A SUM CONNECTED WITH QUADRATIC RESIDUES

L. CARLITZ

1. Let p be a prime >2 and m an arbitrary positive integer; define

$$S_m = \sum_{r=0}^{m} (-1)^{m-r} \left(\frac{r}{p}\right) \binom{m}{r}, \tag{1.1}$$

where (r/p) is the Legendre symbol. We consider the problem of finding the highest power of p dividing S_m. A little more generally, if we put

$$S_m(a) = \sum_{r=0}^{m} (-1)^{m-r} \left(\frac{r+a}{p}\right) \binom{m}{r}, \tag{1.2}$$

where a is an arbitrary integer, we seek the highest power of p dividing $S_m(a)$. Clearly $S_m = S_m(0)$, and $S_m(a) = S_m(b)$ when $a \equiv b \pmod{p}$.

In the first place it follows from (1.2) that $S_m(a)$ satisfies the recurrence

$$S_{m+1}(a) = \Delta S_m(a) = S_m(a+1) - S_m(a), \tag{1.3}$$

where it is understood that Δ applies only to a. Repeated application of (1.3) gives

$$S_{m+r}(a) = \Delta^r S_m(a) = \sum_{s=0}^{r} (-1)^{r-s} \binom{r}{s} S_m(a+s). \tag{1.4}$$

We may also write (1.3) in the form

$$S_m(a+1) = S_{m+1}(a) + S_m(a), \tag{1.5}$$

which implies

$$S_m(a+r) = \sum_{s=0}^{r} \binom{r}{s} S_{m+s}(a). \tag{1.6}$$

In particular for $r=p$, (1.6) becomes

$$\sum_{s=1}^{p} \binom{p}{s} S_{m+s}(a) = 0. \tag{1.7}$$

2. It follows from

Received August 8, 1955.

$$\left(\frac{r}{p}\right) \equiv r^{(p-1)/2} \pmod{p}$$

that

$$\left(\frac{r}{p}\right) \equiv r^{p^n(p-1)/2} \pmod{p^{n+1}}$$

for arbitrary $n \geqq 0$. Consequently (1.2) becomes

$$S_m(a) = \sum_{r=0}^{m} (-1)^{m-r} \binom{m}{r} (r+a)^{p^n(p-1)/2} \pmod{p^{n+1}}. \tag{2.1}$$

We recall that for arbitrary positive k

$$\frac{1}{m!} \sum_{r=0}^{m} (-1)^{m-r} \binom{m}{r} (r+a)^k \tag{2.2}$$

is an integer (for $a = 0$, (2.2) is a Stirling number of the second kind). If now $E_p(m)$ denotes the highest power of p dividing $m!$, it is clear from (2.1) that

$$S_m(a) \equiv 0 \pmod{p^{E_p(m)}}. \tag{2.3}$$

In view of the definition of $E_p(m)$, (2.3) may be restated in the following way: $S_m(a)/m!$ is integral (mod p).

3. It may be possible to improve (2.3). We make use of the following familiar formula for Gauss sums (see for example [2, Th. 215]):

$$\sum_{s=1}^{p-1} \left(\frac{s}{p}\right) \varepsilon^{rs} = \left(\frac{r}{p}\right) G_p \qquad (\varepsilon = e^{2\pi i/p}), \tag{3.1}$$

where

$$G_p = \sum_{s=1}^{p-1} \left(\frac{s}{p}\right) \varepsilon^s = \begin{cases} p^{1/2} & (p \equiv 1 \pmod{4}) \\ ip^{1/2} & (p \equiv 3 \pmod{4}). \end{cases} \tag{3.2}$$

Note that (3.1) is valid for all r. It follows that

$$G_p S_m(a) = \sum_{r=0}^{m} (-1)^{m-r} \sum_{s=1}^{p-1} \left(\frac{s}{p}\right) \varepsilon^{(r+a)s}$$

so that

$$G_p S_m(a) = \sum_{s=1}^{p-1} \left(\frac{s}{p}\right) \varepsilon^{as} (\varepsilon^s - 1)^m. \tag{3.3}$$

Clearly (3.3) implies

$$G_p S_m(a) \equiv 0 \pmod{(\varepsilon - 1)^m}, \tag{3.4}$$

where we are now operating in the cyclotomic field $k(\varepsilon)$. Since in this field we have

$$(3.5)\qquad (p) = (\varepsilon - 1)^{p-1},$$

(3.2) and (3.4) yield

$$(3.6)\qquad S_m(a) \equiv 0 \pmod{(\varepsilon - 1)^{m-(p-1)/2}}.$$

Define the integer h by means of

$$(3.7)\qquad (h-1)(p-1) < m - \frac{1}{2}(p-1) \leqq h(p-1).$$

Since $S_m(a)$ is a rational integer, it follows from (3.6) and (3.7) that

$$(3.8)\qquad S_m(a) \equiv 0 \pmod{p^h},$$

which again is valid for all a.

We recall that

$$E_p(m) = \left[\frac{m}{p}\right] + \left[\frac{m}{p^2}\right] + \ldots < \frac{m}{p-1};$$

hence using (3.7) we may verify that $h \geqq E_p(m)$ so that (3.8) implies (2.3). In particular for

$$\frac{1}{2}(p-1) < m \leqq p-1,$$

$h = 1$ while $E_p(m) = 0$. The difference $h - E_p(m)$ may indeed be arbitrarily large; for example if

$$p^k - 1 - \frac{1}{2}(p-1) < m \leqq p^k - 1,$$

we find that

$$E_p(m) = \frac{p^k - 1}{p-1} - k, \quad h = \frac{p^k - 1}{p-1},$$

so that $h - E_p(m) = k$.

4. Returning to (3.3) we consider the particular case

$$(4.1)\qquad m - \frac{1}{2}(p-1) = h(p-1);$$

for such m the value of h computed by means of (3.7) will coincide with the value of h in (4.1). Now (3.3) implies

$$(4.2)\qquad (\varepsilon-1)^{-m}G_p S_m(a)=\sum_{s=1}^{p-1}\left(\frac{s}{p}\right)\varepsilon^{as}\left(\frac{\varepsilon^s-1}{\varepsilon-1}\right)^m.$$

We shall compute the residue of the right member (mod $\varepsilon-1$). Since

$$\varepsilon^{as}\equiv 1,\quad \frac{\varepsilon^s-1}{\varepsilon-1}\equiv s,$$

it is evident that (4.2) becomes

$$(4.3)\qquad \begin{aligned}(\varepsilon-1)^{-m}G_p S_m(a)&\equiv\sum_{s=1}^{p-1}\left(\frac{s}{p}\right)s^m\equiv\sum_{s=1}^{p-1}\left(\frac{s}{p}\right)s^{(p-1)/2}\\ &=\sum_{s=1}^{p-1}s^{p-1}\equiv -1 \pmod{\varepsilon-1}.\end{aligned}$$

Next we replace (3.5) by the more exact statement

$$(4.4)\qquad p\equiv(\varepsilon-1)^{p-1}\pmod{(\varepsilon-1)^p},$$

which is easily proved. Also if $p=2k+1$, the identity (see for example [3, *p*. 176])

$$\sum_0^{p-1}\varepsilon^{s(s+1)}=\prod_1^k(1-\varepsilon^{-2(2s-1)})$$

implies

$$(4.5)\qquad G_p=\sum_0^{p-1}\varepsilon^{s^2}\equiv(-1)^k(\varepsilon-1)^k k!\pmod{(\varepsilon-1)^{k+1}}.$$

Using (4.4) and (4.5), (4.3) becomes

$$(4.6)\qquad p^{-h}S_m(a)\equiv -(-1)^k/k!\pmod{p}.$$

Hence for m satisfying (4.1) the exponent h furnishes the highest power of p dividing $S_m(a)$ and the residue of $p^{-h}S_m(a)$ satisfies (4.6). Note also that the right member of (4.6) is independent of a.

5. When m does not satisfy (4.1) it is more difficult to simplify the right member of (4.2). Let

$$(5.1)\qquad (h-1)(p-1)<m-\frac{1}{2}(p-1)<h(p-1);$$

it is convenient to put

$$m+l=h(p-1)+\frac{1}{2}(p-1) \quad (1 \leqq l \leqq p-2). \tag{5.2}$$

Thus it is clear from (3.8) that the right member of (4.2) is divisible by $(\varepsilon-1)^l$ and we have

$$(\varepsilon-1)^{-h(p-1)}G_pS_m(a) \equiv (\varepsilon-1)^{-l}\sum_{s=1}^{p-1}\left(\frac{s}{p}\right)\varepsilon^{as}\left(\frac{\varepsilon^s-1}{\varepsilon-1}\right)^m \pmod{\varepsilon-1}. \tag{5.3}$$

We accordingly seek the residue of

$$T_m(a)=\sum_{s=1}^{p-1}\left(\frac{s}{p}\right)\varepsilon^{as}\left(\frac{\varepsilon^s-1}{\varepsilon-1}\right)^m \pmod{(\varepsilon-1)^{l+1}}. \tag{5.4}$$

Clearly we may put

$$T_m(a) \equiv A_0+A_1(\varepsilon-1)+\ldots+A_l(\varepsilon-1)^l,$$

where the A's are rational integers; it follows from (3.8) that $A_0 \equiv \ldots \equiv A_{l-1} \equiv 0 \pmod p$ and may therefore be ignored. Thus in the expansion of the right member of (5.4) we need only retain the term in $(\varepsilon-1)^l$. Now we have

$$\left(\frac{(1+x)^s-1}{x}\right)^m = x^{-m}\sum_{r=0}^{m}(-1)^{m-r}\binom{m}{r}(1+s)^{rs},$$

so that

$$\begin{aligned}(1+x)^{as}\left(\frac{(1+x)^s-1}{x}\right)^m &= x^{-m}\sum_{r=0}^{m}(-1)^{m-r}\binom{m}{r}(1+x)^{(a+r)s} \\ &= \sum_{r=0}^{m}(-1)^{m-r}\binom{m}{r}\sum_{t=0}^{(a+r)s}\binom{(a+r)s}{t}x^{t-m}.\end{aligned}$$

Hence by the above remark we get

$$(\varepsilon-1)^{-l}T_m(a) \equiv \sum_{s=1}^{p-1}\left(\frac{s}{p}\right)\sum_{r=0}^{m}(-1)^{m-r}\binom{m}{r}\binom{(a+r)s}{m+l} \pmod{\varepsilon-1}. \tag{5.5}$$

To further simplify this result note that the inner sum in the right member is the m-th difference of a polynomial in a of degree $m+l$; thus only terms of degree $\geqq m$ make any contribution. Now for a term of degree t, where $m \leqq t \leqq m+l$, we get

$$\sum_{s=1}^{p-1}\left(\frac{s}{p}\right)s^t \equiv \sum_{s=1}^{p-1}s^{(p-1)/2+t},$$

and in view of (5.2) this sum vanishes $\pmod p$ unless $t=m+l$ in which case the sum $\equiv -1$. Thus (5.5) becomes

$$(5.6)\quad (\varepsilon-1)^{-l}T_m(a) \equiv -\frac{1}{(m+l)!}\sum_{r=0}^{m}(-1)^{m-r}\binom{m}{r}(a+r)^{m+l} \pmod{\varepsilon-1}.$$

Finally as in the proof of (4.6), we may simplify the left member of (5.3). Thus using (5.4) and (5.6) we obtain

$$(5.7)\quad p^{-h}S_m(a) \equiv -\frac{(-1)^k}{k!}\,\frac{1}{(m+l)!}\sum_{r=0}^{m}(-1)^{m-r}\binom{m}{r}(a+r)^{m+l} \pmod{p},$$

where $p=2k+1$ and h and l are defined by (5.1) and (5.2). When m satisfies (4.1) it is easily verified that (5.7) reduces to (4.6). Thus (5.7) holds for all m. We may therefore state the following

THEOREM. *Let $p=2k+1$ be a prime, a an arbitrary integer and m a positive integer; define h and l by means of*

$$(h-1)(p-1) < m-\frac{1}{2}(p-1) \leqq h(p-1), \quad m+l=h(p-1)+\frac{1}{2}(p-1).$$

Then $S_m(a)$ satisfies (5.7). *In particular when $l=0$,* (5.7) *reduces to*

$$(5.8)\qquad p^{-h}S_m(a) \equiv -\frac{(-1)^k}{k!} \pmod{p} \quad (l=0).$$

Comparison of (5.7) with (2.1) leads to a rather curious congruence.

It should be remarked that the right member of (5.7) may be divisible by p; thus we have not in all cases determined the highest power of p dividing $S_m(a)$. However when $m=h(p-1)+(p-1)/2$, h is the correct exponent.

For small values of l, the right member of (5.7) can be reduced further using known properties of Stirling numbers of the second kind (see for example [1, §58] and [4]):

$$A_{m+l,m} = \frac{1}{m!}\sum_{r=0}^{m}(-1)^{m-r}\binom{m}{r}r^{m+l}.$$

We have in particular

$$A_{m+1,m} = \frac{1}{2}m(m+1),$$

$$A_{m+2,m} = \frac{1}{24}m(m+1)(m+2)(3m+1),$$

$$A_{m+3,m} = \frac{1}{48}m^2(m+1)^2(m+2)(m+3).$$

On the other hand it is clear that (5.7) can be rewritten as

$$(5.9)\qquad p^{-h}S_m(a) = -\frac{(-1)^k}{k!}\frac{1}{(m+1)\dots(m+l)}\sum_{t=m}^{m+l}\binom{m+l}{t}a^{m+l-t}A_{m+l,t} \pmod{p}.$$

Thus for example, when $a=0$, (5.9) yields

$$p^{-h}S_m \equiv \begin{cases} -\dfrac{(-1)^k}{k!}\dfrac{m}{2} & (l=1) \\ -\dfrac{(-1)^k}{k!}\dfrac{m(3m+1)}{24} & (l=2) \\ -\dfrac{(-1)^k}{k!}\dfrac{m^2(m+1)}{48} & (l=3). \end{cases}$$

6. When $p=3$ it is easily proved that

$$(6.1)\qquad S_m(a) = \begin{cases} (-3)^{3/2}\left(\dfrac{2m+a}{3}\right) & (m \text{ even}) \\ (-3)^{(m-1)/2}c & (m \text{ odd}), \end{cases}$$

where $c=-2$ for $3/m$, $c=+1$ for $3+m$. It is easily verified that (6.1) is in agreement with the general results above.

In conclusion a word may be said about the sum

$$(6.2)\qquad R_m(a) = \sum_{r=0}^{m}\left(\frac{r+a}{p}\right)\binom{m}{r}.$$

If $m = m_1p + m_0$, $r = r_1p + r_0$, $0 \leqq m_0 < p$, $0 \leqq r_0 < p$,

then
$$\binom{m}{r} \equiv \binom{m_1}{r_1}\binom{m_0}{r_0} \pmod{p},$$

so that (6.2) becomes

$$R_m(a) \equiv \sum_r \left(\frac{r_0+a}{p}\right)\binom{m_1}{r_1}\binom{m_0}{r_0} \equiv 2^{m_1}R_{m_0}(a). \pmod{p}.$$

Thus to find the residue (mod p) of $R_m(a)$ it suffices to consider the case $0 \leqq m < p$. However it is not evident how to find the residue in this case.

References

[1] C. Jordan, Calculus of finite differences, second edition, New York, 1947.

[2] E. Landau, Vorlesungen über Zahlentheorie, vol. 1, Leipzig, 1927.

[3] T. Nagell, Introduction to number theory, New York, 1951.

[4] M. Ward, The representation of Stirling's numbers and Stirling's polynomials as sums of factorials, American Journal of Mathematics, **56** (1934), pp. 87–95.

Duke University