ON DIFFERENCE SETS

By S. Chowla

Institute for Advanced Study, Princeton, New Jersey

Communicated by Oswald Veblen, December 5, 1948

It is known that the existence of $m + 1$ integers (called a perfect difference set of order $m + 1$) $d_1, d_2, \ldots, d_{m+1}$ such that the congruence $d_i - d_j \equiv n(\text{mod } m^2 + m + 1)$ has exactly one solution for every $n \not\equiv 0(\text{mod } m^2 + m + 1)$, leads to the construction of a finite projective plane with $m + 1$ points on a line. All known cases of such planes have $m = p^g$, where p is a prime and g is a positive integer. It seems natural to conjecture that a perfect difference set of order $m + 1$ can exist only if m is a power of a prime. Only recently Bruck and Ryser (*Bull. Am. Math. Soc.*) announced the startling result that there exists no finite projective plane with $m + 1$ points on a line whenever $m \equiv 1$ or $2(\text{mod } 4)$, provided m is divisible by a prime $4k + 3$ to an odd power. It follows from their result that for such values of m there exists no perfect difference set (P.D.S.) or order $m + 1$. Moreover Singer proved the existence of a P.D.S. of order $m + 1$, whenever $m = p^g$.

In this paper I obtain some (but not all) assertions on the non-existence of perfect difference sets implied by the results of Bruck and Ryser. I also obtain some results not implied by their work. For example, I prove that there exists no P.D.S. of order $m + 1$ when $m = 10$ or 159.

We introduce the idea of a difference set (D.S.) of m numbers (mod g). We call the set of m numbers $d_1, d_2, \ldots, d_m$ a difference set (mod g) if the congruence $d_i - d_j \equiv n(\text{mod } g)$ has the same number of solutions [which must be $m(m - 1)/(g - 1)$] for every $n \not\equiv 0 (\text{mod } g)$. The set of 5 numbers 1, 3, 4, 5, 9 furnishes an example of a D.S. of 5 numbers (mod 11). Again the set of 4 numbers 0, 1, 3, 9 forms a D.S. (mod 13). [This set occurs in Veblen and Bussey, *Trans. Am. Math. Soc.*, 1906, and is used to generate a finite projective plane with 4 points on a line.]

We now prove

THEOREM 1. *Let m and g be positive integers such that $m(m - 1) \equiv 0(\text{mod } g - 1)$. Write $\theta = m - m(m - 1)/(g - 1)$. Let g contain a prime factor $\lambda \equiv 3(\text{mod } 4)$ such that $-\lambda$ is a quadratic non-residue of some prime factor ϕ of θ, where ϕ occurs in θ to an odd power. Then there exists no D.S. of m numbers (mod g).*

Proof: If possible let there exist a D.S. of m numbers (mod g), say the numbers $d_1, d_2, \ldots, d_m$. Consider the sum

$$S = \sum_{j=1}^{m} \rho^{d_j},$$

where $\rho = \exp(2\pi i/\lambda)$. Clearly S is an algebraic integer of the field $K(\rho)$. Further, since the d's form a difference set (mod g), we have

$$S\bar{S} = m + \frac{m(m-1)}{(g-1)} \{\rho + \rho^2 + \rho^3 + \ldots + \rho^g\}$$

$$= m - \frac{m(m-1)}{(g-1)} = \theta,$$

$$S\bar{S} = \theta \qquad (1)$$

Now it is implicit in the theory of cyclotomy (as developed by Gauss) that the norm of S in the field generated by ρ is an integer of the form $(u^2 + \lambda v^2)/4$, where u and v are integers (we here use the fact that λ is of the form $4k + 3$). On the other hand it follows from (1) that this norm is also equal to $\theta^{(\lambda - 1)/2}$. Hence we have

$$u^2 + \lambda v^2 = 4\cdot\theta^{(\lambda - 1)/2}.$$

Since $(\lambda - 1)/2$ is odd, it follows from the last equation that $-\lambda$ is a quadratic residue of ϕ contrary to our assumption. Our theorem is proved.

Examples: 1. There exists no P.D.S. of order 7; i.e., there exists no D.S. of 7 numbers (mod 43). [Problem proposed by Veblen in *Am. Math. Monthly*, **13**, 46 (1906).]

Proof: Here $g = \lambda = 43$, $\theta = 7 - \frac{4^2}{4^2} = 6$; take $\theta = 3$. Clearly $-\lambda$ is a quadratic non-residue of ϕ.

2. There exists no P.D.S. of order 11, i.e., there exists no D.S. of 11 numbers (mod 111). This result is new.

Proof: Here $g = 111$, $\lambda = 3$, $\theta = 10$. Take $\phi = 5$. Clearly $-\lambda$ is a quadratic non-residue of ϕ.

3. There exists no P.D.S. of order 22 (Bruck and Ryser), i.e., no D.S. of 22 numbers (mod 463).

Proof: Here $g = \lambda = 463$, $\theta = 22$. Take $\phi = 11$. Clearly $-\lambda$ is a quadratic non-residue of ϕ.

4. There exists no P.D.S. of order 160. This result is new.

Proof: We show that there cannot exist a D.S. of 160 numbers (mod $159^2 + 159 + 1$). Since $159^2 + 159 + 1 \equiv 0 \pmod{19}$, we may take $\lambda = 19$. Take $\phi = 3$ since $\theta = 159$. Clearly $-\lambda$ is a quadratic non-residue of ϕ.