ARTICLE IN PRESS YJNTH:5757

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

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Differences between elements of the same order in a finite field

Joshua Harrington[a], Lenny Jones[b,*]

[a] Department of Mathematics, Cedar Crest College, Allentown, PA, USA
[b] Department of Mathematics, Shippensburg University, PA, USA

ARTICLE INFO

Article history:
Received 23 January 2017
Received in revised form 12 April 2017
Accepted 20 April 2017
Available online xxxx
Communicated by D. Goss

MSC:
primary 11A07
secondary 11B39, 12Y05

Keywords:
Finite field
Order
Resultant
Primitive root
Primitive divisor

ABSTRACT

In 1975, Michael Szalay showed that for any prime $p > 10^{19}$ and any integer δ with $1 \leq \delta \leq p-1$, there exist at least two primitive roots g and h modulo p such that $g - h \equiv \delta \pmod{p}$. Very recently, Brazelton, Harrington, Kannan and Litman have shown that for any $n > 6$, there exists a prime $p \equiv 1 \pmod{n}$ for which there are two elements a and b of order n modulo p such that $a - b \equiv 1 \pmod{p}$. In this article, we extend these ideas to investigate arbitrary differences δ between elements of the same arbitrary order n modulo a prime $p \equiv 1 \pmod{n}$. Moreover, we show how all elements of a specific order n can be derived from a single fixed difference δ. Finally, we deduce a result concerning the differences between primitive roots for certain primes $p \equiv 3 \pmod{4}$.

1. Introduction

In 1975, Michael Szalay [9] proved the following theorem.

* Corresponding author.
E-mail addresses: Joshua.Harrington@cedarcrest.edu (J. Harrington), lkjone@ship.edu (L. Jones).

http://dx.doi.org/10.1016/j.jnt.2017.04.008
0022-314X/© 2017 Elsevier Inc. All rights reserved.

Theorem 1.1. *For all primes $p > 10^{19}$ and any integer δ with $1 \leq \delta \leq p-1$, there exist at least two primitive roots g and h modulo p such that $g - h \equiv \delta \pmod{p}$.*

Very recently, Brazelton, Harrington, Kannan and Litman [2] have broadened the focus from elements of order $p-1$ to elements of arbitrary order n modulo p, while fixing the difference δ between elements of the same order n at $\delta = 1$. In particular, they have proven the following result.

Theorem 1.2. *There exists a prime $p \equiv 1 \pmod{n}$ such that the finite field $\mathbb{F}_p$ contains consecutive elements of order n if and only if $n \notin \{1, 2, 3, 6\}$.*

In this article, we extend these ideas to investigate arbitrary differences δ between elements of the same arbitrary order n in the finite field $\mathbb{F}_p$. More precisely, we prove the following.

Theorem 1.3. *Let $\delta \geq 1$, $n \geq 3$ and $m \geq 3$ be integers such that m is not a power of 2, and let*

$$\mathcal{B} = \{(1,3), (1,6), (2,4), (2,8), (2,4m), (3,3), (3,6)\}.$$

Then, for any pair $(\delta, n) \notin \mathcal{B}$, there exists a prime $p \equiv 1 \pmod{n}$, $p < (\delta+2)^n$, with elements $\alpha, \beta \in \mathbb{F}_p$ of order n such that

$$\alpha - \beta \equiv \delta \pmod{p}.$$

Moreover, all elements of order n in $\mathbb{F}_p$ can be effectively determined in terms of δ.

Remark 1.4. We conjecture that the set $\mathcal{B}$ in Theorem 1.3 can be reduced to

$$\mathcal{B} = \{(1,3), (1,6), (2,4), (2,8), (2,12), (2,24), (3,3), (3,6)\}.$$

Corollary 1.5. *Let $\delta \geq 1$ be an integer. If $p \equiv 3 \pmod{4}$ is prime and p is a primitive divisor of $L_{(p-1)/2}(\delta)$, where $L_{(p-1)/2}(\delta)$ is the Lucas polynomial of index $(p-1)/2$ specialized at δ, then there exist primitive roots α and β modulo p such that*

$$\alpha - \beta \equiv \delta \pmod{p}.$$

Moreover, all primitive roots can be effectively determined in terms of δ.

2. General preliminaries

For an integer $m \geq 0$, we define the mth Fermat number as $F_m = 2^{2^m} + 1$. The following theorem is due to Lucas [7].

Please cite this article in press as: J. Harrington, L. Jones, Differences between elements of the same order in a finite field, J. Number Theory (2017), http://dx.doi.org/10.1016/j.jnt.2017.04.008