Pacific Journal of Mathematics

SYMMETRIES FOR SUMS OF THE LEGENDRE SYMBOL

WELLS JOHNSON AND KEVIN J. MITCHELL

Vol. 69, No. 1 May 1977

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 $1 \leqq r \leqq n$,*

$$\left(\frac{q}{p}\right)S_r^n = \sum_{j=0}^{[(q-1)/2]} S_{jn+r}^{nq} + \left(\frac{-1}{p}\right)\sum_{j=1}^{[q/2]} S_{jn-r+1}^{nq} .$$

Proof. Write $S_r^n = \sum_{j=-[(q-1)/2]}^{[q/2]} S_r^n(j)$, where $S_r^n(j) = \sum_j (a/p)$, and where the sum $\sum_j$ runs over those integers a in the indexing set of S_r^n for which $a \equiv jp \pmod q$. Clearly each index a in S_r^n occurs exactly once in some unique $S_r^n(j)$. By a simple change of variable, if $j > 0$, then $S_r^n(j) = (-q/p)S_{jn-r+1}^{nq}$, while $S_r^n(j) = (q/p)S_{|j|n+r}^{nq}$ for $j \leqq 0$. The result follows by multiplying both sides of the equation by (q/p).

The indices $jn - r + 1$ and $jn + r$ are all $\leqq nq/2$ for $r \leqq n/2$. In the particular case that $p \equiv 3 \pmod 4$ and $n = 2$, $r = 1$, the theorem reduces to a theorem of Holden [6], as stated and proved by Berndt and Chowla [2]:

COROLLARY 1 (H. Holden). *If* $p \equiv 3 \pmod 4$ *and* $p \nmid q$, *then*

$$\sum_{j=1}^{[q/2]} S_{2j}^{2q} = 0 \qquad \text{if} \quad \left(\frac{q}{p}\right) = 1 , \quad \text{and}$$

$$\sum_{j=0}^{[(q-1)/2]} S_{2j+1}^{2q} = 0 \qquad \text{if} \quad \left(\frac{q}{p}\right) = -1 .$$

All the corollaries of [2] thus follow, including $S_1^4 = 0$ for $p \equiv 3 \pmod 8$, $S_2^4 = 0$ for $p \equiv 7 \pmod 8$, and $S_2^6 = 0$ for $p \equiv 11 \pmod{12}$. When $p \equiv 1 \pmod 4$, analogous results can be derived from the theorem. A summary of these results these appear in the tables in the next section.

If $q = 2$ and $r = 1$, then for arbitrary $n \geqq 1$, the theorem becomes

$$\left(\frac{2}{p}\right)S_1^n = \left(\frac{2}{p}\right)(S_1^{2n} + S_2^{2n}) = S_1^{2n} + \left(\frac{-1}{p}\right)S_n^{2n} .$$

Thus if $(2/p) = 1$, the following general symmetry holds:

COROLLARY 2. *For* $p \equiv \pm 1 \pmod 8$, $S_2^{2n} = (-1/p)S_n^{2n}$ *for* $n \geqq 1$.

If $(2/p) = -1$, there is merely a general linear relation among S_1^{2n}, S_2^{2n} and S_n^{2n}:

COROLLARY 3. *If* $p \equiv \pm 3 \pmod 8$, *then* $2S_1^{2n} + S_2^{2n} + (-1/p)S_n^{2n} = 0$ *for all* $n \geqq 1$.

If $n = 3r - 1$ for $r \geqq 1$, and $q = 2$ in the theorem, it follows that

$$\left(\frac{2}{p}\right)S_r^n = \left(\frac{2}{p}\right)(S_{2r-1}^{2n} + S_{2r}^{2n}) = S_r^{2n} + \left(\frac{-1}{p}\right)S_{2r}^{2n} .$$

Hence for $(2/p) = (-1/p)$, the following general symmetry holds:

COROLLARY 4. *If* $p \equiv 1, 3 \pmod 8$ *and* $n = 3r - 1$ *for* $r \geqq 1$, *then* $S_r^{2n} = (2/p)S_{2r-1}^{2n}$.

This corollary implies again the known result $S_1^4 = 0$ for $p \equiv 3 \pmod 8$, as well as $S_2^{10} = (2/p)S_3^{10}$, $S_3^{16} = (2/p)S_5^{16}$, $S_4^{22} = (2/p)S_7^{22}$, etc. for $p \equiv 1$ or $3 \pmod 8$.

For $1 \leqq i \leqq n$, the theorem implies that $(2/p)S_i^n = S_i^{2n} + (-1/p)S_{n-i+1}^{2n}$. Now if $p \equiv 1 \pmod 4$ and n is odd, $n \geqq 3$, then the sum of all of the above equations for $1 \leqq i \leqq (n-1)/2$ gives

$$\left(\frac{2}{p}\right)(S_1^2 - S_n^{2n}) = S_1^2 - S_{(n+1)/2}^{2n} .$$

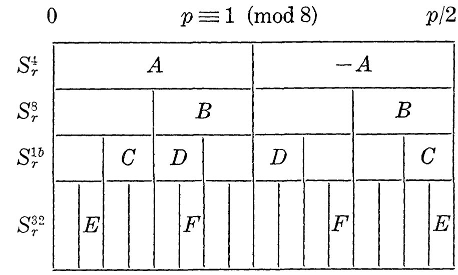
However, $S_1^2 = 0$ in this case, so that the following general symmetry holds:

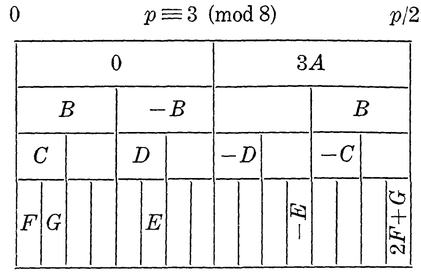
COROLLARY 5. *If* $p \equiv 1 \pmod 4$ *and* n *is odd*, $n \geqq 3$, *then* $S_n^{2n} = (2/p)S_{(n+1)/2}^{2n}$.

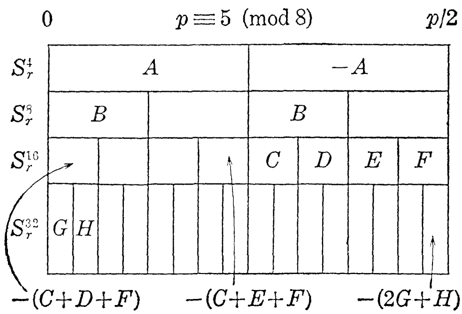
Particular cases of the general symmetries of Corollaries 2-5 appear often in the tables of the next section.

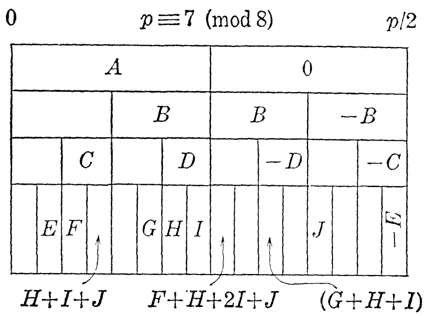
3. **Tables of symmetries.** Various choices for the values of n, r, and q in the theorem produce linear relations among the S_r^n. The tables below summarize some of the simpler symmetries for the S_r^n which follow from these linear relations. Not all known linear relations among the S_r^n are presented, and a blank merely indicates that no simple symmetry exists. These tables were first suggested to us by a computer search over several primes. Each can be proved quite easily from the theorem (although some require considerable patience). The columns are arranged so that the primes $p \equiv 3 \pmod 4$ are on the right. Also, 0 stands for the value "zero," and not the letter "oh."

The first set of tables displays symmetries which depend upon the quadratic character of -1 and $2 \pmod p$):

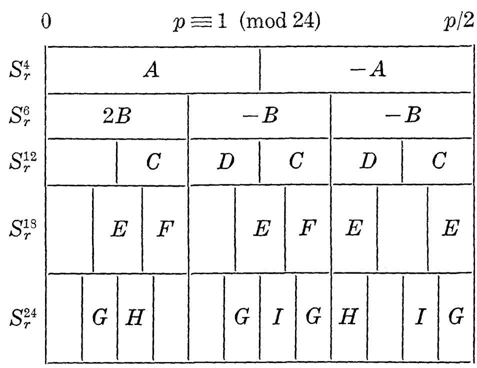


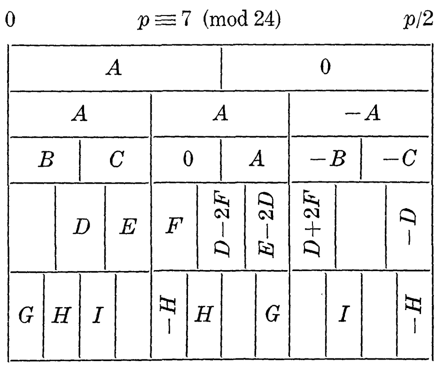


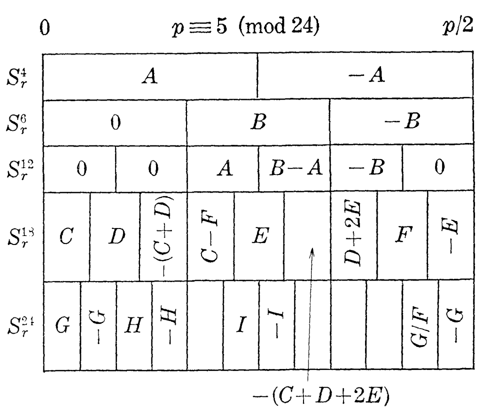


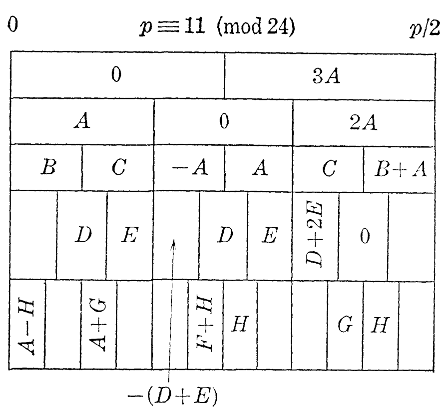


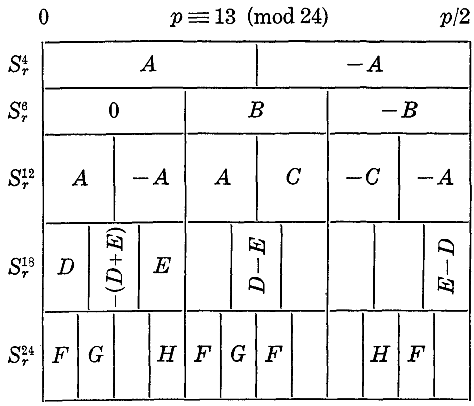
The next set of tables presents symmetries which depend upon the quadratic character of -1, 2, and 3 (mod p):

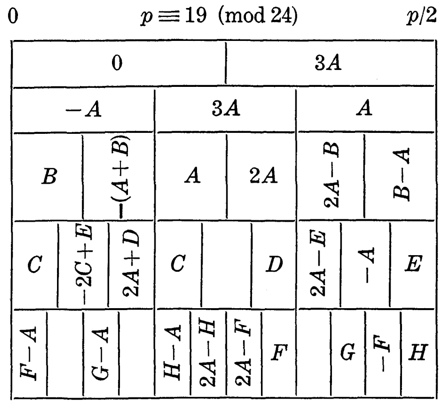


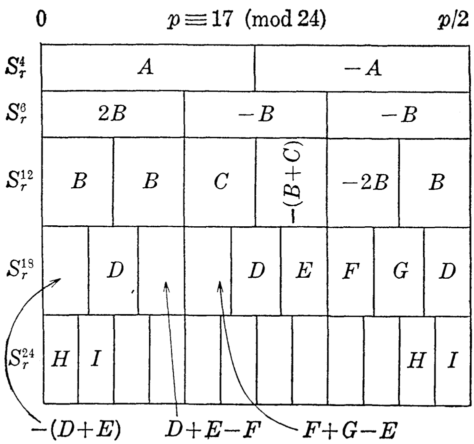


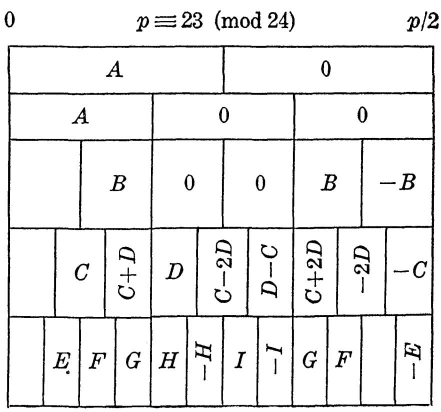












The following tables, which are presented in a slightly different format, show symmetries which depend upon the quadratic character of -1, 2, 5 and -1, 2, 7 (mod p), respectively:

0 $p/2$

$p \pmod{40}$	S_1^{10}	S_2^{10}	S_3^{10}	S_4^{10}	S_5^{10}
$p\equiv 1,9,17,33$	B	A	A	$-(B+3A)$	A
$p\equiv 3,27$	0	A	$-A$		A
$p\equiv 7,23$	$2B$	A	$A-2B$	B	$-A$
$p\equiv 11,19$	B	$-A$	A	A	$2B-A$
$p\equiv 13,21,29,37$	$A+B$	$-(A+2B)$	A	B	$-A$
$p\equiv 31,39$		A	$3A$	$-A$	$-A$

	0					$p/2$
p (mod 56)	S_1^{14}	S_2^{14}	S_3^{14}	S_4^{14}	S_5^{14}	S_6^{14}	S_7^{14}
$p \equiv 1,9,17,25,33,41$		A	B	A		B	A
$p \equiv 3,19,27$	B	A	0	$-A$		0	$2B+A$
$p \equiv 5,13,29,37,45,53$	A	B		$2A+B$	$A+B$		$-(2A+B)$
$p \equiv 11,43,51$	B	D	$-A$	$2A-D$	C	A	$A-B-C$
$p \equiv 15,23,39$	B	A	C	D	$A-B-C$	$A-(C+D)$	$-A$
$p \equiv 31,47,55$		A	$2A$	B	$\frac{1}{2}(3A+B)$	$-(A+B)$	$-A$

4. **Zero sums.** If $S_r^n = 0$, then the number of quadratic residues equals the number of nonresidues in the interval $((r-1)(p/n), r(p/n))$. Berndt and Chowla [2] listed several instances where $S_r^n = 0$ for primes $p \equiv 3 \pmod 4$. Using the theorem and the tables, this list can now be expanded somewhat:

$S_1^2 = 0$ for $p \equiv 1 \pmod 4$
$S_1^4 = 0$ for $p \equiv 3 \pmod 8$
$S_2^4 = 0$ for $p \equiv 7 \pmod 8$
$S_1^6 = 0$ for $p \equiv 5 \pmod 8$
$S_2^6 = 0$ for $p \equiv 11 \pmod{12}$
$S_1^{12} = S_2^{12} = S_6^{12} = 0$ for $p \equiv 5 \pmod{24}$
$S_3^{12} = 0$ for $p \equiv 7 \pmod{24}$
$S_8^{18} = 0$ for $p \equiv 11 \pmod{24}$
$S_3^6 = S_3^{12} = S_4^{12} = 0$ for $p \equiv 23 \pmod{24}$
$S_1^{10} = S_6^{20} = 0$ for $p \equiv 3, 27 \pmod{40}$
$S_3^{14} = S_6^{14} = 0$ for $p \equiv 3, 9, 27 \pmod{56}$
$S_{10}^{30} = 0$ for $p \equiv 11, 59 \pmod{120}$
$S_7^{30} = 0$ for $p \equiv 17, 113 \pmod{120}$.

In addition, there are other subintervals of $(0, p)$ for which the sum of Legendre symbols vanishes:

$S_2^6 + S_3^6 = 0$ for $p \equiv 5 \pmod 8$
$S_6^{24} + S_7^{24} = 0$ for $p \equiv 5 \pmod{24}$
$S_2^{12} + S_3^{12} = S_4^{12} + S_5^{12} = 0$ for $p \equiv 13 \pmod{24}$
$S_2^{12} + S_3^{12} + S_4^{12} = 0$ for $p \equiv 17 \pmod{24}$
$S_2^{18} + S_3^{18} + S_4^{18} = 0$ for $p \equiv 11 \pmod{24}$
$S_2^{10} + S_3^{10} = 0$ for $p \equiv 3, 11, 19, 27 \pmod{40}$
$S_2^{14} + S_3^{14} + S_4^{14} = 0$ for $p \equiv 3, 19, 27 \pmod{56}$
$S_4^{30} + S_5^{30} = 0$ for $p \equiv 11, 59 \pmod{120}$.

5. **Class numbers.** For $p \equiv 3 \pmod 4$ in the first two sets of tables above, it is always true (by Dirichlet) that $A = h(-p)$, and hence $A > 0$. In a preliminary version of this paper, the first-named

author [7] derived from the Voronoi congruences for the Bernoulli numbers the values of S_1^6, S_3^{12}, S_4^{12}, S_3^6 in terms of $h(-p)$ for primes $p \equiv 3 \pmod 4$. The results are originally due to Holden [6], who gave a more complicated proof depending upon class number formulas for binary quadratic forms. Apostol [1] used the properties of the Bernoulli polynomials to obtain some of the same results.

It follows that for $p \equiv 3 \pmod 4$, $S_1^6 = \pm h(-p)$, the minus sign holding only for $p \equiv 19 \pmod{24}$. Hence for $p \equiv 3 \pmod 4$, the interval $(0, p/6)$ always contains more residues than non-residues unless $p \equiv 19 \pmod{24}$, when the opposite is true. Tables for the class numbers $h(-p)$ for $p \equiv 3 \pmod 4$ have been compiled for $p < 166{,}807$ by Ordman [11] and Newman [10] using the theory of reduced quadratic forms. Other techniques were employed by Duport and Dussaud [4, 5]. We have computed tables of $h(-p)$ for $p \equiv 3 \pmod 4$, $p < 200{,}000$, by simply evaluating S_1^6 directly. These results agree with those reported earlier.

This theory can also be used to obtain in an elementary way some rough upper bounds for the values of $h(-p)$ when $p \equiv 3 \pmod 4$. If $p \equiv 19 \pmod{24}$, for example, it follows from the fact that $S_4^{12} = 2h(-p)$ that $h(-p) \leqq (p+5)/24$. Since $h(-p)$ is known to be odd, it follows that $h(-p) = 1$ for $p = 19$ and $p = 43$ without any computation whatsoever. Similarly, if $p \equiv 43$ or $67 \pmod{120}$, the tables imply that $2h(-p) = S_{10}^{30}$. Hence $h(-p) \leqq (p+17)/60$ if $p \equiv 43 \pmod{120}$ and $h(-p) \leqq (p-7)/60$ if $p \equiv 67 \pmod{120}$. In particular, $h(-43) = h(-67) = 1$, again with absolutely no computation needed. It should be noted that there are better bounds for $h(-p)$, especially for large p, namely the bound $(1/3)\sqrt{p}\log p$ obtained by Slavutskiĭ [12] using analytic methods.

Karpinski [8] showed that many of the values $A, B, C, \cdots$ in the tables can be expressed as linear combinations of the class numbers $h(-kp)$, $k = 1, 2, 3, \cdots$. It follows from his resuts that, among other things, there are always more residues than non-residues in the intervals $(p/8, p/4)$ and $(p/4, 3p/8)$ for $p \equiv 7 \pmod 8$. For more results along these lines, the reader is referred to Lerch [9], and the unpublished work of B. Berndt and Y. Yamamoto.

References

1. T. M. Apostol, *Quadratic residues and Bernoulli numbers*, Delta (Waukesha), **1** (1968/70), 21–31.

2. B. C. Berndt and S. Chowla, *Zero sums of the Legendre symbol*, Nordisk Math. Tidskr., **22** (1974), 5–8.

3. Z. I. Borevich and I. R. Shafarevich, *Number Theory*, "Nauka," Moscow, (1964); English transl., Pure and Appl. Math., **20**, Academic Press, New York, (1966).

4. J.-P. Duport and R. Dussaud, *Sur la détermination en machine des nombres*

premiers p de la forme $p = 4n + 3$ *à séquence binaire unique et du nombre h de classes d'idéaux du corps* $Q(\sqrt{(-p)})$, C. R. Acad. Sci. Paris Sér A-B, **269** (1969), A923–A925.

5. ———, *Sur la détermination en machine du nombre h de classes d'idéaux de l'anneau des entiers du corps* $Q(\sqrt{-p})$, C. R. Acad. Sci. Paris Sér A-B, **270** (1970), A129–A132.

6. H. Holden, *On various expressions for h, the number of properly primitive classes for a determinant* $-p$, *where p is of the form* $4n + 3$ *and is a prime or the product of primes* (Second paper), Messenger of Math., **35** (1906), 102–110.

7. W. Johnson, *Class numbers and the distribution of quadratic residues*, Notices Amer. Math. Soc., **22** (1975), A66.

8. L. Karpinski, *Über die Verteilung der quadratischen Reste*, J. Reine Angew. Math., **127** (1904), 1–19.

9. M. Lerch, *Essais sur le calcul du nombre des classes de formes quadratiques binaires aux coefficients entiers*, Acta Math., **29** (1905), 333–424.

10. M. Newman, *Table of the class number* $h(-p)$ *for p prime*, $p \equiv 3 \pmod 4$, $101987 \leqq p \leqq 166807$. UMT 50, Math. Comp., **23** (1969), 683.

11. E. T. Ordman, *Tables of the class numbers for negative prime discriminants*, UMT 29, Math. Comp., **23** (1969), 458.

12. I. S. Slavutskiĭ, *Upper bounds and numerical calculation of the number of ideal classes of real quadratic fields*, Amer. Math. Soc. Trans., (2) **82** (1969), 67–71.

Received August 5, 1976

BOWDOIN COLLEGE
AND
BROWN UNIVERSITY

Printed in Japan by International Academic Printing Co., Ltd., Tokyo, Japan

Pacific Journal of Mathematics

Vol. 69, No. 1 May, 1977