PACIFIC JOURNAL OF MATHEMATICS
Vol. 82, No. 1, 1979

A COMBINATORIAL PROBLEM IN FINITE FIELDS, I

GERALD MYERSON

Given a subgroup G of the multiplicative group of a finite field, we investigate the number of representations of an arbitrary field element as a sum of elements, one from each coset of G. When G is of small index, the theory of cyclotomy yields exact results. For all other G, we obtain good estimates.

This paper formed a portion of the author's doctoral dissertation.

Let $p = 2n + 1$ be an odd prime. Consider the 2^n sums represented by the expression

$$\pm 1 \pm 2 \pm 3 \pm \cdots \pm n .$$

How do these sums distribute themselves among the residue classes modulo p? The answer is, as uniformly as possible; in fact, if we define $N(a)$ as the number of ways of choosing the signs so that $\pm 1 \pm 2 \pm \cdots \pm n \equiv a \pmod p$ then we have

THEOREM 1.

$$N(a) = \frac{1}{p}\left(2^n - \left(\frac{2}{p}\right)\right) \textit{ for } a \neq 0 \pmod p ,$$
$$N(0) = \frac{1}{p}\left(2^n - \left(\frac{2}{p}\right)\right) + \left(\frac{2}{p}\right) .$$

Here $(2/p)$ *is the Legendre symbol, that is,*

$$\left(\frac{2}{p}\right) = \begin{cases} 1 \textit{ if } 2 \textit{ is a quadratic residue } \pmod p \\ -1 \textit{ if } 2 \textit{ is not a quadratic residue } \pmod p . \end{cases}$$

Our proof of Theorem 1 will rest on the following lemmas.

LEMMA 2. *If* $ab \not\equiv 0 \pmod p$ *then* $N(a) = N(b)$.

Proof. Assume $\sum_{k=1}^{n} u_k k \equiv a \pmod p$, with $u_k \in \{1, -1\}$. Since $ab \not\equiv 0 \pmod p$ there is a c such that $ac \equiv b \pmod p$. Thus we have $\sum_{k=1}^{n} u_k ck \equiv b \pmod p$. Now for $k = 1, 2, \cdots, n$, let $ck \equiv u_k' m_k \pmod p$, where $1 \leqq m_k \leqq n$, $u_k' \in \{1, -1\}$; these conditions determine m_k and u_k' uniquely. Thus,

$$b \equiv \sum_{k=1}^{n} u_k ck \equiv \sum_{k=1}^{n} u_k u_k' m_k \equiv \sum_{k=1}^{n} u_k'' m_k \pmod p ,$$