Journal of Number Theory ••• (••••) •••–•••

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Existence of pair of primitive elements over finite fields of characteristic 2

Rajendra K. Sharma *, Ambrish Awasthi, Anju Gupta

Department of Mathematics, IIT Delhi, Hauz Khas, New Delhi 110016, India

ARTICLE INFO

Article history:
Received 23 August 2017
Received in revised form 23 March 2018
Accepted 14 May 2018
Available online xxxx
Communicated by A. Pal

MSC:
12E20
11T23

Keywords:
Finite field
Primitive element
Character

ABSTRACT

In this article, we give a sufficient condition for the existence of a primitive element α in $\mathbb{F}_{2^k}$ such that $f(\alpha)$ is also primitive in $\mathbb{F}_{2^k}$, where $f(x) = \frac{ax^2+bx+c}{dx^2+ex+f} \in \mathbb{F}_{2^k}(x)$ with $a, d \neq 0$. Subsequently, using this condition we derive the values of k for which $\mathbb{F}_{2^k}$ contains primitive pairs of the form $(\alpha, f(\alpha))$ for $f(x) = \frac{ax^2+bx+c}{dx^2+ex+f}$ and $a, d \neq 0$.

1. Introduction

Let $\mathbb{F}_q$ be a finite field with $q = p^k$ elements. An element $\alpha \in \mathbb{F}_q$ is said to be *primitive* if α is a generator of the multiplicative cyclic group $\mathbb{F}_q^*$ of non zero elements of $\mathbb{F}_q$. The least degree monic polynomial over $\mathbb{F}_p$ having α as a root is called a *primitive polynomial*. Primitive elements find a lot of applications in cryptography and coding

* Corresponding author.
E-mail addresses: rksharma@maths.iitd.ac.in (R.K. Sharma), ambrishawasthi@yahoo.com (A. Awasthi), anjugju@gmail.com (A. Gupta).

https://doi.org/10.1016/j.jnt.2018.05.016
0022-314X/

theory as they are generators of groups of non zero elements of finite fields. Some of the areas in cryptography like Diffie–Hellman key exchange protocol and discrete log problem find lot of applications of primitive elements. Therefore it becomes very important to investigate an element for primitivity. Another interesting problem related to primitive elements is the existence of primitive pairs $(\alpha, \beta) \in \mathbb{F}_q$ where β is some rational function of α over $\mathbb{F}_q$.

We define a pair $(\alpha, f(\alpha))$ in $\mathbb{F}_q \times \mathbb{F}_q$ as a *primitive pair* in $\mathbb{F}_q$, for some rational function $f(x) \in \mathbb{F}_q(x)$, if α and $f(\alpha)$ both are primitive in $\mathbb{F}_q$. Given an element $\alpha \in \mathbb{F}_q$ it is very difficult, in general, to say whether $f(\alpha)$ is primitive in $\mathbb{F}_q$. However some progress has been made in this area for suitable $f(x)$. Firstly given $\alpha, f(\alpha)$ need not be a primitive element for example take $\alpha = 1$ and $f(x) = x + 1$ over $\mathbb{F}_2$. Taking $f(x) = \frac{1}{x}$, we see that $(\alpha, f(\alpha) = \frac{1}{\alpha})$ is always a primitive pair in $\mathbb{F}_q$, for all q, whenever α is primitive. Cohen in this direction proved the existence of primitive pairs $(\alpha, f(\alpha) = \alpha + \frac{1}{\alpha})$. Cohen [5] also proved that primitive pairs of the form $(\alpha, f(\alpha) = (\alpha+1))$ exist for $q \geq 3, q \not\equiv 7 \pmod{12}$ and $q \not\equiv 1 \pmod{60}$. Chou and Cohen [4] further proved the existence of primitive pairs $(\alpha, f(\alpha) = \frac{1}{\alpha})$ such that α and $f(\alpha)$ both have trace zero over $\mathbb{F}_q$. Wang et al. [12] proved the existence of primitive pairs $(\alpha, f(\alpha) = \alpha + \frac{1}{\alpha})$ in $\mathbb{F}_{q^n}$ where $q = 2^k, k \geq 4$, for odd $n \geq 13$. Cohen finally settled the question for $\mathbb{F}_{2^k}$ raised by Wang et al. by proving the following result.

Theorem 1.1. *[6, Theorem 1] Let $q \geq 8$ be a power of 2. Then $\mathbb{F}_q$ contains a primitive pair $(\alpha, f(\alpha) = \alpha + \frac{1}{\alpha})$.*

A *normal element* of a field $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ is an element $\alpha \in \mathbb{F}_{q^n}$ such that $\{\alpha, \alpha^q \ldots \alpha^{q^{n-1}}\}$ forms a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. We define a pair $(\alpha, f(\alpha))$ in $\mathbb{F}_{q^n} \times \mathbb{F}_{q^n}$ as a *normal pair* of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, for some rational function $f(x) \in \mathbb{F}_{q^n}(x)$, if α and $f(\alpha)$ both are normal elements of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Kapetanakis considered the problem of existence of primitive pairs of the form $(\alpha, f(\alpha) = \frac{a\alpha+b}{c\alpha+d})$ simultaneously with the condition that the pair is normal. He gave the following result.

Theorem 1.2. *[10] Let $q \geq 23$ be a prime power, $n \geq 17$ an integer and $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{F}_q)$, such that if A has exactly two non-zero entries and q is odd, then the quotient of these entries is a square in $\mathbb{F}_{q^n}$. There exists some $\alpha \in \mathbb{F}_{q^n}$ such that both α and $\frac{a\alpha+b}{c\alpha+d}$ are simultaneously primitive and normal.*

Anju and Sharma studied the problem of existence of primitive pairs $(\alpha, f(\alpha))$ where $f(x) = x^2 + x + 1$ and proved the following result.

Theorem 1.3. *[3, Theorem 3.1] Let $q = p^k$ for some prime $p \neq 3$ and n be a positive integer and let $\omega(q^n - 1)$ be the number of prime divisors of $q^n - 1$. If $q^{\frac{n}{2}} > 2^{2\omega(q^n-1)+1}$, then there exists a primitive pair $(\alpha, f(\alpha) = (\alpha^2 + \alpha + 1))$ in $\mathbb{F}_q$.*

Please cite this article in press as: R.K. Sharma et al., Existence of pair of primitive elements over finite fields of characteristic 2, J. Number Theory (2018), https://doi.org/10.1016/j.jnt.2018.05.016