社団法人 情報処理学会 研究報告
IPSJ SIG Technical Reports

2005－ＣＳＥＣ－30（９）
2005／7／21

yツイストを用いた素数位数楕円曲線生成法の性能評価

小原真由美† 野上保之† 森川良孝†

† 岡山大学大学院自然科学研究科

あらまし 本稿では，変数yに関するツイスト方法を議論し，その観点から，とくに$y^2 = x^3 + a$のような形の楕円曲線が素数位数をもつための幾つかの必要条件を示す．そして，従来のツイスト手法を組み合わせることにより，6個の楕円曲線を考え，定義体の標数pが$p > 3, 3 \mid (p-1)$を満たすとき，その6曲線のうち2曲線のみが素数位数に成りうることを示し，その場合の定義体の拡大次数は2^i3^jでなければならないことを示す．その後，1つの素数位数楕円曲線を生成するのにかかる計算時間について，虚数乗法を用いた場合と比較し性能を評価する．

キーワード 楕円曲線，ツイスト，平方剰余/非剰余，3乗剰余/非剰余

Performance of Prime Order Elliptic Curve Generation based on y-twist

Mayumi OBARA†, Yasuyuki NOGAMI†, and Yoshitaka MORIKAWA†

† The graduate school of natural science and technology, Okayama University

Abstract This paper proposes a new twist technique and then shows some necessary conditions for prime order curves in the form $y^2 = x^3 + a$. Then, by combining x-twist and y-twist, we consider six elliptic curves. For these six elliptic curves, when the characteristic p of the definition field F_q satisfies that $p > 3$ and $3 \mid (p-1)$, we show that it is possible for only two elliptic curves among the six curves defined over F_q, $q = p^{2^i3^j}$ to have prime orders, where i, j are non-negative integers. Then, we show an example of prime order curve. After that, compared to the complex multiplication method, we evaluate the performance of the proposed method.

Key words elliptic curve, twist, quadratic residue/non-residue, 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 elliptic curve;

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

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

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

as $\#\tilde{E}(F_q) = 2q + 2 - \#E(F_q)$, where A is a quadratic power non residue in the definition field F_q. For the order $\#\tilde{E}(F_q)$, we do not need another order counting computation. Our motivation comes from this technique that effectively uses a quadratic power non-residue, this paper proposes a new twist technique that is closely related to complex multiplication method and then shows some necessary conditions for prime order curves in the form Eq.(2a).

This paper particularly deals with elliptic curves in the form

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

In this paper, we refer to the previously introduced twist technique Eqs.(1) as x-twist and we propose y-twist as follows;

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

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

where B is an element in F_q^*. First, we show some properties of the order of y-twisted elliptic curve corresponding to whether or not B is a third power residue in the definition field F_q. Then, by combining x-twist and y-twist, we can consider six elliptic curves. For the orders of these six elliptic curves, a lot of considerations have been already given from several theoretical viewpoints such as complex multiplication [3]. In this paper, when the characteristic p of the definition field F_q satisfies that $p > 3$ and $3 \mid (p-1)$, from the viewpoints of x-twist and y-twist, we show that it is possible for only two elliptic curves among the six curves defined over F_q, $q = p^{2^i 3^j}$ to have prime orders, where i, j are non-negative integers. Then, we show an example of prime order curve.

Throughout this paper, $q = p^m$ and p is the characteristic. F_q and F_{q^n} mean a finite field and its n-th extension field, respectively, where m and n are positive integers. F_q^* and $F_{q^n}^*$ mean their multiplicative group, respectively.

2. Fundamentals of elliptic curve

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

2.1 Power residue and non residue in finite field

For two elements α, β in finite field F_q, if the relation $\alpha = \beta^2$ holds, it is said that α is a quadratic power residue(QR) in F_q, otherwise it is said that α is a quadratic power non residue(QNR) in F_q. In the same, if $\alpha = \beta^3$ holds, it is said that α is a third power residue(TR) in F_q, otherwise it is said that α is a third power non residue(TNR) in F_q. In this paper, if α is a QR and a TR in F_q, we say that α is a sixth power residue(SR) in F_q; however, if α is a QNR and a TNR in F_q, we especially say that α is a quadratic power and third power non residue in F_q and we use **QTNR** as its abbreviation.

2.2 Coefficient field and definition field

In this paper, we particularly deal with the following elliptic curves;

$$E(x,y) = \begin{cases} x^3 + b + y^2 + y = 0 & \text{when } p = 2 \\ x^3 + b - y^2 = 0 & \text{when } p \geqq 3 \end{cases}, \quad (3)$$

where $b \in F_q^*$ and p is the characteristic of F_q. In other words, $E(x,y)$ in this paper has only the third-degree term x^3 with respect to the variable x. 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^n} as the coefficient and definition field, when $n = 1$, it means that these fields are same.

2.3 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^n}, respectively, the order $\#E(F_{q^n})$ 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^n}, respectively. Let $t = q + 1 - \#E(F_q)$ be the trace of $E(F_q)$, then we have

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

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

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 $\#E(F_{q^n})$ 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^n}, respectively, the order is given by Eq.(4). By using the base trace t, that is $t = q + 1 - \#E(F_q)$, $t^{[n]}$ shown in Eq.(4) is given by

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

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

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

2.4 Conventional twist

2.4.1 when $p = 2$

For an original defining equation $E(x,y)$ as shown in Eq.(3), the following $\phi_k E(x,y)$ is called the *twist* or *twisted curve* of E;

$$\phi_k E(x,y) = x^3 + b + kA + y^2 + y = 0, \quad k = 0, 1, \quad (7)$$

where A is a non-zero element in the definition field F_q. When $k = 1$, corresponding to whether $\mathrm{Tr}(A)$ is zero or one,

where $\mathrm{Tr}(x) = x + x^p + \cdots x^{p^{n-1}}$, the order $\#\phi_1 E(F_q)$ of the twisted elliptic curve $\phi_1 E(x,y)$ becomes as follows;

$$\#\phi_1 E(F_q) = \begin{cases} q+1-t_{\phi_0} & \text{when } \mathrm{Tr}(A)=0 \\ q+1+t_{\phi_0} & \text{when } \mathrm{Tr}(A)=1 \end{cases}, \quad (8)$$

where $t_{\phi_0} = q+1-\#\phi_0 E(F_q)$.

In what follows, we refer to this *twist* operation Eq.(7) as *additive twist*.

2.4.2 when $p \geqq 3$

In this case, the following $\phi_k E(x,y)$ is the twisted curve;

$$\begin{aligned} \phi_k E(x,y) &= A^{3k} E(A^{-k}x, 0) - y^2 \\ &= x^3 + A^{3k}b - y^2 = 0, \quad k = 0,1, \end{aligned} \quad (9)$$

where A is a non-zero element in the definition field F_q. When $k=1$, corresponding to whether A is a QR or QNR, the order $\#\phi_1 E(F_q)$ becomes as follows;

$$\#\phi_1 E(F_q) = \begin{cases} q+1-t_{\phi_0} & \text{when } A \text{ is a QR} \\ q+1+t_{\phi_0} & \text{when } A \text{ is a QNR} \end{cases}, (10)$$

where $t_{\phi_0} = q+1-\#\phi_0 E(F_q)$.

In what follows, we refer to this *twist* operation Eq.(9) as *x-twist*.

3. *y*-twist for elliptic curves in the form Eq.(3)

In this section, let the extension degree n be 1, in other words, both the coefficient and definition field are F_q.

3.1 *y*-twist

For an original defining equation $E(x,y)$ defined as Eq.(3), we consider the following elliptic curve $\psi_l E(x,y)$, $l = 0,1,2$;

$$\begin{aligned} \psi_l E(x,y) &= x^3 + B^{2l} E(0, B^{-l} y) \\ &= \begin{cases} x^3 + B^{2l}b + y^2 + B^l y & (p=2) \\ x^3 + B^{2l}b - y^2 & (p \geqq 3) \end{cases}, \end{aligned} \quad (11)$$

where B is a non-zero element in the definition field F_q. In what follows, we particularly deal with the case that $q-1$ is divisible by 3 and the other cases such as $p=3$ are shown in **Sec.**4.. When 3 divides $q-1$, corresponding to whether $E(0,y)$ is irreducible or reducible over the definition field F_q, the orders $\#\psi_0 E(F_q)$, $\#\psi_1 E(F_q)$, and $\#\psi_2 E(F_q)$ of $\psi_0 E(x,y)$, $\psi_1 E(x,y)$, and $\psi_2 E(x,y)$ over F_q are written as follows;

when $E(0,y)$ is irreducible over F_q,

$$\#\psi_0 E(F_q) = 3N_{\psi_0} + 1, \quad (12a)$$

$$\#\psi_1 E(F_q) = 3N_{\psi_1} + 1, \quad (12b)$$

$$\#\psi_2 E(F_q) = 3N_{\psi_2} + 1, \quad (12c)$$

when $E(0,y)$ is reducible over F_q,

$$\#\psi_0 E(F_q) = 3N_{\psi_0} + 2 + 1, \quad (13a)$$

$$\#\psi_1 E(F_q) = 3N_{\psi_1} + 2 + 1, \quad (13b)$$

$$\#\psi_2 E(F_q) = 3N_{\psi_2} + 2 + 1. \quad (13c)$$

N_{ψ_0}, N_{ψ_1}, and N_{ψ_2} shown in the above equations are the numbers of non-zero TRs in the following sets, respectively;

$$\{\psi_0 E(0,i),\ \forall i \in F_q\}, \quad (14a)$$

$$\{\psi_1 E(0,i),\ \forall i \in F_q\}, \quad (14b)$$

$$\text{and } \{\psi_2 E(0,i),\ \forall i \in F_q\}. \quad (14c)$$

In addition, corresponding to whether B is a TR or TNR in F_q, the following relation holds for N_{ψ_0}, N_{ψ_1}, and N_{ψ_2};

when B is a TR in F_q,

$$N_{\psi_0} = N_{\psi_1} = N_{\psi_2}, \quad (15)$$

when B is a TNR in F_q and $E(0,y)$ is irreducible,

$$N_{\psi_0} + N_{\psi_1} + N_{\psi_2} = q, \quad (16)$$

when B is a TNR in F_q and $E(0,y)$ is reducible,

$$N_{\psi_0} + N_{\psi_1} + N_{\psi_2} + 2 = q. \quad (17)$$

The proofs for these relations are shown in Appendix.A. In what follows, we refer to the operation Eq.(11) as *y-twist*. From the above viewpoint, we can also consider additive twist and *x*-twist. In the case that 3 does not divide $q-1$, the orders are uniquely determined [3].

3.2 The orders of *y*-twisted curves

In this section, we consider *y*-twist as shown in Eq.(11) that uses a TNR B in F_q. From Weil's theorem and Eq.(6), we have the following relations;

$$\#\psi_l E(F_q) \mid \#\psi_l E(F_{q^3}), \quad l = 0,1,2. \quad (18)$$

Since a TNR in F_q becomes a TR in F_{q^3} (*see* Appendix.B), the TNR B 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.**3.1 and as shown in Eq.(15), we have

$$\#\psi_0 E(F_{q^3}) = \#\psi_1 E(F_{q^3}) = \#\psi_2 E(F_{q^3}), \quad (19)$$

accordingly we have

$$\#\psi_l E(F_q) \mid \#\psi_0 E(F_{q^3}), \quad l = 0,1,2. \quad (20)$$

Fig.1 is an image of this relation. Let t_{ψ_0}, t_{ψ_1}, and t_{ψ_2} be the traces of elliptic curves $\psi_0 E(F_q)$, $\psi_1 E(F_q)$, and $\psi_2 E(F_q)$, respectively, as follows;

$$t_{\psi_0} = q+1-\#\psi_0 E(F_q), \tag{21}$$
$$t_{\psi_1} = q+1-\#\psi_1 E(F_q), \tag{22}$$
$$t_{\psi_2} = q+1-\#\psi_2 E(F_q). \tag{23}$$

From Weil's theorem and Eq.(5), we have

$$\begin{aligned}\#\psi_0 E(F_{q^3}) &= q^3+1-(t_{\psi_0}^3-3qt_{\psi_0}) &(24a)\\ &= q^3+1-(t_{\psi_1}^3-3qt_{\psi_1}) &(24b)\\ &= q^3+1-(t_{\psi_2}^3-3qt_{\psi_2}). &(24c)\end{aligned}$$

Noting that these traces $t_{\psi_0}, t_{\psi_1}, t_{\psi_2}$ are not equal to 0 (*cf.* Appendix.E), from Eqs.(24) we find that the following $f(t)=0$ has solutions $t = t_{\psi_0}, t_{\psi_1}, t_{\psi_2}$;

$$\begin{aligned}f(t) &= t^3-3qt-q^3-1+\#\psi_0 E(F_{q^3})\\ &= t^3-3qt-(t_{\psi_0}^3-3qt_{\psi_0}).\end{aligned} \tag{25}$$

These solutions t_{ψ_0}, t_{ψ_1}, and t_{ψ_2} are easily computed by Cornacchia's algorithm (*see* **Sec.4.**, **Sec.4. 2**). We can also show the following relations;

$$\#\psi_0 E(F_{q^3}) = \#\psi_0 E(F_q)\#\psi_1 E(F_q)\#\psi_2 E(F_q), \tag{26}$$
$$t_{\psi_0}^{[3]} = t_{\psi_0} t_{\psi_1} t_{\psi_2}. \tag{27}$$

4. Prime order elliptic curves in the form Eq.(3)

In what follows, we particularly consider the case that the characteristic $p>3$ and $3 \mid (p-1)$. By combining x-twist and y-twist, we can consider six varieties of elliptic curves in the form Eq.(3) as follows;

Let b_p be a non-zero element in the prime field F_p. By using a QTNR C in the definition field F_q, we can consider the following six curves;

$$E_{00}(x,y) = x^3+b_p-y^2=0, \tag{28a}$$
$$E_{01}(x,y) = x^3+C^2b_p-y^2=0, \tag{28b}$$
$$E_{02}(x,y) = x^3+C^4b_p-y^2=0, \tag{28c}$$
$$E_{10}(x,y) = x^3+C^3b_p-y^2=0, \tag{28d}$$
$$E_{11}(x,y) = x^3+C^5b_p-y^2=0, \tag{28e}$$
$$E_{12}(x,y) = x^3+Cb_p-y^2=0. \tag{28f}$$

For these six elliptic curves $E_{00},\cdots,E_{12}$, the following relations hold from the viewpoints of additive twist(x-twist) ϕ_0,ϕ_1 and y-twist ψ_0,ψ_1,ψ_2;

$$E_{00} = E_{00}, \tag{29a}$$
$$E_{01} = \psi_1 E_{00}, \tag{29b}$$
$$E_{02} = \psi_2 E_{00}, \tag{29c}$$
$$E_{10} = \phi_1 E_{00}, \tag{29d}$$
$$E_{11} = \psi_1 E_{10} = \phi_1 E_{01} = \phi_1(\psi_1 E_{00}), \tag{29e}$$
$$E_{12} = \psi_2 E_{10} = \phi_1 E_{02} = \phi_1(\psi_2 E_{00}). \tag{29f}$$

Therefore, the five curves $E_{01},\cdots,E_{12}$ are given from E_{00} by combining additive twist(x-twist) and y-twist operations. **Fig.**2 shows an image of these relations.

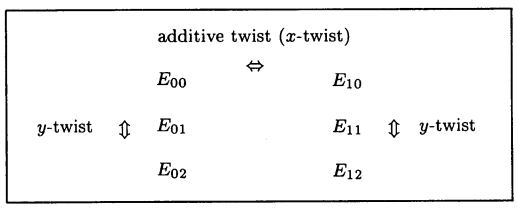

Figure 2 additive twist(x-twist) and y-twist relations among the six curves

Accordingly, there are six varieties of orders as follows;

$$\#E_{00}(F_q) = q+1-t_{00}, \tag{30a}$$
$$\#E_{01}(F_q) = q+1-t_{01}, \tag{30b}$$
$$\#E_{02}(F_q) = q+1-t_{02}, \tag{30c}$$
$$\#E_{10}(F_q) = q+1-t_{10} = q+1+t_{00}, \tag{30d}$$
$$\#E_{11}(F_q) = q+1-t_{11} = q+1+t_{01}, \tag{30e}$$
$$\#E_{12}(F_q) = q+1-t_{12} = q+1+t_{02}, \tag{30f}$$

where $t_{00},\cdots,t_{12}$ are the traces of $E_{00}(F_q),\cdots,E_{12}(F_q)$, respectively. The right hand sides of Eq.(30d), Eq.(30e), and Eq.(30f) are given from the viewpoint of additive twist(x-twist). Therefore, if we know one of the orders $\#E_{00}(F_q),\cdots,\#E_{12}(F_q)$ or one of the traces $t_{00},\cdots,t_{12}$. We can also show that $t_{00},\cdots,t_{12}$ are different to each other when $3 \mid (p-1)$.

4.1 Prime order curves

In this section, let q be equal to p^m, we show that it is possible for only two elliptic curves among the six curves defined over F_q, $q=p^{2^i3^j}$ to have prime orders, where i,j are non-negative integers. We note that the constant term $b_p = E_{00}(0,0)$ is a non-zero element in the prime field F_p.

In this case, if we know the base trace t_B or the base order $\#E_{00}(F_p)$ as

$$t_B = p+1-\#E_{00}(F_p), \tag{31}$$

from Weil's theorem and Eq.(5), we obtain $\#E_{00}(F_q)$ as

$$\begin{aligned}\#E_{00}(F_q) &= q+1-t_{00},\ t_{00}\\ &= \sum_{i=0}^{\lfloor m/2\rfloor}\frac{m}{m-i}{}_{m-i}C_i(-p)^i {t_B}^{m-2i}.\end{aligned} \tag{32}$$

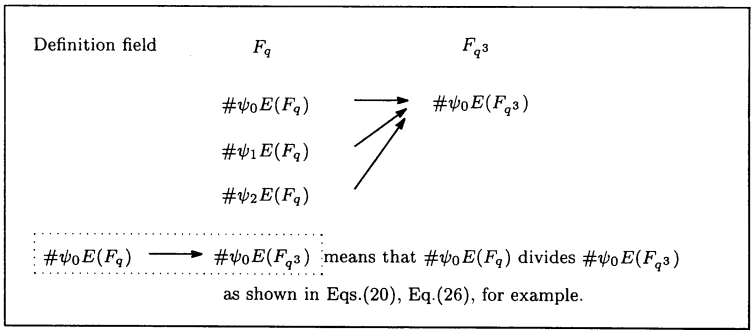

Figure 1 Order relations among six curves over F_{q^3}

For this problem, we can obtain the base trace t_B by computing the base order $\#E_{00}(F_p)$; however, as shown in Sec.4. 2, we can easily compute t_B by Cornacchia's algorithm, accordingly we can calculate the six traces $t_{00}, \cdots, t_{12}$ by Eq.(32). By using $\#E_{00}(F_q)$ or t_{00}, from the viewpoints of x-twist and y-twist we can determine the other orders $\#E_{01}(F_q), \cdots, \#E_{12}(F_q)$ as follows;

Let us prepare the six elliptic curves Eqs.(28) with a SR $b_p \in F_p^*$ such that $b_p^{(p-1)/6} \equiv 1 \bmod p$. In this case, since $E_{00}(x,0)$ and $E_{00}(0,y)$ are reducible over F_q [4], $\#E_{00}(F_q)$ is divisible by 6. On the other hand, the other five orders are not divisible by 6. **Table** 1 shows the irreducibility of $E_{kl}(x,0)$, that of $E_{kl}(0,y)$, and whether or not $\#E_{kl}(F_q)$ is divisible by 2 or 3, where $k = 0,1$ and $l = 0,1,2$. According to **Table** 1, we can find that it is possible for only two curves $E_{11}(F_q)$ and $E_{12}(F_q)$ to have prime orders. In addition, if the extension degree m has a factor $m' \neq 2$ or 3, we can find a QTNR C in $F_{p^{m/m'}}$ [4], where $F_{p^{m/m'}}$ is a proper subfield in F_{p^m}, accodingly from Weil's theorem we have

$$\begin{aligned} &\#E_{11}(F_{p^{m/m'}}) \mid \#E_{11}(F_{p^m}), \\ &\#E_{12}(F_{p^{m/m'}}) \mid \#E_{12}(F_{p^m}). \end{aligned} \tag{33}$$

Therefore, it is obvious that both $E_{11}(F_q)$ and $E_{12}(F_q)$ are not prime numbers. Otherwise, we cannot find a QTNR C in any a proper subfields [4], accordingly we cannot deduce such a relation and it is possible for two curves $E_{11}(F_q)$ and $E_{12}(F_q)$ to have prime orders. In other words, it is necessary for prime order curves in the form Eq.(3) to be defined over $F_{p^{2^i 3^j}}$, where i and j are non-negative integers.

4. 2 How to compute the base trace t_B

In this section, let the coefficient and definition fields be the prime field F_p, of course we consider a QTNR C in F_p, and let us consider three elliptic curves $E_{00}(F_p)$, $E_{01}(F_p)$, and $E_{02}(F_p)$ as shown in Eqs.(28). From the viewpoint of y-twist, their traces t_{00}, t_{01}, and t_{02} are the solutions of the following equation;

$$\begin{aligned} f(t) &= t^3 - 3pt - (t_{00}^3 - 3pt_{00}) && \text{(34a)} \\ &= t^3 - 3pt - (t_{01}^3 - 3pt_{01}) && \text{(34b)} \\ &= t^3 - 3pt - (t_{02}^3 - 3pt_{02}). && \text{(34c)} \end{aligned}$$

We can also say that t_{01} and t_{02} are the solutions of the following equation;

$$f'(t) = f(t)/(t - t_{00}) = t^2 - t_{00}t + (t_{00}^2 - 3p). \tag{35}$$

Therefore, denoting the discriminant of $f'(t)$ by $D(f')$, since the equation $f'(t) = 0$ has two integer solutions, $D(f')$ should be written as

$$D(f') = 3(4p - t_{00}^2) = X^2, \ X \in Z, \tag{36}$$

to be more detailed with $X = 3X'$,

$$4p - t_{00}^2 = 3X'^2, \ X' \in Z. \tag{37}$$

Eq.(37) is given by using t_{00}; however, we can consider the same equations by using the other traces such as t_{01}, consequently $t_{00}, \cdots, t_{12}$ must satisfy

$$4p = t^2 + 3s^2, \ s \in Z. \tag{38}$$

In addition, we can easily compute t that satisfies Eq.(38) by Cornacchia's algorithm [1], accordingly we can calculate the six solutions $t_{00}, \cdots, t_{12}$ by Eq.(25) and Eqs.(30). In this case, $t_B = t_{00}$, therefore, from the six candidates we can distinguish t_B by checking whether or not $p+1-t_B$ is divisible by 6. Our proposal, that is y-twist, is closely related to the well-known complex multiplication; however, our proposal is not so complicated as compared to the complex multiplication, therefore, we can easily extend y-twist for hyper elliptic curves in the form $y^2 = x^5 + a$, $a \in F_q$ by using 5-th power residue/non-residue.

4. 3 An example of prime order curve

Let the characteristic p be a prime number 1073831833 and let the definition field be the third extension field F_{p^3}. In this case, we have the following prime order curve;

$$E(x,y) = x^3 + \theta - y^2 = 0, \ \theta \in F_{p^3}, \tag{39a}$$

Table 1 Irreducibility and divisibility

	$E_{kl}(x,y)^{\dagger}$	$E_{kl}(x,0)^{*}$	$E_{kl}(0,y)^{*}$	divisible by	not divisible by
E_{00}	$x^3+b_p-y^2$	○	○	6	–
E_{01}	$x^3+C^2b_p-y^2$	×	○	3	2
E_{02}	$x^3+C^4b_p-y^2$	×	○	3	2
E_{10}	$x^3+C^3b_p-y^2$	○	×	2	3
E_{11}	$x^3+C^5b_p-y^2$	×	×	–	6
E_{12}	$x^3+Cb_p-y^2$	×	×	–	6

$^{\dagger}b_p$ is a SR in F_p and C is a QTNR in F_q. $k=0,1$ and $l=0,1,2$.

*○ and × mean reducible and irreducible over F_p, respectively.

$$\#E(F_{p^3}) = 12382513853184433328952823 39 \quad (39b)$$

(93bits prime number),

where $\theta=\omega+2\omega^p+5\omega^{p^2}$. $\{\omega,\omega^p,\omega^{p^2}\}$ is a normal basis in F_{p^3} and ω satisfies

$$\omega=\tau+\tau^{-1}, \quad (40)$$

where τ is a zero of $f(x)=x^6+x^5+x^4+x^3+x^2+x+1$ and $f(x)$ is an irreducible polynomial of degree 6 over F_p.

Table 2 shows the average computation times needed for generating a prime order elliptic curve by using complex multiplication-based algorithm, y-twist over F_p, and y-twist over F_{p^3}. The authors used Pentium4(3GHz), C language, and the library for doing number theory(NTL). From the table, we find that the proposed method is enough practical.

5. Conclusion

This paper has particularly dealt with elliptic curves in the form

$$E(x,y)=x^3+b-y^2=0,\ b\in F_q^*. \quad (41a)$$

In this paper, we referred to the conventional twist technique as x-twist(additive twist) and we proposed y-twist as follows;

$$E'(x,y) = x^3+bB^2-y^2=0, \quad (41b)$$

$$E''(x,y) = x^3+bB^4-y^2=0, \quad (41c)$$

where B is an element in F_q^*. First, we showed some properties of the order of y-twisted elliptic curve corresponding to whether or not B was a third power residue in the definition field F_q. Then, by combining x-twist and y-twist, we considered six elliptic curves and we showed that it is possible for only two elliptic curves among the six curves defined over F_q, $q=p^{2^i3^j}$ to have prime orders, where i,j are non-negative integers. Then, we showed an example of prime order curve. Our proposal, that is y-twist, is closely related to the well-known complex multiplication; however, our proposal is not so complicated as compared to the complex multiplication, therefore, we can easily extend y-twist for hyper elliptic curves in the form $y^2=x^5+a$, $a\in F_q$ by using 5-th power residue/non-residue.

Reference

[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] F.Morain, http://www.lix.polytechnique.fr/Labo /Francois.Morain/

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

Appendix

A. The orders of y-twisted curves

If $\psi_0E(0,y)=E(0,y)$ is irreducible over F_q, $\psi_1E(0,y)$ and $\psi_2E(0,y)$ are also irreducible. On the other hand, if $\psi_0E(0,y)$ is reducible over F_q, $\psi_1E(0,y)$ and $\psi_2E(0,y)$ are also reducible. In addition, each $\psi_0E(0,y)$, $\psi_1E(0,y)$, and $\psi_2E(0,y)$ has two distinct zeros in F_q because $b\neq 0$ and the characteristic p is not equal to 3. In what follows, $l=0,1,2$ and note that -1 is a TR in F_q.

When $E(0,y)$ is irreducible over F_q, we have the following rational points;

· For $i\in F_q$ such that $\psi_lE(0,i)$ is a TR in F_q, $x^3=-\psi_lE(0,i)$ generates three rational points on the curve.

· For $i\in F_q$ such that $\psi_lE(0,i)$ is a TNR in F_q, $x^3=-\psi_lE(0,i)$ 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 $i\in F_q$ such that $\psi_lE(0,i)$ is not equal to 0 and a TR in F_q, $x^3=-\psi_lE(0,i)$ generates three rational points.

Table 2 Average computation time for generating a prime order elliptic curve

[unit:*sec*]

	complex multiplication	y-twist over F_p†	y-twist over F_{p^3}††
160 bits*	30.1	0.23	0.02
180 bits*	41.5	0.29	0.03
200 bits*	59.3	0.50	0.04

* The size of the order of elliptic curve.

† The sizes of the characteristic p are 160, 180, 200 bits, respectively.

†† The sizes of the characteristic p are 54, 60, 67 bits, respectively.

· For $i \in F_q$ such that $\psi_l E(0,i)$ is not equal to 0 and a TNR in F_q, $x^3 = -\psi_l E(0,i)$ generates no rational points.
· For $i \in F_q$ such that $\psi_l E(0,i)$ is equal to 0, $x^3 = -\psi_l E(0,i)$ 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, the orders are written as Eqs.(13).

Let N_{ψ_0} be the number of i's such that $E(0,i), i \in F_q$ is a non-zero TR in F_q, let N_{ψ_1} and N_{ψ_2} be the numbers of i's such that $E(0,i), i \in F_q$ is a TypeI and a TypeII TNR in F_q, respectively. The notations **TypeI and TypeII TNR** are defined in Appendix.B. First, we consider $\psi_0 E(x,y)$, $\psi_1 E(x,y)$, $\psi_2 E(x,y)$ as

$$\psi_0 E(x,y) : x^3 = -E(0,y), \tag{42a}$$
$$\psi_1 E(x,y) : x^3 = -B^2 E(0,B^{-1}y), \tag{42b}$$
$$\psi_2 E(x,y) : x^3 = -B^4 E(0,B^{-2}y). \tag{42c}$$

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

$$x^3 = -E(0,y), \tag{43a}$$
$$x^3 = -E(0,B^{-1}y), \tag{43b}$$
$$x^3 = -E(0,B^{-2}y), \tag{43c}$$

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

$$\begin{aligned}\{E(0,i), \forall i \in F_q\} &= \{E(0,B^{-1}i), \forall i \in F_q\} \\ &= \{E(0,B^{-2}i), \forall i \in F_q\}.\end{aligned} \tag{44}$$

Therefore, if B is a TR in F_q, by multiplying B^2 and B^4 as shown in Eqs.(42), TRs in $\{E(0,i), \forall i \in F_q\}$ become TRs in F_q and TNRs in $\{E(0,i), \forall i \in F_q\}$ become TNRs in F_q again. Consequently, we have the relation Eq.(15).

Let us denote $\{E(0,i), \forall i \in F_q\}$ by R. When B^2 is a TypeII TNR in F_q and $E(0,y)$ is irreducible over F_q, for example, by multiplying B^2 as shown in Eq.(42b) and **Fig.**3(b), we find

· N_{ψ_0} non-zero TRs in R become N_{ψ_0} TypeII TNRs in F_q,
· N_{ψ_1} TypeI TNRs in R become N_{ψ_1} non-zero TRs in F_q,
· N_{ψ_2} TypeII TNRs in R become N_{ψ_2} TypeI TNRs in F_q.

In the same, by multiplying B^4 as shown in Eq.(42c) and **Fig.**3(c), we find

· N_{ψ_0} non-zero TRs in R become N_{ψ_0} TypeI TNRs in F_q,
· N_{ψ_1} TypeI TNRs in R become N_{ψ_1} TypeII TNRs in F_q,
· N_{ψ_2} TypeII TNRs in R become N_{ψ_2} non-zero TRs in F_q,

where in this case we should note that B^4 becomes a TypeI TNR in F_q. Consequently, we have the relation Eq.(16). **Fig.**3 shows an image of these relations. On the other hand, when B^2 is a TNR in F_q and $E(0,y)$ is reducible over F_q, $B^2E(0,i)$ and $B^4E(0,i)$ also become 0 for $i \in F_q$ such that $E(0,i) = 0$. Therefore, noting that $E(0,y)$ has two distinct zeros in F_q, we have Eq.(17).

C. 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;

$$\text{non-zero TRs} \cdots \left\{g^{3j},\ j = 0,1,\cdots,(q-4)/3\right\}, \tag{45a}$$
$$\text{TypeI TNRs} \cdots \left\{g^{3j+1},\ j = 0,1,\cdots,(q-4)/3\right\}, \tag{45b}$$
$$\text{TypeII TNRs} \cdots \left\{g^{3j+2},\ j = 0,1,\cdots,(q-4)/3\right\}, \tag{45c}$$

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;

$$x^{(q^3-1)/3} = \left(x^{q-1}\right)^{(q^2+q+1)/3} = 1, \tag{46}$$

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}.

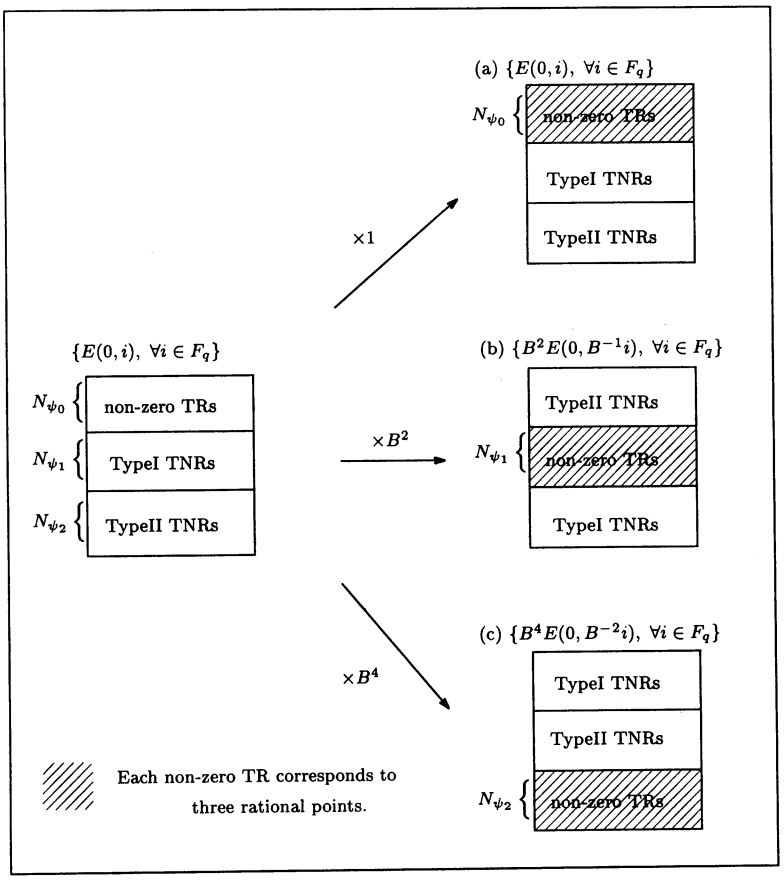

Figure 3 The relation among N_{ψ_0}, N_{ψ_1}, and N_{ψ_2} when B^2 is a TypeII TNR in F_q