# MAILLET'S DETERMINANT

L. CARLITZ AND F. R. OLSON

1. Let $p$ be a prime $\geqq 3$. If $(r, p)=1$, define $r'$ by means of $rr' \equiv 1 \pmod{p}$; the symbol $R(r)$ will denote the least positive residue of $r \pmod{p}$. Following Maillet we define the determinant $D_p$ by means of

$$D_p = \left| R(rs') \right| \qquad (r, s = 1, \cdots, (p-1)/2). \tag{1.1}$$

Maillet raised the question whether $D_p \neq 0$ for all $p$. Malo computed $D_p$ for several small values of $p$:

$$D_3 = 1, \qquad D_5 = -5, \qquad D_7 = 7^2, \qquad D_{11} = 11^4, \quad D_{13} = -13^5,$$

and conjectured that generally

$$D_p = (-p)^{(p-3)/2}. \tag{1.2}$$

For references see [2, pp. 340–342].

Making use of the easily proved transformation

$$D_p = (-p)^{(p-3)/2} \left| \left[ \frac{rs'}{p} \right] \right| \qquad (r, s = 2, \cdots, (p-1)/2) \tag{1.3}$$

which is obtained by subtracting $r$ times the first row of $D_p$ from the $r$th row, it is evident that $D_p$ is indeed divisible by the power of $p$ indicated in (1.2). In turn (1.3) may be further simplified by successive row subtractions to

$$D_p = (-p)^{(p-3)/2} \left| \left[ \frac{rs'}{p} \right] - \left[ \frac{(r-1)s'}{p} \right] \right| \qquad (r, s = 2, \cdots, (p-1)/2). \tag{1.4}$$

It is also not difficult to show that

$$D_p = \pm \left| p + R(rs) \right| \qquad (r, s = 1, \cdots, (p-1)/2) \tag{1.5}$$

which in turn reduces to

$$D_p = \pm p^{(p-3)/2} \left| \left[ \frac{rs}{p} \right] - \left[ \frac{(r-1)s}{p} \right] \right| \qquad (r, s = 3, \cdots, (p-1)/2). \tag{1.6}$$

This formula is particularly convenient for computation. Note that

Received by the editors May 25, 1954.

the elements in the determinants in (1.4) and (1.6) consist only of zeros and ones.

By means of (1.6) it is not difficult to verify that (1.2) holds for $p=17$ and 19 but not for $p=23$; in the last case an additional factor 3 occurs. Thus Malo's conjecture is not correct. We shall however show that $D_p$ never vanishes. This is a consequence of the formula proved below:

$$D_p = \pm p^{(p-3)/2}h, \tag{1.7}$$

where $h$ denotes the first factor of the class number of the cyclotomic field $k(e^{2\pi i/p})$.

Some related determinants are discussed briefly in §3.

2. Put

$$D_p(x) = | x + R(rs') | \qquad (r, s = 1, \cdots, (p-1)/2), \tag{2.1}$$

so that $D_p(0)=D_p$. Since the last column of $D_p$ consists of the numbers $p-2, p-4, \cdots, 1$, it follows that by addition of twice the first column to the last column of both $D_p$ and $D_p(x)$ we get

$$D_p(x) = \frac{3x+p}{p} D_p. \tag{2.2}$$

If we take $x=-p/2$ then (2.2) becomes

$$D_p' = -D_p/2, \tag{2.3}$$

where

$$D_p' = D_p(-p/2) = | \{rs'\} | \qquad (r, s = 1, \cdots, (p-1)/2) \tag{2.4}$$

and

$$\{r\} = R(r) - p/2. \tag{2.5}$$

Note that (2.5) implies

$$\{-r\} = -\{r\}. \tag{2.6}$$

In the next place let $g$ denote a primitive root (mod $p$) and put

$$D_p'' = | \{g^{i-j}\} | \qquad (i, j = 0, \cdots, (p-3)/2). \tag{2.7}$$

Except for sign and order, the numbers

$$\{1\}, \{g\}, \cdots, \{g^{(p-3)/2}\}$$

are the same as the numbers $\{1\}, \{2\}, \cdots, \{(p-1)/2\}$. Conse-

quently comparison of (2.4) and (2.7) shows that

$$D_p' = \pm D_p''. \tag{2.8}$$

Since $g^{(p-1)/2} \equiv -1$, it follows from (2.6) that $D_p''$ is not a circulant. However, if $\alpha$ denotes a primitive $(p-1)$th root of unity, then clearly

$$D_p''' = \left| \{g^{i-j}\}\alpha^{i-j} \right| \qquad (i, j = 0, \cdots, (p-1)/2) \tag{2.9}$$

is a circulant; moreover it is evident that

$$D_p'' = D_p'''. \tag{2.10}$$

Using the familiar formula for a circulant, (2.9) yields

$$D_p''' = \prod_{i=0}^{(p-3)/2} \sum_{j=0}^{(p-3)/2} \{g^{i-j}\}\alpha^{i(2j+1)}. \tag{2.11}$$

Now on the other hand the first factor of the class number of $k(e^{2\pi i/p})$ is given by [3, p. 35]

$$h = (2p)^{-(p-3)/2} \prod_{j=0}^{(p-3)/2} \phi(\alpha^{2j+1}), \tag{2.12}$$

where

$$\phi(x) = \sum_{i=0}^{p-2} R(g^i)x^i.$$

Then if $\beta = \alpha^{2j+1}$,

$$\begin{aligned} \phi(\beta) &= \sum_{i=0}^{(p-3)/2} R(g^i)\beta^i - \sum_{i=0}^{(p-3)/2} R(-g^i)\beta^i \\ &= \sum_{i=0}^{(p-3)/2} (2R(g^i) - p)\beta^i = 2\sum_{i=0}^{(p-3)/2} \{g^i\}\beta^i. \end{aligned}$$

Hence using (2.3), (2.8), (2.10), (2.11), and (2.12) we get

$$h = \pm p^{-(p-3)/2} D_p, \tag{2.13}$$

which proves (1.7).

It follows at once from (2.13) that

$$D_p \neq 0 \tag{2.14}$$

for all $p \geqq 3$. On the other hand Kummer's criterion [3, p. 35] for divisibility of $h$ by $p$ shows that

$$p^{(p-1)/2} \mid D_p \tag{2.15}$$

if and only if $p$ divides the numerator of one of the Bernoulli numbers $B_2, B_4, \cdots, B_{p-3}$; moreover we can assert that (2.15) holds for infinitely many primes $p$.

3. By a formula of Eisenstein

$$\left[\frac{m}{n}\right] = \frac{m}{n} - \frac{1}{2} + \frac{1}{2n}\sum_{k=1}^{n-1} \sin\frac{2km\pi}{n}\cot\frac{k\pi}{n}.$$

This implies

$$\{m\} = -\sum_{k=1}^{(p-1)/2} \sin\frac{2km\pi}{p}\cot\frac{k\pi}{p},$$

where $\{m\}$ is defined by (2.5). Replacing $m$ by $rs'$ we get

$$\{rs'\} = -\sum_{k=1}^{(p-1)/2} \sin\frac{2kr\pi}{p}\cot\frac{ks\pi}{p},$$

and therefore

$$D_p' = (-1)^{(p-1)/2}\left|\sin\frac{2rs\pi}{p}\right|\cdot\left|\cot\frac{rs\pi}{p}\right|,$$

where in each determinant $r, s = 1, \cdots, (p-1)/2$. Now since

$$|\sin 2rs\pi/p|^2 = 2^{-(p-1)}p^{(p-1)/2},$$

it follows, using (2.3), that $|\cot rs\pi/p| = \pm 2^{(p-3)/2}p^{-(p-1)/4}D_p$. Hence (2.13) yields

$$|\cot rs\pi/p| = \pm 2^{(p-3)/2}p^{(p-5)/4}h. \tag{3.1}$$

Again, recalling the definition of the Dedekind sum

$$s(r, p) = \sum_{k=1}^{p-1}\frac{k}{p}\left(\frac{rk}{p} - \left[\frac{rk}{p}\right] - \frac{1}{2}\right) = \frac{1}{p^2}\sum_{k=1}^{p-1} k\{rk\}$$

and Rademacher's formula (for an elementary proof see [1])

$$s(r, p) = \frac{1}{4p}\sum_{k=1}^{p-1}\cot\frac{rk\pi}{p}\cot\frac{k\pi}{p},$$

we see that

$$s(rt', p) = \frac{1}{2p}\sum_{k=1}^{(p-1)/2}\cot\frac{rk\pi}{p}\cot\frac{tk\pi}{p}, \tag{3.2}$$

where as above $tt' \equiv 1 \pmod{p}$. If we put

$$\Delta_p = \left| s(rt', p) \right| \qquad (r, t = 1, \cdots, (p-1)/2),$$

it follows from (3.2) that

$$\Delta_p = (2p)^{-(p-1)/2} \left| \cot rt\pi/p \right|^2.$$

Consequently by (3.1)

$$\Delta_p = 2^{(p-5)/2} p^{-2} h^2. \tag{3.3}$$

*Added in proof.* Professor S. Chowla has kindly informed the writers that he and A. Weil had proved the formula (1.7) several years ago but had not published the result.

## References

1. T. M. Apostol, *Theorems on generalized Dedekind sums*, Pacific Journal of Mathematics vol. 2 (1952) pp. 1–9.

2. T. Muir, *Contributions to the history of determinants* 1900–1920, Glasgow, 1930.

3. H. S. Vandiver and G. E. Wahlin, Bulletin of the National Research Council, No. 62, Washington, D. C., 1928.

Duke University