An extension for residue difference sets

Derek Jennings a,*, Kevin Byard b

a Faculty of Mathematics, University of Southampton, Southampton, Hampshire, S017 1BJ, UK
b Department of Physics, University of Southampton, Southampton, Hampshire, S017 1BJ, UK

Abstract

In this paper we extend the idea of residue difference sets, with existence theorems being established for certain classes of primes.

1. Introduction

Lehmer showed [8] that there do not exist any residue difference sets of sextic residues modulo a prime p, and Chowla showed [4] that the biquadratic residues modulo p, where \( p \equiv 1 (\text{mod} 4) \), form a difference set if

\[
\frac{p - 1}{4} = x^2,
\]

where \( x \) is an odd integer. In this paper we extend the idea of a residue difference set to recover ‘residue difference sets’ for sextic residues. We will refer to this new type of residue difference set as a qualified residue difference set. For both biquadratic and sextic residues we determine precisely those primes \( p \) for which these qualified residue difference sets exist.

Qualified residue difference sets have properties similar to those of the established residue difference sets [1,8], and may therefore have applications in fields such as digital space communications [6], aperture synthesis [7], and gamma-ray coded aperture imaging [3]. What is of use here is the following two-valued property of a sum function which we illustrate with \( p = 17 \) (see Theorem 1).

Take the quadratic residues of 17 which are not biquadratic residues, that is \{2, 8, 9, 15\} (the biquadratic residues of 17 are \{1, 4, 13, 16\}). Count the number of the set \{2 + t, 8 + t, 9 + t, 15 + t\} which are biquadratic residues of 17 for each \( t \) from 0 to 16 (= \( p - 1 \)). We find that for \( t = 0 \) this sum is 0 and for \( 1 \leq t \leq 16 \) this sum is 1.

* Corresponding author.
Definition. Let $R = \{r_1, r_2, \ldots, r_k\}$ be the set of $n$th power residues of a prime $p = kn + 1$. We call $R$ a qualified residue difference set if there exists some non-zero integer $m \notin R$ which is such that if we form all the non-zero differences

$$r_i - mr_j \pmod{p}: \ 1 \leq i, j \leq k,$$

we obtain every positive integer $\leq p - 1$ exactly $\lambda$ times. $m$ will be called a qualifier, of multiplicity $\lambda$, for $R$.

2. The main results

The purpose of this paper is to present the following two theorems. All of the primes given by these theorems yield sum functions with a two-valued property similar to that illustrated with $p = 17$ in the introduction.

Theorem 1. Biquadratic qualified residue difference sets exist for prime $p$ if and only if

$$p = 16x^2 + 1,$$

where $x$ is an integer, and the qualifiers are exactly all the quadratic residues which are not biquadratic residues.

So the sequence of primes having biquadratic qualified residue difference sets starts $17, 257, 401, \ldots$

Theorem 2. Sextic qualified residue difference sets exist for prime $p$ if and only if

$$p = 108x^2 + 1,$$

where $x$ is an integer, and the qualifiers are exactly all the cubic residues which are not sextic residues.

So the sequence of primes having sextic qualified residue difference sets starts $109, 433, 3889, \ldots$

3. A necessary and sufficient condition for qualified residue difference sets

We first establish a few short lemmas and some preliminary results.

Lemma 1. If $m$ is a qualifier for the qualified residue difference set $R$ then $mr_1, mr_2, \ldots, mr_k$ are also qualifiers for $R$.

Proof. $mR = mr_iR$ for all $r_i$. □
Lemma 2. If $m$ is a qualifier for $R$ then 

\[ \lambda = \frac{k}{n} \text{ and } p = \lambda n^2 + 1, \]

where $p = kn + 1$ and $\lambda$ is the multiplicity of $m$.

**Proof.** Since $m \not\in R$ there are $k^2$ non-zero differences $r_i - mr_j$. Hence $(p - 1)\lambda = k^2$. \[ \square \]

Let $p = kn + 1$ be a prime and $g$ a primitive root of $p$. We say that the number $N$ belongs to residue class $\sigma$ with respect to $g$ if for some $0 \leq i \leq k - 1$ 

\[ N \equiv g^{i+n} \pmod{p}. \]

The cyclotomic constant $(i, j)$ denotes the number of solutions of the congruence 

\[ 1 + g^{in+i} \equiv g^{i+n+j} \pmod{p}, \]

where $0 \leq i, j \leq n - 1$ and $0 \leq u, v \leq k - 1$. The definition of $(i, j)$ is extended to $\mathbb{Z} \times \mathbb{Z}$ by periodicity modulo $n$. We have from Dickson [5]:

\[ (i, j) = (j, i) \quad \text{if } k \text{ even}, \quad (1) \]

\[ (i, j) = (j + n/2, i + n/2) \quad \text{if } k \text{ odd}, \quad (2) \]

\[ \sum_{j=0}^{n-1} (i, j) = k - \delta_i, \quad i = 0, 1, \ldots, (n - 1), \quad (3) \]

where

\[ \delta_i = \begin{cases} 1 & \text{if } k \text{ is even and } i = 0, \text{ or if } k \text{ is odd and } i = n/2, \\ 0 & \text{otherwise}. \end{cases} \]

The following theorem gives a necessary and sufficient condition for a qualified residue difference set to exist.

**Theorem 3.** $m$ is a qualifier for the residue set $R = \{r_1, r_2, \ldots, r_k\}$ of $n$th power residues of $p = kn + 1$, where $m$ belongs to residue class $n - \sigma$ ($\sigma \neq 0$, since $m \not\in R$), if and only if the cyclotomic constants 

\[ (s, \sigma) = \frac{k}{n}, \]

where $s = 0, 1, \ldots, (n - 1)$ and $k/n = \lambda$ is the multiplicity of the qualified residue difference set.

**Proof.** Suppose that $m$ is a qualifier for the set $R$ of $n$th power residues of a prime $p = kn + 1$, belonging to residue class $n - \sigma$ and of multiplicity $\lambda$. For each $t = 1, 2, \ldots, (p - 1)$ the congruence modulo $p$

\[ r_i - mr_j \equiv t \]
has exactly $\lambda$ solutions. Multiplying through by $\tilde{m}\tilde{r}_j$, where $m\tilde{m} \equiv 1$ and $r_j\tilde{r}_j \equiv 1$, we have

$$m\tilde{m}\tilde{r}_j + 1 \equiv \tilde{m}r_j.$$

(4)

Since $m$ belongs to residue class $n-\sigma$, $\tilde{m}$ belongs to residue class $\sigma$. Now $m\tilde{m}\tilde{r}_j$ belongs to residue class $\sigma + s$, where $s$ is the residue class of $t$, and $\tilde{m}r_j\tilde{r}_j$ belongs to residue class $\sigma$. Now $t$ takes on any value from 1 to $(p-1)$ and (4) always has $\lambda$ solutions. Hence, we have

$$(\sigma + s, \sigma) = \lambda \quad \text{for } s = 0, 1, \ldots, (n-1),$$

and so

$$(s, \sigma) = \lambda \quad \text{for } s = 0, 1, \ldots, (n-1).$$

Therefore, we have shown the necessity of the condition in Theorem 3. We now need to prove that it is sufficient.

Suppose that the $(s, \sigma)$ are all equal for a given $\sigma \neq 0$ then we have

$$(s, \sigma) = \sum_{i=0}^{n-1} (i, \sigma)/n.$$  

(5)

For even $k$, using (1) and (3), since $\sigma \neq 0$ we have

$$\sum_{i=0}^{n-1} (i, \sigma) = \sum_{i=0}^{n-1} (\sigma, i) = k.$$  

For odd $k$, using (2) for the first equality, periodicity modulo $n$ for the second and (3), along with $\sigma \neq 0$, for the third equality we have

$$\sum_{i=0}^{n-1} (i, \sigma) = \sum_{i=0}^{n-1} (\sigma + n/2, i + n/2)$$

$$= \sum_{i=0}^{n-1} (\sigma + n/2, i) = k.$$  

Hence in both cases it follows that

$$\sum_{i=0}^{n-1} (i, \sigma) = k.$$  

(6)

Therefore we have from (5) and (6), $(s, \sigma) = \lambda$. Hence, the condition is sufficient and Theorem 3 is proved. □

**Corollary.** Qualified quadratic residue difference sets exist if and only if $p \equiv 1 \pmod{4}$.  

Proof. For all primes \( p \equiv 1 (\text{mod} 4) \) we have \([5, \text{p.394 (18)}]\)

\[
(0, 1) = (1, 1) = (p - 1)/4.
\]

Therefore no such sets exist for \( p \equiv 3 (\text{mod} 4) \) and by the above theorem they do exist for all \( p \equiv 1 (\text{mod} 4) \).

The above corollary contrasts with the normal residue difference set case where a quadratic residue difference set exists for \( p \equiv 3 (\text{mod} 4) \) and no such set exists for \( p \equiv 1 (\text{mod} 4) \) [8].

4. Proof of Theorem 1

The proofs of Theorems 1 and 2 are similar in that they both use Theorem 3 and make extensive use of formulae from [5]. Since the proofs are essentially case by case checks, for brevity we present only the proof of Theorem 1.

Proof. Let \( n = 4 \) and \( m \) be a qualifier for the set of residues \( R \), where \( m \) belongs to residue class \( 4 - \sigma \). Since \( m \not\in R \) we have \( \sigma \neq 0 \). Therefore, \( \sigma = 1, 2 \) or \( 3 \). First, we show that we must have \( \sigma = 2 \).

Suppose \( \sigma = 1 \), then by Theorem 3 we have \((0, 1) = (p - 1)/16\). Now Lemma 2 shows, for \( n = 4 \), \( p = 16\lambda + 1 \). Hence \( k = 4\lambda \) is even, and for even \( k \) \((0, 1) = (1, 0)\) by (1). Therefore,

\[
(1, 0) = (p - 1)/16.
\]

For \( n = 4 \) the cyclotomic constant \((1,0)\) was given by Gauss in terms of the quadratic partition \( p = A^2 + 4B^2 \), \( A \equiv 1 (\text{mod} 4) \). We have

\[
16(1,0) = p - 2A - 3.
\]

However, (8) and (9) imply \( A = -1 \) which is a contradiction, since \( A \equiv 1 (\text{mod} 4) \). Therefore, \( \sigma \neq 1 \). Suppose \( \sigma = 3 \), then by Theorem 3 we have

\[
(3, 3) = (p - 1)/16.
\]

Now from [5, \text{p. 400 (48)}] \((3, 3) = (0, 1) = (1, 0)\). So using (9) and (10) we again have \( A = -1 \), a contradiction. Therefore, \( \sigma \neq 3 \).

Hence, we can only have \( \sigma = 2 \). So suppose \( \sigma = 2 \), then by Theorem 3, we have

\[
(0, 2) = (p - 1)/16,
\]

and from [5, \text{p. 400 (52)}] we have

\[
16(0,2) = p - 3 + 2A,
\]

where \( p = A^2 + 4B^2 \), \( A \equiv 1 (\text{mod} 4) \). Now (11) and (12) combine to give \( A = 1 \). Hence we must have \( p = 1 + 4B^2 \), and since \( p \equiv 1 (\text{mod} 16) \), by Lemma 2, \( B \) must be even. Therefore, \( p = 16x^2 + 1 \).
We now need to prove the converse i.e. if \( p = 16x^2 + 1 \) then a qualifier belonging to residue class 2 for the biquadratic residues of \( p \) exists. From Theorem 3 it is enough to show

\[ (0, 2) = (1, 2) = (2, 2) = (3, 2) = (p - 1)/16. \]  \hspace{1cm} (13)

From [5, p. 400 (48)] we have

\[ (0, 2) = (2, 2) \quad \text{and} \quad (1, 2) = (3, 2), \]  \hspace{1cm} (14)

and from [5, p. 400 (52)] we have

\[ 16(1, 2) = p + 1 - 2A, \]  \hspace{1cm} (15)

where \( p = A^2 + 4B^2, A \equiv 1 \pmod{4} \). Now \( p = 16x^2 + 1 \) and so \( A = 1 \), since the representation of \( p \) as the sum of two squares is unique up to order and sign. Now (12), (14) and (15) combine to give (13), and so the converse is proved. Since any qualifier must belong to residue class 2, we can now use Lemma 1 to show that the qualifiers are exactly the members of residue class 2. That is, they are the quadratic residues which are not biquadratic residues. Hence Theorem 1 is proved. \( \square \)

References