JOURNAL OF NUMBER THEORY **18**, 306–312 (1984)

On Maillet Determinant

KAI WANG

Department of Mathematics, Wayne State University, Detroit, Michigan 48202

Communicated by Hans Zassenhaus

Received April 13, 1982

For a positive integer m, let $A = \{1 \leqslant a < m/2 \mid (a, m) = 1\}$ and let $n = |A|$. For an integer x, let $R(x)$ be the least positive residue of x modulo m and if $(x, m) = 1$, let x' be the inverse of x modulo m. If m is odd, then $|R(ab')|_{a,b \in A} = -2^{1-n}(\prod_\chi (\sum_{a=1}^{m-1} a\chi(a)))$, where χ runs over all the odd Dirichlet characters modulo m.

1. INTRODUCTION

For an arbitrary positive integer m, let $A = \{1 \leqslant a < m/2 \mid (a, m) = 1\}$ and let $n = |A|$. For any integer x, let $R(x)$ be the least positive residue of x modulo m and for $(x, m) = 1$, let x' be the inverse of x modulo m. The Maillet determinant is an $n \times n$ determinant defined by

$$D_m = |R(ab')|_{a,b \in A}.$$

About twenty years ago, Carlitz and Olson [2] proved the following interesting formula for $m = p$ an odd prime,

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

where h denotes the first factor of the class number of the cyclotomic field $k(e^{2\pi i/p})$. The purpose of this note is to study the Maillet determinant for an arbitrary m. The main result is

THEOREM 1.1. *Let m be a positive integer. If m is odd, then*

$$D_m = -2^{1-n} \prod_{\chi \text{odd}} \left(\sum_{a=1}^{m-1} a\chi(a) \right),$$

where χ runs over all the odd Dirichlet characters modulo m.

Our approach which is different from [2] was motivated by our recent

0022-314X/84 $3.00

study of Chowla's theorem [3, 5]. Our method also yields information about the Maillet determinant when m is even and when A is an arbitrary coset representative of the subgroup $\{\pm 1\}$ in the group Z_m^x of units modulo m. If $m = p$ a prime, then our formula reduces to Carlitz and Olson's formula. We are also able to determine the sign in their formula.

We refer to [1, 4] for the basic knowledge on Dirichlet characters and related results.

2. General Case

Let m be a fixed positive integer and let

$$Z_m^x = \{1 \leqslant a < m \mid (a, m) = 1\}$$

be the group of units modulo m. Then the order of Z_m^x is equal to $\varphi(m)$, where $\varphi(m)$ is the euler function. Let A be a set of coset representatives of the subgroup $\{\pm 1\}$ in Z_m^x in a fixed order. Then $|A| = \frac{1}{2}\varphi(m)$. For a Dirichlet character χ modulo m, let $S(\chi) = \sum_{a \in Z_m^x} a\chi(a)$ and $T_A(\chi) = \sum_{a \in A} \chi(a)$. We will prove the formula for the Maillet determinant defined over A.

THEOREM 2.1. *With above notations,*

$$|R(ab')|_{a,b \in A} = 2^{-\varphi(m)/2} \left(\prod_{\chi} S(\chi)\right) \left(1 + \frac{2m}{\varphi(m)} \sum_{\chi} \frac{|T_A(\chi)|^2}{S(\chi)}\right),$$

where χ runs over all odd Dirichlet characters modulo m.

Proof. Recall that a Dirichlet character χ is odd if $\chi(-1) = -1$. Let $\{\chi_1, ..., \chi_n\}$ be the set of all odd Dirichlet characters modulo m, where $n = \varphi(m)/2$. Let $A = \{a_1, ..., a_n\}$ and let

$$\Omega = n^{-1/2} [\chi_i(a_j)]_{1 \leqslant i,j \leqslant n}.$$

It follows immediately from the orthogonal relations of characters

$$\frac{1}{\varphi(m)} \sum_{a \in Z_m^x} \chi_i(a) \overline{\chi_j(a)} = \delta_{ij}$$

that Ω is unitary and

$$\begin{aligned} \sum_{\chi \text{ odd}} \chi(a) &= n \quad &&\text{if} \quad a = 1, \\ &= -n \quad &&\text{if} \quad a = m-1, \\ &= 0 \quad &&\text{otherwise,} \end{aligned}$$

and

$$\sum_{a \in A} \chi_i(a)\,\overline{\chi_j(a)} = n\delta_{ij}.$$

It is clear that

$$|R(ab')|_{a,b \in A} = |\Omega[R(ab')]\Omega^*| = \left|\frac{1}{n}\sum_{a \in A}\sum_{b \in A} \chi_i(a)\,R(ab')\,\overline{\chi_j(b)}\right|.$$

For convenience, let

$$x_{ij} = \sum_{a \in A}\sum_{b \in A} \chi_i(a)\,R(ab')\,\overline{\chi_j(b)}.$$

Note that

$$\begin{aligned}
&\sum_{a \in Z_m^x}\sum_{b \in Z_m^x} \chi_i(a)\,R(ab')\,\overline{\chi_j(b)}\\
&\quad= \sum_{c \in Z_m^x}\sum_{b \in Z_m^x} \chi_i(cb)\,R(c)\,\overline{\chi_j(b)}\\
&\quad= \left(\sum_{b \in Z_m^x} \chi_i(b)\,\overline{\chi_j(b)}\right)\left(\sum_{c \in Z_m^x} R(c)\,\chi_i(c)\right)\\
&\quad= \delta_{ij}\varphi(m)\,S(\chi_i).
\end{aligned}$$

On the other hand,

$$\begin{aligned}
&\sum_{a \notin A}\sum_{b \in A} \chi_i(a)\,R(ab')\,\overline{\chi_j(b)}\\
&\quad= \sum_{a \in A}\sum_{b \in A} \chi_i(m-a)\,R((m-a)b')\,\overline{\chi_j(b)}\\
&\quad= -\sum_{a \in A}\sum_{b \in A} \chi_i(a)(m - R(ab'))\,\overline{\chi_j(b)} \quad (\text{because } R(m-x) = m - R(x))\\
&\quad= -m\left(\sum_{a \in A} \chi_i(a)\right)\left(\sum_{b \in A} \overline{\chi_j(b)}\right) + \sum_{a \in A}\sum_{b \in A} \chi_i(a)\,R(ab')\,\overline{\chi_j(b)}\\
&\quad= -mT_A(\chi_i)\,T_A(\bar{\chi}_j) + x_{ij}.
\end{aligned}$$

Similarly, we have

$$\sum_{a \in A}\sum_{b \notin A} \chi_i(a)\,R(ab')\,\overline{\chi_j(b)} = -mT_A(\chi_i)\,T_A(\bar{\chi}_j) + x_{ij},$$

$$\sum_{a \notin A}\sum_{b \notin A} \chi_i(a)\,R(ab')\,\overline{\chi_j(b)} = x_{ij}.$$

It follows that

$$x_{ij}=\frac{n}{2}\delta_{ij}S(\chi_j)+\frac{m}{2}T_A(\chi_i)\,T_A(\bar{\chi}_j),$$

for $1\leqslant i,j\leqslant n$. Using the following formula for determinants,

$$|\delta_{ij}y_i+1|_{1\leqslant i,j\leqslant n}=\left(\prod_{i=1}^{n}y_i\right)\left(1+\sum_{i=1}^{n}\frac{1}{y_i}\right),$$

we have

$$\begin{aligned}
|R(ab')|_{a,b\in A}&=n^{-n}\,|x_{ij}|\\
&=n^{-n}\left|\frac{n}{2}\delta_{ij}S(\chi_j)+\frac{m}{2}T_A(\chi_i)\,T_A(\bar{\chi}_j)\right|\\
&=n^{-n}\left(\frac{m}{2}\right)^n\prod_{i=1}^{n}T_A(\chi_i)\prod_{j=1}^{n}T_A(\bar{\chi}_j)\left|\frac{n}{m}\delta_{ij}\frac{S(\chi_j)}{T_A(\chi_i)\,T_A(\bar{\chi}_j)}+1\right|\\
&=\left(\frac{m}{2n}\right)^n\left(\prod_{i=1}^{n}T_A(\chi_i)\,T_A(\bar{\chi}_i)\right)\left(\prod_{i=1}^{n}\frac{n}{m}\frac{S(\chi_j)}{T_A(\chi_i)\,T_A(\bar{\chi}_i)}\right)\\
&\quad\times\left(1+\sum_{i=1}^{n}\frac{mT_A(\chi_i)\,T_A(\bar{\chi}_i)}{n\,S(\chi_i)}\right)\\
&=2^{-n}\left(\prod_{i=1}^{n}S(\chi_i)\right)\left(1+\frac{m}{n}\sum_{i=1}^{n}\frac{|T_A(\chi_i)|^2}{S(\chi_i)}\right).
\end{aligned}$$

This completes the proof of Theorem 2.1.

3. Odd Case

In this section, let m be an odd integer and let

$$A=\{a\in Z_m^x\,|\,1\leqslant a<m/2\}.$$

We will show that the formula in Theorem 2.1 can be greatly simplified. For simplicity, let $T(\chi)=T_A(\chi)$. We will need

Lemma 3.1. *Let χ be an odd Dirichlet character modulo m. Then*

$$T(\chi)=\frac{1}{m}\,(\overline{\chi(2)}-2)\,S(\chi).$$

Proof. In the following computations, $a, b \in Z_m^\times$.

$$(1-2\chi(2))\,S(\chi) = \sum' a\chi(a) - \sum' 2a\chi(2a)$$

$$= \sum'_{a \text{ odd}} a\chi(a) - \sum'_{m > a > m/2} 2a\chi(2a)$$

$$= \sum'_{a \text{ odd}} a\chi(a) - \sum'_{m > a > m/2} 2a\chi(2a-m)$$

$$= \sum'_{a \text{ odd}} a\chi(a) - \sum'_{b \text{ odd}} (m+b)\,\chi(b)$$

$$= -m \sum'_{a \text{ odd}} \chi(a) = m \sum'_{a \text{ odd}} \chi(m-a)$$

$$= m\chi(2) \sum'_{1 \leqslant b < m/2} \chi(b) = m\chi(2)\,T(\chi).$$

This implies the lemma.

THEOREM 3.2. *If m is odd and $A = \{a \in Z_m^\times \mid 1 \leqslant a < m/2\}$, then*

$$|R(ab')|_{a,b \in A} = (-1)2^{1-(1/2)\varphi(m)} \prod_{\chi \text{ odd}} S(\chi).$$

Proof. By Lemma 3.1,

$$\sum'_{\chi \text{odd}} \frac{|T(\chi)|^2}{S(\chi)} = \frac{1}{m} \sum'_{\chi \text{odd}} (\bar{\chi}(2)-2)\,T(\bar{\chi})$$

$$= \frac{1}{m}\left(\sum'_{\chi \text{odd}} \chi(2)\,T(\chi) - 2\sum'_{\chi \text{odd}} T(\chi)\right)$$

$$= \frac{1}{m}\left(\sum'_{a \in A} \sum'_{\chi \text{odd}} \chi(2a) - 2\sum'_{a \in A} \sum'_{\chi \text{odd}} \chi(a)\right)$$

$$= \frac{1}{m}(-\varphi(m) - 2\varphi(m)) = \frac{-3}{2}\varphi(m),$$

since

$$\sum'_{\chi \text{odd}} \chi(a) = \begin{cases} 1 & \text{if } a = 1, \\ -1 & \text{if } a = m-1, \\ 0 & \text{otherwise.} \end{cases}$$

Now Theorem 3.2 follows easily from Theorem 2.1.

COROLLARY 3.3. *If $m = p$, an odd prime, then*

$$|R(ab')|_{a,b\in A} = (-p)^{(1/2)(p-3)}h,$$

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

Proof. It is known [4] that under the assumption

$$h = 2^{1-n}p \prod_{\chi \text{odd}} \left| \frac{T(\chi)}{2-\chi(2)} \right|,$$

where $n = \frac{1}{2}(p-1)$. By Theorem 3.2 and Lemma 3.1,

$$\begin{aligned} |R(ab')|_{a,b\in A} &= (-1)2^{1-n} \prod_{\chi \text{odd}} \frac{pT(\chi)}{\overline{\chi(2)}-2} \\ &= (-1)^{n+1}2^{1-n}p^n \frac{\chi\prod_{\text{odd}}^{T(\chi)}}{\chi\prod_{\text{odd}}^{2-\chi(2)}} \\ &= (-1)^{n+1}p^{n-1}h = (-p)^{n-1}h. \end{aligned}$$

COROLLARY 3.4. *If m is odd and $B = \{ka \mid a \in A\}$, where $(k, m) = 1$, then*

$$|R(ab')|_{a,b\in B} = (-1)2^{1-(1/2)\varphi(m)} \prod_{\chi \text{odd}} S(\chi).$$

Proof. This follows immediately from the observation

$$|T_B(\chi)|^2 = \left| \sum_{a\in A} \chi(ka) \right|^2 = |\chi(k)T(\chi)|^2 = |\chi(k)|^2\,|T(\chi)|^2 = |T(\chi)|^2.$$

4. EVEN CASE

There is not much that can be done to the formula for the Maillet determinant where $m \equiv 2 \pmod 4$. However, when $m \equiv 0 \pmod 4$, the formula can also be simplified as in the odd case as shown in Theorem 4.1.

THEOREM 4.1. *Suppose that $m > 4$ and $m \equiv 0 \pmod 4$. Let $A = \{a \in Z_m^\times \mid 1 \leqslant a < m/2\}$. Then*

$$|R(ab')|_{a,b\in A} = -2^{-\varphi(m)/2} \prod_{\chi \text{odd}} S(\chi).$$

We will only outline the proofs and leave the details to the readers. Let $m = 4k$, $k > 1$. Since $(2k-1)^2 \equiv 1 \pmod m$, $\chi(2k-1) = \pm 1$. Note that there are exactly $\frac{1}{4}\varphi(m)$ odd Dirichlet characters χ such that $\chi(2k-1)=1$ (resp. -1). Let χ be an odd Dirichlet character. If $\chi(2k-1)=1$, then $S(\chi)=-(m/2)\,T(\chi)$ and if $\chi(2k-1)=-1$, then $T(\chi)=0$. This implies that

$$1+\frac{2m}{\varphi(m)}\sum_{\chi\,\mathrm{odd}}\frac{|T(\chi)|^2}{S(\chi)}=-1,$$

and our formula.

References

1. Z. Borevich and I. Shafarevich, "Number Theory," Academic Press, New York, 1966.
2. L. Carlitz and F. R. Olson, Maillet's determinant, *Proc. Amer. Math. Soc.* **6** (1955), 265–269.
3. S. Chowla, The nonexistence of nontrivial linear relations between the roots of a certain irreducible equation, *J. Number Theory* **2** (1970), 120–123.
4. D. A. Marcus, "Number Field," Springer-Verlag, New York, Berlin, 1977.
5. K. Wang, On a theorem of S. Chowla, *J. Number Theory* **14** (1982), 1–4.