Memoirs of the Faculty of Engineering, Okayama University, Vol.40, pp.83-94, January, 2006

The Orders of Elliptic Curves $y^2 = x^3 + b,\ b \in F_q^*$

Yasuyuki Nogami† Yoshitaka Morikawa†
The Graduate School of Natural Science and Technology
Okayama University
Okayama 700-8530 Japan

(Received December 5, 2005)

This paper particularly deals with elliptic curves in the form of $E(x, y) = y^2 - x^3 - b = 0,\ b \in F_q^*$, where 3 divides $q-1$. In this paper, we refer to the well-known twist technique as x-twist and propose y-twist. By combining x-twist and y-twist, we can consider six elliptic curves and this paper proposes a method to obtain the orders of these six curves by counting only one order among the six curves.
Keywords: elliptic curve, twist, third power residue/non-residue

1 Introduction

In the modern information-oriented society, various devices are connected via the Internet. Information security technology has played a key role in protecting the devices or important information from evil Internet users. Especially, the public-key cryptosystem has many uses such as to sign digitally. The Rivest Shamir Adleman (RSA) cryptosystem has been the most widely used, but its key for ensuring security is approximately 2000 bits in length. On the other hand, since the elliptic curve cryptosystem(ECC) attains the same security level with an approximately 7-fold smaller key length as compared to the RSA, the ECC has received much attention and has been implemented on various processors.

For ensuring sufficient security and constructing the ECC, we have to compute the order of the elliptic curve and then check the order. Some fast order counting algorithms have been proposed[1],[2]; however, in general these algorithms take a lot of computation time and the computation is quite complicated, in general. In order to systematically generate a lot of secure curves, we often use twist technique[1]. Using twist technique, if we compute the order $\#E(F_q)$ of the curve;

$$E(x, y) = y^2 - x^3 - ax - b = 0,\ a, b \in F_q, \tag{1a}$$

then we also know the order $\#\tilde{E}(F_q)$ of its twisted curve;

$$\tilde{E}(x, y) = y^2 - x^3 - aA^2x - bA^3 = 0,\ A \in F_q^*, \tag{1b}$$

as $\#\tilde{E}(F_q) = 2q + 2 - \#E(F_q)$, where q is a power of a prime number larger than three, F_q is a finite field, and A is a quadratic power non residue in F_q. For the order $\#\tilde{E}(F_q)$, we do not need another order counting computation. Our motivation comes from this technique, this paper proposes a method to obtain six orders of six elliptic curves by order counting only once.

This paper particularly deals with elliptic curves in the form of

$$E(x, y) = y^2 - x^3 - b = 0,\ b \in F_q^*. \tag{2a}$$

It is well-known that that the order of Eq.(2a) is $q + 1$ when 3 does not divide $q - 1$, therefore the curve is a

†E-mail: {nogami,morikawa}@cne.okayama-u.ac.jp

kind of super-singular curves[1]. Supersingular curves are not secure from Frey Rück attack[3], therefore ECC does not use them. On the other hand, when 3 divides $q-1$, such a property has not been shown yet. This paper deals with the case that 3 divides $q-1$. In this paper, we refer to the above introduced twist technique Eqs.(1) as x-twist and propose y-twist as follows ;

$$E'(x,y) = y^2 - x^3 - bB^2 = 0, \quad (2b)$$
$$E''(x,y) = y^2 - x^3 - bB^4 = 0, \quad (2c)$$

where B is an element in F_q^*. By combining x-twist and y-twist, we can consider six elliptic curves from $E(x,y)$ given by Eq.(2a) and this paper proposes a method to obtain the six orders of these six elliptic curves by counting the order of only one of these six curves. From the viewpoints of x-twist and y-twist, in this paper we show the following properties; 1) elliptic curves in the form of Eq.(2a) are not super-singular when q is a prime number larger than 3, 2) the above mentioned six orders are distinct when the extension degree of the definition field is an odd number, 3) there exist prime order curves among the six curves, 4) the orders of elliptic curves in the form of Eq.(2a) are systematically determined without counting the orders when the definition field is $F_{q^{3^i}}$, where i is a non negative integer, and so on.

Throughout this paper, q is a power of an odd prime number larger than 3. F_q and F_{q^m} mean a finite field and its m-th extension field, respectively, where m is a positive integer. F_q^* and $F_{q^m}^*$ mean their multiplicative group, respectively.

2 Fundamentals of elliptic curve

In this section, we go over the fundamentals of elliptic curve.

2.1 Coefficient field and definition field

When the characteristic of F_q is not equal to 2 or 3, an elliptic curve over F_q is generally defined by

$$E(x,y) = y^2 - x^3 - ax - b = 0, \quad a, b \in F_q. \quad (3)$$

The solutions (x,y) to Eq.(3) are called F_q-rational points when the coordinates of x and y lie in F_q. This paper deals with elliptic curves whose coordinates lie in some extension field but coefficients a, b lie in its proper subfield. In order to distinguish these fields, we call the field of a, b coefficient field and that of coordinates x, y definition field. In what follows, we use F_q and F_{q^m} as the coefficient and definition field, when $m=1$, it means that these fields are same.

2.2 Weil's theorem

F_q-rational points on an elliptic curve form an additive Abelian group. In this paper, we denote this group and its order by $E(F_q)$ and $\#E(F_q)$, respectively. When the coefficient and definition fields are F_q and its extension field F_{q^m}, respectively, the order $\#E(F_{q^m})$ is given by using $\#E(F_q)$ as follows ;

Theorem 1 *Let the coefficient and definition fields be F_q and its extension field F_{q^m}, respectively. Let $t = q + 1 - \#E(F_q)$ be the trace of $E(F_q)$, then we have*

$$\#E(F_{q^m}) = q^m + 1 - t^{[m]}, \quad t^{[m]} = \alpha^m + \beta^m, \quad (4)$$

where α and β are complex numbers such that $\alpha\beta = q$ and $\alpha + \beta = t$, and $t^{[m]}$ is the trace of $E(F_{q^m})$.

In this paper, we call the above order $\#E(F_q)$ the *base order* and correspondingly we call its trace t the *base trace*. Theorem 1 indicates that, when the coefficient field is a proper subfield of the definition field, we can obtain the order $\#E(F_{q^m})$ by using the base trace t or the base order $\#E(F_q)$.

When the coefficient and definition fields are a finite field F_q and its extension field F_{q^m}, respectively, the order is given by Eq.(4). By using the base trace t, that is $t = q + 1 - \#E(F_q)$, $t^{[m]}$ shown in Eq.(4) is given by

$$t^{[m]} = \sum_{i=0}^{\lfloor m/2 \rfloor} \frac{m}{m-i} \binom{m-i}{i} (-q)^i t^{m-2i}, \quad (5)$$

where $\lfloor m/2 \rfloor$ means the greatest integer less than or equal to $m/2$. It is well-known that $\#E(F_{q^m})$ is divisible by the base order $\#E(F_q)$ as

$$\#E(F_q) \mid \#E(F_{q^m}). \quad (6)$$

2.3 Twist

For an original defining equation;

$$E(x,y) = y^2 - x^3 - ax - b = 0 \quad a, b \in F_q, \quad (7a)$$

the following $\tilde{E}(x,y)$ is called the *twist* of $E(x,y)$;

$$\tilde{E}(x,y) = y^2 - x^3 - aA^2x - bA^3 = 0, \quad (7b)$$

where A is a non-zero element in the definition field F_{q^m}. Corresponding to whether A is a quadratic residue (QR) or a quadratic non-residue (QNR), the order $\#\tilde{E}(F_{q^m})$ of the twisted elliptic curve $\tilde{E}(x,y)$ becomes as follows ;

$$\#\tilde{E}(F_{q^m}) = \begin{cases} q^m + 1 - t^{[m]} & \text{when } A \text{ is a QR} \quad (8a) \\ q^m + 1 + t^{[m]} & \text{when } A \text{ is a QNR} \quad (8b) \end{cases}$$

In what follows, we refer to this *twist* operation as *x-twist.*

2.4 Super-singular curves

In this paper, we particularly deal with elliptic curves in the form of

$$E(x,y) = y^2 - x^3 - b, \quad b \in F_q^*. \tag{9}$$

In what follows, let the defining equation $E(x,y)$ be in the form of Eq.(9). When 3 does not divide $q-1$, it is known that the order $\#E(F_q)$ and its trace t of the elliptic curve $E(x,y)$ becomes $q+1$ and 0, respectively, that is a kind of super-singular curve[1]. Since super-singular curves are not secure from Frey Rück attack[3], super-singular curves are not suitable for ECC. On the other hand, when 3 divides $q-1$, if q is a prime number p, $E(x,y)$ in the form of Eq.(9) is not super-singular as shown in Appendix.A. In this paper, we particularly consider the case that 3 divides $q-1$.

3 x-twist and y-twist

For elliptic curves in the form of Eq.(9), we consider x-twist and then propose y**-twist**. By combining x-twist and y-twist, we can prepare six elliptic curves. For these six curves, we show some properties and then show that these six curves have distinct orders when q is an odd power of a prime number p.

3.1 x-twist

For an original defining equation;

$$E(x,y) = y^2 - x^3 - b = 0, \quad b \in F_q^*, \tag{10a}$$

we can consider the x-twisted curve $\tilde{E}(x,y)$ as

$$\tilde{E}(x,y) = y^2 - x^3 - bA^3 = 0, \tag{10b}$$

where A is a non-zero element in the definition field F_{q^m}. Corresponding to whether or not A is a QR, the order is given by Eqs.(8). For the defining equation $E(x,y)$, in this paper, let $\phi_0(E)$ and $\phi_1(E)$ denote the elliptic curves that are x-twisted by using a QR and QNR in F_{q^m}, respectively. Accordingly, the orders of $\phi_0(E)$ and $\phi_1(E)$ are given by Eq.(8a) and Eq.(8b), respectively.

3.2 y-twist

For an original defining equation;

$$E(x,y) = y^2 - x^3 - b = 0, \quad b \in F_q^*, \tag{11a}$$

we consider the following elliptic curves $E'(x,y)$ and $E''(x,y)$;

$$E'(x,y) = y^2 - x^3 - bB^2 = 0, \tag{11b}$$
$$E''(x,y) = y^2 - x^3 - bB^4 = 0, \tag{11c}$$

where B is a non-zero element in the definition field F_{q^m}. Corresponding to whether $E(0,y)$ is irreducible or reducible over F_{q^m}, the orders $\#E(F_{q^m})$, $\#E'(F_{q^m})$, and $\#E''(F_{q^m})$ of $E(x,y)$, $E'(x,y)$, and $E''(x,y)$ over F_{q^m} becomes as follows ;

when $E(0,y)$ is irreducible over F_{q^m},

$$\#E(F_{q^m}) = 3N + 1, \tag{12a}$$
$$\#E'(F_{q^m}) = 3N' + 1, \tag{12b}$$
$$\#E''(F_{q^m}) = 3N'' + 1. \tag{12c}$$

when $E(0,y)$ is reducible over F_{q^m},

$$\#E(F_{q^m}) = 3N + 2 + 1, \tag{13a}$$
$$\#E'(F_{q^m}) = 3N' + 2 + 1, \tag{13b}$$
$$\#E''(F_{q^m}) = 3N'' + 2 + 1. \tag{13c}$$

N, N', N'' are the numbers of non-zero TRs in the following sets, respectively;

$$\{E(0,i),\ \forall i \in F_{q^m}\}, \tag{14a}$$
$$\{E'(0,i),\ \forall i \in F_{q^m}\}, \tag{14b}$$
$$\text{and} \quad \{E''(0,i),\ \forall i \in F_{q^m}\}. \tag{14c}$$

Moreover, corresponding to whether B is a third power residue (TR) or a third power non-residue (TNR) in F_{q^m}, the following relation holds for N, N', N'' ;

when B is a TR in F_{q^m},

$$N = N' = N'', \tag{15}$$

when B is a TNR in F_{q^m} and $E(0,y)$ is irreducible,

$$N + N' + N'' = q^m, \tag{16}$$

when B is a TNR in F_{q^m} and $E(0,y)$ is reducible,

$$N + N' + N'' + 2 = q^m. \tag{17}$$

The proof for these relations is shown in Appendix.B. In what follows, we refer to the operation shown in

Eqs.(11) as *y-twist*. For the defining equation $E(x,y)$, in this paper, $\psi_0(E)$ shows the elliptic curve that is y-twisted by using a TR in F_{q^m}. $\psi_1(E)$ and $\psi_2(E)$ show the elliptic curves that are y-twisted by using a TNR in F_{q^m} as shown in Eq.(11b) and Eq.(11c), respectively. Correspondingly, the orders of $\psi_0(E)$, $\psi_1(E)$, and $\psi_2(E)$ are given as Eqs.(12), Eqs.(13), Eq.(15) $\sim$ Eq.(17).

From the above viewpoint, we can also consider x-twist (*see* Appendix.C).

3.3 Six orders of elliptic curves $E(x,y) = y^2 - x^3 - b,\ b \in F_q^*$

Let us prepare a non-zero element $b \in F_q$ such that b is QNR and TNR in F_q. By using such an element b, we can consider the following six elliptic curves ;

$$\begin{aligned} E_1(x,y) &= y^2 - x^3 - b = 0, & (18a)\\ E_2(x,y) &= y^2 - x^3 - b^2 = 0, & (18b)\\ E_3(x,y) &= y^2 - x^3 - b^3 = 0, & (18c)\\ E_4(x,y) &= y^2 - x^3 - b^4 = 0, & (18d)\\ E_5(x,y) &= y^2 - x^3 - b^5 = 0, & (18e)\\ E_6(x,y) &= y^2 - x^3 - b^6 = 0. & (18f) \end{aligned}$$

Noting that $E_1(0,y)$ is irreducible over F_q[4], the following relations hold from the viewpoints of x-twist ϕ_0, ϕ_1 and y-twist ψ_0, ψ_1, ψ_2;

$$\begin{aligned} E_1 &= E_1, & (19a)\\ E_3 &= \psi_1(E_1), & (19b)\\ E_5 &= \psi_2(E_1), & (19c)\\ E_4 &= \phi_1(E_1), & (19d)\\ E_6 &= \psi_1(E_4) = \phi_1(E_3) = \psi_1(\phi_1(E_1)), & (19e)\\ E_2 &= \psi_2(E_4) = \phi_1(E_5) = \psi_2(\phi_1(E_1)). & (19f) \end{aligned}$$

Therefore, elliptic curves $E_2 \sim E_6$ are given from E_1 by combining x-twist and y-twist operations. Fig.1 shows an image of these relations.

Therefore, there are six base orders as follows ;

$$\begin{aligned} \#E_1(F_q) &= q + 1 - t_1, & (20a)\\ \#E_3(F_q) &= q + 1 - t_3, & (20b)\\ \#E_5(F_q) &= q + 1 - t_5, & (20c)\\ \#E_4(F_q) &= q + 1 - t_4 = q + 1 + t_1, & (20d)\\ \#E_6(F_q) &= q + 1 - t_6 = q + 1 + t_3, & (20e)\\ \#E_2(F_q) &= q + 1 - t_2 = q + 1 + t_5, & (20f) \end{aligned}$$

where $t_1 \sim t_6$ are the base traces of $E_1 \sim E_6$, respectively. In addition, from the viewpoints of x-twist and y-twist, we can easily find that every elliptic curve in the form of Eq.(9) has one of these six base orders. In other words, every elliptic curve in the form of Eq.(9) is isomorphic to a certain one of these six curves. Especially, when q is an odd power of a prime number p, these six curves have distinct orders as shown in Appendix.D.

In what follows, we use the fact that $\#E_3(F_q)$ and $\#E_6(F_q)$ are even numbers because $E_3(x,0)$ and $E_6(x,0)$ are reducible over F_q[1]. Since this paper deals with q as a power of an odd prime number $p > 3$, t_3 and t_6 are even integers. On the other hand, $\#E_1(F_q)$, $\#E_2(F_q)$, $\#E_4(F_q)$, and $\#E_5(F_q)$ are odd numbers.

4 Determining the orders of $E(x,y) = y^2 - x^3 - b,\ b \in F_q^*$

From Eqs.(20), we find that the six orders $\#E_1(F_q) \sim \#E_6(F_q)$ can be determined from t_1, t_3, and t_5. In this section, we show a method to obtain t_3 and t_5 from only t_1. From Weil's theorem, as shown in Eq.(6), we have

$$\#E_i(F_q) \mid \#E_i(F_{q^3}),\quad i = 1,2,3,4,5,6. \qquad (21)$$

Since a TNR in F_q becomes a TR in F_{q^3}(*see* Appendix.E), the TNR $b = -E(0,0)$ becomes a TR in F_{q^3}, this is the reason why we consider the third extension field F_{q^3}. Therefore, as introduced in Sec.3.2 and as shown in Eq.(15), we have

$$\#E_1(F_{q^3}) = \#E_3(F_{q^3}) = \#E_5(F_{q^3}), \qquad (22)$$
$$\#E_4(F_{q^3}) = \#E_6(F_{q^3}) = \#E_2(F_{q^3}), \qquad (23)$$

accordingly we have

$$\#E_i(F_q) \mid \#E_1(F_{q^3}),\quad i = 1,3,5, \qquad (24a)$$
$$\#E_i(F_q) \mid \#E_4(F_{q^3}),\quad i = 4,6,2. \qquad (24b)$$

In addition, from Weil's theorem and Eq.(5), we have

$$\begin{aligned} \#E_1(F_{q^3}) &= q^3 + 1 - (t_1^3 - 3qt_1) & (25a)\\ &= q^3 + 1 - (t_3^3 - 3qt_3) & (25b)\\ &= q^3 + 1 - (t_5^3 - 3qt_5), & (25c) \end{aligned}$$

and also we have

$$\begin{aligned} &\#E_4(F_{q^3})\\ =\ & q^3 + 1 - (t_4^3 - 3qt_4) = q^3 + 1 + (t_1^3 - 3qt_1) & (26a)\\ =\ & q^3 + 1 - (t_6^3 - 3qt_6) = q^3 + 1 + (t_3^3 - 3qt_3) & (26b)\\ =\ & q^3 + 1 - (t_2^3 - 3qt_2) = q^3 + 1 + (t_5^3 - 3qt_5). & (26c) \end{aligned}$$

$$\begin{array}{cccc} & & x\text{-twist} \Leftrightarrow & & \\ & E_1(x,y) = y^2 - x^3 - b & & E_4(x,y) = y^2 - x^3 - b^4 & \\ y\text{-twist} \Updownarrow & E_3(x,y) = y^2 - x^3 - b^3 & & E_6(x,y) = y^2 - x^3 - b^6 & \Updownarrow y\text{-twist} \\ & E_5(x,y) = y^2 - x^3 - b^5 & & E_2(x,y) = y^2 - x^3 - b^2 & \end{array}$$

Figure 1: x-twist and y-twist relations among the six curves

From Eqs.(25) and Eqs.(26), we find that the following $f_1(t) = 0$ and $f_4(t) = 0$ have solutions $t = t_1, t_3, t_5$ and $t = t_4, t_6, t_2$, respectively.

$$\begin{aligned} f_1(t) &= t^3 - 3qt - q^3 - 1 + \#E_1(F_{q^3}) \\ &= t^3 - 3qt - t_1^{[3]}, \qquad (27a) \\ f_4(t) &= t^3 - 3qt - q^3 - 1 + \#E_4(F_{q^3}) \\ &= t^3 - 3qt - t_4^{[3]}. \qquad (27b) \end{aligned}$$

Next, let us consider how to obtain t_3 and t_5 by using $f_1(t)$ and its zero t_1. By computing the order $\#E_1(F_q)$, we can obtain t_1 as

$$t_1 = q + 1 - \#E_1(F_q). \qquad (28)$$

Since $f_1(t_1) = 0$, by using Eq.(25a), we can factorize $f_1(t)$ as

$$f_1(t) = (t-t_1)(t^2+t_1t+s), \quad s = t_1^{[3]}/t_1 = t_1^2-3q, \qquad (29)$$

therefore we obtain t_3 and t_5 by solving the quadratic equation $f_1(t)/(t-t_1) = 0$ that is $t^2 + t_1t + s = 0$, $s = t_1^{[3]}/t_1 = t_1^2 - 3q$. From this quadratic equation, we can easily obtain two solutions t_a and t_b as t_3 and t_5.

As previously mentioned, since t_5 is an odd number and t_3 is an even number, we can easily distinguish whether the obtained t_a is t_3 or t_5, and so on. After that, we can determine t_4, t_6, and t_2 as follows ;

$$t_4 = -t_1,\ t_6 = -t_3,\ t_2 = -t_5. \qquad (30)$$

Consequently, by computing only $\#E_1(F_q)$, we can obtain $\#E_2(F_q) \sim \#E_6(F_q)$ without any complicated computation. It only requires solving the quadratic equation $f_1(t)/(t-t_1) = 0$, where t_1 is given as Eq.(28).

As shown in Appendix.F, we can also show the following relations ;

$$\begin{aligned} \#E_1(F_{q^3}) &= \#E_1(F_q)\#E_3(F_q)\#E_5(F_q), \qquad (31a) \\ \#E_4(F_{q^3}) &= \#E_4(F_q)\#E_6(F_q)\#E_2(F_q). \qquad (31b) \end{aligned}$$

$$\begin{aligned} t_1^{[3]} &= t_1t_3t_5, \qquad (32a) \\ t_4^{[3]} &= t_4t_6t_2. \qquad (32b) \end{aligned}$$

4.1 Extension

In the same way, we can consider the following six curves that are given as x-twisted and y-twisted curves of $E_1(x,y)$ and $E_4(x,y)$ over F_{q^3} ;

$$\begin{aligned} E_1(x,y) &= y^2 - x^3 - b = 0, \qquad (33a) \\ E_7(x,y) &= y^2 - x^3 - C^2b = 0, \qquad (33b) \\ E_8(x,y) &= y^2 - x^3 - C^4b = 0, \qquad (33c) \\ E_4(x,y) &= y^2 - x^3 - b^4 = 0, \qquad (33d) \\ E_9(x,y) &= y^2 - x^3 - C^2b^4 = 0, \qquad (33e) \\ E_{10}(x,y) &= y^2 - x^3 - C^4b^4 = 0, \qquad (33f) \end{aligned}$$

where C is a TNR in F_{q^3}. For these six curves, Fig.2 shows the x-twist and y-twist relations and Fig.3 shows the order relations. We should note that a QNR in F_q also becomes a QNR in $F_{q^{3^i}}$ [4], where i is a positive integer, therefore b becomes a TR in F_{q^3}; however, b is still a QNR in F_{q^3}.

For the six curves Eqs.(33), the x-twist and y-twist relations are written as

$$\begin{aligned} E_1 &= E_1, \qquad (34a) \\ E_7 &= \psi_1(E_1), \qquad (34b) \\ E_8 &= \psi_2(E_1), \qquad (34c) \\ E_4 &= E_4, \qquad (34d) \\ E_9 &= \psi_1(E_4) = \phi_1(E_7) = \psi_1(\phi_1(E_1)), \qquad (34e) \\ E_{10} &= \psi_2(E_4) = \phi_1(E_8) = \psi_2(\phi_1(E_1)). \qquad (34f) \end{aligned}$$

From Weil's theorem and Eq.(5), the orders are given as follows ;

$$\#E_1(F_{q^3}) = q^3 + 1 - t_1^{[3]} = q^3 + 1 - (t_1^3 - 3qt_1) \qquad (35a)$$

x-twist $\Leftrightarrow$

$E_1(x,y) = y^2 - x^3 - b$ $\quad$ $E_4(x,y) = y^2 - x^3 - b^4$

y-twist $\Updownarrow$ $E_7(x,y) = y^2 - x^3 - C^2 b$ $\quad$ $E_9(x,y) = y^2 - x^3 - C^2 b^4$ $\Updownarrow$ y-twist

$E_8(x,y) = y^2 - x^3 - C^4 b$ $\quad$ $E_{10}(x,y) = y^2 - x^3 - C^4 b^4$

Figure 2: x-twist and y-twist relations among the six curves over F_{q^3}

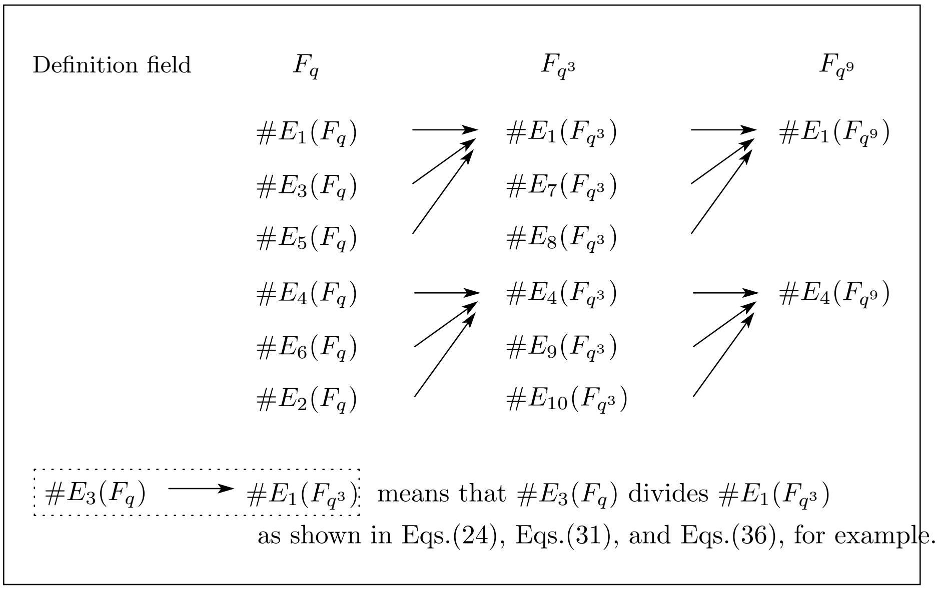

Figure 3: Order relations among six curves over F_{q^3}

$$\begin{aligned}
\#E_7(F_{q^3}) &= q^3+1-t_7, && (35b)\\
\#E_8(F_{q^3}) &= q^3+1-t_8, && (35c)\\
\#E_4(F_{q^3}) &= q^3+1-t_4^{[3]} = q^3+1+t_1^{[3]} \\
&= q^3+1+(t_1^3-3qt_1), && (35d)\\
\#E_9(F_{q^3}) &= q^3+1-t_9 = q^3+1+t_7, && (35e)\\
\#E_{10}(F_{q^3}) &= q^3+1-t_{10} = q^3+1+t_8, && (35f)
\end{aligned}$$

where $t_7 \sim t_{10}$ are the traces of $E_7(F_{q^3}) \sim E_{10}(F_{q^3})$, respectively. As shown in Eq.(35a), we can easily determine $\#E_1(F_{q^3})$ and $t_1^{[3]}$ by using only the base trace t_1. In the same way of the previous section, we have

$$\#E_i(F_{q^3}) \mid \#E_1(F_{q^9}),\quad i = 1,7,8, \qquad (36a)$$
$$\#E_i(F_{q^3}) \mid \#E_4(F_{q^9}),\quad i = 4,9,10. \qquad (36b)$$

In addition, we have

$$\begin{aligned}
\#E_1(F_{q^9}) &= q^9+1-\left((t_1^{[3]})^3 - 3q^3 t_1^{[3]}\right) && (37a)\\
&= q^9+1-(t_7^3-3q^3t_7) && (37b)\\
&= q^9+1-(t_8^3-3q^3t_8). && (37c)
\end{aligned}$$

Therefore, we can obtain t_7 and t_8 by solving the following quadratic equation ;

$$f_1^{[3]}(t) = (t-t_1^{[3]})(t^2+t_1^{[3]}t+u),\ \ u = t_1^{[9]}/t_1^{[3]} = (t_1^{[3]})^2-3q^3, \qquad (38)$$

where $t_1^{[9]}$ is given from Eq.(37a) as follows;

$$t_1^{[9]} = q^9+1-\#E_1(F_{q^9}) = (t_1^{[3]})^3 - 3q^3 t_1^{[3]}. \qquad (39)$$

From this quadratic equation, we can easily obtain two solutions t_c and t_d as t_7 and t_8. In this case, both t_7 and t_8 are odd integers, therefore we can not distinguish them in the same way of the previous section; however, we can distinguish them by generating a random rational point P on the elliptic curve $E_7(x,y)$ and then checking the order as follows ;

$$(q^3+1-t_c)P = \mathcal{O}\ \ or\ \ (q^3+1-t_d)P = \mathcal{O}, \qquad (40)$$

where $\mathcal{O}$ is the point at infinity. Consequently, the orders $\#E_1(F_{q^3}) \sim \#E_{10}(F_{q^3})$ can be determined from only the base trace t_1, furthermore the orders of elliptic curves in the form of $E(x,y) = y^2 - x^3 - b = 0$ whose coefficient and definition fields are $F_{q^{3^i}}$ are systematically determined from only the base trace t_1.

5 Experimental result

In this section, let us consider that q is a prime number $p > 3$, therefore the base field F_q is a prime field F_p. We use five prime numbers $7, 13, 19$ as the characteristic p that satisfies $3 \mid (p-1)$. Table 1 shows examples.

For example, let us consider $p = 7$ on Table 1. In this case, we prepare the following six defining equations $E_1(x,y) \sim E_6(x,y)$;

$$E_1(x,y) = y^2 - x^3 - 3 = 0, \quad (41a)$$
$$E_2(x,y) = y^2 - x^3 - 3^2 = y^2 - x^3 - 2 = 0, \quad (41b)$$
$$E_3(x,y) = y^2 - x^3 - 3^3 = y^2 - x^3 - 6 = 0, \quad (41c)$$
$$E_4(x,y) = y^2 - x^3 - 3^4 = y^2 - x^3 - 4 = 0, \quad (41d)$$
$$E_5(x,y) = y^2 - x^3 - 3^5 = y^2 - x^3 - 5 = 0, \quad (41e)$$
$$E_6(x,y) = y^2 - x^3 - 3^6 = y^2 - x^3 - 1 = 0, \quad (41f)$$

we compute only the base order $\#E_1(F_7) = 13$ and we have $t_1 = -5$. Therefore, according to Eq.(29), we have the following quadratic equation ;

$$f_1(t)/(t - t_1) = t^2 - 5t + 4 = 0. \quad (42)$$

Solving this quadratic equation, we obtain two solutions $(t_a, t_b) = (4, 1)$ as two base traces (t_3, t_5). As previously mentioned, t_3 must be an even number, therefore we can determine $t_3 = 4$ and $t_5 = 1$. Consequently, from Eqs.(20), we have

$$\#E_1(F_7) = 13,\quad \#E_3(F_7) = 4,\quad \#E_5(F_7) = 7, \quad (43a)$$
$$\#E_4(F_7) = 3,\quad \#E_6(F_7) = 12,\quad \#E_2(F_7) = 9. \quad (43b)$$

Table 2 shows the six orders $\#E_1(F_{q^3})$, $\#E_4(F_{q^3})$, and $\#E_7(F_{q^3}) \sim \#E_{10}(F_{q^3})$. Let us consider the case that $p = 7$. We have already known $\#E_1(F_{7^3})$ and $t_1^{[3]}$. Therefore, according to Eq.(38), we have

$$f_1^{[3]}(t)/(t - t_1^{[3]}) = t^2 - 20t - 629 = 0. \quad (44)$$

By solving this quadratic equation, we obtain two solutions $(t_c, t_d) = (37, -17)$ as two traces (t_7, t_8). Then, we have two orders 307 and 361 as $\#E_7(F_{7^3})$ and $\#E_8(F_{7^3})$. We can distinguish these orders by an elliptic curve scalar multiplication. After that, from Eqs.(35) we can obtain $\#E_9(F_{7^3})$ and $\#E_{10}(F_{7^3})$.

As shown in the tables, some prime order elliptic curves exist. Therefore, we can apply the proposed method for effectively generating prime order curves. In addition, on the tables we can observe that the six curves have six distinct orders since the extension degrees of F_p and F_{p^3} are odd numbers 1 and 3.

6 Conclusion

This paper has particularly dealt with elliptic curves in the form of

$$E(x,y) = y^2 - x^3 - b = 0,\ b \in F_q^*, \quad (45a)$$

where 3 divides $q-1$. In this paper, we referred to the well-known twist technique as x-twist and proposed y-twist as follows ;

$$E'(x,y) = y^2 - x^3 - bB^2 = 0, \quad (45b)$$
$$E''(x,y) = y^2 - x^3 - bB^4 = 0, \quad (45c)$$

where B is an element in F_q^*. By combining x-twist and y-twist, we considered six elliptic curves from $E(x,y)$ and this paper proposed a method to obtain the six orders of these six elliptic curves by counting the order of only one of these six curves. In addition, from the viewpoints of x-twist and y-twist, this paper showed some properties such as; the above mentioned six orders are distinct when the extension degree of the definition field is an odd number.

References

[1] I.Blake, G.Seroussi, and N.Smart, Elliptic Curves in Cryptography, LNS 265, Cambridge University Press, 1999.

[2] T.Satoh, "The Canonical Lift of an Ordinary Elliptic Curve over a Finite Field and its Point Counting," Jour. of the Ramanujan Mathematical Society, vol.15, pp.247-270, 2000.

[3] G.Frey and H.Rück, "A Remark Concerning m-Divisibility and the Discrete Logarithm in the Divisor Class Group of Curves," Math. Comp. **62**, 1994.

[4] R.Lidl and H.Niederreiter, Finite Fields, Encyclopedia of Mathematics and Its Applications, Cambridge University Press, 1984.

Table 1: Six base orders, traces, two solutions of $f_1(t)/(t-t_1)$

p		Const.†	Order**	Trace	$\#E_1(F_{p^3})$	$f_1(t)/(t-t_1)$	Solutions t_a, t_b
7	E_1	3	13^*	-5	364	t^2-5t+4	$4, 1$
	E_2	2	9	-1			
	E_3	6	4	4			
	E_4	4	3^*	5			
	E_5	5	7^*	1			
	E_6	1	12	-4			
13	E_1	2	19^*	-5	2128	$t^2-5t-14$	$7, -2$
	E_2	4	21	-7			
	E_3	8	16	-2			
	E_4	3	9	5			
	E_5	6	7^*	7			
	E_6	12	12	2			
19	E_1	2	13^*	7	6916	t^2+7t-8	$1, -8$
	E_2	4	21	-1			
	E_3	8	28	-8			
	E_4	16	27	-7			
	E_5	13	19^*	1			
	E_6	7	12	8			

† Const. means the constant term $E(0,0)$.

** $\#E_1(F_p) \sim \#E_6(F_p)$ are tabulated. * prime order.

Table 2: $\#E_1(F_{p^3})$, $\#E_1(F_{p^9})$, two solutions of $f_1^{[3]}(t)/(t-t_1^{[3]})$, six orders over F_{p^3}

p	$\#E_1(F_{p^3})$	$\#E_1(F_{p^9})$	$f_1^{[3]}(t)/(t-t_1^{[3]})$	Solutions t_c, t_d	Orders**
7	364	40341028	$t^2-20t-629$	$37, -17$	364
					327
					307^*
					324
					361
					381
13	2128	10604617744	$t^2+70t-1691$	$19, -89$	2128
					2109
					2179^*
					2268
					2287^*
					2217
19	6916	322686721084	$t^2-56t-17441$	$163, -107$	6916
					6753
					6697
					6804
					6967^*
					7023

** $\#E_1(F_{p^3})$, $\#E_4(F_{p^3})$, and $\#E_7(F_{p^3}) \sim \#E_{10}(F_{p^3})$ are tabulated. * prime order.

Appendix

A. $E(x, y) = y^2 - x^3 - b,\ b \in F_p^*$ is not super-singular

As shown in Appendix.B, the order $\#E(F_q)$ of the curve Eq.(9) is written as

$$\#E(F_q) = 3N + 1 \ \mathit{or}\ 3N + 2 + 1, \qquad (46)$$

where N is a certain number. In other words, $\#E(F_q) \not\equiv 2 \pmod 3$. Therefore, noting that 3 divides $q-1$, it is shown that the trace $t = q+1-\#E(F_q)$ is not equal to 0. When q is an odd prime number p, the elliptic curve $E(F_p)$ is not super-singular if and only if its trace t is not equal to 0. Consequently, it is shown that $E(F_p)$ defined by $E(x, y) = y^2 - x^3 - b,\ b \in F_p^*$ is not super-singular.

B. The orders of y-twisted curves

If $E(0, y)$ is irreducible over F_{q^m}, $E'(0, y)$ and $E''(0, y)$ are also irreducible. On the other hand, if $E(0, y)$ is reducible over F_{q^m}, $E'(0, y)$ and $E''(0, y)$ are also reducible, in addition each $E(0, y)$, $E'(0, y)$, and $E''(0, y)$ has two distinct zeros in F_{q^m} because $b \neq 0$ and the characteristic p is larger than 3 in this paper.[4].

When $E(0, y)$ is irreducible over F_{q^m}, we have the following rational points ;

- For $i \in F_{q^m}$ such that $E(0, i)$ is a TR in F_{q^m},

  $x^3 = E(0, i)$ generates three rational points on the curve.

- For $i \in F_{q^m}$ such that $E(0, i)$ is a TNR in F_{q^m},

  $x^3 = E(0, i)$ generates no rational points on the curve.

Therefore, when $E(0, y)$ is irreducible, the orders are written as Eqs.(12). On the other hand, when $E(0, y)$ is reducible, we have the following rational points;

- For $i \in F_{q^m}$ such that $E(0, i)$ is not equal to 0 and a TR in F_{q^m},

  $x^3 = E(0, i)$ generates three rational points on the curve.

- For $i \in F_{q^m}$ such that $E(0, i)$ is not equal to 0 and a TNR in F_{q^m},

  $x^3 = E(0, i)$ generates no rational points.

- For $i \in F_{q^m}$ such that $E(0, i)$ is equal to 0,

  $x^3 = E(0, i)$ generates one rational point $(x, y) = (0, i)$.

Therefore, when $E(0, y)$ is reducible, noting that $E(0, y)$ has two distinct zeros in F_{q^m}, the orders are written as Eqs.(13).

Let N be the number of i's such that $E(0, i), i \in F_{q^m}$ is a non-zero TR in F_{q^m}, let N' and N'' be the numbers of i's such that $E(0, i), i \in F_{q^m}$ is a TypeI and a TypeII TNR in F_{q^m}, respectively. The notations **TypeI and TypeII TNR** are defined in Appendix.E. First, we consider $E(x, y)$, $E'(x, y)$, and $E''(x, y)$ as

$$\begin{aligned} E(x, y) &: \ x^3 = E(0, y), & (47a)\\ E'(x, y) &: \ x^3 = B^2 E(0, B^{-1}y), & (47b)\\ E''(x, y) &: \ x^3 = B^4 E(0, B^{-2}y). & (47c) \end{aligned}$$

We can easily understand that the following three curves has the same order;

$$\begin{aligned} x^3 &= E(0, y), & (48a)\\ x^3 &= E(0, B^{-1}y), & (48b)\\ x^3 &= E(0, B^{-2}y), & (48c) \end{aligned}$$

because $y = B^{-1}y$ and $y = B^{-2}y$ are isomorphic variable transformations. In other words, the following relation holds ;

$$\begin{aligned} \{E(0, i), \forall i \in F_{q^m}\} &= \{E(0, B^{-1}i), \forall i \in F_{q^m}\}\\ &= \{E(0, B^{-2}i), \forall i \in F_{q^m}\}. \quad (49) \end{aligned}$$

Therefore, if B is a TR in F_{q^m}, by multiplying B^2 and B^4 as shown in Eqs.(47), TRs in $\{E(0, i), \forall i \in F_{q^m}\}$ become TRs in F_{q^m} and TNRs in $\{E(0, i), \forall i \in F_{q^m}\}$ become TNRs in F_{q^m} again. Consequently, we have the relation Eq.(15).

When B^2 is a TypeII TNR in F_{q^m} and $E(0, y)$ is irreducible over F_{q^m}, for example, by multiplying B^2 as shown in Eq.(47b) and Fig.4-(b), we find

- N non-zero TRs in $\{E(0, i), \forall i \in F_{q^m}\}$ become N TypeII TNRs in F_{q^m},
- N' TypeI TNRs in $\{E(0, i), \forall i \in F_{q^m}\}$ become N' non-zero TRs in F_{q^m},
- N'' TypeII TNRs in $\{E(0, i), \forall i \in F_{q^m}\}$ become N'' TypeI TNRs in F_{q^m}.

In the same, by multiplying B^4 as shown in Eq.(47c) and Fig.4 (c), we find

- N non-zero TRs in $\{E(0, i), \forall i \in F_{q^m}\}$ become N TypeI TNRs in F_{q^m},
- N' TypeI TNRs in $\{E(0, i), \forall i \in F_{q^m}\}$ become N' TypeII TNRs in F_{q^m},

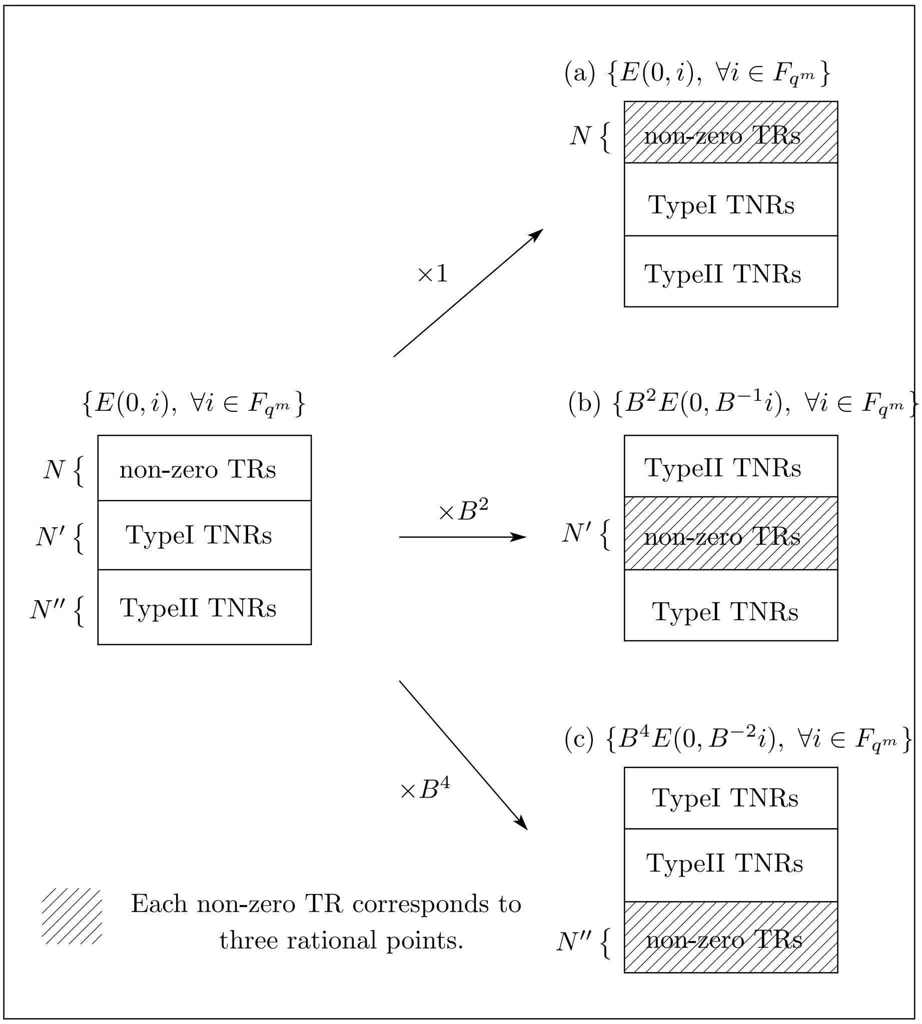

Figure 4: The relation among N, N', and N'' when B^2 is a TypeII TNR in F_{q^m}

- N'' TypeII TNRs in $\{E(0,i), \forall i \in F_{q^m}\}$ become N'' non-zero TRs in F_{q^m},

where in this case we should note that B^4 becomes a TypeI TNR in F_{q^m}. Consequently, we have the relation Eq.(16). Fig.4 shows an image of these relations. On the other hand, when B^2 is a TNR in F_{q^m} and $E(0,y)$ is reducible over F_{q^m}, $B^2E(0,i)$ and $B^4E(0,i)$ also become 0 for $i \in F_q^m$ such that $E(0,i)=0$. Therefore, noting that $E(0,y)$ has two distinct zeros in F_{q^m}, we have Eq.(17).

C. Eqs.(12), Eqs.(13), Eqs.(14), and Eq.(15)∼Eq.(17) for x-twist

Let us consider the defining equations Eqs.(10). Corresponding to whether $E(x,0)$ is irreducible or reducible over F_{q^m}, the orders $\#E(F_{q^m})$ and $\#\tilde{E}(F_{q^m})$ of $E(x,y)$ and $\tilde{E}(x,y)$ over F_{q^m} becomes as follows ;

when $E(x,0)$ is irreducible over F_{q^m},

$$\#E(F_{q^m}) = 2M+1, \tag{50a}$$
$$\#\tilde{E}(F_{q^m}) = 2\tilde{M}+1. \tag{50b}$$

when $E(x,0)$ is reducible over F_{q^m},

$$\#E(F_{q^m}) = \begin{cases} 2M+1+1 \\ 2M+3+1 \end{cases}$$
$$\text{when } \begin{cases} E(x,0) \text{ has one zero in } F_{q^m} \\ E(x,0) \text{ has three zeros in } F_{q^m} \end{cases}, \tag{51a}$$

$$\#\tilde{E}(F_{q^m}) = \begin{cases} 2\tilde{M}+1+1 \\ 2\tilde{M}+3+1 \end{cases}$$
$$\text{when } \begin{cases} E(x,0) \text{ has one zero in } F_{q^m} \\ E(x,0) \text{ has three zeros in } F_{q^m} \end{cases}. \tag{51b}$$

M and $\tilde{M}$ are the numbers of non-zero QRs in the following sets, respectively;

$$\{E(i,0),\ \forall i \in F_{q^m}\} \quad (52a)$$
$$\text{and} \quad \left\{\tilde{E}(i,0),\ \forall i \in F_{q^m}\right\}. \quad (52b)$$

Moreover, corresponding to whether A is a QR or a QNR in F_{q^m}, the following relation holds for M and $\tilde{M}$;

when A is a QR in F_{q^m},

$$M = \tilde{M}, \quad (53)$$

when A is a QNR in F_{q^m} and $E(x,0)$ is irreducible,

$$M + \tilde{M} = q^m, \quad (54)$$

when A is a QNR in F_{q^m} and $E(x,0)$ is reducible,

$$\begin{cases} M + \tilde{M} + 1 = q^m \\ M + \tilde{M} + 3 = q^m \end{cases}$$
$$\text{when} \begin{cases} E(x,0) \text{ has one zero in } F_{q^m} \\ E(x,0) \text{ has three zeros in } F_{q^m} \end{cases}. \quad (55)$$

In this case, we should note that $E(x,0)$ does not have any duplicated zeros because of ECC implementation. Most of these properties are well-known[1].

D. Six distinct orders

From Eqs.(12), Eqs.(13), Eqs.(14), and Fig.1, we can easily find that the six orders $\#E_1(F_q) \sim \#E_6(F_q)$ are distinct when $\#E_1(F_q)$, $\#E_3(F_q)$, and $\#E_5(F_q)$ are distinct. In this section, we show that $\#E_1(F_q)$, $\#E_3(F_q)$, and $\#E_5(F_q)$ are distinct when q is an odd power of a prime number p.

If two of three orders $\#E_1(F_q)$, $\#E_3(F_q)$, and $\#E_5(F_q)$ are same, two of three traces t_1, t_3, and t_5 are same. It means that $f_1(t)$ defined by Eq.(27a) has duplicate solutions. We can easily check it by whether or not the discriminant $D(f_1)$ of $f_1(t)$ is equal to 0, where $D(f_1)$ is given by

$$D(f_1) = -108q^3 + 27\left(-t_1^{[3]}\right)^2. \quad (56)$$

Therefore, noting that $t_1^{[3]} = q^3 + 1 - \#E_1(F_{q^3})$, we have

$$-4q^3 + (t_1^{[3]})^2 = 0. \quad (57)$$

For the above equation, there are no solutions with respect to $t_1^{[3]}$ if q is an odd power of a prime number p, where p is the characteristic. Consequently, in this case, the six curves $E_1(x,y) \sim E_6(x,y)$ have distinct orders.

If Eq.(57) is satisfied, it is possible for the six orders not to be distinct. Moreover, in this case, since the trace $t_1^{[3]}$ of the curve $E_1(F_{q^3})$ is divisible by the characteristic, some of the six curves $E_1(F_{q^3})$, $E_4(F_{q^3})$, $E_7(F_{q^3}) \sim E_{10}(F_{q^3})$ are super-singular.

E. A TNR in F_q becomes a TR in F_{q^3}

When 3 divides $q-1$, non-zero TRs and TNRs in F_q are given as follows ;

$$\text{non-zero TRs} : \left\{g^{3j},\ j = 0,1,2,\cdots,(q-4)/3\right\}, \quad (58a)$$
$$\text{TypeI TNRs} : \left\{g^{3k+1},\ k = 0,1,2,\cdots,(q-4)/3\right\}, \quad (58b)$$
$$\text{TypeII TNRs} : \left\{g^{3l+2},\ l = 0,1,2,\cdots,(q-4)/3\right\}, \quad (58c)$$

where g is a generator of F_q^*. These notations are also used in Appendix.A.

Let us consider a TNR x in F_q. We can check whether x is a TR or a TNR in F_{q^3} by calculating $x^{(q^3-1)/3}$, the calculation result becomes as follows ;

$$x^{(q^3-1)/3} = \left(x^{q-1}\right)^{(q^2+q+1)/3} = 1, \quad (59)$$

where we note that $x^{(q-1)} = 1$ and $(q^3-1)/(q-1) = q^2+q+1$ is divisible by 3[4]. Consequently, it is shown that a TNR in F_q becomes a TR in F_{q^3}.

F. Proof of Eqs.(31) and Eqs.(32)

First, since Eq.(27a) has t_1, t_3, and t_5 as its solutions, we have

$$t_1 + t_3 + t_5 = 0, \quad (60a)$$
$$t_1t_3 + t_1t_5 + t_3t_5 = -3q, \quad (60b)$$
$$t_1t_3t_5 = q^3 + 1 - \#E_1(F_{q^3}). \quad (60c)$$

From Weil's theorem, we have

$$t_1^{[3]} = -q^3 - 1 + \#E_1(F_{q^3}), \quad (61)$$

therefore, we obtain Eqs.(32b) from Eq.(60c). In the same way, we can show Eq.(32a).

Next, let us consider the following product;

$$\begin{aligned} &\#E_1(F_q)\#E_3(F_q)\#E_5(F_q) \\ = &\ (q+1-t_1)(q+1-t_3)(q+1-t_5). \end{aligned} \quad (62)$$

By using Eqs.(60), we can develop the right-hand side of the above equation as

$$= \quad (q+1)^3 - (t_1+t_3+t_5)(q+1)^2 +$$

$$\begin{aligned} & (t_1t_3 + t_1t_5 + t_3t_5)(q+1) - t_1t_3t_5 \\ = \; & (q+1)^3 - 3q(q+1) - q^3 - 1 + \#E_1(F_{q^3}) \\ = \; & \#E_1(F_{q^3}). \end{aligned} \quad (63)$$

Consequently, we have Eq.(31a). In the same way, we can show Eq.(31b).