairing are called pairing-friendly elliptic curves. Thus, constructing pairing-friendly curves is one of the most important issues in cryptography. Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$, and let r be a prime factor of $\#E(\mathbb{F}_q)$. Then, the conditions in which E is pairing-friendly are when 1) r is a large enough prime, 2) the smallest positive integer k satisfying $r \,|\, (q^k - 1)$ satisfies $4 \leq k \leq 24$, and 3) $\rho = \log q / \log r$ is closed to 1.

For pairing-friendly supersingular elliptic curves, the k automatically becomes $4, 6, 2$ if characteristics of $\mathbb{F}_q$ are $2, 3, p \geq 5$, respectively [23]. Thus, the k of supersingular curves of characteristics 2 and 3 are suitable for pairings. However, one has to construct an ordinal (non-supersingular) elliptic curve if one needs an elliptic curve that has the embedding degree > 6.

Pairing-friendly ordinal elliptic curves over prime field $\mathbb{F}_p$ were first constructed by Miyaji, Nakabayashi, and Tanaka [24], and elliptic curves constructed by this method are called MNT curves. Since then, some other methods for constructing pairing-friendly ordinal elliptic curves have been developed by some researchers, for example, Cocks and Pinch [10], Barreto et al. [3], Brezing and Weng [9], Dupont et al. [12], Galbraith et al. [15], Barreto and Naehrig (BN) [4], Freeman [13], and Tanaka and Nakamula [29, 30]. When one constructs a pairing-friendly elliptic curve using these methods, one also uses the complex multiplication (CM) method, which usually costs a lot. However, in several exceptional cases, including the BN method [4], the CM method just takes several scalar multiplications on $E(\mathbb{F}_p)$ to check its order.

The purpose of this paper is to omit even any scalar multiplication to construct a BN curve. Specifically, this paper gives BN curves and twists of them of fixed coefficients. There is an early study by Devegili et al. [11], in which a condition of p that the curve $y^2 = x^3+3$ over $\mathbb{F}_p$ becomes a BN curve is discussed without proof. This paper shows that the order of elliptic curves $y^2 = x^3 \pm 2$ and $y^2 = x^3 \pm 16$ over $\mathbb{F}_{p(z)}$, which are BN curves or twists of BN curves, is given by 6 polynomials in z classified by z mod 12, where $p(z)$ is a prime represented as $p(z) = 36z^4 + 36z^3 + 24z^2 + 6z + 1$ with an integer z. For example, the order of $\#E(\mathbb{F}_{p(z)})$ with $E : y^2 = x^3 + 2$ is given by $n(z) = 36z^4 + 36z^3 + 18z^2 + 6z + 1$ for any prime $p(z)$ with $z \equiv 2, 11 \pmod{12}$, that is, such E is a BN curve. Therefore, to construct a BN curve, it is enough to find an integer z with $z \equiv 2, 11 \pmod{12}$ of appropriate size such that $p(z)$ and $n(z)$ are primes without using the CM method. Moreover, this curve has an obvious point $(-1, 1)$, so one does not need to find a point for a base point for pairing-cryptosystems.

2 Elliptic Curve and Pairing

This section outlines properties of elliptic curve, twist, pairing, and pairing-friendly conditions.

2.1 Elliptic Curve

Let $p \geq 5$ be a prime, and q a power of p. For an elliptic curve over the finite field $\mathbb{F}_q$

$$E : y^2 = x^3 + ax + b, \quad a^3 + 27b^2 \neq 0, \tag{1}$$

the set of $\mathbb{F}_q$-rational points of E, $E(\mathbb{F}_q)$, is defined as

$$E(\mathbb{F}_q) = \{(x, y) \in \mathbb{F}_q \times \mathbb{F}_q : y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\},$$

where $\mathcal{O} = [0, 1, 0]$ in the projective coordinate is the point at infinity[1]. $E(\mathbb{F}_q)$ is known to form an additive group with $\mathcal{O}$ as zero. An integer t defined as

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

[1] This paper has to use the projective coordinate to show the proposed theorem in Sec. 5. For two projective points $[X_0, Y_0, Z_0]$ and $[X_1, Y_1, Z_1]$, $[X_0, Y_0, Z_0]$ is equal to $[X_1, Y_1, Z_1]$ if $X_1 = rX_0, Y_1 = rY_0, Z_1 = rZ_0$ $(r \neq 0)$ are satisfied.

is called the trace of $E(\mathbb{F}_q)$. Let r be the largest prime factor of $\#E(\mathbb{F}_q)$. Then, the smallest integer $k > 1$ satisfying $r \mid (q^k - 1)$ is called the embedding degree of E. The discriminant of E is defined as $\Delta(E) = -16(a^3 + 27b^2)$, and the j-invariant of E is defined as $j(E) = -12^3 a^3/\Delta(E)$. Given any $j_0 \in \mathbb{F}_q^*$ one can construct an elliptic curve with j-invariant j_0 [27, III.1.4]. For finite fields $\mathbb{F}_q$ of characteristic ≥ 5, it follows that

$$j(E) = 0 \Leftrightarrow E : y^2 = x^3 + b,\ b \in \mathbb{F}_q^* \tag{2}$$

by the definition of the j-invariant.

2.2 Twist

For two elliptic curves E and E' over $\mathbb{F}_q$, E' is called a twist of E over $\mathbb{F}_q$ of degree d if there exists an isomorphism $\psi_d : E' \to E$ over $\mathbb{F}_{q^d}$ and d is minimal[2]. If there is the mapping ψ_d, d is equal to 1, 2, 3, 4, or 5 [19, X.5.4]. It is known that

$$\begin{aligned} &E' \text{ is a twist of } E \text{ of any degree}\\ &\quad \Leftrightarrow j(E') = j(E)\\ &\quad \Leftrightarrow \text{the embedding degree of } E = \text{that of } E'. \end{aligned} \tag{3}$$

If E' is a twist of degree 1, then $\#E(\mathbb{F}_q) = \#E'(\mathbb{F}_q)$. However, if E' is a twist of E of degree $d > 1$, then $\#E(\mathbb{F}_q) \neq \#E'(\mathbb{F}_q)$. $\#E'(\mathbb{F}_q)$ is represented as Table 1 [17], where t is the trace of E.

Table 1. The order of $\#E'(\mathbb{F}_q)$ of twists of E

degree	$\#E'(\mathbb{F}_q)$	equations f satisfies
$d = 2$	$q + 1 + t$	
$d = 3$	$q + 1 - (3f - t)/2$	$t^2 - 4q = -3f^2$
	$q + 1 - (-3f - t)/2$	$t^2 - 4q = -3f^2$
$d = 4$	$q + 1 + f$	$t^2 - 4q = -f^2$
	$q + 1 - f$	$t^2 - 4q = -f^2$
$d = 6$	$q + 1 - (-3f + t)/2$	$t^2 - 4q = -3f^2$
	$q + 1 - (3f + t)/2$	$t^2 - 4q = -3f^2$

In this paper, let E_b be denoted by the elliptic curve

$$E_b : y^2 = x^3 + b$$

for any b.

[2] E' is often not called the twist of E if $d = 1$. However, in this paper E' with $d = 1$ is also called the twist.

Remark 1.
Elliptic curve $E_{b'}$ is a twist of another elliptic curve E_b for any non-zero b and b' due to Eqs. (2) and (3). □

Remark 2.
Let q be a prime power with $q \equiv 1 \pmod 6$. Consider two elliptic curves $E : y^2 = x^3 + b$ and $E' : y^2 = x^3 + b/\delta$ over $\mathbb{F}_q$. Thus, there is a mapping $\psi : E' \to E, (x, y) \mapsto (\sqrt[3]{\delta}, \sqrt{\delta}y)$.

If δ is square and cube in $\mathbb{F}_q$, then $\sqrt[3]{\delta}, \sqrt{\delta} \in \mathbb{F}_q$, and thus ψ is an isomorphism over $\mathbb{F}_q$. Therefore, E' is a twist of E of degree 1 and one sees $\#E'(\mathbb{F}_q) = \#E(\mathbb{F}_q)$.

If δ is non-square and cube in $\mathbb{F}_q$, then $\sqrt[3]{\delta} \in \mathbb{F}_q, \sqrt{\delta} \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$, and thus ψ is an isomorphism over $\mathbb{F}_{q^2}$. Therefore, E' is a twist of E of degree 2, and one sees $\#E'(\mathbb{F}_q) = q + 1 + t = 2q + 2 - \#E(\mathbb{F}_q)$ due to Table 1. □

2.3 Pairing

Let r a prime, let G_1 and G_2 be additive groups of order r, and let G_3 be a multiplicative group of degree r. Then, a mapping $e : G_1 \times G_2 \to G_3$ is called pairing if it has bilinearity ($e(aP, bQ) = e(P, Q)^{ab}$ is held for any $P \in G_1, Q \in G_2$ and any integers a and b) and non-degeneracy (there are P and Q such that $e(P, Q) \neq 1$).

The Ate pairing [17] this paper targets is a pairing defined on ordinal elliptic curves that is suitable for fast implementation. Moreover, improved variants of Ate pairing have been developed, such as optimized Ate pairing [22], R-ate pairing [19], and Xate pairing [25].

When an ordinal elliptic curve E over $\mathbb{F}_p$ defining Ate pairing has the embedding degree 12, and E has a twist E' of degree 6 with the mapping $\psi_6 : E' \to E$ over $\mathbb{F}_{p^2}$ (not over $\mathbb{F}_p$) (An instance of such a curve E is a BN curve [4] described in Sec. 3.3), Ate pairing

$$E(\mathbb{F}_p)[r] \times E'(\mathbb{F}_{p^2})[r] \to \mathbb{F}_{p^{12}}^*$$

is defined as $e(P, Q) = f_{t,Q'}(P)^{(q^k-1)/r} \in \mathbb{F}_{p^{12}}^*$, where $Q' = \psi(Q)$ and $f_{t,Q'}$ is a function the devisor of which satisfies $(f_{t,Q'}) = t(Q') - (tQ') - (t-1)(\mathcal{O})$.

2.4 Pairing-Friendly Elliptic Curve

Elliptic curves suitable for constructing pairing are called pairing-friendly elliptic curves. Let E be an elliptic curve over $\mathbb{F}_q$, and let r be the largest prime factor of $\#E(\mathbb{F}_q)$. Then, the conditions in which E is pairing-friendly are as follows [14].

Condition 1 (Pairing-friendly conditions).
(c1) *The prime r is large enough. ($\#E(\mathbb{F}_q) = r$ is best.)*
(c2) *The embedding degree k is proper. (That k satisfies $4 \leq k \leq 24$ is best.)*
(c3) *A value $\rho = \log q / \log r$ is closed to* 1. *($\rho = 1$ is best.)*

3 Current Methods for Constructing Elliptic Curves

This section briefly outlines the CM method that constructs an elliptic curve that has a desirable order and current methods for constructing pairing-friendly elliptic curves.

3.1 Complex Multiplication (CM) Method [2]

The CM method is an algorithm for constructing an elliptic curve E over $\mathbb{F}_p$ that has a desirable order n from the prime p, the trace $t = p + 1 - n$, and a square-free integer D satisfying

$$DV^2 = p^2 - 4t. \tag{4}$$

The CM method consists of three steps: (a) computing the j-invariant, (b) deciding coefficients, and (c) checking the order.

Computing the j-invariant step computes j_0 from input (p, t, D) such that j_0 becomes the j-invariant of an elliptic curve that has an order over $\mathbb{F}_p$ equal to n. When deciding coefficients, coefficients of an elliptic curve that has the j-invariant equal to j_0 are generated due to a method of [27, III.1.4], say E. As described in Sec. 2.2, although E is always a twist of the elliptic curve the order of which is n, the order of E is not always equal to that of the curve. Thus, one needs to check the order. When doing this, a point $(\mathcal{O} \neq)G \in E(\mathbb{F}_p)$ is picked up, and nG is computed. If nG is equal to $\mathcal{O}$, that means E has the order n, then the CM method returns E. If not, E has a different order from n and one has to return to step (b).

Step (a) is the main part of CM method and costs much more than parts (b) and (c). The CM method returns j-invariant 0 when $D = 3$. Therefore, if only the case of $D = 3$ is dealt with as a BN curve [4], then the main part (a) of the CM method is skipped[3].

3.2 Current Methods for Constructing Pairing-Friendly Elliptic Curves

Miyaji, Nakabayashi, and Tanaka first researched constructing pairing-friendly ordinal elliptic curves and they dealt with the case of the embedding degree $k = 3, 4, 6$ [24]. Curves constructed by their method are called MNT curves. Since then, methods for constructing pairing-friendly ordinal elliptic curves have been developed by some researchers, for example, Cocks and Pinch [10], Barreto et al. [3], Brezing and Weng [9], Dupont et al. [12], Galbraith et al. [15], Barreto and Naehrig, Freeman [13], and Tanaka and Nakamula [29, 30].

These methods usually discussed how to find a prime p, a trace t, and a square-free integer D satisfying Eq. (4) and Condition 1 in Sec. 2.4. After one finds such p, t, and d, then one usually uses the CM method to construct a

[3] Also, computing j-invariant step can be omitted in the case of $D = 1$.

pairing-friendly elliptic curve (refer to Sec. 3.1). In several cases, such as Barreto and Naehrig's work [4], one does not need the main step (a) of the CM method described in Sec. 3.1.

3.3 Barreto-Naehrig (BN) Curve [4]

Barreto and Naehrig developed a method for constructing pairing-friendly elliptic curves with $k = 12$ and $\rho \approx 1$. Such curves are most suitable for 128-bit security, which is expected to become standard security in the near future [21], corresponding to 3,072-bit RSA and 256-bit elliptic curve cryptography.

Let $t(Z)$, $n(Z)$, and $p(Z)$ be the following polynomials in Z,

$$\left.\begin{aligned} t(Z) &= 6Z^2 + 1, \\ n(Z) &= 36Z^4 + 36Z^3 + 24Z^2 + 6Z + 1, \\ p(Z) &= n(Z) + t(Z) - 1 \\ &= 36Z^4 + 36Z^3 + 18Z^2 + 6Z + 1. \end{aligned}\right\} \tag{5}$$

Then, $p(Z)$ and $t(Z)$ satisfy

$$4p(Z) - t(Z)^2 = 3 \cdot (5Z^2 + 4Z + 1)^2. \tag{6}$$

Therefore, one selects an integer z so that both $p(z)$ and $n(z)$ become primes, and one has $D = 3$ at Eq. (4). Then, the CM method returns the j-invariant 0 from inputs $p(z)$, $t(z)$, and $D = 3$ described in Sec. 3.1, and thus one does not need the main step (a) of the CM method. Therefore, the BN method is one of the most efficient methods for constructing pairing-friendly elliptic curves. To construct a pairing-friendly elliptic curve with the embedding degree 12 using BN method, first find an integer z of appropriate size so that $p(z)$ and $n(z)$ are primes using primality tests. Next, choose $b(\neq 0)$ at random. Then, for the elliptic curve $E_b : y^2 = x^3 + b$ over $\mathbb{F}_{p(z)}$, the order $\#E(\mathbb{F}_q)$ is equal to $n(z)$ with a probability of 1/6. Then, one carries out steps (b) and (c) of the CM method to check the order described at Sec. 3.1.

On the other hand, in a study by Devegili et al. [11], b is fixed to 3 and a condition of p that E_b over $\mathbb{F}_p$ becomes a BN curve. Then, one can omit any scalar multiplication to construct a BN curve.

In this paper, primes $p(z)$ represented as Eq. (5) that have an integer z are called *BN primes*. The purpose of this paper is similar to the study by Devegili et al. [11], however, this paper discusses a condition of not primes $p(z)$ but integers z that $E_{\pm 2}$ or $E_{\pm 16}$ become BN curves or twists of them and gives a strict proof.

4 Mathematic Preliminary

This section introduces a theorem that explains the number of points of a curve $u^3 + v^3 + 1 = 0$ and theorems about quadratic and cubic residue, to which Sec. 5 refers.

Theorem 1 (Gauss' Theorem).
Let p be a prime with $p \equiv 1 \pmod 3$, and let M_p be the number of projective points of the curve over $\mathbb{F}_p$,

$$C : u^3 + v^3 + 1 = 0.$$

Then, there are integers A and B so that

$$4p = A^2 + 27B^2. \tag{7}$$

A and B are unique up to changing their signs, and if we fix the sign of A so that $A \equiv 1 \pmod 3$, then

$$M_p = p + 1 + A.$$

Proof) Refer to Silverman and Tate [28]. □

Next, a famous theorem about quadratic residue is explained.

Theorem 2.
Let p be an odd prime, and let $(\frac{\cdot}{\cdot})$ be the Legendre symbol.
(a) Quadratic residue of -1:

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \textit{if } p \equiv 1 \pmod 4, \\ -1 & \textit{if } p \equiv 3 \pmod 4. \end{cases}$$

(b) Quadratic residue of 2:

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \textit{if } p \equiv \pm 1 \pmod 8, \\ -1 & \textit{if } p \equiv \pm 3 \pmod 8. \end{cases}$$

(c) Multiplicative property:

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

(d) Quadratic reciprocity:
Let p' be a prime deferent from p. Then,

$$\left(\frac{p'}{p}\right) = \begin{cases} -\left(\dfrac{p}{p'}\right) & \textit{if } p \equiv p' \equiv 3 \pmod 4, \\ \left(\dfrac{p}{p'}\right) & \textit{Otherwise.} \end{cases}$$

Proof) Refer to Koblitz [18]. □

Last, the remainder of this section explains cubic residue and introduces Euler's conjecture[4] on cubic residue.

[4] Although Euler's conjecture is traditionally called "conjecture", it has already been proven.

Let p be a prime with $p \equiv 1 \pmod 3$. Then, a primitive cubic root $w \in \mathbb{F}_p^*$ exists. Let g be a generator of $\mathbb{F}_p^*$. Then, any element $f \in \mathbb{F}_p^*$ can be represented as $f = g^l$ for an integer $0 \leq l \leq p-2$. Let a symbol $\left(\text{-}\right)_3$ be defined as

$$\left(\frac{f}{p}\right)_3 = w^l.$$

The element f is called cubic residue module p if $\left(\frac{e}{p}\right)_3 = 1$, and f is called cubic non-residue modulo p if it not cubic residue modulo p.

Theorem 3 (Euler's Conjecture).
(a) Any prime p with $p \equiv 1 \pmod 3$ can be represented as $p = a^3 + 3b^2$ for some integers a and b. Let $m = a + b$ and $n = a - b$. Then, $4p$ is written as $4p = (m+n)^2 + 3(m-n) = (2m-n)^2 + 3n^2 = (2n-m)^2 + 3m^2$, and exactly one of m, n and $m - n$ is a multiple of 3.
(b) For $p = a^2 + 3b^2$ the following is held.

$$\left(\frac{2}{p}\right)_3 = 1 \Leftrightarrow 3 \,|\, b. \tag{8}$$

$$\left(\frac{3}{p}\right)_3 = 1 \Leftrightarrow 9 \,|\, b, \;\; or\; 9 \,|\, (a+b), \;\; or\; 9 \,|\, (a-b). \tag{9}$$

$$\left(\frac{6}{p}\right)_3 = 1 \Leftrightarrow 9 \,|\, b, \;\; or\; 9 \,|\, (a+2b), \;\; or\; 9 \,|\, (a-2b). \tag{10}$$

Proof) Refer to Lemmermeyer [20]. □

Remark 3.
Theorem 1 ensures that the representation $4p = A^2 + 27B^2$ exists for any prime p with $p \equiv 1 \pmod 3$. However, it does not explain how to find such A and B. Theorem 3 ensures that the representation $p = a^2 + 3b^2$ exists for any prime p with $p \equiv 1 \pmod 3$. However, it does not explain how to find such a and b. □

5 Proposed Method

This section explains a method for constructing BN curves and twists of BN curves suitable for pairing-bases cryptosystems using just primality tests without the CM method. To accomplish this, Theorem 4, which describes the number of points of elliptic curves $E_{\pm 2} : y^2 = x^3 \pm 2$ and $E_{\pm 16} : y^2 = x^3 \pm 16$ over $\mathbb{F}_{p(z)}$ for any BN prime $p(z)$, has to be proven.

5.1 Quadratic and Cubic Residue Module BN Prime

To consider the number of points on BN curves and twists of BN curves one needs quadratic and cubic residue judgments modulo BN primes. Note that BN primes $p(z) = 36z^4 + 36z^3 + 24z + 6z + 1$ can be represented as

$$p(z) = (6z^2 + 3z + 1)^2 + 3z^2. \tag{11}$$

This representation is very important. One can set $a = 6z^2 + 3z + 1, b = z$ at Theorem 3-(b), and this fact derives the following lemma required to prove Theorem 4.

Lemma 1 (Quadratic and cubic residue modulo BN primes).
For BN primes $p(z) = 36z^4 + 36z^3 + 24z + 6z + 1$ the following is held.
(a) Quadratic residue of -1:

$$\left(\frac{-1}{p(z)}\right) = \begin{cases} 1 & \textit{if } z \textit{ is even}, \\ -1 & \textit{if } z \textit{ is odd}. \end{cases}$$

(b) Quadratic residue of 2:

$$\left(\frac{2}{p(z)}\right) = \begin{cases} 1 & \textit{if } z \equiv 0, 1 \pmod 4, \\ -1 & \textit{if } z \equiv 2, 3 \pmod 4. \end{cases}$$

(c) Quadratic residue of 3:

$$\left(\frac{3}{p(z)}\right) = \begin{cases} 1 & \textit{if } z \textit{ is even}, \\ -1 & \textit{if } z \textit{ is odd}. \end{cases}$$

(d) Quadratic residue of -3:

$$\left(\frac{-3}{p(z)}\right) = 1 \textit{ for all BN primes } p(z).$$

(e) Cubic residue of -1:

$$\left(\frac{-1}{p(z)}\right)_3 = 1 \textit{ for all BN primes } p(z).$$

(f) Cubic residue of 2:

$$\left(\frac{2}{p(z)}\right)_3 \begin{cases} = 1 & \textit{if } z \equiv 0 \pmod 3, \\ \neq 1 & \textit{if } z \equiv 1, 2 \pmod 3. \end{cases}$$

(g) Cubic residue of 3:

$$\left(\frac{3}{p(z)}\right)_3 \begin{cases} = 1 & \textit{if } z \equiv 0, 1, 5 \pmod 9, \\ \neq 1 & \textit{if } z \equiv 2, 3, 4, 6, 7, 8 \pmod 9. \end{cases}$$

(h) Cubic residue of 6:

$$\left(\frac{6}{p(z)}\right)_3 \begin{cases} = 1 & \textit{if } z \equiv 0, 2, 4 \pmod 9, \\ \neq 1 & \textit{if } z \equiv 1, 3, 5, 6, 7, 8 \pmod 9. \end{cases}$$

(Proof) (a) If z is even, $p(z)$ satisfies $p(z) \equiv 1 \pmod 4$. Then, one has $\left(\frac{-1}{p(z)}\right) = 1$ due to Theorem 2-(a). If z is odd, $p(z)$ satisfies $p(z) \equiv 3 \pmod 4$. Then, one has $\left(\frac{-1}{p(z)}\right) = -1$.

(b) Due to Theorem 2-(b), if $z \equiv 0, 1, 2, 3 \pmod 4$, one has $\left(\frac{2}{p(z)}\right) = 1, 1, -1, -1$ since $p(z) \equiv 1, 7, 5, 3 \pmod 8$, respectively.

(c) If z is even, $p(z) \equiv 1 \pmod 4$ and $p(z) \equiv 1 \pmod 3$ are satisfied. Then, one has

$$\begin{aligned}\left(\frac{3}{p(z)}\right) &= \left(\frac{p(z)}{3}\right) \text{ due to Theorem 2-(d)}\\ &= \left(\frac{1}{3}\right)\\ &= 1.\end{aligned}$$

If z is odd, $p(z) \equiv 3 \pmod 4$ and $p(z) \equiv 1 \pmod 3$ are satisfied. Then, one has

$$\begin{aligned}\left(\frac{3}{p(z)}\right) &= -\left(\frac{p(z)}{3}\right) \quad \text{due to Theorem 2-(d)}\\ &= -\left(\frac{1}{3}\right)\\ &= -1.\end{aligned}$$

(d) It is easy to see that (d) is satisfied due to (a), (c) and Theorem 2-(c).

(e) Since $-1 = (-1)^3$, -1 is cubic residue modulo any prime.

(f) Since any BN prime can be represented as $p(z) = (6z^2 + 3z + 1)^2 + 3z^2$, one can set $a = 6z^2 + 3z + 1, b = z$ at Theorem 3-(b). Then, one sees the following is held due to Eq. (8) of Theorem 3-(b).

$$\begin{aligned}\left(\frac{2}{p(z)}\right)_3 = 1 &\Leftrightarrow 3 \mid z \qquad \text{due to Eq. (8)}\\ &\Leftrightarrow z \equiv 0 \pmod 3.\end{aligned}$$

(g) When $a = 6z^2 + 3z + 1, b = z$ are set, one has $a + b = 6z^2 + 4z + 1,\ a - b = -6z^2 - 2z - 1$. Due to Eq. (9) it is seen that

$$\begin{aligned}\left(\frac{3}{p(z)}\right)_3 = 1 &\Leftrightarrow \begin{cases} 9 \mid z, \text{ or}\\ 9 \mid (6z^2 + 4z + 1), \text{ or}\\ 9 \mid (-6z^2 - 2z - 1), \end{cases}\\ &\Leftrightarrow \begin{cases} z \equiv 0 \pmod 9, \text{ or}\\ z \equiv 5 \pmod 9, \text{ or}\\ z \equiv 1 \pmod 9. \end{cases}\end{aligned}$$

(h) When $a = 6z^2 + 3z + 1, b = z$ are set, one has $2a + b = 6z^2 + 5z + 1,\ 2a - b = -6z^2 - z - 1$. Due to Eq. (10) it is seen that

$$\left(\frac{6}{p(z)}\right)_3 = 1 \Leftrightarrow \begin{cases} 9 \mid z, \text{ or} \\ 9 \mid (6z^2 + 5z + 1), \text{ or} \\ 9 \mid (-6z^3 - z - 1), \end{cases}$$
$$\Leftrightarrow \begin{cases} z \equiv 0 \pmod 9, \text{ or} \\ z \equiv 4 \pmod 9, \text{ or} \\ z \equiv 2 \pmod 9. \end{cases}$$

□

Remark 4.
Due to Lemma 1, one sees that quadratic and cubic residue of some integers modulo BN primes $p(z)$ are characterized by z rather than $p(z)$. □

5.2 Order of $E_{\pm 16}$ and $E_{\pm 2}$

This section proves the following theorem describing orders $\#E_{\pm 16}(\mathbb{F}_{p(z)})$ and $\#E_{\pm 2}(\mathbb{F}_{p(z)})$ over $\mathbb{F}_{p(z)}$, where $p(z) = 36z^4 + 36z^3 + 24z^2 + 6z + 1$ is each BN prime.

Theorem 4. (**Proposed Theorem**)
Let $p(z) = 36z^4 + 36z^3 + 24z^2 + 6z + 1$ be a BN prime, and let polynomials $n_0(z)$, $n_1(z)$, $n_2(z)$, $n_3(z)$, $n_4(z)$, and $n_5(z)$ be defined as follows.

$$\begin{aligned} n_0(z) &= 12z^2(3z^2 + 3z + 1) \\ n_1(z) &= 36z^4 + 36z^3 + 18z^2 + 1 \\ n_2(z) &= 3(12z^4 + 12z^3 + 10z^2 + 2z + 1) \\ n_3(z) &= 4(9z^4 + 9z^3 + 9z^2 + 3z + 1) \\ n_4(z) &= 3(12z^4 + 12z^3 + 10z^2 + 4z + 1) \\ n_5(z) &= 36z^4 + 36z^3 + 18z^2 + 6z + 1 \end{aligned}$$

Then, elliptic curves $E_{\pm 16} : y^2 = x^3 \pm 16$ and $E_{\pm 2} : y^2 = x^3 \pm 2$ over $\mathbb{F}_{p(z)}$ have the embedding degree 12, and the following is held.
(a) $\#E_{16}(\mathbb{F}_{p(z)})$:

$$\#E_{16}(\mathbb{F}_{p(z)}) = \begin{cases} n_0(z) & \textit{if } z \equiv 0 \pmod 3, \\ n_4(z) & \textit{if } z \equiv 1 \pmod 3, \\ n_2(z) & \textit{if } z \equiv 2 \pmod 3. \end{cases}$$

(b) $\#E_{-16}(\mathbb{F}_{p(z)})$:

$$\#E_{-16}(\mathbb{F}_{p(z)}) = \begin{cases} n_0(z) & \textit{if } z \equiv 0 \pmod 6, \\ n_1(z) & \textit{if } z \equiv 1 \pmod 6, \\ n_2(z) & \textit{if } z \equiv 2 \pmod 6, \\ n_3(z) & \textit{if } z \equiv 3 \pmod 6, \\ n_4(z) & \textit{if } z \equiv 4 \pmod 6, \\ n_5(z) & \textit{if } z \equiv 5 \pmod 6. \end{cases}$$

(c) $\#E_2(\mathbb{F}_{p(z)})$*:*

$$\#E_2(\mathbb{F}_{p(z)}) = \begin{cases} n_0(z) & \textit{if } z \equiv 0, 9 \pmod{12}, \\ n_1(z) & \textit{if } z \equiv 7, 10 \pmod{12}, \\ n_2(z) & \textit{if } z \equiv 5, 8 \pmod{12}, \\ n_3(z) & \textit{if } z \equiv 3, 6 \pmod{12}, \\ n_4(z) & \textit{if } z \equiv 1, 4 \pmod{12}, \\ n_5(z) & \textit{if } z \equiv 2, 11 \pmod{12}. \end{cases}$$

(d) $\#E_{-2}(\mathbb{F}_{p(z)})$*:*

$$\#E_{-2}(\mathbb{F}_{p(z)}) = \begin{cases} n_0(z) & \textit{if } z \equiv 0, 3 \pmod{12}, \\ n_1(z) & \textit{if } z \equiv 1, 10 \pmod{12}, \\ n_2(z) & \textit{if } z \equiv 8, 11 \pmod{12}, \\ n_3(z) & \textit{if } z \equiv 6, 9 \pmod{12}, \\ n_4(z) & \textit{if } z \equiv 4, 7 \pmod{12}, \\ n_5(z) & \textit{if } z \equiv 2, 5 \pmod{12}. \end{cases}$$

Proof) The proof is done at Sec. 5.3. □

Remark 5 (Relationship between Theorem 4 and BN curve).
Curves in Theorem 4 that have order $n_5(z)$ are BN curves because $n_5(z)$ is equal to $n(z)$ at Eq. (5). Other curves in Theorem 4 are twists of BN curves. □

Remark 6 (Pairing-friendliness).
Since $n_1(z)$ and $n_5(z)$ are irreducible, $n_1(z)$ and $n_5(z)$ may become primes for appropriate z. Therefore, curves in Theorem 4 that have order $n_1(z)$ or $n_5(z)$ may be pairing-friendly. □

Remark 7 (Obvious point).
Elliptic curves E_{16} and $E_{\pm 2}$ over $\mathbb{F}_{p(z)}$ have obvious points $(0, 4) \in E_{16}(\mathbb{F}_{p(z)})$, $(-1, 1) \in E_2(\mathbb{F}_{p(z)})$, and $(3, 5) \in E_{-2}(\mathbb{F}_{p(z)})$, respectively. Therefore, when one uses these curves to construct a pairing-based cryptosystem, one does not need to find a base point. □

Remark 8 (Elliptic curves suitable for pairing-based cryptosystems).
Due to Theorem 4 and Remarks 6 and 7, elliptic curves E_2 with $z \equiv 2, 7, 10, 11 \pmod{12}$ and E_{-2} with $z \equiv 1, 2, 5, 10 \pmod{12}$ are suitable for pairing-based cryptosystems since they may have prime order and always have an obvious point. □

5.3 Proof of Theorem 4

The outline of the proof of Theorem 4 is as follows. First, polynomials which generate A and B satisfying Eq. (7) of Theorem 1 are constructed by using Theorem 3. Then, one can explicitly see the number of points of the curve $C : u^3 + v^3 + 1 = 0$ due to Theorem 1. Next, $\#C(\mathbb{F}_{p(z)}) = \#E_{-432}(\mathbb{F}_{p(z)})$ is shown. Last, considering twists of E_{-432} derives Theorem 4.

Lemma 2.
Let $p(z) = 36z^4 + 36z^3 + 24z^2 + 6z + 1$ be a BN prime, and let C be a curve defined as

$$C : x^3 + y^3 + 1 = 0$$

as well as Theorem 1. Then, the following is held.
(a) $\#C(\mathbb{F}_p)$ is given by the following.

$$\#C(\mathbb{F}_p) = \begin{cases} 12z^2(3z^2+3z+1) & \textit{if } z \equiv 0 \pmod 3, \\ 3(12z^4+12z^3+10z^2+4z+1) & \textit{if } z \equiv 1 \pmod 3, \\ 3(12z^4+12z^3+10z^2+2z+1) & \textit{if } z \equiv 2 \pmod 3. \end{cases}$$

(b) $C(\mathbb{F}_{p(z)})$ has 3 points at infinity.
(c) One has $\#C(\mathbb{F}_{p(z)}) = \#E_{-432}(\mathbb{F}_{p(z)})$.

Proof) (a) Any BN prime $p(z)$ is represented as $p(z) = (6z^2+3z+1)^2 + 3z^2$, and thus $a = 6z^2+3z+1$ and $b = z$ can be set for a and b of Theorem 3. Let $m = a+b$ and $n = a-b$. Then, exactly one of $m = 6z^2+4z+1$, $n = 6z^2+2z+1$, and $m-n = 2z$ is a multiple of 3 due to Theorem 3. Consider three cases divided by the value z mod 3.

Case 1: $z \equiv 0 \pmod 3$
In this case, $m-n = 2z$ is a multiple of 3. Thus, one has

$$4p(z) = (m+n)^2 + 3(m-n)^2 = (12z^2+6z+2)^2 + 27\left(\frac{2z}{3}\right)^2.$$

Therefore, A of Theorem 1 is written as $A = -12z^2-6z-2$. One sees $\#C(\mathbb{F}_{p(z)}) = p(z)+1+A = 12z^2(3z^2+3z+1)$ due to Theorem 1.

Case 2: $z \equiv 1 \pmod 3$
In this case, $n = 6z^2+2z+1$ is a multiple of 3. Thus, one has

$$4p(z) = (2m-n)^2 + 3n^2 = (6z^2+6z+1)^2 + 27\left(\frac{6z^2+2z+1}{3}\right)^2.$$

Therefore, A of Theorem 1 is written as $A = 6z^2+6z+1$. One sees $\#C(\mathbb{F}_{p(z)}) = p(z)+1+A = 3(12z^4+12z^3+10z^2+4z+1)$ due to Theorem 1.

Case 3: $z \equiv 2 \pmod 3$
In this case, $m = 6z^2+4z+1$ is a multiple of 3, so one has

$$4p(z) = (m-2n)^2 + 3m^2 = (6z^2+1)^2 + 27\left(\frac{6z^2+4z+1}{3}\right)^2,$$

and A of Theorem 1 is $A = -6z^2-1$. Then, one sees $\#C(\mathbb{F}_{p(z)}) = p(z)+1+A = 3(12z^4+12z^3+10z^2+2z+1)$ due to Theorem 1.

(b) The curve C is represented as

$$U^3 + V^3 + W^3 = 0$$

in the projective coordinate. Projective points on C satisfying $W=0$ are exactly $[-1,1,0]$, $[-1,\omega,0]$, and $[-1,\omega^2,0]$, where w is the primitive cubic root of 1. These 3 points are those at infinity of C. Then, whether they are included in $C(\mathbb{F}_{p(z)})$ or not has to be checked.

It is known that $-1,1,0\in\mathbb{F}_{p(z)}$, and thus $[-1,1,0]\in C(\mathbb{F}_{p(z)})$. All BN primes $p(z)$ satisfy $p(z)\equiv 1 \pmod 3$, so one sees $w\in\mathbb{F}_{p(z)}$, which means $[-1,\omega,0],[-1,\omega^2,0]\in C(\mathbb{F}_{p(z)})$. Therefore, $[1,-1,0]$, $[1,\omega,0]$, $[1,\omega^2,0]\in C(\mathbb{F}_{p(z)})$, that is, $C(\mathbb{F}_{p(z)})$ has 3 points at infinity.
(c) For curves $E_{-432}: y^2=x^3-432$ and $C: u^3+v^3+1=0$, let a mapping $\zeta: E_{-432}(\mathbb{F}_{p(z)})\to C(\mathbb{F}_{p(z)})$ be defined as

$$(x,y)\to\left(\frac{-36+y}{6x},\frac{-36-y}{6x}\right).$$

Moreover, let another mapping $\xi: C(\mathbb{F}_{p(z)})\to E_{-432}(\mathbb{F}_{p(z)})$ be defined as

$$(u,v)\to\left(\frac{-12}{u+v},\frac{u-v}{u+v}\right).$$

Note that dividing by 6 in $\mathbb{F}_{p(z)}$ is possible because each BN prime $p(z)\geq 5$ for any integer z. These mappings are inexact because ζ is not defined for the point at infinity and points the x coordinate of which are 0, and ξ is not defined for points at infinity and points satisfying $u+v=0$. Defining sets as

$$\begin{aligned}
E_{-432}^{\mathcal{O}} &= \{\text{Set of the point at infinity in } E_{-432}(\mathbb{F}_{p(z)})\},\\
E_{-432}^{x=0} &= \{(x,y)\in E_{-432}(\mathbb{F}_{p(z)}) : x=0\},\\
C^{\mathcal{O}} &= \{\text{Set of points at infinity in } C(\mathbb{F}_{p(z)})\},\\
C^{u+v=0} &= \{(u,v)\in C(\mathbb{F}_{p(z)}) : u+v=0\},
\end{aligned}$$

mappings ζ and ξ are strictly defined as follows.

$$\begin{aligned}
\zeta: E_{-432}(\mathbb{F}_{p(z)})\backslash(E_{-432}^{\mathcal{O}}\cup E_{-432}^{x=0}) &\to C(\mathbb{F}_{p(z)})\\
(x,y) &\mapsto \left(\frac{-36+y}{6x},\frac{-36-y}{6x}\right)\\
\xi: C(\mathbb{F}_{p(z)})\backslash(C^{\mathcal{O}}\cup C^{u+v=0}) &\to E_{-432}(\mathbb{F}_{p(z)})\\
(u,v) &\mapsto \left(\frac{-12}{u+v},\frac{u-v}{u+v}\right)
\end{aligned}$$

Thus, one sees $\xi\circ\zeta(x,y)=(x,y)$ for any $(x,y)\in E_{-432}(\mathbb{F}_{p(z)})\backslash(E_{-432}^{\mathcal{O}}\cup E_{-432}^{x=0})$ and $\zeta\circ\xi(u,v)=(u,v)$ for any $(u,v)\in C(\mathbb{F}_{p(z)})\backslash(C^{\mathcal{O}}\cup C^{u+v=0})$. Therefore, ζ and ξ are inverse to each other, which means that they are one-to-one mappings, and thus one sees

$$\#E_{-432}(\mathbb{F}_{p(z)})\backslash(E_{-432}^{\mathcal{O}}\cup E_{-432}^{x=0})=\#C(\mathbb{F}_{p(z)})\backslash(C^{\mathcal{O}}\cup C^{u+v=0}).$$

Therefore, to show $\#E_{-432}(\mathbb{F}_{p(z)})=\#C(\mathbb{F}_{p(z)})$, it is enough to show

$$\#E_{-432}^{\mathcal{O}}+\#E_{-432}^{x=0}=\#C^{\mathcal{O}}+\#C^{u+v=0}, \tag{12}$$

because $\#E_{-432}^{\mathcal{O}} \cap \#E_{-432}^{x=0}$ and $\#C^{\mathcal{O}} \cap \#C^{u+v=0}$ are empty sets. Due to (b), one soon sees $\#C^{\mathcal{O}} = 3$ and $\#E_{-432}^{\mathcal{O}} = 1$.

Next, consider $\#E_{-432}^{x=0}$. Substituting $x = 0$ for $y^2 = x^3 - 432$ that is equation of E_{-432}, one has $y = \pm\sqrt{-432} = \pm 12\sqrt{-3}$. Due to Lemma 1-(d), one sees $\sqrt{-3} \in \mathbb{F}_{p(z)}$, and thus $\pm 12\sqrt{-3} \in \mathbb{F}_{p(z)}$. Thus, one has $E_{-432}^{x=0} = \{(0, 12\sqrt{-3}),\ (0, -12\sqrt{-3})\}$, which means $\#E_{-432}^{x=0} = 2$.

Last, consider $\#C^{u+v=0}$. Substituting $v = -u$ for $u^3 + v^3 + 1 = 0$, which is the equation of C, one has a contradictory equation $1 = 0$, which means $\#C^{u+v=0} = 0$.

Therefore, one sees $\#C(\mathbb{F}_{p(z)}) = \#E_{-432}(\mathbb{F}_{p(z)})$ due to Eq. (12) since $\#E_{-432}^{\mathcal{O}} = 1$, $\#E_{-432}^{x=0} = 2$, $\#C^{\mathcal{O}} = 3$, and $\#C^{u+v=0} = 0$. □

Now, this paper will complete proving Theorem 4.

Proof of Theorem 4-(a):

Due to Lemma 1-(d), -3 is quadratic residue modulo any BN prime $p(z)$. Thus, $-27 = (-3)^3$ is quadratic and cubic residue modulo $p(z)$. Due to Remark 2 $E_{16} : y^2 = x^3 - 432/(-27)$ is a twist of $E_{-432} : x^3 = y^2 - 432$ of degree 1, which means $\#E(\mathbb{F}_{p(z)}) = \#E_{-432}\mathbb{F}_{p(z)}$. Due to Lemma 2-(c), one sees $\#E(\mathbb{F}_{p(z)}) = \#C(\mathbb{F}_{p(z)})$, which completely proves (a).

Proof of Theorem 4-(b):

First, consider the case where z is even. Due to Lemma 1-(a) and (e), -1 is quadratic and cubic residue modulo $p(z)$. Due to Remark 2, $E_{-16} : y^2 = x^3 + 16/(-1)$ is a twist of $E_{16} : y^2 = x^3 + 16$ of degree 1. Therefore, one sees $\#E_{-16}(\mathbb{F}_{p(z)}) = \#E_{16}(\mathbb{F}_{p(z)})$, which completely proves (b) in the case where z is even.

Next, consider the case where z is odd. Due to Lemma 1-(a) and (e), -1 is non-quadratic and cubic residue modulo $p(z)$. Due to Remark 2, $E_{-16} : y^2 = x^3 + 16/(-1)$ is a twist of $E_{16} : y^2 = x^3 + 16$ of degree 2. Therefore, one writes $\#E_{16}(\mathbb{F}_{p(z)}) = p(z) + 1 - t$, and thus one has $\#E_{-16}(\mathbb{F}_{p(z)}) = p + 1 + t$, which completes the proof of (b) in the case where z is odd.

Proof of Theorem 4-(c) and (d):

For the proof, one divides set of z's into 2 cases, $z \equiv 0, 1 \pmod 4$ and $z \equiv 2, 3 \pmod 4$.

Case 1: $z \equiv 0, 1 \pmod 4$

In this case 2 is quadratic residue modulo $p(z)$, and thus 2^3 is quadratic and cubic residue modulo any $p(z)$. Due to Remark 2 E_2 and E_{-2} are twists of E_{16} and E_{-16} of degree 1, respectively. Thus, one has $\#E_2(\mathbb{F}_{p(z)}) = \#E_{16}(\mathbb{F}_{p(z)})$, and $\#E_{-2}(\mathbb{F}_{p(z)}) = \#E_{-16}(\mathbb{F}_{p(z)})$. Therefore, due to Theorem 4-(a) and (b) one sees

$$\#E_2(\mathbb{F}_{p(z)}) = \begin{cases} n_0(z) \text{ if } z \equiv 0 \pmod 3 \text{ and } z \equiv 0, 1 \pmod 4 \\ \qquad \text{(namely, } z \equiv 0, 9 \pmod{12}\text{)}, \\ n_4(z) \text{ if } z \equiv 1 \pmod 3 \text{ and } z \equiv 0, 1 \pmod 4 \\ \qquad \text{(namely, } z \equiv 1, 4 \pmod{12}\text{)}, \\ n_2(z) \text{ if } z \equiv 2 \pmod 3 \text{ and } z \equiv 0, 1 \pmod 4 \\ \qquad \text{(namely, } z \equiv 5, 8 \pmod{12}\text{)}. \end{cases}$$

$$\#E_{-2}(\mathbb{F}_{p(z)}) = \begin{cases} n_0(z) \text{ if } z \equiv 0 \pmod 6 \text{ and } z \equiv 0,1 \pmod 4 \\ \qquad \text{(namely, } z \equiv 0 \pmod{12}\text{)}, \\ n_1(z) \text{ if } z \equiv 1 \pmod 6 \text{ and } z \equiv 0,1 \pmod 4 \\ \qquad \text{(namely, } z \equiv 1 \pmod{12}\text{)}, \\ n_2(z) \text{ if } z \equiv 2 \pmod 6 \text{ and } z \equiv 0,1 \pmod 4 \\ \qquad \text{(namely, } z \equiv 8 \pmod{12}\text{)}, \\ n_3(z) \text{ if } z \equiv 3 \pmod 6 \text{ and } z \equiv 0,1 \pmod 4 \\ \qquad \text{(namely, } z \equiv 9 \pmod{12}\text{)}, \\ n_4(z) \text{ if } z \equiv 4 \pmod 6 \text{ and } z \equiv 0,1 \pmod 4 \\ \qquad \text{(namely, } z \equiv 5 \pmod{12}\text{)}, \\ n_5(z) \text{ if } z \equiv 5 \pmod 6 \text{ and } z \equiv 0,1 \pmod 4 \\ \qquad \text{(namely, } z \equiv 4 \pmod{12}\text{)}. \end{cases}$$

Case 2: $z \equiv 2, 3 \pmod 4$

In this case 2 is quadratic non-residue modulo $p(z)$ due to Lemma 1-(b), and thus 2^3 is quadratic non-residue and cubic residue modulo $p(z)$. Due to Remark 2 E_2 and E_{-2} are twists of E_{16} and E_{-16} of degree 2, respectively. Therefore, one sees $\#E_2(\mathbb{F}_{p(z)}) = 2p(z) + 1 - \#E_{16}(\mathbb{F}_{p(z)})$ and $\#E_{-2}(\mathbb{F}_{p(z)}) = 2p(z) + 1 - \#E_{-16}(\mathbb{F}_{p(z)})$. Due to that, $n_0(z) = 2p(z)+2-n_3(z)$, $n_1(z) = 2p(z)+2-n_4(z)$, $n_2(z) = 2p(z)+2-n_5(z)$, $n_3(z) = 2p(z)+2-n_0(z)$, $n_4(z) = 2p(z)+2-n_1(z)$, and $n_5(z) = 2p(z)+2-n_2(z)$ are satisfied and Theorem 4-(a) and (b), one sees

$$\#E_2(\mathbb{F}_{p(z)}) = \begin{cases} n_3(z) \text{ if } z \equiv 0 \pmod 3 \text{ and } z \equiv 2,3 \pmod 4 \\ \qquad \text{(namely, } z \equiv 3, 6 \pmod{12}\text{)}, \\ n_1(z) \text{ if } z \equiv 1 \pmod 3 \text{ and } z \equiv 2,3 \pmod 4 \\ \qquad \text{(namely, } z \equiv 7, 10 \pmod{12}\text{)}, \\ n_5(z) \text{ if } z \equiv 2 \pmod 3 \text{ and } z \equiv 2,3 \pmod 4 \\ \qquad \text{(namely, } z \equiv 2, 11 \pmod{12}\text{)}. \end{cases}$$

$$\#E_{-2}(\mathbb{F}_{p(z)}) = \begin{cases} n_3(z) \text{ if } z \equiv 0 \pmod 6 \text{ and } z \equiv 2,3 \pmod 4 \\ \qquad \text{(namely, } z \equiv 6 \pmod{12}\text{)}, \\ n_4(z) \text{ if } z \equiv 1 \pmod 6 \text{ and } z \equiv 2,3 \pmod 4 \\ \qquad \text{(namely, } z \equiv 7 \pmod{12}\text{)}, \\ n_5(z) \text{ if } z \equiv 2 \pmod 6 \text{ and } z \equiv 2,3 \pmod 4 \\ \qquad \text{(namely, } z \equiv 2 \pmod{12}\text{)}, \\ n_0(z) \text{ if } z \equiv 3 \pmod 6 \text{ and } z \equiv 2,3 \pmod 4 \\ \qquad \text{(namely, } z \equiv 3 \pmod{12}\text{)}, \\ n_1(z) \text{ if } z \equiv 4 \pmod 6 \text{ and } z \equiv 2,3 \pmod 4 \\ \qquad \text{(namely, } z \equiv 10 \pmod{12}\text{)}, \\ n_2(z) \text{ if } z \equiv 5 \pmod 6 \text{ and } z \equiv 2,3 \pmod 4 \\ \qquad \text{(namely, } z \equiv 11 \pmod{12}\text{)}. \end{cases}$$

Last, let us consider why $E_{\pm 16}$ and $E_{\pm 2}$ have the embedding degree 12. Let E_b be a BN curve. Then, E_b has the embedding degree 12. $E_{\pm 16}$ and $E_{\pm 2}$ are twists of E_b, so $E_{\pm 16}$ and $E_{\pm 2}$ also have the embedding degree 12 due to Eq. (2).
□

5.4 Method for Constructing Pairing-Friendly Elliptic Curves Using Theorem 4

As described in Remark 8, E_2 over $\mathbb{F}_{p(z)}$ with $z \equiv 2, 7, 10, 11 \pmod{12}$ and E_{-2} over $\mathbb{F}_{p(z)}$ with $z \equiv 1, 2, 5, 10 \pmod{12}$ are suitable for pairing-based cryptosystems. Now, pick up E_2 over $\mathbb{F}_{p(z)}$ with $z \equiv 2, 11 \pmod{12}$ as an example. To construct a pairing-friendly elliptic curve that has an obvious point, one just finds an integer z such that $p(z)$ and $n_5(z)$ are primes. Then, one obtains a pairing-friendly elliptic curve E_2 over $\mathbb{F}_{p(z)}$, meaning $\#E_2(\mathbb{F}_{p(z)}) = n_5(z)$, the embedding degree 12, and has a point $(-1, 1)$ due to Theorem 4.

Example When $z = 6332666225848387499$ is selected at Theorem 4, both $p(z)$ and $n_5(z)$ become primes of 256-bit. Therefore, one sees $E_2 : y^2 = x^3 + 2$ is a BN curve, that is, a pairing-friendly curve that has the embedding degree 12 with an obvious point $(-1, 1)$.

5.5 Comparison with proposed and current methods

Consider how to construct a pairing-friendly elliptic curve with a point for a base point of pairing-based cryptosystem using the current and the proposed methods.

In current methods, first one find a prime p and the prime order n using primality tests, and a square-free integer D of Eq. (6) satisfying Condition 1. Next one uses the CM method, which consists of three steps: computing the j-invariant that is main step, deciding coefficients, and checking the order, from p, n and D to construct a desirable elliptic curves described in Sec. 3.1. When $D = 1$ or 3, computing the j-invariant step, which is the main step in the CM method, can be skipped. After this, one searches for the point on the elliptic curve. If there is an obvious point, for example, $(1, 2) \in E_3 : y^2 = x^3 + 3$, finding a point a can be skipped, but if not, one has to compute a square root in $\mathbb{F}_p$ to find a point. Therefore, one needs at least primality tests and order checking to construct a pairing-friendly elliptic curve. Note that checking the order takes nonnegligible cost in terms of implementation and time.

On the other hand, the proposed method for constructing pairing-friendly elliptic curve (BN curves or twist of BN curves) does not need to use the CM method nor find a point. One just needs primality tests, which are also needed to set not only pairing-based but also major public key cryptosystems such as RSA and elliptic curve cryptosystems, to find a prime and an order.

6 Conclusion

This paper has explained that elliptic curves $E_{\pm 16} : y^2 = x^3 \pm 16$ and $E_{\pm 2} : y^2 = x^3 \pm 2$ over $\mathbb{F}_{p(z)}$, which are Barreto-Naehrig (BN) curves or twists of BN curves, have the embedding degree 12 and their orders are decided by some polynomials using Gauss' theorem and Euler's conjecture, where $p(z)$ is a BN prime represented as $p(z) = 36z^4 + 36z^3 + 18z^2 + 6z + 1$. Consequently, one can construct pairing-friendly elliptic curves without using the CM method or even checking the order. Specifically, E_2 over $\mathbb{F}_{p(z)}$ with $z \equiv 2, 7, 10, 11 \pmod{12}$ and E_{-2} over $\mathbb{F}_{p(z)}$ with $z \equiv 1, 2, 5, 10 \pmod{12}$ may have a prime order, and have an advantage of having an obvious point.

References

1. S. Al-Riyami, K. Paterson, "Certificateless public key cryptography," *ASIACRYPT 2003*, LNCS 2894, pp. 452-473. Springer, 2003.
2. A. Atkin and F. Morain, "Elliptic Curves and Primality Proving," *Math. Comp.* Vol. 61, No. 203, pp. 29-68, 1993.
3. P. Barreto, B. Lynn, and M. Scott, "Constructing elliptic curves with prescribed embedding degrees," *SCN 2002*, LNCS 2576, pp. 257-267, 2002.
4. P. Barreto and M. Naehrig, "Pairing-friendly elliptic curves of prime order," *SAC 2005*, LNCS 3897, pp. 319-331, 2006.
5. D. Boneh, G. Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," *EUROCRYPT 2004*, LNCS 3027, pp. 506-522, 2004.
6. D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," *SIAM Journal of Computing*, Vol. 32, No. 3, pp. 586-615, 2003.
7. D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and verifiably encrypted signatures from bilinear maps," *EUROCRYPT 2003*, LNCS 2656, pp. 416-432, 2003.
8. D. Boneh, G. Gentry, and B. Waters, "Collusion resistant broadcast encryption with short ciphertexts and private keys," *CRYPTO 2005*, LNCS 3621, pp. 258-275, 2005.
9. F. Brezing and A. Weng, "Elliptic curves suitable for pairing based cryptography," *Designs, Codes and Cryptography*, Springer–Verlag, Vol. 37, No. 1, pp. 133-141, 2005.
10. C. Cocks and R. Pinch, "Identity-based cryptosystems based on the Weil pairing," Unpublished manuscript, 2001.
11. A. Devegili, M. Scott and R. Dahab, "Implementing cryptographic pairings over Barreto-Naehrig curves," *Pairing 2007*, LNCS 4575, pp. 197-207, 2007.
12. R. Dupont, A. Enge, and F. Morain, "Building curves with arbitrary small MOV degree over finite prime fields," *Journal of Cryptology*, Vol. 18, No. 2, pp. 79-89, 2005.
13. D. Freeman, "Constructing pairing-friendly elliptic curves with embedding degree 10," *Algorithmic Number Theory*, LNCS 4076, pp. 452-465, 2006.
14. D. Freeman, M. Scott, and E. Teske, "A taxonomy of pairing-friendly elliptic curves," *Journal of Cryptology*, Vol. 23, No. 2, Springer, 2009.
15. S. Galbraith, J. McKee, and P. Valença, "Ordinary abelian varieties having small embedding degree," *Finite Fields and Their Applications*, Vol. 13, Iss.4, pp. 800-814, 2007.
16. F. Hess, "Efficient identity based signature schemes based on pairings," *SAC 2002*, LNCS 2595, pp. 310-324, 2003.
17. F. Hess, N. Smart, and F. Vercauteren, "The Eta pairing revisited," *IEEE Transactions on Information Theory*, Vol. 52, pp. 4595-4602, 2006.
18. N. Koblitz, *A course in number theory and cryptography*, Springer–Verlag, 1994.

19. E. Lee, H. Lee, and C. Park, "Efficient and generalized pairing computation on abelian varieties," Cryptology ePrint Archieve, Report 2008/40, 2008.
20. F. Lemmermeyer, *Reciprocity laws*, Springer–Verlag, 2000.
21. A. Lenstra and E. Verheul, "Selecting cryptographic key sizes," *Journal of Cryptology*, Vol. 14, No. 4, pp. 255-293, Springer, 2001.
22. S. Matsuda, N. Kanayama, F. Hess, and E. Okamoto, "Optimized versions of the Ate and twisted Ate pairings," *Cryptography and Coding*, LNCS 4887, pp. 302-312, 2007.
23. A. Menezes, T. Okamoto, and S. Vanstone, "Reducing elliptic curve logarithms to logarithms in a finite field," *IEEE Transactions on Information Theory*, Vol. 39, No. 5, pp. 1639-1646, 1993.
24. A. Miyaji, M. Nakabayashi, and S. Takano, "New explicit conditions of elliptic curve traces for FR-reduction," *IEICE Transactions on Fundamentals*, Vol. E84-A, No. 5, pp. 1234-1243, 2001.
25. Y. Nogami, M. Akane, Y. Sakemi, H. Kato, and Y. Morikawa, "Integer variable χ-based Ate pairing," *Pairing 2008*, LNCS 5209, pp. 178-191, 2008.
26. R. Sakai, K. Ohgishi, and M. Kasahara, "Cryptosystems based on pairing," In *SCIS 2000*, Okinawa, Japan, 2000.
27. J. Silverman, *The arithmetic of elliptic curves*, Springer–Verlag, 1986.
28. J. Silverman and J. Tate, *Rational points on elliptic curves*, Springer–Verlag, 1992.
29. S. Tanaka and K. Nakamula, "More constructing pairing-friendly elliptic curves for cryptography," `http://arxiv.org/PS_cache/arxiv/pdf/0711/0711.1942v1.pdf` .
30. S. Tanaka and K. Nakamula, "Constructing pairing-friendly elliptic curves using factorization of cyclotomic polynomials," *Pairing 2008*, LNCS 5209, pp. 136-145, 2008.
31. F. Zhang and K. Kim, "ID-based blind signature and ring signature from pairings," *ASIACRYPT 2002*, LNCS 2501, pp. 629-637, 2002.