A GENERALIZATION OF MAILLET'S DETERMINANT AND A BOUND FOR THE FIRST FACTOR OF THE CLASS NUMBER¹

L. CARLITZ

1. Let p be a prime ≥ 3 . For $(r, p) = 1$ define r' by means of $rr' \equiv 1 \pmod{p}$; also let $R(r)$ denote the least positive residue of $r \pmod{p}$. Maillet defined the determinant D_p of order $(p-1)/2$ by means of

$$(1) \quad D_p = |R(rs')| \quad (r, s = 1, \dots, (p-1)/2)$$

and raised the question whether $D_p \neq 0$ for all p . Malo computed D_p for $p \leq 13$ and conjectured that

$$(2) \quad D_p = (-p)^{(p-3)/2}.$$

For references see [6, pp. 340–342].

It was shown in [3] that

$$(3) \quad D_p = \pm p^{(p-3)/2} h,$$

where h denotes the first factor of the class number of the cyclotomic field $R(e^{2\pi i/p})$, and R denotes the rational field. Thus $D_p \neq 0$ but Malo's conjecture (2) is seen to be incorrect. It should be noted that D_p had been discussed earlier by Turnbull [7].

The first step in the proof of (3) is the easily proved relation

$$(4) \quad D'_p = -\frac{1}{2} D_p,$$

where

$$(5) \quad D'_p = \left| R(rs') - \frac{p}{2} \right| \quad (r, s = 1, \dots, (p-1)/2).$$

Since

$$R(r) - \frac{p}{2} = p \left(\frac{r}{p} - \left[\frac{r}{p} \right] - \frac{1}{2} \right),$$

(5) suggests the generalization

$$(6) \quad D_p^{(n)} = \left| p^n \overline{B}_n \left(\frac{rs'}{p} \right) \right| \quad (r, s = 1, \dots, (p-1)/2),$$

Received by the editors April 25, 1960.

¹ Supported in part by National Science Foundation, Grant G-9425.

where $\overline{B}_n(x)$ is the Bernoulli function defined by

$$(7) \quad \overline{B}_n(x) = B_n(x) \quad (0 \leq x < 1), \quad \overline{B}_n(x+1) = \overline{B}_n(x);$$

$B_n(x)$ is the Bernoulli polynomial of degree n . It is easily verified that for $n=1$ the determinant $D_p^{(n)}$ reduces to D_p' .

We shall require the known formula

$$(8) \quad \overline{B}_n(-x) = (-1)^n \overline{B}_n(x),$$

which is an easy consequence of (7).

Now let g denote a primitive root (mod p) and put

$$(9) \quad E_p^{(n)} = \left| p^n \overline{B}_n \left(\frac{g^{i-j}}{p} \right) \right| \quad (i, j = 0, 1, \dots, (p-3)/2).$$

Except for sign and order the numbers

$$\overline{B}_n \left(\frac{1}{p} \right), \quad \overline{B}_n \left(\frac{g}{p} \right), \dots, \overline{B}_n \left(\frac{g^{(p-3)/2}}{p} \right)$$

are the same as the numbers

$$\overline{B}_n \left(\frac{1}{p} \right), \quad \overline{B}_n \left(\frac{2}{p} \right), \dots, \overline{B}_n \left(\frac{p-1}{2p} \right).$$

It accordingly follows that

$$(10) \quad D_p^{(n)} = \pm E_p^{(n)}.$$

It is now convenient to treat separately the cases n even and n odd. When n is even it follows from (8) that $E_p^{(n)}$ is a circulant. If α denotes a primitive $(p-1)$ th root of unity, then we have

$$\begin{aligned} E_p^{(n)} &= \prod_{i=0}^{(p-3)/2} \sum_{j=0}^{(p-3)/2} p^n \overline{B}_n \left(\frac{g^j}{p} \right) \alpha^{2ij} \\ &= \left(\frac{p^n}{2} \right)^{(p-1)/2} \prod_{i=0}^{(p-3)/2} \sum_{j=0}^{p-2} \overline{B}_n \left(\frac{g^j}{p} \right) \alpha^{2ij}. \end{aligned}$$

If $\chi(r)$ denotes a typical multiplicative character (mod p) we may write this in the form

$$(11) \quad E_p^{(n)} = \left(\frac{p^n}{2} \right)^{(p-1)/2} \prod_{\chi(-1)=1} \sum_{r=1}^{p-1} B_n \left(\frac{r}{p} \right) \chi(r) \quad (n \text{ even}),$$

the product extending over the $(p-1)/2$ character such that $\chi(-1) = 1$.

In the next place, when n is odd, $E_p^{(n)}$ is not a circulant. However,

$$C_p^{(n)} = \left| p^n \bar{B}_n \left(\frac{g^{i-j}}{p} \right) \alpha^{i-j} \right| \quad (i, j = 0, 1, \dots, (p-3)/2)$$

is a circulant and clearly

$$(12) \quad C_p^{(n)} = E_p^{(n)}.$$

Also we have

$$\begin{aligned} C_p^{(n)} &= \prod_{i=0}^{(p-3)/2} \sum_{j=0}^{(p-3)/2} p^n \bar{B}_n \left(\frac{g^j}{p} \right) \alpha^{(2i+1)j} \\ &= \left(\frac{p^n}{2} \right)^{(p-1)/2} \prod_{i=0}^{(p-3)/2} \sum_{j=0}^{p-2} \bar{B}_n \left(\frac{g^j}{p} \right) \alpha^{(2i+1)j}, \end{aligned}$$

which may be written in the form

$$(13) \quad C_p^{(n)} = \left(\frac{p^n}{2} \right)^{(p-1)/2} \prod_{(-1) \rightarrow -1}^{p-1} \sum_{r=1}^{p-1} B_n \left(\frac{r}{p} \right) \chi(r) \quad (n \text{ odd}).$$

Leopoldt [5] has defined a generalized Bernoulli number B_χ^n , where χ denotes a primitive character (mod f). We shall be interested only in the case $f=p$, when

$$(14) \quad B_\chi^n = p^{n-1} \sum_{r=1}^{p-1} \chi(r) B_n \left(\frac{r}{p} \right).$$

Making use of (14), it is evident that (11) and (13) reduce to

$$(15) \quad E_p^{(n)} = \left(\frac{p}{2} \right)^{(p-1)/2} \prod_{\chi(-1)=-1} B_\chi^n \quad (n \text{ even}),$$

$$(16) \quad C_p^{(n)} = \left(\frac{p}{2} \right)^{(p-1)/2} \prod_{\chi(-1)=-1} B_\chi^n \quad (n \text{ odd}).$$

Let K denote the cyclotomic field $k(e^{2\pi i/p})$ and K_0 the maximal real subfield of K . If $\zeta_K(s)$, $\zeta_{K_0}(s)$ denote the Dedekind zeta functions of K and K_0 , respectively, then [5, p. 135]

$$\zeta_{K_0}(n) = (-1)^{m((n/2)+1)} \frac{(2\pi)^{mn} d_{K_0}^{1/2} B_{K_0}^n}{2^m d_{K_0}^n (n!)^m} \quad (n \text{ even}),$$

$$\frac{\zeta_K(n)}{\zeta_{K_0}(n)} = (-1)^{m(n+1)/2} \frac{(2\pi)^{mn} (d_K/d_{K_0})^{(1/2)n} B_{K/K_0}^n}{2^m (n!)^m} \quad (n \text{ odd}),$$

where $m = (p-1)/2$, d_K, d_{K_0} denote the discriminants of the respective fields and

$$(17) \quad B_{K_0}^n = \prod_{\chi(-1)=1} B_{\chi}^n \quad (n \text{ even}),$$

$$(18) \quad B_{K/K_0}^n = \prod_{\chi(-1)=-1} B_{\chi}^n \quad (n \text{ odd});$$

in view of (15) and (16) $B_{K_0}^n$ and B_{K/K_0}^n are rational. Comparing with (15) and (16) and making use of (10) and (12), it follows in particular that

$$(19) \quad D_p^{(n)} \neq 0 \quad (n = 1, 2, 3, \dots).$$

Returning to (15) and (16), it is clear that to find the highest power of p dividing $D_p^{(n)}$ it is necessary to have more precise information about the arithmetic nature of B_{χ}^n . Now by the final theorem in Leopoldt's paper [5] (see also [2, Theorem 3]) if

$$\frac{n}{p-1} = \frac{r}{d} \quad ((r, d) = 1),$$

and if the character χ is of order d , then the denominator of B_{χ}^n is divisible by the first power of a certain prime ideal $\mathfrak{p}$ of the first degree of the field $k(\chi)$. As χ runs through the characters of order d , $\mathfrak{p}$ runs through the set of conjugate prime ideals. It follows that the denominators of the products occurring in (15) and (16) are divisible by the first power of p . Consequently $D_p^{(n)}$ is divisible by at least $p^{(p-3)/2}$ for all $n \geq 1$.

2. Kummer [4, p. 473] stated that h , the first factor of the class number of the cyclotomic field $R(e^{2\pi i/p})$, satisfies

$$h \sim \frac{p^{(p+3)/4}}{2^{(p-3)/2} \pi^{(p-1)/2}} = P.$$

Some years ago Ankeny and Chowla [1] proved the weaker result

$$(20) \quad \lim_{p \rightarrow \infty} \frac{\log h/P}{\log p} = 0.$$

It may be of interest to point out that the following upper bound for h :

$$(21) \quad h < 2^{-(p-1)/4} (p-1)^{(p+3)/4} < 2^{-(p-1)/4} p^{(p+3)/4},$$

can be obtained very easily by making use of (3) above.

Let

$$D = |a_{rs}| \quad (r, s = 1, \dots, n)$$

be an arbitrary real determinant of order n and put

$$\sum_{s=1}^n a_{rs}^2 = a_r^2 \quad (r = 1, \dots, n);$$

then by Hadamard's lemma [8, p. 212]

$$(22) \quad |D| \leq a_1 a_2 \cdots a_n.$$

In particular if $|a_{rs}| < M$ then

$$(23) \quad |D| \leq n^{n/2} M^n.$$

Applying (23) to the determinant (1) we get

$$(24) \quad |D_p| \leq \left(\frac{p-1}{2}\right)^{(p-1)/4} (p-1)^{(p-1)/2} = 2^{-(p-1)/4} (p-1)^{3(p-1)/4}.$$

Clearly (3) and (24) imply (21).

We can improve (21) as follows. It is proved in [3] that for $p > 5$

$$(25) \quad D_p = \pm p^{(p-3)/2} D_p'',$$

where

$$D_p'' = \left| \left[\frac{rs}{p} \right] - \left[\frac{(r-1)s}{p} \right] \right| \quad (r, s = 3, 4, \dots, (p-1)/2).$$

The elements of D_p'' consist of zeros and ones. Also we have

$$\begin{aligned} \sum_{r=3}^{(p-1)/2} \left(\left[\frac{rs}{p} \right] - \left[\frac{(r-1)s}{p} \right] \right) \\ &= \left[\frac{(p-1)s/2}{p} \right] - \left[\frac{2s}{p} \right] = \left[\frac{(p-1)s/2}{p} \right], \\ \frac{1}{2} (p-1)(2t) &= (p-1)t = (t-1)p + (p-t), \\ \frac{1}{2} (p-1)(2t-1) &= (p-1)t - \frac{1}{2} (p-1) \\ &= (t-1)p + \left(\frac{1}{2} (p+1) - t \right), \end{aligned}$$

so that

$$\sum_{r=3}^{(p-1)/2} \left(\left[\frac{rs}{p} \right] - \left[\frac{(r-s)s}{p} \right] \right) = \begin{cases} t-1 & (s=2t) \\ t-1 & (s=2t-1). \end{cases}$$

Hence applying (22) we get

$$|D_p''|^2 \leq \prod_{s=3}^{(p-1)/2} \left[\frac{s-1}{2} \right],$$

so that

$$|D_p''| \leq \begin{cases} (m-1)! & (p=4m+1) \\ (m-1)!m^{1/2} & (p=4m+3). \end{cases}$$

By (3) and (25) this yields

$$(26) \quad h \leq \begin{cases} (m-1)! & (p=4m+1) \\ (m-1)!m^{1/2} & (p=4+3). \end{cases}$$

While (26) is stronger than (21) it does not yield (20).

REFERENCES

1. N. C. Ankeny and S. Chowla, *The class number of the cyclotomic field*, Canad. J. Math. vol. 3 (1951) pp. 486-494.
2. L. Carlitz, *Arithmetic properties of generalized Bernoulli numbers*, J. Reine Angew. Math. vol. 202 (1959) pp. 174-182.
3. L. Carlitz and F. R. Olson, *Maillet's determinant*, Proc. Amer. Math. Soc. vol. 6 (1955) pp. 265-269.
4. E. E. Kummer, *Sur la théorie des nombres complexes composés de racines de l'unité et de nombres entiers*, J. Math. Pures Appl. vol. 16 (1851) pp. 377-498.
5. H. W. Leopoldt, *Eine Verallgemeinerung der Bernoullischen Zahlen*, Abh. Math. Sem. Univ. Hamburg vol. 22 (1958) pp. 131-140.
6. T. Muir, *Contributions to the history of determinants 1900-1920*, Glasgow, Blackie, 1930.
7. H. W. Turnbull, *On certain modular determinants*, Edinburgh Math. Notes no. 32 (1941) pp. 23-30.
8. E. T. Whittaker and G. N. Watson, *Modern analysis*, 4th edition, Cambridge, University Press, 1927.

DUKE UNIVERSITY