ON MULTIPLIERS OF DIFFERENCE SETS[1]

BY

H. B. MANN AND S. K. ZAREMBA

For the notation and terminology used in this paper see [1] chapters 6 and 7, except that we shall write groups multiplicatively. Let $\left(\frac{a}{m}\right)$ denote the Jacobi symbol [4, page 168], ζ_m a primitive m-th root of unity, and R the field of rational numbers.

Newman [3] proved the following theorem: *If D is a cyclic difference set with parameters v, k, λ, $n = k - \lambda = 2q$, q a prime, $(7q, v) = 1$ then q is a multiplier of D.*

Turyn [5] generalized Newman's result in various ways. Turyn's result is the following:

THEOREM 1. *Let D be an Abelian difference set with parameters v, k, λ having $n = k - \lambda = 2\prod_{i=1}^{s} q_i^{a_i}$, q_i odd primes, $(v, q_i) = 1$. Let $t \equiv q_i^{b_i}\ (v)$, $i = 1, \cdots, s$. If $v \equiv 0\ (7)$ let $\left(\frac{t}{7}\right) = +1$. Then t is a multiplier of D.*

Turyn also remarks that $\left(\frac{t}{7}\right) = +1$ if $v \equiv 0\ (7)$ and if any of the a_i is odd. This follows because $\left(\frac{t}{7}\right) = -1$ implies $q_i^{3b_i} \equiv -1\ (7)$ and by Theorem 7.2 of [1] a_i must be even.

In this paper we shall be able to remove the restriction $\left(\frac{t}{7}\right) = +1$ for $v \equiv 0\ (7)$ for a number of cases including all difference sets with $n > \lambda$ and $(\lambda, \prod_{i=1}^{s} q_i) = 1$.

We note in particular that for $s = 1$, Theorem 1 implies that q_1 is multiplier if $\left(\frac{q_1}{7}\right) = +1$ and that q_1^2 is always multiplier.

The cases which are not settled by Turyn's theorem are of special interest because the existence of such a difference set with $\left(\frac{t}{7}\right) = -1$ would in fact disprove the conjecture that every divisor of n is multiplier. For $\left(\frac{t}{7}\right) = -1$ implies $\left(\frac{q_1}{7}\right) = -1$ and Corollary 7.2.2 of [1] shows that q_1 is not a multiplier since n is not a square. We shall however be able to prove nonexistence of a difference set in a large class of cases including all difference sets with $n > \lambda$ and $(\lambda, \prod_{i=1}^{s} q_i) = 1$.

Combining Turyn's result with theorem 7.3 of [1] we can restrict ourselves to values v, k, λ where

$$\text{I} \qquad \begin{gathered} k - \lambda = n = 2q^2, \qquad q = \prod_{i=1}^{s} q_i^{a_i} \\ t \equiv q_i^{b_i}\ (v),\ i = 1, \cdots, s, \qquad v \equiv 0\ (7),\ \left(\frac{t}{7}\right) = -1, \\ n > \lambda \geqq q^2, \end{gathered}$$

where the q_i are distinct odd primes.

Received August 21, 1967.

[1] Sponsored by the Mathematics Research Center, United States Army, Madison, Wisconsin.

It follows from I that $\left(\frac{q_i}{7}\right) = -1$ and that $b_i \equiv 1$ (2). This implies that the parity of the order of t mod any divisor of v is the same as that of q_i and in particular that $\left(\frac{q_i}{v_1}\right) = \left(\frac{t}{v_1}\right)$ for every divisor v_1 of v.

We first prove

THEOREM 2. *There is no difference set with parameters v, k, λ satisfying* I *in a group G of order v with a subgroup of order* 49.

Proof. Under the conditions of theorem 2 there exists a homomorphism mapping G into G_1, a group of order 49. This homomorphism extends to the groupring of G. Let $D_1 = \sum_{g \in G_1} a_g\, g$ correspond to D in this homomorphism. Then

$$D_1 D_1(-1) = \mu G_1 + 2q^2, \tag{1}$$

where μ is an integer. Now let q_1 be a prime factor of q. Then since $\left(\frac{q_1}{7}\right) = -1$ we have $q_1^3 \equiv -1$ (7) and $q_1^{21} \equiv -1$ (49). Hence

$$(\chi(D_1(-1)), q_1^{a_1}) = (\chi(D_1), q_1^{a_1}) = q_1^{a_1}$$

for every non-principal character χ of G_1. Since this is true for every prime factor q_i of q we have

$$\chi(D_1) \equiv 0 \quad (q)$$

for every non-principal character of G_1. Hence from lemma 7.3 of [1] we get

$$D_1 = \mu_1 G_1 + qH, \qquad \mu_1 \text{ integral.} \tag{2}$$

Substituting this into (1) gives

$$HH(-1) = \mu^* G_1 + 2, \tag{3}$$

with integral μ^*.

The following lemma shows that (3) cannot be solved in integers.

LEMMA. *Let $A = \sum a_g\, g$ be an element of the grouping of a group G of order v over the integers where v is a power of an odd prime. Suppose*

$$AA(-1) = n + \lambda G. \tag{4}$$

Let
$$x^2 = n + \tau v, \quad 0 < x < v;$$
then
$$n + \tau \geqq x. \tag{5}$$

Moreover equality in (5) *implies that either A or $-A$ is congruent to a difference set* mod G.

Proof. From (4) we have

$$\begin{aligned} \sum a_g &= \varepsilon x + rv \qquad \varepsilon = \pm 1 \\ \left(\sum a_g\right)^2 &= n + \lambda v \qquad (6) \\ \sum a_g^2 &= n + \lambda. \end{aligned}$$

The first two equations of (6) give

$$\lambda = \tau + 2\varepsilon r x + r^2 v. \tag{7}$$

We set $a_g = r + b_g$ then

$$\sum b_g = \varepsilon x$$

and

$$n + \lambda = \sum a_g^2 = r^2 v + 2r \sum b_g + \sum b_g^2 = r^2 v + 2r\varepsilon x + \sum b_g^2 .$$

Combining this with (7) we get

$$n + \tau = \sum b_g^2 \geqq \left| \sum b_g \right| = x.$$

Moreover equality implies that b_g can take only the values 1 or 0, if we choose A so that $a_g > 0$ for at least one g. Hence the lemma.

Applying the lemma to (3) we have $n = 2, x = 10, \tau = 2$ which shows that (3) has no integral solutions and proves Theorem 2.

THEOREM 3. *If the conditions* I *are satisfied and if a prime factor* q_1 *of* q *is of even order with respect to a prime factor* p *of* v, $p \neq 7$, *then no* v, k, λ *difference set exists.*

Proof. We map G homomorphically into the group R_p of residues mod p. This mapping maps D into $D_1 = \sum_{i=0}^{p-1} a_i x^i$, where x is a generator of R_p, satisfying (for some integer μ)

$$D_1 D_1(-1) = \mu R_p + 2q^2$$

The conditions I imply that

$$(\chi(D_1(t)), q) = (\chi(D_1), q)$$

and therefore

$$\chi(D_1)\chi(D_1(-t)) \equiv 0 \quad (q^2)$$

for every non-principal character χ of R_p. Hence

$$D_1 D_1(-t) = \mu R_p + q^2 F \tag{8}$$

where $\chi_1(F) = 2$ and $FF(-1) = 4$. A calculation presented in detail in [2] shows this to be impossible for $p \neq 7$ unless $F = 2x^j$. Multiplying (8) by $D_1(t)$ we get $D_1(t) = x^{-j} D_1$. But if q_1 is of even order with respect to p then t must be of even order with respect to p (see condition I). Hence we have

$$t^f \equiv -1 \quad (p)$$

for some f, and it follows that

$$D_1(-1) = D_1(t^f) = x^u D_1 .$$

But this contradicts

$$\chi(D_1)\chi(D_1(-1)) = 2q^2$$

because 2 is not a square in $R(\zeta_p)$.

This completes the proof of Theorem 3.

We now consider the case $n > \lambda$, $(\lambda, q) = 1$. We have

$$k^2 - n = k^2 - 2q^2 \equiv 0 \quad (\lambda), \qquad k - 2q^2 = \lambda$$

Hence

$$(9) \qquad 4q^4 - 2q^2 \equiv 0 \quad (\lambda) \qquad 4q^2 - 2 \equiv 0 \quad (\lambda).$$

Since $2q^2 > \lambda > q^2$ this implies

$$4q^2 - 2 = 2\lambda \quad \text{or} \quad 4q^2 - 2 = 3\lambda.$$

But $4q^2 \not\equiv 2$ (3) and therefore $\lambda = 2q^2 - 1$. Hence the only solution in this case is

$$(10) \qquad v = 8q^2 - 1, \qquad k = 4q^2 - 1, \qquad \lambda = 2q^2 - 1.$$

We now assume that the conditions I are satisfied and the parameters v, k, λ are given by (10). An easy calculation shows that

$$\left(\frac{q_1}{v}\right) = +1$$

for every prime divisor q_1 of q. Hence if $v = 7v_1$, $(v_1, 7) = 1$ and $\left(\frac{q_1}{7}\right) = -1$ we have

$$\left(\frac{q_1}{v_1}\right) = -1.$$

Hence

$$\left(\frac{q_1}{p}\right) = -1$$

for some prime divisor of v_1. Hence no difference set can exist by Theorem 3. Together with Theorems 1 and 2 and Theorem 7.3 of [1] we therefore have

THEOREM 4. *Let G be an Abelian group. Assume that G has a difference set D with $n = k - \lambda = 2n_1$, $(\lambda, n_1) = 1$, $n > \lambda$, and that $t \equiv q_i^{f_i}$ (v) for every prime divisor q_i of n_1 and some integer f_i. Then t is a multiplier of D.*

If we drop the restriction $n > \lambda$ then (9) has the additional solution $\lambda = 4q^2 - 2$, and this gives

$$v = 9q^2 - 2, \qquad k = 6q^2 - 2, \qquad \lambda = 4q^2 - 2.$$

The complementary solution to this is

$$(11) \qquad v = 9q^2 - 2, \qquad k = 3q^2, \qquad \lambda = q^2.$$

If the parameters are given by (11) then $\left(\frac{q_1}{v}\right) = \left(\frac{2}{q_1}\right)$. If $v = 7v_1$, $(7, v_1) = 1$ and if $\left(\frac{q_1}{7}\right) = -1$ then

$$\left(\frac{q_1}{v_1}\right) = -\left(\frac{2}{q_1}\right).$$

Hence by Theorem 3 if a difference set with the parameters (11) exists we must have

$$\left(\frac{2}{q_1}\right) = -1. \tag{12}$$

Hence we have the following theorem:

THEOREM 5. *Suppose a difference set with parameters given by* (11) *exists in an Abelian group G of order $v = 7v_1$, $(7, v_1) = 1$. Suppose moreover that the conditions* I *are satisfied. Then* $\left(\frac{2}{q_1}\right) = -1$ *for every divisor q_1 of q.*

REFERENCES

1. H. B. MANN, *Addition theorems*, Wiley, New York, 1965.
2. R. L. MCFARLAND, *A generalization of a result of Newman on multipliers of difference sets*, J. Res. Nat. Bureau Standards, vol. 69B (1965), pp. 319–322.
3. MORRIS NEWMAN, *Multipliers of difference sets.*, Canad. J. Math., vol. 15, (1963), pp. 121–124.
4. B. M. STEWART, *Theory of numbers*, Macmillan, New York, 1952.
5. RICHARD J. TURYN, *The multiplier theorem for difference sets*, Canad. J. Math., vol. 16 (1964), pp. 386–388.

UNIVERSITY OF WISCONSIN
MADISON, WISCONSIN