Asian-European Journal of Mathematics
Vol. 11, No. 2 (2018) 1850031 (14 pages)

DOI: 10.1142/S1793557118500316

On primitive normal elements over finite fields

Anju* and R. K. Sharma†

Department of Mathematics
Indian Institute of Technology Delhi
New Delhi 110016, India
**anjugju@gmail.com*
†rksharmaiitd@gmail.com

Communicated by Jiping Zhang
Received April 28, 2016
Accepted March 3, 2017
Published May 15, 2017

Let $\mathbb{F}_{q^n}$ be an extension of the field $\mathbb{F}_q$ of degree n, where $q = p^k$ for some positive integer k and prime p. In this paper, we establish a sufficient condition for the existence of a primitive element $\alpha \in \mathbb{F}_{q^n}$ such that $\alpha^2 + \alpha + 1$ is also primitive as well as a primitive normal element α of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ such that $\alpha^2 + \alpha + 1$ is primitive.

Keywords: Finite field; normal element; primitive element; character.

AMS Subject Classification: 12E20, 11T23

1. Introduction

Let $\mathbb{F}_q$ be a finite field of order $q = p^k$, for some prime p and some positive integer k. Consider an extension $\mathbb{F}_{q^n}$ of $\mathbb{F}_q$ of degree n. An element $\alpha \in \mathbb{F}_{q^n}$ is called a *normal element* of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, if $\{\alpha, \alpha^q, \dots, \alpha^{q^{n-1}}\}$ is a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. This basis is called a *normal basis*. Normal bases are widely used in applications of finite fields such as coding theory, cryptography, signal processing [1, 17, 18]. The advantage of using normal basis representation yields efficient exponentiation, as the qth powers of elements are given by a cyclic-bit-shift of the corresponding co-ordinate vector. It is well known [16, Theorem 2.35] that $\mathbb{F}_{q^n}$ always contains a normal basis generator over $\mathbb{F}_q$. For basics on normal bases over finite fields, reader is referred to [2].

Further, for any finite field $\mathbb{F}_q$, its multiplicative group $\mathbb{F}_q^*$ is cyclic. The generators of $\mathbb{F}_q^*$ are called *primitive elements* of $\mathbb{F}_q$. Any field $\mathbb{F}_q$ has $\phi(q-1)$ primitive elements, where ϕ is the Euler's phi-function. Many authors have studied primitive elements over finite fields such as Carlitz and Davenport [3, 10]. Primitive

*Corresponding author.

elements are widely used in cryptography, coding theory and design theory. Primitive elements play a very important role in cryptosystems based on the multiplicative cyclic groups of nonzero elements of a finite field, for example ElGamal cryptosystem, and Diffie–Hellman key exchange protocol as a primitive element is an element of highest possible order and describes the field fully. The discrete log problem on such a group with primitive element as the generator will require maximum computation. It is a central problem in computational number theory to construct a primitive element in a finite field. Even determining a primitive element in a finite field is hard. There is no polynomial time algorithm to compute a primitive element, though there are $\phi(q-1)$ primitive elements in a finite field of q-elements, finding one may be difficult. In this paper, we prove the existence of a primitive element in terms of another primitive element, thus making a choice between them for an application. An element is called *primitive normal* if it is both primitive and normal. A primitive normal basis is a normal basis generated by a primitive element. Firstly, Carlitz [3] studied primitive normal bases. More precisely, in [3, 4], he proved that except for finitely many exclusive values of q, every finite field $\mathbb{F}_{q^n}$ contains a primitive normal element over $\mathbb{F}_q$. The existence of a primitive normal element of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ when q is a prime, was proved by Davenport [10]. Lenstra and Schoof [14] completely resolved the question of the existence of primitive normal elements for all field extensions $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Cohen and Huczynska [7] gave the first computer-free proof of the result of Lenstra and Schoof.

In general, for any primitive element $\alpha \in \mathbb{F}_q$, $f(\alpha)$ (where f is any rational function) need not be primitive in $\mathbb{F}_q$, for example, if we take the polynomial function $f(x) = x+1$ over the field $\mathbb{F}_2$ of order 2. Then 1 is the only primitive element of $\mathbb{F}_2$, but $f(1) = 0$ is not primitive. But for $f(x) = \frac{1}{x}$, $f(\alpha)$ is primitive in $\mathbb{F}_q$ whenever α is. Many researchers have worked in this direction. In 1985, Cohen [6] proved the existence of two consecutive primitive elements in a finite field $\mathbb{F}_q$, with $q > 3$, $q \not\equiv 7 \mod 12$ and $q \not\equiv 1 \mod 60$. He and Han [12] studied primitive elements in the form of $\alpha + \alpha^{-1}$ over finite fields. In 2012, Wang *et al.* [21] gave a sufficient condition on the existence of α such that α and $\alpha + \alpha^{-1}$ are both primitive for the case $2|q$. Liao *et al.* [15] generalized their results to the case that q is any prime power. In 2014, Cohen [9] completed the existence results obtained by Wang *et al.* [21] for finite fields of characteristic 2. Tian and Qi [19] proved that there exists a primitive element $\alpha \in \mathbb{F}_{q^n}$, such that both α and α^{-1} are normal elements of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, when $n \geq 32$. Later, Cohen and Huczynska [8] proved that for any prime power q and any integer $n \geq 2$, there exists an element $\alpha \in \mathbb{F}_{q^n}$ such that both α and α^{-1} are primitive normal over $\mathbb{F}_q$ except when (q, n) is one of the pairs $(2, 3)$, $(2, 4)$, $(3, 4)$, $(4, 3)$, $(5, 4)$. Chou and Cohen [5] completely resolved the question whether there exists a primitive element α such that α and α^{-1} both have trace zero over $\mathbb{F}_q$. In 2014, Kapetanakis [13], proved that with a few exceptions, for every q, n and $a, b, c, d \in \mathbb{F}_q$, there exists some primitive $x \in \mathbb{F}_{q^n}$ such that both x and $(ax+b)/(cx+d)$ produce a normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. In this paper, we study the question of the existence of a primitive element $\alpha \in \mathbb{F}_{q^n}$, such that for the rational expression $f(x) = x^2+x+1$, $f(\alpha)$ is also a primitive element of $\mathbb{F}_{q^n}$. We also study the question of the existence of a primitive normal element α of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ such that $\alpha^2+\alpha+1$ is also a primitive element of $\mathbb{F}_{q^n}$. Throughout the paper, we shall use the notation $\mathfrak{P}$ for the set of (q,n), such that $\mathbb{F}_{q^n}$ contains a primitive element α such that $\alpha^2+\alpha+1$ is also primitive and $\mathfrak{N}$ for the set of (q,n) such that $\mathbb{F}_{q^n}$ contains a primitive normal element α such that $\alpha^2+\alpha+1$ is also primitive. For any positive integer $m > 1$ and any $g \in \mathbb{F}_q[x]$, $\omega(m)$ and $\Omega_q(g)$ are used to denote the number of prime divisors of m, and the number of monic irreducible divisors of g over $\mathbb{F}_q$, respectively.

2. Preliminaries

In this section, q is an arbitrary prime power. For any divisor e of $q-1$, call $\xi \in \mathbb{F}_q^*$ *e-free* if, for any $d|e$, $\xi = \gamma^d$, $\gamma \in \mathbb{F}_q$, implies $d = 1$ i.e. if $\gcd(d, \frac{q-1}{\mathrm{ord}_q(\alpha)}) = 1$. Hence, an element $\alpha \in \mathbb{F}_q^*$ is primitive if and only if it is $(q-1)$-free.

The additive group of $\mathbb{F}_{q^n}$ is an $\mathbb{F}_q[x]$-module under the rule,

$$f\,o\,x = \sum_{i=1}^{t} f_i x^{q^i}; \quad \text{for } x \in \mathbb{F}_{q^n} \quad \text{and} \quad f(x) = \sum_{i=1}^{t} f_i x^i \in \mathbb{F}_q[x].$$

For $\xi \in \mathbb{F}_{q^n}$, the $\mathbb{F}_q$-order of ξ is defined to be the monic $\mathbb{F}_q$-divisor g of x^n-1 of minimal degree such that $g\,o\,\xi = 0$. If $\xi \in \mathbb{F}_{q^n}$ has $\mathbb{F}_q$-order g, then $\xi = h\,o\,v$ for some $v \in \mathbb{F}_{q^n}$, where $h = \frac{x^n-1}{g}$. Let M be a divisor of x^n-1. If $\alpha = h\,o\,v$ (where $v \in \mathbb{F}_{q^n}$, h is a divisor of M) implies $h = 1$, we say that α is *M-free* in $\mathbb{F}_{q^n}$. Hence, an element of $\mathbb{F}_{q^n}$ is normal over $\mathbb{F}_q$ if and only if its $\mathbb{F}_q$-order is x^n-1.

Next, we give the definition of a character of a finite abelian group and some results related to that.

Definition 2.1. A character χ of a finite abelian group G is a homomorphism from G into the multiplicative group U of complex numbers of absolute value 1. The characters of G form a group under multiplication, which is isomorphic to G and denoted by $\widehat{G}$. Furthermore, the character χ_0, where $\chi_0(g) = 1$ for all $g \in G$ is the trivial character of G.

In a finite field $\mathbb{F}_q$, there are two types of finite abelian groups, the additive group $\mathbb{F}_q$ and the multiplicative group $\mathbb{F}_q^*$. So we talk about two types of characters of a finite field, characters of $\mathbb{F}_q$ are called *additive characters* and characters of $\mathbb{F}_q^*$ are called *multiplicative characters.* The multiplicative characters are extended to zero using the rule,

$$\chi(0) := \begin{cases} 0 & \text{if } \chi \neq \chi_0 \\ 1 & \text{if } \chi = \chi_0. \end{cases}$$

Since $\widehat{\mathbb{F}_q^*} \cong \mathbb{F}_q^*$, we have that $\widehat{\mathbb{F}_q^*}$ is cyclic and for any divisor d of $q-1$, there are exactly $\phi(d)$ characters of order d in $\widehat{\mathbb{F}_q}^*$. Following Cohen and Huczynska [7, 8], it can be shown that for any $m|q-1$, the characteristic function for the subset of m-free elements of $\mathbb{F}_q^*$ is defined by

$$\rho_m : \alpha \mapsto \theta(m) \sum_{d|m} \frac{\mu(d)}{\phi(d)} \sum_{\chi_d} \chi_d(\alpha),$$

where $\theta(m) := \frac{\phi(m)}{m}$, μ is Möbius function, and χ_d stands for any multiplicative character of order d. Further, $\widehat{\mathbb{F}_{q^n}}$ is an $\mathbb{F}_q[x]$-module under the rule $\psi\, o\, f(\alpha) = \psi(f\, o\, \alpha)$, for $\psi \in \widehat{\mathbb{F}_{q^n}}, f \in \mathbb{F}_q[x]$, and $\alpha \in \mathbb{F}_{q^n}$. For any (monic) $\mathbb{F}_q$-divisor g of $x^n - 1$, a typical additive character ψ_g of $\mathbb{F}_q$-order g is one such that $\psi_g\, o\, g$ is the trivial character in $\mathbb{F}_{q^n}$, and g is minimal (in terms of degree) with this property. Further, there are $\Phi_q(g)$ characters ψ_g, where $\Phi_q(g) = (\mathbb{F}_q[x]/g\mathbb{F}_q[x])^*$ is the analogue of Euler function on $\mathbb{F}_q[x]$.

In an analogy to the above, the characteristic function for the set of g-free elements in $\mathbb{F}_{q^n}$, for any $g|x^n - 1$ is given by

$$\kappa_g : \alpha \mapsto \Theta(g) \sum_{h|g} \frac{\mu'(h)}{\Phi(h)} \sum_{\psi_h} \psi_h(\alpha),$$

where $\Theta(g) := \frac{\Phi(g)}{q^{\deg(g)}}$, the internal sum runs over additive characters ψ_h of $\mathbb{F}_q$-order h, and μ' is the analogue of the Möbius function which is defined by the rule,

$$\mu'(g) := \begin{cases} (-1)^s & \text{if } g \text{ is a product of } s \text{ distinct monic irreducible polynomials} \\ 0 & \text{otherwise.} \end{cases}$$

We shall need the following results.

Lemma 2.1 ([16, Theorem 5.4]). *If χ is any nontrivial character of a finite abelian group G and ξ is a nontrivial element of G, then*

$$\sum_{\xi \in G} \chi(\xi) = 0 \quad \textit{and} \quad \sum_{\chi \in \widehat{G}} \chi(\xi) = 0.$$

Lemma 2.2 ([16, Theorem 5.11]). *Let χ be a nontrivial multiplicative character and ψ be a nontrivial additive character of $\mathbb{F}_q$, then*

$$\left| \sum_{\alpha \in \mathbb{F}_q^*} \chi(\alpha)\psi(\alpha) \right| = q^{1/2}.$$

Lemma 2.3 ([20]). *Let χ_1 and χ_2 be two multiplicative nontrivial characters of the finite field $\mathbb{F}_q$. Let $f_1(x)$ and $f_2(x)$ be two monic pairwise prime polynomials in $\mathbb{F}_q[x]$, such that none of $f_i(x)$ is of the form $g(x)^{\mathrm{ord}(\chi_i)}$ for $i = 1, 2$, where $g(x) \in \mathbb{F}_q[x]$ with degree at least 1. Let n_1 and n_2 be the degrees of largest square free divisors of f_1 and f_2, respectively. Then we have*

$$\left| \sum_{\alpha \in \mathbb{F}_q} \chi_1(f_1(\alpha))\chi_2(f_2(\alpha)) \right| \leq (n_1 + n_2 - 1)\sqrt{q}.$$

Lemma 2.4 ([16, Theorem 5.41]). *Let χ be a multiplicative character of $\mathbb{F}_q$ of order $m > 1$ and let $f \in \mathbb{F}_q[x]$ be a monic polynomial of positive degree such that $f(x)$ is not of the form $g(x)^m$, where $g(x) \in \mathbb{F}_q[x]$ with degree at least 1. Let d be the number of distinct roots of f in its splitting field over $\mathbb{F}_q$. Then for every $a \in \mathbb{F}_q$, we have*

$$\left|\sum_{c\in\mathbb{F}_q} \chi(af(c))\right| \le (d-1)q^{1/2}.$$

The next lemma is a consequence of [11, Theorem 5.6 and Remark 5.7].

Lemma 2.5 ([11]). *Let $f_1(x), f_2(x), \ldots, f_s(x) \in \mathbb{F}_{q^n}[x]$ be distinct irreducible polynomials over $\mathbb{F}_{q^n}$, and $g(x)$ be a rational function over $\mathbb{F}_{q^n}$. Let $\chi_1, \chi_2, \ldots, \chi_s$ be multiplicative characters of $\mathbb{F}_{q^n}$, and let ψ be a nontrivial additive character of $\mathbb{F}_{q^n}$. Suppose that $g(x)$ is not of the form $r(x)^q - r(x)$ in $\mathbb{F}_q(x)$. Then*

$$\left|\sum_{\substack{\alpha\in\mathbb{F}_{q^n},\\ f_i(\alpha)\neq 0, g(\alpha)\neq\infty}} \chi_1(f_1(\alpha))\chi_2(f_2(\alpha))\cdots\chi_s(f_s(\alpha))\psi(g(\alpha))\right|$$
$$\le (n_1+n_2+n_3+n_4-1)q^{n/2},$$

where $n_1 = \sum_{j=1}^{s}\deg(f_j)$, $n_2 = \max(\deg(g), 0)$, n_3 is the degree of the denominator of $g(x)$ and n_4 is the sum of degrees of those irreducible polynomials dividing the denominator of g, but distinct from $f_j(x)$ $(j = 1, \ldots, s)$.

Lemma 2.6 ([14]). *Let $n > 1$, $l > 1$ be integers and Λ be a set of primes $\le l$. Set $L = \prod_{r\in\Lambda} r$. Assume that every prime factor $r < l$ of n is contained in Λ. Then*

$$\omega(n) \le \frac{\log n - \log L}{\log l} + |\Lambda|. \tag{2.1}$$

Let m be a positive integer and p_m be the mth prime. Now if we take $l = p_m$, and then Λ is the set of primes no more than p_m, $|\Lambda| = m$, so the inequality (2.1) becomes

$$\omega(N) \le \frac{\log N - \sum_{i=1}^{m}\log p_i}{\log p_m} + m. \tag{2.2}$$

Lemma 2.7 ([14]). *Let q be a prime power and n be a positive integer. Let $\Omega = \Omega_q(x^n - 1)$. Then we have $\Omega \le \{n + \gcd(n, q-1)\}/2$. In particular, $\Omega \le n$, and $\Omega = n$ if and only if $n|q-1$. Moreover, $\Omega \le \frac{3}{4}n$ if $q-1$ is not divisible by n.*

3. Main Results

Let $N_q(m_1, m_2)$ be the number of $\alpha \in \mathbb{F}_q$, such that α is m_1-free and $\alpha^2+\alpha+1$ is m_2-free and $N_q(m_1, m_2, g)$ be the number of $\alpha \in \mathbb{F}_q$, such that α is m_1-free and g-free and $\alpha^2+\alpha+1$ is m_2-free, where m_1, m_2 are positive integers and g is any polynomial over $\mathbb{F}_q$. In this section, we shall use the notation χ_1 to denote the trivial multiplicative character as it has order 1.

Theorem 3.1 *Let $q = p^k$ for some prime $p \neq 3$ and n be a positive integer and let $\omega = \omega(q^n - 1)$. If $q^{\frac{n}{2}} > 2^{2\omega+1}$, then $(q, n) \in \mathfrak{P}$.*

Proof. By definition

$$\begin{aligned} N_{q^n}(q^n-1, q^n-1) &= \sum_{\alpha \in \mathbb{F}_{q^n}^*} \rho_{q^n-1}(\alpha)\rho_{q^n-1}(\alpha^2+\alpha+1) \\ &= \theta(q^n-1)^2 \sum_{\alpha \in \mathbb{F}_{q^n}^*} \sum_{d,h \mid q^n-1} \frac{\mu(d)\mu(h)}{\phi(d)\phi(h)} \sum_{\chi_d,\chi_h} \chi_d(\alpha)\chi_h(\alpha^2+\alpha+1) \\ &= \theta(q^n-1)^2(S_1+S_2+S_3+S_4), \end{aligned}$$

where

$$\begin{aligned} S_1 &= \sum_{\alpha \in \mathbb{F}_{q^n}^*} \sum_{d=1=h} \frac{\mu(d)\mu(h)}{\phi(d)\phi(h)} \sum_{\chi_d,\chi_h} \chi_d(\alpha)\chi_h(\alpha^2+\alpha+1) \\ &= \sum_{\alpha \in \mathbb{F}_{q^n}^*} \left(\frac{\mu(1)}{\phi(1)}\right)^2 \sum_{\chi_1} \chi_1(\alpha)\chi_1(\alpha^2+\alpha+1) \\ &= \sum_{\alpha \in \mathbb{F}_{q^n}^*} 1 = q^n - 1. \end{aligned}$$

$$\begin{aligned} |S_2| &= \left| \sum_{\alpha \in \mathbb{F}_{q^n}^*} \sum_{1 \neq d \mid q^n-1} \frac{\mu(d)}{\phi(d)} \sum_{\chi_d} \chi_d(\alpha)\chi_1(\alpha^2+\alpha+1) \right| \\ &= \left| \sum_{\alpha \in \mathbb{F}_{q^n}^*} \sum_{1 \neq d \mid q^n-1} \frac{\mu(d)}{\phi(d)} \sum_{\chi_d} \chi_d(\alpha) \right| \\ &\leq \sum_{1 \neq d \mid q^n-1} \frac{|\mu(d)|}{\phi(d)} \sum_{\chi_d} \left| \sum_{\alpha \in \mathbb{F}_{q^n}^*} \chi_d(\alpha) \right|. \end{aligned}$$

Using Lemma 2.1, we get

$$\begin{aligned} |S_2| &= 0. \\ |S_3| &= \left| \sum_{\alpha \in \mathbb{F}_{q^n}^*} \sum_{1 \neq h \mid q^n-1} \frac{\mu(h)}{\phi(h)} \sum_{\chi_h} \chi_h(\alpha^2+\alpha+1)\chi_1(\alpha) \right| \\ &\leq \sum_{\substack{1 \neq h \mid q^n-1, \\ h \text{ squarefree}}} \frac{1}{\phi(h)} \sum_{\chi_h} \left| \sum_{\alpha \in \mathbb{F}_{q^n}} \chi_h(\alpha^2+\alpha+1) - \chi_h(1) \right|. \end{aligned}$$

By Lemma 2.4, we have $|\sum_{\alpha\in\mathbb{F}_{q^n}} \chi_h(\alpha^2+\alpha+1)| \le q^{n/2}$, using this and the facts that $\sum_{\chi_h} 1 = \phi(h)$ and $\sum_{\substack{1\neq h|q^n-1,\\ h \text{ squarefree}}} 1 = 2^\omega - 1$, we get

$$|S_3| \le (q^{n/2}+1)(2^\omega - 1).$$

$$\begin{aligned}|S_4| &= \left|\sum_{\alpha\in\mathbb{F}^*_{q^n}} \sum_{1\neq d,h|q^n-1} \frac{\mu(d)\mu(h)}{\phi(d)\phi(h)} \sum_{\chi_d,\chi_h} \chi_d(\alpha)\chi_h(\alpha^2+\alpha+1)\right| \\ &\le \sum_{\substack{1\neq d,h|q^n-1,\\ d,h \text{ squarefree}}} \frac{1}{\phi(d)\phi(h)} \sum_{\chi_d,\chi_h} \left|\sum_{\alpha\in\mathbb{F}^*_{q^n}} \chi_d(\alpha)\chi_h(\alpha^2+\alpha+1)\right|.\end{aligned}$$

Using Lemma 2.3, we get

$$\begin{aligned}|S_4| &\le \sum_{\substack{1\neq d,h|q^n-1,\\ d,h \text{ squarefree}}} \frac{1}{\phi(d)\phi(h)} \sum_{\chi_d,\chi_h} 2q^{n/2} \\ &= 2q^{n/2}(2^w-1)^2.\end{aligned}$$

Hence, we have

$$\begin{aligned}&|N_{q^n}(q^n-1, q^n-1) - \theta(q^n-1)^2(q^n-1)| \\ &\quad \le \theta(q^n-1)^2\{(q^{n/2}+1)(2^\omega-1) + 2q^{n/2}(2^\omega-1)^2\}. \end{aligned} \tag{3.1}$$

So, our aim is to find (q,n) for which $N_{q^n}(q^n-1, q^n-1) > 0$. From (3.1), it is clear that $N_{q^n}(q^n-1, q^n-1)$ will be greater than 0, if we have $q^n - 1 > (q^{n/2}+1)(2^\omega - 1) + 2q^{n/2}(2^\omega-1)^2$, which can be obtained if we take

$$q^{n/2} > 2^{2\omega+1}. \tag{3.2}$$

Hence, the desired result is obtained. □

Corollary 3.1. *Let $q = 2^k$ and n be a positive integer. If $n \ge 14$ and $k \ge 5$, then $(q,n) \in \mathfrak{P}$.*

Proof. By Lemma 2.6, we have

$$\omega(q^n-1) \le \frac{\log(q^n-1) - \sum_{i=1}^m \log p_i}{\log p_m} + m < \frac{n\log q - \sum_{i=1}^m \log p_i}{\log p_m} + m. \tag{3.3}$$

Equation (3.2) is equivalent to,

$$\omega < \frac{n\log q}{\log 16} - \frac{1}{2}. \tag{3.4}$$

From (3.3), it is clear that (3.4) holds true if

$$\frac{n\log q}{\log 16} - \frac{n\log q}{\log p_m} > m + \frac{1}{2} - \frac{\sum_{i=1}^m \log p_i}{\log p_m}. \tag{3.5}$$

Since $\frac{1}{\log 16} - \frac{1}{\log p_m} > 0 \Leftrightarrow m \ge 7$, we may choose any $m \ge 7$ to check (3.5).

Table 1.

$k =$	1	2	3	4
$n \geq$	70	35	24	18

If we choose $m = 20$, then left side of (3.5) is positive, so we have

$$n > \frac{m + \frac{1}{2} - \frac{\sum_{i=1}^{m} \log p_i}{\log p_m}}{\frac{\log q}{\log 16} - \frac{\log q}{\log p_m}}. \tag{3.6}$$

Since $\sum_{i=1}^{m} \log p_i \leq m \log p_m$, the right-hand side of (3.6) is a decreasing function of q. It is easy to check that the inequality (3.6) is true if we take $q = 32$ and $n \geq 14$. Hence if $q \geq 32$ and $n \geq 14$, then $(q, n) \in \mathfrak{P}$. □

Remark 3.1. When $2^k < 32$ i.e. $k < 5$, the values of n such that $(2^k, n) \in \mathfrak{P}$, are obtained by using software Mathematica 4.1 and listed in Table 1.

Remark 3.2. The proof of Theorem 3.1 is not valid for $p = 3$ as in this case $f(x) = x^2 + x + 1 = (x - 1)^2$, and $2 | q^n - 1$. So Lemma 2.4 is not applicable in that case, which is a key requirement in the proof of Theorem 3.1. In fact, for $p = 3$, we have $\alpha^2 + \alpha + 1 = (\alpha - 1)^2$, which cannot be primitive.

The following lemma provide us an estimation of the size of $2^{\omega(I)}$ for any positive integer I. The proof of the Lemma is obvious using multiplicativity.

Lemma 3.1. *For any positive integer I, $2^{\omega(I)} < C(I) I^{1/5}$, where $C(I) < 11.25$. Moreover,*

$$C(I) < \begin{cases} 7.77 & \text{if } 5 \nmid I \\ 8.31 & \text{if } 7 \nmid I. \end{cases}$$

Corollary 3.2. *Let $q = p^k$, where k is a positive integer and $p > 3$ is a prime. If n is a positive integer such that $nk \geq 30$, then $(q, n) \in \mathfrak{P}$.*

Proof. By Lemma 3.1 and Theorem 3.1, we see that $N_{q^n}(q^n - 1, q^n - 1) > 0$ if

$$q^{n/10} > 2C(q^n - 1)^2. \tag{3.7}$$

Equation (3.7) holds true for all $p \geq 11$ and $nk \geq 23$, since $C(q^n - 1) < 11.25$. If $p = 7$, then $C(q^n - 1) < 8.31$ and (3.7) holds for all $nk \geq 26$. If $p = 5$, then $C(q^n - 1) < 7.77$ and (3.7) is true for all $nk \geq 30$. Hence $(q, n) \in \mathfrak{P}$ for all $p \geq 5$ and $nk \geq 30$. □

Theorem 3.2. *Let $q = p^k$ for some prime $p \neq 3$ and positive integer k. Let n be any positive integer. If $q^{n/2} > 3 \cdot 2^{2\omega + \Omega}$, then $(q, n) \in \mathfrak{N}$, where $\Omega = \Omega_q(x^n - 1)$ and $\omega = \omega(q^n - 1)$.*

Proof.

$$N_{q^n}(q^n-1, q^n-1, x^n-1) = \sum_{\alpha\in\mathbb{F}^*_{q^n}} \rho_{q^n-1}(\alpha)\rho_{q^n-1}(\alpha^2+\alpha+1)\kappa_{x^n-1}(\alpha)$$

$$= \theta(q^n-1)^2\Theta(x^n-1) \sum_{\alpha\in\mathbb{F}^*_{q^n}} \sum_{d,h|q^n-1} \sum_{g|x^n-1} \frac{\mu(d)\mu(h)\mu'(g)}{\phi(d)\phi(h)\Phi(g)}$$

$$\sum_{\chi_d,\chi_h} \sum_{\psi_g} \sum_{\alpha\in\mathbb{F}^*_{q^n}} \chi_d(\alpha)\chi_h(\alpha^2+\alpha+1)\psi_g(\alpha) = \theta(q^n-1)^2\Theta(x^n-1)\left(\sum_{i=1}^{8} S_i{}'\right),$$

where, $\Phi(g) = \Phi_q(g)$,

$$S_1{}' = \sum_{\alpha\in\mathbb{F}^*_{q^n}} \sum_{d=1=h} \sum_{g=1} \frac{\mu(d)\mu(h)\mu'(g)}{\phi(d)\phi(h)\Phi(g)} \sum_{\chi_d,\chi_h} \sum_{\psi_g} \chi_d(\alpha)\chi_h(\alpha^2+\alpha+1)\psi_g(\alpha)$$

$$= \sum_{\alpha\in\mathbb{F}^*_{q^n}} 1 = q^n - 1.$$

$$S_2{}' = \sum_{\alpha\in\mathbb{F}^*_{q^n}} \sum_{1\neq d|q^n-1} \frac{\mu(d)}{\phi(d)} \sum_{\chi_d} \chi_d(\alpha)\chi_1(\alpha^2+\alpha+1)\psi_1(\alpha) = S_2.$$

$$S_3{}' = \sum_{\alpha\in\mathbb{F}^*_{q^n}} \sum_{1\neq h|q^n-1} \frac{\mu(h)}{\phi(h)} \sum_{\chi_h} \chi_h(\alpha^2+\alpha+1)\chi_1(\alpha)\psi_1(\alpha) = S_3.$$

$$S_4{}' = \sum_{\alpha\in\mathbb{F}^*_{q^n}} \sum_{1\neq d,h|q^n-1} \frac{\mu(d)\mu(h)}{\phi(d)\phi(h)} \sum_{\chi_d,\chi_h} \chi_d(\alpha)\chi_h(\alpha^2+\alpha+1)\psi_1(\alpha) = S_4.$$

$$|S_5{}'| = \left|\sum_{\alpha\in\mathbb{F}^*_{q^n}} \sum_{1\neq g|x^n-1} \frac{\mu'(g)}{\Phi(g)} \sum_{\psi_g} \psi_g(\alpha)\right|$$

$$= \left|\sum_{1\neq g|x^n-1} \frac{\mu'(g)}{\Phi(g)} \sum_{\psi_g} \sum_{\alpha\in\mathbb{F}^*_{q^n}} \psi_g(\alpha)\right|$$

$$\leq \sum_{\substack{1\neq g|x^n-1,\\ g \text{ squarefree}}} \frac{|\mu'(g)|}{\Phi(g)} \sum_{\psi_g} \left|\sum_{\alpha\in\mathbb{F}^*_{q^n}} \psi_g(\alpha)\right|.$$

By using Lemma 2.1, the facts $\sum_{\psi_g} 1 = \Phi(g)$ and $\sum_{\substack{1\neq g|x^n-1,\\ g \text{ squarefree}}} = 2^\Omega - 1$, we get

$$|S_5{}'| \leq (2^\Omega - 1).$$

$$|S_6{}'| = \left|\sum_{\alpha\in\mathbb{F}^*_{q^n}} \sum_{1\neq d|q^n-1} \sum_{1\neq g|x^n-1} \frac{\mu(d)\mu'(g)}{\phi(d)\Phi(g)} \sum_{\chi_d} \sum_{\psi_g} \chi_d(\alpha)\psi_g(\alpha)\right|$$

$$= \left| \sum_{1\neq d|q^n-1} \sum_{1\neq g|x^n-1} \frac{\mu(d)\mu'(g)}{\phi(d)\Phi(g)} \sum_{\chi_d}\sum_{\psi_g}\sum_{\alpha\in\mathbb{F}_{q^n}^*} \chi_d(\alpha)\psi_g(\alpha) \right|$$

$$\leq \sum_{\substack{1\neq d|q^n-1,\\ d \text{ squarefree}}} \sum_{\substack{1\neq g|x^n-1,\\ g \text{ squarefree}}} \frac{1}{\phi(d)\Phi(g)} \sum_{\chi_d}\sum_{\psi_g} \left| \sum_{\alpha\in\mathbb{F}_{q^n}^*} \chi_d(\alpha)\psi_g(\alpha) \right|.$$

Using Lemma 2.2, we have

$$|S_6{}'| \leq q^{n/2}(2^\omega - 1)(2^\Omega - 1).$$

$$|S_7{}'| = \left| \sum_{\alpha\in\mathbb{F}_{q^n}^*} \sum_{1\neq h|q^n-1} \sum_{1\neq g|x^n-1} \frac{\mu(h)\mu'(g)}{\phi(h)\Phi(g)} \sum_{\chi_h}\sum_{\psi_g} \chi_h(\alpha^2+\alpha+1)\psi_g(\alpha) \right|$$

$$= \left| \sum_{1\neq h|q^n-1} \sum_{1\neq g|x^n-1} \frac{\mu(h)\mu'(g)}{\phi(h)\Phi(g)} \sum_{\chi_h}\sum_{\psi_g}\sum_{\alpha\in\mathbb{F}_{q^n}^*} \chi_h(\alpha^2+\alpha+1)\psi_g(\alpha) \right|$$

$$\leq \sum_{\substack{1\neq h|q^n-1,\\ h \text{ squarefree}}} \sum_{\substack{1\neq g|x^n-1,\\ g \text{ squarefree}}} \frac{1}{\phi(h)\Phi(g)} \sum_{\chi_h}\sum_{\psi_g} \left| \sum_{\alpha\in\mathbb{F}_{q^n}^*} \chi_h(\alpha^2+\alpha+1)\psi_g(\alpha) \right|.$$

By Lemma 2.5, we have $|\sum_{\alpha\in\mathbb{F}_{q^n}^*} \chi_h(\alpha^2+\alpha+1)\psi_g(\alpha)| \leq (2q^{n/2}+1)$, hence, we get

$$|S_7{}'| \leq (2q^{n/2}+1)(2^\omega - 1)(2^\Omega - 1).$$

$$|S_8{}'| = \left| \sum_{\alpha\in\mathbb{F}_{q^n}^*} \sum_{1\neq d,h|q^n-1} \sum_{1\neq g|x^n-1} \frac{\mu(d)\mu(h)\mu'(g)}{\phi(d)\phi(h)\Phi(g)} \right.$$

$$\left. \times \sum_{\chi_d,\chi_h}\sum_{\psi_g} \chi_d(\alpha)\chi_h(\alpha^2+\alpha+1)\psi_g(\alpha) \right|$$

$$= \left| \sum_{1\neq d,h|q^n-1} \sum_{1\neq g|x^n-1} \frac{\mu(d)\mu(h)\mu'(g)}{\phi(d)\phi(h)\Phi(g)} \sum_{\chi_d,\chi_h}\sum_{\psi_g}\sum_{\alpha\in\mathbb{F}_{q^n}^*} \chi_d(\alpha)\chi_h(\alpha^2+\alpha+1)\psi_g(\alpha) \right|$$

$$\leq \sum_{\substack{1\neq d,h|q^n-1,\\ d,h \text{ squarefree}}} \sum_{1\neq g|x^n-1} \frac{1}{\phi(d)\phi(h)\Phi(g)} \sum_{\chi_d,\chi_h}\sum_{\psi_g}$$

$$\times \left| \sum_{\alpha\in\mathbb{F}_{q^n}^*} \chi_d(\alpha)\chi_h(\alpha^2+\alpha+1)\psi_g(\alpha) \right|.$$

By Lemma 2.5, we have $|\sum_{\alpha\in\mathbb{F}_{q^n}^*}\chi_d(\alpha)\chi_h(\alpha^2+\alpha+1)\psi_g(\alpha)|\le 3q^{n/2}$, hence, we get

$$|S_8'|\le 3q^{n/2}(2^\omega-1)^2(2^\Omega-1).$$

Hence, we have $|N_{q^n}(q^n-1,q^n-1,x^n-1)-\theta(q^n-1)^2\Theta(x^n-1)(q^n-1)|\le \theta(q^n-1)^2\Theta(x^n-1)\{(q^{n/2}+1)(2^\omega-1)+2q^{n/2}(2^\omega-1)^2+(2^\Omega-1)+q^{n/2}(2^\omega-1)(2^\Omega-1)+(2q^{n/2}+1)(2^\omega-1)(2^\Omega-1)+3q^{n/2}(2^\omega-1)^2(2^\Omega-1)\}$.

So in order to have $N_{q^n}(q^n-1,q^n-1,x^n-1)>0$, it is sufficient to have $q^n-1>(q^{n/2}+1)(2^\omega-1)+2q^{n/2}(2^\omega-1)^2+(2^\Omega-1)+q^{n/2}(2^\omega-1)(2^\Omega-1)+(2q^{n/2}+1)(2^\omega-1)(2^\Omega-1)+3q^{n/2}(2^\omega-1)^2(2^\Omega-1)$ and this holds if

$$q^{n/2}>3\cdot 2^{2\omega+\Omega}, \tag{3.8}$$

which is the desired result. □

From (3.3), it is clear that (3.8) holds true if

$$\frac{n\log q}{\log 4}-\frac{2n\log q}{\log p_m}>2m+\frac{2\log 3}{\log 4}-\frac{2\sum_{i=1}^m\log p_i}{\log p_m}+\Omega. \tag{3.9}$$

By Lemma 2.7, it is clear that $\Omega\le an$ for a non-negative integer a, which is decided by whether $n|q-1$ or not. Using this in (3.9), we get

$$\frac{n\log q}{\log 4}-\frac{2n\log q}{\log p_m}>2m+\frac{2\log 3}{\log 4}-\frac{2\sum_{i=1}^m\log p_i}{\log p_m}+na,$$

which is equivalent to

$$\left(\frac{\log q}{\log 4}-\frac{2\log q}{\log p_m}-a\right)n>2m+\frac{2\log 3}{\log 4}-\frac{2\sum_{i=1}^m\log p_i}{\log p_m}. \tag{3.10}$$

The left-hand side of (3.10) must be positive, hence we get $\frac{1}{\log 4}-\frac{2}{\log p_m}>0\Rightarrow m\ge 7$. So we can choose a suitable $m\ge 7$ and prove that the most of (q,n) satisfy the above sufficient condition.

Hence, the values of $q=2^k$ and n such that $(q,n)\in\mathfrak{N}$ can be obtained as in the following corollary.

Corollary 3.3. *Let $q=2^k$ and n be a positive integer with $n|q-1$. If $n\ge 27$, then $(q,n)\in\mathfrak{N}$.*

Proof. By Lemma 2.7, we know that when $n|q-1$, then $\Omega=n$. Hence $a=1$. If we choose $m=25$, then from (3.9), we have

$$\log q>\frac{1+(2m+\frac{2\log 3}{\log 4}-\frac{2\sum_{i=1}^m\log p_i}{\log p_m})/n}{\frac{1}{\log 4}-\frac{2}{\log p_m}}. \tag{3.11}$$

Since $\sum_{i=1}^m\log p_i\le m\log p_m$, we get that the right-hand side of (12) is a decreasing function of n. It is easy to check that when $n=27$, then inequality holds true only

Table 2.

$n =$	1	3	5	7	9	11	13	15	17	19	21	23	25
$k \geq$	82	31	21	16	14	12	11	11	10	9	9	9	9

if $q \geq 130$. Since q is a power of 2, when $n \geq 27$ and $n|q-1$, then q has to be greater than 130. Hence $(q,n) \in \mathfrak{N}$, if $n \geq 27$. □

Remark 3.3. When $n < 25$, by using software Mathematica 4.1, we obtain the range of k such that $(2^k, n) \in \mathfrak{N}$, the result is listed in Table 2. In this case, we are considering only odd values of n as $n|q-1$.

Corollary 3.4. *Let $q = 2^k$ and n be a positive integer with $n \nmid q-1$. If $n \geq 15$ and $k \geq 10$, then $(q,n) \in \mathfrak{N}$.*

Proof. As $n \nmid q-1$ so by Lemma 2.7, we have $\Omega \leq \frac{3}{4}n$, that is $a = \frac{3}{4}$. Choose $m = 25$, then by (3.10), we have

$$n > \frac{2m - \frac{2\sum_{i=1}^{m} \log p_i}{\log p_m} + \frac{2\log(3)}{\log(4)}}{\frac{\log q}{\log 16} - \frac{2\log q}{\log p_m} - \frac{3}{4}}. \tag{3.12}$$

Since $\sum_{i=1}^{m} \log p_i \leq m \log p_m$, we get that the right-hand side of (3.12) is a decreasing function of q. It is clear that when $k \geq 10$, and $n \geq 15$, the above inequality is true that is, $(q,n) \in \mathfrak{N}$ if $n \geq 15$ and $k \geq 10$. □

Remark 3.4. The left-hand side of (3.10) is positive only if $k > 3$. Hence when $3 < k < 10$, we obtain the values of n such that $(q,n) \in \mathfrak{N}$, by using software Mathematica 4.1 and the result is listed in Table 3.

Remark 3.5. As stated in Remark 3.2, the existence of primitive normal elements $\alpha \in \mathbb{F}_{q^n}$ such that $\alpha^2 + \alpha + 1$ is primitive is not possible when $p = 3$.

Corollary 3.5. *Let $q = p^k$, where k is a positive integer and $p > 3$ is a prime and n be a positive integer with $n|q-1$. If $n \geq 39$, then $(q,n) \in \mathfrak{N}$.*

Proof. By Lemmas 2.7, 3.1 and Theorem 3.2, we see that $N_{q^n}(q^n-1, q^n-1, x^n-1) > 0$ if

$$q^{n/10} > 3C(q^n-1)^2 2^n. \tag{3.13}$$

Table 3.

$k =$	4	5	6	7	8	9
$n \geq$	396	64	34	24	19	15

Equation (3.13) is equivalent to

$$\log q > \frac{10 \log 379.69}{n} + 10 \log 2. \tag{3.14}$$

The right-hand side of (3.14) is a decreasing function of n. It can be easily checked that when $n = 39$ then (3.14) is true for all $q \geq 41$. Since $n|q-1$, if $n \geq 39$, then q will have to be greater than 41. So $(q, n) \in \mathfrak{N}$ for all $n \geq 39$ and all q such that $n|q-1$. □

Corollary 3.6. *Let $q = p^k$, where k is a positive integer and $p > 3$ is a prime and n be a positive integer with $n \nmid q-1$. If $p \geq 5$, $k \geq 3$ and $n \geq 48$, then $(q, n) \in \mathfrak{N}$.*

Proof. By Lemmas 2.7, 3.1 and Theorem 3.2, we see that $N_{q^n}(q^n-1, q^n-1, x^n-1) > 0$ if

$$q^{n/10} > 3C(q^n-1)^2 2^{\frac{3}{4}n}. \tag{3.15}$$

Equation (3.15) is equivalent to

$$n > \frac{\log 379.69}{\frac{1}{10}\log q - \frac{3}{4}\log 2}. \tag{3.16}$$

Clearly, the right-hand side of the (3.16) is a decreasing function of q and it is positive when $q > 181$. It can be easily checked that if $q = 5^3$, then (3.14) is true for all $n \geq 48$. So $(q, n) \in \mathfrak{N}$ for all $p \geq 5$, $k \geq 3$ and all $n \geq 48$. □

Acknowledgments

This work has been supported by CSIR, New Delhi, Govt. of India, Under Grant No. F.No. 09/086(1145)/2012-EMR-1. We would like to thank the referee for his valuable comments and suggestions. These have led to a better presentation and improved the quality of the paper.

References

1. G. B. Agnew, R. C. Mullin, I. M. Onyszchuk and S. A. Vanstone, An implementation for a fast public key cryptosystem, *J. Cryptology* **3** (1991) 63–79.
2. I. F. Blake, X. H. Gao, R. C. Mullin, S. A. Vanstone and T. Yaghoobian, *Applications of Finite Fields* (Kluwer Academic Publishers, Boston, 1993).
3. L. Carlitz, Primitive roots in a finite fields, *Trans. Amer. Math. Soc.* **73**(3) (1952) 373–382.
4. L. Carlitz, Some problems involving primitive roots in a finite field, *Proc. Natl. Acad. Sci. USA* **38**(4) (1952) 314–318.
5. W. S. Chou and S. D. Cohen, Primitive elements with zero traces, *Finite Fields Appl.* **7** (2001) 125–141.
6. S. D. Cohen, Consecutive primitive roots in a finite field, *Proc. Amer. Math. Soc.* **93**(2) (1985) 189–197.
7. S. D. Cohen and S. Huczynska, The primitive normal basis theorem without a computer, *J. Lond. Math. Soc.* **67**(1) (2003) 41–56.

8. S. D. Cohen and S. Huczynska, The strong primitive normal basis theorem, *Acta Arith.* **143**(4) (2010) 299–332.
9. S. D. Cohen, Pair of primitive elements in fields of even order, *Finite Fields Appl.* **28** (2014) 22–42.
10. H. Davenport, Bases for finite fields, *J. Lond. Math. Soc.* **43** (1968) 21–39.
11. L. Fu and D. Q. Wan, A class of incomplete character sums, *Q. J. Math.* **65** (2014) 1195–1211.
12. L. B. He and W. B. Han, Research on primitive elements in the form $\alpha + \alpha^{-1}$ over $\mathbb{F}_q$, *J. Inf. Eng. Univ.* **4**(2) (2003) 97–98.
13. G. Kapetanakis, Normal bases and primitive elements over finite fields, *Finite Fields Appl.* **26** (2014) 123–143.
14. H. W. Lenstra Jr. and R. J. Schoof, Primitive normal bases for finite fields, *Math. Comp.* **48** (1987) 217–231.
15. Q. Liao, J. Li and K. Pu, On the existence for some special primitive elements in finite fields, *Chin. Ann. Math. B* **37** (2016) 259–266.
16. R. Lidl and H. Niederreiter, *Finite Fields*, 2nd edn. (Cambridge University Press, Cambridge, 1997).
17. J. L. Massey and J. K. Omura, Computational method and apparatus for finite field arithmatic, US Patent 4587627 (1986).
18. R. C. Mullin, I. M. Onyszchuk and S. A. Vanstone, Computational method and apparatus for finite field multiplication, US Patent 4745568.
19. T. Tian and W. F. Qi, Primitive normal element and its inverse in finite fields, *Math. Comp. Acta Math. Sinica* (Chin. Ser.) **49**(3) (2006) 657–668.
20. D. Q. Wan, Generators and irreducible polynomials over finite fields, *Math. Comp.* **66** (1997) 1195–1212.
21. P. P. Wang, X. W. Cao and R. Q. Feng, On the existence of some specific elements in finite fields of characteristic 2, *Finite Fields Appl.* **18**(4) (2012) 800–813.