S_p-Sets with Multiplier p

Bernt Lindström
Department of Mathematics
Royal Institute of Technology
S-100 44 Stockholm
Sweden

Dedicated to Hans-Olov Zetterström on his 65th Birthday

ABSTRACT. An S_h-*set* (mod m) is a set S of integers such that the sums $a_1 + a_2 + \cdots + a_h$ of elements $a_1 \leq a_2 \leq \cdots \leq a_h$ from S are distinct (mod m). A *multiplier* μ of S is an integer such that $\mu S \equiv S$ (mod m).

We observe that $\mu \geq h$ is necessary for a multiplier $\mu > 1$ and prove that equality is possible at least when $h = p$ is a prime (Theorem).

S_h-sets (mod m) are sets S of integers such that all sums of h elements from S, with repetitions permitted, are distinct (mod m). Classical examples are the B_h-sets of Bose and Chowla [1] of size $q = p^k$ and $m = q^h - 1$. Only recently I could prove in [2] that a translate of B_2-sets has multiplier p. A *multiplier* μ of an S_h-set S (mod m) has the property that $\mu S \equiv S$ (mod m). Modified Bose-Chowla S_h-sets S (mod $p^h - 1$) of prime size p have multiplier p when h divides $p - 1$ by Theorem 1 in [3]. In this case the multiplier is $p \geq h + 1$.

We observe that $\mu \geq h$ is necessary when $\mu > 1$ is multiplier of a S_h-set S.

For, assume that $\mu < h$ and $a \in S$, hence $\mu a, \mu^2 a \in S$. Then we have

$$\mu a + \cdots + \mu a (h \text{ terms}) = a + \cdots + a(\mu \text{ terms}) + \mu a + \ldots + \mu a(h - \mu - 1 \text{ terms}) + \mu^2 a$$

and S is not an S_h-set.

ARS COMBINATORIA 59(2001), pp. 193-194

I will prove that the equality $\mu = h$ is possible (Theorem 1).

Consider the equation $X^q = X + 1$ over $GF(p)$, $q = p^k$. We find by induction over $v \geq 1$ for any root X

$$X^{q^v} = X + v. \tag{1}$$

When $v = p$ we have $X^{q^p} = X$ and X belongs to $GF(q^p)$. Let θ be a primitive element in this field and define

$$S(q) = \{a\colon 1 \leq a < q^p - 1, \theta^{aq} = \theta^a + 1\} \tag{2}$$

(i.e., θ^a, $a \in S(q)$, are the roots of $X^q - X - 1$).

Observe that $a \in S(q)$ implies $pa \in S(q) \pmod{q^p - 1}$, i.e., p is multiplier of $S(q)$, since $\theta^{aqp} = \theta^{ap} + 1$.

Theorem 1. *$S(q)$ is a S_p-set $\pmod{q^p - 1}$ of size q with multiplier p.*

Proof: It remains to prove that $S(q)$ is an S_p-set. Let $a_1, \ldots, a_p \in S(q)$ and write $X_i = \theta^{a_i}$ $(i = 1, \ldots, p)$. I will prove that the product $Y_p = X_1 \ldots X_p = \theta^{a_1 + \cdots + a_p}$ determines $\{X_1, \ldots, X_p\}$ uniquely. Write

$$\prod_{i=1}^{p}(X - X_i) = X^p - Y_1 X^{p-1} + \cdots - Y_p, \tag{3}$$

i.e., $Y_1, \ldots, Y_p$ are the basic symmetric functions of $X_1, \ldots, X_p$. We have then, by (1) and (3), for $v \geq 1$

$$Y_p^{q^v} = \prod_{i=1}^{p} X_i^{q^v} = \prod_{i=1}^{p}(X_i + v) = v^p + Y_1 v^{p-1} + \cdots + Y_p.$$

Hence, for $v = 1, 2, \ldots, p - 1$,

$$Y_1 v^{p-1} + Y_2 v^{p-2} + \cdots + Y_{p-1} v = Y_p^{q^v} - Y_p - v^p. \tag{4}$$

This is a linear system of equations in $Y_1, \ldots, Y_{p-1}$ the determinant (almost a "Vandermonde") of which is $\pm(p-1)!(p-2)!\ldots! \neq 0$ in $GF(p)$. It follows that $Y_1, Y_2, \ldots, Y_{p-1}$ are uniquely determined by $Y_p = X_1 X_2 \ldots X_p$. We conclude that $a_1 + \cdots + a_p$ determines $\{a_1, a_2, \ldots, a_p\} \pmod{q^p - 1}$, which was to be proved.

References

[1] R.C. Bose and S. Chowla, Theorems in the additive theory of numbers, *Comment. Math. Helv.* **37** (1962–63), 141–147.

[2] B. Lindström, A translate of Bose-Chowla B_2-sets, *Studia Scient. Math. Hungarica* (to appear).

[3] A.M. Odlyzko and W.D. Smith, Nonabelian sets with distinct k-sums, *Discrete Math.* **146** (1995), 169–177.