ON THE SUM $\sum_{a=1}^{p-1}\left(\frac{a}{p}\right)a$

M. G. Monzingo
Southern Methodist University, Dallas, TX 75275
(Submitted March 1988)

In this note, the sum

$\sum_{a=1}^{p-1}\left(\frac{a}{p}\right)a$, where p is an odd prime and $\left(\frac{a}{p}\right)$ is the Legendre symbol,

will be written in an expanded form. Special cases of this form yield the results that, for $p \equiv 7 \pmod 8$,

$$\sum_{a=1}^{(p-1)/2}\left(\frac{a}{p}\right)a = 0,$$

and for $p \equiv 3 \pmod 8$,

$$\sum_{a=1}^{(p-1)/2}\left(\frac{a}{p}\right) \text{ is an odd multiple of 3.}$$

This latter result implies that for such primes the difference in the number of quadratic residues and quadratic nonresidues in the first half of the interval $1 \le a \le p - 1$ must be an odd multiple of three.

Let p be an odd prime, and let $\left(\frac{a}{p}\right)$ denote the Legendre symbol.

Theorem 1: Let q, $1 \le q \le p - 1$, be a divisor of $p - 1$ and k such that $p - 1 = kq$; then,

$$S = \sum_{a=1}^{p-1}\left(\frac{a}{p}\right)a$$

satisfies

$$(*) \qquad \left\{\left(\frac{q}{p}\right)q - 1\right\}S = p\left\{(q-1)\sum_{t=0}^{k-1}\left(\frac{tq+1}{p}\right) + (q-2)\sum_{t=0}^{k-1}\left(\frac{tq+2}{p}\right) + \cdots + \sum_{t=0}^{k-1}\left(\frac{tq+(q-1)}{p}\right)\right\}.$$

Proof: $\left(\frac{q}{p}\right)qS = \sum_{a=1}^{p-1}\left(\frac{qa}{p}\right)qa.$

This sum can be expanded as follows:

$$(1) \qquad \sum_{s=1}^{q}\left\{\sum_{a=(s-1)k+1}^{sk}\left(\frac{qa}{p}\right)qa\right\} = \sum_{s=1}^{q}\left\{\sum_{t=1}^{k}\left(\frac{((s-1)k+t)q}{p}\right)((s-1)k+t)q\right\}.$$

Next, $((s-1)k + t)q = (s-1)kq + tq$
$= (s-1)(p-1) + tq$
$= (s-1)p + tq - (s-1)$
$= (s-1)p + (t-1)q + (q - (s-1)).$

Substitution into the right-hand side of (1) and noting that $(s - 1)p \equiv 0 \pmod{p}$ yields

$$(2)\qquad \sum_{s=1}^{q}\left\{\sum_{t=1}^{k}\left(\frac{(t-1)q + q - (s-1)}{p}\right)\{(s-1)p + (t-1)q + (q - (s-1)\}\right\}.$$

In (2), letting $v = q - (s - 1)$, splitting the sum, and summing on v yields

$$(3)\qquad \sum_{v=1}^{q}\left\{\sum_{t=1}^{k}\left(\frac{(t-1)q + v}{p}\right)((t-1)q + v)\right\} + \sum_{v=1}^{q}\left\{\sum_{t=1}^{k}\left(\frac{(t-1)q + v}{p}\right)(q - v)p\right\}.$$

Note that the first sum in (3) is S. In the second sum, replace $t - 1$ with t; then, the second sum can be written

$$p\sum_{v=1}^{q-1}\left\{(q - v)\sum_{t=0}^{k-1}\left(\frac{tq + v}{p}\right)\right\}.$$

Putting the pieces together, we have

$$\left(\frac{q}{p}\right)qS = S + p\sum_{v=1}^{q-1}\left\{(q - v)\sum_{t=0}^{k-1}\left(\frac{tq + v}{p}\right)\right\},$$

from which the conclusion follows.

Corollary 1: If q, $1 < q \le p - 1$, is a quadratic residue modulo p, then $q - 1$ divides

$$(q - 2)\sum_{t=0}^{k-1}\left(\frac{tq + 2}{p}\right) + \cdots + \sum_{t=0}^{k-1}\left(\frac{tq + (q - 1)}{p}\right).$$

And, if q, $1 \le q < p - 1$, is a quadratic nonresidue modulo p, then $q + 1$ divides

$$(q - 1)\sum_{t=0}^{k-1}\left(\frac{tq + 1}{p}\right) + \cdots + \sum_{t=0}^{k-1}\left(\frac{tq + (q - 1)}{p}\right).$$

Proof: In the second case, $(q/p) = -1$, and so $q + 1$ divides the left side of (*) and, consequently, the right side of (*). The conclusion follows by noting that $(q + 1, p) = 1$. The first case follows in a similar fashion with $q - 1$ replacing $q + 1$, and by noting that the first sum on the right side of (*) is multiplied by $q - 1$.

Example: Let $p = 17$ and $q = 4$; then $k = 4$. Since 4 is a quadratic residue, the conclusion from Corollary 1 is that 3 divides

$$2\sum_{t=0}^{3}\left(\frac{4t + 2}{17}\right) + \sum_{t=0}^{3}\left(\frac{4t + 3}{17}\right).$$

Corollary 2: If $p \equiv 7 \pmod{8}$, then $S = -p\sum_{a=1}^{(p-1)/2}\left(\frac{a}{p}\right)$.

Proof: In Theorem 1, let $q = 2$ and, hence, 2 is a quadratic residue. Thus,

$$S = p\sum_{t=0}^{k-1}\left(\frac{2t + 1}{p}\right);$$

that is,

$$S = p \sum_{\substack{a=1 \\ a \text{ odd}}}^{p-1} \left(\frac{a}{p}\right).$$

The desired conclusion is obtained from the following:

$$\sum_{\substack{a=1 \\ a \text{ odd}}}^{p-1} \left(\frac{a}{p}\right) = -\sum_{\substack{a=2 \\ a \text{ even}}}^{p-1} \left(\frac{a}{p}\right) = -\sum_{a=1}^{(p-1)/2} \left(\frac{2a}{p}\right) = -\left(\frac{2}{p}\right)\sum_{a=1}^{(p-1)/2} \left(\frac{a}{p}\right) = -\sum_{a=1}^{(p-1)/2} \left(\frac{a}{p}\right).$$

Note that the conclusion in Corollary 2 also holds with $p \equiv 1 \pmod 8$, but trivially; both S and the sum are zero.

Theorem 2: If $p \equiv 3 \pmod 8$, $p > 3$, then 3 divides $\sum_{a=1}^{(p-1)/2} \left(\frac{a}{p}\right)$.

Proof: Let $q = 2$; then q is a quadratic nonresidue, and so Corollary 1 implies that 3 divides

$$\sum_{t=0}^{k-1} \left(\frac{2t+1}{p}\right),$$

that is,

$$\sum_{\substack{a=1 \\ a \text{ odd}}}^{p-1} \left(\frac{a}{p}\right).$$

Now, by an argument similar to that used in the proof of Corollary 2; the conclusion follows.

Example: Let $p = 11$; then the quadratic residues are 1, 3, 4, 5, and 9, while the quadratic nonresidues are 2, 6, 7, 8, and 10. Hence, the sum in Theorem 2 is

$$\left(\frac{1}{11}\right) + \left(\frac{2}{11}\right) + \left(\frac{3}{11}\right) + \left(\frac{4}{11}\right) + \left(\frac{5}{11}\right) = 1 - 1 + 1 + 1 + 1 = 3.$$

Note that the conclusion in Theorem 2 also holds for $p \equiv 5 \pmod 8$, but trivially; the sum in question is zero.

Also note that in Theorem 2 with $p \equiv 3 \pmod 8$, $(p-1)/2$ is odd. Therefore, the sum in Theorem 2 has an odd number of terms, each one equal to ± 1. It follows, then, that the number of quadratic residues and quadratic nonresidues are opposite in parity. Hence, from Theorem 2, the difference in the numbers of quadratic residues and quadratic nonresidues in the interval from 1 to $(p-1)/2$ must be an odd multiple of three.

Theorem 3: If $p \equiv 7 \pmod 8$, then $\sum_{a=1}^{(p-1)/2} \left(\frac{a}{p}\right)a = 0$.

Proof: $$S = \sum_{a=1}^{p-1} \left(\frac{a}{p}\right)a = \sum_{a=1}^{(p-1)/2} \left(\frac{a}{p}\right)a + \sum_{b=(p+1)/2}^{p-1} \left(\frac{b}{p}\right)b.$$

In the last sum, let $b = p - a$; then this sum can be rewritten as

$$\sum_{a=1}^{(p-1)/2} \left(\frac{p-a}{p}\right)(p-a) = \sum_{a=1}^{(p-1)/2} \left(\frac{a}{p}\right)a - p\sum_{a=1}^{(p-1)/2} \left(\frac{a}{p}\right),$$

since $\left(\frac{p-a}{p}\right) = -\left(\frac{a}{p}\right)$. Hence,

$$S = 2\sum_{a=1}^{(p-1)/2} \left(\frac{a}{p}\right)a - p\sum_{a=1}^{(p-1)/2} \left(\frac{a}{p}\right).$$

[Note that this equation also holds for $p \equiv 3 \pmod 8$ since, in this case, it is also true that

$$\left(\frac{p-a}{p}\right) = -\left(\frac{a}{p}\right).]$$

Now, from Corollary 2,

$$S = -p\sum_{a=1}^{(p-1)/2}\left(\frac{a}{p}\right),$$

and so

$$\sum_{a=1}^{(p-1)/2}\left(\frac{a}{p}\right)a = 0.$$

*****

REFEREES Continued from page 2

SCHINZEL, A.
Polish Academy of Science
SHANNON, A.G.
University of Technology-Sydney
SHIUE, P.J.
University of Nevada
SIVARAMAKRISHNAN, R.
University of Calicut
STEWART, C.L.
University of Waterloo
SUBBARAO, M.V.
University of Alberta
SUBRAMANIAN, P.R.
University of Madras
TOGNETTI, K.
University of Wollongong
TURNER, J.C.
University of Waikato
TURNER, S.J.
Babson College
VELEZ, W.
University of Arizona
WADDILL, M.E.
Wake Forest University
WAGSTAFF, S.S.
Purdue University
WATERHOUSE, W.C.
Pennsylvania State University
WEST, D.B.
Princeton, New Jersey
WIMP, J.
Drexel University
YOKOTA, H.
Hiroshima Institute of Technology
YOUNG, A.
Loyola College