Finite Fields and Their Applications 46 (2017) 139–146

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Nonexistence of twenty-fourth power residue addition sets

Ron Evans [a,*], Mark Van Veen [b]

[a] *Department of Mathematics, University of California at San Diego, La Jolla, CA 92093-0112, United States*
[b] *Varasco LLC, 2138 Edinburg Avenue, Cardiff by the Sea, CA 92007, United States*

ARTICLE INFO

Article history:
Received 23 November 2016
Received in revised form 2 February 2017
Accepted 17 March 2017
Available online xxxx
Communicated by Stephen D. Cohen

MSC:
05B10
11T22
11T24
15A06

Keywords:
Power residues
Difference sets
Qualified difference sets
Jacobi sums
Cyclotomic numbers

ABSTRACT

Let $n > 1$ be an integer, and let $\mathbb{F}_p$ denote a field of p elements for a prime $p \equiv 1 \pmod{n}$. By 2015, the question of existence or nonexistence of n-th power residue difference sets in $\mathbb{F}_p$ had been settled for all $n < 24$. We settle the case $n = 24$ by proving the nonexistence of 24-th power residue difference sets in $\mathbb{F}_p$. We also prove the nonexistence of *qualified* 24-th power residue difference sets in $\mathbb{F}_p$. The proofs make use of a Mathematica program which computes formulas for the cyclotomic numbers of order 24 in terms of parameters occurring in quadratic partitions of p.

* Corresponding author.
E-mail addresses: revans@ucsd.edu (R. Evans), mark@varasco.com (M. Van Veen).

http://dx.doi.org/10.1016/j.ffa.2017.03.009
1071-5797/

1. Introduction

For an integer $n > 1$, let p be a prime of the form $p = nf + 1$. Let H_n denote the set of nonzero n-th power residues in $\mathbb{F}_p$, where $\mathbb{F}_p$ is the field of p elements. For $\epsilon \in \{0, 1\}$, define $H_{n,\epsilon} = H_n \cup \{1 - \epsilon\}$. Note that the set $H_{n,\epsilon}$ has $f + \epsilon$ elements.

Fixing $m \in \mathbb{F}_p^*$, Lam [12] called $H_{n,\epsilon}$ an n-th power residue addition set if the list of differences $s - mt \in \mathbb{F}_p^*$ with $s, t \in H_{n,\epsilon}$ hits each element of $\mathbb{F}_p^*$ the same number of times. If m is an n-th power residue, such an addition set is called an n-th power residue difference set. If m is not an n-th power residue, then as in [3, p. 94], such an addition set is called a qualified n-th power residue difference set with qualifier m.

Let g denote a primitive root modulo p. For integers s, t modulo n, the cyclotomic number $C_n(s, t)$ of order n is defined to be the number of elements $N \in \mathbb{F}_p$ for which both N/g^s and $(N + 1)/g^t$ are nonzero n-th power residues in $\mathbb{F}_p$. If $H_{n,\epsilon}$ is a difference set, then necessarily [9, p. 677] n is even, f is odd, and

$$n^2 C_n(s, 0) = p - 1 + 2n\epsilon - n, \quad 1 \le s < n/2. \tag{1.1}$$

If $H_{n,\epsilon}$ is a qualified difference set, then necessarily [3, Theorems 2.1 and 2.2] n is even, f is even, and

$$n^2 C_n(s, n/2) = p - 1 + 2n\epsilon, \quad 1 \le s < n/2. \tag{1.2}$$

For $n < 24$, it is known that $H_{n,\epsilon}$ can be a difference set only in the three exceptional cases $H_{2,\epsilon}$, $H_{4,\epsilon}$, $H_{8,\epsilon}$ listed in [3, (1.1)–(1.3)]. This follows from the work of a number of different authors during the period 1933–2015. For references, consult Xia [13], who has extended the results to fields of q elements, where q is a prime power. In Section 4, we prove that $H_{24,\epsilon}$ cannot be a difference set, by showing that (1.1) cannot hold for $n = 24$. Partial results in this direction had been obtained in 1983 by the first author [9].

For $n < 22$, it is known that $H_{n,\epsilon}$ can be a qualified difference set only in the three exceptional cases $H_{2,\epsilon}$, $H_{4,\epsilon}$, $H_{6,\epsilon}$ listed in [3, (1.4)–(1.6)]. In Section 3, we prove that $H_{24,\epsilon}$ cannot be a qualified difference set, by showing that (1.2) cannot hold for $n = 24$.

Our proofs depend on formulas for the cyclotomic numbers $C_{24}(s, t)$. Printed tables of these formulas were archived in 1979 [8], but it is much more useful to have digital access. Thus we wrote a Mathematica program [10] to compute the formulas for $C_{24}(s, t)$. This program is described in the next section.

We remark that besides their use for analyzing power residue difference sets, cyclotomic numbers have applications to such topics as counting points on elliptic curves [14], Gauss periods and complexity of normal bases for finite fields [4,11], cyclic codes [6], cryptographic functions [5], residuacity [1, Chapter 7], linear complexity of sequences [2], and almost difference sets [7].