# CONCERNING DIFFERENCE SETS

T. G. OSTROM

A set of integers $\{a_0, a_1, \ldots, a_n\}$ is said to be a difference set modulo $N$ if the set of differences $\{a_i - a_j\}$ $(i, j = 0, 1, \ldots, n)$ contains each non-zero residue mod $N$ exactly once. It follows that $N$ and $n$ are connected by the relation $N = n^2 + n + 1$. If $\{a_0, a_1, \ldots, a_n\}$ is a difference set mod $N$, so is the set $\{a_0 + s, a_1 + s, \ldots, a_n + s\}$ $(s = 0, 1, \ldots, N)$. These difference sets form a finite projective plane of $N$ points, with each difference set constituting a line in the plane. Conversely, given a finite projective plane of $N$ points and a cyclic collineation of order $N$, the collineation leads to a numbering of the points so that each line becomes a difference set. Singer [5] has shown that a difference set can be constructed whenever $n$ is a prime power and has conjectured that there are difference sets in no other cases. Hall [3] has shown that there are no difference sets for any composite $n$ less than or equal to 100 and Mann and Evans [2] have extended this result to $n$ less than or equal to 1600.

Hall [3] has defined a "multiplier" as any number $q$ such that the set $\{qa_i\}$ $(i = 0, 1, \ldots, n)$ is the same as the set $\{a_j + s\}$ $(j = 0, 1, \ldots, n)$ for some $s$. He has shown that every factor of $n$ is a multiplier. He has also shown that for each $N$ which permits a difference set, there is at least one difference set which is fixed by all multipliers. Mann [4] has shown that if there is a difference set mod $N$ and a multiplier of even order, $n$ must be a square.

In this paper we show that, under certain conditions, the multipliers form a cyclic group. We use this result to obtain extensions of some theorems of Mann and Evans [2] concerning the possible orders of multipliers of a difference set. These theorems have a definite bearing on the question as to which values of $n$ permit difference sets. Mann and Evans used their theorems, along with some other results, to show that no difference sets can exist when $n$ is a composite number less than 1600. On the basis of computations in individual cases, the author conjectures that theorems of this type may eliminate all composite values of $n$, thus leading to a complete solution of the problem.

DEFINITION. Let $N_1$ be a prime factor of $N$. (1) We shall say that $N_1$ is of *type I* if there is some multiplier $q$ (mod $N$) such that the exponent to which $q$ belongs mod $N$ is greater than the exponent to which it belongs mod $N_1$. (2) We shall say that $N_1$ is of *type II* if every multiplier mod $N$ belongs to the same exponent mod $N$ as it does mod $N_1$.

*Remark.* No divisor of zero mod $N$ can be a multiplier since, if a difference set $\{a_0, a_1, \ldots a_n\}$ be multiplied by a divisor of zero, at least one of the differ-

Received August 12, 1952; in revised form October 15, 1952.

ences $\{a_i - a_j\}$ $(i \neq j)$ will be carried into zero. Hence every prime factor of $N$ is either of type I or type II.

THEOREM 1. *Suppose that there is a difference set* mod $N$ *and that* $N$ *has a prime factor* $N'$ *of type* I. *Let* $t$ *be the exponent to which the multiplier* $q$ *(of the definition above) belongs* mod $N'$. *Let* $N_1 = (q^t - 1, N)$. *Then* (a) $N'$ *divides* $N_1 \neq N$, (b) $N_1$ *is of the form* $n_1^2 + n_1 + 1$, (c) *there is a difference set* mod $N_1$ *and every multiplier for the difference sets* mod $N$ *is a multiplier for the difference sets* mod $N_1$.

*Proof.* The proof follows immediately from Hall [**3**, Theorem 4.5] and the definition of a factor of type I, since $q^t$ is a multiplier.

*Remark.* If $N_1$ in Theorem 1 is less than $1600^2 + 1600 + 1$, $n_1$ must be a prime power. If, in addition, $n$ is divisible by 2 or 3, then $n_1$ must be a power of 2 or 3 respectively, since Hall has proved that 2 can be a multiplier only if $n_1$ is even, while Mann [**4**] has proved that 3 can be a multiplier only if $n_1$ is congruent to zero mod 3.

COROLLARY 1. *Suppose that* $n = m^r$, *where* $(r, 3) = 1$ *and there is a difference set* mod $N = n^2 + n + 1$. *Then there is a difference set* mod $N_1 = m^2 + m + 1$ *and every multiplier* mod $N$ *is a multiplier* mod $N_1$.

*Proof.* Let $(m - 1, N) = N'$. Then $m \equiv 1 \pmod{N'}$,

$$N = m^{2r} + m^r + 1 \equiv m^2 + m + 1 \equiv 3 \pmod{N'}.$$

Hence $N' = 1$ or 3 and, if $N' = 3$, $m^2 + m + 1 \equiv 0 \pmod 3$. In no case is $n^2 + n + 1 \equiv 0 \pmod 9$. Hence $(m^3 - 1,\ m^{2r} + m^r + 1) = m^2 + m + 1$, provided $(r, 3) = 1$.

COROLLARY 2. *The only difference sets for* $n$ *less than* $1600^2$ *in which there is a multiplier of even order are those in which* $n$ *is an even power of a prime.*

*Proof.* Mann has proved that if there is a multiplier of even order, $n$ must be a square. If $n = m^2$, there is a difference set mod $(m^2 + m + 1)$. If $m \leqslant 1600$, $m$ must be a prime power.

THEOREM 2. *If* $N$ *contains a prime factor* $N_1$ *of type* II, *the multipliers form a cyclic multiplicative group.*

*Proof.* The product of two multipliers is a multiplier. Obviously the multipliers form a group. Let the multipliers be reduced mod $N_1$. Since $N_1$ is prime, the images of the multipliers in the residue system mod $N_1$ form a cyclic group. We shall show that any two different multipliers $q_1$ and $q_2$ have different images in the residue system mod $N_1$. Suppose that $q_1 \equiv q_2 \pmod{N_1}$, where $q_1$ and $q_2$ are multipliers. Since the multipliers form a group, we may write $q_2 \equiv q_1 q_3 \pmod N$, where $q_3$ is a multiplier. Thus $q_1 \equiv q_2 \equiv q_1 q_3 \pmod{N_1}$ and $q_1(q_3 - 1) \equiv 0 \pmod{N_1}$. Now $q_1 \not\equiv 0 \pmod{N_1}$ since divisors of zero cannot be multipliers.

But $N_1$ is prime, so $q_3 - 1 \equiv 0 \pmod{N_1}$. Since $N_1$ is of type II, this implies that $q_3 - 1 \equiv 0 \pmod{N}$ and hence $q_1 \equiv q_2 \pmod{N}$. Thus the mapping of multipliers is 1 to 1, and the multipliers must form a cyclic group mod $N$.

THEOREM 3. *Suppose that:*

(1) *there is a difference set* mod $N = n^2 + n + 1$,

(2) $N = N_1 N_2 \ldots N_k$, *where* $N_i$ *is prime* $(i = 1, 2, \ldots, k)$,

(3) $n$ *is not a square*,

(4) *for some* $i$, $N_i$ *is of type* II;

*then the order* $S$ *of the group of multipliers is odd and divides* $\phi(N_i) = N_i - 1$.

*Proof.* If $S$ is even, the order of the primitive multiplier is even and $n$ must be a square. The order of any non-zero residue mod $N_i$ divides $\phi(N_i)$. If $N_i$ is of type II, the order of every multiplier mod $N_i$ is the same as its order mod $N$.

THEOREM 3.1. *If the hypotheses of Theorem* 3 *are valid and*

(5) $N_i$ *is of type* II *for* $i = 1, 2, \ldots, k$,

(6) $n + 1 \equiv 0 \pmod{3}$,

*then* $S$ *divides* $n + 1$.

*Proof.* Mann and Evans have shown that 0 is not contained in the difference set fixed under all multipliers if $n + 1 \equiv 0 \pmod{3}$. Let $q$ be the primitive multiplier. Then (for any number $a \not\equiv 0$) if $a$ is in the fixed difference set, $a, aq, \ldots, aq^{S-1}$ are all incongruent mod $N$ and all included in the fixed difference set. The $n + 1$ numbers in this fixed set therefore occur in subsets of $S$ each.

THEOREM 3.2 *If* (1), (2), (3), (5) *are all satisfied and* $n \equiv 0 \pmod{3}$ *then* $S$ *divides* $n$.

*Proof.* Mann and Evans have shown that 0 is contained in the fixed difference if $n \equiv 0 \pmod{3}$. As in Theorem 3.1, the $n$ non-zero numbers in the fixed difference set occur in subsets of $S$ each.

*Remark.* If $n - 1 \equiv 0 \pmod{3}$, $N \equiv 0 \pmod{3}$ and 3 is a factor of type I.

THEOREM 3.3 *Suppose that:*

(1) *there is a difference set* mod $N$,

(2) $N = N_1 N_2$ ($N_1$ *and* $N_2$ *not necessarily prime*),

(3) *every factor of* $N_2$ *is of type* II *with respect to* $N$,

(4) $(q^\alpha - 1, N) = N_1$, *where* $\alpha < S$ *and* $q$ *is the primitive multiplier;*

*then* $N_1$ *is of the form* $n_1^2 + n_1 + 1$ *and* $S$ *divides* $n - n_1$.

*Proof.* By Theorem 1, there is a difference set mod $N_1$ and $N_1 = n_1^2 + n_1 + 1$. By Mann and Evans [2, Theorem 6], there are $n_1 + 1$ multiples of $N_2$ in the fixed difference set. If $a$ is any residue mod $N$ which is not a multiple of $N_2$, let $t$ be the least power of the primitive multiplier $q$ such that $aq^t \equiv a \pmod{N}$. Then $a(q^t - 1) \equiv 0 \pmod{N = N_1 N_2}$. Hence $q^t - 1 \equiv 0$ mod some factor of

$N_2$. Since all factors of $N_2$ are of type II with respect to $N$, $t = S$. Thus the $n - n_1$ residues in the fixed difference set which are non-multiples of $N_2$ occur in sets $a, aq, \ldots, aq^{S-1}$ of $S$ each, and $S$ divides $n - n_1$.

Theorems 3.1, 3.2, and 3.3 are extensions of Corollaries 5.1, 5.2, and Theorem 9, respectively, of Mann and Evans [**2**]. The proofs are similar in form to those given in [**2**].

As an example of the way in which Theorem 1 can be applied, suppose that $n$ is even and $n \equiv 5$ or 25 (mod 31). Then 2 is a multiplier and $(2^5 - 1, N) = 31$. But 2 is not a multiplier for the difference set mod 31; hence, by Theorem 1, there can be no difference set mod $N$.

As an example of the application of the other theorems, consider the case $n = 411$, $N = 313 \cdot 541$. Neither 313 nor 541 is of the form $n_1^2 + n_1 + 1$; hence, by Theorem 1, neither can be of type I. By Theorem 3, $S$ divides $313 - 1 = 3 \cdot 8 \cdot 13$ and $541 - 1 = 4 \cdot 5 \cdot 27$. By Theorem 3.2, $S$ divides $n = 3 \cdot 137$. Hence $S$ must be 3. Since 3 (which should be a multiplier) is not of order 3, there can be no difference set.

## References


1. R. H. Bruck and H. J. Ryser, *The nonexistence of certain finite projective planes*, Can. J. Math., *1* (1949), 88–93.
2. T. A. Evans and H. B. Mann, *On simple difference sets*, Sankhyā, *11* (1951), 357–364.
3. Marshall Hall, *Cyclic projective planes*, Duke Math. J., *14* (1947), 1079–1090.
4. H. B. Mann, *Some theorems on difference sets*, Can. J. Math., *4* (1952), 222–226.
5. James Singer, *A theorem in finite projective geometry and some applications to number theory*, Trans. Amer. Math. Soc., *43* (1938), 377–385.


*Montana State University*