Pacific Journal of Mathematics

POWER CHARACTER MATRICES

D. H. LEHMER

Vol. 10, No. 3 November 1960

POWER CHARACTER MATRICES

D. H. LEHMER

Introduction. In 1956 [4] we gave two classes of matrices whose elements are simple functions of their row and column numbers and whose characteristic roots, inverse, determinant as well as the general element of any power of the matrix can be given explicitly. The elements of these matrices are simple real functions of the real non-principal character χ modulo an odd prime. Such matrices are useful as test matrices in checking out automatic machine programs for general matrices with real elements. In this paper we present corresponding matrices with complex elements which may be used likewise as test matrices. The elements are based on kth power characters χ which are complex roots of unity if $k > 2$.

The general method for finding characteristic roots is the same in both papers and depends on the simple fact that the roots of a polynomial are determined by the sums of like powers of its roots.

All matrices in this paper are square and of order $p - 1$ where p is an odd prime.

NOTATION AND DEFINITIONS. Let k be an integer greater than 1. Let $p = kt + 1$ be a prime and let g be a fixed primitive root of p. Let $\alpha = \exp\{2\pi i/k\}$. The kth power character χ, depending on g, is defined by

$$\chi(h) = \begin{cases} 0 \text{ if } p \text{ divides } h \\ \alpha^{\text{ind}h} \text{ otherwise} \end{cases}$$

where $\text{ind}\, h = \text{ind}_g h$ is the index of h to the base g defined modulo $p - 1$ by

$$g^{\text{ind}h} \equiv h (\text{mod } p) .$$

The following well-known properties of χ are simple consequences of our definition of χ and are used many times in the sequel.

$$\chi(h + p) = \chi(h)$$

$$\chi(h_1 h_2) = \chi(h_1)\chi(h_2) \tag{1}$$

$$\bar{\chi}(h) = 1/\chi(h) = \chi(\bar{h}) \qquad (h\bar{h} \equiv 1 \pmod p)$$

$$\chi(h)^k = \begin{cases} 0 \text{ if } p \mid h \\ 1 \text{ otherwise} \end{cases}$$

$$\sum_{h=1}^{p-1} [\chi(h)]^r = \begin{cases} p - 1 \text{ if } k \mid r \\ 0 \quad \text{otherwise} . \end{cases} \tag{2}$$

Received November 12, 1959. This paper is the result of unsponsored research.

By way of examples, if $k = 4$, $p = 5$, $g = 2$ we have

$$\chi(0) = 0, \quad \chi(1) = 1, \quad \chi(2) = i, \quad \chi(3) = -i, \quad \chi(4) = -1$$

and if $k = 3$, $p = 7$, $g = 3$ we have

$$\chi(0) = 0, \ \chi(1) = 1, \ \chi(2) = \omega^2, \ \chi(3) = \omega, \ \chi(4) = \omega, \ \chi(5) = \omega^2, \ \chi(6) = 1$$

where $\omega = e^{2\pi i/3}$.

For simplicity we denote $\chi(-1)$ by ε. Thus

$$\varepsilon = (-1)^t . \tag{3}$$

In particular, $\varepsilon = 1$ when k is odd.

We use two types of Kronecker symbol

$$\delta_i^j = \begin{cases} 1 \text{ if } i \equiv j \pmod{p} \\ 0 \text{ otherwise} \end{cases}$$

and

$$\delta_{\chi(i)}^{\chi(j)} = \begin{cases} 1 \text{ if } \chi(i) = \chi(j) \\ 0 \text{ otherwise} . \end{cases}$$

Thus

$$k\delta_{\chi(i)}^{\chi(j)} = \sum_{\nu=0}^{k-1} [\chi(i/j)]^\nu . \tag{4}$$

Matrices of the first kind. We begin with a very simple type of matrix based on an arbitrary matrix N of $\kappa \leqq k$ rows and columns

$$N = \{\alpha_{rs}\} \qquad (r, s = 1(1)\kappa)$$

whose characteristic roots

$$\rho_1, \rho_2, \cdots, \rho_\kappa$$

are supposed known. The matrix M of order $p - 1 = kt$ is defined by

$$M = \{a_{ij}\}, \ a_{ij} = \sum_{r,s=1}^{\kappa} \alpha_{rs}\chi(i^{r-1}/j^{s-1}) . \tag{5}$$

We denote the general elements of N^m and M^m by $\alpha_{rs}^{(m)}$ and $a_{ij}^{(m)}$. We can then state:

THEOREM 1. *The general element $a_{ij}^{(m)}$ of M^m is given by*

$$a_{ij}^{(m)} = (p-1)^{m-1} \sum_{r,s=1}^{\kappa} \alpha_{rs}^{(m)}\chi(i^{r-1}/j^{s-1}) .$$

REMARK. Thus, aside from the factor $(p-1)^{m-1}$, M^m is the same

function of N^m that M is of N.

Proof. The theorem is trivial for $m = 1$. If true for $m = n$ we may write

$$\begin{aligned} a_{ij}^{(n+1)} &= \sum_{h=1}^{p-1} a_{ih} a_{hj}^{(n)} \\ &= (p-1)^{n-1} \sum_{h=1}^{p-1} \left\{ \sum_{r,s=1}^{\kappa} \alpha_{rs} \chi(i^{r-1}/h^{s-1}) \right\} \left\{ \sum_{u,v=1}^{\kappa} \alpha_{uv}^{(n)} \chi(h^{u-1}/j^{v-1}) \right\} \\ &= (p-1)^{n-1} \sum_{r,s=1}^{\kappa} \sum_{u,v=1}^{\kappa} \alpha_{rs} \alpha_{uv}^{(n)} \chi(i^{r-1}/j^{v-1}) \sum_{h=1}^{p-1} \chi(h^{u-s}) \,. \end{aligned}$$

By (1) and (2) the inner sum vanishes unless $u = s$ in which case the sum is $q - 1$. Hence

$$\begin{aligned} a_{ij}^{(n+1)} &= (p-1)^n \sum_{s=1}^{\kappa} \sum_{r,v=1}^{\kappa} \alpha_{rs} \alpha_{sv}^{(n)} \chi(i^{r-1}/j^{v-1}) \\ &= (p-1)^n \sum_{r,v=1}^{\kappa} \alpha_{rv}^{(n+1)} \chi(i^{r-1}/j^{v-1}) \,. \end{aligned}$$

Thus the induction is complete.

THEOREM 2. *The characteristic roots of M are*

$$(p-1)\rho_1, (p-1)\rho_2, \cdots, (p-1)\rho_\kappa, 0, 0, \cdots, 0 \,.$$

Proof. Let m be any positive integer and consider the trace of M^m. This is the sum of the mth powers of the roots of M. It is also

$$\begin{aligned} \sum_{i=1}^{p-1} \alpha_{ii}^{(m)} &= (p-1)^{m-1} \sum_{r,s=1}^{\kappa} \sum_{i=1}^{p-1} \alpha_{rs}^{(m)} \chi(i^{r-s}) = (p-1)^m \sum_{r=1}^{\kappa} \alpha_{rr}^{(m)} \\ &= (p-1)^m \sum_{r=1}^{\kappa} \rho_r^m = \sum_{r=1}^{\kappa} [(p-1)\rho_r]^m + \sum_{r=\kappa+1}^{p-1} 0^m \,. \end{aligned}$$

Since this is true for all integers m, the roots of M must be those stated in the theorem.

It follows from Theorem 2 that M and N have the same rank. That the rank of M cannot exceed k follows directly from the definition of M. In fact if $i_1 \equiv i_2 \pmod{k}$ then by (5) $a_{i_1 j} = a_{i_2 j}$ so the number of distinct rows of M cannot exceed the number k of incongruent numbers i modulo k. Actually the matrix may be partitioned into t^2 equal matrices of k rows and columns since $a_{i_1 j_1} = a_{i_2 j_2}$ whenever $i_1 \equiv i_2$ and $j_1 \equiv i_2$ modulo k.

We turn now to a much more sophisticated class of matrices.

Matrices of the second kind. We define the matrix M of order $p - 1$ by

$$M = \{a_{ij}\} \text{ where } a_{ij} = \chi(i-j) .$$

This matrix has been considered recently by L. Carlitz [1] who found its determinant. Before attempting a further analysis of M we need to recall a few well-known facts from cyclotomy. We shall use Jacobi's ψ-function defined for $r = 1(1)k-1$ by

$$\psi_r = \sum_{s=1}^{p-2} \alpha^{\text{ind}s-(r+1)\,\text{ind}(1+s)} = \sum_{s=1}^{p-2} \chi(s)[\chi(1+s)]^{-r-1} .$$

LEMMA 1.
$$\psi_r = \varepsilon\psi_{k-1-r}$$
$$\psi_{k-1} = -\varepsilon .$$

Proof. To prove the second statement we note that by definition

$$\psi_{k-1} = \sum_{s=1}^{p-2} \chi(s) = 0 - \chi(p-1) = -\varepsilon .$$

To prove the first statement we make the substitution

$$s \equiv -u/(1+u) \pmod{p} .$$

Thus we find

$$\psi_r = \sum_{s=1}^{p-2} \chi(s)[\chi(1+s)]^{k-r-1} = \sum_{u=1}^{p-2} \chi(-u)[\chi(1+u)]^{r-k} = \varepsilon\psi_{k-r-1} .$$

This completes the proof of Lemma 1.

We now introduce the following sum

$$(6) \qquad S_r(i,j) = \sum_{h=0}^{p-1} \chi(i-h)[\chi(h-j)]^r \qquad (r = 1(1)k) .$$

LEMMA 2.

$$S_r(i,j) = \begin{cases} \varepsilon(p\delta_i^j - 1) & \text{if } r = k-1 \\ [\chi(i-j)]^{r+i}\psi_r & \text{otherwise} . \end{cases}$$

Proof. Suppose first that $i = j$ then

$$S_r(i,j) = S_r(i,i) = \varepsilon \sum_{h=0}^{p-1} [\chi(h-i)]^{r+1} .$$

By (2) the sum is $p-1$ or 0 according as $r = k-1$ or not. Next we let $i \neq j$ and make the substitution

$$h \equiv i + (i-j)s \pmod{p}$$

in (6)

$$S_r(i,j) = \sum_{s=0}^{p-1} \chi(j-i)\chi(s)[\chi(i-j)\chi(1+s)]^r$$

$$= \varepsilon[\chi(i-j)]^{r+1}\sum_{s=1}^{p-1}\chi(s)[\chi(1+s)]^r$$
$$= \varepsilon[\chi(i-j)]^{r+1}\psi_{k-r-1} = [\chi(i-j)]^{r+1}\psi_r$$

by Lemma 1. If $r = k-1$ this is $-\varepsilon$ by Lemma 1.

THEOREM 3. *Let M be the matrix whose general element is $a_{ij} = \chi(i-j)$ and let $a_{ij}^{(r)}$ be the general element of M^r. Then, if $1 \leq r \leq k-1$,*

$$a_{ij}^{(r)} = \Pi_{r-1}\chi^r(i-j) - \sum_{\mu=1}^{r-1}\Pi_{r-\mu-1}\Pi_{\mu-1}\chi^\mu(i)\chi^{r-\mu}(-j)$$

where

$$\Pi_m = \psi_1\psi_2\cdots\psi_m .$$

Proof. The theorem is true for $r = 1$. If true for $r < k-1$ it may be proved true for $r+1$ as follows.

$$a_{ij}^{(r+1)} = \sum_{h=1}^{p-1} a_{ih}a_{hj}^{(r)}$$
$$= \Pi_{r-1}\sum_{h=1}^{p-1}\chi(i-h)[\chi(h-j)]^r$$
$$- \sum_{\mu=1}^{r-1}\Pi_{r-\mu-1}\Pi_{\mu-1}\sum_{h=1}^{p-1}\chi(i-h)[\chi(h)]^\mu[\chi(-j)]^{r-\mu}$$
$$= \Pi_{r-1}[S_r(i,j) - \chi(i)[\chi(-j)]^r]$$
$$- \sum_{\mu=1}^{r-1}\Pi_{r-\mu-1}\Pi_{\mu-1}S_\mu(i,0)[\chi(-j)]^{r-\mu} .$$

Applying Lemma 2 we find

$$a_{ij}^{(r+1)} = \Pi_{r-1}[\chi(i-j)]^{r+1}\psi_r - \chi(i)\Pi_{r-1}[\chi(-j)]^r$$
$$- \sum_{\mu=1}^{r-1}\Pi_{r-\mu-1}\Pi_{\mu-1}[\chi(i)]^{1+\mu}\psi_\mu\chi(-j)^{r-\mu}$$
$$= \Pi^r[\chi(i-j)]^{r+1} - \sum_{\nu=1}^{r}\Pi_{r-\nu}\Pi_{\nu-1}[\chi(i)]^\nu[\chi(-j)]^{r+1-\nu} .$$

Thus the induction is complete.

As might be expected, the matrix M^k has an entirely different structure. In fact we have

THEOREM 4. $a_{ij}^{(k)} = \varepsilon\Pi_{k-2}\{p\delta_i^j - k\delta_{\chi(i)}^{\chi(j)}\}$.

Proof. By Theorem 3 with $r = k-1$

$$a_{ij}^{(k)} = \sum_{h=1}^{p-1} a_{ih}a_{hj}^{(k-1)}$$
$$= \Pi_{k-2}\sum_{h=1}^{p-1}\chi(i-h)[\chi(h-j)]^{k-1}$$

$$
\begin{aligned}
&- \sum_{\mu=1}^{k-2} \Pi_{k-\mu-2}\Pi_{\mu-1} \sum_{h=1}^{p-1} \chi(i-h)[\chi(h)]^{\mu}[\chi(-j)]^{k-1-\mu} \\
&= \Pi_{k-2}[S_{k-1}(i,j) - \chi(i)[\chi(-j)]^{k-1}] \\
&\quad - \sum_{\mu=1}^{k-2} \Pi_{k-2-\mu}\Pi_{\mu-1} S_{\mu}(i,0)[\chi(-j)]^{k-1-\mu} .
\end{aligned}
$$

By Lemma 2

$$
\Pi_{k-2-\mu}\Pi_{\mu-1}S_{\mu}(i,0) = [\chi(i)]^{1+\mu}\Pi_{\mu}\Pi_{k-2-\mu} .
$$

But by Lemma 1

$$
\begin{aligned}
\Pi_{\mu}\Pi_{k-2-\mu} &= \prod_{\lambda=1}^{\mu} \psi_{\lambda} \prod_{\lambda=1}^{k-2-\mu} \psi_{k-\mu-1-\lambda} \\
&= \prod_{\lambda=1}^{\mu} \psi_{\lambda} \prod_{\lambda=1}^{k-2-\mu} \psi_{\lambda+\mu}\varepsilon_k^{k-2-\mu} \\
&= \varepsilon^{k-\mu}\Pi_{k-2} .
\end{aligned}
$$

Substituting back into our expression for $a_{ij}^{(k)}$ and using (6) and (4) we have

$$
\begin{aligned}
a_{ij}^{(k)} &= \Pi_{k-2}\Big\{\varepsilon(p\delta_i^j - 1) - \varepsilon\chi(i)[\chi(j)]^{k-1} - \varepsilon\sum_{\mu=1}^{k-2}[\chi(i)]^{1+\mu}[\chi(j)]^{k-1-\mu}\Big\} \\
&= \varepsilon\Pi_{k-2}\Big\{p\delta_i^j - \sum_{\nu=0}^{k-1}[\chi(i/j)]^{\nu}\Big\} = \varepsilon\Pi_{k-2}\{p\delta_i^j - k\delta_{\chi(i)}^{\chi(j)}\}
\end{aligned}
$$

which is the theorem.

We now consider powers of the matrix M^k.

THEOREM 5. *The general element of $M^{k\nu}$ is given by*

$$
a_{ij}^{(k\nu)} = \varepsilon^{\nu}\Pi_{k-2}^{\nu}\{p^{\nu}\delta_i^j - k[(p^{\nu}-1)/(p-1)]\delta_{\chi(i)}^{\chi(j)}\} .
$$

Proof. For simplicity we write $\sigma(p^{\nu-1})$ for $(p^{\nu}-1)/(p-1) = 1 + p + \cdots + p^{\nu-1}$.

Let

$$
b_{ij} = p\delta_i^j - k\delta_{\chi(i)}^{\chi(j)} .
$$

By Theorem 4 it suffices to show that

$$
b_{ij}^{(\nu)} = p^{\nu}\delta_i^j - k\sigma(p^{\nu-1})\delta_{\chi(i)}^{\chi(j)} .
$$

This is true for $\nu = 1$. If true for $\nu = m$ we may write

$$
\begin{aligned}
b_{ij}^{(m+1)} &= \sum_{h=1}^{p-1} b_{ih}b_{hj}^{(m)} = \sum_{h=1}^{p-1} \{p\delta_i^h - k\delta_{\chi(i)}^{\chi(h)}\}\{p^m\delta_h^j - k\sigma(p^{m-1})\delta_{\chi(h)}^{\chi(j)}\} \\
&= p^{m+1}\delta_i^j - k(p^m + p\sigma(p^{m-1}) + k\frac{p-1}{k}\sigma(p^{m-1}))\delta_{\chi(i)}^{\chi(j)} \\
&= p^{m+1}\delta_i^j - k\sigma(p^m)\delta_{\chi(i)}^{\chi(j)} .
\end{aligned}
$$

Thus the induction from m to $m+1$ is complete.

THEOREM 6. *The characteristic polynomial of* M,

$$F(\lambda) = |\chi(i-j) - \lambda\delta_i^j| ,$$

is a polynomial of degree t *in* λ^k.

Proof. It suffices to prove that $F(\lambda) = F(\alpha^{-1}\lambda)$. For if

$$F(\lambda) = \sum_{n=0}^{p-1} a_n\lambda^n = \sum_{n=0}^{p-1} a_n\alpha^{-n}\lambda^n$$

so that

$$a_n(\alpha^n - 1) = 0 ,$$

it follows that $a_n = 0$ if n is not a multiple of k. Now

$$\begin{aligned} F(\lambda\alpha^{-1}) &= |\chi(i-j) - \lambda\alpha^{-1}\delta_i^j| \\ &= |\alpha\chi(i-j) - \lambda\delta_i^j| \end{aligned}$$

and

$$\alpha\chi(i-j) = \chi(g)\chi(i-j) = \chi(gi-gj) .$$

If now we permute the rows of the determinant $F(\lambda)$, replacing the ith row by the i'th where $i' \equiv gi \pmod p$ and then the columns, replacing the jth column by the j'th where $j' \equiv gj \pmod p$ we obtain a new matrix $M' - \lambda I$ whose general element is

$$\chi(gi-gj) - \lambda\delta_{gi}^{gj} = \alpha\chi(i-j) - \lambda\delta_i^j .$$

Since the two determinants are identical we have $F(\lambda) \equiv F(\alpha^{-1}\lambda)$.

We are now able to determine the characteristic roots of M without any difficulty.

THEOREM 7. *The characteristic roots of* $M = \{\chi(i-j)\}$ *are the* kth *roots of* $\varepsilon\Pi_{k-2}$ *and the* kth *roots of* $\varepsilon p\Pi_{k-2}$, *the latter roots each having multiplicity* $t-1$. *That is, the characteristic polynomial of* M *is*

$$|M - \lambda I| = (\lambda^k - \varepsilon\Pi_{k-2})(\lambda^k - \varepsilon p\Pi_{k-2})^{t-1} .$$

Proof. By Theorem 6 it suffices to show that

$$|M^k - \lambda I| = (\lambda - \varepsilon\Pi_{k-2})^k(\lambda - \varepsilon p\Pi_{k-2})^{p-1-k} . \tag{7}$$

Now the trace of $M^{k\nu}$ is the sum of the νth powers of the characteristic roots of M^k and is, by Theorem 5

$$\sum_{i=1}^{p-1} a_{ii}^{(k\nu)} = \varepsilon^{\nu}\Pi_{k-2}^{\nu}\left[p^{\nu} - k\frac{p^{\nu}-1}{p-1}\right](p-1)$$
$$= k(\varepsilon\Pi_{k-2})^{\nu} + (p-1-k)(\varepsilon p\Pi_{k-2})^{\nu} .$$

This being true for all integers ν it follows that the quantities raised to the νth power are the roots of M^k with the indicated multiplicities. This established (7) and hence the theorem.

THEOREM 8. *The determinant of* $M = \{\chi(i-j)\}$ *is* $p^{t-1}\Pi_{k-2}^{t}$.

Proof. Setting $\lambda = 0$ in Theorem 7 we find

$$|M| = (-\varepsilon)^t \Pi_{k-2}^{t} p^{t-1} .$$

But, by (3),

$$(-\varepsilon)^t = (-1)^{t^2+t} = 1 .$$

COROLLARY. *If* ν *is any positive integer, the determinant*

$$\left| p^{\nu}\delta_i^j - k\frac{p^{\nu}-1}{p-1}\delta_{\chi(i)}^{\chi(j)} \right| = p^{(p-1-k)\nu} .$$

Proof. This follows by combining Theorem 8 with Theorem 5. Theorem 8 was proved by L. Carlitz [1] in quite a different way.

THEOREM 9. *The inverse of* M *has for its general element*

$$a_{ij}^{(-1)} = \varepsilon p^{-1}[\bar{\chi}(i-j) - \bar{\chi}(i) - \bar{\chi}(-j)] . \tag{8}$$

Proof. If we denote the right-hand member of (8) by c_{ij} we find

$$\sum_{h=1}^{p-1} a_{ih}c_{hj} = \varepsilon p^{-1}\sum_{h=1}^{p-1}\{\chi(i-h)([\chi(h-j)]^{k-1} - [\chi(h)]^{k-1} - [\chi(-j)]^{k-1})\}$$
$$= \varepsilon p^{-1}\{S_{k-1}(i,j) - \chi(i)[\chi(-j)]^{k-1} - S_{k-1}(i,0) + \chi(i)[\chi(-j)]^{k-1}\}$$
$$= \varepsilon p^{-1}\{\varepsilon(p-1)\delta_i^j + (1-\delta_i^j)(-\varepsilon) - (-\varepsilon)\}$$
$$= p^{-1}[p\delta_i^j] = \delta_i^j .$$

If we make use of a little more cyclotomy we can give a variant of Theorem 7 in terms of pth roots of unity. Let

$$\rho = e^{2\pi i/p}$$

then the Lagrange resolvent (α^r, ρ) is defined by

$$(\alpha^r, \rho) = \sum_{h=1}^{p-1}[\chi(h)]^r\rho^h .$$

LEMMA 3.

$$(\alpha, \rho)(\alpha^r, \rho) = \begin{cases} (\alpha^{r+1}, \rho)\psi_r & \text{if } r = 1(1)k-2 \\ \varepsilon p & \text{if } r = k-1 . \end{cases}$$

Proof.

$$(\alpha, \rho)(\alpha^r, \rho) = \sum_{i=0}^{p-1} \rho^i \sum_{h=0}^{p-1} \chi(i-h)[\chi(h)]^r$$
$$= \sum_{i=0}^{p-1} \rho^i S_r(i, 0) .$$

If $r = k-1$ we have by Lemma 1,

$$\sum_{i=1}^{p-1} \rho^i S_{k-1}(i, 0) = S_{k-1}(0, 0) + \sum_{i=1}^{p-1} \rho^i \psi_{k-1} = \varepsilon(p-1) - (-\varepsilon) = \varepsilon p .$$

If $r < k-1$

$$\sum_{i=0}^{p-1} \rho^i S_r(i, 0) = \psi_r \sum_{i=1}^{p-1} [\chi(i)]^{r+1} \rho^i = (\alpha^{r+1}, \rho)\psi_r .$$

LEMMA 4. $\varepsilon p \Pi_{k-2} = (\alpha, \rho)^k$.

Proof. By Lemma 3

$$\prod_{r=1}^{k-1} \{(\alpha, \rho)(\alpha^r, \rho)\} = \Pi_{k-2} \varepsilon p \prod_{r=2}^{k-1} (\alpha^r, \rho) .$$

Cancellation gives

$$(\alpha, \rho)^k = \varepsilon p \Pi_{k-2} .$$

We may now restate Theorem 7 as follows.

THEOREM 10. *The characteristic roots of M are*

$$(\alpha, \rho)\alpha^r \text{ and } |p^{-1/k}|(\alpha, \rho)\alpha^r \qquad (r = 0\ (1)k-1)$$

each of the second set having multiplicity $t-1$.

THEOREM 11. *The determinant of M is $\varepsilon(\alpha, \rho)^{p-1}/p$.*

EXAMPLES. For small values of k it is possible to give more or less precise formulas for ψ_r and hence to give more specific information about the matrix $M = \{\chi(i-j)\}$.

For $k = 2$ the product Π_{k-2} is empty. There is only one character function χ, Legendre's symbol, and the matrix M is independent of the choice of primitive roots g of p. Theorem 7 tells us that the characteristic equation of M is

$$|M - \lambda I| = (\lambda^2 - (-1)^{(p-1)/2})(\lambda^2 - (-1)^{(p-1)/2}p)^{(p-3)/2} .$$

We note incidentally that the characteristic roots of M are real if and only if $\chi(i-j)=\chi(j-i)$, that is if and only if M is symmetric. The determinant of M is $p^{(p-3)/2}$.

When $k>2$ the matrix M will depend upon the particular choice of g. This choice affects the values of ψ_r and Π_{k-2}. For example if $k=3$ and $p=13$ we find that

$$\Pi_{k-2}=\psi_1=\begin{cases}-4-3\omega & \text{if } g=2 \text{ or } 11\\ -4-3\omega^2 & \text{if } g=6 \text{ or } 7\,.\end{cases}$$

For small k, ψ_r can be expressed in terms of certain "quadratic partitions" of p which have been tabulated. These expressions sometimes contain unfortunate ambiguities as we shall see. In case 2 is not a kth power these ambiguities can be eliminated by a method suggested by Emma Lehmer [5]. The proofs of the following results will be included in a paper by her on Jacobi Functions, [6].

For $k=3$ Carlitz gives the formula

$$\psi_1=a+b\omega \text{ or } a+b\omega^2$$

where

$$a^2-ab+b^2=p \quad (a\equiv -1 \pmod 3 \quad b\equiv 0 \pmod 3)\,.$$

There are, in fact, two pairs (a, b) and $(a-b, -b)$ with this property. In case 2 is not cube modulo p this ambiguous statement can be made unequivocal as follows.

THEOREM 12. *For $k=3$ let $p=3t+1$ be a prime having 2 as a cubic non-residue, so that, uniquely*

$$p=A^2+3B^2 \qquad (A\equiv B\equiv 1 \pmod 3)\,.$$

Then

$$\psi_1=2B+(B-A)\chi(2)\,.$$

Cunningham [3] gives values of $|A|$ and $|B|$ for all $p<100000$. If 2 is a cubic residue of p these is no non-ambiguous formula for ψ_1 known. The first three primes not covered by Theorem 12 are $p=31, 43$, and 109. For these, ψ_1 has the following values.

$$\begin{aligned} p&=31 \quad \psi_1=5+6\chi(3)\\ p&=43 \quad \psi_1=-1+6\chi(3)\\ p&=109 \quad \psi_1=-7-12\chi(3)\,.\end{aligned}$$

For $k=4$ Carlitz's formulas for ψ_1 and ψ_2 are not only ambiguous but slightly incorrect. We can state ambiguously

$$\psi_1 = -(a \pm ib) = (-1)^{(p-1)/4}\psi_2$$

where

$$a^2 + b^2 = p \qquad a \equiv 1 \pmod 4 .$$

Again, if 2 is not a quartic residue of p, we can give the following precise determinations of ψ_1 and ψ_2.

THEOREM 13. *Let 2 be a quadratic non-residue of* $p = 4t + 1$. *If 2 is a quadratic non-residue so that, uniquely*

$$p = a^2 + b^2 \qquad (a \equiv b/2 \equiv 1 \pmod 4)$$

then

$$\psi_1 = -(a + b\chi(2)) = -\psi_2 .$$

If 2 is a quadratic residue of p so that

$$2 \equiv m^2 \pmod p$$

and, uniquely,

$$p = a^2 + b^2 \quad (a \equiv 1 \pmod 4), \quad b/4 \equiv (-1)^{(p-1)/8} \pmod 4 ,$$

then

$$\psi_1 = -(a + b\chi(m)) = \psi_2 .$$

The first two primes not covered by Theorem 13 are 73 and 89. Here we find

$$p = 73, \qquad \psi_1 = 3 + 8\chi(5) = \psi_2 .$$
$$p = 89, \qquad \psi_1 = -5 + 8\chi(3) = \psi_2 .$$

Cunningham [3] gives $|a|$ and $|b|$ for all $p < 100000$.

For $k = 5$, the functions ψ_1, ψ_2 and $\psi_3 = \psi_1$ can be made to depend on the integers x, u, v, w in the representation

$$16p = x^2 + 50u^2 + 50v^2 + 125w^2 \tag{9}$$

where

$$xw = v^2 - u^2 - 4uv \tag{10}$$

and

$$x \equiv 1 \pmod 5 . \tag{11}$$

In fact if we set

$$\theta_1 = \sqrt{10 + 2\sqrt{5}} = 4 \sin 72°$$
$$\theta_2 = \sqrt{10 - 2\sqrt{5}} = 4 \sin 36°$$

then

$$4\psi_1 = x + 5\sqrt{5w} + i\{(u+2v)\theta_1 + (2u-v)\theta_2\} = 4\psi_3 \tag{12}$$

$$4\psi_2 = x - 5\sqrt{5w} + i\{(v-2u)\theta_1 + (u+2v)\theta_2\} \tag{13}$$

$$64\Pi_3 = 64\psi_1^2\psi_2 = (x^3 - 625xw^2 - 2500uvw - 8px)$$

$$-10\sqrt{5}(125w^3 + 3x^2w + 20xuv - 8pw) \tag{14}$$

$$+ i\{[5vx^2 - 125w^2(4u+3v) - 50xw(2u-v) - 500u^2v]\theta_1$$

$$+ [5ux^2 - 125w^2(3u-4v) - 50xw(u+2v) - 500uv^2]\theta_2\} .$$

Unfortunately these statements are ambiguous. In fact if

$$\text{(I)} \quad (x, u, v, w)$$

is any solution of (9) subject to (10) and (11) then all solutions are given by (I) and

$$\text{(II)} \quad (x, v, -u, -w)$$

$$\text{(III)} \quad (x, -v, u, -w)$$

$$\text{(IV)} \quad (x, -u, -v, w) .$$

In case 2 is not a quintic residue of p the ambiguity can be removed as follows.

THEOREM 14. *Let* (x, u, v, w) *be that solution of* (9), (10) *and* (11) *for which* $u \equiv 0 \pmod 2$ *and* $v \equiv x + u \pmod 4$. *Then in* (12), (13) *and* (14) *replace* (x, u, v, w) *by* (I), (II), (III), *or* (IV) *according as* $\operatorname{ind} 2 \equiv 1$, 2, 3 *or* $4 \pmod 5$ *to eliminate ambiguity.*

For example, if $p = 31$ and $g = 12$ for which $\operatorname{ind} 2 = 6 \equiv 1 \pmod 5$ we take the solution

$$(x, u, v, w) = (11, 2, 1, -1)$$

of (9). Then (12), (13) and (14) give.

$$4\psi_1 = 11 - 5\sqrt{5} + (4\theta_1 + 3\theta_2)i$$

$$4\psi_2 = 11 + 5\sqrt{5} - (3\theta_1 - 4\theta_2)i$$

$$16\Pi_3 = -409 - 125\sqrt{5} - 5(14\theta_1 - 27\theta_2)i.$$

If, on the other hand, we choose $g = 3$, the least primitive root of 31, then $\operatorname{ind} 2 = 24 \equiv 4 \pmod 5$. In this case we must take solution IV namely $(11, -2, -1, -1)$. Now the former ψ_1, ψ_2 and Π_3 are replaced by their complex conjugates. The choices of $g = 11$ or 17 give a different pair of conjugate values.

There is no extensive table of (x, u, v, w) in (9). However these values may be obtained from tables of Tanner [7] for $p < 10000$.

In terms of his $(q_0, q_1, q_2, q_3, q_4)$ one has.

$$x = 5q_0 + 1$$
$$5u = q_1 + 2q_2 - 2q_3 - q_4$$
$$5v = 2q_1 - q_2 + q_3 - 2q_4$$
$$5w = q_1 - q_2 - q_3 + q_4 .$$

As a matter of fact,

$$\psi_1 = q_0 + q_1\alpha + q_2\alpha^2 + q_3\alpha^3 + q_4\alpha^4$$
$$\psi_2 = q_0 + q_3\alpha + q_1\alpha^2 + q_4\alpha^3 + q_2\alpha^4$$

for some choices of primitive roots, not specified.

Finally we consider the case of $k = 6$. This case depends directly on the case $k = 3$. By Lemma 1

$$\Pi_4 = (\psi_1\psi_2)^2 .$$

Also

$$\psi_2 = \chi(-4)\psi_1$$

and

$$\psi_1 = \chi(-4)\psi_1^*$$

where ψ_1^* is the function ψ_1 for $k = 3$. Hence

$$\Pi_4 = (\psi_1^*)^4 .$$

Since the above was submitted for publication, a paper by Carlitz [2] has appeared in which a proof of Theorem 10 is given by a different method. Less explicit results are given for the more general matrices $\{c + \chi(i - j)\}$ and $\{c + \chi(a + i + j)\}$. There is also a proof of Theorem 2 for $k = 2$.

BIBLIOGRAPHY

1. L. Carlitz, *Some cyclotomic determinants*, Calcutta Math. Soc. Bull., **49** (1957), 49–51.
2. ———, *Some cyclotomic matrices*, Acta Arithmetica, **5** (1959), 292–308.
3. A. J. C. Cunningham, *Quadratic Partitions*, London 1904.
4. D. H. Lehmer, *On certain character matrices*, Pacific. J. Math., **6**, (1956), 491–499.
5. Emma Lehmer, *On Euler's criterion*, Australian Journal of Math., **1** (1959), 64–70.
6. ———, *Jacobi Functions*, Pacific J. Math. **10** (1960), pp. 887–893.
7. H. W. L. Tanner, *On the binomial equation* $x^p - 1 = 0$: *quinquisection*, London Math. Soc., Proc. s.l., **18** (1887), 214–234, *Complex primes formed with the fifth roots of unity*, Ibid. **24** (1893), 223–272.

PACIFIC JOURNAL OF MATHEMATICS

Mathematical papers intended for publication in the *Pacific Journal of Mathematics* should be typewritten (double spaced), and the author should keep a complete copy. Manuscripts may be sent to any one of the four editors. All other communications to the editors should be addressed to the managing editor, L. J. Paige at the University of California, Los Angeles 24, California.

50 reprints per author of each article are furnished free of charge; additional copies may be obtained at cost in multiples of 50.

The *Pacific Journal of Mathematics* is published quarterly, in March, June, September, and December. The price per volume (4 numbers) is $12.00; single issues, $3.50. Back numbers are available. Special price to individual faculty members of supporting institutions and to individual members of the American Mathematical Society: $4.00 per volume; single issues, $1.25.

Subscriptions, orders for back numbers, and changes of address should be sent to Pacific Journal of Mathematics, 2120 Oxford Street, Berkeley 4, California.

Printed at Kokusai Bunken Insatsusha (International Academic Printing Co., Ltd.), No. 6, 2-chome, Fujimi-cho, Chiyoda-ku, Tokyo, Japan.

PUBLISHED BY PACIFIC JOURNAL OF MATHEMATICS, A NON-PROFIT CORPORATION

The Supporting Institutions listed above contribute to the cost of publication of this Journal, but they are not owners or publishers and have no responsibility for its content or policies.

Pacific Journal of Mathematics
Vol. 10, No. 3 November, 1960