Note on families of pairing-friendly elliptic curves with small embedding degree

Keiji Okano

Tsuru University, 3-8-1 Tahara, Tsuru, Yamanashi 402-8555, Japan
E-mail okano@tsuru.ac.jp

Received May 11, 2016, Accepted August 1, 2016

Abstract
The set of pairing-friendly elliptic curves that are generated by given polynomials forms a complete family. Although a complete family with a $\rho$-value of 1 is the ideal case, there is only one such example that is known. We prove that there are no ideal families with embedding degree 3, 4, or 6 and that many complete families with embedding degree 8 or 12 are nonideal, even if we choose noncyclotomic families.

Keywords elliptic curves, pairing-based cryptography, embedding degree

Research Activity Group Algorithmic Number Theory and Its Applications

1. Introduction
Pairing-based cryptographic schemes, which have been suggested independently by Boneh-Franklin [1] and Sakai-Ohgishi-Kasahara [2], are based on pairings on elliptic curves. They fit many novel protocols for which no other practical implementation is known; see [3] for survey. One of the features of these schemes is that they require so-called pairing-friendly elliptic curves, which have special properties, whereas the elliptic ElGamal cryptosystems can be implemented by using almost randomly generated elliptic curves. More precisely, a pairing-friendly elliptic curve $E$ over a finite field $F_q$ has the following properties (see [3]): (i) The curve has a subgroup $G$ of large prime order $r$ such that $r \mid q^k - 1$ for some integer $k$, and $r \mid q^i - 1$ for $0 < i < k$. (ii) The parameters $q$, $r$, and $k$ should be chosen such that $r \geq \sqrt{q}$ and $k < (\log_q r)/8$, which mean that the discrete logarithm problem is not only infeasible both in $G$ and $F_q^*$ but also the pairings can be computed. Here, $k$ is called the embedding degree of $E$ with respect to $r$. In other words, the embedding degree is the degree of the extension field over $F_q$ to which the pairing maps. Also, we define the $\rho$-value of $E$ as $\rho(E) = (\log q)/(\log r)$.

In general, curves with small $\rho$-values are desirable in order to speed up the arithmetic on elliptic curves. If $\rho(E) \approx 1$, then the curve is ideal. Although there are some methods for constructing pairing-friendly elliptic curves, it is known to be very rare that $\rho$ takes the value almost 1. Recently, it has been found that such ideal curves are also required in the theory of zk-SNARK [4], which is an application for which these had not been assumed.

In practice, we need to construct curves of a specified bit size for each of various embedding degrees. To this end, in order to describe the families of pairing-friendly elliptic curves, we give four polynomials $t(x)$, $r(x)$, $q(x)$, and $y(x)$, instead of the trace $t$ of the Frobenius map on $E$, the above two parameters $r$ and $q$. The families of pairing-friendly elliptic curves that are generated by such polynomials are called complete families, and we consider them in this paper. Moreover, when $r(x)$ is chosen to be a cyclotomic polynomial, this yields the most popular complete family, known as the cyclotomic case (see Section 2 for more details).

We also define the $\rho$-value for complete families (Definition 6). The case where the $\rho$-value equals 1 is also ideal, while this is not true for most cases. We thus consider the question, under what conditions is the $\rho$-value equal to or close to 1? There is only one known example of a complete family with $\rho = 1$; it was constructed by Barreto and Naehrig [5] (Remark 8). Various approaches have been used to search for the ideal case; see, for example, [3,6–8].

In this paper, we show that there is no ideal case for which $k = 3$, 4, or 6. In addition, we consider the cases of $k = 8$ and 12, including noncyclotomic cases.

Theorem 1 Let $k = 3$, 4, or 6. There are no complete families of elliptic curves with embedding degree $k$ such that $\rho = 1$.

Theorem 2 Let $k = 8$ or 12, and $D$ a square-free positive integer. Suppose that $(t(x), r(x), q(x))$ parameterizes a complete family of elliptic curves with complex multiplication (CM) discriminant $D$ and embedding degree $k$. If

$$\sqrt{-D} \in \mathbb{Q}(\zeta_k) \text{ and } \deg r(x) \neq 2 \deg t(x),$$

then $\rho \neq 1$. Here, $\zeta_k$ is a primitive $k$th root of unity.

Under the assumption of Theorem 2, we see that $D = 1$ or 2 (resp. 1 or 3) if $k = 8$ (resp. $k = 12$). We denote the $k$th cyclotomic polynomial and Euler’s totient function as $\Phi_k(x)$ and $\varphi(x)$, respectively. Note that it is known that $r(x)$ is a factor of $\Phi_k(t(x) - 1)$, and the degree of $r(x)$ is a multiple of $\varphi(k)$. Moreover, note that if $\deg t(x) = 2$, then $\Phi_k(t(x) - 1)$ is irreducible in the case where $k = 8$ (see [9]), and, in the case $k = 12$, a family with $\rho = 1$ is given by [5], which satisfies $\deg r(x) = 2 \deg t(x)$. 


2. Family of Pairing-Friendly Elliptic Curves

In this section, we briefly explain the strategy for constructing complete families of pairing-friendly elliptic curves as proposed by Brezing and Weng [10]. For an elliptic curve \( E/\mathbb{F}_q \), define \( t \) by the trace of the Frobenius map on \( E \). Then, the order of \( E(\mathbb{F}_t) \) is described as \( \#E(\mathbb{F}_t) = q + 1 - t \).

**Definition 3** Let \( E/\mathbb{F}_q \) be an elliptic curve. Suppose that \( E(\mathbb{F}_t) \) has a subgroup of order \( r \) with \( \gcd(r, q) = 1 \). The embedding degree of \( E \) with respect to \( r \) is the extension degree \( [\mathbb{F}_q(\mu_r) : \mathbb{F}_q] \). Here, \( \mu_r \) is the set of all \( r \)th roots of unity in an algebraic closure of \( \mathbb{F}_q \).

If \( r \) is a prime such that \( r \nmid q \), then \( E \) has embedding degree \( k \) with respect to \( r \) if and only if \( r \mid \Phi_k(t - 1) \) [3, Remark 2.2 and Proposition 2.4].

We now describe the CM method, which is a strategy for constructing elliptic curves with given parameters.

**Theorem 4** (Atkin and Morain [11]) Let \( k \) be a positive integer. Suppose that there are some \( t, r, q \in \mathbb{Z} \) satisfying the following properties:

(i) \( r \) is a prime, and \( q \) is a power of a prime.
(ii) \( r \mid q^k - 1 \) and \( \gcd(t, q) = 1 \).
(iii) There exist some \( y \in \mathbb{Z} \) and some square-free positive integer \( D \) such that an equation \( Dy^2 = 4q - t^2 \) holds.

Then, computing the Hilbert class polynomial of \( \mathbb{Q}(\sqrt{-D}) \), we can construct an ordinary elliptic curve \( E/\mathbb{F}_q \) that satisfies the following:

(a) \( \#E(\mathbb{F}_t) = q + 1 - t \), and there is a subgroup of \( E(\mathbb{F}_t) \) with prime order \( r \).
(b) The embedding degree with respect to \( r \) is \( k \).

In this paper, according to [3], we call \( D \) itself (not the discriminant of \( \mathbb{Q}(\sqrt{-D}) \)) a CM discriminant. For applications, it is necessary to be able to construct curves of a specified bit size. To this end, we introduce the families of pairing-friendly curves. According to [3], we introduce the following definition.

**Definition 5** Let \( f(x) \) be a polynomial in \( \mathbb{Q}[x] \).

(i) If there is some \( a \in \mathbb{Z} \) such that \( f(a) \in \mathbb{Z} \), then we say that \( f(x) \) represents integers.
(ii) Assume that \( f(x) \) is nonconstant, irreducible, and represents integers. If \( f(x) \) has a positive leading coefficient and \( \gcd(f(x), x) \) such that \( f(x) \in \mathbb{Z}[x] \) is a prime, and \( r \) \( \Phi_k(t - 1) \).

It is conjectured that if \( f(x) \) represents primes, then \( f(x) \) has infinitely many prime values.

**Definition 6** Let \( k \) be a positive integer, and \( D \) a positive square-free integer. Suppose that a triple of non-zero polynomials \( (t(x), r(x), q(x)) \) in \( \mathbb{Q}[x]^3 \) satisfies the following conditions:

(i) \( r(x) \) and \( q(x) \) represent primes.
(ii) \( r(x) \mid q(x) + 1 - t(x) \), i.e., there exists \( h(x) \in \mathbb{Q}[x] \) such that \( h(x)r(x) = q(x) + 1 - t(x) \).
(iii) \( r(x) \mid \Phi_k(t(x) - 1) \).

(iv) There is some \( y(x) \in \mathbb{Q}[x] \) such that \( Dy(x)^2 = 4q(x) - t(x)^2 = 4h(x)r(x) - (t(x) - 2)^2 \).

Then, we say that \( (t(x), r(x), q(x)) \) parameterizes a complete family of pairing-friendly elliptic curves with embedding degree \( k \) and CM discriminant \( D \). Moreover, we define \( \rho = \rho(t, r, q, y) := \frac{\deg y(x)}{\deg r(x)} = \frac{2\max\{\deg y(x), \deg t(x)\}}{\deg r(x)} \).

We note that, as [3] says, it may happen that \( (t(x), r(x), q(x)) \) does not lead to any explicit examples of elliptic curves; for example, \( p(x), q(x) \) may be never integers simultaneously. However, it is no problem in this paper, since we use the condition that \( r(x) \) is irreducible and \( q(x) \) represents primes instead of (i).

If \( (t(x), r(x), q(x)) \) parameterizes a complete family with embedding degree \( k \), then \( r(x) \) defines a field \( \mathbb{Q}[x]/(r(x)) \) that is isomorphic to a field containing the \( k \)th cyclotomic field and the imaginary quadratic field \( \mathbb{Q}(\sqrt{-D}) \), and then \( t(x) - 1 \) corresponds to a primitive \( k \)th root of unity by Definition 6 (iii)(iv).

**Theorem 7** (Brezing-Weng [10]) Let \( k \) be a positive integer, and let \( D \) be a positive square-free integer. Then, execute the following steps.

1. Choose an algebraic number field \( K \) that contains the \( k \)th cyclotomic field and \( \mathbb{Q}(\sqrt{-D}) \).
2. Find an irreducible polynomial \( r(x) \in \mathbb{Z}[x] \) with positive leading coefficient and an isomorphism such that \( \mathbb{Q}[x]/(r(x)) \rightarrow K \).
3. Let \( t(x) - 1 \in \mathbb{Q}[x] \) be a polynomial mapping to a fixed \( k \)th root of unity \( \zeta_k \in K \) by the above isomorphism.
4. Let \( y(x) \in \mathbb{Q}[x] \) be a polynomial mapping to \( (\zeta_k - 1)/\sqrt{-D} \in K \) by the above isomorphism.
5. Put \( q(x) := (t(x)^2 + Dy(x)^2)/4 \in \mathbb{Q}[x] \).

If \( q(x) \) and \( r(x) \) represent primes, then the triple \( (t(x), r(x), q(x)) \) parameterizes a complete family of elliptic curves with embedding degree \( k \) and CM discriminant \( D \). We note that \( t(x), y(x) \) are determined up to modulus \( r(x) \).

**Remark 8** The choice of \( r(x) \) is an important part of this algorithm. When \( r(x) \) is chosen to be a cyclotomic polynomial \( \Phi_k(x) \mod 1 \), this yields the most popular complete family; this is called the cyclotomic case. Several examples are collected in [3,6]. Barreto and Naehrig [5] gave an example of \( \rho = 1 \) with \( k = 12 \) and \( D = 3: t(x) = 6x^2 + 1, r(x) = 36x^4 + 36x^3 + 18x^2 + 6x + 1, q(x) = 36x^4 + 36x^3 + 24x^2 + 6x + 1 \). This is the only known example of a complete family of curves with a \( \rho \)-value of 1.

3. Proof of Theorem 1

First, we show Theorem 1 for the case where \( \sqrt{-D} \in \mathbb{Q}(\zeta_k) \). The proof is similar to in [7, Proposition 4.1]. Let \( \zeta_k \) be a primitive \( k \)th root of unity corresponding to \( t(x) - 1 \) under a fixed isomorphism \( \mathbb{Q}[x]/(r(x)) \cong K \subset \mathbb{Q}(\zeta_k) \). For simplicity, put \( X = t(x) - 1 \). Assume that \( \deg t(x) < \deg r(x) \) and \( \deg y(x) < \deg r(x) \). Suppose
that $k = 4$. Then, $\Phi_4(x) = x^2 + 1$, $D = 1$, and so $\sqrt{-1}$ corresponds to $s(x) = \pm X$. Therefore, we have

$$y(x) \equiv \frac{(X - 1)s(x)}{-1} \equiv \pm (X + 1) \mod r(x),$$

since $r(x) \mid \Phi_4(X)$. By $\deg(t(x)) < \deg(r(x))$, we see that $y(x) = \pm (X + 1)$. Hence, $q(x) = (t(x)^2 + Dg(x)^2)/4 = (X + 1)^2/2$. This contradicts the assumption that $q(x)$ represents primes. Therefore, $\deg(t(x)) \geq \deg(r(x))$ or $\deg(y(x)) \geq \deg(r(x))$, and so $\rho \geq 2$ if $k = 4$. In the same way, using $\Phi_3(x) = x^2 + x + 1$ and $\Phi_6(x) = x^2 - x + 1$, we obtain $\rho \geq 2$ for the cases $k = 3$ and 6.

Next, we show the case where $\sqrt{-D} \notin \mathbb{Q}(\zeta_k)$. Assume that $\rho = 1$. Put $X = t(x) - 1$ and $m = \deg(t(x))$. Note that $m > 1$ by $\sqrt{-D} \notin \mathbb{Q}(\zeta_k)$. Then, since $r(x) \mid \Phi_k(X)$, the degree of $\Phi_k(X)$ with respect to $X$ is 2 and $\rho = \deg(t(x))/\deg(r(x))$, we may assume that

$$r(x) = \Phi_k(X).$$

**Lemma 9** If $k = 3, 4$, or 6 and $\rho = 1$, then $\deg(y(x)) = m/2$.

**Proof** Since $\deg X = m$, the $\mathbb{Q}$-vector space $\mathbb{Q}[x]_{2m-1}$, which consists of all polynomials with degree less than $2m = \deg r(x)$, has bases consisting of

$$x^{m-1}X, \quad x^{m-2}X, \quad \ldots, \quad xX, \quad X, \quad x^{m-1}, \quad x^{m-2}, \quad \ldots, \quad x, \quad 1.$$

We consider the polynomial $(X - 1)s(x)$ that is congruent to $-Dy(x)$ modulo $r(x)$. We can write $s(x) \in \mathbb{Q}[x]_{2m-1}$ uniquely as

$$s(x) = (F_1(x)x + a_1)X + (F_2(x)x + a_2)$$

for some $a_1 \in \mathbb{Q}$ and $F_1(x)$ that satisfy $\deg F_1(x) \leq m - 2$ ($i = 1, 2$). Therefore,

$$(X - 1)s(x) = F_1(x)xX^2 + a_1X^2 + (F_2(x) - F_1(x))xX + (a_2 - a_1)X - (F_2(x)x + a_2). \quad (1)$$

Note that $F_1(x)xX^2, a_1X^2, \text{ and } (F_1(x) - F_2(x))xX$ do not have any terms that are of the same degree as those of the others. On the other hand, dividing $(X - 1)s(x)$ by $r(x) = \Phi_k(X)$, there are some $G(x) \in \mathbb{Q}[x]$ and $b \in \mathbb{Q}$ such that

$$(X - 1)s(x) = -Dy(x) + (G(x)x + b)\Phi_k(X). \quad (2)$$

Here, $\deg G(x) \leq m - 2$, since $\deg((X - 1)s(x)) < m + 2m = 3m$ and $\deg y(x) < 2m$.

If $k = 4$, then $\Phi_4(X) = X^2 + 1$. Thus, the right-hand side of (2) becomes

$$-Dy(x) + G(x)xX^2 + bX^2 + G(x)x + b. \quad (3)$$

Since $\deg y(x) \leq m$, the terms in (1) and (3) of degree greater than $m$ coincide. Therefore, we obtain $G(x) = F_1(x) = F_2(x)$, $a_1 = b$. Thus,

$$-Dy(x) = (a_2 - a_1)X - 2F_1(x)x - (a_2 + a_1),$$

and so

$$D^2y(x)^2 = -4(a_2 - a_1)F_1(x)xX + 4F_1(x)^2x^2$$

$$+ 4(a_2 + a_1)F_1(x)x + \text{(polynomial of } X). \quad (4)$$

Since $r(x) = \Phi_4(X) \in \mathbb{Q}[X]$, we see that $Dy(x)^2 = 4hr(x) - (X - 1)^2 \in \mathbb{Q}[X]$. If we combine this with (4) and $\deg X \geq 2$, we obtain

$$F_1(x) = 0 \text{ or } a_1 = a_2.$$  

Otherwise, the leading term of $-4(a_2 - a_1)F_1(x)xX$ does not vanish, which contradicts $D^2y(x)^2 \in \mathbb{Q}[X]$. Assume that $F_1(x) = 0$. Then, $F_2(x) = 0$, and so $s(x) = a_1X + a_2 \in \mathbb{Q}[X]$. This implies that $\sqrt{-D} \in \mathbb{Q}(\zeta_k)$, which contradicts our assumption. Hence, we have $F_1(x) \neq 0$ and $a_1 = a_2 = b$; we also have $-Dy(x) = -2F_1(x)x - 2a_1$. Thus, $\deg y(x)^2 \leq 2(m - 1)$. By $y(x)^2 \in \mathbb{Q}[X]$ and $\deg X = m$, we have $\deg y(x) = m/2$. In the same way, we can obtain the same result if $k = 3$ or 6, as follows.

Suppose that $k = 3$. Then $r(x) = \Phi_3(X) = X^2 + X + 1$, and so the right-hand side of (2) becomes

$$-Dy(x) + G(x)xX^2 + bX^2 + G(x)xX + bX + G(x)x + b.$$  

Comparing this with (1), we obtain $G(x) = F_1(x) = F_2(x) - F_1(x) + b = a_1$, since $\deg y(x) \leq m$. Thus,

$$-Dy(x) = (a_2 - 2a_1)X - 3F_1(x)x - (a_2 + a_1),$$

and so

$$D^2y(x)^2 = -6(a_2 - 2a_1)F_1(x)xX + 9F_1(x)^2x^2$$

$$+ 6(a_2 + a_1)F_1(x)x + \text{(polynomial of } X).$$

By $D^2y(x)^2 \in \mathbb{Q}(X)$ and $\deg X \geq 2$, we obtain

$$F_1(x) = 0 \text{ or } 2a_1 = a_2.$$  

If we assume that $F_1(x) = 0$, then this contradicts $\sqrt{-D} \notin \mathbb{Q}(\zeta_k)$ in the same way as in the case $k = 4$. Hence, we have $F_1(x) \neq 0$ and $a_2 = 2a_1$. We have $-Dy(x) = -3F_1(x)x - 3a_1$, and so we have $\deg y(x) = m/2$ in the same way as in the case $k = 4$.

Suppose that $k = 6$. Then, $r(x) = \Phi_6(X) = X^2 - X + 1$, and the right-hand side of (2) becomes

$$-Dy(x) + G(x)xX^2 + bX^2 - G(x)xX - bX + G(x)x + b.$$  

Comparing this with (1), we obtain $G(x) = F_1(x) = -F_2(x) + F_1(x), b = a_1$, since $\deg y(x) \leq m$. Thus,

$$-Dy(x) = a_2X - F_1(x)x - (a_2 + a_1),$$

and so

$$D^2y(x)^2 = -2a_2F_1(x)xX + F_1(x)^2x^2$$

$$+ 2(a_2 + a_1)F_1(x)x + \text{(polynomial of } X).$$

By $D^2y(x)^2 \in \mathbb{Q}(X)$ and $\deg X \geq 2$, we obtain

$$F_1(x) = 0 \text{ or } a_2 = 0.$$  

If we assume that $F_1(x) = 0$, then this induces a contradiction in the same way as in the case $k = 4$. Hence $F_1(x) \neq 0$ and $a_2 = 0$. We have $-Dy(x) = -F_1(x)x - a_1$, and so we have $\deg y(x) = m/2$ in the same way as in the case $k = 4$.

(QED)

Assume that $\rho = 1$. Then, $\deg y(x) = m/2$ by Lemma 9. For each $k, Dy(x)^2 = 4\Phi_k(X) - (X - 1)^2$ has degree $m$. Hence, if $k = 3, 4,$ or 6, then $h = 1/4$ and $Dy(x)^2 = 3X, 2X,$ or $X$, respectively. Then, $q(x) = (t(x)^2 + Dy(x)^2)/4$ becomes

$$\frac{X^2 + 5X + 1}{4}, \quad \frac{X^2 + 4X + 1}{4}, \quad \text{or } \frac{X^2 + 3X + 1}{4}$$

if $k = 3, 4,$ or 6, respectively. None of these can represent integers, and so this would contradict the assumption.
Therefore, we have shown that $\rho$ cannot be 1.

4. Proof of Theorem 2

We now show Theorem 2. Let $m = \deg t(x)$. Note that $r(x)$ satisfies $r(x) \mid \Phi_k(t(x) - 1)$, and it is known that $\varphi(k) \mid \deg r(x)$ (see [3, Theorem 5.1]). Therefore, there is some integer $n \leq m$ such that

$$\deg r(x) = 4n,$$

since $\varphi(8) = \varphi(12) = 4$. Furthermore, if $4n < 2m$, then we obtain $\rho > 1$ from $\rho \geq 2\deg t(x)/\deg r(x)$. Therefore, we may assume that $m \leq 2n$. If we combine the assumption that $\deg r(x) \neq 2\deg t(x)$ with these facts, then we obtain

$$n \leq m < 2n.$$  \hfill (5)

We may also assume that $\deg y(x) < \deg r(x)$. Let $\zeta = \zeta_k$ be a primitive $k$th root of unity corresponding to $t(x) - 1$ under a fixed isomorphism $\mathbb{Q}[x]/(t(x)) \cong K \supset \mathbb{Q}(\zeta_k)$. For $\alpha \in \mathbb{Q}(\zeta)$, we define $P(\alpha) = P(\alpha; x) \in \mathbb{Q}[x]$ by the polynomial corresponding to $\alpha$ of degree less than $4n$. For example, $P(\zeta) = t(x) - 1$, $P((\zeta - 1)\sqrt{-D}) = -Dy(x)$. Furthermore, we see $P(\alpha + \beta) = P(\alpha) + P(\beta)$ holds for any $\alpha, \beta \in \mathbb{Q}(\zeta)$. Now, we assume that $\rho = 1$. Then, since $2\deg t(x) < \deg r(x)$ by (5), we have

$$\deg y(x) = 2n.$$  \hfill (6)

Moreover, since $\deg (P(\zeta^2)) = 2m < 4n$, again by (5), we have $P(\zeta^2) = P(\zeta)$. To prove the theorem, we consider $(\zeta - 1)\sqrt{-D}$ and $(\zeta - 1)\sqrt{-D}$.

Suppose that $k = 8$ and $D = 1$. Then, $\sqrt{-1} = \zeta^2$, and

$$-Dy(x) = P\left((\zeta - 1)\zeta^2\right) = P\left((\zeta^3 - \zeta^2)\right) = \pm P(\zeta^3) \neq P(\zeta).$$

From this, (5), and (6), we obtain

$$\deg P(\zeta^3) \leq 2m.$$  \hfill (7)

On the other hand, we have $\deg (P(\zeta)P((\zeta - 1)\sqrt{-1})) = m + 2n < 4n$ by (5). Since $\zeta^4 = 1$, we obtain

$$P\left((\zeta^3 + 1)\right) = P\left(\zeta(\zeta - 1)\sqrt{-1}\right) = P(\zeta)P\left(\zeta - 1\sqrt{-1}\right).$$

In particular, $P(\zeta^3 + 1)$ has degree $m + 2n$. However, by (7), $\deg P(\zeta^3 + 1) \leq 2m$, and so $2n \leq m$. This contradicts (5). Thus, $\rho \neq 1$ in this case.

The other cases can be proven in the same way. Suppose that $k = 8$ and $D = 2$. Then, $\sqrt{-2} = \pm (\zeta + \zeta^3)$, and so

$$-Dy(x) = P\left((\zeta - 1)\zeta^3\right) = \mp P(\zeta^3) \neq P(\zeta^3 - 1).$$

From this, (5), and (6), we obtain $\deg P(\zeta^3) \leq 2m$. On the other hand, since $\zeta^4 - \zeta^2 + 1 = 0$, from the above approach, we know that

$$P(\zeta(\zeta - 1)\sqrt{-1}) = P(\pm (\zeta^3 - \zeta^2 - \zeta + 1))$$

has degree $m + 2n$. However, $\deg P(\zeta^3 - \zeta^2 - \zeta + 1) \leq 2m$, and so $2n \leq m$. This contradicts 5. Thus, $\rho \neq 1$.

Finally, suppose that $k = 12$ and $D = 3$. Then, $\sqrt{-3} = \pm (2\zeta^2 - 1)$, and so

$$-Dy(x) = P\left((\zeta - 1)\zeta^2\right) = \pm 2P(\zeta^2) \neq P(2\zeta^2 - 1).$$

From this, (5), and (6), we obtain $\deg P(\zeta^3) \leq 2m$. On the other hand, since $\zeta^4 - \zeta^2 + 1 = 0$, from the above approach, we know that

$$P(\zeta(\zeta - 1)\sqrt{-1}) = P(\pm (\zeta^3 - \zeta^2 - \zeta + 1))$$

has degree $m + 2n$. However, $\deg P(\zeta^3 - \zeta^2 - \zeta + 1) \leq 2m$, and so $2n \leq m$. This contradicts 5. Thus, $\rho \neq 1$.

From this, (5), and (6), we obtain $\deg P(\zeta^3) \leq 2m$. On the other hand, since $\zeta^4 - \zeta^2 + 1 = 0$, from the above approach, we know that

$$P(\zeta(\zeta - 1)\sqrt{-1}) = P(\pm (\zeta^3 - \zeta^2 - \zeta + 1))$$

has degree $m + 2n$. However, $\deg P(\zeta^3 - \zeta^2 - \zeta + 1) \leq 2m$, and so $2n \leq m$. This contradicts 5. Thus, $\rho \neq 1$.

Finally, suppose that $k = 12$ and $D = 3$. Then, $\sqrt{-3} = \pm (2\zeta^2 - 1)$, and so

$$-Dy(x) = P\left((\zeta - 1)\zeta^2\right) = \pm 2P(\zeta^2) \neq P(2\zeta^2 - 1).$$

From this, (5), and (6), we obtain $\deg P(\zeta^3) \leq 2m$. On the other hand, since $\zeta^4 - \zeta^2 + 1 = 0$, from the above approach, we know that

$$P(\zeta(\zeta - 1)\sqrt{-1}) = P(\pm (\zeta^3 - \zeta^2 - \zeta + 1))$$

has degree $m + 2n$. However, $\deg P(\zeta^3 - \zeta^2 - \zeta + 1) \leq 2m$, and so $2n \leq m$. This contradicts 5. Thus, $\rho \neq 1$.

Finally, suppose that $k = 12$ and $D = 3$. Then, $\sqrt{-3} = \pm (2\zeta^2 - 1)$, and so

$$-Dy(x) = P\left((\zeta - 1)\zeta^2\right) = \pm 2P(\zeta^2) \neq P(2\zeta^2 - 1).$$

From this, (5), and (6), we obtain $\deg P(\zeta^3) \leq 2m$. On the other hand, since $\zeta^4 - \zeta^2 + 1 = 0$, from the above approach, we know that

$$P(\zeta(\zeta - 1)\sqrt{-1}) = P(\pm (\zeta^3 - \zeta^2 - \zeta + 1))$$

has degree $m + 2n$. However, $\deg P(\zeta^3 - \zeta^2 - \zeta + 1) \leq 2m$, and so $2n \leq m$. This contradicts 5. Thus, $\rho \neq 1$.

Finally, suppose that $k = 12$ and $D = 3$. Then, $\sqrt{-3} = \pm (2\zeta^2 - 1)$, and so

$$-Dy(x) = P\left((\zeta - 1)\zeta^2\right) = \pm 2P(\zeta^2) \neq P(2\zeta^2 - 1).$$

From this, (5), and (6), we obtain $\deg P(\zeta^3) \leq 2m$. On the other hand, since $\zeta^4 - \zeta^2 + 1 = 0$, from the above approach, we know that

$$P(\zeta(\zeta - 1)\sqrt{-1}) = P(\pm (\zeta^3 - \zeta^2 - \zeta + 1))$$

has degree $m + 2n$. However, $\deg P(\zeta^3 - \zeta^2 - \zeta + 1) \leq 2m$, and so $2n \leq m$. This contradicts 5. Thus, $\rho \neq 1$.