Computer Investigation of Difference Sets

By Harry S. Hayashi

1. Introduction. By a difference set of order k and multiplicity λ is meant a set of k distinct residues $r_1, r_2, \cdots, r_k \pmod v$ such that the congruence $r_i - r_j \equiv d \pmod v$ has exactly λ solutions for each $d \not\equiv 0 \pmod v$. Difference sets arise in a natural way in many combinatorial and statistical problems and have been extensively studied. There is given in [2] a survey of all difference sets wth parameters v, k, λ for which k is in the range $3 \leqq k \leqq 50$. In making that survey, Hall discovered a family of difference sets described by the following theorem.

THEOREM. *A set of complete 6th power residue classes (with or without the residue zero) forming a difference set modulo a prime* $p = 6f + 1$ *consists of either* (1) *the quadratic residues when* $p \equiv 3 \pmod 4$ *or* (2) *the 6th power residue classes* 0, 3 *and* c *where* $\operatorname{ind}_g 3 = c$, g *is the arbitrarily chosen primitive root, and* p *is of the form* $p = 4x^2 + 27$.

The proof of this theorem consisted of an exhaustive search on the SWAC computer, utilizing a method based on Dickson's [1] formulas for the cyclotomic numbers of order 6.

This paper discusses a similar difference set search on the Control Data Corporation 1604A computer for primes of the form $p = 10f + 1$, utilizing Whiteman's [5] formulas for the cyclotomic numbers of order 10. The result of this effort is summarized by:

THEOREM. *A set of complete 10th power residue classes (with or without the residue zero) forming a difference set modulo a prime* $p = 10f + 1$ *consists of either* (1) *the quadratic residues when* $p \equiv 3 \pmod 4$ *or* (2) *the 10th power residue classes* 0 *and* 1 *where* $p = 31$ *and* $g = 11$.

2. Cyclotomy. Let e be a fixed positive integer. Consider a prime p of the form $p = ef + 1$ and let g be a primitive root of p. For each pair of integers h, k let (h, k) be the number of ordered pairs s, t of integers in the range $0 \leqq s \leqq f - 1$, $0 \leqq t \leqq f - 1$ such that:

$$g^{es+k} - g^{et+h} \equiv 1 \pmod p. \tag{2.1}$$

Then the (h, k) are called cyclotomic numbers of order e. From (2.1) we have the property of periodicity, modulo e:

$$(h, k) = (h', k') \tag{2.2}$$

if $h = h' \pmod e$, $k = k' \pmod e$.

If g_1 is another primitive root of p, then for some integer u prime to ef, $g^u \equiv g_1 \pmod p$. Substituting in (2.1) we see that

$$(uh, uk)_g = (h, k)_{g_1}. \tag{2.3}$$

If v is any integer prime to e, there exists at least one integer u prime to ef such that $u \equiv v \pmod e$. Hence by (2.2) we have $(uh, uk) = (vh, vk)$. From this result

Received July 10, 1964.

and (2.3) we conclude that there are $\phi(e)$ sets of cyclotomic numbers of order e and they can be generated by $g^{v_1}, \cdots, g^{v_{\phi(e)}}$ where $v_1, \cdots, v_{\phi(e)}$ are prime to ef and form a reduced residue system modulo e.

For further reference we state the following properties of cyclotomic numbers, the proofs of which may be found in [1].

$$(h, k) = (e - h, k - h), \tag{2.4}$$

$$(h, k) = \begin{cases} (k, h) & \text{if } f \text{ even}, \\ \left(k + \frac{e}{2}, h + \frac{e}{2}\right) & \text{if } f \text{ odd}. \end{cases} \tag{2.5}$$

It is known that if $p \equiv 1 \pmod 5$, then there are exactly four integral solutions of the pair of diophantine equations:

$$\begin{aligned} xw &= v^2 - 4uv - u^2, \\ 16p &= x^2 + 50u^2 + 50v^2 + 125w^2, \end{aligned} \tag{2.6}$$

with x uniquely determined by the condition $x \equiv 1 \pmod 5$. The four solutions are (x, u, v, w), $(x, -u, -v, w)$, $(x, v, -u, -w)$, and $(x, -v, u, -w)$, each solution corresponding to one of the $\phi(10) = 4$ sets of cyclotomic numbers of order 10. For primes of the form $p = 10f + 1$, Whiteman derived explicit formulas for their cyclotomic numbers in terms of x, u, v, w, and p. There are 10 sets of formulas depending on the parity of f and the quintic residue character of 2 modulo p. The five sets corresponding to f odd are listed in Tables A0 through A4. Due to the relations (2.2), (2.4) and (2.5) the 100 cyclotomic numbers have at most 22 different values and these relations are summarized in Table B. The letter m in Am indicates the index of 2 (mod 5).

TABLE A0

$$\begin{aligned}
400(0, 0) &= 4P + 32X - 76 \\
400(0, 1) &= 4P + 2X + 100U + 100V - 50W + 4 \\
400(0, 2) &= 4P + 2X - 100U + 100V - 150W + 4 \\
400(0, 3) &= 4P + 2X - 100U + 100V + 50W + 4 \\
400(0, 4) &= 4P + 2X + 100U + 100V + 150W + 4 \\
400(0, 5) &= 4P - 48X + 4 \\
400(0, 6) &= 4P + 2X - 100U - 100V + 150W + 4 \\
400(0, 7) &= 4P + 2X + 100U - 100V + 50W + 4 \\
400(0, 8) &= 4P + 2X + 100U - 100V - 150W + 4 \\
400(0, 9) &= 4P + 2X - 100U - 100V - 50W + 4 \\
400(1, 0) &= 4P - 8X + 100V - 36 \\
400(1, 1) &= 4P - 8X - 100V - 36 \\
400(1, 2) &= 4P + 2X + 50W + 4 \\
400(1, 3) &= 4P + 2X - 50W + 4 \\
400(1, 4) &= 4P + 2X - 150W + 4 \\
400(1, 8) &= 4P + 2X - 50W + 4 \\
400(1, 9) &= 4P + 2X + 50W + 4 \\
400(2, 0) &= 4P - 8X + 100U - 36 \\
400(2, 1) &= 4P + 2X - 150W + 4 \\
400(2, 2) &= 4P - 8X - 100U - 36 \\
400(2, 3) &= 4P + 2X + 150W + 4 \\
400(3, 1) &= 4P + 2X + 150W + 4
\end{aligned}$$

TABLE A1

$$
\begin{aligned}
400(0,0) &= 4P + 7X - 50U + 25W - 76\\
400(0,1) &= 4P + 2X + 100V + 250W + 4\\
400(0,2) &= 4P - 23X + 50U - 25W + 4\\
400(0,3) &= 4P + 2X + 50U - 150V + 100W + 4\\
400(0,4) &= 4P + 2X - 50U - 50V + 4\\
400(0,5) &= 4P + 27X + 150U - 75W + 4\\
400(0,6) &= 4P + 2X + 100V - 150W + 4\\
400(0,7) &= 4P - 23X + 50U - 25W + 4\\
400(0,8) &= 4P + 2X - 150U + 50V - 100W + 4\\
400(0,9) &= 4P + 2X - 50U - 50V + 4\\
400(1,0) &= 4P - 8X - 36\\
400(1,1) &= 4P - 8X + 50U - 50V + 50W - 36\\
400(1,2) &= 4P + 2X - 50U - 50V + 4\\
400(1,3) &= 4P + 2X + 100U - 50W + 4\\
400(1,4) &= 4P + 2X - 50U - 50V + 4\\
400(1,8) &= 4P + 2X + 100V + 250W + 4\\
400(1,9) &= 4P + 2X + 50U + 50V - 100W + 4\\
400(2,0) &= 4P + 17X + 50U - 25W - 36\\
400(2,1) &= 4P + 2X + 50U + 50V - 100W + 4\\
400(2,2) &= 4P - 8X - 50U + 50V - 50W - 36\\
400(2,3) &= 4P + 2X - 100U - 50W + 4\\
400(3,1) &= 4P + 2X - 100V + 50W + 4
\end{aligned}
$$

TABLE A2

$$
\begin{aligned}
400(0,0) &= 4P + 7X - 50V - 25W - 76\\
400(0,1) &= 4P + 2X + 150U + 50V - 100W + 4\\
400(0,2) &= 4P + 2X - 100U + 150W + 4\\
400(0,3) &= 4P + 2X + 50U - 50V + 4\\
400(0,4) &= 4P - 23X + 50V + 25W + 4\\
400(0,5) &= 4P + 27X + 150V + 75W + 4\\
400(0,6) &= 4P + 2X - 50U - 150V + 100W + 4\\
400(0,7) &= 4P + 2X - 100U - 250W + 4\\
400(0,8) &= 4P + 2X + 50U - 50V + 4\\
400(0,9) &= 4P - 23X + 50V + 25W + 4\\
400(1,0) &= 4P - 8X - 50U - 50V + 50W - 36\\
400(1,1) &= 4P + 17X + 50V + 25W - 36\\
400(1,2) &= 4P + 2X - 100U - 250W + 4\\
400(1,3) &= 4P + 2X + 50U - 50V + 4\\
400(1,4) &= 4P + 2X + 100U - 50W + 4\\
400(1,8) &= 4P + 2X - 50U + 50V + 100W + 4\\
400(1,9) &= 4P + 2X + 100V + 50W + 4\\
400(2,0) &= 4P - 8X - 36\\
400(2,1) &= 4P + 2X - 100V + 50W + 4\\
400(2,2) &= 4P - 8X + 50U + 50V - 50W - 36\\
400(2,3) &= 4P + 2X - 50U + 50V + 100W + 4\\
400(3,1) &= 4P + 2X + 50U - 50V + 4
\end{aligned}
$$

3. Difference Sets. Let $D = (d_1, d_2, \cdots, d_k)$ and $D' = (d_1', \cdots, d_k')$ be difference sets on the same parameters v, k, λ. Let t be an integer such that t is prime to v and let s be an arbitrary integer. Then it is easy to see that $E = (td_1, \cdots, td_k)$ and $E' = (d_1' + s, \cdots, d_k' + s)$ are also difference sets. Suppose that t and s can

TABLE A3

$$
\begin{aligned}
400(0,0) &= 4P + 7X + 50V - 25W - 76\\
400(0,1) &= 4P - 23X - 50V + 25W + 4\\
400(0,2) &= 4P + 2X - 50U + 50V + 4\\
400(0,3) &= 4P + 2X + 100U - 250W + 4\\
400(0,4) &= 4P + 2X + 50U + 150V + 100W + 4\\
400(0,5) &= 4P + 27X - 150V + 75W + 4\\
400(0,6) &= 4P - 23X - 50V + 25W + 4\\
400(0,7) &= 4P + 2X - 50U + 50V + 4\\
400(0,8) &= 4P + 2X + 100U + 150W + 4\\
400(0,9) &= 4P + 2X - 150U - 50V - 100W + 4\\
400(1,0) &= 4P + 17X - 50V + 25W - 36\\
400(1,1) &= 4P - 8X + 50U + 50V + 50W - 36\\
400(1,2) &= 4P + 2X - 100V + 50W + 4\\
400(1,3) &= 4P + 2X + 50U - 50V + 100W + 4\\
400(1,4) &= 4P + 2X - 100U - 50W + 4\\
400(1,8) &= 4P + 2X - 50U + 50V + 4\\
400(1,9) &= 4P + 2X + 100U - 250W + 4\\
400(2,0) &= 4P - 8X - 50U - 50V - 50W - 36\\
400(2,1) &= 4P + 2X + 100V + 50W + 4\\
400(2,2) &= 4P - 8X - 36\\
400(2,3) &= 4P + 2X + 50U - 50V + 100W + 4\\
400(3,1) &= 4P + 2X - 50U + 50V + 4
\end{aligned}
$$

TABLE A4

$$
\begin{aligned}
400(0,0) &= 4P + 7X + 50U + 25W - 76\\
400(0,1) &= 4P + 2X + 50U + 50V + 4\\
400(0,2) &= 4P + 2X + 150U - 50V - 100W + 4\\
400(0,3) &= 4P - 23X - 50U - 25W + 4\\
400(0,4) &= 4P + 2X - 100V - 150W + 4\\
400(0,5) &= 4P + 27X - 150U - 75W + 4\\
400(0,6) &= 4P + 2X + 50U + 50V + 4\\
400(0,7) &= 4P + 2X - 50U + 150V + 100W + 4\\
400(0,8) &= 4P - 23X - 50U - 25W + 4\\
400(0,9) &= 4P + 2X - 100V + 250W + 4\\
400(1,0) &= 4P - 8X - 50U + 50V + 50W - 36\\
400(1,1) &= 4P - 8X - 36\\
400(1,2) &= 4P + 2X - 50U - 50V - 100W + 4\\
400(1,3) &= 4P + 2X - 100V + 250W + 4\\
400(1,4) &= 4P + 2X + 50U + 50V + 4\\
400(1,8) &= 4P + 2X - 100U - 50W + 4\\
400(1,9) &= 4P + 2X + 50U + 50V + 4\\
400(2,0) &= 4P - 8X + 50U - 50V - 50W - 36\\
400(2,1) &= 4P + 2X - 50U - 50V - 100W + 4\\
400(2,2) &= 4P + 17X - 50U - 25W - 36\\
400(2,3) &= 4P + 2X + 100U - 50W + 4\\
400(3,1) &= 4P + 2X + 100V + 50W + 4
\end{aligned}
$$

be determined such that $E = E'$. Then in classifying difference sets it is natural to define D and D' as isomorphic.

It can be shown that the complement of a difference set is also a difference set. In particular, the complement of a difference set composed of complete eth power residue classes is a difference set composed of complete eth power residue classes plus the residue zero.

TABLE B

	0	1	2	3	4	5	6	7	8	9
0	00	01	02	03	04	05	06	07	08	09
1	10	11	12	13	14	06	04	14	18	19
2	20	21	22	23	18	07	14	03	13	23
3	22	31	31	20	19	08	18	13	02	12
4	11	21	31	21	10	09	19	23	12	01
5	00	10	20	22	11	00	10	20	22	11
6	10	00	19	23	12	01	11	21	31	21
7	20	19	08	18	13	02	12	22	31	31
8	22	23	18	07	14	03	13	23	20	21
9	11	12	13	14	06	04	14	18	19	10

In this table the entry in row h and column k is equal to (h, k).

Consider now a difference set with v a prime of the form $p = 10f + 1$ and its k elements composed of complete 10th power residue classes modulo $10f$, with or without the residue zero. If f is even, then -1 is a 10th power residue. This leads to a contradiction of the fact that every difference occurs equally often. Therefore, we conclude that f is odd.

We see from (2.1) that (i, j) is the number of solutions of $y - x \equiv 1 \pmod{p}$ with y in residue class i and x in residue class j. Multiplying by d in class k we have $y_1 - x_1 \equiv d \pmod{p}$ with y_1 in class $j + k$ and x_1 in class $i + k$. Thus $y - x \equiv d \pmod{p}$ has, for a fixed d in class k, $(i - k, j - k)$ solutions with y in class j and x in class i.

If our difference set is composed of the classes $i_1, \cdots, i_n$, then the number of occurrences of the difference d in class u is $N_u = \sum_{r=1}^{n} \sum_{s=1}^{n} (i_r - u, i_s - u)$ with $N_0 = N_1 = \cdots = N_9$. By (2.3) we have that N_u is identical to N_{u+5}. Therefore, we have at most 5 distinct expressions for the N_u.

By substituting the expressions from Table A into the equations $N_0 - N_1 = 0$, $N_2 - N_1 = 0$, $N_3 - N_2 = 0$ and $N_4 - N_3 = 0$, we arrive at a system of four linear equations in the unknowns x, u, v and w (p cancels out each time). The solution of this system will correspond to the p and g that define the difference set.

Therefore choosing ind 2 and a set of residue classes $i_1, \cdots, i_n$ leads to a system of linear equations in x, u, v, w whose solution, if it satisfies the added constraints $xw = v^2 - 4uw - u^2$ and $x \equiv 1 \pmod{5}$, will correspond to a difference set.

With zero included, N_u is increased by 1 if the difference set contains the class u_1 and $u_1 \equiv u \pmod{5}$. Otherwise, the N_u is the same as before. Therefore by increasing N_u when appropriate, then forming the system of linear equations in x, u, v, w and solving as before, we can find difference sets composed of complete residue classes plus the residue zero.

4. Computational Procedure. By considering all combinations of residue classes up to and including the combinations of five classes twice, once with and once without the residue zero, we essentially exhaust all cases. The one-residue classes are isomorphic to residue difference sets and Whiteman [5] proved that none exist. We therefore start with combinations of two classes.

Most of the isomorphic cases were eliminated before the machine computation. The discussion that follows concerning the first two types of isomorphism applies with or without the zero. To illustrate how the isomorphs were disposed of, the case of three classes will be briefly discussed.

The cases can be represented by i_1, i_2, i_3 where $0 \leqq i_1 < i_2 < i_3 \leqq 9$. However, since $[i_1 - a, i_2 - a, i_3 - a] \cong [i_1, i_2, i_3]$ due to the fact that every nonzero a mod p is prime to p, we need only consider $[0, i_2, i_3]$, $0 < i_2 < i_3 \leqq 9$.

If $[0, i_2, i_3]$ is a difference set for a given g, then $[0, vi_2, vi_3]$ is the same difference set for a primitive root g^u where $uv \equiv 1 \pmod{10}$. This follows from the discussion in connection with (2.3). We will therefore cover the case $[0, vi_2, vi_3]$ when we consider $[0, i_2, i_3]$.

The third type of isomorphism, due to translates of the residues themselves, cannot be dealt with similarly since the classes do not map in a systematic way. This type was handled after the machine computation.

5. Results. The procedure described in Article 3 was programmed and yielded the following difference sets:

(1) $[0, 1]$, $m \equiv 2 \pmod 5$, $p = 31$, $g = 17$, $D = (1, 5, 17, 22, 23, 25)$. This is isomorphic to $(1, 2, 4, 9, 13, 19)$.

(2) $[0, 1]$, $m \equiv 3 \pmod 5$, $p = 31$, $g = 24$, $D = (1, 5, 11, 24, 25, 27)$. This is isomorphic to $(1, 2, 4, 9, 13, 19)$.

(3) $[0, 2, 4, 6, 8]$, all m and p. Since we assumed that $p \equiv 11 \pmod{20}$, we have the quadratic residues of primes $p \equiv 3 \pmod 4$.

(4) $[0, 1, 2, 4, 5]$, $m \equiv 2 \pmod 5$, $p = 11$, $g = 8$, $D = (1, 4, 8, 9, 10)$. This is isomorphic to the set of quadratic residues $(1, 3, 4, 5, 9)$.

(5) $[0, 1, 2, 5]$ and 0, $m \equiv 4 \pmod 5$, $p = 11$, $g = 6$, $D = (0, 1, 3, 6, 10)$. This is isomorphic to the set of quadratic residues $(1, 3, 4, 5, 9)$.

(6) $[0, 1, 2, 3, 6]$ and 0, $m \equiv 3 \pmod 5$, $p = 11$, $g = 7$, $D = (0, 1, 2, 4, 5, 7)$. D's complement is isomorphic to the set of quadratic residues $(1, 3, 4, 5, 9)$.

(7) $[0, 2, 4, 6, 8]$ and 0, all m and p. We have here the complement of the set of quadratic residues of primes $p \equiv 3 \pmod 4$.

These were all the difference sets of this type.

The set mentioned in (1) and (2), $(1, 2, 4, 9, 13, 19)$, is the known planar set listed in [4]. The set of quadratic residues of primes $p \equiv 3 \pmod 4$ mentioned in (3), (4), (5), (6) and (7) is the family discovered by E. Lehmer [3].

6. Conclusion. There were no new difference sets uncovered by this computational project. The outcome seems to indicate that the type of family discovered by Hall for the case $p = 6f + 1$, f odd, is rare. The author plans to attempt a similar search with primes of the form $p = 12f + 1$, f odd, based on Whiteman's formulas [6] for the cyclotomic numbers of order 12 in the near future.

System Sciences Division of Control Data Corporation
Los Angeles, California

→ L. E. Dickson, "Cyclotomy, higher congruences and Waring's problem," *Amer. J. Math.*, v. 57, 1935, p. 391–424.

2. M. Hall, Jr., "A survey of difference sets," *Proc. Amer. Math. Soc.*, v. 7, 1956, p. 975–986. MR **18**, 560.

3. E. Lehmer, "On residue difference sets," *Canad. J. Math.*, v. 5, 1953, p. 425–432. MR **15**, 10.

4. H. J. Ryser, *Combinatorial Mathematics*, Carus Mathematical Monographs, No. 14, Math. Assoc. Amer., Wiley, New York, 1963. MR **27** #51.

5. A. L. Whiteman, *The Cyclotomic Numbers of Order Ten*, Proc. Sympos. Appl. Math., v. 10, Amer. Math. Soc., Providence, R. I., 1960, p. 95–111. MR **22** #4682.

6. A. L. Whiteman, "The cyclotomic numbers of order twelve," *Acta Arith.*, v. 6, 1960, p. 53–76. MR **22** #9480.