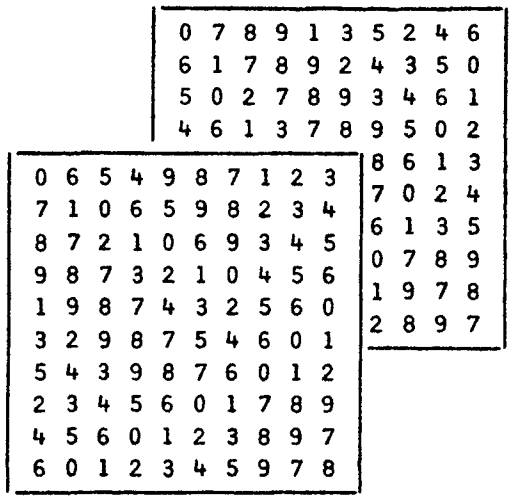
** *Sponsored by the Mathematics Research Center, USA, Madison, Wisconsin, under contract No. DA-31-124-ARO-D-462.*

* *Lecture given at the Department of Statistics, University of North Carolina at Chapel Hill, during the Combinatorial Mathematics Year.*



COMBINATORIAL
MATHEMATICS
YEAR

February 1969 - June 1970

ON SUMS OF K-TH POWERS IN A FINITE FIELD*

by

Henry B. Mann**
University of Wisconsin
Madison, Wisconsin

Department of Statistics
University of North Carolina at Chapel Hill

Institute of Statistics Mimeo Series No. 600.31

June, 1970

ON SUMS OF K-TH POWERS IN A FINITE FIELD*

Henry B. Mann**
University of Wisconsin
Madison, Wisconsin

Let p be a prime and let F be the field with $p^n = q$ elements. We shall prove the following theorem.

THEOREM: *Let $k < p$ and $q-1 \equiv 0 \pmod{k}$. Let $a_1,\ldots,a_j$ be non-0 elements of F. Let*

(1) $K_j = \{a_1x_1^k + \ldots + a_jx_j^k;\ x_\alpha \in F,\ \alpha = 1,\ldots,j\}$. *Then either* $K_j = F$ *or* $|K_j| \geq j\,\frac{q-1}{k} + 1$.

PROOF: Let G be the additive group of F. The theorem is true for $j = 1$. Assume it true for $j-1$, $j \geq 2$. By a theorem of Kneser (Theorem 1.5 of [1]), there exists a subgroup H of G such that $K_j+H = K_j$ and

(2) $|K_j| \geq |K_{j-1}+H| + |K_1+H| - |H|$.

Let H_1 be the largest subgroup of G such that $K_j+H_1 = K_j$. Let $h \in H_1$. Then for any choice of $z,x_1,\ldots,x_j \in F$ there exist $y_1,\ldots,y_j \in F$ such that

$$\sum_{a=1}^{j} a_\alpha(z^{-1}x_\alpha)^k + h = \sum_{a=1}^{j} a_\alpha y_\alpha^k.$$

Hence

---

* *Lecture given at the Department of Statistics, University of North Carolina at Chapel Hill, during the Combinatorial Mathematics Year.*

** *Sponsored by the Mathematics Research Center, USA, Madison, Wisconsin, under contract No. DA-31-124-ARO-D-462.*

$$\sum_{\alpha=1}^{j} a_\alpha x_\alpha^k + z^k h = \sum_{\alpha=1}^{j} a_\alpha (z y_\alpha)^k$$

so that $z^k h \in H$ for all z. Hence, if $|H| > 1$

$$|H| \geq |K_1| = \frac{p^n-1}{k} + 1 > p^n - 1 .$$

whence $H = G$. If $H = G$, then $K_j = G$ and we are through. If $|H| = 1$, then

$$K_j \geq (j-1)\frac{p^n-1}{k} + 1 + \frac{p^n-1}{k} = j\frac{p^n-1}{k} + 1$$

Q.E.D.

COROLLARY. Let $(k, q-1) = k_1$. If $k_1 < p$, then either $K_j = G$ or

$$|K_j| \geq j\frac{p^n-1}{k_1} + 1.$$

Let $k = k_1 k_1^*$ then $\left(\frac{q-1}{k_1}, k_1^*\right) = 1$. Thus every k_1-th power is a k_1^*-th power hence a k-th power and the corollary follows from the theorem.

In particular it follows that $K_{k_1} = G$.