Discrete Mathematics 71 (1988) 87–88
North-Holland

COMMUNICATION

SUMS OF SUBSEQUENCES MODULO PRIME POWERS

N. ALON

Department of Mathematics, Sackler Faculty of Exact Sciences, Tel Aviv University, Tel Aviv, Israel

Received 29 February 1988
Communicated by I. Gessel

For a sequence $S = (a_1, a_2, \ldots, a_m)$ of residues mod n and for $0 \leq j < n$ let $f_n(S; j)$ denote the number of subsequences of S the sum of whose elements is congruent to j mod n. Proving a conjecture of Bulman-Fleming and Wang (see [1]), Guichard, (see [2]), has recently shown that if $m \geq n$ and n is a power of 2 then for every such S and j, $f_n(S; j)$ is even. Here we present a different, much shorter proof of a more general result. For S and j as above let $E_n(S; j)$ denote the number of subsequences of S consisting of an even number of members whose sum is congruent to j mod n. Similarly, let $O_n(S; j)$ denote the number of subsequences of S consisting of an odd number of members whose sum is congruent to j mod n. Clearly $f_n(S; j) = E_n(S; j) + O_n(S; j)$.

Theorem. *Let $n = p^k$ be a prime power and let $S = (a_1, a_2, \ldots, a_m)$ be a sequence of residues* mod n. *For each $1 \leq i \leq m$ let b_i be the maximum power of p that divides a_i, i.e. $b_i = \max(p^j : p^j \mid a_i)$. Then*

$$E_n(S; j) \equiv O_n(S; j) (\mathrm{mod}\, p) \quad \textit{for every } 0 \leq j < n \tag{1}$$

if and only if $\sum_{i=1}^{m} b_i \geq n$.

Proof. Define

$$g(x) = \prod_{i=1}^{m} (1 - x^{a_i}).$$

Let $h(x)$ be the remainder in the quotient $g(x)/(1 - x^n)$. Clearly, for every $0 \leq j < n$, the coefficient of x^j in $h(x)$ is precisely the difference $E_n(S; j) - O_n(S; j)$. However, over the field with p elements GF(p), $1 - x^n = (1 - x)^n$, as n is a power of p. Consequently, (1) holds if and only if $(1 - x)^n \mid g(x)$ over GF(p). For each $1 \leq i \leq m$, $a_i = b_i r_i$, where b_i is a power of p and p does not divide r_i.

Therefore, $(1-x)^{b_i}$ is the maximum power of $1-x$ that divides, over GF(p), the polynomial $1-x^{a_i}=(1-x)^{b_i}(1+x^{b_i}+x^{2b_i}+\cdots+x^{(r_i-1)b_i})$. We conclude that $(1-x)^n \mid g(x)$ over GF(p) if and only if $\sum_{i=1}^{m} b_i \geq n$. As the former condition is equivalent to (1), this completes the proof of the theorem. □

An immediate corollary of the above theorem is the following.

Corollary. *Let $n=p^k$ be a prime power and let $S=(a_1, a_2, \ldots, a_m)$ be a sequence of residues* mod n. *If $m \geq n$ then $E_n(S;j) \equiv O_n(S;j) (\mathrm{mod}\, p)$ for every $0 \leq j < n$.*

As a special case of the last corollary notice that if $n=2^k$ is a power of 2 and $S=(a_1, a_2, \ldots, a_m)$ is a sequence of residues mod n, where $m \geq n$, then $f_n(S;j)=E_n(S;j)+O_n(S;j)$ is even for every $0 \leq j \leq n$. This result was proved in [2] in a different method. □

References

[1] S. Bulman-Fleming and E.T.H. Wang, On n-divisible subsequences, to appear.
[2] D.R. Guichard, Two theorems on the addition of residue classes, to appear.