SOME THEOREMS ON DIFFERENCE SETS

HENRY B. MANN

A set $a_1, \ldots, a_k$ of different residues mod v is called a difference set (v, k, λ) $(v > k > \lambda)$ if the congruence $a_i - a_j \equiv d \pmod{v}$ has exactly λ solutions for $d \not\equiv 0 \pmod{v}$. Singer [**4**] has demonstrated the existence of a difference set $(v, k, 1)$ if $k - 1$ is a prime power, and difference sets for $\lambda > 1$ have been constructed by various authors; but necessary and sufficient conditions for the existence of a (v, k, λ) are not known. It has not been possible so far to find a difference set with $\lambda = 1$ if $k - 1$ is not a prime power and it has therefore been conjectured that no such difference set exists. The condition

$$k(k-1) = \lambda(v-1) \tag{1}$$

is trivial. Owing to the efforts of Hall [**2**] and Hall and Ryser [**3**] efficient necessary conditions are now available by which a large number of (v, k, λ) can be shown to be impossible. Hall [**2**] in particular succeeded in eliminating all doubtful cases of $(v, k, 1)$ with $k - 1 \leqslant 100$ and this bound could easily be extended upward. It is the purpose of the present paper to improve some of the results of Hall [**2**] and Hall and Ryser [**3**].

A number t is called a multiplier of (v, k, λ) if $\{ta_i\} \equiv \{a_j + s\} \pmod{v}$ for some s. Hall and Ryser [**3**] generalizing a theorem of Hall [**2**] proved that every prime divisor p of $k - \lambda = n$ is a multiplier provided $p > \lambda$. The restriction $p > \lambda$ can sometimes be obviated by remembering that the residues which are not in (v, k, λ) form a $(v, v - k, v - 2k + \lambda)$ with the same multiplier system as (v, k, λ).

We shall prove the following:

THEOREM 1. *If t is of even order with respect to a prime divisor q of v then n is a square if $\left(\frac{t}{q}\right) = -1$. If $\left(\frac{t}{q}\right) = +1$ then $n = b^2$ or a^2q^3, where a, b are integers.* Thus always $n = b^2$ if $n \not\equiv 0 \pmod{q}$.

Proof. Let t have order $2f$ with respect to q then $t^f \equiv -1 \pmod{q}$. We put

$$\theta(x) = x^{a_1} + \ldots + x^{a_k}.$$

Since t is a multiplier, we have for some s,

$$\theta(x^{t^f}) \equiv x^s\theta(x) \qquad \mathrm{mod}\,(x^v - 1). \tag{2}$$

Substituting a primitive qth root of unity ζ for x we have

$$\theta(\zeta^{t^f}) = \theta(\zeta^{-1}) = \zeta^s\theta(\zeta). \tag{3}$$

Received December 11, 1950

https://doi.org/10.4153/CJM-1952-020-4 Published online by Cambridge University Press

The prime q must be odd, hence $2r \equiv s \pmod q$, and since

$$\theta(x)\theta(x^{-1}) \equiv n + \lambda(1 + \ldots + x^{v-1}) \qquad \mod (x^v - 1)$$

it follows that

$$(4) \qquad (\zeta^r \theta(\zeta))^2 = n.$$

In the field $\mathfrak{F}(\zeta)$ generated by ζ over the field of rational numbers the field $\mathfrak{F}(\sqrt{\pm q})$ is the only quadratic subfield. Hence either n is a square or $n = a^2 q$.

In the latter case we have

$$(4a) \qquad (\zeta^r \theta(\zeta)) = \pm a\sqrt{q}.$$

The Galois group of $\mathfrak{F}(\zeta)$ over $\mathfrak{F}(\sqrt{q})$ is the group of automorphisms $\zeta \rightarrow \zeta^a$ where a is a quadratic residue mod q. If $\left(\frac{t}{q}\right) = -1$ then $\zeta \rightarrow \zeta^t$ maps $\sqrt{q}$ into $-\sqrt{q}$. Hence if t is a multiplier,

$$\zeta^{rt}\theta(\zeta^t) = \zeta^{rt+s_1}\theta(\zeta) = \mp a\sqrt{q},$$
$$\zeta^{rt+s_1-r} = -1,$$

but this is impossible since q is odd.

The congruences $n \equiv 0 \pmod q$, $v \equiv 0 \pmod q$ imply $n \equiv 0 \pmod{q^2}$, since

$$(5) \qquad \lambda v = n^2 + (2\lambda - 1)n + \lambda^2;$$

but $n \equiv 0 \pmod{q^2}$ and $n = a^2 q$ imply $a \equiv 0 \pmod q$, which proves the second part of Theorem 1.

THEOREM 1a. *If under the conditions of Theorem* 1 *we have* $v = q$, *then* $k = v - 1$.

For then $(v, n) = 1$ and following the proof of Theorem 1 we are led to the equation

$$\zeta^r \theta(\zeta) = \pm b, \qquad b \text{ integral.}$$

But this relation is impossible unless $k = v - 1$.

Theorem 1 is a considerable improvement over Hall's Corollary 4.7 and Hall and Ryser's Theorem 3.2.

Theorem 1 has many applications. We give a few indicating its use. In the following corollaries let p always denote a prime divisor of n which exceeds λ and suppose that (v, k, λ) exists. We also assume $v \equiv 1 \pmod 2$ since for $v \equiv 0 \pmod 2$, n must always be a square [1].

COROLLARY 1. *If* $\lambda = 1$ *and* $n \equiv n_1$ *or* $n_1^2 \mod (n_1^2 + n_1 + 1)$ *and* p *is of even order with respect to* $n_1^2 + n_1 + 1$, *then* n *is a square.*

For then $v = n^2 + n + 1 \equiv 0 \bmod (n_1^2 + n_1 + 1)$. Thus p is of even order with respect to a prime divisor q of v. Also in this case $(v, n) = 1$.

For instance n must be a square in the following cases:

$$\begin{array}{ll}
n \equiv 1 \pmod{3} & p \equiv 2 \pmod{3} \\
n \equiv 2,\ 4 \pmod{7} & p \equiv 3, 5, 6 \pmod{7} \\
n \equiv 3,\ 9 \pmod{13} & p \equiv 2, 4, 5, 6, 7, 8, 10, 11, 12 \pmod{13} \\
n \equiv 5, 25 \pmod{31} & \left(\frac{p}{31}\right) = -1 \\
n \equiv 6, 36 \pmod{43} & \left(\frac{p}{43}\right) = -1 \\
n \equiv 7, 11 \pmod{19} & \left(\frac{p}{19}\right) = -1
\end{array}$$

and so forth.

COROLLARY 2. *If a multiplier is quadratic non-residue modulo a prime divisor of v then n is a square. Moreover, if v is prime then $k = v - 1$.*

COROLLARY 3. *If*

$$\left(\frac{(-1)^{\frac{1}{2}(v-1)}\lambda}{p}\right) = -1$$

then n is a square; if further v is a prime then (v, k, λ) is impossible.

For by (5) we have

$$\left(\frac{\lambda v}{p}\right) = \left(\frac{\lambda^2}{p}\right) = +1;$$

hence

$$\left(\frac{v}{p}\right) = \left(\frac{\lambda}{p}\right).$$

But

$$\left(\frac{p}{v}\right) = (-1)^{\frac{1}{2}(p-1)\frac{1}{2}(v-1)}\left(\frac{v}{p}\right) = \left(\frac{(-1)^{\frac{1}{2}(v-1)}\lambda}{p}\right),$$

and the corollary follows from Theorems 1 and 1a.

The case (91, 45, 22) already eliminated by Hall and Ryser is also quickly disposed of by Theorem 1, since $23 \equiv -3 \pmod{13}$ and -3 has the order 6 (mod 13).

We shall call a prime p an extraneous multiplier if p is a multiplier but $n \not\equiv 0 \pmod{p}$. We shall prove

THEOREM 2. *The prime p is a multiplier if and only if*

$$\theta(x)^p \equiv x^s\theta(x) \qquad \operatorname{modd}(p, x^v - 1). \tag{6}$$

If p is an extraneous multiplier then

$$\theta(x)^{p-1} \equiv x^s \qquad \operatorname{modd}(p, x^v - 1) \tag{6'}$$

https://doi.org/10.4153/CJM-1952-020-4 Published online by Cambridge University Press

if $k \not\equiv 0 \pmod{p}$, *and*

$$\theta(x)^{p-1} \equiv x^s - T(x) \qquad \text{modd}(p, x^v - 1), \tag{6''}$$

$T(x) = 1 + x + \ldots + x^{v-1}$, *if* $k \equiv 0 \pmod{p}$.

Proof. If p is a multiplier we have

$$x^s\theta(x) \equiv \theta(x^p) \equiv \theta(x)^p \qquad \text{modd}(p, x^v - 1).$$

On the other hand, $\theta(x)^p \equiv x^s\theta(x)$, modd $(p, x^v - 1)$, implies $\theta(x^p) \equiv x^s\theta(x)$, modd $(p, x^v - 1)$. Since $\theta(x^p)$ and $x^s\theta(x)$ are polynomials whose coefficients are either 1 or 0, it follows from this that

$$\theta(x^p) \equiv x^s\theta(x) \qquad \text{mod}(x^v - 1).$$

Hence p is a multiplier.

If p is an extraneous multiplier we multiply (6) by $\theta(x^{-1})$ and obtain

$$\theta(x)^{p-1}(n + \lambda T(x)) \equiv x^s(n + \lambda T(x)) \qquad \text{modd } (p, x^v - 1), \tag{7}$$

$$n\theta(x)^{p-1} + \lambda k^{p-1}T(x) \equiv x^s(n + \lambda T(x)) \qquad \text{modd } (p, x^v - 1). \tag{7'}$$

If $k \not\equiv 0 \pmod{p}$ then $k^{p-1} \equiv 1 \pmod{p}$. If $k \equiv 0 \pmod{p}$ then $n \equiv -\lambda \pmod{p}$. Also $x^sT(x) \equiv T(x)$, mod $(x^v - 1)$, and the second part of the theorem follows easily from (7) and (7′).

COROLLARY 1. *If 2 is a multiplier for* (v, k, λ) *then either* $n \equiv 0 \pmod{2}$ *or* $k = v - 1$.

For otherwise Theorem 2 gives either

$$\theta(x) \equiv x^s \qquad \text{modd } (2, x^v - 1),$$

or

$$\theta(x) \equiv x^s + T(x) \qquad \text{modd } (2, x^v - 1)$$

and the corollary follows.

COROLLARY 2. *If 3 is a multiplier for* $(v, k, 1)$ *then* $n \equiv 0 \pmod{3}$.

For otherwise either

$$\theta(x)^2 \equiv x^s \qquad \text{modd } (3, x^v - 1), \tag{8}$$

or

$$\theta(x)^2 \equiv x^s - T(x) \qquad \text{modd } (3, x^v - 1). \tag{8'}$$

But x^m occurs in $\theta(x)^2$ only if $m = a_i + a_j$ and then exactly twice if $i \neq j$ and exactly once if $i = j$, whilst x^m does not occur for exactly $\frac{1}{2}n(n + 1)$ values of m. Thus (8) and (8′) are both impossible, and the corollary follows.

The following two theorems serve to show the non-existence of $(v, k, 1)$ in a large number of doubtful cases.

THEOREM 3. *If* t_1, t_2, t_3, t_4 *are multipliers of* $(v, k, 1)$ *such that* $t_1 + t_2 \equiv t_3$, $t_2 \not\equiv t_4 \pmod v$ *then* $t_1 + t_4$ *is not a multiplier.*

For in this case we have a difference set $a_1, \ldots, a_k$ which remains fixed under all multipliers [**2**]. If $t_1 + t_4 \equiv t_5 \pmod v$ is a multiplier, then for every a in this difference set

$$at_1 + at_2 \equiv at_3 \equiv a_k \pmod v,$$

$$at_1 + at_4 \equiv at_5 \equiv a_l \pmod v,$$

$$a_k - a_l \equiv at_2 - at_4 \pmod v.$$

Hence, since $\lambda = 1$, either $at_2 \equiv a_k \pmod v$ which implies $a \equiv 0$ or $at_2 \equiv at_4$, $a(t_2 - t_4) \equiv 0 \pmod v$. Hence for all a we have $a(t_2 - t_4) \equiv 0 \pmod v$; but since every $m \equiv a_i - a_j \pmod v$ it follows that $t_2 - t_4 \equiv 0 \pmod v$.

COROLLARY 1. *If* 2, p, q *are multipliers for* $(v, k, 1)$ *and* $p \not\equiv q \pmod v$ *then* $p + q$ *is not a multiplier.*

This follows since $p + p = 2p$ is a multiplier.

COROLLARY 2. *If* 2 *and* $2^k + 1$ *are multipliers then* $2^k \equiv 1 \pmod v$. *If* 2 *and* $2^k - 1$ *are multipliers then* $2^k - 1 \equiv 1 \pmod v$.

This follows at once from Corollary 1 with $p = 1$.

THEOREM 4. *If* t_1, t_2, t_3, t_4 *are multipliers for* $(v, k, 1)$ *and* $(t_1 - t_2) = (t_3 - t_4)$ *then*

$$(t_1 - t_2)(t_1 - t_3) \equiv 0 \pmod v. \tag{9}$$

For again let $a_1, \ldots, a_k$ be the set that remains fixed under all multipliers. Then for any a in this set,

$$t_1a - t_2a \equiv t_3a - t_4a \pmod v.$$

Hence either $t_1a \equiv t_2a \pmod v$ or $t_1a \equiv t_3a \pmod v$. Hence for all a, and therefore for every number m, we must have

$$(t_1 - t_2)(t_1 - t_3)m \equiv 0 \pmod v,$$

whence the theorem.

Theorem 4 was extensively used, but not explicitly stated, by Hall [**2**].

REFERENCES

1. S. Chowla and H. J. Ryser, *Combinatorial problems*, Can. J. Math., vol. 2 (1950), 93–99.
2. Marshall Hall, Jr., *Cyclic projective planes*, Duke Math. J., vol. 14 (1947), 1079–1090.
3. Marshall Hall, Jr. and H. J. Ryser, *Cyclic incidence matrices*, Can. J. Math., vol. 4 (1951), 495–502.
4. James Singer, *A theorem in finite projective geometry and some applications to number theory*, Trans. Amer. Math. Soc., vol. 43 (1938), 377–385.

Ohio State University