Finite Fields and Their Applications 51 (2018) 388–406

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Linear combinations of primitive elements of a finite field

Stephen D. Cohen [a], Tomás Oliveira e Silva [b], Nicole Sutherland [c], Tim Trudgian [d,*,1]

[a] *School of Mathematics and Statistics, University of Glasgow, Scotland, UK*
[b] *Departamento de Electrónica, Telecomunicações e Informática / IEETA, University of Aveiro, Portugal*
[c] *Computational Algebra Group, School of Mathematics and Statistics, University of Sydney, Australia*
[d] *School of Physical, Environmental and Mathematical Sciences, The University of New South Wales Canberra, Australia*

ARTICLE INFO

Article history:
Received 17 November 2017
Received in revised form 2 February 2018
Accepted 26 February 2018
Communicated by Steven Wang

MSC:
11T30
11L03

Keywords:
Primitive roots
Finite fields
Character sums
Prime sieve

ABSTRACT

We examine linear sums of primitive roots and their inverses in finite fields. In particular, we refine a result by Li and Han, and show that every $p > 13$ has a pair of primitive roots a and b such that $a + b$ and $a^{-1} + b^{-1}$ are also primitive roots mod p.

* Corresponding author.
E-mail addresses: stephen.cohen@glasgow.ac.uk (S.D. Cohen), tos@ua.pt (T. Oliveira e Silva), nicole.sutherland@sydney.edu.au (N. Sutherland), t.trudgian@adfa.edu.au (T. Trudgian).

[1] Supported by Australian Research Council Future Fellowship FT160100094.

https://doi.org/10.1016/j.ffa.2018.02.009
1071-5797/

1. Introduction

Let $\mathbb{F}_q$ denote the finite field of order q, a power of the prime p. The proliferation of primitive elements of $\mathbb{F}_q$ gives rise to many interesting properties. For example, it was proved in [4] that for any non-zero $\alpha, \beta, \epsilon \in \mathbb{F}_q$ the equation $\epsilon = a\alpha + b\beta$ is soluble in primitive elements a, b provided that $q > 61$. Since a is primitive if and only if a^{-1}, its multiplicative inverse in $\mathbb{F}_q$, is primitive, one may look for linear relations amongst primitive elements and their inverses and, as in the above example, seek a lower bound on q beyond which such relations hold – this is the purpose of the current paper.

Given arbitrary non-zero elements $u, v \in \mathbb{F}_q$, call a pair (a, b) of primitive elements of $\mathbb{F}_q$ (u, v)-*primitive* if additionally the elements $ua + vb$ and $va^{-1} + ub^{-1}$ are each primitive. The task is to find an asymptotic expression for $N = N(q, u, v)$, defined as the number of (u, v)-primitive pairs (a, b) in $\mathbb{F}_q$.

In the situation in which $\mathbb{F}_q$ is a prime field, i.e., $q = p$, this problem was introduced by Li and Han [7]. In that context, a, b are considered to be integers in $I_p = \{1, 2, \dots, p-1\}$ with inverses $a^{-1}, b^{-1} \in I_p$. Similarly, u, v can be taken to be in I_p. To state the result of [7] we introduce some notation. For a positive integer m let $\omega(m)$ be the number of distinct prime divisors of m and $W(m) = 2^{\omega(m)}$ be the number of square-free divisors of m. Further, define $\theta(m)$ as $\phi(m)/m$, where ϕ is Euler's function, and $\tau(m) = \prod_{l|m} \left(1 - \frac{1}{l-1} + \frac{1}{(l-1)^2}\right)$, where the product is taken over all $\omega(m)$ distinct prime divisors l of m.

Theorem 1 *(Li–Han). Let p be an odd prime and n any integer in I_p. Set $\theta = \theta(p-1)$, $\tau = \tau(p-1)$ and $W = W(p-1)$. Then*

$$\left|N(p, 1, n) - \theta^3 \tau \cdot (p-1)^2\right| \le 5\theta^4 W^4 p^{3/2}. \tag{1.1}$$

Li and Han gave the following as corollaries to Theorem 1.

Corollary 1 *(Li–Han). Every sufficiently large p has primitive roots a and b such that both $a+b$ and $a^{-1}+b^{-1}$ are also primitive. Also, every sufficiently large p has primitive roots a and b such that both $a-b$ and $b^{-1}-a^{-1}$ are also primitive.*

We establish an improved estimate for $N(q, u, v)$ in the case of a general finite field.

Theorem 2. *Let $q > 2$ be a prime power. Set $\theta = \theta(q-1), \tau = \tau(q-1), W = W(q-1)$. Then, for arbitrary non-zero $u, v \in \mathbb{F}_q$,*

$$\left|N(q, u, v) - \theta^3 \tau \cdot (q-1)\ q\right| \le \theta^4 W^3 \cdot (q-1)\sqrt{q}. \tag{1.2}$$

The principal improvement in Theorem 2 over Theorem 1 is the reduction from W^4 to W^3 in the error term. Its effect can be described as follows. Let $\mathcal{S}$ be the set of prime powers q such that, for any pair of non-zero elements (u, v) in $\mathbb{F}_q$, there exists a