ON THE ORDER OF THE POLYNOMIAL $x^p - x - a$

XIWANG CAO

ABSTRACT. In this note, we prove that the order of $x^p - x - 1 \in \mathbb{F}_p[x]$ is $\frac{p^p-1}{p-1}$, where p is a prime and $\mathbb{F}_p$ is the finite field of size p. As a consequence, it is shown that $x^p - x - a \in \mathbb{F}_p[x]$ is primitive if and only if a is a primitive element in $\mathbb{F}_p$.

1. INTRODUCTION

Let $\mathbb{F}_q$ be the finite field of size q, where $q = p^e$ is a prime power. A monic polynomial $f(x) = x^n + \sum_{i=1}^{n} a_i x^{n-i} \in \mathbb{F}_q[x]$ is said to be *primitive* if it is irreducible over $\mathbb{F}_q$ and any root of $f(x)$ can be used to generate the multiplicative group $\mathbb{F}_{q^n}^*$ of $\mathbb{F}_{q^n}$. The *order* of $f(x)$, denoted by $\mathrm{ord}(f)$, is the smallest positive integer r such that $f(x)|(x^r - 1)$ in $\mathbb{F}_q[x]$. When $f(x)$ is irreducible over $\mathbb{F}_q$, the order of $f(x)$ is equal to the order of its roots in the multiplicative group $\mathbb{F}_{q^n}^*$ (see [5, p. 77], Theorem 3.3). Therefore $f(x)$ is primitive if and only if the order of $f(x)$ is $q^n - 1$. Primitive polynomials are important objects in their own, and they are also important for various applications of finite fields. So it is of great interest to know whether for a given q and n there exists a primitive polynomial of degree n over $\mathbb{F}_q$ satisfying certain additional conditions. One such question is whether there exists a primitive polynomial $f(x) = x^n + \sum_{i=1}^{n} a_i x^{n-i}$ of degree n in $\mathbb{F}_q[x]$ with $a_1, a_2, \cdots, a_k$ prescribed, where $1 \le k \le n$. When $k = 1$, this question was settled by Cohen [1], Jungnickel and Vanstone [4] with a positive answer. When $k = 2$, we have the following result due to Han [3].

Result 1. *Let $n \ge 7$ be an integer, and let $a_1, a_2 \in \mathbb{F}_q$ be given, where q is an odd prime power. Then there always exists a primitive polynomial $f(x) \in \mathbb{F}_q[x]$ of the form $f(x) = x^n + \sum_{i=1}^{n} a_i x^{n-i}$.*

In this note, we consider polynomials of the form $g(x) = x^p - x - a \in \mathbb{F}_p[x]$. When $a = 1$, J. Y. Shi and Z. H. Wang [7] conjectured that $\mathrm{ord}(g) = \frac{p^p-1}{p-1}$, and verified the validity of his conjecture for ANY prime number $p \le 41$. We confirm this conjecture in this note by proving the following results.

Theorem 1.1. *The order of the polynomial $x^p - x - 1 \in \mathbb{F}_p[x]$ is $\frac{p^p-1}{p-1}$.*

Theorem 1.2. *The polynomial $x^p - x - a \in \mathbb{F}_p[x]$ is primitive if and only if a is primitive in $\mathbb{F}_p$.*

Theorem 1.3. *The polynomial $h(x) = x^{\frac{p^p-1}{p-1}} - x - 1$ is irreducible over $\mathbb{F}_p$.*

The main idea in our proofs of Theorem 1.1 and Theorem 1.2 is to use the following lemma, see [5, p. 123], Theorem 3.84.

Lemma 1.4. *Let p be a prime. Then the polynomial $x^p - x - a \in \mathbb{F}_p[x]$ is primitive if and only if a is a primitive element of $\mathbb{F}_p$ and $\mathrm{ord}(x^p - x - 1) = \frac{p^p-1}{p-1}$.*

The statement in Theorem 1.2 is quite simple. But we could not find it in the exisiting literature. Also by Lemma 1.4, it is easy to see that Theorem 1.2 is equivalent to Shi's Conjecture.

Key words and phrases. finite fields, primitive polynomials, primitive elements.

[1]Research supported in part by NNSF Grant 10771100.

We note that when $p = 2$, the aforementioned results are trivial. Thus in what follows, we always assume that p is an odd prime. In this case, we had to study the decomposition of the $p-$associate polynomial of the polynomial $x^p - x - 1$, and use a result on the q-*modulus* which is defined as follows.

Definition 1.5. *A finite-dimensional vector space M over $\mathbb{F}_q$ is called a $q-$modulus if $a^q \in M$ for every $a \in M$.*

A polynomial $L(x) \in \mathbb{F}_q[x]$ is called a $q-$polynomial if it has the form $L(x) = \sum_{i=0}^{m-1} a_i x^{q^i} \in \mathbb{F}_q[x]$. The following Lemmas are proved in [5].

Lemma 1.6. [5, p. 110, Theorem 3.63] *Let $f(x) = x^n + \sum_{i=0}^{n-1} a_i x^i$ be irreducible in $\mathbb{F}_q[x]$ and let $F(x) = x^{q^n} + \sum_{i=0}^{n-1} a_i x^{q^i}$ be its linearized $q-$associated. Then the degree of every irreducible factor of $F(x)/x$ in $\mathbb{F}_q[x]$ is equal to* $\mathrm{ord}(f(x))$.

Lemma 1.7. [5, p. 110 Theorem 3.65] *The monic polynomial $L(x)$ is a $q-$polynomial over $\mathbb{F}_q$ if and only if each root of $L(x)$ has the same multiplicity, which is* 1 *or a power of q, and the roots forms a $q-$modulus.*

2. Preliminaries

In order to prove the main results, we need to study some $p-$modulus and the related $p-$polynomials. The following Lemma is proved in [5].

Lemma 2.1. [5, p. 103, Theorem 3.52] *Let M be a linear subspace of $\mathbb{F}_{q^m}$, considered as a vector space over $\mathbb{F}_q$. Then for every nonnegative integer k the polynomial*

$$L(x) = \prod_{\beta \in M} (x - \beta)^{q^k}$$

is a $q-$polynomial over $\mathbb{F}_{q^m}$.

Let $L_1(x)$, $L_2(x)$ be two linearized polynomials over $\mathbb{F}_{q^m}$, we define *symbolic multiplication* of $L_1(x)$ and $L_2(x)$ by

$$L_1(x) \otimes L_2(x) = L_1(L_2(x)).$$

If $L(x), L_1(x)$ and $L_2(x)$ are $q-$polynomials satisfying $L(x) = L_1(x) \otimes L_2(x)$, then we say that $L_1(x)$ *symbolically divides* $L(x)$.

Definition 2.2. *The polynomials*

$$l(x) = \sum_{i=0}^{n} a_i x^i \text{ and } L(x) = \sum_{i=0}^{n} a_i x^{q^i}$$

over $\mathbb{F}_{q^m}$ are called $q-$associates of each other. More specifically, $l(x)$ is the conventional $q-$associate of $L(x)$ and $L(x)$ is the linearized $q-$associate of $l(x)$.

By these definitions, we have the following Lemma.

Lemma 2.3. [5, p. 108, Corollary 3.60] *Let $L_1(x)$ and $L(x)$ be $q-$polynomials over $\mathbb{F}_q$ with conventional $q-$associates $l_1(x)$ and $l_(x)$. Then $L_1(x)$ symbolically divides $L(x)$ if and only if $l_1(x)$ divides $l(x)$.*

Now, we have the following Lemma:

Lemma 2.4. *Let M and U be linear space over $\mathbb{F}_q$ and $U \subseteq M$. Define*

$$L_M(x) = \prod_{\beta \in M} (x - \beta), L_U(x) = \prod_{\gamma \in U} (x - \gamma).$$

Then there is a $q-$polynomial $L(x)$ such that

$$L_M(x) = L(L_U(x)).$$

In other words, $L_U(x)$ symbolically divides $L_M(x)$.

Proof. For every $\beta \in M$, there are elements $\gamma \in U, \beta' \in M/U$ such that $\beta = \beta' + \gamma$. Thus

$$\begin{aligned} L_M(x) &= \prod_{\beta' \in M/U} \prod_{\gamma \in U} (x - \gamma - \beta') \\ &= \prod_{\beta' \in M/U} L_U(x - \beta') \\ &= \prod_{\beta' \in M/U} \left[L_U(x) - L_U(\beta') \right]. \end{aligned}$$

Since L_U is $\mathbb{F}_q-$linear, $\{L_U(\beta') | \beta' \in M/U\}$ is a $\mathbb{F}_q-$linear space, thus by Lemma 2.1, there is a $q-$polynomial $L(x)$ such that

$$L_M(x) = L(L_U(x)).$$

□

3. The proofs

We note that Theorem 1.2 follows immediately from Theorem 1.1 and Lemma 1.4. Now we give the proof of Theorem 1.1.

Let $g(x) = x^p - x - 1$, $G(x) = x^{p^p} - x^p - x$. Firstly, we know that $g(x)$ is irreducible over $\mathbb{F}_p$ ([5, p.120], Corollary 3.79). Suppose that $\mathrm{ord}(g(x)) = e$ and denote $\frac{p^p-1}{p-1}$ by Q. Then by Lemma 1.6, we have

$$\begin{aligned} G(x) &= x \prod_{j=1}^{Q/e} \prod_{k=1}^{p-1} \prod_{i=0}^{e-1} (x - k\alpha_j^{p^i}) \\ &= x \prod_{j=1}^{Q/e} \prod_{i=0}^{e-1} (x^{p-1} - \alpha_j^{p^i(p-1)}) \end{aligned} \tag{3.1}$$

where α_j's are the non-conjugate roots of $G(x)$. We note that α can not be conjugate to $k\alpha$ for any $k(\neq 1) \in \mathbb{F}_p$, the reason of this fact is as follows. If $k\alpha = \alpha^{p^t}$ holds for an integer t, then $\alpha^{(p^t-1)(p-1)} = 1$. Now

$$\begin{aligned} \gcd(Q, p-1) &= \gcd(1 + p + p^2 + \cdots + p^{p-1}, p-1) \\ &= (1 + ((p-1)+1) + ((p-1)+1)^2 + \cdots + ((p-1)+1)^{p-1}, p-1) \\ &= \gcd(p, p-1) = 1, \end{aligned}$$

we have $\gcd(\frac{p^e-1}{p-1}, p-1) = \gcd(1 + p + p^2 + \cdots + p^{e-1}, p-1) = \gcd(e, p-1) = 1$. Thus we have

$$\begin{aligned} 1 &= \alpha^{\gcd((p^t-1)(p-1), p^e-1)} \\ &= \alpha^{(p-1)\gcd\left((p-1)\frac{p^t-1}{p-1}, \frac{p^e-1}{p-1}\right)} \\ &= \alpha^{(p-1)\gcd(\frac{p^t-1}{p-1}, \frac{p^e-1}{p-1})} \\ &= \alpha^{\gcd(p^t-1, p^e-1)}. \end{aligned}$$

Therefore, $\alpha^{p^t-1} = 1$ and $k = 1$.

Let $V = \{x \in \mathbb{F}_{p^e} | G(x) = 0\}$. Then V is a $p-$dimensional $p-$modulus over $\mathbb{F}_p$. Moreover, we have

Claim 1: $\{\alpha, \alpha^p, \cdots, \alpha^{p^{p-1}}\}$ forms a basis of V, where α is a root of $G(x)$ and $\alpha \neq 0$.

Proof. If there are some $k_1, k_2, \cdots, k_p \in \mathbb{F}_p$ with at least one element is nonzero such that

$$k_1\alpha + k_2\alpha^p + \cdots + k_p\alpha^{p^{p-1}} = 0,$$

then the $p-$module generated by $\{\alpha, \alpha^p, \cdots, \alpha^{p^{p-1}}\}$ forms a submodule of V, we denote this $p-$module by W and $W(x) = \prod_{w\in W}(x-w) = \sum_{i=0}^{p-1} b_i x^{p^i}$. Since W is a $p-$module, we know that $W(x) \in \mathbb{F}_p[x]$. Moreover, by Lemma 2.4, $W(x)$ symbolically divides $G(x)$, thus the polynomial $\sum_{i=0}^{p-1} b_i x^i \in \mathbb{F}_p[x]$ divides $g(x)$ (Lemma 2.3). Since $g(x)$ is irreducible over $\mathbb{F}_p$, we get a contradiction. □

Claim 2: For every integer s and integer t, $0 < s, t < p$, we have

$$\alpha^{p^{sp^t}} = \sum_{i=0}^{s} t^{s-i}\binom{s}{i}\alpha^{p^i}. \tag{3.2}$$

Proof. Since $\alpha^{p^p} = \alpha^p + \alpha$, we have

$$\begin{aligned}\alpha^{p^{2p}} &= (\alpha^{p^p})^{p^p} = (\alpha+\alpha^p)^{p^p}\\ &= \alpha^{p^p} + (\alpha^{p^p})^p = \alpha + \alpha^p + \alpha^p + \alpha^{p^2}\\ &= \alpha + 2\alpha^p + \alpha^{p^2}.\end{aligned}$$

Suppose that $\alpha^{p^{sp}} = \sum_{i=0}^{s}\binom{s}{i}\alpha^{p^i}$, then

$$\begin{aligned}&\alpha^{p^{(s+1)p}} = \left(\alpha^{p^{sp}}\right)^{p^p}\\ =\ &\left(\sum_{i=0}^{s}\binom{s}{i}\alpha^{p^i}\right)^{p^p} = \sum_{i=0}^{s}\binom{s}{i}(\alpha^{p^p})^{p^i}\\ =\ &\sum_{i=0}^{s}\binom{s}{i}(\alpha+\alpha^p)^{p^i} = \sum_{i=0}^{s}\binom{s}{i}(\alpha^{p^i}+\alpha^{p^{i+1}})\\ =\ &\sum_{i=0}^{s+1}\binom{s+1}{i}\alpha^{p^i}.\end{aligned}$$

By induction, we know that

$$\alpha^{p^{ps}} = \sum_{i=0}^{s}\binom{s}{i}\alpha^{p^i} \tag{3.3}$$

holds for any nonnegative integer s.

Taking $s = p^{t-1}, p^{t-2}, \cdots, 1$ in (3.3) respectively, we have

$$\alpha^{p^{p^t}} = \alpha + \alpha^{p^{t-1}} = \alpha + (\alpha + \alpha^{p^{p^{t-2}}}) = \cdots = t\alpha + \alpha^p. \tag{3.4}$$

Therefore, by a similar procedure as the proof of (3.3), we obtain that

$$\alpha^{p^{sp^t}} = \sum_{i=0}^{s} t^{s-i}\binom{s}{i}\alpha^{p^i}.$$

□

Denote

$$\begin{aligned}
\sigma_1 := \sigma_1(x_1, x_2, \cdots, x_n) &= \sum_{i=1}^{n} x_i \\
\sigma_2 := \sigma_2(x_1, x_2, \cdots, x_n) &= \sum_{i<j} x_i x_j \\
\sigma_3 := \sigma_3(x_1, x_2, \cdots, x_n) &= \sum_{i<j<k} x_i x_j x_k \\
\cdots\cdots &\ \vdots\ \cdots\cdots \\
\sigma_n := \sigma_n(x_1, x_2, \cdots, x_n) &= x_1 x_2 \cdots x_n.
\end{aligned}$$

By Vieta's Theorem, $x_1, x_2, \cdots, x_n$ are the roots of the equation

$$X^n - \sigma_1 X^{n-1} + \sigma_2 X^{n-2} + \cdots + (-1)^n \sigma_n = 0. \tag{3.5}$$

Claim 3: For integers $x_1, x_2, \cdots, x_n$, $0 \le x_i < p, i = 1, 2, \cdots, n$, we have

$$\alpha^{p^{p^{x_1}+p^{x_2}+\cdots+p^{x_n}}} = \sigma_n \alpha + \sigma_{n-1}\alpha^p + \cdots + \sigma_j \alpha^{p^{n-j}} + \cdots + \sigma_1 \alpha^{p^{n-1}} + \alpha^{p^n}. \tag{3.6}$$

Proof. By (3.4), we have

$$\begin{aligned}
\alpha^{p^{p^{x_1}+p^{x_2}}} &= \left(\alpha^{p^{p^{x_1}}}\right)^{p^{p^{x_2}}} \\
&= (x_1\alpha + \alpha^p)^{p^{p_2^x}} \\
&= x_1 \alpha^{p^{p^{x_2}}} + \left(\alpha^{p^{p^{x_2}}}\right)^p \\
&= x_1(x_2\alpha + \alpha^p) + (x_2\alpha + \alpha^p)^p \\
&= (x_1x_2)\alpha + (x_1 + x_2)\alpha^p + \alpha^{p^2}.
\end{aligned}$$

Similarly, we have

$$\begin{aligned}
\alpha^{p^{p^{x_1}+p^{x_2}+p^{x_3}}} &= \left(\alpha^{p^{p^{x_1}+p^{x_2}}}\right)^{p^{p^{x_3}}} \\
&= \left((x_1x_2)\alpha + (x_1 + x_2)\alpha^p + \alpha^{p^2}\right)^{p^{p^{x_3}}} \\
&= (x_1x_2)(x_3\alpha + \alpha^p) + (x_1 + x_2)(x_3\alpha + \alpha^p)^p + (x_3\alpha + \alpha^p)^{p^2} \\
&= (x_1x_2x_3)\alpha + (x_1x_2 + x_1x_3 + x_2x_3)\alpha^p + (x_1 + x_2 + x_3)\alpha^{p^2} + \alpha^{p^3}.
\end{aligned}$$

By this way, step by step, we obtain the identity (3.6).

□

Define a set $C_\alpha = \{\beta \in V | \beta \text{ is a conjugate of } k\alpha \text{ for some } k \in \mathbb{F}_p^*\}$.
Claim 4: $|C_\alpha| \ge p^{p-1}(p-1)$, where $|C_\alpha|$ denotes the cardinality of the set C_α.

Proof. Let $n = p$ in the equations (3.5) and (3.6). Since there are p^p choices of $x_1, x_2, \cdots, x_p \in \mathbb{F}_p$, there are p^{p-1} choices of $\sigma_1, \sigma_2, \cdots, \sigma_p$ satisfying (3.6). If there are two multi-sets $\{x_1, x_2, \cdots, x_p\} \subseteq \mathbb{F}_p, \{x_1', x_2', \cdots, x_p'\} \subseteq \mathbb{F}_p$ such that

$$\alpha^{p^{p^{x_1}+p^{x_2}+\cdots+p^{x_n}}} = \alpha^{p^{p^{x_1'}+p^{x_2'}+\cdots+p^{x_n'}}}, \tag{3.7}$$

then by (3.6), we have that

$$\begin{aligned}\alpha^{p^{p^{x_1}+p^{x_2}+\cdots+p^{x_p}}} &= \sigma_p\alpha+\sigma_{p-1}\alpha^p+\cdots+\sigma_j\alpha^{p^{p-j}}+\cdots+\sigma_1\alpha^{p^{p-1}}+\alpha^{p^p}\\ &= (\sigma_p+1)\alpha+(\sigma_{p-1}+1)\alpha^p+\sigma_{p-2}\alpha^{p^2}+\cdots+\sigma_1\alpha^{p^{p-1}}\end{aligned}$$

and

$$\alpha^{p^{p^{x'_1}+p^{x'_2}+\cdots+p^{x'_p}}} = (\sigma'_p+1)\alpha+(\sigma'_{p-1}+1)\alpha^p+\sigma'_{p-2}\alpha^{p^2}+\cdots+\sigma'_1\alpha^{p^{p-1}},$$

where

$$\begin{aligned}\sigma'_1 &= \sum_{i=1}^{p} x'_i\\ \sigma'_2 &= \sum_{i<j} x'_ix'_j\\ \sigma'_3 &= \sum_{i<j<k} x'_ix'_jx'_k\\ \cdots &\ \vdots\ \cdots\cdots\\ \sigma'_p &= x'_1x'_2\cdots x'_p.\end{aligned}$$

By Claim 1, we have $\sigma_i=\sigma'_i, i=1,2,\cdots,p$ and thus $\{x_1,x_2,\cdots,x_p\}=\{x'_1,x'_2,\cdots,x'_p\}$ as two multi-sets.

If there are two multi-sets $\{x_1,x_2,\cdots,x_p\}\subseteq\mathbb{F}_p, \{x'_1,x'_2,\cdots,x'_p\}\subseteq\mathbb{F}_p$ and $k\in\mathbb{F}_p$ such that

$$\alpha^{p^{p^{x_1}+p^{x_2}+\cdots+p^{x_n}}} = k\alpha^{p^{p^{x'_1}+p^{x'_2}+\cdots+p^{x'_n}}}, \tag{3.8}$$

then we have two integers $s\le s'$ such that

$$\alpha^{p^{s'-s}} = k\alpha. \tag{3.9}$$

Thus $k\alpha$ is conjugate to α, so that $k=1$. This completes the proof of Claim 4. □

Claim 5: $Q=e$.

Proof. By Claim 4, if α and γ are roots of $G(x)$ and $\gamma\notin C_\alpha$, then it is easily seen that $C_\alpha\cap C_\gamma=\Phi$, the empty set. Hence we know that

$$|V|=p^p\ge|C_\alpha|+|C_\gamma|+1\ge 2p^{p-1}(p-1)+1$$

which implies that $p<2$, a contradiction. Therefore, we have that $V=C_\alpha\cup\{0\}$ and so that $Q=e$ (see (3.1)). □

This completes the proof of Theorem 1.1.

We can say something more about the order of the roots of $G(x)$. For every integer s, $0<s<Q$, let $s=\sum_{i=0}^{p-1}s_ip^i$ be its $p-adic$ expansion. Denote $wt(s)=\sum_{i=0}^{p-1}s_i$. From (3.6), it follows that $\alpha^{p^s}\ne\alpha$ if $wt(s)\le p-1$ (the coefficient of $\alpha^{p^{wt(s)}}$ in (3.6) is nonzero).

When $wt(s)=p$, let $s=p^{x_1}+p^{x_2}+\cdots+p^{x_p}$. Then

$$\begin{aligned}\alpha^{p^{p^{x_1}+p^{x_2}+\cdots+p^{x_p}}} &= \sigma_p\alpha+\sigma_{p-1}\alpha^p+\cdots+\sigma_j\alpha^{p^{p-j}}+\cdots+\sigma_1\alpha^{p^{p-1}}+\alpha^{p^p}\\ &= (\sigma_p+1)\alpha+(\sigma_{p-1}+1)\alpha^p+\sigma_{p-2}\alpha^{p^2}+\cdots+\sigma_1\alpha^{p^{p-1}}.\end{aligned}$$

Thus, if $\alpha^{p^s} = \alpha$, then

$$\begin{aligned} \sigma_p &= 0 \\ \sigma_{p-1} &= -1 \\ \sigma_{p-2} &= 0 \\ \vdots &\ \vdots\ \vdots \\ \sigma_1 &= 0. \end{aligned}$$

Therefore, by Vieta's Theorem, $x_1, x_2, \cdots, x_p$ are the roots of the equation $X^p - X = 0$. This equation has no multiple roots, so that $\{x_1, x_2, \cdots, x_p\} = \{0, 1, 2, \cdots, p-1\}$, and $s = Q$. This proves that when $wt(s) = p$, then $\alpha^{p^s} = \alpha$ if and only if $s = Q$.

The proof of Theorem 1.3.

Proof. It is easily seen from the proof of Theorem 1.1 that

$$G(x) = xh(x^{p-1}) = x \prod_{i=0}^{Q-1} (x^{p-1} - \alpha^{p^i(p-1)})$$

and $h(x) = \prod_{i=0}^{Q-1}(x - \alpha^{p^i(p-1)})$ is irreducible over $\mathbb{F}_p$.

□

Remark: (1) Let L/K be a cyclic extension of degree $p = Char(K)$, where K is an arbitrary field of character p. Then there exists an element $\gamma \in L$ such that $L = K(\gamma)$, and $\gamma^p - \gamma = c \in K$, $c \neq \alpha^p - \alpha$ for all $\alpha \in K$. Such an extension is called an *Artin-Schreier extension* of degree p [8, p.239]. This extension is an interesting cyclic extension, the automorphism of L/K are given by $\sigma(\gamma) = \gamma + \nu$ with $\nu \in \mathbb{Z}/p\mathbb{Z} \subseteq K$. Any element $\gamma_1 \in L$ such that $L = K(\gamma_1)$ and $\gamma_1^p - \gamma_1 \in K$ is called an *Artin-Schreier generator* for L/K. Any two Artin-Schreier generators γ and γ_1 are related as follows: $\gamma_1 = \mu\gamma + (b^p - b)$ with $0 \neq \mu \in \mathbb{Z}/p\mathbb{Z}$ and $b \in K$. From Theorem 1.1, we know that when $K = \mathbb{F}_p$, a is a primitive element of $\mathbb{F}_p$, ξ is a root of $x^p - x - 1$, then $a\xi$ is a primitive element of $\mathbb{F}_{p^p}$. Thus there exists a primitive element of $\mathbb{F}_{p^p}$ such that it is an Artin-Schreier generator.

(2) There is another way to prove that the order of the polynomial $x^p - x - 1$ is $\frac{p^p-1}{p-1}$, the procedure is as follows:

(i) Since $x^p - x - 1$ is irreducible over $\mathbb{F}_p$, $\{1, \xi, \xi^2, \cdots, \xi^{p-1}\}$ forms a $\mathbb{F}_p-$ basis of $\mathbb{F}_{p^p}$, where $\xi \in \mathbb{F}_{p^p}$ is a root of $x^p - x - 1$;

(ii) For integers $x_1, x_2, \cdots, x_n$, $0 \leq x_i < p, i = 1, 2, \cdots, n$, since $\xi^p = \xi + 1$, by an easy induction, we know that $\xi^{p^{x_i}} = x_i + \xi$, thus we have

$$\xi^{p^{x_1}+p^{x_2}+\cdots+p^{x_n}} = \sigma_n + \sigma_{n-1}\xi + \cdots + \sigma_j\xi^{n-j} + \cdots + \sigma_1\xi^{n-1} + \xi^n. \tag{3.10}$$

(iii) By (3.10), we know that if there are $x_i, x_i', i = 1, 2, \cdots, p$, $k \in \mathbb{F}_p$ such that

$$\xi^{p^{x_1}+p^{x_2}+\cdots+p^{x_p}} = k\xi^{p^{x_1'}+p^{x_2'}+\cdots+p^{x_p'}}$$

then $k = 1$ and $\{x_1, x_2, \cdots, x_p\} = \{x_1', x_2', \cdots, x_p'\}$.

Thus, if we define a set $c_\xi = \{\zeta \in \mathbb{F}_{p^p} | \zeta = k\xi^t,\ t \text{ is an integer and } k \in \mathbb{F}_p^*\}$, then $|c_\xi| \geq (p-1)p^{p-1}$;

(iv) Since c_ξ forms a multiplicative subgroup of $\mathbb{F}_{p^p}^*$, $p^p - 1 = u|c_\xi|$ holds for a positive integer u, thus

$$u = \frac{p^p - 1}{|c_\xi|} < \frac{p^p - 1}{p^{p-1}(p-1)} < 2.$$

Therefore, we have $|c_\xi| = p^p - 1$, and so there is a element k in $\mathbb{F}_p$ such that $k\xi^t$ is a primitive element of $\mathbb{F}_{p^p}$.

(v) Since $\gcd(Q, p-1) = 1$, the order of $k\xi^t$, denoted by $o(k\xi^t)$, is $p^p - 1 = o(k\xi^t) = o(k)o(\xi^t) \leq (p-1)o(\xi) \leq (p-1)Q = p^p - 1$, thus, $o(\xi) = e = Q$.

This procedure is somewhat simple than that we presented in Section 3. However, by this method, we can not obtain the irreducibility of the polynomial $x^Q - x - 1$ over $\mathbb{F}_p$, this is the reason why we use the language of $p-$modules.

Acknowledgment

The author would like to express his grateful thankfulness to Professor Qing Xiang, Professor Lei Hu and Professor Shuhong Gao for valuable discussions.

References

[1] S. D. Cohen, Primitive elements and polynomials with arbitary trace, Discrete Math. 83 (1990), 1-7.
[2] S. D. Cohen and D. Mills, Primitive polynomials with first and second coefficients prescribed. Finite fields and their applications, 9(2003), 334-350.
[3] W. B. Han, The coefficents of primitive polynomials over finite fields, Math. of Computation, Vol. 65, Number 213, January 1996, 331-340.
[4] D. Jungnickel and S. A. Vanstone, On primitive polynomials over finite fields, J. Algebra 124 (1989), 337-353.
[5] R. Lidl and H. Niederreiter, Introduction to Finite Fields and Their Applications, Cambridge University Press, Revised edition, 1994.
[6] H. W. Lenstra Jr, R. J. Schoof, Primitive normal bases for finite fields, Math. of Computation, Vol. 48, Number 177, January 1987, 217-231.
[7] J. Y. Shi and Zhen-hua Wang, The order of a root of $x^p - x - 1$ over $\mathbb{F}_p$, Journal of East China Normal University (Natural Science), No.2, Jun. 2004, 1-4.
[8] Henning Stichtenoth, Algebraic function fields and codes. Springer-Verlag, Berlin, 1993.

Xiwang Cao is with the School of Mathematical Sciences, Nanjing University of Aeronautics and Astronautics, Nanjing 210016, P. R. China; State Key Lab. of Information Security, Beijing 100049, P. R. China. email: xwcao@nuaa.edu.cn