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 curves that are pairing-friendly and have the embedding degree 12 having fixed coefficients, by using just primality tests without the complex multiplication method. Moreover, this paper discusses their twists. Specifically, this paper explains that the number of points on elliptic curves $y^2 = x^3 \pm 16$ and $y^2 = x^3 \pm 2$ over $\mathbb{F}_{p(z)}$ is given by one of 6 polynomials in z, $n_0(z), \cdots, n_5(z)$, classified by the value of z mod 12 for a prime $p(z) = 36z^4+36z^3+24z^2+6z+1$ with z an integer. The polynomial $n_5(z)$ represents the number of points on BN curves. For example, elliptic curve $y^2 = x^3 + 2$ over $\mathbb{F}_{p(z)}$ always becomes a BN curve for any integer z with $z \equiv 2, 11 \pmod{12}$. Then, to construct a pairing-friendly elliptic curve, it is enough to find an integer z of appropriate size such that $p(z)$ and $n_5(z)$ are primes.

Keywords: 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 called pairing-based cryptosystems (PBCs) 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 PBCs. 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 $r \mid (q^k - 1)$ satisfies $2 \leq k \leq 24$, and 3) $\rho = \log q / \log r$ is closed to 1. Such k's are called the embedding degree of E with respect to r.

For pairing-friendly supersingular elliptic curves, the maximal embedding degree becomes $4, 6, 2$ if characteristics of $\mathbb{F}_q$ are $2, 3, p \geq 5$, respectively [23]. Then one has to construct an ordinary (non-supersingular) elliptic curve if one needs an elliptic curve that has the embedding degree > 6.

Pairing-friendly ordinary 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 ordinary elliptic curves have been developed by some researchers (refer to Sec. 3.2). When one constructs a pairing-friendly elliptic curve using these methods, one also uses the complex multiplication (CM) method, which can be computationally expensive. 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 with fixed coefficients. 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 because all have j-invariant 0, is given by one of 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, $\#E(\mathbb{F}_{p(z)})$ 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 PBCs.

2 Elliptic Curves and Pairings

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

2.1 Elliptic Curves

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 on 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 $t = q + 1 - \#E(\mathbb{F}_q)$ 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 $k \geq 1$ satisfying $r \mid (q^k - 1)$ is

[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.

called the embedding degree of E with respect to r. The discriminant of E is defined as $\Delta(E) = -16(4a^3 + 27b^2)$, and the j-invariant of E is defined as $j(E) = -48^3a^3/\Delta(E)$. 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 Twists

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 6 [27, X.5.4]. It is known that

$$E' \text{ is a twist of } E \text{ of any degree} \Leftrightarrow j(E') = j(E). \tag{3}$$

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
$d = 2$	$q + 1 + t$	
$d = 3$	$q + 1 - (3f - t)/2$	$t^2 - 4q = -3f^2$
	$q + 1 - (-3f - t)/2$	$t^2 - 4q = -3f^2$
$d = 4$	$q + 1 + f$	$t^2 - 4q = -f^2$
	$q + 1 - f$	$t^2 - 4q = -f^2$
$d = 6$	$q + 1 - (-3f + t)/2$	$t^2 - 4q = -3f^2$
	$q + 1 - (3f + t)/2$	$t^2 - 4q = -3f^2$

Let E be an elliptic curve of $\mathbb{F}_q$, let t be the trace of E, and let E' be a twist of E of degree 2. Then, due to Table 1, $\#E'(\mathbb{F}_q) = q + 1 + t = 2q + 2 - \#E(\mathbb{F}_q)$. Therefore, one has the following lemma.

Lemma 1.
Let E be an elliptic curve over $\mathbb{F}_q$.
(a) If E' is a twist of E of degree 1 then $\#E'(\mathbb{F}_q) = \#E(\mathbb{F}_q)$.
(b) If E' is a twist of E of degree 2 then $\#E'(\mathbb{F}_q) = 2q + 2 - \#E(\mathbb{F}_q)$.

Remark 1.
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 $\psi : E' \to E, (x, y) \mapsto (\sqrt[3]{\delta}, \sqrt{\delta}y)$.

[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.

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 $\#E'(\mathbb{F}_q) = 2q + 2 - \#E(\mathbb{F}_q)$ due to Lemma 1.

Let E_b be denoted by the elliptic curve $E_b : y^2 = x^3 + b$ for any b.

Remark 2.
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).

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 order r. Then, a mapping $e : G_1 \times G_2 \to G_3$ is a bilinear pairing if it satisfies the following properties: bilinearity (i.e. $e(aP, bQ) = e(P, Q)^{ab}$ is satisfied for any $P \in G_1, Q \in G_2$ and any integers a and b), and non-degeneracy (i.e. there are P and Q such that $e(P, Q) \neq 1$).

The Ate pairing [17] this paper targets is a pairing defined on ordinary 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 ordinary 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 $2 \leq k \leq 24$ 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 CM Method

The CM method [2] 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

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

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 n over $\mathbb{F}_p$. In deciding coefficients step, 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 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). It is known that the CM method returns j-invariant 0 when $D = 3$. Therefore, if the case of $D = 3$ is considered, as is the case for BN curves, 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 ordinary 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 ordinary 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 [4], Freeman [13], Freeman et al. [14], 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, which can be computationally expensive, to construct a 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] Also, computing j-invariant step can be skipped in the case of $D = 1$.

3.3 BN Curves

Barreto and Naehrig developed a method for constructing pairing-friendly elliptic curves with $k = 12$ and $\rho \approx 1$ [4]. 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 cryptosystems (ECCs).

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

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

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

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

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.

It was observed by Devegili et al. [11] that, in practice, when p satisfies some equivalence conditions then E_3 is the BN curve. Performing the scalar multiplication step in this case is not necessary.

In this paper, primes given by $p(z)$ for some integer z are called *BN primes*. We show that the number of points on $E_{\pm 2}$ and $E_{\pm 16}$ over BN prime fields are given by one of six polynomials in z. Whenever z satisfies particular congruence conditions, the number of points is $n(z)$ and these elliptic curves are BN curves.

4 Mathematic Preliminaries

This section introduces a theorem that explains the number of points on a curve $u^3 + v^3 + 1 = 0$ and theorems about quadratic and cubic residues, 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 on 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 (-) be the Legendre symbol.
(a) $\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4, \\ -1 & \text{if } p \equiv 3 \pmod 4. \end{cases}$

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

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

(d) Let p' be a prime different from p. Then,

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

Proof) Refer to Koblitz [18]. □

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

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 a cubic residue module p if $\left(\frac{e}{p}\right)_3 = 1$, and otherwise f is called a cubic non-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 true.

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

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

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

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

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 using just primality tests without the CM method. To accomplish this, Theorem 4 at Sec. 5.2, which describes the number of points on 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 Residues Module BN Primes

To determine BN curves and twists thereof it is necessary to have some knowledge of quadratic and cubic residues 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 for the proof of Theorem 4.

Lemma 2 (Quadratic and cubic residues modulo BN primes).
For BN primes $p(z) = 36z^4 + 36z^3 + 24z + 6z + 1$ *the followings are true.*

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

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

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

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

(e) $\left(\dfrac{-1}{p(z)}\right)_3 = 1$ *for all BN primes* $p(z)$.

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

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

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

(Proof) Refer to Appendix A.1. □

Remark 4.
Due to Lemma 2, one sees that the quadratic and cubic residue status of some integers modulo BN primes $p(z)$ *can be characterized by* z.

5.2 Orders 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.*

$$n_0(z) = 12z^2(3z^2 + 3z + 1), \qquad n_1(z) = 36z^4 + 36z^3 + 18z^2 + 1,$$
$$n_2(z) = 3(12z^4 + 12z^3 + 10z^2 + 2z + 1), \quad n_3(z) = 4(9z^4 + 9z^3 + 9z^2 + 3z + 1),$$
$$n_4(z) = 3(12z^4 + 12z^3 + 10z^2 + 4z + 1), \quad n_5(z) = 36z^4 + 36z^3 + 18z^2 + 6z + 1.$$

Then, the numbers of points on $E_{\pm 16}$ *and* $E_{\pm 2}$ *are given by:*

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

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

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

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

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), then they are pairing-friendly. Other curves in Theorem 4 are twists of BN curves the embedding degree of which is not equal to 12, then they are not pairing-friendly. However, note that curves in Theorem 4 that have order $n_1(z)$ that is irreducible may be used for ECCs because ECCs do not care about the embedding degree.

Remark 6 (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 PBC or an ECC, one does not need to find a base point.

Remark 7 (Elliptic curves suitable for PBCs or ECCs).
Due to Theorem 4 and Remarks 5 and 6, E_2 over $\mathbb{F}_{p(z)}$ with $z \equiv 2,11 \pmod{12}$ and E_{-2} over $\mathbb{F}_{p(z)}$ with $z \equiv 2,5 \pmod{12}$ are suitable for PBCs if $p(z)$ and $n_5(z)$ are primes. Of course they are also suitable for ECCs. In addition, elliptic curves E_2 over $\mathbb{F}_{p(z)}$ with $z \equiv 7,10 \pmod{12}$ and E_{-2} over $\mathbb{F}_{p(z)}$ with $z \equiv 1,10 \pmod{12}$ are suitable for ECCs if $p(z)$ and $n_1(z)$ are primes.

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 on 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 3.
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 true.
(a) $\#C(\mathbb{F}_p)$ is given by:

$$\#C(\mathbb{F}_p) = \begin{cases} 12z^2(3z^2+3z+1) \ (= n_0(z)) & \textit{if } z \equiv 0 \pmod{3}, \\ 3(12z^4+12z^3+10z^2+4z+1) \ (= n_4(z)) & \textit{if } z \equiv 1 \pmod{3}, \\ 3(12z^4+12z^3+10z^2+2z+1) \ (= n_2(z)) & \textit{if } z \equiv 2 \pmod{3}, \end{cases}$$

where $n_0(z)$, $n_2(z)$, and $n_4(z)$ are of Theorem 4.
(b) $C(\mathbb{F}_{p(z)})$ has 3 points at infinity.
(c) $\#C(\mathbb{F}_{p(z)}) = \#E_{-432}(\mathbb{F}_{p(z)})$, that is,

$$\#E_{-432}(\mathbb{F}_p) = \begin{cases} 12z^2(3z^2+3z+1) & (=n_0(z)) \ \text{if } z \equiv 0 \pmod 3, \\ 3(12z^4+12z^3+10z^2+4z+1) & (=n_4(z)) \ \text{if } z \equiv 1 \pmod 3, \\ 3(12z^4+12z^3+10z^2+2z+1) & (=n_2(z)) \ \text{if } z \equiv 2 \pmod 3, \end{cases}$$

Proof) Refer to Appendix A.2. □

Lemma 4.
Let $p(z)$ be a BN prime, let E and E' be elliptic curves over $\mathbb{F}_{p(z)}$, and let $n_0(z), \cdots, n_5(z)$ be of Theorem 4. Then, the followings are true.
(a) If E' is a twist of E degree 1 then

$$\#E'(\mathbb{F}_{p(z)}) = \#E(\mathbb{F}_{p(z)}).$$

(b) If E' is a twist of E degree 2 then $\#E'(\mathbb{F}_{p(z)})$ is given by

$$\#E'(\mathbb{F}_{p(z)}) = \begin{cases} n_3(z) & \text{if } \#E(\mathbb{F}_{p(z)}) = n_0(z), \\ n_5(z) & \text{if } \#E(\mathbb{F}_{p(z)}) = n_2(z), \\ n_1(z) & \text{if } \#E(\mathbb{F}_{p(z)}) = n_4(z). \end{cases}$$

Proof) Refer to Appendix A.3. □

Now, this paper will complete proving Theorem 4.
Proof of Theorem 4-(a):
Note that the statement of Theorem 4-(a) is same as $\#E_{16}(\mathbb{F}_{p(z)}) = \#E_{-432}(\mathbb{F}_{p(z)})$ due to Lemma 3-(c). Therefore, it is enough to show $\#E_{16}(\mathbb{F}_{p(z)}) = \#E_{-432}(\mathbb{F}_{p(z)})$. Due to Lemma 2-(d), -3 is a quadratic residue modulo any BN prime $p(z)$. Thus, $-27 = (-3)^3$ is a quadratic and cubic residue modulo $p(z)$. Due to Remark 1, $E_{16} : y^2 = x^3 - 432/(-27)$ is a twist of $E_{-432} : x^3 = y^2 - 432$ of degree 1, which means $\#E_{16}(\mathbb{F}_{p(z)}) = \#E_{-432}(\mathbb{F}_{p(z)})$ due to Lemma 4-(a).
Proof of Theorem 4-(b):
First, consider the case where z is even. Due to Lemma 2-(a) and (e), -1 is a quadratic and cubic residue modulo $p(z)$. Due to Remark 1, $E_{-16} : y^2 = x^3 + 16/(-1)$ is a twist of $E_{16} : y^2 = x^3 + 16$ of degree 1. Therefore, one sees $\#E_{-16}(\mathbb{F}_{p(z)}) = \#E_{16}(\mathbb{F}_{p(z)})$ due to Lemma 4-(a). Therefore, due to Theorem 4-(a), one sees

$$\#E_{-16}(\mathbb{F}_{p(z)}) =$$
$$\begin{cases} n_0(z) & \text{if } z \equiv 0 \pmod 3 \text{ and } z \equiv 0 \pmod 2 \quad (\text{i.e. } z \equiv 0 \pmod 6), \\ n_4(z) & \text{if } z \equiv 1 \pmod 3 \text{ and } z \equiv 0 \pmod 2 \quad (\text{i.e. } z \equiv 4 \pmod 6), \\ n_2(z) & \text{if } z \equiv 2 \pmod 3 \text{ and } z \equiv 0 \pmod 2 \quad (\text{i.e. } z \equiv 2 \pmod 6). \end{cases}$$

Next, consider the case where z is odd. Due to Lemma 2-(a) and (e), -1 is a quadratic non-residue and cubic residue modulo $p(z)$. Due to Remark 1,

$E_{-16} : y^2 = x^3 + 16/(-1)$ is a twist of $E_{16} : y^2 = x^3 + 16$ of degree 2. Therefore, due to Theorem 4-(a) and Lemma 4-(b), one sees

$$\#E_{-16}(\mathbb{F}_{p(z)}) = \begin{cases} n_3(z) & \text{if } z \equiv 0 \pmod 3 \text{ and } z \equiv 1 \pmod 2 \quad (\text{i.e. } z \equiv 3 \pmod 6), \\ n_5(z) & \text{if } z \equiv 1 \pmod 3 \text{ and } z \equiv 1 \pmod 2 \quad (\text{i.e. } z \equiv 5 \pmod 6), \\ n_1(z) & \text{if } z \equiv 2 \pmod 3 \text{ and } z \equiv 1 \pmod 2 \quad (\text{i.e. } z \equiv 1 \pmod 6). \end{cases}$$

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 a quadratic residue modulo $p(z)$, and thus 2^3 is a quadratic and cubic residue modulo $p(z)$. Due to Remark 1, E_2 and E_{-2} are twists of E_{16} and E_{-16} of degree 1, respectively. Thus, due to Lemma 4-(a), 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

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

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

Case 2: $z \equiv 2, 3 \pmod 4$
In this case 2 is a quadratic non-residue modulo $p(z)$ due to Lemma 2-(b), and thus 2^3 is a quadratic non-residue and cubic residue modulo $p(z)$. Due to Remark 1, E_2 and E_{-2} are twists of E_{16} and E_{-16} of degree 2, respectively. Therefore, due to Theorem 4-(a), (b) and Lemma 4-(b), one sees

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

$$\#E_{-2}(\mathbb{F}_{p(z)}) =$$

$$\begin{cases} n_3(z) & \text{if } z \equiv 0 \pmod 6 \text{ and } z \equiv 2,3 \pmod 4 \quad (\text{i.e. } z \equiv 6 \pmod{12}), \\ n_4(z) & \text{if } z \equiv 1 \pmod 6 \text{ and } z \equiv 2,3 \pmod 4 \quad (\text{i.e. } z \equiv 7 \pmod{12}), \\ n_5(z) & \text{if } z \equiv 2 \pmod 6 \text{ and } z \equiv 2,3 \pmod 4 \quad (\text{i.e. } z \equiv 2 \pmod{12}), \\ n_0(z) & \text{if } z \equiv 3 \pmod 6 \text{ and } z \equiv 2,3 \pmod 4 \quad (\text{i.e. } z \equiv 3 \pmod{12}), \\ n_1(z) & \text{if } z \equiv 4 \pmod 6 \text{ and } z \equiv 2,3 \pmod 4 \quad (\text{i.e. } z \equiv 10 \pmod{12}), \\ n_2(z) & \text{if } z \equiv 5 \pmod 6 \text{ and } z \equiv 2,3 \pmod 4 \quad (\text{i.e. } z \equiv 11 \pmod{12}). \end{cases}$$

The proof of Theorem 4 is completed. □

5.4 Method for Constructing BN Curves Using Theorem 4

As described in Remark 7, E_2 over $\mathbb{F}_{p(z)}$ with $z \equiv 2, 11 \pmod{12}$ and E_{-2} over $\mathbb{F}_{p(z)}$ with $z \equiv 2, 5 \pmod{12}$ are BN curves with an obvious point. Now, pick up E_2 over $\mathbb{F}_{p(z)}$ with $z \equiv 2, 11 \pmod{12}$ as an example. To construct a BN curve with an obvious point, one just finds an integer z such that $p(z)$ and $n_5(z)$ are primes. Then, one obtains a BN 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 elliptic curve that has the embedding degree 12 with an obvious point $(-1, 1)$.

5.5 Comparison of proposed and current methods

Consider how to construct a pairing-friendly elliptic curve with a point for a base point of a PBC 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. (4) 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 can be skipped. For example, Algorithm 1 of [4], which is the original paper BN curves whose D is 3, is one of the most efficient current one for constructing pairing-friendly elliptic curves. It skips the main step of the CM method and takes 6 scalar multiplications on average.

After this, one searches for a point on the elliptic curve for a base point of PBC. If there is an obvious point, for example, $(1, 2) \in E_3 : y^2 = x^3 + 3$, finding a point 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 BN curve does not need to perform scalar multiplication, use the CM method, nor find a point. One

just needs primality tests, which are also needed to construct not only PBCs but also major public key cryptosystems such as RSA and ECC, to find a prime and an order.

6 Conclusion

This paper has explicitly provided the order of 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 BN curves or twists of BN curves, by one of 6 polynomials using Gauss' theorem and Euler's conjecture, where $p(z)$ is a BN prime represented as $p(z) = 36z^4 + 36z^3 + 18z^2 + 6z + 1$. Especially, E_2 over $\mathbb{F}_{p(z)}$ with $z \equiv 2, 11 \pmod{12}$ and E_{-2} over $\mathbb{F}_{p(z)}$ with $z \equiv 2, 5 \pmod{12}$ are BN curves with an obvious point for a base point of PBC. Consequently, one can construct pairing-friendly elliptic curves without using the CM method or even checking the order.

References

1. Al-Riyami, S.S., Paterson, K.G.: Certificateless public key cryptography. In: Laih, C.S. (Ed.) ASIACRYPT 2003. LNCS, vol. 2894, pp. 452-473. Springer, Heidelberg (2003)
2. Atkin, L.A.O., Morain, F.: Elliptic Curves and Primality Proving. Math. Comp. 61, 29-68 (1993)
3. Barreto, P.S.L.M., Lynn, B., Scott, M.: Constructing elliptic curves with prescribed embedding degrees. In: Cimato, S., Galdi, C., Persiano, G. (Eds.) SCN 2002. LNCS, vol. 2576, pp. 257-267. Springer, Heidelberg (2002)
4. Barreto, P.S.L.M., Naehrig, M.: Pairing-friendly elliptic curves of prime order. In: Preneel, B., Tavares, S. (Eds.) SAC 2005. LNCS, vol. 3897, pp. 319-331. Springer, Heidelberg (2006)
5. Boneh, D., Crescenzo, G.D., Ostrovsky, R., Persiano, G.: Public key encryption with keyword search, In: Cachin, C., Camenisch, J. (Eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 506-522. Springer, Heidelberg (2004)
6. Boneh, D., Franklin, M.: Identity-based encryption from the Weil pairing. In: Kilian, J. (Ed.) SIAM Journal of Computing. LNCS, vol. 32, pp. 586-615. Springer, Heidelberg (2003)
7. Boneh, D., Gentry, C., Lynn, B., Shacham, H.: Aggregate and verifiably encrypted signatures from bilinear maps. In: Biham, E. (Ed.) EUROCRYPT 2003. LNCS, vol. 2656, pp. 416-432. Springer, Heidelberg (2003)
8. Boneh, D., Gentry, C., Waters, B.: Collusion resistant broadcast encryption with short ciphertexts and private keys. In: Shoup, V. (Ed.) CRYPTO 2005. LNCS, vol. 3621, pp. 258-275. Springer, Heidelberg (2005)
9. Brezing, F., Weng, A.: Elliptic curves suitable for pairing based cryptography. Designs, Codes and Cryptography. Springer–Verlag. 37, 133-141 (2005)
10. Cocks, C., Pinch, R.: Identity-based cryptosystems based on the Weil pairing. Unpublished manuscript. (2001)
11. Devegili, A.J., Scott, M., Dahab, R.: Implementing cryptographic pairings over Barreto-Naehrig curves. In: Takagi, T., Okamoto, T., Okamoto, E., Okamoto, T. (Eds.) Pairing 2007. LNCS, vol. 4575, pp. 197-207. Springer, Heidelberg (2007)

12. Dupont, R., Enge, A., Morain, F.: Building curves with arbitrary small MOV degree over finite prime fields. Journal of Cryptology. 18, 79-89 (2005)
13. Freeman, D.: Constructing pairing-friendly elliptic curves with embedding degree 10. In: Hess, F., Pauli, S., Pohst, M. (Eds.) Algorithmic Number Theory. LNCS, vol. 4076, pp. 452-465. Springer, Heidelberg (2006)
14. Freeman, D., Scott, M., Teske, E.: A taxonomy of pairing-friendly elliptic curves. Journal of Cryptology. 23, (2009)
15. Galbraith, S.D., McKee, J.F., Valença, P.C.: Ordinary abelian varieties having small embedding degree. Finite Fields and Their Applications. 13, 800-814 (2007)
16. Hess, F.: Efficient identity based signature schemes based on pairings. In: Nyberg, K., Heys, H. (Eds.) SAC 2002. LNCS, vol. 2595, pp. 310-324. Springer, Heidelberg (2003)
17. Hess, F., Smart, N., and Vercauteren, F.: The Eta pairing revisited. IEEE Transactions on Information Theory, 52, 4595-4602 (2006)
18. Koblitz, N.: A course in number theory and cryptography. Springer–Verlag (1994)
19. Lee, E., Lee, H. and Park, C.: Efficient and generalized pairing computation on abelian varieties. Cryptology ePrint Archieve, Report 2008/40 (2008)
20. Lemmermeyer F.: Reciprocity laws, Springer–Verlag (2000)
21. Lenstra, A.K. and Verheul, E.R.: Selecting cryptographic key sizes. Journal of Cryptology, 14, 4, 255-293, Springer (2001)
22. Matsuda, S., Kanayama, N., Hess, F., and Okamoto, E.: Optimized versions of the Ate and twisted Ate pairings. In: Galbraith, S.D. (Eds.) Cryptography and Coding, LNCS, vol. 4887, pp. 302-312, Springer, Heidelberg (2007)
23. Menezes, A., Okamoto, T., and S. Vanstone, S.: Reducing elliptic curve logarithms to logarithms in a finite field. IEEE Transactions on Information Theory, 39, 5, 1639-1646 (1993)
24. Miyaji, A., Nakabayashi, M., and Takano, S.: New explicit conditions of elliptic curve traces for FR-reduction. IEICE Transactions on Fundamentals, E84-A, 5, 1234-1243 (2001)
25. Nogami, Y., Akane, M., Sakemi, Y., Kato, H., and Morikawa, Y.: Integer variable χ-based Ate pairing. In: Galbraith, S.D. and Paterson, K.G. (Eds.) Pairing 2008, LNCS, 5209, pp. 178-191, Springer, Heidelberg (2008)
26. Sakai, R., Ohgishi, K., and Kasahara, M.: Cryptosystems based on pairing. In SCIS 2000, Okinawa, Japan (2000)
27. Silverman, J.H.: The arithmetic of elliptic curves. Springer–Verlag (1986)
28. Silverman, J.H. and Tate, J.: Rational points on elliptic curves. Springer–Verlag (1992)
29. Tanaka, S. and Nakamula, K.: More constructing pairing-friendly elliptic curves for cryptography. In: Shacham, H. and Waters, B. (Eds) `http://arxiv.org/PS_cache/arxiv/pdf/0711/0711.1942v1.pdf`
30. Tanaka, S. and Nakamula, K.: Constructing pairing-friendly elliptic curves using factorization of cyclotomic polynomials. In: Galbraith, S.D. and Paterson, K.G. (Eds.) Pairing 2008, LNCS, vol. 5209, pp. 136-145, Springer, Heidelberg (2008)
31. Zhang, F. and Kim, K.: ID-based blind signature and ring signature from pairings. In: Zheng, Y. (Ed.) ASIACRYPT 2002, LNCS, vol. 2501, pp. 629-637, Springer, Heidelberg (2002)

A Proofs of Lemmas

A.1 Proof of Lemma 2

(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

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

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

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

□

A.2 Proof of Lemma 3

(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 (over the algebraic closure of $\mathbb{F}_{p(z)}$) 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.

The point $[-1, 1, 0]$ is included in $C(\mathbb{F}_{p(z)})$ since $-1, 0, 1 \in \mathbb{F}_{p(z)}$. 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

$$(u, v) \to \left(\frac{-12}{u + v}, \frac{-36(u - v)}{u + v} \right).$$

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.

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

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

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

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

Next, consider $\#E^{x=0}_{-432}$. 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 2-(d), one sees $\sqrt{-3} \in \mathbb{F}_{p(z)}$, and thus $\pm 12\sqrt{-3} \in \mathbb{F}_{p(z)}$. Thus, one has $E^{x=0}_{-432} = \{(0, 12\sqrt{-3}),\ (0, -12\sqrt{-3})\}$, which means $\#E^{x=0}_{-432} = 2$.

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 $\#E^{\mathcal{O}}_{-432} = 1$, $\#E^{x=0}_{-432} = 2$, $\#C^{\mathcal{O}} = 3$, and $\#C^{u+v=0} = 0$. □

A.3 Proof of Lemma 4

(a): Due to the definition of twist, if E' is a twist of E of degree 1 then $\#E'(\mathbb{F}_{p(z)}) = \#E(\mathbb{F}_{p(z)})$. (Also refer to Remark 1.)
(b): One has the followings by direct computations.

$$\begin{aligned} n_3(z) &= 2p(z) + 1 - n_0(z), \\ n_5(z) &= 2p(z) + 1 - n_2(z), \\ n_1(z) &= 2p(z) + 1 - n_4(z). \end{aligned}$$

By the assumption, E' is a twist of E of degree 2. Therefore, if $\#E(\mathbb{F}_{p(z)}) = n_0(z),\ n_2(z),\ n_4(z)$ then $\#E'(\mathbb{F}_{p(z)}) = n_3(z),\ n_5(z),\ n_1(z)$, respectively, due to Lemma 1. □