Hokkaido Mathematical Journal Vol. 9 (1980) p. 135-137

Note on intersections of translates of powers in finite fields

By Ronald J. EVANS

(Received July 18, 1979)

Let F be a finite field of odd order q. Fix integers t, $n\geq 2$ with $n|(q-1)$. Let R denote the set of $(q-1)/n$ nonzero n-th powers in F. For $a\in F$, let R_a denote the translate $R+a$, and for $A\subset F$, define $R_A=\bigcap_{a\in A} R_a$. In this note, we consider the following problem suggested by N. Ito. Find the fields F for which

(1) $\qquad R_A\neq R_B$ whenever $A\neq B$ and $\min(|A|, |B|)=t$.

We will give a number theoretical proof of the following theorem.

THEOREM: *Let* $Q(n, t)=2X^2+Y+2X\sqrt{X^2+Y}$, *where*

$$X=tn^t-\frac{(n+1)(n^t-1)}{2(n-1)}-\frac{n(t^2-t)}{4}-\frac{(t^2+t)}{4}$$

and

$$Y=\frac{tn^t}{n-1}+\frac{n(t^2-t)}{2}-\frac{(t^2+t)}{2}.$$

Then (1) *holds whenever* $q>Q(t, n)$.

An easily proved consequence is:

COROLLARY: *If* $q>(2t+1)^2n^{2t}$, *then* (1) *holds.*

If we were to let $t=1$, then (1) would in fact hold for all fields F. Equivalently, R is distinct from each of its translates $R+a$ $(a\neq 0)$. To see this, assume that $R=R+a$ for some $a\neq 0$. Then R is the disjoint union of sets of the form $\{x+a, x+2a, \cdots, x+pa\}$, where p is the characteristic of F. Thus p divides $|R|=(q-1)/n$, a contradiction.

In studying Hadamard matrices and block design, Ito [1, Lemma 5] showed in the case $n=t=2$, $q\equiv -1 \pmod 4$ that (1) holds for $q>7$. No better lower bound for q exists, since $R_{\{0,1\}}=R_{\{0,2\}}$ when $q=7$. Now, the only odd prime powers between 7 and $Q(2,2)\cong 14.56$ are 9, 11, 13, and inspection easily shows that (1) holds for these values of q when $n=t=2$. Thus our theorem proves Ito's result in the more general setting $q\equiv\pm 1 \pmod 4$.

For large values of n or t, $Q(n, t)$ is undoubtedly far from the best