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

L. CARLITZ

1. Let \( p \) be a prime \( \geq 3 \). 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

\[
D_p = \left| R(rs') \right| \quad (r, s = 1, \ldots, (p - 1)/2)
\]

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

\[
D_p = (-p)^{(p-3)/2}.
\]

For references see [6, pp. 340–342].

It was shown in [3] that

\[
D_p = \pm p^{(p-2)/2} h,
\]

where \( h \) denotes the first factor of the class number of the cyclotomic field \( \mathbb{Q}(\zeta^{2i/p}) \), 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

\[
D_p' = -\frac{1}{2} D_p,
\]

where

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

Since

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

(5) suggests the generalization

\[
D_p^{(n)} = \left| p^n B_n \left( \frac{rs'}{p} \right) \right| \quad (r, s = 1, \ldots, (p - 1)/2),
\]

Received by the editors April 25, 1960.

1 Supported in part by National Science Foundation, Grant G-9425.
where $B_n(x)$ is the Bernoulli function defined by

$$
B_n(x) = B_n(x) \quad (0 \leq x < 1), \quad B_n(x + 1) = B_n(x);
$$

$B_n(x)$ 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

$$
B_n(-x) = (-1)^n B_n(x),
$$

which is an easy consequence of (7).

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

$$
E_p^{(n)} = \left| p^n B_n \left( \frac{g^{i-j}}{p} \right) \right| \quad (i, j = 0, 1, \ldots, (p - 3)/2).
$$

Except for sign and order the numbers

$$
B_n\left( \frac{1}{p} \right), \quad B_n\left( \frac{g}{p} \right), \ldots, B_n\left( \frac{g^{(p-3)/2}}{p} \right)
$$

are the same as the numbers

$$
B_n\left( \frac{1}{p} \right), \quad B_n\left( \frac{2}{p} \right), \ldots, B_n\left( \frac{p-1}{2p} \right).
$$

It accordingly follows that

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

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 $\alpha$ denotes a primitive $(p-1)$th root of unity, then we have

$$
E_p^{(n)} = \prod_{i=0}^{(p-1)/2} \sum_{j=0}^{(p-3)/2} p^n B_n \left( \frac{g^i}{p} \right) \alpha^{ij} = \left( \frac{p^n}{2} \right)^{(p-1)/2} \prod_{i=0}^{(p-3)/2} \sum_{j=0}^{(p-3)/2} B_n \left( \frac{g^i}{p} \right) \alpha^{ij}.
$$

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

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

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

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use
In the next place, when \( n \) is odd, \( E_p^{(n)} \) is not a circulant. However, 

\[
C_p^{(n)} = \left| p^n B_n \left( \frac{g_i^j}{\rho} \right) \alpha_i \right| \quad (i, j = 0, 1, \ldots, (p - 3)/2)
\]

is a circulant and clearly

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

Also we have

\[
C_p^{(n)} = \prod_{i=0}^{(p-3)/2} \sum_{j=0}^{(p-3)/2} p^n B_n \left( \frac{g_i^j}{\rho} \right) \alpha_i^{(2i+1)j}
\]

\[
= \left( \frac{p^n}{2} \right)^{(p-1)/2} \prod_{r=1}^{(p-1)/2} \sum_{r=1}^{p-1} B_n \left( \frac{r}{\rho} \right) \chi(r)
\]

which may be written in the form

\[
(13) \quad C_p^{(n)} = \left( \frac{p^n}{2} \right)^{(p-1)/2} \prod_{x(-1)=1} B_x^n \left( \frac{r}{\rho} \right) \chi(r) \quad (n \text{ odd}).
\]

Leopoldt [5] has defined a generalized Bernoulli number \( B_x^n \), where \( \chi \) denotes a primitive character \((\text{mod } f)\). We shall be interested only in the case \( f = p \), when

\[
(14) \quad B_x^n = p^{n-1} \sum_{r=1}^{p-1} \chi(r) B_n \left( \frac{r}{\rho} \right).
\]

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

\[
(15) \quad E_p^{(n)} = \left( \frac{p}{2} \right)^{(p-1)/2} \prod_{x(-1)=1} B_x^n \quad (n \text{ even}),
\]

\[
(16) \quad C_p^{(n)} = \left( \frac{p}{2} \right)^{(p-1)/2} \prod_{x(-1)=1} B_x^n \quad (n \text{ odd}).
\]

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]

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

\[
\frac{\xi_K(n)}{\zeta_{K_0}(n)} = (-1)^{m(n+1)/2} \frac{(2\pi)^{mn} (d_K/d_{K_0})^{(1/2)n} B_{K/K_0}^n}{2^m (n!)^m} \quad (n \text{ odd}),
\]
where \( m = (p - 1)/2 \), \( d_K, d_{K_0} \) denote the discriminants of the respective fields and

\[
B^n_{K_0} = \prod_{x(-1)^{n-1} = 1} B^n_x \quad (n \text{ even}),
\]

\[
B^n_{K/K_0} = \prod_{x(-1)^{n-1} = -1} B^n_x \quad (n \text{ odd});
\]

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

\[
D_p^{(n)} \neq 0 \quad (n = 1, 2, 3, \ldots).
\]

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 \( B^n_x \). Now by the final theorem in Lehmer's paper [5] (see also [2, Theorem 3]) if

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

and if the character \( \chi \) is of order \( d \), then the denominator of \( B^n_x \) is divisible by the first power of a certain prime ideal \( p \) of the first degree of the field \( k(\chi) \). As \( \chi \) runs through the characters of order \( d \), \( p \) 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 \( \mathbb{Q}(e^{2\pi i/p}) \), satisfies

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

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

\[
\lim_{p \to \infty} \frac{\log h/P}{\log p} = 0.
\]

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

\[
h < 2^{-(p-1)/4}(p - 1)^{(p+3)/4} < 2^{-(p-1)/4} p^{(p+3)/4},
\]

can be obtained very easily by making use of (3) above.
Let
\[ D = \begin{vmatrix} a_{rs} \end{vmatrix} \quad (r, s = 1, \ldots, n) \]
be an arbitrary real determinant of order \( n \) and put
\[ \sum_{r=1}^{n} a_{rr}^2 = a_r^2 \quad (r = 1, \ldots, n); \]
then by Hadamard's lemma [8, p. 212]
\[ |D| \leq a_1 a_2 \cdots a_n. \]
In particular if \( |a_{rs}| < M \) then
\[ |D| \leq n^{n/2} M^n. \]

Applying (23) to the determinant (1) we get
\[ |D_p| \leq \left( \frac{p-1}{2} \right)^{(p-1)/4} \left( p-1 \right)^{(p-1)/2} = 2^{-(p-1)/4}(p-1)^{3/2(p-1)/4}. \]
Clearly (3) and (24) imply (21).

We can improve (21) as follows. It is proved in [3] that for \( p > 5 \)
\[ D_p = \pm p^{(p-1)/2} D_p'', \]
where
\[ D_p'' = \left| \begin{bmatrix} rs \\ p \end{bmatrix} - \begin{bmatrix} (r-1)s \\ p \end{bmatrix} \right| \quad (r, s = 3, 4, \ldots, (p-1)/2). \]
The elements of \( D_p'' \) consist of zeros and ones. Also we have
\[ \sum_{r,s=3}^{(p-1)/2} \left( \begin{bmatrix} rs \\ p \end{bmatrix} - \begin{bmatrix} (r-1)s \\ p \end{bmatrix} \right) \]
\[ = \begin{bmatrix} (p-1)s/2 \\ p \end{bmatrix} - \begin{bmatrix} 2s \\ p \end{bmatrix} = \begin{bmatrix} (p-1)s/2 \\ p \end{bmatrix}, \]

\[ \frac{1}{2} (p-1)(2l) = (p-1)l = (l-1)p + (p-l), \]

\[ \frac{1}{2} (p-1)(2l - 1) = (p-1)l - \frac{1}{2} (p-1) \]
\[ = (l-1)p + \left( \frac{1}{2} (p+1) - l \right), \]
so that
A GENERALIZATION OF MAILLET'S DETERMINANT

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

Hence applying (22) we get

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

so that

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

By (3) and (25) this yields

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

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

References


Duke University