ON RESIDUE DIFFERENCE SETS

EMMA LEHMER

1. Introduction. In recent years the subject of difference sets has attracted a considerable amount of attention in connection with problems in finite geometries [**4**]. Difference sets arising from higher power residues were first discussed by Chowla [**1**], who proved that biquadratic residues modulo p form a difference set if $(p-1)/4$ is an odd square. In this paper we shall prove a similar result for octic residues and develop some necessary conditions which will eliminate all odd power residue difference sets and many others. We also prove that a perfect residue difference set (that is, one in which every difference appears exactly once) contains all the powers of 2 modulo p.

DEFINITION. *An nth power residue difference set of multiplicity* λ *with respect to a prime* p is the set

$$r_1, r_2, \ldots, r_k$$

of nth power residues of a prime $p = kn + 1$, which is such that if we form all the $k(k-1)$ non-zero differences

$$r_a - r_b \pmod{p} \qquad (a \neq b),$$

we will obtain every positive integer $\leqslant p - 1$ exactly λ times. Hence

$$\lambda = (k-1)/n \quad \text{and} \quad p = \lambda n^2 + n + 1.$$

If $\lambda = 1$, the set will be called a perfect residue difference set. In this case $k = n + 1$ and $p = n^2 + n + 1$.

In order to study these sets efficiently we will need to use some properties of the cyclotomic numbers (i, j) introduced by Gauss and developed by Dickson [**2**], together with an additional lemma about their parity, which is a generalization of a lemma given by the author in an earlier paper [**5**].

2. Cyclotomic numbers. Let $p = nk + 1$ be a prime and let g be a primitive root of p. We shall say that a number N belongs to the residue class i with respect to g if $N \equiv g^{mn+i} \pmod{p}$. The cyclotomic constant (i, j) denotes the number of members of the residue class i which are followed by a member of the residue class j, or in other words, the number of solutions of the congruence

$$g^{\nu n+i} + 1 \equiv g^{\mu n+j} \qquad \pmod{p},$$

where i and j are $\leqslant n-1$, while ν and μ are $\leqslant k-1$.

Received August 29, 1952.

https://doi.org/10.4153/CJM-1953-047-3 Published online by Cambridge University Press

We shall borrow the following properties of cyclotomic numbers (all of which can be very readily derived) from Dickson [2, p. 394, (14), (15), (17)]:

2.1 $$(i, j) = (j, i), \qquad (n - i, j - i) = (i, j), \qquad k \text{ even}$$

2.2 $$(i, j) = (j + \tfrac{1}{2}n, i + \tfrac{1}{2}n), \qquad (n - i, j - i) = (i, j), \qquad k \text{ odd}$$

2.3 $$\sum_{j=0}^{n-1} (i, j) = k - \epsilon_i, \qquad (i = 0, 1, \ldots, n - 1),$$

where

$$\epsilon_i = \begin{cases} 1 \text{ if } k \text{ is even and } i = 0, \text{ or if } k \text{ is odd and } i = \tfrac{1}{2}n. \\ 0 \text{ otherwise.} \end{cases}$$

LEMMA 1. *The cyclotomic numbers* $(0, j)$ *are odd or even according as* 2 *belongs to the residue class* j *or not.*

Proof. For every pair r, $r + 1$ such that r is a residue and hence belongs to residue class zero, while $r + 1$ belongs to the residue class j, there corresponds a pair $\bar{r}$, $\bar{r} + 1$, where $r\bar{r} \equiv 1 \pmod{p}$, which is also such that $\bar{r}$ belongs to class zero while $\bar{r} + 1 \equiv \bar{r}\,(r + 1)$ belongs to class j. Therefore the contribution to the cyclotomic number $(0, j)$ is even unless $r \equiv \bar{r}$. This implies that r is either 1 or $p - 1$. The case $r = p - 1$ does not produce a solution since $r + 1 \equiv 0$ is not admissible, while the case $r = 1$, $r + 1 = 2$ gives an unpaired solution if and only if 2 belongs to class j. Hence the lemma.

3. Connection between residue difference sets and cyclotomic constants.

THEOREM 1. *A necessary and sufficient condition that the class of nth power residues form a difference set is that the cyclotomic numbers*

$$(i, 0) = (k - 1)/n \qquad (i = 0, 1, \ldots, n - 1),$$

where $(k - 1)/n = \lambda$ *is the multiplicity of the difference set.*

Proof. First suppose that the residues form a difference set of multiplicity λ so that for every positive integer d there are λ solutions of the congruence $r_a - r_b \equiv d \pmod{p}$. Multiplying this congruence by $\bar{r}_b$, we have

$$d\,\bar{r}_b + 1 \equiv r_a \bar{r}_b \qquad \pmod{p}.$$

We note that the right-hand side belongs to the residue class zero, and that $d\bar{r}_b$ belongs to the same class as d. Denoting this class by i we have $(i, 0) = \lambda$. But since d was arbitrary this must hold for all i.

Conversely, if all the $(i, 0)$ are equal, then

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

But it follows readily from 2.3 with the help of either 2.1 or 2.2 that in all cases

https://doi.org/10.4153/CJM-1953-047-3 Published online by Cambridge University Press

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

hence the common value of all the $(i, 0)$ is in fact $(k - 1)/n$. Moreover, the correspondence set up in the first part of the proof is obviously one to one, hence the residues form a difference set of multiplicity $\lambda = (k - 1)/n$ if all the $(i, 0)$ are equal.

THEOREM II. *There exists no residue difference set for n odd; or for n even and k even.*

Proof. If n is odd, then k must be even, but for even k we have by 2.1 the equality $(0, i) = (i, 0)$. Hence Theorem I states in this case that the cyclotomic constants $(0, i)$ are all equal. But by Lemma I one of these quantities is odd while the others are even. Hence we have arrived at a contradiction and the theorem follows.

THEOREM III. *If n is even and $k = (p - 1)/n$ is odd, then a necessary and sufficient condition for the set of nth power residues modulo p to form a difference set is that*

$$(i, 0) = (k - 1)/n \qquad (i = 0, 1, \ldots, \tfrac{1}{2}n - 1).$$

Proof. It follows readily from 2.2 that

$$(i + \tfrac{1}{2}n, 0) = (i, 0),$$

hence the theorem follows from Theorem I.

4. Multipliers. The notion of a multiplier was introduced by Hall [4] and is as follows: A number t is called a multiplier of a set $r_1, r_2, \ldots, r_k$ if the set $tr_1, tr_2, \ldots, tr_k$ is congruent to the set $r_1 + s, r_2 + s, \ldots, r_k + s$ in some order for some number s. The following theorem is true of multipliers of residue difference sets.

THEOREM IV. *The set of multipliers of a residue difference set is the set itself.*

Proof. That every element of the set is a multiplier is obvious because it leaves the set unaltered and $s = 0$. Suppose now that we have a multiplier t which is not in the residue set and let t belong to the residue class $\tau \neq 0$. Then all the numbers $tr_1, tr_2, \ldots, tr_k$ will also belong to the residue class τ. Hence in this case $s \neq 0$. Let s belong to the residue class σ. The congruence $r_a + s \equiv tr_b \pmod{p}$ implies, by multiplying by $\bar{s}$, that $r_a\bar{s} + 1 \equiv t\bar{s}r_b \pmod{p}$. But the number of solutions of the last congruence is $(n - \sigma, \tau - \sigma) = k$, but by 2.1 or 2.2 this implies $(\sigma, \tau) = k$. But by 2.3

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

hence all $(\sigma, j) = 0$ for $j \neq \tau$. But, for a difference set $(\sigma, 0) = (k - 1)/n \neq 0$. Hence we have arrived at a contradiction and the theorem follows.

https://doi.org/10.4153/CJM-1953-047-3 Published online by Cambridge University Press

5. Perfect residue difference sets. Hall [4] has proved that for $\lambda = 1$ every divisor of n is a multiplier of any difference set modulo $n^2 + n + 1$. He also proved that 2 and 3, as well as 18 other pairs of numbers, cannot both be multipliers. We now apply these results to residue difference sets.

THEOREM V. *A perfect residue difference set contains all the powers of* 2 *modulo* p.

Proof. Since, by Theorem II, n must be even, 2 divides n and hence is a multiplier of the difference set by Hall's theorem. But every multiplier is in the set by Theorem IV, hence 2 is an nth power residue and hence all powers of 2 are nth power residues and are in the set.

COROLLARY. *If the exponent of* 2 (mod p) *is exactly* $n + 1$, *then the set consists of powers of* 2 *exclusively.*

THEOREM VI. *The only perfect residue difference sets with* $p < 2561600$ *are for* $n = 2$, $p = 7$ *and for* $n = 8$, $p = 73$.

Proof. Evans and Mann [3] have recently proved that there exists no perfect difference set for $n < 1600$, unless n is a prime or a power of a prime. In our case since $n^2 + n + 1$ must be a prime p, n must be of the form $2^{2\nu+1}$. The only such $n < 1600$ which lead to prime values of p are $n = 2$, 8, and 512. The first two lead to well-known sets of quadratic residues 1, 2, 4 (mod 7), and octic residues 1, 2, 4, 8, 16, 32, 37, 55, and 64 (mod 73), respectively.

The remaining case of $p = 262657$, $n = 512$, satisfies, as far as the writer has been able to ascertain, all known necessary conditions for a difference set. It has no multipliers other than powers of 2 less than 783, and can be generated by 783^α, $\alpha = 0, 1, \ldots, 512$. An inspection of the set shows however, that

$$3 \equiv 783^{133} - 783^{513} \equiv 783^{149} - 783^{483} \qquad (\text{mod } 262657)$$

$$\equiv 4 - 1 \equiv 89788 - 89785.$$

Hence this is not a perfect difference set after all.

6. Special values of *n*. For $n = 2$, Theorem III gives no further restriction on p beyond $\lambda = (0, 0) = (p - 3)/4$, which is satisfied. Hence there exists a difference set of quadratic residues for all p $\equiv 3$ (mod 4). This is a well-known result. By Theorem II we need to consider only odd values of k.

For $n = 4$, the cyclotomic constants were given by Gauss in terms of the quadratic partition $p = x^2 + 4y^2$, $x \equiv 1$ (mod 4).

$$16(0, 0) = p + 2x - 7, \qquad 16(1, 0) = p - 2x - 3.$$

The condition $(0, 0) = (1, 0)$ implies $x = 1$ or $p = 1 + 4y^2$. Hence $k = (p - 1)/4 = y^2$. Since k is odd, k must be an odd square, which is Chowla's theorem.

For $n = 6$, the cyclotomic constants can be easily derived from Dickson's results in terms of the quadratic partition $p = A^2 + 3B^2$, $A \equiv 1$ (mod 3).

https://doi.org/10.4153/CJM-1953-047-3 Published online by Cambridge University Press

Case 1. 2 is a cubic residue. In this case the condition

$$36(0,0) = p - 11 - 8A = 6(k-1)$$

leads to $A = -\frac{1}{2}$, which is impossible, since A is an integer.

Case 2. 2 is a cubic non-residue. In this case

$$36(0,0) = p - 11 - 2A = 6(k-1)$$

leads to $A = -2$, while

$$36(1,0) = p - 5 + 4A + 6B, \quad 36(2,0) = p - 5 - 2A - 6B$$

or

$$36(1,0) = p - 5 - 2A + 6B, \quad 36(2,0) = p - 5 + 4A - 6B$$

(according as 2 belongs to class one or two), so that the condition $(1,0) = (2,0)$ implies $2B = -A = 2$, or $B = 1$ and $p = 7$. This is a trivial case since the only sextic residue modulo 7 is $r = 1$, so that in this case $\lambda = 0$. In other words, there exists no difference set of sextic residues.

For $n = 8$, a little more work is required to derive the needed cyclotomic numbers from the groundwork laid by Dickson. These numbers are given in terms of the quadratic partitions.

$$p = a^2 + 2b^2 = x^2 + 4y^2 = 8k + 1, \; a \equiv x \equiv 1 \pmod 4)$$

Case I. 2 is a quartic residue, then

$$64(0,0) = p - 15 - 2x, \quad 64(2,0) = p - 2x - 8a - 7$$

$$64(1,0) = 64(3,0) = p - 7 + 2x + 4a.$$

The condition

$$(0,0) = (1,0) = (2,0) = (3,0) = (p-9)/64$$

implies $a = 1$, $x = -3$. Hence

$$p = 1 + 2b^2 = 9 + 4y^2, \text{ or } b^2 - 2y^2 = 4.$$

Letting $b = 2t$, $y = 4u$, we have the condition

$$t^2 - 8u^2 = 1,$$

where $k = (p-1)/8 = t^2$ and $\lambda = (p-9)/64 = u^2$. The first non-trivial solution of this Pell equation is $t = 3$, $u = 1$, giving $p = 73$. The even-ordered solutions of this Pell equation lead to values of p which are multiples of 3. The odd-ordered solutions give odd values of u and lead to values of p which satisfy the recurring series

$$p_m = 1154p_{m-1} - p_{m-2} - 5760, \quad p_0 = 73, \quad p_1 = 73.$$

https://doi.org/10.4153/CJM-1953-047-3 Published online by Cambridge University Press

This gives

$$p_2 = 78409 = 89 \cdot 881$$

$$p_3 = 90478153 = 4993 \cdot 18121$$

$$p_4 = 104411704393 = \text{prime}$$

$$p_5 = 120491016385609 = 1721 \cdot 70012211729.$$

These factorizations were made on the SWAC. The prime p_4 is the modulus for a difference set with $k = 114243^2$ elements of multiplicity $\lambda = 40391^2$.

Case II. 2 is a quartic non-residue. In this case

$$64(0,0) = p - 15 - 10x - 8a, \quad 64(2,0) = p + 6x - 7$$

and the condition $(0,0) = (2,0) = (p-9)/64$ leads to $x = -\frac{1}{3}$, but this is impossible. We can therefore summarize our results on octic residues in the following theorem.

THEOREM VII. *The set of octic residues modulo p forms a difference set if and only if the number of terms* $k = (p-1)/8$ *and the multiplicity* $\lambda = (p-9)/64$ *are both odd squares.*

COROLLARY. *An octic residue difference set contains all powers of* 2 *modulo p.*

It is known that the condition for octic residuacity of 2 is that $\frac{1}{4}y$ be odd[1] for $p \equiv 9 \pmod{16}$. But in our case $u = \frac{1}{4}y$ is odd. Hence 2, and therefore all its powers, are octic residues.

Finally, we discuss briefly the impossibility of residue sets for $n = 10$, when 2 is a quintic residue. The cyclotomic numbers for $n = 10$ are given in terms of the solutions of

$$16p = x^2 + 50u^2 + 50v^2 + 125w^2, \qquad xw = v^2 - 4uv - u^2.$$

If 2 is a quintic residue, Dickson gives for k odd

$$100(0,0) = p - 19 + 8x$$

and the condition $(0,0) = (p-11)/100$ implies $x = 1$; but it has been proved by the author [**5**], that if 2 is a quintic residue, x must be even. Hence we have arrived at a contradiction and there is no difference set in this case.

The cyclotomic numbers have not been worked out in sufficient detail to complete the case in which 2 is a quintic non-residue. The same holds true for larger values of n such as 12 and 16, although a certain amount of work has been done in these cases.

[1] This can be made to follow readily from Lemma I and the expression for (0, 0) in the octic case. In fact for $p \equiv 9 \pmod{16}$ and (0, 0) odd we have $64\ (0,0) = p - 15 - 2x \equiv 64 \pmod{128}$. Hence $x \equiv 8v + 29 \pmod{64}$, which implies $y \equiv 4 \pmod 8$. Similarly if 2 is an octic non-residue (0, 0) is even and $y \equiv 0 \pmod 8$.

7. Modified residue difference sets. Hall points out that Theorem II holds if zero is counted as a residue and that we can obtain further residue sets for quartic residues. We will show that this can also be done for octic residue sets, but that no other new cases arise.

If zero is counted as a residue, then the multiplicity λ is given by $\lambda = (k + 1)/n$ and we have an analogue of Theorem III, namely

THEOREM III′. *If n is even and $k = (p - 1)/n$ is odd, then a necessary and sufficient condition for the set of nth power residues and zero to be a difference set is that*

$$1 + (0, 0) = (i, 0) = (k + 1)/n, \qquad i = 1, 2, \ldots, \tfrac{1}{2}n - 1.$$

We now discuss the cases $n = 4$ and $n = 8$. For $n = 4$ the conditions of Theorem III′ give

$$p + 2x + 9 = p - 2x - 3 = p + 3.$$

This implies $x = -3$ so that $p = 9 + 4y^2$. Since $k = (p - 1)/4$ is odd, $y = k - 2$ must also be odd and we have an analogue of Chowla's theorem:

The quartic residues and zero form a difference set modulo p if and only if $k - 2 = (p - 9)/4$ is an odd square.

For $n = 8$, if 2 is a quartic residue, we have by Theorem III′

$$p + 49 - 2x = p - 2x - 8a - 7 = p + 7.$$

This implies $x = 21$, $a = -7$. Hence

$$p = 49 + 2b^2 = 441 + 4y^2 \quad \text{or} \quad b^2 - 2y^2 = 196.$$

Letting, as before, $b = 2t$, $y = 4u$, we have

$$t^2 - 8u^2 = 49.$$

As before, this leads to a sequence of p's which can be defined by the recurrence

$$p_m = 1154p_{m-1} - p_{m-2} - 282240,$$

where $p_0 = 697$, $p_1 = 26041$, and m can take on positive and negative values. The smallest prime value in this sequence is $p_1 = 26041$, and there are no other primes less than $p_{-3} = 34352398777$. The prime $p = 26041$ gives a difference set with $k = 3255$, $\lambda = 407$. This set contains 3256 elements including 0 and all 465 powers of 4 modulo 26041. It can be generated by powers of 7.

If 2 is a quartic non-residue we have

$$64(2,0) = p + 6x - 7 = p + 7,$$

which is impossible. Hence we can state an analogue of Theorem VII, namely

THEOREM VII′. *The set of octic residues and zero forms a residue set modulo p if and only if $k - 6 = (p - 9)/8$ is an odd square, while $\lambda - 7 = (p - 441)/64$ is an even square.*

That $(p - 441)/64 = u^2$ is even follows from the fact that this time the odd values of u gave multiples of three for p, and are therefore eliminated. Since $\lambda - 7$ is even, λ is again odd. Since $u = \frac{1}{4}y$ is even, 2 is not an octic residue (see footnote 1). Hence we can state:

COROLLARY. *An octic residue difference set which includes zero contains all powers of 4 modulo p.*

It can be easily seen, as before, that the cases $n = 2$, 6, and 10 lead to contradictions, so that we have been able to discover difference sets for only $n = 4$ and 8. It would be of interest to find out if the next possible case is $n = 12$ or $n = 16$.

In order to get a perfect residue difference set, when zero is counted as a residue, we must have

$$p = n^2 - n + 1 = (n - 1)^2 + (n - 1) + 1.$$

For quartic residues $n = 4$, $p = 13$, the numbers 0, 1, 3, 9 form such a set, but there is none for octic residues since $7^2 + 7 + 1 = 57$ is not a prime.

REFERENCES

1. S. Chowla, *A property of biquadratic residues*, Proc. Nat. Acad. Sci. India, Sec. A, *14* (1944), 45–46.
2. L. E. Dickson, *Cyclotomy, higher congruences and Waring's problem*, Amer. J. Math., *57* (1935), 391–424.
3. T. A. Evans and H. B. Mann, *On simple difference sets*, Sankhyā, *2* (1951), 357–364.
4. Marshall Hall, Jr., *Cyclic projective planes*, Duke Math. J., *14* (1947), 1079–1090.
5. Emma Lehmer, *The quintic character of* 2 *and* 3, Duke Math. J., *18* (1951), 11–18.

Pacific Palisades, California

https://doi.org/10.4153/CJM-1953-047-3 Published online by Cambridge University Press