Qualified residue difference sets with zero

Derek Jennings*, Kevin Byard

Faculty of Mathematics, University of Southampton, Southampton, Hampshire, SO17 1BJ, UK

Received 13 February 1996; revised 24 January 1997; accepted 24 February 1997

Abstract

We previously established that biquadratic qualified residue difference sets exist for primes $p$ if and only if $p = 16x^2 + 1$ and sextic qualified residue difference sets exist if and only if $p = 108x^2 + 1$. For example such sets exist for the primes 17 and 109, respectively. In this paper we point out that if zero is counted as a residue then we can obtain further qualified residue difference sets for both the biquadratic and the sextic residues. We give two theorems which state precisely when such biquadratic and sextic residue sets exist and a further existence theorem for more general powers.

AMS classification: 11T22; 05B10

1. Introduction

Lehmer showed [9] that there do not exist any residue difference sets of sextic residues. In [7] we extended the idea of a residue difference set to recover sextic difference sets for primes of the form $108x^2 + 1$. The new type of difference sets, called a qualified residue difference sets (qrds for short), is defined as follows.

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 $m \not\in R$ which is such that if we form all the non-zero differences

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

We obtain every positive integer $\leq p - 1$ exactly $\lambda$ times. We call $m$ a qualifier of multiplicity $\lambda$ for $R$.

* Correspondence address: 4 Barford Close, North Millers Dale, Chandlers Ford, Hampshire, SO53 1TH, UK.
Biquadratic qrds exist if and only if \( p = 16x^2 + 1 \) and sextic qrds exist if and only if \( p = 108x^2 + 1 \). If zero is counted as a residue we can obtain further qrds for both biquadratic and sextic residues. It may be of some interest to compare our results with the following known results for the biquadratic case:

1. the non-zero fourth powers in \( F_p \) form a regular difference set when \( p \) is a prime of the form \( 4x^2 + 1 \), for odd \( x \), and
2. the non-zero fourth powers including zero in \( F_p \) form a regular difference set when \( p \) is a prime of the form \( 4x^2 + 9 \), for odd \( x \).

Similar to the former qrds these new difference sets may have applications in fields such as digital space communications [6], aperture synthesis [8] and gamma-ray coded aperture imaging [2, 3].

2. The biquadratic and sextic residues

**Theorem 1.** The biquadratic residues and zero form a qualified residue difference set modulo \( p \) if and only if

\[ p = 16x^2 + 9, \]

where \( x \) is an integer. The qualifiers are exactly all the quadratic residues which are not biquadratic residues.

**Theorem 2.** The sextic residues and zero form a qualified residue difference set modulo \( p \) if and only if

\[ p = 108x^2 + 25, \]

where \( x \) is an integer. The qualifiers are exactly all the cubic residues which are not sextic residues.

The sequence of primes having such biquadratic difference sets starts 73, 409, 1033, … and for sextic sets the sequence starts 457, 997, 1753, … .

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

To establish Theorem 3 and hence Theorems 1 and 2 we require the following lemma.

**Lemma.** If \( m \) is a qualifier for \( R^* = \{0, r_1, r_2, \ldots, r_k\} \) (the set of \( n \)th power residues and zero) then

\[ \lambda = (k + 2)/n \quad \text{and} \quad p = \lambda n^2 - 2n + 1, \]

where \( p = kn + 1 \) and \( \lambda \) is the multiplicity of \( m \).
Proof. There are \((k + 1)^2\) differences (including zero)
\[ r_i - mr_j \pmod{p}, \]
where \(r_i, r_j \in R^\ast\). Zero appears only once and the numbers \(1, 2, \ldots, p - 1\) appear exactly \(\lambda\) times. Hence
\[ \lambda(p - 1) + 1 = (k + 1)^2. \]
Now \(p = kn + 1\) and so \(\lambda kn + 1 = (k + 1)^2\). Therefore \(\lambda = (k + 2)/n\). Substituting \(k = \lambda n - 2\) in \(p = kn + 1\) gives \(p = \lambda n^2 - 2n + 1\). □

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 \(0 \leq i \leq k - 1\)
\[ N \equiv g^{in+\sigma} \pmod{p}. \]
The cyclotomic constant \((i, j)\) denotes the number of solutions of the congruence
\[ 1 + g^{un+i} \equiv g^{in+j} \pmod{p}, \]
where \(0 \leq i, j \leq n - 1\) and \(0 \leq u, v \leq k - 1\). The definition of \((i, j)\) is extended to \(Z \times Z\) by periodicity modulo \(n\).

The following theorem is the analogue of Theorem 3 in [7]. It gives a necessary and sufficient condition for qualified residue difference sets with zero to exist.

**Theorem 3.** If prime \(p = kn + 1\) \((k\ even)\) then a necessary and sufficient condition for the set \(R^\ast = \{0, r_1, r_2, \ldots, r_k\}\) \((n\ power\ residues\ and\ zero)\) to form a qualified residue difference set, with qualifier \(m\) of multiplicity \(\lambda\) belonging to residue class \(n - \sigma\) \((\sigma \neq 0,\ since\ m \notin R^\ast)\), is that
\[ 1 + (0, \sigma) = 1 + (\sigma, \sigma) = (s, \sigma) = (k + 2)/n = \lambda, \]
where \(1 \leq s \leq n - 1\) \((s \neq \sigma)\).

**Proof.** Suppose that \(m\) is a qualifier for the set \(R^\ast = \{r_0, r_1, r_2, \ldots, r_k\}\) of \(n\)th power residues and zero \((r_0 = 0)\) of the prime \(p = kn + 1\), where \(m\) belongs to residue class \(n - \sigma\) and is of multiplicity \(\lambda\). For each \(t = 1, 2, \ldots, (p - 1)\) the congruence modulo \(p\)
\[ r_i - mr_j \equiv t : 0 \leq i, j \leq k \quad (1) \]
has exactly \(\lambda\) solutions (it only has one when \(t = 0\) i.e. \(i = j = 0\)). For \(j \neq 0\) multiply through by \(\tilde{m}\tilde{r}_j\), where \(m\tilde{m} \equiv 1\) and \(\tilde{r}_j \equiv 1\), then rearrange to obtain
\[ 1 + \tilde{m}\tilde{r}_jt \equiv \tilde{m}\tilde{r}_jr_i. \quad (2) \]
Now \(m\) belongs to residue class \(n - \sigma\), so \(\tilde{m}\) belongs to residue class \(\sigma\). Also \(\tilde{m}\tilde{r}_jt\) belongs to residue class \(\sigma + s\), where \(s\) is the residue class of \(t\), and \(\tilde{m}\tilde{r}_jr_i\) belongs...
to residue class \( \sigma \). Now \( t \) takes on any value from 1 to \( p-1 \) and together (1) (with exactly one of \( i \) or \( j = 0 \)) and (2) \((i \neq 0, j \neq 0)\) always have \( \lambda \) solutions.

When \( j = 0 \), (1) has a solution when \( t \) belongs to residue class zero and when \( i = 0 \), (1) has a solution when \( t \) belongs to the residue class of \(-1\) plus \( n - \sigma \). Now \( g \) is a primitive root of \( p \) and so \(-1 \equiv g((p-1)/2) \). But \((p-1)/2 = kn/2 = in + \alpha \) (\( \alpha \) being the residue class of \(-1\)). So for even \( k \), \( \alpha = 0 \). Therefore when \( i = 0 \) and \( k \) is even (1) has a solution when \( t \) belongs to residue class \( n - \sigma \). Hence

\[
(\sigma + s, \sigma) = \lambda - \delta_s \quad \text{for} \quad s = 0, 1, 2, \ldots, n - 1,
\]

where \( \delta_s \) is the number of solutions given by (1). We have shown for even \( k \)

\[
\delta_\sigma = \begin{cases} 
1, & s = 0 \text{ or } n - \sigma, \\
0, & \text{otherwise}.
\end{cases}
\]

So by periodicity modulo \( n \) of the cyclotomic constants \((i, j)\) we have for \( 0 \leq s \leq n - 1 \)

\[
(s, \sigma) = \begin{cases} 
\lambda - 1, & s = 0 \text{ or } \sigma, \\
\lambda, & \text{otherwise}.
\end{cases}
\]

This proves the conditions of the theorem are necessary. We must now show that they are sufficient. Suppose that for a given \( \sigma \neq 0 \)

\[
1 + (0, \sigma) = 1 + (\sigma, \sigma) = (s, \sigma), \quad s = 1, 2, \ldots, n - 1 (s \neq \sigma)
\]

then

\[
n(s, \sigma) = 2 + \sum_{i=0}^{n-1} (i, \sigma). \quad (3)
\]

Now \( k \) is even and \( \sigma \neq 0 \). Therefore,

\[
\sum_{i=0}^{n-1} (i, \sigma) = \sum_{i=0}^{n-1} (\sigma, i) = k, \quad (4)
\]

where we have used the following two properties of cyclotomic numbers for the first and second equalities, respectively:

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

and

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

where

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

Now (3) and (4) combine to give \((s, \sigma) = (k + 2)/n\) and the converse is proved. The lemma completes the proof of the theorem. \( \square \)
4. Proof of Theorem 1

Let \( n = 4 \) and \( m \) be a qualifier for the set \( R^* \) of \( n \)th power residues and zero, where \( m \) belongs to residue class \( 4 - \sigma \). Now \( m \notin R^* \) and so \( \sigma \neq 0 \). Therefore \( \sigma = 1, 2 \) or 3.

We first show that \( \sigma = 2 \) by showing that it cannot equal 1 or 3.

Suppose \( \sigma = 1 \) then by Theorem 3 we have

\[
1 + (0, 1) = 1 + (1, 1) = (2, 1) = (3, 1) = (p + 7)/16
\]

(5)

since \( (k + 2)/4 = (p + 7)/16 \) when \( k = (p - 1)/4 \).

For \( n = 4 \) the cyclotomic constant \((1,0)\) was given by Gauss in terms of the quadratic partition \( p = A^2 + 4B^2, \ A \equiv 1 \pmod{4} \) and \( 16(1,0) = p - 2A - 3 \).

Now for even \( k \) \((1,0) = (0,1) \). Therefore using (5)

\[
16 + p - 2A - 3 = p + 7 \implies A = 3.
\]

But \( A \equiv 1 \pmod{4} \) and so \( \sigma \neq 1 \).

Suppose \( \sigma = 3 \) then by Theorem 3 we have

\[
1 + (0, 3) = 1 + (3, 3) = (1, 3) = (2, 3) = (3, 2) = (p + 7)/16.
\]

(6)

From [5, p. 400, (48)] for \( n = 4 \) and \( k \) even \((3,3) = (0,1)\), and so using (6) following the above argument \( \sigma \neq 3 \). Hence we can only have \( \sigma = 2 \). So suppose \( \sigma = 2 \) then by Theorem 3 we have

\[
1 + (0, 2) = 1 + (2, 2) = (1, 2) = (3, 2) = (p + 7)/16.
\]

(7)

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

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

(8)

Now (7) and (8) give \( p + 7 - 16 = p - 3 + 2A \) and so \( p = -3 \), therefore \( p = 9 + 4B^2 \).

From the lemma \( p \equiv 9 \pmod{16} \) therefore \( B \) must be even, and so \( p = 9 + 16x^2 \).

We now need to prove the converse, i.e., if \( p = 9 + 16x^2 \) then a qualifier belonging to residue class 2 for the biquadratic residues and zero exists. From Theorem 3 it is enough to show

\[
1 + (0, 2) = 1 + (2, 2) = (1, 2) = (3, 2) = (p + 7)/16.
\]

(9)

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

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

(10)

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

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

(11)

where \( p = A^2 + 4B^2, \ A \equiv 1 \pmod{4} \). Now \( p = 9 + 16x^2 \) and so \( A = -3 \) since the representation of \( p \) as the sum of two squares is unique up to order and sign. Therefore (10) and (11) give

\[
(1, 2) = (3, 2) = (p + 7)/16.
\]

(12)
Also using (8) we have $16(0,2) = p - 9 = (p + 7) - 16$ and so

$$1 + (0,2) = (p + 7)/16.$$  \hspace{1cm} (13)

Now (10), (12) and (13) combine to give (9) and the theorem is proved. $\Box$

Theorem 2 can be proved by a similar method, but since there are many more case by case checks for $n = 6$ we just outline the proof. We first show that 2 is a cubic residue of $p$ by proving that $\sigma$ cannot equal any of 1, 2, 3, 4 or 5 if 2 belongs to residue class 1 or 2. We then show that $\sigma = 3$ by proving that $\sigma$ cannot equal any of 1, 2, 4 or 5 when 2 is a cubic residue of $p$. To obtain the form of $p$ we use the formulae from [5, pp. 408–409] for the cyclotomic constants in terms of the quadratic partition $p = A^2 + 3B^2$, $A \equiv 1 \pmod{3}$.

References