

MNT Elliptic Curves with Non-Prime Order

Maciej Grześkowiak

Adam Mickiewicz University

Faculty of Mathematics and Computer Science

Uniwersytetu Poznańskiego 4, 61-614 Poznań, Poland

maciejg@amu.edu.pl

Abstract. Miyaji, Nakabayashi, and Takano proposed an algorithm for the construction of prime order pairing-friendly elliptic curves with embedding degrees $k = 3, 4, 6$. We present a method for generating generalized MNT curves. The order of such pairing-friendly curves is the product of two distinct prime numbers.

Keywords: Pairing-based cryptography, MNT elliptic curves, Pell's equation.

1. Introduction

Let E be an elliptic curve defined over a finite field \mathbb{F}_p , where p is a prime. Let $\#E(\mathbb{F}_p)$ be the order of the group of \mathbb{F}_p -rational points of E . Let $n \neq p$ be a prime divisor of $\#E(\mathbb{F}_p)$. The embedding degree of E with respect to n is the smallest positive integer k such that $n \mid p^k - 1$, but n does not divide $p^d - 1$ for $d \mid k$, $d < k$, [7]. This condition is equivalent to $n > k$ divides $\Phi_k(p)$, where $\Phi_k(x)$ is the k th cyclotomic polynomial. Elliptic curves over \mathbb{F}_p that have a large subgroup of prime order n and a small embedding degree k are commonly referred to as pairing-friendly with respect to n and embedding degree k [7].

Many pairing-based cryptographic protocols require generating pairing-friendly elliptic curves. For instance: one-round three-way key exchange [9], identity-based encryption [2], identity-based signature [4], and short signature schemes [3]. From the security point of view, it is essential to find a pairing-friendly curve E over \mathbb{F}_p such that the discrete logarithm problems in the group $E(\mathbb{F}_p)$, in the order q subgroups of $E(\mathbb{F}_p)$, and in the multiplicative group $\mathbb{F}_{p^k}^*$ are computationally infeasible. The creators of the initial pairing-based protocols suggested utilizing supersingular elliptic curves.

However, these curves are restricted to an embedding degree $k = 2$ for prime fields and $k \leq 6$ in general [7]. Therefore, ordinary curves are necessary for higher embedding degrees.

A typical pairing-friendly ordinary elliptic curve construction method consists of two main steps. First, we find prime numbers n, p , integers $t \neq 0, 1, 2$ and $k \geq 3$ such that

$$|t| \leq 2p^{1/2}, \quad n \mid p + 1 - t, \quad n \mid \Phi_k(p). \quad (1)$$

We refer to t as the trace of Frobenius. By the Hasse-Weil bound $t = p + 1 - \#E(\mathbb{F}_p)$ satisfies $|t| \leq 2\sqrt{p}$. For every $|t| \leq 2p^{1/2}$, there exists an elliptic curve E over \mathbb{F}_p whose Frobenius trace is exactly t (see [14]). In the second step, we find the equation of the curve E over \mathbb{F}_p with $\#E(\mathbb{F}_p) = p + 1 - t$. By (1), it is obvious that we can write the integer

$$t^2 - 4p = \Delta y^2, \quad \Delta, y \in \mathbb{Z}, \quad (2)$$

in the unique form, where $\Delta < 0$ is a square-free integer. The above equation is called the CM equation and the integer Δ is called the CM discriminant. For given p, t , the Complex Multiplication (CM) method can be used to construct the curve equation over \mathbb{F}_p . Unfortunately, the CM algorithm is effective if Δ is small, that is $|\Delta| < 10^{10}$ [7]. In practical applications, the number k should be small, for example, $k \leq 100$, while the quotient $\log n / \log p$ should be close to one.

In [12], Miyaji, Nakabayashi, and Takano proposed an algorithm (the MNT method) for the construction of prime order pairing-friendly elliptic curves with embedding degrees $k = 3, 4, 6$. They found families of polynomials $(n_k(x), p_k(x), t_k(x))$ in $\mathbb{Z}[x]$ satisfying

$$n_k(x) = p_k(x) + 1 - t_k(x), \quad n_k(x) \mid \Phi_k(p_k(x)), \quad |t_k(x)| \leq 2\sqrt{p_k(x)}, \quad (3)$$

(see Table 1). In this case, the corresponding CM equation can be written as

$$t_k(x)^2 - 4p_k(x) = \Delta Y^2, \quad Y \in \mathbb{Z},$$

where $\Delta < 0$ is a square-free integer. Multiplying the quadratic equation above by a constant factor and completing the squares, we obtain Pell's equation

$$X^2 - 3\Delta Y^2 = m, \quad m = -8, k = 4, 6 \quad \text{or} \quad m = 24, k = 3, \quad (4)$$

where $X = X(x), Y \in \mathbb{Z}$.

k	$n_k(x)$	$p_k(x)$	$t_k(x)$	Pell's equation
6	$4x^2 \pm 2x + 1$	$4x^2 + 1$	$1 \pm 2x$	$(6x \pm 1)^2 + 3\Delta Y^2 = -8$
4	$x^2 + 2x + 2, x^2 + 1$	$x^2 + x + 1$	$-x, x + 1$	$(3x + t)^2 - 3\Delta Y^2 = -8, t = 1, 2$
3	$12x^2 \pm 6x + 1$	$12x^2 - 1$	$\pm 6x - 1$	$(6x \pm 3)^2 - 3\Delta Y^2 = 24$

Table 1. MNT families

We will call equation (4) generalized Pell's equation. This observation above leads to the MNT algorithm [12]. To find a desired curve, perform the following steps. Fix $k \in \{3, 4, 6\}$ and select

square-free integer $|\Delta| < 10^{10}$. Find the solution (X_0, Y_0) of (4), where $X_0 = X(x_0)$, such that the corresponding numbers $n = n_k(x_0)$ and $p = p_k(x_0)$ are simultaneously primes. Finally, use the CM method to construct the curve equation over \mathbb{F}_p . For a deeper discussion of the theory of Pell equations, we refer the reader to [13].

Luca and Shparlinski [11] gave some heuristic estimates on the number of elliptic curves which can be produced by the MNT algorithm. Let $E(z)$ denote the expected total number of all isogeny classes of MNT curves over all finite fields with embedding degree k and CM discriminant $|\Delta| \leq z$. Then we have

$$E(z) \ll \frac{z}{(\log z)^2}.$$

From the above estimate, the elliptic curves generated by the MNT algorithm are rare. We refer the reader to [11] for a deeper discussion of the lower bound of the generalized version of the function $E(z)$.

On the other hand, in most applications, an elliptic curve with $\#E(\mathbb{F}_p) = qn$ is acceptable, where q is small. Barreto and Scott used this idea in [1]. In particular, they extended the MNT algorithm to construct more Pell equations for $q > 1$. Galbraith, McKee, and Valença [8] generalize the MNT method by giving families of ordinary curves corresponding to non-prime group orders $\#E(\mathbb{F}_p) = qn$ with a prime n , $q = 2, 3, 4, 5$ and $k = 3, 4, 6$. Fotiadis and Konstantinou [6] extend the search to the MNT ordinary families with larger no prime cofactors $5 < q < 48$, and $k = 3, 4, 6$. In [5], the authors propose a general algorithm for constructing pairing-friendly elliptic curves with an arbitrary embedding degree. For a treatment of a more general case construction of pairing-friendly curves, we refer the reader to [7]. Let us fix a positive integers h and $k \in \{3, 4, 6\}$. Let $\mathcal{F}_k(h)$ denote the set of all possible families of MNT curves $(n_k(x), p_k(x), t_k(x))$ corresponding to group orders $\#E(\mathbb{F}_p) = qn$ with embedding degrees k , where $1 \leq q \leq h$. In [10], an algorithm was presented that outputs $\mathcal{F}_k(h)$. The algorithm idea is based on the following observations. From (3) we have,

$$\Phi_k(p_k(x)) \equiv \Phi_k(t_k(x) - 1) \pmod{n_k(x)}.$$

Choose $a, b \in \mathbb{Z}$. If $t_k(x) = ax + b$, then (3) shows that the degree of the polynomial $n_k(x)$ is equal to 2. Therefore, we can write,

$$\Phi_k(t_k(x) - 1) = d \cdot n_k(x), \quad d \in \mathbb{Z},$$

where d is the smallest common multiple of the coefficients of $\Phi_k(t_k(x) - 1)$. Now, assume that $n_k(x)$ is irreducible over \mathbb{Z} and there exists $q \in \mathbb{Z}$ such that

$$p_k(x) = q \cdot n_k(x) + t_k(x) - 1, \tag{5}$$

where $p_k(x)$ is irreducible over \mathbb{Z} . If moreover,

$$|t_k(x)| \leq 2\sqrt{p_k(x)}, \tag{6}$$

then we can use the polynomials $(n_k(x), p_k(x), t_k(x))$ above to construct the corresponding an elliptic MNT curve with q dividing $\#E(\mathbb{F}_p)$. From the above observations, it is easy to construct an algorithm

that finds all possible pairs of integer numbers a and b such that the corresponding conditions (5) and (6) are satisfied (see [10]). Given embedding degree k and a positive integer h , the algorithm tests all possible pairs of integers $|a| \leq 4h$ and $|b| < 4h$ to determine whether they satisfy the following condition. For fixed a, b , is there a positive integer $1 \leq q < h$ satisfying (5), (6) such that the corresponding polynomials $n_k(x)$ and $p_k(x)$ are irreducible over \mathbb{Z} ? If the condition is satisfied, for such a and b a family of polynomials $(n_k(x), p_k(x), t_k(x))$ is computed. We refer the reader to [10] for more details. It is easy to see that the algorithm takes no more than $O(h^3)$ steps to check all possible integers $|a| \leq 4h$, $|b| < 4h$ with $1 \leq q < h$. Therefore, given h , calculating $\mathcal{F}_k(h)$ using the algorithm shown in [10] may require an exponential number of steps. In [10], the authors computed the corresponding families of polynomials for $h = 6$ and $k = 3, 4, 6$. Now, we introduce the following definition.

Definition 1.1. Fix $k \in \{3, 4, 6\}$ and a prime $q \equiv 1 \pmod{k}$. The triple $(n_k(x), p_k(x), t_k(x))$ polynomials in $\mathbb{Z}[x]$ parameterizes a family of generalized MNT elliptic curves with embedding degree k if

$$qn_k(x) = p_k(x) + 1 - t_k(x), \quad qn_k(x) \mid \Phi_k(p_k(x)), \quad t_k(x)^2 - 4p_k(x) \leq 0, \quad (7)$$

and polynomials $n_k(x), p_k(x)$ are irreducible over \mathbb{Z} .

Remark 1.2. We see at once that if there is $x_0 \in \mathbb{Z}$ such that $n = n_k(x_0)$, and $p = p_k(x_0)$ are simultaneously prime, then there exists elliptic curve E defined over finite field \mathbb{F}_p such that

$$\#E(\mathbb{F}_p) = qn = p + 1 - t, \quad t = t_k(x_0).$$

Remark 1.3. Let $\#E(\mathbb{F}_p) = qn$. If $E(\mathbb{F}_p)$ has an embedding degree k with respect to n , then an embedding degree with respect to q can be generally different from k . Definition 1.1 covers the case where the embedding degree of $E(\mathbb{F}_p)$ equals k for any prime divisor of $\#E(\mathbb{F}_p)$ (see Proposition 2.4, [7]). It is clear that the families of polynomials satisfying Definition 1.1 belong to $\mathcal{F}_k(h)$.

The present paper extends the idea of effective polynomial families, first introduced in [12]. Our method generates families of polynomials that satisfy the properties of Definition 1.1. In particular, we propose methods for generating families of ordinary curves corresponding to non-prime group orders when q is any given prime number. By including an infinite family of prime cofactors in the analysis, we obtain a class of polynomial families belonging to $\mathcal{F}_k(h)$. For a given $k \in \{3, 4, 6\}$ and prime number $q < h$, our method finds a single family of polynomials of $\mathcal{F}_k(h)$ in a polynomial time with respect to the number of bits h . It is enough to calculate the root $x \pmod{q}$ of a given explicit quadratic polynomial to do so (see Theorems below). This property significantly speeds up the algorithm presented in the paper [10], which systematically calculates all possible solutions to the problem and checks each for a valid solution. For given a list of large prime numbers $q_i < h$, with $i = O(\log^c h)$, $c > 0$ and k , the approach presented in this paper allows us to efficiently determine the corresponding class of families of polynomials in $\mathcal{F}_k(h)$ while using the algorithm from [10] to this task would require exponential time with respect to h . We provide the corresponding generalized Pell

equation for the constructed families to construct desired elliptic curves effectively. All this together allows us to build an algorithmic method analogous to the algorithm in [12].

The remaining part of the paper is organized as follows. In Section 2, our families of polynomials are presented. Section 3 contains a detailed analysis of our constructions.

2. Main theorems

Throughout this paper, $\Delta < 0$ is a square-free rational integer. We denote by \mathbb{Z} the ring of integers numbers. Let k be a positive integer, and let $\Phi_k(x) \in \mathbb{Z}[x]$ be the k th cyclotomic polynomial; this is a unique monic polynomial of degree $\varphi(k)$ whose roots are the complex primitive k th roots of unity, where φ is Euler's totient function. In this article, we will consider only the case $k = 3, 4, 6$. For the convenience of the reader, we recall that

$$\Phi_3(x) = x^2 + x + 1, \quad \Phi_4(x) = x^2 + 1, \quad \Phi_6(x) = x^2 - x + 1.$$

In the following subsections, we will present parametric families of polynomials that are useful in constructing generalized MNT elliptic curves over a finite field with an embedding degree k .

2.1. The case $k = 6$

Theorem 2.1. Fix $j \in \{3, 6\}$, a prime $q \equiv 1 \pmod{6}$ or $q = 3$. Let $s < q$ be a root of $\Phi_j(x) \pmod{q}$. If $p_6(x) = \Phi_4(qx + s)$,

$$n_6(x) = \begin{cases} qx^2 + (2s + 1)x + \Phi_3(s)/q, & \text{if } q \mid \Phi_3(s), \\ qx^2 + (2s - 1)x + \Phi_6(s)/q, & \text{if } q \mid \Phi_6(s). \end{cases}$$

and

$$t_6(x) = \begin{cases} 1 - qx - s, & \text{if } q \mid \Phi_3(s), \\ 1 + qx + s, & \text{if } q \mid \Phi_6(s), \end{cases}$$

then polynomials $(n_6(x), p_6(x), t_6(x))$ parameterizes a family of generalized MNT elliptic curves with embedding degree 6. Moreover, the family has the corresponding generalized Pell equations

$$X^2 + 3\Delta Y^2 = -8, \quad X = \begin{cases} 3(qx + s) + 1 & \text{if } q \mid \Phi_3(s), \\ 3(qx + s) - 1 & \text{if } q \mid \Phi_6(s). \end{cases}$$

Proof:

See Section 3.1. □

Remark 2.2. Taking $j \in \{3, 6\}$, $q = 1$, $s = 0$, and $x = \pm 2y$ in Theorem 2.1, we obtain the MNT family with embedding degree 6.

Remark 2.3. Taking $q = 3$, $s = 1$ in Theorem 2.1, we get family belonging to the set $\mathcal{F}_6(6)$ (see Table 4, [10]).

2.2. The case $k = 4$

Theorem 2.4. Fix a prime $q \equiv 1 \pmod{4}$ or $q = 2$. Let $s < q$ or $s - 1 < q$ be a root of $\Phi_4(x) \pmod{q}$. If $p_4(x) = \Phi_6(qx + s)$,

$$n_4(x) = \begin{cases} qx^2 + 2sx + \Phi_4(s)/q, & \text{if } q \mid \Phi_4(s), \\ qx^2 + (2s - 2)x + \Phi_4(s - 1)/q, & \text{if } q \mid \Phi_4(s - 1). \end{cases}$$

and

$$t_4(x) = \begin{cases} 1 - qx - s, & \text{if } q \mid \Phi_4(s), \\ qx + s, & \text{if } q \mid \Phi_4(s - 1), \end{cases}$$

then polynomials $(n_4(x), p_4(x), t_4(x))$ parameterizes a family of generalized MNT elliptic curves with embedding degree 4. Moreover, the family has the corresponding generalized Pell equations

$$X^2 + 3\Delta Y^2 = -8, \quad X = \begin{cases} 3(qx + s) + 1 & \text{if } q \mid \Phi_4(s), \\ 3(qx + s) + 2 & \text{if } q \mid \Phi_4(s - 1). \end{cases}$$

Proof:

See Section 3.2. □

Remark 2.5. Taking $q = 1$, $s = 0$, and $x = \pm y$ in Theorem 2.4, we obtain the MNT family with embedding degree 4.

q	s	$n_k(x)$	$p_k(x)$	$t_k(x)$
2	1	$2x^2 + 2x + 1$	$4x^2 + 2x + 1$	$-2x$
5	2	$5x^2 + 4x + 1$,	$25x^2 + 15x + 3$	$-5x - 1$
5	3	$5x^2 + 6x + 2$	$25x^2 + 25x + 7$	$-5x - 1$

Table 2. MNT families

Remark 2.6. Taking q and s as in Table 2 and applying them to Theorem 2.4, we immediately get families belonging to the set $\mathcal{F}_4(6)$ (see Table 3, [10]).

2.3. The case $k = 3$

Theorem 2.7. Let $g_0(x) = 3x^2 - 1$, $g_1(x) = 3x^2 - 3x + 1$, $g_2(x) = 3x^2 + 3x + 1 \in \mathbb{Z}[x]$. Fix a prime $q \equiv 1 \pmod{3}$, and let $s < q$ be a root of $g_1(x) \pmod{q}$ or $g_2(x) \pmod{q}$. If $p_3(x) = g_0(qx + s)$,

$$n_3(x) = \begin{cases} 3qx^2 + (6s - 3)x + g_1(s)/q, & \text{if } q \mid g_1(s), \\ 3qx^2 + (6s + 3)x + g_2(s)/q, & \text{if } q \mid g_2(s), \end{cases}$$

and

$$t_3(x) = \begin{cases} 3(qx + s) - 1, & \text{if } q \mid g_1(s), \\ 1 - 3(qx + s), & \text{if } q \mid g_2(s), \end{cases}$$

then polynomials $(n_3(x), p_3(x), t_3(x))$ parameterizes a family of generalized MNT elliptic curves with embedding degree 3. Moreover, the family has the corresponding generalized Pell equations

$$X^2 + 3\Delta Y^2 = 24, \quad X = 3(qx + s) + 3.$$

Remark 2.8. Taking $q = 1$, $s = 0$, and $x = \pm 2y$ in Theorem 2.7, we obtain the MNT family with embedding degree 3.

3. Proof of Theorems

3.1. The case $k = 6$

Lemma 3.1. Fix a prime $q \equiv 1 \pmod{6}$ or $q = 3$. Let $\Phi_6(s) \equiv 0 \pmod{q}$ or $\Phi_3(s) \equiv 0 \pmod{q}$. Then we have,

$$\begin{cases} \Phi_6(\Phi_4(qx + s)) = qf_1(x)f_2(x), & \text{if } q \mid \Phi_3(s), \\ \Phi_6(\Phi_4(qx + s)) = qf_3(x)f_4(x), & \text{if } q \mid \Phi_6(s), \end{cases} \quad (8)$$

for $x \in \mathbb{Z}$ and polynomials $f_i(x)$ are irreducible over \mathbb{Z} , $i = 1, 2, 3, 4$, where

$$\begin{aligned} f_1(x) &= qx^2 + (2s + 1)x + \Phi_3(s)/q, & f_2(x) &= q^2x^2 + (2s - 1)qx + \Phi_6(s), \\ f_3(x) &= q^2x^2 + (2s + 1)qx + \Phi_3(s), & f_4(x) &= qx^2 + (2s - 1)x + \Phi_6(s)/q. \end{aligned}$$

Proof:

If $q \equiv 1 \pmod{6}$, then -3 is a quadratic residue \pmod{q} , and a root of $\Phi_j(x) \pmod{q}$ can be computed, $j = 3, 6$. It is easily seen that $\Phi_3(1) \equiv \Phi_6(2) \equiv 0 \pmod{3}$. A trivial verification shows that,

$$\Phi_6(\Phi_4(x)) = \Phi_3(x)\Phi_6(x), \quad x \in \mathbb{Z}. \quad (9)$$

Let s be a root of $\Phi_k(x) \pmod{q}$, $k = 3$ or $k = 6$. From (9) it follows that,

$$\Phi_6(\Phi_4(qx + s)) = \Phi_3(qx + s)\Phi_6(qx + s) = \begin{cases} qf_1(x)f_2(x), & \text{if } q \mid \Phi_3(s), \\ qf_3(x)f_4(x), & \text{if } q \mid \Phi_6(s), \end{cases}$$

where

$$\begin{aligned} f_1(x) &= qx^2 + (2s + 1)x + \Phi_3(s)/q, & f_2(x) &= q^2x^2 + (2s - 1)qx + \Phi_6(s), \\ f_3(x) &= q^2x^2 + (2s + 1)qx + \Phi_3(s), & f_4(x) &= qx^2 + (2s - 1)x + \Phi_6(s)/q. \end{aligned}$$

The polynomials f_i are irreducible over \mathbb{Z} , $i = 1, 2, 3, 4$. Indeed, $\Delta(f_i)$ the discriminants of f_i are negative,

$$\begin{aligned}\Delta(f_1) &= (2s+1)^2 - 4\Phi_3(s) = -3, & \Delta(f_2) &= q^2((2s-1)^2 - 4\Phi_6(s)) = -3q^2, \\ \Delta(f_3) &= q^2((2s+1)^2 - 4\Phi_3(s)) = -3q^2, & \Delta(f_4) &= (2s-1)^2 - 4\Phi_6(s) = -3.\end{aligned}$$

This finishes the proof. \square

We are now in a position to prove Theorem 2.1.

Proof:

Let $q \equiv 1 \pmod{6}$ be a prime or $q = 3$, and let $\Phi_3(s) \equiv 0 \pmod{q}$. We will show that polynomials $n_6(x)$, $p_6(x)$ and $t_6(x)$ satisfy the conditions (7). We have,

$$\begin{aligned}qn_6(x) &= q^2x^2 + (2s+1)qx + \Phi_3(s) = \Phi_4(qx+s) + qx + s \\ &= p_6(x) + 1 - t_6(x),\end{aligned}$$

so $qn_6(x) \mid p_6(x) + 1 - t_6(x)$. An easy computation shows that,

$$t_6(x)^2 - 4p_6(x) = -3(qx+s)^2 - 2(qx+s) - 3 < 0. \quad (10)$$

Since $n_6(x) = f_1(x)$, (8) shows that

$$qn_6(x) \mid \Phi_6(p_6(x)).$$

The polynomials $n_6(x)$ and $p_6(x)$ are irreducible over \mathbb{Z} , which is clear from Lemma 3.1 and is easy to check. So the polynomials $n_6(x)$, $p_6(x)$ and $t_6(x)$ satisfy Definition 1.1. Fix x for the moment. We can write (10) in the form

$$t_6(x)^2 - 4p_6(x) = -3(qx+s)^2 - 2(qx+s) - 3 = \Delta Y^2, \quad Y \in \mathbb{Z},$$

where $\Delta < 0$ is a square-free integer. Multiplying the above equation by -3 , we obtain

$$X^2 + 3\Delta Y^2 = -8, \quad X = 3(qx+s) + 1.$$

The same proof works if $\Phi_6(s) \equiv 0 \pmod{q}$. The details are left to the reader. This finishes the proof. \square

3.2. The case $k = 4$

Lemma 3.2. Fix a prime $q \equiv 1 \pmod{4}$ or $q = 2$. If $\Phi_4(s) \equiv 0 \pmod{q}$ or $\Phi_4(s-1) \equiv 0 \pmod{q}$. Then we have

$$\begin{cases} \Phi_4(\Phi_6(qx+s)) = qf_5(x)f_6(x), & \text{if } q \mid \Phi_4(s), \\ \Phi_4(\Phi_6(qx+s)) = qf_7(x)f_8(x), & \text{if } q \mid \Phi_4(s-1), \end{cases}$$

for $x \in \mathbb{Z}$, and polynomials $f_i(x) \in \mathbb{Z}[x]$ are irreducible over \mathbb{Z} , $i = 5, 6, 7, 8$, where

$$\begin{aligned}f_5(x) &= qx^2 + 2sx + \Phi_4(s)/q, & f_6(x) &= q^2x^2 + (2s-2)qx + \Phi_4(s-1), \\ f_7(x) &= q^2x^2 + 2sqx + \Phi_4(s), & f_8(x) &= qx^2 + (2s-2)x + \Phi_4(s-1)/q.\end{aligned}$$

Proof:

If $q \equiv 1 \pmod{4}$, then -1 is a quadratic residue \pmod{q} , and a root of $\Phi_4(x) \pmod{q}$ can be computed. It is easily seen that $\Phi_2(1) \equiv 0 \pmod{3}$. A trivial verification shows that,

$$\Phi_4(\Phi_6(x)) = \Phi_4(x)\Phi_4(x-1), \quad x \in \mathbb{Z}. \quad (11)$$

Let s be a root of $\Phi_4(x) \pmod{q}$ or let $\Phi_4(s-1) \equiv 0 \pmod{q}$. From (11) it follows that,

$$\Phi_4(\Phi_6(qx+s)) = \begin{cases} qf_5(x)f_6(x), & \text{if } q \mid \Phi_4(s), \\ qf_7(x)f_8(x), & \text{if } q \mid \Phi_4(s-1), \end{cases} \quad (12)$$

where

$$\begin{aligned} f_5(x) &= qx^2 + 2sx + \Phi_4(s)/q, & f_6(x) &= q^2x^2 + (2s-2)qx + \Phi_4(s-1), \\ f_7(x) &= q^2x^2 + 2sqx + \Phi_4(s), & f_8(x) &= qx^2 + (2s-2)x + \Phi_4(s-1)/q. \end{aligned}$$

The polynomials f_i are irreducible over \mathbb{Z} , $i = 5, 6, 7, 8$. Indeed, $\Delta(f_i)$ the discriminants of f_i are negative,

$$\begin{aligned} \Delta(f_5) &= 4s^2 - 4\Phi_4(s) = -4, & \Delta(f_6) &= q^2((2s-2)^2 - 4\Phi_4(s-1)) = -4q^2, \\ \Delta(f_7) &= q^2(4s^2 - 4\Phi_4(s)) = -4q^2, & \Delta(f_8) &= (2s-2)^2 - 4\Phi_4(s-1) = -4. \end{aligned}$$

This finishes the proof. \square

We are now in a position to prove Theorem 2.4.

Proof:

Fix a prime $q \equiv 1 \pmod{4}$ or $q = 2$, and let $\Phi_4(s) \equiv 0 \pmod{q}$. We will show that polynomials $n_4(x)$, $p_4(x)$ and $t_4(x)$ satisfy the conditions (7). We have,

$$\begin{aligned} qn_4(x) &= q^2x^2 + 2sqx + \Phi_4(s) = (qx+s)^2 + 1 \\ &= \Phi_6(qx+s) + (qx+s) = p_4(x) + 1 - t_4(x) \end{aligned}$$

so $qn_4(x) \mid p_4(x) + 1 - t_4(x)$. A trivial verification shows that

$$t_4(x)^2 - 4p_4(x) = -3(qx+s)^2 - 2(qx+s) - 3 < 0. \quad (13)$$

Since $n_4(x) = f_5(x)$, (12) shows that

$$qn_4(x) \mid \Phi_4(p_4(x)).$$

The polynomials $n_4(x)$ and $p_4(x)$ are irreducible over \mathbb{Z} , which is clear from Lemma 3.2 and is easy to check. So the polynomials $n_4(x)$, $p_4(x)$ and $t_4(x)$ satisfy Definition 1.1. Fix x for the moment. We can write (13) in the form

$$t_4(x)^2 - 4p_4(x) = -3(qx+s)^2 - 2(qx+s) - 3 = \Delta Y^2, \quad Y \in \mathbb{Z},$$

where $\Delta < 0$ is a square-free integer. Multiplying the above equation by -3 , we obtain

$$X^2 + 3\Delta Y^2 = -8, \quad X = 3(qx+s) + 1$$

The same proof works if $\Phi_4(s-1) \equiv 0 \pmod{q}$. The details are left to the reader. This finishes the proof. \square

3.3. The case $k = 3$

Lemma 3.3. Let $g_0(x) = 3x^2 - 1$, $g_1(x) = 3x^2 - 3x + 1$ and $g_2(x) = 3x^2 + 3x + 1 \in \mathbb{Z}[x]$. Fix a prime $q \equiv 1 \pmod{6}$, and let $g_1(s) \equiv 0 \pmod{q}$ or $g_2(s) \equiv 0 \pmod{q}$. Then we have,

$$\begin{cases} \Phi_3(g_0(qx + s)) = qf_9(x)f_{10}(x), & \text{if } q \mid g_1(s), \\ \Phi_3(g_0(qx + s)) = qf_{11}(x)f_{12}(x), & \text{if } q \mid g_2(s) \end{cases} \quad (14)$$

$x \in \mathbb{Z}$ and polynomials $f_i(x) \in \mathbb{Z}[x]$ are irreducible over \mathbb{Z} , $i = 9, 10, 11, 12$, where

$$\begin{aligned} f_9(x) &= 3qx^2 + (6s - 3)x + g_1(s)/q, & f_{10}(x) &= 3q^2x^2 + (6s + 3)qx + g_2(s), \\ f_{11}(x) &= 3q^2x^2 + (6s - 3)qx + g_1(s), & f_{12}(x) &= 3qx^2 + (6s + 3)x + g_2(s)/q. \end{aligned}$$

Proof:

If $q \equiv 1 \pmod{6}$, then -3 is a quadratic residue \pmod{q} , and a root of $g_j(x) \pmod{q}$ can be computed, $j = 1, 2$. A trivial verification shows that,

$$\Phi_3(g_0(x)) = g_1(x)g_2(x), \quad x \in \mathbb{Z}. \quad (15)$$

Let s be a root of $g_k(x) \pmod{q}$, $j = 1$ or $j = 2$. From (15) it follows that,

$$\begin{cases} \Phi_3(g_0(qx + s)) = qf_9(x)f_{10}(x), & \text{if } q \mid g_1(s), \\ \Phi_3(g_0(qx + s)) = qf_{11}(x)f_{12}(x), & \text{if } q \mid g_2(s), \end{cases}$$

where

$$\begin{aligned} f_9(x) &= 3qx^2 + (6s - 3)x + g_1(s)/q, & f_{10}(x) &= 3q^2x^2 + (6s + 3)qx + g_2(s), \\ f_{11}(x) &= 3q^2x^2 + (6s - 3)qx + g_1(s), & f_{12}(x) &= 3qx^2 + (6s + 3)x + g_2(s)/q. \end{aligned}$$

The polynomials $f_i(x)$ are irreducible over \mathbb{Z} , $i = 9, 10, 11, 12$. Indeed, $\Delta(f_i)$ the discriminants of f_i are negative,

$$\begin{aligned} \Delta(f_9) &= (6s - 3)^2 - 12g_1(s) = -3, & \Delta(f_{10}) &= q^2((6s + 3)^2 - 12g_2(s)) = -3q^2, \\ \Delta(f_{11}) &= q^2((6s - 3)^2 - 12g_1(s)) = -3q^2, & \Delta(f_{12}) &= (6s + 3)^2 - 12g_2(s) = -3. \end{aligned}$$

This finishes the proof. □

We are now in a position to prove Theorem 2.7.

Proof:

Let $q \equiv 1 \pmod{6}$ be a prime, and let $g_1(s) \equiv 0 \pmod{q}$. We will show that polynomials $n_3(x)$, $p_3(x)$ and $t_3(x)$ satisfy the conditions (7). We have,

$$\begin{aligned} qn_3(x) &= 3q^2x^2 + (6s - 3)qx + g_1(s) = p_3(qx + s) - 3(qx + s) - \\ &= p_3(x) + 1 - t_3(x) \end{aligned}$$

so $qn_3(x) \mid p_3(x) + 1 - t_3(x)$. An easy computation shows that,

$$t_3(x)^2 - 4p_3(x) = -3(qx + s)^2 - 6(qx + s) + 5 < 0. \quad (16)$$

Since $n_3(x) = f_9(x)$, (14) shows that

$$qn_3(x) \mid \Phi_3(p_3(x)).$$

The polynomials $n_3(x)$ and $p_3(x)$ are irreducible over \mathbb{Z} , which is clear from Lemma 3.3 and is easy to check. So the polynomials $n_3(x)$, $p_3(x)$ and $t_3(x)$ satisfy Definition 1.1. Fix x for the moment. We can write (16) in the form

$$t_3(x)^2 - 4p_3(x) = -3(qx + s)^2 - 6(qx + s) + 5 = \Delta Y^2, \quad Y \in \mathbb{Z},$$

where $\Delta < 0$ is a square-free integer. Multiplying the above equation by -3 , we obtain

$$X^2 + 3\Delta Y^2 = 24, \quad X = 3(qx + s) + 3.$$

The same proof works for $g_2(s) \equiv 0 \pmod{q}$. The details are left to the reader. This finishes the proof. \square

References

- [1] Barreto P, Scott M. Generating more MNT Elliptic Curves. *Designs, Codes and Cryptography*, 2006. **38**:209–217.
- [2] Boneh D, Franklin M. Identity-based encryption from the Weil pairing. *SIAM J. Comput.*, 2003. **32**(3):586–615.
- [3] Boneh D, Lynn B, Shacham H. Short signatures from the Weil pairing. In: ASIACRYPT. 2001 pp. 514–532.
- [4] Choon J, Cheon J. An Identity-Based Signature from Gap Diffie-Hellman Groups. In: Desmedt Y (ed.), Public Key Cryptography, volume 2567 of *Lecture Notes in Computer Science*. Springer. ISBN 3-540-00324-X, 2003 pp. 18–30.
- [5] Duan P, Cui S, Chan C. Finding More Non-Supersingular Elliptic Curves for Pairing-Based Cryptosystems. *International Journal of Information Technology*, 2005. **2**(2):157–163.
- [6] Fotiadis G, Konstantinou E. On the Efficient Generation of Generalized MNT Elliptic Curves. In: Algebraic Informatics. 2013 pp. 147–159.
- [7] Freeman D, Scott M, Teske E. A taxonomy of pairing-friendly elliptic curves. *J. Cryptology*, 2010. **23**(2):224–280.
- [8] Galbraith S, McKee J, Valença P. Ordinary abelian varieties having small embedding degree. *Finite Fields and Their Applications*, 2007. **13**(4):800–814.
- [9] Joux A. A one round protocol for tripartite Diffie-Hellman. *J. Cryptology*, 2004. **17**(4):263–276.

- [10] Le D, Mrabet NE, Tan CH. On Near Prime-Order Elliptic Curves with Small Embedding Degrees. In: On Near Prime-Order Elliptic Curves with Small Embedding Degrees. In: Maletti, A. (eds) Algebraic Informatics. CAI 2015. LNCS 9270. 2015 pp. 140–151.
- [11] Luca F, Shparlinski I. Elliptic Curves with Low Embedding Degree. *Journal of Cryptology*, 2006. **19**:553–562.
- [12] Miyaji A, Nakabayashi M, Takano S. New Explicit conditions of elliptic curve traces for FR-reduction. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, 2001. **84**(5):1234–1243.
- [13] Mollin R. Fundamental Number Theory with Applications. CRC Press, 1997.
- [14] Silverman J. The Arithmetic of Elliptic Curves. Springer, 1985.