PACIFIC JOURNAL OF MATHEMATICS
Vol. 69, No. 1, 1977

SYMMETRIES FOR SUMS OF THE LEGENDRE SYMBOL

WELLS JOHNSON AND KEVIN J. MITCHELL

Symmetries are presented for sums of the Legendre symbol (a/p) over certain subintervals of $(0, p)$. The results follow from an elementary theorem which establishes linear relations among these sums. The list of subintervals of $(0, p)$ for which the number of quadratic residues equals the number of non-residues is extended. Some simple applications to the determination of the class number of the imaginary quadratic fields $Q(\sqrt{-p})$ are also given.

1. Introduction.

If p is an odd prime, let (a/p) denote the Legendre symbol for $p \nmid a$. The sums S_r^n are defined by

$$S_r^n = \sum_{(r-1)(p/n)<a<r(p/n)} (a/p)\,, \qquad 1 \leqq r \leqq n\,.$$

Clearly $S_1^1 = \sum_{0<a<p} (a/p) = 0$ and $S_r^n = (-1/p)S_{n-r+1}^n$, which together imply that $S_1^2 = 0$ if $p \equiv 1 \pmod 4$. If $p \equiv 3 \pmod 4$, however, Dirichlet (cf. [3], page 346) showed that S_1^2 is a multiple of the class number $h(-p)$ of the imaginary quadratic field $Q(\sqrt{-p})$. Because of the symmetry given above, it has been customary to take n even, and to evaluate S_r^n only for $1 \leqq r \leqq (n/2)$.

According to Karpinski [8], the sums S_r^n were first studied by Gauss and Dedekind for certain small values of r and n. Their results were extended by Karpinski [8], Holden [6], and, more recently, by Berndt and Chowla [2]. In this paper an elementary, but general theorem is proved and shown to reduce to many of the results in the references above in special cases. Repeated applications of the theorem produce linear relations among the sums S_r^n, which, in turn, imply certain symmetries for these sums. Many of these symmetries are tabulated in the third section. Several instances where the values of S_r^n are known to vanish for certain primes p are listed as well. Finally, the relationships between the values of the sums S_r^n and the class numbers of imaginary quadratic fields are discussed.

2. Main theorem.

The following elementary theorem forms the basis for the tables of symmetries which follow. The ideas in the proof go back to Gauss and Dedekind, and the proof itself closely parallels that given by Berndt and Chowla [2].

THEOREM. *Suppose p is a prime and $p \nmid q$. Then for $1 \leqq r \leqq n$,*