The Number of the Irreducible Cubic Polynomials in the Form of $x^3 + ax + b$ with a Certain Fixed Element a

Yasuyuki Nogami[†] Yoshitaka Morikawa[†]

The Graduate School of Natural Science and Technology
Okayama University
Okayama 700-8530 Japan

(Received November 8, 2006)

In this paper, we first show the number of x's such that $x^2 + u, u \in F_p^*$, becomes a quadratic residue in F_p, and then this number is proven to be equal to $(p+1)/2$ if $-u$ is a quadratic residue in F_p, which is a necessary fact for the following. With respect to the irreducible cubic polynomials over F_p in the form of x^3+ax+b, we give a classification based on the trace of an element in F_{p^3} and based on whether or not the coefficient of x, i.e. the parameter a, is a quadratic residue in F_p. According to this classification, we can know the minimal set of the irreducible cubic polynomials, from which all the irreducible cubic polynomials can be generated by using the following two variable transformations: $x = x + i, x = j^{-1}x,\ i, j \in F_p,\ j \neq 0$. Based on the classification and that necessary fact, we show the number of the irreducible cubic polynomials in the form of $x^3+ax+b, b \in F_p$, where a is a certain fixed element in F_p.

Keywords: Irreducible cubic polynomial, trace, quadratic residue

1 Introduction

In the modern network-connected society, information security technologies have played a key role in protecting the various devices or the top secret information from the unauthorized invasion and the evil Internet users. As security technologies, both the Rivest Shamir Adleman (RSA) cryptosystem and the elliptic curve cryptosystem (ECC) can provide a secure environment, where communication can be conducted without fear. However, the ECC offers the equivalent security with 7-fold smaller length key, compared to the RSA cryptosystem. In the other words, ECC provides a more secure environment for the same key sizes. On the other hand, two decades of research led to a number of fascinating attacks on the RSA cryptosystem, which also make it unsafe. Therefore, the ECC has received much attention and has been implemented on various processors[1],[2].

In the previous works[3],[4], the authors have carried out the studies on a elliptic curve defined by

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

The security of ECC relies upon the difficulty of an elliptic curve discrete logarithm problem[5]. Since there were many attacks that make the elliptic curve discrete logarithm problem easier to be resolved, in practice, the order of the curve should have a 160 bits prime factor at least for the sufficient security[6]. It is said that a prime order elliptic curve is suitable for constructing an ECC from the viewpoints of security and implementation[7]. So, researching how to fast generate the prime order elliptic curves is very important. In general, the order of an elliptic curve is calculated for an arbitrary parameter pair a, b shown in Eq.(1), which means that the prime order elliptic curves must be searched in a so large range. Thus it will take a lot of time to generate the prime order elliptic curves by the current algorithms[3],[7],[8]. Since $E(x, 0)$, i.e. x^3+ax+b, is an irreducible cubic polynomial when the order of the elliptic curve is a prime number[5], it might be possible to consider only those parameter pairs a, b of the irreducible polynomials. In the other words, the prime order elliptic curves can be searched in a much smaller range, which makes it possible to fast generate the prime order elliptic curves. If we know the classification of the irreducible cubic polynomials, then we can generate all the others through one irreducible cubic polynomial. However, as far as the authors know, no special methods for classifying the irreducible cubic polynomials have been published. This is a big motivation to investigate the classification of the irreducible cubic polynomials in the present study.

Although a prime order elliptic curve is necessary to construct an ECC, we need not to know all kinds of the prime order elliptic curves. In order to reduce the computations in the algorithm, we thus fix the coefficient of x in Eq.(1), i.e. a, in the present study.

In this paper, we first show the number of x's such that $x^2+u, u \in F_p^*$, becomes a quadratic residue in F_p, and then this number is proven to be equal to $(p+1)/2$ if $-u$ is a quadratic residue in F_p. We need this fact in the following. Then with respect to the irreducible cubic polynomials over F_p in the form of x^3+ax+b, we give a classification based on the trace of an element in F_{p^3} and based on whether or not the coefficient of x, i.e. the parameter a, is a quadratic residue in F_p. According to this classification, we can know the minimal set of the irreducible cubic polynomials, from which all the irreducible cubic polynomials can be generated by using the following two variable transformations:

$$x = x + i,\ x = j^{-1}x, \quad i \in F_p,\ j \in F_p^*. \tag{2}$$

To be more detailed, in the case of $3 \not| \ (p-1)$, by using the above two transformations, all the irreducible cubic polynomials can be classified by the form of

$$x^3 + a_q x + b,\ x^3 + a_{\bar{q}} x + b, \quad b \in F_p, \tag{3}$$

where a_q and $a_{\bar{q}}$ are a non-zero quadratic residue and non residue in F_p, respectively. On the other hand, in the case of $3 \mid (p-1)$, two irreducible cubic binomials $x^3 + b_{\bar{T}}$ and $x^3 + b_{\bar{T}}^2$ are additionally required, where $b_{\bar{T}}$ is a cubic non residue in F_p. For elliptic curves, the former and latter variable transformations of Eq.(2) correspond to the isomorphic transformation and the twist operation, respectively[5]. Based on the classification and that necessary fact, we show the number of the irreducible cubic polynomials in the form of $x^3 + ax + b, b \in F_p$, where a is a certain fixed element in F_p.

Throughout this paper, $X \mid Y$ and $X \not| \ Y$ mean that Y is divisible by X and Y is not divisible by X, respectively. F_p and F_{p^3} mean a prime field and its third extension field, respectively, where the characteristic p is a prime number greater than 3. F_p^* and $F_{p^3}^*$ mean the multiplicative groups of F_p and F_{p^3}, respectively. Without any additional explanation, the polynomials are all the cubic monic polynomials.

2 Fundamentals

In this section, we first review the definition of quadratic residue and trace of an element in a extension field, and then show the relation between an irreducible cubic polynomial and an ECC.

2.1 Quadratic residue and non residue

In a finite field F_{p^m}, where p is an odd prime number, we can use Euler's criterion to test whether or not an arbitrary element A is a quadratic residue

$$A^{(p^m-1)/2} = \begin{cases} 0 \ or \ 1 & \text{quadratic residue} \\ -1 & \text{quadratic non residue} \end{cases}. \tag{4}$$

In the following, quadratic residue and quadratic non-residue are abbreviated as QR and QNR, respectively. If A is a QR, then A has its square roots in F_{p^m}, otherwise, A does not have them in F_{p^m}. In the following, we will use the fact that AB is a QR in F_{p^m} if and only if both A and B are QRs or QNRs in F_{p^m}, where B is an arbitrary element in F_{p^m}.

2.2 Trace of an element in a finite field

For $A \in F_{p^m}$, the trace T_A is defined by

$$\mathrm{T}_A = A + A^p + \cdots + A^{p^{m-1}}, \tag{5}$$

where T_A is always an element in F_p, which is independent of the value of $A \in F_{p^m}$. Since the present study only consider the irreducible cubic polynomials over F_p, we define the function $\mathrm{Tr}(x)$ as

$$\mathrm{Tr}(x) = x + x^p + x^{p^2}, \tag{6}$$

and it follows that $\mathrm{Tr}(A)$ is the trace of $A \in F_{p^3}$ with respect to F_p. Based on Eq.(6), the following relation holds for $\forall\ a, b \in F_p$:

$$\mathrm{Tr}(ax+b) = a\mathrm{Tr}(x) + b\mathrm{Tr}(1), \tag{7}$$

it follows that $\mathrm{Tr}(x)$ is a linear function over F_p. If ω is the zero of an irreducible cubic monic polynomial $f(x)$, then $-\mathrm{Tr}(\omega)$ is simply the coefficient of the quadratic term of $f(x)$[9]. In the following, without any explanations, *the trace of irreducible polynomial* means the trace of zeros of the irreducible polynomial, and the terminology *trace* is defined by Eq.(6).

2.3 The elliptic curve cryptosystem

In general, an elliptic curve used for the cryptosystem is given by

$$E(x,y) = x^3 + Ax + B - y^2,\ A, B \in F, \tag{8}$$

where F is a certain finite field and the characteristic of F is a prime number greater than 3. If $E(x,y)$ is a prime order elliptic curve, then $E(x,0)$, i.e. x^3+Ax+B is an irreducible cubic polynomial. On the hand, if $E(x,0)$ is an irreducible cubic polynomial, then $E(x,y)$ might be a prime order elliptic curve.

3 The number of x's such that $x^2 + u, u \in F_p^*$ becomes a quadratic residue in F_p

In this section, we mainly consider the number of QRs in S_u, denoted by N_u, and the number of QNRs in S_u, denoted by $\overline{N}_u$, which is a mathematical preparation for the following section, where S_u is defined by

$$\begin{aligned} s_u(x) &= x^2 + u,\ u \in F_p^*, & \text{(9a)}\\ S_u &= \{s_u(0), s_u(1), \cdots, s_u(p-1)\}. & \text{(9b)}\end{aligned}$$

From Eq.(9b), we have $N_u + \overline{N}_u = |S_u| = p$, which implies

$$\overline{N}_u = p - N_u. \tag{10}$$

For example, when $p = 7$ and $u = 3$, as shown in Table 1, we have

$$S_3 = \{3,4,0,5,5,0,4\},\ N_3 = 4,\ \overline{N}_3 = 3. \tag{11}$$

Table 1: $s_3(x) = x^2 + 3$ over F_7

x	x^2	$s_3(x)$	QR/QNR of $s_3(x)$
0	0	3	×
1	1	4	○
2	4	0	○
3	2	5	×
4	2	5	×
5	4	0	○
6	1	4	○

Notations : ○ $\cdots$QR, × $\cdots$QNR.

Because of Eq.(10), we only need to consider N_u in what follows.

In fact, the value of N_u can be expressed as shown in Table 2. From Table 2, we can see that the value of N_u depends on whether or not $4 \mid (p-1)$ and whether or not u is a QR.

Table 2: The value of $N_u,\ u \in F_p^*$

	$4 \mid (p-1)$	$4 \not\mid (p-1)$
when u is a QR	$\frac{p+1}{2}$	$\frac{p-1}{2}$
when u is a QNR	$\frac{p-1}{2}$	$\frac{p+1}{2}$

In order to prove Table 2, first, assume $s'_u(x) = s_u(lx)$ for $l \in F_p^*$, and then we have

$$\begin{aligned} s'_u(x) &= l^2x^2 + u, & \text{(10a)}\\ S'_u &= \{s'_u(0), s'_u(1), \cdots, s'_u(p-1)\}. & \text{(10b)}\end{aligned}$$

If the two sets consist of the same elements, then the two sets are regarded as the same set, for example, if $S_A = \{1,1,2,2,3,3,4\}$ and $S_B = \{1,3,2,4,1,2,3\}$, then we have $S_A = S_B$. In this case, from Eq.(9b) and (10b), we can easily know that $S_u = S'_u$.

Next, we consider $s_{l^{-2}u}(x)$ and $S_{l^{-2}u}$, which are given by

$$\begin{aligned} s_{l^{-2}u}(x) &= l^{-2}s'_u(x) = x^2 + l^{-2}u, & \text{(11a)}\\ S_{l^{-2}u} &= \{s_{l^{-2}u}(0), s_{l^{-2}u}(1), \cdots, s_{l^{-2}u}(p-1)\}\\ &= \{l^{-2}s'_u(0), l^{-2}s'_u(1), \cdots, l^{-2}s'_u(p-1)\}. & \text{(11b)}\end{aligned}$$

Since l^{-2} is a QR, the element $l^{-2}s'_u(i)(i{=}0,1,\cdots,p{-}1)$ is a QR if and only if $s'_u(i)$ $(i{=}0,1,\cdots,p{-}1)$ is a QR$(*)$. From $(*)$ and $S_u = S'_u$, we can know

$$N_{l^{-2}u} = N_u, \tag{12}$$

where $N_{l^{-2}u}$ denotes the number of QRs in $S_{l^{-2}u}$. Therefore, the value of N_u, $\forall u \in F_p^*$, depends on whether or not u is a QR in F_p. In what follows, when u is a QR, N_u is denoted by N_Q; when u is a QNR, N_u is denoted by $N_{\overline{Q}}$.

Finally, we consider the set S that is given by

$$S = \{S_0, S_1, \cdots, S_{p-1}\},\ |S| = p^2, \tag{13a}$$

where S_0 is given by

$$s_0(x) = x^2 + 0,\ S_0 = \{s_0(0), s_0(1), \cdots, s_0(p-1)\}, \tag{13b}$$

and $|S|$ denotes the total number of the elements in the subsets $S_0, S_1, \cdots$, and S_{p-1}. To be more detailed, the above defined S can be rewritten as

$$\begin{aligned} S \ = \ \{&0^2{+}0, 1^2{+}0, \cdots, (p-1)^2{+}0,\\ &0^2{+}1, 1^2{+}1, \cdots, (p-1)^2{+}1,\\ &0^2{+}2, 1^2{+}2, \cdots, (p-1)^2{+}2,\\ &\qquad\vdots\\ &0^2{+}(p{-}1), 1^2{+}(p{-}1), \cdots, (p{-}1)^2{+}(p{-}1)\}. \end{aligned} \tag{13c}$$

From Eq.(13c), we can find that the numbers of 0's, 1's, $\cdots$, and $p-1$'s in S are equal to each other. Therefore, the number of QRs in S can be gotten by

$$p + \frac{(p-1)N_Q}{2} + \frac{(p-1)N_{\overline{Q}}}{2} = \frac{p(p+1)}{2}, \tag{14}$$

where the first term of the left hand is the number of QRs in S_0, the second term is that of QRs in S_u $'s$ when u is a non-zero QR, and the third term is that of QRs in S_u $'s$ when u is a QNR.

In the above, we have deduced a relation between N_Q and $N_{\overline{Q}}$ as shown in Eq.(14). In the following Sec.3.1 and Sec.3.2, under the condition of $4 \nmid (p-1)$ or $4 \mid (p-1)$, we are about to deduce another relation between N_Q and $N_{\overline{Q}}$, and then, from this relation and Eq.(14), we can get the results shown in Table 2.

3.1 In the case of $4 \nmid (p-1)$

For $p = 7$, Table 1 shows the distribution of QRs and QNRs of S_u when u is a QNR 3 in F_7; Table 3 shows the distribution of QRs and QNRs of S_u when u is a QR 4 in F_7. The reason why we consider the cases of $u = 3$ and 4 for $p = 7$ is that

$$4 = (-1) \times 3, \tag{15}$$

in other words 4 is the additive inverse of 3 in F_7.

Table 3: $s_4(x) = x^2 + 4$ over F_7

x	x^2	$s_4(x)$	QR/QNR of $s_4(x)$
0	0	4	○
1	1	5	×
2	4	1	○
3	2	6	×
4	2	6	×
5	4	1	○
6	1	5	×

Notations : ○$\cdots$QR, ×$\cdots$QNR.

When $4 \nmid (p{-}1)$, -1 is a QNR in F_p [10], from Eq.(15) it follows that 3 is a QNR if and only if 4 is a QR. Generally speaking, in the case of $4 \nmid (p-1)$, if u_q is a QR in F_p, then $-u_q$ is a QNR in F_p.

As shown in Table 1 and Table 3, $s_3(\pm 1)$ and $s_4(\pm 2)$ are QRs. Moving the term $+3$ to the other side of Eq.(16a) as shown in Eq.(16c), we obtain Eq.(16b).

$$s_3(\pm 1) = 1 + 3 = 4,\ \text{where 4 is a QR}, \tag{16a}$$

$$s_4(\pm 2) = 4 + 4 = 1,\ \text{where 1 is a QR}, \tag{16b}$$

$$1 = 4 - 3 = 4 + 4 = 1,\ \text{where } -3 = 4 \text{ in } F_7. \tag{16c}$$

Generally speaking, for any QR $q_1 \in F_p$, we have

$$s_u(\pm\sqrt{q_1}) = q_1 + u = q_2,\ \text{where } q_2 \text{ is a QR}, \tag{17a}$$

Moving $+u$ to the other side of Eq.(17a), we obtain

$$s_{-u}(\pm\sqrt{q_2}) = q_2 + (-u) = q_1,\ \text{where } q_1 \text{ is a QR}. \tag{17b}$$

In the case of $4 \nmid (p{-}1)$, u is a QR if and only if $-u$ is a QNR, therefore, two QRs $s_u(\pm\sqrt{q_1})$ in S_u correspond to two QRs $s_{-u}(\pm\sqrt{q_2})$ in S_{-u}, in other words, it is a two-to-two mapping between S_u and S_{-u}.

The only exception is the case that $s_u(x)$ or $s_{-u}(x)$ is 0. As shown in Table 1, $s_3(\pm 2)$ is equal to 0, it follows that two QRs $s_3(\pm 2)$ correspond to one QR $s_4(0)$:

$$s_3(\pm 2) \ = \ 4 + 3 = 0,\ \text{where 0 is a QR}, \tag{18a}$$

$$s_4(0) \ = \ 0 - 3 = 4,\ \text{where 4 is a QR}, \tag{18b}$$

where we can obtain Eq.(18b) by moving +3 to the other side of Eq.(18a). Generally speaking, we find that two QRs $s_u(\pm\sqrt{q_3})$ correspond to one QR $s_{-u}(0)$:

$$\begin{aligned} s_u(\pm\sqrt{q_3}) &= q_3 + u = 0, \text{ where } 0 \text{ is a QR,} &\text{(19a)}\\ s_{-u}(0) &= 0 - u = q_3, \text{ where } q_3 \text{ is a QR.} &\text{(19b)}\end{aligned}$$

In other words, this is a two-to-one mapping between S_u and S_{-u}. This two-to-one mapping is basically caused by the following: a non-zero QR has two square roots, however, the zero element only has one square root, i.e. the zero element itself. Therefore, either S_u or S_{-u} that contains the zero element has one more QR than the other. In the case of $4 \not| \ (p-1)$, S_u contains the zero element if and only if u is a QNR. Consequently, we obtain the following relation between N_Q and $N_{\overline{Q}}$:

$$N_{\overline{Q}} = N_Q + 1. \qquad (20)$$

From Eq.(14) and (20), we have

$$N_Q = \frac{(p-1)}{2}, \quad N_{\overline{Q}} = \frac{(p+1)}{2}. \qquad (21)$$

3.2 In the case of $4 \mid (p-1)$

For $p = 13$, Table 4 shows the distribution of QRs and QNRs of S_u when u is a QNR 11 in F_{13}; Table 5 shows the distribution of QRs and QNRs of S_u when u is a QR 10 in F_{13}. The reason why we consider the cases of $u = 11$ and 10 for $p = 7$ is that

$$10 = (-5) \times 11, \qquad (22)$$

where 5 is a QNR in F_{13}.

As shown in Table 4 and Table 5, $s_{11}(\pm 2)$ and $s_{10}(\pm 6)$ are QNRs. Moving +11 to the other side of Eq.(23a) as shown in Eq.(23c), and then multiplying by 5 as shown in Eq.(23d), we can obtain Eq.(23b).

$$\begin{aligned} s_{11}(\pm 2) &= 4 + 11 = 2, \text{ where } 2 \text{ is a QNR,} &\text{(23a)}\\ s_{10}(\pm 6) &= 10 + 10 = 7, \text{ where } 7 \text{ is a QNR,} &\text{(23b)}\\ 4 &= 2 - 11, &\text{(23c)}\\ &\downarrow &\\ 4 \times 5 &= 10 + (-5) \times 11 &\text{(23d)}\\ &= 10 + 10 = 7, \text{ where } -5 \times 11 = 10 &\text{(23e)}\end{aligned}$$

Generally speaking, for any QR $q_1 \in F_p$, we have

$$s_u(\pm\sqrt{q_1}) = q_1 + u = \overline{q}_2, \text{ where } \overline{q}_2 \text{ is a QNR.} \qquad (24a)$$

Table 4: $s_{11}(x) = x^2 + 11$ over F_{13}

x	x^2	$s_{11}(x)$	QR/QNR of $s_{11}(x)$
0	0	11	×
1	1	12	○
2	4	2	×
3	9	7	×
4	3	1	○
5	12	10	○
6	10	8	×
7	10	8	×
8	12	10	○
9	3	1	○
10	9	7	×
11	4	2	×
12	1	12	○

Notations : ○ ⋯QR, × ⋯QNR.

Moving $+u$ to the other side of the above equation, and then multiplying a QNR $\bar{q} \in F_p$, we can obtain

$$s_{-\bar{q}u}(\pm\sqrt{\bar{q}\bar{q}_2}) = \bar{q}\bar{q}_2 + (-\bar{q}u) = \bar{q}q_1, \qquad (24b)$$

where $\bar{q}q_1$ is a QNR. Therefore, two QNRs $s_u(\pm\sqrt{q_1})$ in S_u correspond to two QNRs $s_{-\bar{q}u}(\pm\sqrt{\bar{q}\bar{q}_2})$ in $S_{-\bar{q}u}$, in other words, it is a two-to-two mapping between S_u and $S_{-\bar{q}u}$. Note that $\bar{q}\bar{q}_2$ is a QR, $\bar{q}q_1$ is a QNR, and in the case of $4 \mid (p-1)$, u is a QR if and only if $-\bar{q}u$ is a QNR. As shown in Table 4 and Table 5, the only exception is

$$\begin{aligned} s_{11}(0) &= 0 + 11 = 11, \text{ where } 11 \text{ is a QNR,} &\text{(25a)}\\ s_{10}(\pm 4) &= 16 + 10 = 0, \text{ where } 0 \text{ is a QR.} &\text{(25b)}\end{aligned}$$

Generally speaking, the only exception is that a QNR $s_u(0)$ corresponds to two QRs $s_{-\bar{q}u}(\pm\sqrt{\bar{q}\bar{q}_3})$:

$$\begin{aligned} s_u(0) &= 0 + u = \bar{q}_3, &\text{(26a)}\\ s_{-\bar{q}u}(\pm\sqrt{\bar{q}\bar{q}_3}) &= \bar{q}\bar{q}_3 - \bar{q}u = 0, &\text{(26b)}\end{aligned}$$

where $\bar{q}_3$ is a QNR, 0 is a QR, and $\bar{q}\bar{q}_3$ is a QR. In other words, this is a two-to-one mapping between S_u and $S_{-\bar{q}u}$. It follows that either S_u or $S_{-\bar{q}u}$, containing the zero element, has one more QR than the other. In order to satisfy Eq.(26b), $-\bar{q}u$ must be a QR, i.e. u must be a QNR. In the case of $4 \mid (p-1)$, S_u contains the zero element if and only if u is a QR, which implies $0 \in S_{-\bar{q}u}$. In the case of $4 \mid (p-1)$, we thus have

$$N_Q = N_{\overline{Q}} + 1. \qquad (27)$$

Table 5: $s_{10}(x) = x^2 + 10$ over F_{13}

x	x^2	$s_{10}(x)$	QR/QNR of $s_{10}(x)$
0	0	10	○
1	1	11	×
2	4	1	○
3	9	6	×
4	3	0	○
5	12	9	○
6	10	7	×
7	10	7	×
8	12	9	○
9	3	0	○
10	9	6	×
11	4	1	○
12	1	11	×

Notations : ○ $\cdots$QR, × $\cdots$QNR.

From Eq.(14) and (27), we can obtain

$$N_Q = \frac{(p+1)}{2}, \quad N_{\overline{Q}} = \frac{(p-1)}{2}. \tag{28}$$

From what described above, we know $N_u = (p+1)/2$ when S_u contains 0, in other words, when $-u$ is a QR in F_p. In the next section, we will use this result.

4 Classification of the irreducible cubic polynomials over a prime field

In this section, under the condition of $3 \mid (p-1)$ or $3 \not| \ (p-1)$, we first give a classification of the irreducible cubic polynomials over F_p in the form of $x^3 + ax + b$, $b \in F_p$, where a is a certain fixed element in F_p, and then we show the number of those irreducible cubic polynomials.

First, we consider a classification based on the trace. Let I be the set of the irreducible cubic polynomials over F_p, and let I_i be the set of the irreducible cubic polynomials whose trace is equal to i, of course, $i \in F_p$:

$$\begin{aligned} I &= \{h(x) \mid h(x) \mid (x^{p^3} - x)/(x^p - x)\}, && \text{(29a)} \\ I_i &= \{h(x) \mid h(x) \mid \mathrm{Tr}(x) - i,\ h(x) \in I\}, && \text{(29b)} \\ & \qquad 0 \le i \le p-1, \end{aligned}$$

and then I and I_i give a classification as shown in Fig.1, where $(x^{p^3} - x)/(x^p - x)$ is the product of all the irreducible cubic polynomials over F_p and the following equation holds with the trace function Eq.(6)[9]:

$$x^{p^3} - x = \prod_{i=0}^{p-1} (\mathrm{Tr}(x) - i). \tag{30}$$

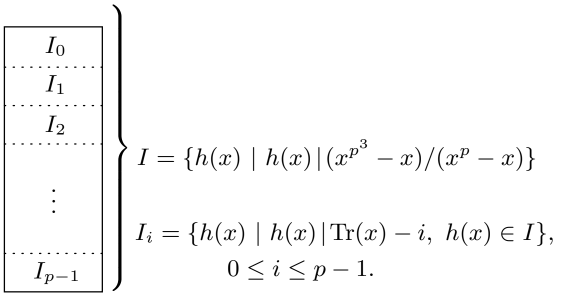
I_0
I_1
I_2
$\vdots$
I_{p-1}
$I = \{h(x) \mid h(x) \,|\, (x^{p^3} - x)/(x^p - x)\}$
$I_i = \{h(x) \mid h(x) \,|\, \mathrm{Tr}(x) - i,\ h(x) \in I\},$
$0 \le i \le p-1.$

Figure 1: Classification of the irreducible cubic polynomials using the trace of finite field element

Let $|I_i|$ denote the number of the irreducible polynomials in I_i, and then we have [9];

$$|I_0| = |I_1| = |I_2| = \cdots = |I_{p-1}|. \tag{31}$$

From the definition of the trace, we have

$$\mathrm{Tr}(x+i) = \mathrm{Tr}(x) + 3i, \quad i \in F_p, \tag{32}$$

where the set $\{3i | i \in F_p\}$ is equal to the set $\{i | i \in F_p\}$. In I_0, the irreducible cubic polynomials have the form of $x^3 + a_0 x + b_0$, from which all the irreducible cubic polynomials over F_p can thus be generated by using the following variable transformations:

$$x = x + i, \ i \in F_p. \tag{33}$$

Therefore, in what follows, we only consider the classification of I_0 in the cases of $3 \not| \ (p-1)$ and $3 \mid (p-1)$.

4.1 In the case of $3 \not| \ (p-1)$

In the case of $3 \not| \ (p-1)$, we classify the irreducible cubic polynomials in I_0 based on whether or not the coefficient of x is a QR. First, the following sets of the irreducible cubic polynomials are considered:

$$I_{0Q} = \{h(x) \mid h(x) \in I_0, h'(0) \text{ is a non zero QR}\}, \tag{34a}$$

$$I_{0\bar{Q}} = \{h(x) \mid h(x) \in I_0, h'(0) \text{ is a QNR}\}, \tag{34b}$$

where $h'(x)$ is the derivative of $h(x)$, it follows that $h'(0)$ is equal to the coefficient of x in $h(x)$. In this case, there does not exist any irreducible binomials over F_p[9]. Eqs.(34) thus give a classification, as shown in Fig.2, and we have the following property:

Proposition 1

$$|I_0| = |I_{0Q}| + |I_{0\bar{Q}}| = \frac{p^2-1}{3}, \tag{35a}$$

$$|I_{0Q}| = |I_{0\bar{Q}}| = \frac{p^2-1}{6}. \tag{35b}$$

Proof : The proof of Eq.(35a) is given from Eq.(6) and the fact that an irreducible cubic polynomial has three conjugates as zeros[9]. Herein, we only need to show the proof of Eq.(35b). First, we suppose an irreducible polynomial $f(x) \in I_0$ in the form of

$$f(x) = x^3 + ax + b, \quad a, b \in F_p, \ a \neq 0. \tag{36}$$

Let τ be a zero of an irreducible polynomial in Fig.2, and τ can be written as a linear combination of two conjugates ω and ω^p:

$$\tau = c_1\omega + c_p\omega^p, \ c_1, c_p \in F_p, \tag{37}$$

where ω is a zero of $f(x)$. Since $\mathrm{Tr}(\omega) = 0$, we have $\mathrm{Tr}(\tau) = 0$. Now, let $M_\tau(x)$ be the minimal polynomial of τ, and then its first-degree coefficient $M'_\tau(0)$ is given by

$$\begin{aligned} M'_\tau(0) &= \tau\tau^p + \tau\tau^{p^2} + \tau^p\tau^{p^2} \\ &= \left(\omega^2 + \omega\omega^p + \omega^{2p}\right)\left(c_1c_p - c_1^2 - c_p^2\right) \\ &= a\left(c_1^2 + c_p^2 - c_1c_p\right). \end{aligned} \tag{38}$$

Therefore, based on Sec.2.1, whether or not the first-degree coefficient of $M_\tau(x)$ is a QR depends on whether or not $c_1^2 + c_p^2 - c_1c_p$ is a QR, where whether or not the parameter a is a QR in F_p can be checked in advance. From Eq.(38), $|I_{0Q}|$ is given by the number of τ's such that $c_1^2 + c_p^2 - c_1c_p$ becomes a QR.

Before counting the number of such τ's, we should note that only zero element satisfies $\mathrm{Tr}(x) = 0$ in F_p[9], in this case, c_1 and c_p are both zero. Since τ is a zero of an irreducible cubic polynomial, when c_1 is a certain element in F_p^*, we can thus develop $c_1^2 + c_p^2 - c_1c_p$ as

$$\begin{aligned} c_1^2 + c_p^2 - c_1c_p &= \frac{c_1^2}{4}\left\{4 + \left(\frac{2c_p}{c_1}\right)^2 - \left(\frac{4c_p}{c_1}\right)\right\} \\ &= \frac{c_1^2}{4}\left\{\left(\frac{2c_p}{c_1} - 1\right)^2 + 3\right\} \\ &= \frac{c_1^2}{4}\left(c^2 + 3\right), \end{aligned} \tag{39}$$

where $c = 2c_p/c_1 - 1$ and c is possible to become an arbitrary element in F_p for $\forall\ c_p \in F_p$. Since $c_1^2/4$ is a QR, the problem whether or not $c_1^2 + c_p^2 - c_1c_p$ is a QR can be converted into the problem whether or not c^2+3 is a QR. In order to get the value of $|I_0|$, we thus consider the number of c's such that $c^2 + 3$ becomes a QR. In the case of $3 \not| \ (p-1)$, $c^2 + 3 = 0$ can not hold for $\forall\ c \in F_p$. Therefore, as described in Sec.3, there exist $(p-1)/2$ c's in F_p such that $c^2 + 3$ becomes a QR. In other words, for a certain $c_1 \in F_p^*$, there exist $(p-1)/2$ c_p's such that $c_1^2 + c_p^2 - c_1c_p$ becomes a QR.

On the other hand, when $c_1 = 0$, we have

$$c_1^2 + c_p^2 - c_1c_p = c_p^2, \tag{40}$$

it follows that there exist $(p-1)$ c_p's in F_p^* such that c_p^2 becomes a QR, where $c_p \neq 0$.

In total, for $c_1 = 0, 1, 2, \cdots, p-1$, the number of combinations of c_1 and c_p such that $c_1^2 + c_p^2 - c_1c_p$ becomes a QR is given by

$$(p-1) \times \frac{p-1}{2} + (p-1) = \frac{p^2-1}{2}. \tag{41}$$

From Eq.(35a) and (41), we can obtain Eq.(35b). ■

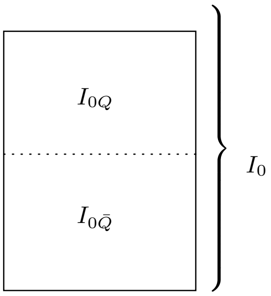

Figure 2: Classification of irreducible cubic polynomials in I_0 based on whether or not the first-degree coefficient is a QR

Next, we consider a more detailed classification in I_{0Q} and $I_{0\bar{Q}}$. For a certain non-zero QR a_q and QNR $a_{\bar{q}}$ in F_p, all non-zero QRs and QNRs are given by Eq.(42a) and Eq.(42b), respectively.

$$a_q, 2^2a_q, 3^2a_q, \cdots, \left(\frac{p-1}{2}\right)^2 a_q, \tag{42a}$$

$$a_{\bar{q}}, 2^2a_{\bar{q}}, 3^2a_{\bar{q}}, \cdots, \left(\frac{p-1}{2}\right)^2 a_{\bar{q}}. \tag{42b}$$

Considering the following sets:

$$\begin{aligned} I_{0Q}(a_q) &= \{h(x) \mid h(x) \in I_0, h'(0) = a_q\}, && (43a) \\ I_{0\bar{Q}}(a_{\bar{q}}) &= \{h(x) \mid h(x) \in I_0, h'(0) = a_{\bar{q}}\}, && (43b) \\ & (a_q \neq 0) \end{aligned}$$

where $I_{0Q}(a_q)$ and $I_{0\bar{Q}}(a_{\bar{q}})$ consist of the irreducible cubic polynomials whose first-degree coefficients are the QR a_q and the QNR $a_{\bar{q}}$, respectively, and then Eqs.(43) give a classification as shown in Fig.3 and we have the following property:

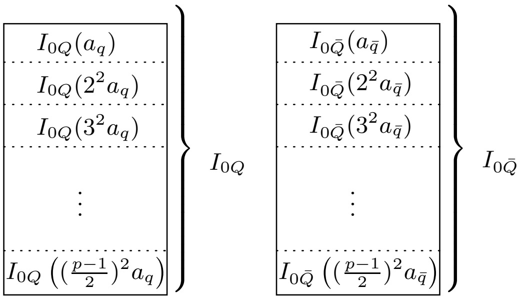
$I_{0Q}(a_q)$
$I_{0Q}(2^2a_q)$
$I_{0Q}(3^2a_q)$
$\vdots$
$I_{0Q}\left((\frac{p-1}{2})^2a_q\right)$
I_{0Q}
$I_{0\bar{Q}}(a_{\bar{q}})$
$I_{0\bar{Q}}(2^2a_{\bar{q}})$
$I_{0\bar{Q}}(3^2a_{\bar{q}})$
$\vdots$
$I_{0\bar{Q}}\left((\frac{p-1}{2})^2a_{\bar{q}}\right)$
$I_{0\bar{Q}}$

Figure 3: A detailed classification in I_0 when $3 \not| \ (p-1)$

Proposition 2

$$|I_{0Q}(j^2a_q)| = |I_{0\bar{Q}}(j^2a_{\bar{q}})| = \frac{p+1}{3}, \quad \text{where } 1 \le j \le \frac{p-1}{2}, \tag{44}$$

Proof : Let us consider an irreducible polynomial $I(x) \in I_{0Q}(a_q)$ in the form of

$$I(x) = x^3 + a_q x + b,\ b \in F_p. \tag{45}$$

Applying the following variable transformation:

$$x = j^{-1}x,\ j \in F_p^* \tag{46}$$

and then multiplying the above $I(x)$ by j^3, we can obtain the following irreducible cubic monic polynomial:

$$I'(x) = x^3 + a_q j^2 x + bj^3. \tag{47}$$

In addition, the transformation Eq.(46) and its inverse transformation holds a one-to-one mapping between $I(x)$ and $I'(x)$. Therefore, $|I_{0Q}(a_q)|$ that is the number of the irreducible polynomials in $I_{0Q}(a_q)$ is equal to $|I_{0Q}(j^2a_q)|$. In the same way, we can also know $|I_{0\bar{Q}}(a_{\bar{q}})| = |I_{0\bar{Q}}(j^2a_{\bar{q}})|$. From Eqs.(35), we thus have

$$\begin{aligned} |I_{0Q}(j^2a_q)| = |I_{0\bar{Q}}(j^2a_{\bar{q}})| &= \frac{p^2-1}{6} \div \frac{p-1}{2}, \\ &= \frac{p+1}{3} \end{aligned} \tag{48}$$

■

From this classification, we can know that the transformations Eq.(46) can determine all the irreducible cubic polynomials in $I_{0Q}(j^2a_q)$ if we can prepare an irreducible cubic polynomial in $I_{0Q}(a_q)$. In the same way, all the irreducible cubic polynomials in $I_{0\bar{Q}}(j^2a_{\bar{q}})$ can be generated by an irreducible cubic polynomial in $I_{0\bar{Q}}(a_{\bar{q}})$.

Consequently, in the case of $3 \not| \ (p-1)$, all the irreducible cubic polynomials over F_p can be generated by the transformations Eq.(33) and Eq.(46) if all the irreducible polynomials in $I_{0Q}(a_q)$ and $I_{0\bar{Q}}(a_{\bar{q}})$ are prepared.

4.2 In the case of $3 \mid (p-1)$

In this case, there exist irreducible binomials x^3+b, $b \in F_p$[9], same as the classification Eqs.(43), we can thus consider the following classifications:

$$\begin{aligned} I_{0Q}(0) &= \{h(x) \mid h(x) \in I_{0Q}, h'(0) = 0\}, && (49a) \\ I_{0Q}(a_q) &= \{h(x) \mid h(x) \in I_{0Q}, h'(0) = a_q\} && (49b) \\ I_{0\bar{Q}}(a_{\bar{q}}) &= \{h(x) \mid h(x) \in I_{0\bar{Q}}, h'(0) = a_{\bar{q}}\}, && (49c) \end{aligned}$$

where $a_q \neq 0$. Eqs.(49) give a classification as shown in Fig.4, that is a detailed classification in I_0, and we have the following property:

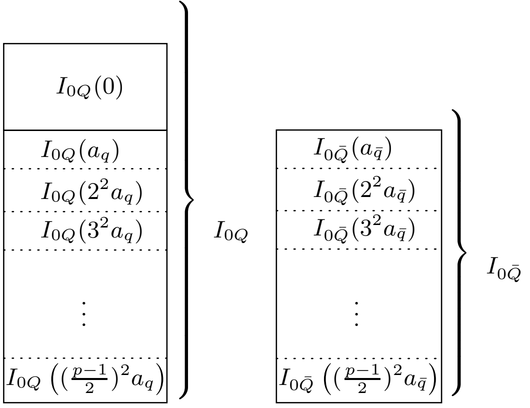
$I_{0Q}(0)$
$I_{0Q}(a_q)$
$I_{0Q}(2^2a_q)$
$I_{0Q}(3^2a_q)$
$\vdots$
$I_{0Q}\left((\frac{p-1}{2})^2a_q\right)$
I_{0Q}
$I_{0\bar{Q}}(a_{\bar{q}})$
$I_{0\bar{Q}}(2^2a_{\bar{q}})$
$I_{0\bar{Q}}(3^2a_{\bar{q}})$
$\vdots$
$I_{0\bar{Q}}\left((\frac{p-1}{2})^2a_{\bar{q}}\right)$
$I_{0\bar{Q}}$

Figure 4: A detailed classification in I_0 when $3 \mid (p-1)$

Proposition 3

$$\begin{aligned} |I_{0Q}(0)| &= \frac{2(p-1)}{3}, && (50a) \\ |I_{0Q}(j^2a_q)| &= |I_{0\bar{Q}}(j^2a_{\bar{q}})| = \frac{p-1}{3}, && (50b) \\ & \text{where } 1 \le j \le \frac{p-1}{2}. \end{aligned}$$

$|I_{0Q}|$, $|I_{0\bar{Q}}|$, and $|I_{0Q}(0)|$ satisfy

$$\begin{aligned} |I_0| &= |I_{0Q}| + |I_{0\bar{Q}}| = \frac{p^2-1}{3}, && (51a) \\ |I_{0\bar{Q}}| &= |I_{0Q}| - |I_{0Q}(0)| = \frac{(p-1)^2}{6}. && (51b) \end{aligned}$$

Proof : Eq.(50a) can be proven by the fact that there exist $2(p-1)/3$ cubic non residues as shown in Eqs.(54). Same as the proof of Eq.(44), we can prove Eq.(50b) by using Eq.(53b). Eq.(51a) can be deduced from Eq.(6)[9]. We thus only need to show the proof of Eq.(51b).

In the case of $3 \mid (p-1)$, Eq.(39) still holds, however, there exists $c \in F_p$ such that $c^2+3=0$. In further detail, there exist $(p+1)/2$ c's in F_p such that c^2+3 becomes a QR, as shown in Sec.3. In addition, there exist $(p-1)$ c_p's in F_p^* such that the right side of Eq.(40), i.e. c_p^2, becomes a QR. Therefore, for $c_1 = 0,1,2,\cdots,p-1$, the number of combinations of c_1 and c_p such that $c_1^p + c_p^p - c_1c_p$ becomes a QR is given by

$$(p-1)\times\frac{p+1}{2}+(p-1)=\frac{p^2+2p-3}{2}. \tag{52}$$

Since there exist $2(p-1)/3$ irreducible binomials over F_p, we thus have

$$\begin{aligned}|I_{0Q}|-|I_{0Q}(0)| &= \frac{p^2+2p-3}{6}-\frac{2(p-1)}{3}\\ &= \frac{(p-1)^2}{6}, \qquad (53a)\\ |I_{0\bar{Q}}| = |I_0|-|I_{0Q}| &= \frac{p^2-1}{3}-\frac{p^2+2p-3}{6}\\ &= \frac{(p-1)^2}{6}. \qquad (53b)\end{aligned}$$

■

In the same way, $I_{0Q}(0)$ can be further classified. $x^3+b, b\in F_p$, is an irreducible if and only if b is a cubic non residue in F_p[9]. Supposing a primitive element $g \in F_p$, we can classify cubic non residues into

$$\begin{aligned}\bar{T}_1 &= \left\{x \mid x = g^{3k+1},\ 0\le k\le\frac{p-4}{3}\right\}, \qquad (54a)\\ \bar{T}_2 &= \left\{x \mid x = g^{3k+2},\ 0\le k\le\frac{p-4}{3}\right\}. \qquad (54b)\end{aligned}$$

It follows that all the irreducible binomials can be divided into two sets: one consists of the irreducible binomials whose constant term belongs to $\bar{T}_1$ and the other consists of the irreducible binomials whose constant term belongs to $\bar{T}_2$. Denoting the two sets by $I_{0Q}(0)_{\bar{T}_1}$ and $I_{0Q}(0)_{\bar{T}_2}$, respectively, as shown in Fig.5, we can classify $I_{0Q}(0)$ by the following:

$$\begin{aligned}I_{0Q}(0)_{\bar{T}_1} &= \{h(x) \mid h(x)\in I_{0Q}(0), h(0)\in\bar{T}_1\}, (55a)\\ I_{0\bar{Q}}(0)_{\bar{T}_2} &= \{h(x) \mid h(x)\in I_{0Q}(0), h(0)\in\bar{T}_2\}. (55b)\end{aligned}$$

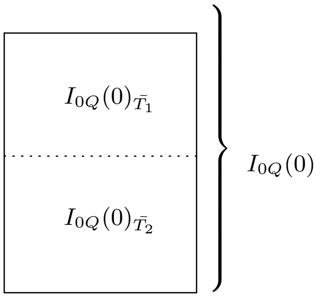

Figure 5: A detailed classification in $I_{0Q}(0)$ with the cubic residue property when $3 \mid (p-1)$

In addition, we consider the two cubic non residues $b_{\bar{T}_1}\in\bar{T}_1$ and $b_{\bar{T}_2}\in\bar{T}_2$, then same as Eqs.(42), we can represent all cubic non residues as

$$g^{3k}b_{\bar{T}_1},\ g^{3k}b_{\bar{T}_2},\quad 0\le k\le\frac{p-4}{3}. \tag{56}$$

Referring to Fig.3, we can thus classify $I_{0Q}(0)$ as shown in Fig.6. If we prepare the irreducible binomials $x^3+b_{\bar{T}_1}$ and $x^3+b_{\bar{T}_2}$, then we can determine all the irreducible binomials in $I_{0Q}(0)_{\bar{T}_1}$ and $I_{0Q}(0)_{\bar{T}_2}$ by using the following variable transformations:

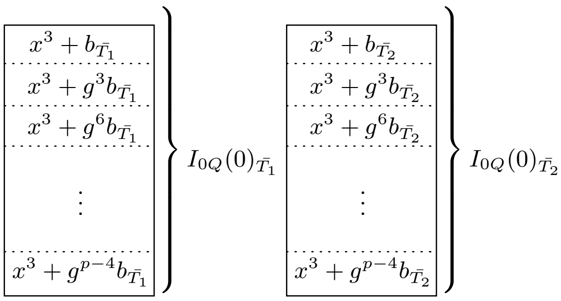

Figure 6: A detailed classification in $I_{0Q}(0)$ when $3 \mid (p-1)$

$$x = g^{-3k}x,\ 0\le k\le\frac{p-4}{3}. \tag{57}$$

As shown in Fig.6, the following relation holds:

$$|I_{0Q}(0)_{\bar{T}_1}| = |I_{0Q}(0)_{\bar{T}_2}|. \tag{58}$$

Consequently, in the case of $3 \mid (p-1)$, we can determine all the irreducible cubic polynomials over F_p by using variable transformations Eq.(33), Eq.(46), and Eq.(57) if we prepare $x^3+b_{\bar{T}_1}$, $x^3+b_{\bar{T}_2}$, $I_{0Q}(a_q)$ and $I_{0\bar{Q}}(a_{\bar{q}})$.

5 Conclusion

In this paper, we first gave a classification of the irreducible cubic polynomials over F_p in the form of $x^3 + ax + b$. According to this classification, we can know the minimal set of the irreducible cubic polynomials, as shown in Table 6, from which all the irreducible cubic polynomials can be generated by using the following isomorphic variable transformations:

$$x = x + i, \; x = j^{-1}x, \quad i \in F_p, \; j \in F_p^*. \tag{59}$$

Then we showed the number of the irreducible cubic polynomials over F_p in the form of $x^3 + ax + b$, where $b \in F_p$ and a is a certain fixed element in F_p. To speak more detailedly, in the case of $3 \not| (p-1)$, this number is equal to $(p+1)/3$; in the case of $3 \,|\, (p-1)$, this number is equal to $2(p-1)/3$ for $a = 0$, or equal to $(p-1)/3$ for $a \neq 0$.

Table 6: Required irreducible cubic polynomials

$3 \not| (p-1)$	$I_{0Q}(a_q), \; I_{0\bar{Q}}(a_{\bar{q}})$
$3 \mid (p-1)$	$I_{0Q}(a_q)$, $I_{0\bar{Q}}(a_{\bar{q}})$, $x^3 + b_{\bar{T}_1}$, $x^3 + b_{\bar{T}_2}$

References

[1] J.Guajardo, R.Blumel, U.Kritieger, and C.Paar, “Efficient Implementation of Elliptic Curve Cryptosystems on the TI MSP430x33x Family of Microcontrollers,” *PKC2001*, LNCS 1992, pp.365-382, 2001.

[2] T.Kobayashi, H.Morita, K.Kobayashi, and F.Hoshino, “Fast Elliptic Curve Algorithm Combining Frobenius Map and Table Reference to Adopt to Higher Characteristic,” *EUROCRYPT’99*, LNCS 1592, pp.176-189, 1999.

[3] Y.Nogami and Y.Morikawa, “Fast Generation of Elliptic Curves with Prime Order over $F_{p^{2^c}}$,” *Proc. of Workshop on Coding and Cryptography* (WCC2003), pp.347-356, 2003.

[4] F. Wang, Y.Nogami, and Y.Morikawa, “A Fast Square Root Computation Using the Frobenius Mapping,” *Fifth International Conference on Information and Communications Security* (ICICS2003), LNCS2836, pp.1-10, 2003.

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

[6] D.Hankerson, A.Menezes, and S.Vanstone, *Guide to Elliptic Curve Cryptography*, Springer, 2004.

[7] K.Horiuchi, Y.Futa, R.Sakai, M.Kaneko, and M.Kasahara, “Construction of Elliptic Curves with Prime Order and Estimation of Its Complexity,” *IEICE Trans.*, **J82-A**, no.8, pp.1269-1277, 1999.

[8] E.Konstantinou, Y.Stamatiou, and C.Zaroliagis, “On the Construction of Prime Order Elliptic Curves,” *INDOCRYPTO2003*, LNCS2904, pp.309-322, 2003.

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

[10] Berlekamp.E.R, *Algebraic Coding Theory*, McGraw-Hill, 1968.