SOME SUMS CONNECTED WITH QUADRATIC RESIDUES

L. CARLITZ

1. A well known theorem of Dirichlet asserts that if p is a prime $\equiv 3 \pmod 4$, then

$$\sum_{r=1}^{(p-1)/2}\left(\frac{r}{p}\right) > 0, \tag{1.1}$$

that is, among the integers $1, 2, \cdots, (p-1)/2$, there are more quadratic residues of p than nonresidues. A concise proof of this theorem has recently been given by Moser [2]; Whiteman [4] has proved several closely related results.

In the present note we indicate a generalization of (1.1) and in particular that for $p \equiv 3 \pmod 4$,

$$\begin{gathered}(-1)^{k+1}\sum_{h=1}^{(p-1)/2}\left(\frac{h}{p}\right)B_{2k+1}\left(\frac{h}{p}\right) \quad \text{and} \\ (-1)^{k}\sum_{h=1}^{(p-1)/2}\left(\frac{h}{p}\right)E_{2k}\left(\frac{2h}{p}\right)\end{gathered} \tag{1.2}$$

are positive for $k \geqq 0$, while for $p \equiv 1 \pmod 4$,

$$\begin{gathered}(-1)^{k+1}\sum_{h=1}^{(p-1)/2}\left(\frac{h}{p}\right)B_{2k}\left(\frac{h}{p}\right) \quad \text{and} \\ (-1)^{k}\sum_{h=1}^{(p-1)/2}\left(\frac{h}{p}\right)E_{2k-1}\left(\frac{2h}{p}\right)\end{gathered} \tag{1.3}$$

are positive for $k \geqq 1$. In (1.2) and (1.3), $B_k(x)$ and $E_k(x)$ denote the Bernoulli and Euler polynomials, respectively, of degree k.

2. In the familiar summation [1, p. 153]

$$\sum_{r=1}^{p-1}\left(\frac{r}{p}\right)e^{2\pi irn/p} = \begin{cases}\left(\dfrac{n}{p}\right)p^{1/2} & (p \equiv 1 \pmod 4), \\ i\left(\dfrac{n}{p}\right)p^{1/2} & (p \equiv 3 \pmod 4),\end{cases} \tag{2.1}$$

which is valid for all n, we first take $p \equiv 3 \pmod 4$. Then (2.1) becomes

Presented to the Society, September 5, 1952; received by the editors May 12, 1952.

$$(2.2) \qquad \sum_{r=1}^{m}\left(\frac{r}{p}\right)\sin\frac{2\pi rn}{p}=\frac{1}{2}\left(\frac{n}{p}\right)p^{1/2} \qquad (p=2m+1).$$

If we multiply both sides of (2.2) by a_n and sum over n, then

$$(2.3) \qquad \sum_{r=1}^{m}\left(\frac{r}{p}\right)f\left(\frac{2r}{p}\right)=\frac{1}{2}p^{1/2}\sum_{n=1}^{\infty}\left(\frac{n}{p}\right)a_n,$$

where

$$f(x)=\sum_{n=1}^{\infty}a_n\sin n\pi x$$

If we assume a_n real and $\sum a_n$ absolutely convergent, then we may be able to infer from (2.3) that the sum in the left member is positive. For example let $a_{rs}=a_ra_s$ for arbitrary integers r, s and let $|a_n|<1$ for all n, then

$$\sum_{n=1}^{\infty}\left(\frac{n}{p}\right)a_n=\prod_{q}\left\{1-\left(\frac{q}{p}\right)a_q\right\}^{-1}>0;$$

the product extends over all primes q. In some instances the assumption of absolute convergence can be weakened.

In particular if we make use of the expansion [3, p. 65]

$$B_{2k+1}(x)=(-1)^{k+1}\frac{2(2k+1)!}{(2\pi)^{2k+1}}\sum_{n=1}^{\infty}\frac{\sin 2n\pi x}{n^{2k+1}},$$

then (2.3) becomes

$$(2.4) \qquad \begin{aligned}(-1)^{k+1}\sum_{h=1}^{m}\left(\frac{h}{p}\right)B_{2k+1}\left(\frac{h}{p}\right) &=\frac{(2k+1)!p^{1/2}}{(2\pi)^{2k+1}}\sum_{n=1}^{\infty}\frac{\left(\frac{n}{p}\right)}{n^{2k+1}}\\ &=\frac{(2k+1)!p^{1/2}}{(2\pi)^{2k+1}}\prod_{q}\left\{1-\frac{\left(\frac{q}{p}\right)}{q^{2k+1}}\right\}^{-1},\end{aligned}$$

where the product extends over all primes q. We infer that the left member of (2.4) is positive for $k\geqq 0$ (the case $k=0$ requires special treatment since the convergence of the series on the right is not absolute).

Similarly it follows from [3, p. 66]

$$E_{2k}(x) = (-1)^k \frac{4(2k)!}{\pi^{2k+1}} \sum_{n=0}^{\infty} \frac{\sin (2n+1)\pi x}{(2n+1)^{2k+1}}$$

that

$$(2.5) \qquad \begin{aligned} (-1)^k \sum_{h=1}^{m} \left(\frac{h}{p}\right) E_{2k}\left(\frac{2h}{p}\right) &= \frac{2(2k)!}{\pi^{2k+1}} p^{1/2} \sum_{n=0}^{\infty} \frac{\left(\frac{2n+1}{p}\right)}{(2n+1)^{2k+1}} \\ &= \frac{2(2k)!}{\pi^{2k+1}} p^{1/2} \prod_{q>2} \left\{1 - \frac{\left(\frac{q}{p}\right)}{q^{2k+1}}\right\}^{-1}. \end{aligned}$$

We infer that the left member of (2.5) is positive for $k \geqq 0$ (again the case $k=0$ requires special treatment; compare [2]).

3. For $p \equiv 1 \pmod 4$, (2.1) becomes

$$(3.1) \qquad \sum_{r=1}^{m} \left(\frac{r}{p}\right) \cos \frac{2\pi r n}{p} = \frac{1}{2}\left(\frac{n}{p}\right) p^{1/2} \qquad (p = 2m+1),$$

by means of which we can again assert an identity like (2.3) where $f(x)$ is now a cosine series. However we shall discuss only the particular cases corresponding to the Bernoulli and Euler polynomials. In the first place, making use of [3, p. 65]

$$B_{2k}(x) = (-1)^{k+1} \frac{2(2k)!}{(2\pi)^{2k}} \sum_{n=1}^{\infty} \frac{\cos 2n\pi x}{n^{2k}},$$

we get

$$(3.2) \qquad (-1)^{k+1} \sum_{h=1}^{m} \left(\frac{h}{p}\right) B_{2k}\left(\frac{h}{p}\right) = \frac{(2k)!}{(2\pi)^{2k}} p^{1/2} \sum_{n=1}^{\infty} \frac{\left(\frac{n}{p}\right)}{n^{2k}}.$$

It follows that the left member of (3.2) is positive for $k \geqq 1$.

Secondly, by means of [3, p. 66]

$$E_{2k-1}(x) = (-1)^k \frac{4(2k-1)!}{\pi^{2k}} \sum_{n=0}^{\infty} \frac{\cos (2n+1)\pi x}{(2n+1)^{2k}},$$

we infer

$$(3.3) \qquad (-1)^k \sum_{h=1}^{m} \left(\frac{h}{p}\right) E_{2k}\left(\frac{2h}{p}\right) = \frac{2(2k-1)!}{\pi^{2k}} \sum_{n=0}^{\infty} \frac{\left(\frac{2n+1}{p}\right)}{(2n+1)^{2k}}.$$

It follows that the left member of (3.3) is positive for $k \geqq 1$.

References

1. E. Landau, *Vorlesungen über Zahlentheorie*, Leipzig, 1927, vol. 1.
2. L. Moser, *A theorem on quadratic residues*, Proceedings of the American Mathematical Society vol. 2 (1951) pp. 503–504.
3. N. E. Nörlund, *Vorlesungen über Differenzenrechnung*, Berlin, 1924.
4. A. L. Whiteman, *Theorems on quadratic residues*, Mathematics Magazine vol. 23 (1949) pp. 71–74.

Duke University

FACTORIZATION OF n-SOLUBLE AND n-NILPOTENT GROUPS

REINHOLD BAER

If n is an integer [positive or negative or 0], and if the elements x and y in the group G meet the requirements

$$(xy)^n = x^n y^n \quad \text{and} \quad (yx)^n = y^n x^n,$$

then we term the elements x and y *n-commutative*. It is not difficult to verify that n-commutativity and $(1-n)$-commutativity are equivalent properties of the elements x and y, that (-1)-commutativity implies ordinary commutativity, and that commuting elements are n-commutative.

From any concept and property involving the fact that certain elements [or functions of elements] commute, one may derive new concepts and properties by substituting everywhere n-commutativity for the requirement of plain commutativity. This general principle may be illustrated by the following examples.

n-abelian groups are groups G such that $(xy)^n = x^n y^n$ for every x and y in G. They have first been discussed by F. Levi [3]; and they will play an important rôle in our discussion. Grün [2] has introduced the *n-commutator subgroup*. It is the smallest normal subgroup J of G such that G/J is n-abelian; and J may be generated by the totality of elements of the form $(xy)^n(x^n y^n)^{-1}$ with x and y in G. Dual to the n-commutator subgroup is the *n-center*. It is the totality of elements z in G such that $(zx)^n = z^n x^n$ and $(xz)^n = x^n z^n$ for every x in G; see Baer [1] for a discussion of this concept.

Received by the editors May 1, 1952.