J. Korean Math. Soc. **46** (2009), No. 1, pp. 1–12

CERTAIN CUBIC POLYNOMIALS OVER FINITE FIELDS

HYUNG DON KIM, JAE MOON KIM, AND IKKWON YIE

ABSTRACT. Motivated by XTR cryptosystem which is based on an irreducible polynomial $x^3 - cx^2 + c^p x - 1$ over F_{p^2}, we study polynomials of the form $F(c,x) = x^3 - cx^2 + c^q x - 1$ over F_{q^2} with $q = p^m$. In this paper, we establish a one to one correspondence between the set of such polynomials and a certain set of cubic polynomials over F_q. Our approach is rather theoretical and provides an efficient method to generate irreducible polynomials over F_{q^2}.

1. Introduction

Throughout this paper, we denote the finite field with p^n elements by F_{p^n}, where p is an odd prime. Recently, in [1], A. K. Lenstra and E. R. Verheul introduced a new cryptosystem called XTR. Let $F(c,x) = x^3 - cx^2 + c^p x - 1$ be an irreducible polynomial in $F_{p^2}[x]$ for some element $c \in F_{p^2}$, and h a root of $F(c,x)$. For each integer k, put $c_k = \mathrm{Tr}(h^k)$, where Tr is the trace from F_{p^6} to F_{p^2}. The idea of XTR (Efficient and Compact Subgroup Trace Representation) is that one can make use of $\{c_k\}$ instead of the subgroup $\langle h \rangle = \{h^k\}$ of $F_{p^6}^*$ in implementing various cryptosystems such as Diffie-Hellman key agreement protocol and ElGamal system. The efficiency of computation of $\{c_k\}$ from given c makes the cryptosystem work and the difficulty of finding k from c_k makes it safe. Note that $\{c_k\}$ is in F_{p^2}, while $\langle h \rangle = \{h^k\}$ is in F_{p^6}. Thus XTR system has the obvious advantages in both computation and communication (XTR reduces the cost to $\frac{1}{3}$) with maintaining the same security level as one works with $\{h^k\}$ ([1]).

Motivated by their work, in this paper, we study cubic polynomials of the form $F(c,x) = x^3 - cx^2 + c^q x - 1$, where $c \in F_{q^2}$ and $F_q = F_{p^m}$ is an arbitrary finite field with q elements of characteristic p. Our primary concern is to study the irreducibility of such polynomials. In [1], [2], and [3], several algorithms of irreducibility test of $F(c,x)$ are given when $q = p$ is a prime. The best algorithm for irreducibility test known so far requires about $1.8 \log_2 p$ multiplications in

Received January 31, 2004.

2000 *Mathematics Subject Classification.* 11T06, 11T55, 11T71.

Key words and phrases. irreducibility, normal basis, Hilbert Theorem 90.

This work is supported by the Korea Research Foundation Grant (KRF-2001-015-DP0007).

F_p. Our approach is somewhat different. Fix a quadratic nonresidue t in F_q. In Section 2.1, we will show that there is a one to one correspondence between the set of irreducible polynomials of the form $x^3 - cx^2 + c^q x - 1$ in $F_{q^2}[x]$ and the set of irreducible polynomials of the form $x^3 - tax^2 + bx + a$ in $F_q[x]$. The correspondence is so explicit that one can determine $c \in F_{q^2}$ from given a and b in F_q, and vice versa. Therefore in order to generate an irreducible polynomial $x^3 - cx^2 + c^q x - 1$ in $F_{q^2}[x]$, start with an irreducible polynomial $x^3 - tax^2 + bx + a$ in $F_q[x]$ and get the corresponding one in $F_{q^2}[x]$. In Section 2.2, we compare the set of all polynomials of the form $x^3 - cx^2 + c^q x - 1$ in $F_{q^2}[x]$ with that consisting of polynomials of the form $x^3 - tax^2 + bx + a$ in $F_q[x]$ regardless of their irreducibilities. We will show that the factorization types of the corresponding polynomials agree under the correspondence. The exact meaning of factorization types will be explained in Section 2. In Section 2.3, we will describe another one to one correspondence. Namely, we will prove that there is a one to one correspondence between the set of irreducible polynomials of the form $x^3 - cx^2 + c^q x - 1$ in $F_{q^2}[x]$ and the set of irreducible polynomials of the form $x^3 + ux^2 - tx + v$ in $F_q[x]$. This correspondence together with the previous one provides an even easier way to generate irreducible polynomials $F(c, x)$.

In Section 3, we discuss several examples. The first example given in Section 3.1 deals with irreducible polynomials over F_p. Section 3.2 explains how to decide whether a given element t in F_q^* is a square. This plays a crucial role in finding irreducible polynomials $F(c, x)$ in extension fields since the correspondences mentioned above are described via a quadratic nonresidue t. In Section 3.3, we give examples of irreducible polynomials $F(c, x)$ in extension fields. Finding irreducible polynomials over extension fields is computationally somewhat complicated. We will use multiplication tables of normal bases to take care of the difficulty. For the concept of multiplication tables, refer to [4].

2. Cubic polynomial $F(c, x) = x^3 - cx^2 + c^q x - 1$ over F_{q^2}

In this section we will show the two one to one correspondences mentioned in the introduction. Let p be an odd prime and fix a quadratic nonresidue t in F_q, where $q = p^m$. Note that a quadratic nonresidue always exists for $p \neq 2$. Let α be an element in F_{q^2} satisfying $\alpha^2 = t$. Then $F_{q^2} = F_q(\alpha)$ and $F_{q^6} = F_{q^3}(\alpha)$, and α satisfies $\alpha^q = (\alpha^2)^{\frac{q-1}{2}}\alpha = t^{\frac{q-1}{2}}\alpha = -\alpha$. For an element c in F_{q^2}, define a cubic polynomial $F(c, x)$ in $F_{q^2}[x]$ by $F(c, x) = x^3 - cx^2 + c^q x - 1$. Let h_1, h_2 and h_3 be the roots of $F(c, x)$. As in [1], one can check $F(c, h_i^{-q}) = 0$, so that $\{h_1, h_2, h_3\} = \{h_1^{-q}, h_2^{-q}, h_3^{-q}\}$. Thus the roots of F satisfy one of the following three:

(i) $h_i = h_i^{-q}$ for $i = 1, 2, 3$,
(ii) $h_1 = h_1^{-q}$, $h_2 = h_3^{-q}$, $h_3 = h_2^{-q}$,
(iii) $h_1 = h_2^{-q}$, $h_2 = h_3^{-q}$, $h_3 = h_1^{-q}$.

Remark 1. (1) Cases (ii) and (iii) should be understood as to hold after a suitable rearrangement of h_1, h_2 and h_3 if necessary.

(2) We classify $F(c,x)$ into types (F-I), (F-II), and (F-III) if the roots of $F(c,x)$ satisfy (i), (ii), and (iii), respectively.

(3) If $h_i = h_i^{-q}$, then h_i is in F_{q^2}. Hence if F is irreducible, then it is of type (F-III).

2.1. First one to one correspondence

In this subsection, we prove the first one to one correspondence. Suppose that $F(x) = F(c,x) = x^3 - cx^2 + c^q x - 1$ is irreducible over F_{q^2}. Since $F_{q^2} = F_q(\alpha)$, we can write c as $c = m + n\alpha$ for some $m, n \in F_q$. Note that if $m = -1$, then $c^q + c = (-1 + n\alpha)^q + (-1 + n\alpha) = -2$, so that $F(-1) = 0$, which contradicts the irreducibility of $F(x)$. Thus $m \neq -1$. Since F is of type (F-III), $h_i = h_i^{-q^3}$ for $i = 1, 2, 3$. So the norm of a root h of $F(c,x)$ from F_{q^6} to F_{q^3} equals 1. Hence, by Hilbert theorem 90, $h = g^{q^3-1}$ for some $g \in F_{q^6}$. Since $F_{q^6} = F_{q^3}(\alpha)$, $g = \gamma_1 + \gamma_2\alpha$ for some γ_1, $\gamma_2 \in F_{q^3}$. So we have $h = g^{q^3-1} = (\gamma_1 + \gamma_2\alpha)^{q^3-1}$. Note that $\alpha^{q^3} = (\alpha^{q^2})^q = \alpha^q = -\alpha$. Thus $\gamma_1 \neq 0$, for otherwise, $h = g^{q^3-1} = \frac{-\gamma_2\alpha}{\gamma_2\alpha} = -1$, which cannot happen since $F(c,x)$ is irreducible. Hence, $h = g^{q^3-1} = (\gamma_1(1 + \frac{\gamma_2}{\gamma_1}\alpha))^{q^3-1} = (1 + \beta\alpha)^{q^3-1}$, where $\beta = \frac{\gamma_2}{\gamma_1}$. Therefore, for each i, $1 \leq i \leq 3$, there is a $\beta_i \in F_{q^3}$ such that $h_i = (1 + \beta_i\alpha)^{q^3-1}$. Now we compare the coefficients of the equation

$$\begin{aligned} F(c,x) &= x^3 - cx^2 + c^q x - 1 \\ &= (x - (1 + \beta_1\alpha)^{q^3-1})(x - (1 + \beta_2\alpha)^{q^3-1})(x - (1 + \beta_3\alpha)^{q^3-1}). \end{aligned}$$

Since

$$(1 + \beta_i\alpha)^{q^3-1} = \frac{1 - \beta_i\alpha}{1 + \beta_i\alpha}$$

by comparing the constant terms, we have

$$\frac{(1 - \beta_1\alpha)(1 - \beta_2\alpha)(1 - \beta_3\alpha)}{(1 + \beta_1\alpha)(1 + \beta_2\alpha)(1 + \beta_3\alpha)} = 1,$$

from which we get

$$\beta_1 + \beta_2 + \beta_3 = -\beta_1\beta_2\beta_3 t.$$

And also by reading the coefficients of x^2, we obtain

$$\begin{aligned} c &= m + n\alpha \\ &= \frac{1 - \beta_1\alpha}{1 + \beta_1\alpha} + \frac{1 - \beta_2\alpha}{1 + \beta_2\alpha} + \frac{1 - \beta_3\alpha}{1 + \beta_3\alpha} \\ &= \frac{3 - (\beta_1\beta_2 + \beta_2\beta_3 + \beta_3\beta_1)t + ((\beta_1 + \beta_2 + \beta_3) - 3\beta_1\beta_2\beta_3 t)\alpha}{1 + (\beta_1\beta_2 + \beta_2\beta_3 + \beta_3\beta_1)t}. \end{aligned}$$

So

$$\begin{aligned} m &= \frac{3-(\beta_1\beta_2+\beta_2\beta_3+\beta_3\beta_1)t}{1+(\beta_1\beta_2+\beta_2\beta_3+\beta_3\beta_1)t}, \\ n &= \frac{-4\beta_1\beta_2\beta_3 t}{1+(\beta_1\beta_2+\beta_2\beta_3+\beta_3\beta_1)t}. \end{aligned}$$

Therefore

$$\frac{n}{m+1} = -\beta_1\beta_2\beta_3 t = \beta_1+\beta_2+\beta_3, \ \frac{3-m}{t(m+1)} = \beta_1\beta_2+\beta_2\beta_3+\beta_3\beta_1.$$

Hence

$$x^3 - \frac{n}{m+1}x^2 + \frac{3-m}{t(m+1)}x + \frac{n}{t(m+1)} = (x-\beta_1)(x-\beta_2)(x-\beta_3).$$

Note that this polynomial is irreducible over F_q since all β_i's are in F_{q^3}, but not in F_q.

To summarize, for each irreducible polynomial $F(x) = F(c,x) = x^3 - cx^2 + c^q x - 1$ in $F_{q^2}[x]$ with $c = m + n\alpha$, we associate an irreducible polynomial $G(x) = x^3 - \frac{n}{m+1}x^2 + \frac{3-m}{t(m+1)}x + \frac{n}{t(m+1)}$ in $F_q[x]$. Note that $G(x)$ is a polynomial of the form $x^3 - atx^2 + bx + a$.

Conversely, suppose an irreducible polynomial $G(x) = x^3 - atx^2 + bx + a$ in $F_q[x]$ is given. Note that $bt \neq -1$, for otherwise, ta would be a root of $G(x)$. Let β_1, β_2 and β_3 be the roots of $G(x)$. By comparing the coefficients of

$$x^3 - atx^2 + bx + a = (x-\beta_1)(x-\beta_2)(x-\beta_3),$$

we have

$$\beta_1+\beta_2+\beta_3 = -\beta_1\beta_2\beta_3 t.$$

Hence

$$(1+\beta_1\alpha)^{q^3-1}(1+\beta_2\alpha)^{q^3-1}(1+\beta_3\alpha)^{q^3-1} = \frac{(1-\beta_1\alpha)(1-\beta_2\alpha)(1-\beta_3\alpha)}{(1+\beta_1\alpha)(1+\beta_2\alpha)(1+\beta_3\alpha)} = 1.$$

Therefore

$$\begin{aligned} &(1+\beta_1\alpha)^{q^3-1}(1+\beta_2\alpha)^{q^3-1} + (1+\beta_2\alpha)^{q^3-1}(1+\beta_3\alpha)^{q^3-1} \\ &\quad + (1+\beta_3\alpha)^{q^3-1}(1+\beta_1\alpha)^{q^3-1} \\ &= \frac{1}{(1+\beta_3\alpha)^{q^3-1}} + \frac{1}{(1+\beta_1\alpha)^{q^3-1}} + \frac{1}{(1+\beta_2\alpha)^{q^3-1}} \\ &= \frac{1+\beta_1\alpha}{1-\beta_1\alpha} + \frac{1+\beta_2\alpha}{1-\beta_2\alpha} + \frac{1+\beta_3\alpha}{1-\beta_3\alpha} \\ &= \left(\frac{1-\beta_1\alpha}{1+\beta_1\alpha} + \frac{1-\beta_2\alpha}{1+\beta_2\alpha} + \frac{1-\beta_3\alpha}{1+\beta_3\alpha}\right)^q. \end{aligned}$$

The last equality holds since we may assume $\beta_1^q = \beta_2, \beta_2^q = \beta_3$ and $\beta_3^q = \beta_1$. Put

$$F(x) = (x-(1+\beta_1\alpha)^{q^3-1})(x-(1+\beta_2\alpha)^{q^3-1})(x-(1+\beta_3\alpha)^{q^3-1}).$$

Then $F(x)$ is irreducible over F_{q^2} since the roots of F are conjugate to each other over F_{q^2}. Put

$$c = (1+\beta_1\alpha)^{q^3-1} + (1+\beta_2\alpha)^{q^3-1} + (1+\beta_3\alpha)^{q^3-1}.$$

Then above computation shows that the coefficient of x equals c^q. Therefore, $F(x)$ is of the form $F(x) = x^3 - cx^2 + c^q x - 1$. Note that

$$\begin{aligned} c &= (1+\beta_1\alpha)^{q^3-1} + (1+\beta_2\alpha)^{q^3-1} + (1+\beta_3\alpha)^{q^3-1} \\ &= \frac{3 - (\beta_1\beta_2+\beta_2\beta_3+\beta_3\beta_1)t + ((\beta_1+\beta_2+\beta_3) - 3\beta_1\beta_2\beta_3 t)\alpha}{1+(\beta_1\beta_2+\beta_2\beta_3+\beta_3\beta_1)t} \\ &= \frac{3-bt+4at\alpha}{1+bt}. \end{aligned}$$

Hence for a given irreducible polynomial $G(x) = x^3 - atx^2 + bx + a$ in $F_q[x]$, we can associate an irreducible polynomial $F(x) = F(c,x) = x^3 - cx^2 + c^q x - 1$ in $F_{q^2}[x]$ with $c = \frac{3-bt+4at\alpha}{1+bt}$. Therefore, we have the following theorem.

Theorem 1. *There is a one to one correspondence between the set of irreducible polynomials in $F_{q^2}[x]$ of the form $x^3 - cx^2 + c^q x - 1$ and the set of irreducible polynomials in $F_q[x]$ of the form $x^3 - atx^2 + bx + a$. The correspondence is given by:*

For a given $F(x) = F(c,x) = x^3 - cx^2 + c^q x - 1$ with $c = m + n\alpha$, we associate $G(x) = x^3 - \frac{n}{m+1}x^2 + \frac{3-m}{t(m+1)}x + \frac{n}{t(m+1)}$.

Conversely, for a given $G(x) = x^3 - atx^2 + bx + a$, we associate $F(c,x) = x^3 - cx^2 + c^q x - 1$ with $c = \frac{3-bt}{1+bt} + \frac{4at}{1+bt}\alpha$.

Proof. It remains to check that the correspondence is one to one. Suppose that $F(x) = x^3 - cx^2 + c^q x - 1$ is given with $c = m + n\alpha$. Then we get $G(x) = x^3 - \frac{n}{m+1}x^2 + \frac{3-m}{t(m+1)}x + \frac{n}{t(m+1)}$. The cubic polynomial over F_{q^2} obtained from $G(x)$ is $F_1(x) = x^3 - c_1 x^2 + c_1^q x - 1$ with $c_1 = \frac{-tb+3}{tb+1} + \frac{4ta}{tb+1}\alpha$, where $a = \frac{n}{t(m+1)}$ and $b = \frac{3-m}{t(m+1)}$. Since

$$c_1 = \frac{-t\frac{3-m}{t(m+1)} + 3}{t\frac{3-m}{t(m+1)} + 1} + \frac{4t\frac{n}{t(m+1)}}{t\frac{3-m}{t(m+1)} + 1}\alpha = m + n\alpha = c,$$

we get $F(c,x)$ back. Conversely, if we start with G and find the corresponding F, then the polynomial in $F_q[x]$ obtained from F is G again. Therefore, the correspondence is one to one. □

2.2. Types of F and G

Let $G(x)$ be any cubic polynomial in $F_q[x]$ of the form $G(x) = x^3 - atx^2 + bx + a$ with $bt \neq -1$. We classify $G(x)$ into three types:

(G-I) $G(x)$ factors into a product of three linear polynomials in $F_q[x]$,

(G-II) $G(x)$ factors into a product of a linear polynomial and a quadratic polynomial in $F_q[x]$,

(G-III) $G(x)$ is irreducible in $F_q[x]$.

Let $F(x)$ be a cubic polynomial in $F_{q^2}[x]$ of the form $F(x) = F(c,x) = x^3 - cx^2 + c^q x - 1$ in $F_{q^2}[x]$ with $m \neq -1$, where $c = m + n\alpha$. Regardless of the irreducibility, we associate $F(c,x)$ to $G(x)$ as in Theorem 1. The same argument of the proof of Theorem 1 shows that this is a one to one correspondence. In this subsection, we will show that under this correspondence, the types of F and G agree.

Corollary 2. *Under the above correspondence, the types of F and G agree.*

Proof. Theorem 1 says that if one of F or G is of type III, then so is the other. Thus it remains to check that the correspondence preserves types I and II. For this, it is enough to show that the number of roots of F satisfying $h^{-q} = h$ equals the number of roots of G in F_q.

Note that a root h of $F(c,x)$ satisfies $h = h^{-q}$ if and only if the norm of h from F_{q^2} to F_q equals 1. By Hilbert theorem 90, the norm of h equals 1 if and only if $h = u^{q-1}$ for some u in F_{q^2}. From the condition $m \neq -1$, one can check that $h = u^{q-1}$ for some $u \in F_{q^2}$ if and only if h is of the form $h = (1+d\alpha)^{q-1}$ for some $d \in F_q$. Thus it suffices to show that $F(c,h) = 0$ if and only if $G(d) = 0$, where $h = (1+d\alpha)^{q-1}$ with $d \in F_q$.

Suppose that $F(c,h) = 0$. Then

$$F(c,h) = \left(\frac{1-d\alpha}{1+d\alpha}\right)^3 - (m+n\alpha)\left(\frac{1-d\alpha}{1+d\alpha}\right)^2 + (m-n\alpha)\left(\frac{1-d\alpha}{1+d\alpha}\right) - 1 = 0.$$

By clearing the denominators, we have

$$(1-d\alpha)^3 - (m+n\alpha)(1-d\alpha)^2(1+d\alpha) + (m-n\alpha)(1-d\alpha)(1+d\alpha)^2 - (1+d\alpha)^3 = 0.$$

This yields

$$t(m+1)d^3 - ntd^2 + (3-m)d + n = 0.$$

Therefore

$$G(d) = d^3 - \frac{n}{m+1}d^2 + \frac{3-m}{t(m+1)}d + \frac{n}{t(m+1)} = 0.$$

The converse can be justified by reversing the order of above computations. This proves the corollary. □

2.3. Second one to one correspondence

In this subsection, we will prove the second correspondence. Namely, we will show that there is a one-to-one correspondence between the set of irreducible polynomials in $F_{q^2}[x]$ of the form $x^3 - cx^2 + c^q x - 1$ and the set of irreducible polynomials in $F_q[x]$ of the form $x^3 + ux^2 - tx + v$. This correspondence is achieved by associating $F(x) = x^3 - cx^2 + c^q x - 1 = (x - (1+\beta_1\alpha)^{q^3-1})(x - (1+\beta_2\alpha)^{q^3-1})(x - (1+\beta_3\alpha)^{q^3-1})$ to $\widetilde{G}(x) = (x - \frac{1}{\beta_1})(x - \frac{1}{\beta_2})(x - \frac{1}{\beta_3})$ instead of $G(x) = (x-\beta_1)(x-\beta_2)(x-\beta_3)$. If $G(x) = (x-\beta_1)(x-\beta_2)(x-\beta_3) = x^3 - atx^2 + bx + a$, then $\widetilde{G}(x) = (x - \frac{1}{\beta_1})(x - \frac{1}{\beta_2})(x - \frac{1}{\beta_3}) = x^3 + \frac{b}{a}x^2 - tx + \frac{1}{a}$.

Thus $\widetilde{G}(x)$ is of the form x^3+ux^2-tx+v with $u=\frac{b}{a}$ and $v=\frac{1}{a}$. Conversely, if $\widetilde{G}(x)=x^3+ux^2-tx+v$, then $G=(\widetilde{\widetilde{G}})(x)=x^3-\frac{t}{v}x^2+\frac{u}{v}x+\frac{1}{v}$.

This correspondence between $G(x)$ and $\widetilde{G}(x)$ gives a one to one correspondence between $F(x)$ and $\widetilde{G}(x)$. To be precise, let $F(c,x)=x^3-cx^2+c^qx-1$, where $c=m+n\alpha$. Then we have $G(x)=x^3-\frac{n}{m+1}x^2+\frac{3-m}{t(m+1)}x+\frac{n}{t(m+1)}$. From $G(x)$, we get $\widetilde{G}(x)=x^3+\frac{3-m}{n}x^2-tx+\frac{t(m+1)}{n}$. Conversely, suppose $\widetilde{G}(x)=x^3+ux^2-tx+v$ is given. Then we get $G(x)=x^3-\frac{t}{v}x^2+\frac{u}{v}x+\frac{1}{v}$. And from $G(x)$, we obtain $F(c,x)=x^3-cx^2+c^qx-1$ with $c=\frac{-t\frac{u}{v}+3}{t\frac{u}{v}+1}+\frac{4t\frac{1}{v}}{t\frac{u}{v}+1}\alpha=\frac{-tu+3v}{tu+v}+\frac{4t}{tu+v}\alpha$.

So we have the following theorem.

Theorem 3. *There is a one-to-one correspondence between the set of irreducible polynomials in $F_{q^2}[x]$ of the form $x^3-cx^2+c^qx-1$ and the set of irreducible polynomials in $F_q[x]$ of the form x^3+ux^2-tx+v. The correspondence is given by:*

For a given $F(c,x)=x^3-cx^2+c^qx-1$ with $c=m+n\alpha$, we associate $\widetilde{G}(x)=x^3+\frac{3-m}{n}x^2-tx+\frac{t(m+1)}{n}$.

Conversely, for a given $\widetilde{G}(x)=x^3+ux^2-tx+v$, we associate $F(c,x)=x^3-cx^2+c^qx-1$ with $c=\frac{-tu+3v}{tu+v}+\frac{4t}{tu+v}\alpha$.

3. Examples of irreducible polynomials $F(c,x)$

In this section we study examples of irreducible polynomials $F(c,x)$ in $F_{q^2}[x]$ by using the methods developed in Section 2.

3.1. Examples when $q=p$

In this subsection, we will find irreducible polynomials $F(c,x)$ in $F_{p^2}[x]$ when $p\not\equiv\pm1 \mod 7$. This example can be generalized to other modulii. Examples of irreducible polynomials $F(c,x)$ over extension fields will be given later.

Let $\zeta=\zeta_7$ be a primitive 7th root of 1. If $p\equiv 3$ or $5 \mod 7$, then $F_p(\zeta)=F_{p^6}$. So $F_p(\zeta+\zeta^{-1})=F_{p^3}$. If $p\equiv 2$ or $4 \mod 7$, then $F_p(\zeta)=F_{p^3}$. Note that $F_p(\zeta+\zeta^{-1})=F_{p^3}$ in this case, too. Thus conjugates of $\zeta+\zeta^{-1}$ over F_p are $\zeta+\zeta^{-1}$, $\zeta^2+\zeta^{-2}$ and $\zeta^4+\zeta^{-4}$. Note that

$$(\zeta+\zeta^{-1})+(\zeta^2+\zeta^{-2})+(\zeta^4+\zeta^{-4})=-1,$$

$$(\zeta+\zeta^{-1})(\zeta^2+\zeta^{-2})+(\zeta^2+\zeta^{-2})(\zeta^4+\zeta^{-4})+(\zeta+\zeta^{-1})(\zeta^4+\zeta^{-4})=-2,$$

and $(\zeta+\zeta^{-1})(\zeta^2+\zeta^{-2})(\zeta^4+\zeta^{-4})=1$.

Therefore $\mathrm{Irr}\,(\zeta+\zeta^{-1},F_p)=x^3+x^2-2x-1$. Let

$$H(x)=\mathrm{Irr}\,(\zeta+\zeta^{-1},F_p)=x^3+x^2-2x-1.$$

Suppose that $p\equiv\pm3 \mod 8$. Then 2 is a quadratic nonresidue mod p. So $H(x)$ itself is of the form $\widetilde{G}(x)=x^3+ux^2-tx+v$ with $u=1,t=2$

and $v = -1$. Thus by using Theorem 3, we obtain an irreducible polynomial $F(c,x) = x^3 - cx^2 + c^p x - 1$ with $c = -5 + 8\alpha$, where $\alpha^2 = t = 2$.

We can play around with $H(x)$ a little more. Suppose that $p \equiv 3 \mod 4$, and consider

$$H(x+2) = \mathrm{Irr}\,(\zeta + \zeta^{-1} - 2, F_p) = x^3 + 7x^2 + 14x + 7.$$

Since $p \equiv 3 \mod 4$, -1 is a quadratic nonresidue mod p. Thus $H(x+2)$ is an irreducible polynomial of the form $G(x) = x^3 - atx^2 + bx + a$ with $a = 7$, $b = 14$ and $t = -1$. Hence, by Theorem 1, the polynomial $F(c,x) = x^3 - cx^2 + c^p x - 1$ with $c = -\frac{17}{13} + \frac{28}{13}\alpha$ is irreducible over F_{p^2}, where $\alpha^2 = -1$.

Next, we consider

$$H(x+1) = \mathrm{Irr}\,(\zeta + \zeta^{-1} - 1, F_p) = x^3 + 4x^2 + 3x - 1.$$

This polynomial cannot be of the form $G(x) = x^3 - atx^2 + bx + a$ for any p since 4 is a square. But if -3 is a quadratic nonresidue mod p, then $x^3 + 4x^2 + 3x - 1$ is of the form $\widetilde{G}(x) = x^3 + ux^2 - tx + v$ with $u = 4$, $v = -1$ and $t = -3$. Hence we get an irreducible polynomial $F(c,x) = x^3 - cx^2 + c^p x - 1$ with $c = -\frac{9}{13} + \frac{12}{13}\alpha$, where $\alpha^2 = -3$. In this way, we can find plenty of irreducible polynomials $F(c,x)$ from a single irreducible polynomial $H(x)$ in $F_p[x]$.

3.2. Squares in F_q

To determine irreducible polynomials $F(c,x)$ from $G(x)$ or $\widetilde{G}(x)$, we need a quadratic nonresidue t in F_q. When $F_q = F_p$, one can easily test whether a given $t \in F_p^*$ is a quadratic nonresidue by just computing the Legendre symbol $(\frac{t}{p})$. In this subsection, we prove a criterion on whether a given t in an extension field F_q^* is a square or not.

Lemma 4. *Let $q = p^m$. Then t is a square in F_q^* if and only if $N(t)$ is a square in F_p^*, where N is the norm map from F_q to F_p.*

Proof. Suppose t is a square in F_q^*. So $t = \gamma^2$ for some $\gamma \in F_q^*$. Then $N(t) = N(\gamma^2) = (N(\gamma))^2$. Thus $N(t)$ is a square in F_p^*. Conversely, suppose $N(t) = d^2$ for some $d \in F_p^*$. Since the norm map is surjective, there is an element $t' \in F_q^*$ such that $N(t') = d$. Then we have $N(t'^2) = d^2 = N(t)$. So, by Hilbert theorem 90, $t = t'^2 \xi^{p-1}$ for some $\xi \in F_q^*$. Hence $t = (\xi^{\frac{p-1}{2}} t')^2$ is a square in F_q^*. □

3.3. Examples over extension fields

Let $q = p^m$ as before. In this subsection, we will find irreducible polynomials $F(c,x)$ over extension fields F_{q^2} under the following restrictions on m and p: (i) $6m + 1 = r$ is a prime, (ii) p is a primitive root mod r, i.e., the multiplicative order of p in $(Z/rZ)^*$ is $r - 1 = 6m$. Note that there are infinitely many such m's and p's: Choose a prime r and a primitive root g mod r such that $r \equiv 1$

mod 6. Then a prime p satisfying $p \equiv g \mod r$ together with $m = \frac{r-1}{6}$ satisfies above conditions.

A brief outline to find irreducible polynomials is as follows. Let $\zeta = \zeta_r$ be a primitive rth root of 1. So we have $F_p(\zeta) = F_{p^{6m}} = F_{q^6}$ with $q = p^m$. Set $\beta = Tr_{F_{q^6}/F_{q^3}}(\zeta) = \zeta + \zeta^{-1}$. Let $H(x) = \mathrm{Irr}\,(\beta, F_q)$ be the irreducible polynomial for β over F_q. By using the multiplication table for β over F_p which can be obtained from that of ζ over F_p, we compute $H(x)$. Then by a change of variables of $H(x)$ to $H(x+k)$ if necessary, we get an irreducible polynomial of the form either $x^3 - atx^2 + bx + a$ or $x^3 + ux^2 - tx + v$. Then by using the correspondences in Section 2, we obtain $F(c, x)$.

Now we study examples. During the computations, N will always mean the norm map from F_q to F_p.

3.3.1. $m = 2$, $p \equiv 2 \mod 13$. Let $\zeta = \zeta_{13}$ be a primitive 13th root of 1. Note that 2 is a primitive root mod 13. Thus if $p \equiv 2 \mod 13$, then $F_p(\zeta) = F_{p^{12}} = F_{q^6}$ with $q = p^2$. Let $\beta = \mathrm{Tr}_{F_{q^6}/F_{q^3}}(\zeta) = \zeta + \zeta^{-1}$ and $\omega = \mathrm{Tr}_{F_{q^3}/F_q}(\beta) = \mathrm{Tr}_{F_{q^6}/F_q}(\zeta)$. The multiplication table of ζ with respect to the normal basis $\{\zeta, \zeta^p, \zeta^{p^2}, \ldots, \zeta^{p^{11}}\}$ over F_p is

$$\begin{bmatrix}
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
-1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{bmatrix}.$$

This table should be interpreted as $\zeta \cdot \zeta = \zeta^p$, $\zeta \cdot \zeta^p = \zeta^{p^4}$, and so on. Note that β and ω are normal elements for F_{q^3} and F_q, respectively over F_p. From the above multiplication table of ζ over F_p, we can read the multiplication tables of β and ω:

$$\begin{bmatrix}
-2 & -1 & -2 & -2 & -2 & -2 \\
1 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 & 1 & 0 \\
0 & 0 & 1 & 0 & 0 & 1 \\
0 & 1 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 1
\end{bmatrix} \quad \text{for } \beta,$$

and

$$\begin{bmatrix} -4 & -3 \\ 3 & 3 \end{bmatrix} \quad \text{for } \omega.$$

Note that $\omega+\omega^p = \mathrm{Tr}_{F_q/F_p}(\omega) = \mathrm{Tr}_{F_{q^6}/F_p}(\zeta) = -1$, since $\mathrm{Irr}(\zeta, F_p) = x^{12} + x^{11}+\cdots+x+1$. From the multiplication table for ω, we have $\omega\cdot\omega^p = 3\omega+3\omega^p = 3(\omega+\omega^p) = -3$. So

$$\mathrm{Irr}(\omega, F_p) = (x-\omega)(x-\omega^p) = x-(\omega+\omega^p)x+\omega\cdot\omega^p = x^2+x-3.$$

Now we compute

$$H(x) = \mathrm{Irr}(\beta, F_q) = (x-\beta)(x-\beta^q)(x-\beta^{q^2}).$$

Clearly $\beta+\beta^q+\beta^{q^2} = \mathrm{Tr}_{F_{q^3}/F_q}(\beta) = \omega$, and $\beta\cdot\beta^q+\beta^q\cdot\beta^{q^2}+\beta\cdot\beta^{q^2} = \mathrm{Tr}_{F_{q^3}/F_q}(\beta\cdot\beta^q)$. And the multiplication table for β says $\beta\cdot\beta^q = \beta\cdot\beta^{p^2} = \beta^{p^3}+\beta^{p^4}$. Thus $\mathrm{Tr}_{F_{q^3}/F_q}(\beta\cdot\beta^q) = \mathrm{Tr}_{F_{q^3}/F_q}(\beta^{p^3}+\beta^{p^4}) = \omega^{p^3}+\omega^{p^4} = \omega^p+\omega = -1$. Finally, we have $\beta\cdot\beta^q\cdot\beta^{q^2} = \beta\cdot(\beta\cdot\beta^q)^q = \beta\cdot(\beta^{p^3}+\beta^{p^4})^{p^2} = (\beta+\beta^{p^2}+\beta^{p^4})^p - 2(\beta+\beta^p+\cdots+\beta^{p^5}) = \omega^p+2 = 1-\omega$. Therefore

$$H(x) = \mathrm{Irr}(\beta, F_q) = x^3-\omega x^2-x+\omega-1.$$

Let us consider

$$H(x-1) = \mathrm{Irr}(\beta+1, F_q) = x^3-(\omega+3)x^2+2(\omega+1)x-1.$$

Since $\mathrm{Irr}(\omega+1, F_p) = (x-1)^2+(x-1)-3 = x^2-x-3$, $N(\omega+1) = -3$. Thus $N(-2(\omega+1)) = (-2)^2(-3)$. Note that this is not a square in F_p if we assume that $p \equiv 2 \mod 3$. Hence $t = -2(\omega+1)$ is a quadratic nonresidue in F_q by Lemma 4. So $H(x-1)$ is of the form $\widetilde{G}(x) = x^3+ux^2-tx+v$ with $u = -(\omega+3), v = -1$ and $t = -2(\omega+1)$. Hence by Theorem 3, we get $c = \frac{-6\omega-15}{6\omega+11} + \frac{-8(\omega+1)}{6\omega+11}\alpha$, where α satisfies $\alpha^2 = t = -2(\omega+1)$. From the equation $\omega^2+\omega-3 = 0$, we have $\frac{1}{6\omega+11} = \frac{6}{53}\omega - \frac{5}{53}$. Therefore we obtain an irreducible polynomial $F(c,x) = x^3-cx^2+c^qx-1$ with $c = -\frac{3}{53}(8\omega+11)+\frac{8}{53}(5\omega-13)\alpha$, where $\alpha^2 = -2(\omega+1)$.

3.3.2. $m = 3$, $p \equiv 2 \mod 19$. Let $\zeta = \zeta_{19}$ be a primitive 19th root of 1. Then 2 is a primitive root mod 19, and so if $p \equiv 2 \mod 19$, then $F_p(\zeta) = F_{p^{18}} = F_{q^6}$ with $q = p^3$. Let $\beta = \mathrm{Tr}_{F_{q^6}/F_{q^3}}(\zeta) = \zeta+\zeta^{-1}$ and $\omega = \mathrm{Tr}_{F_{q^3}/F_q}(\beta)$. As before, the multiplication tables of ζ, β and ω with respect to the obvious normal bases over F_p are

$$\begin{bmatrix}
0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0\\
0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0\\
0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1\\
-1&-1&-1&-1&-1&-1&-1&-1&-1&-1&-1&-1&-1&-1&-1&-1&-1&-1\\
0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0\\
0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0\\
0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0
\end{bmatrix} \quad \text{for } \zeta,$$

$$\begin{bmatrix} -2 & -1 & -2 & -2 & -2 & -2 & -2 & -2 & -2 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \quad \text{for } \beta,$$

and

$$\begin{bmatrix} -4 & -5 & -4 \\ 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix} \quad \text{for } \omega.$$

As in Example 2, from the multiplication table for ω, we see that

$$\mathrm{Irr}\,(\omega, F_p) = x^3 + x^2 - 6x - 7.$$

Let

$$H(x) = \mathrm{Irr}\,(\beta, F_q) = (x-\beta)(x-\beta^q)(x-\beta^{q^2}).$$

Since $\beta + \beta^q + \beta^{q^2} = Tr_{F_{q^3}/F_q}(\beta) = \omega$, $\beta \cdot \beta^q + \beta^q \cdot \beta^{q^2} + \beta \cdot \beta^{q^2} = (\omega^2 - 5)$ and $\beta \cdot \beta^q \cdot \beta^{q^2} = 6 - \omega^2$, we have

$$H(x) = \mathrm{Irr}\,(\beta, F_q) = x^3 - \omega x^2 + (\omega^2 - 5)x + \omega^2 - 6.$$

Note that $N\left(\frac{\omega}{\omega^2-6}\right) = \frac{N(\omega)}{N(\omega^2-6)} = 7$. Thus if 7 is a quadratic nonresidue mod p, then $H(x)$ is of the form $G(x) = x^3 - atx^2 + bx + a$ with $a = \omega^2 - 6$, $b = \omega^2 - 5$ and $t = \frac{\omega}{\omega^2-6}$. Therefore we get $F(c, x) = x^3 - cx^2 + c^q x - 1$ with $c = \frac{4\omega^2-\omega-25}{\omega+1} + \frac{4(-\omega^2+7)}{\omega+1}\alpha$, where $\alpha^2 = t = \frac{\omega}{\omega^2-6}$. Since $\omega^3 + \omega^2 - 6\omega - 7 = 0$, we have $\frac{1}{\omega+1} = \omega^2 - 6$. Hence if $\left(\frac{7}{p}\right) = -1$, then we obtain an irreducible polynomial $F(c, x)$ with $c = (-20\omega^2 + 4\omega + 115) + 4(6\omega^2 - \omega - 35)\alpha$, where $\alpha^2 = t = \frac{\omega}{\omega^2-6} = \omega^2 + \omega$.

References

[1] A. K. Lenstra and E. R. Verheul, *The XTR public key system*, Advances in cryptology—CRYPTO 2000 (Santa Barbara, CA), 1–19, Lecture Notes in Comput. Sci., 1880, Springer, Berlin, 2000.

[2] ———, *Key improvements to XTR*, Advances in cryptology—ASIACRYPT 2000 (Kyoto), 220–233, Lecture Notes in Comput. Sci., 1976, Springer, Berlin, 2000.

[3] ———, *Fast irreducibility and subgroup membership testing in XTR*, Public key cryptography (Cheju Island, 2001), 73–86, Lecture Notes in Comput. Sci., 1992, Springer, Berlin, 2001.

[4] A. J. Menezes, *Applications of Finite Fields*, Kluwer Academic Publishers, 1993.

HYUNG DON KIM
DEPARTMENT OF MATHEMATICS
INHA UNIVERSITY
INCHEON, KOREA
E-mail address: hdkim@math.inha.ac.kr

JAE MOON KIM
DEPARTMENT OF MATHEMATICS
INHA UNIVERSITY
INCHEON, KOREA
E-mail address: jmkim@math.inha.ac.kr

IKKWON YIE
DEPARTMENT OF MATHEMATICS
INHA UNIVERSITY
INCHEON, KOREA
E-mail address: ikyie@math.inha.ac.kr