Pacific Journal of Mathematics

ON CERTAIN CHARACTER MATRICES

D. H. LEHMER

Vol. 6, No. 3 BadMonth 1956

ON CERTAIN CHARACTER MATRICES

D. H. LEHMER

For only a very limited class of matrices M is it possible to give explicit formulas for the determinant, characteristic roots and inverse of M as well as the general element of M^k. Nontrivial instances of such sets of matrices are useful as examples in testing the correctness and efficacy of various matrix computing routines especially when the elements are small integers or simple rational numbers. The purpose of this paper is to indicate two new classes of such matrices which arise from the theory of exponential sums and have as general elements simple functions involving real nonprinciple characters or Legendre symbols.

The same method of determining characteristic roots is used for both types of matrices. It depends on the fact that the roots of a polynomial are determined by the sums of their like powers. That is, if S_k denotes the sum of the kth powers of the roots of a polynomial of degree n and if complex numbers $\rho_1, \rho_2, \cdots, \rho_n$ are exhibited for which

$$\sum_{i=1}^{n} \rho_i^k = S_k \qquad (k=1, \cdots, n) ,$$

then the ρ_i are the roots of the polynomial.

All matrices M are square and of order $p-1$ where p is an odd prime. Their elements involve Legendre's symbol $\chi(n)$ defined by

$$\chi(n)=\left(\frac{n}{p}\right)=\begin{cases} 0 \text{ if } p \text{ divides } n \\ -1 \text{ if the congruence } x^2 \equiv n \pmod{p} \text{ is impossible} \\ +1 \text{ otherwise} \end{cases}$$

Thus for $p=7$

$$\chi(0)=0 \qquad \chi(1)=1 \qquad \chi(2)=1 \qquad \chi(3)=-1$$

$$\chi(4)=1 \qquad \chi(5)=-1 \quad \chi(6)=-1 .$$

Besides the simple properties

$$\chi(i)\chi(j)=\chi(ij)$$

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

Received August 26, 1955. A part of the results of this paper were obtained in 1952 under a contract between the Office of Naval Research and the National Bureau of Standards.

we use the following identities

$$(1)\qquad \sum_{k=1}^{p-1}\chi(n+k)=-\chi(n)$$

$$(2)\qquad \sum_{k=1}^{p-1}\chi(m+k)\chi(n+k)=\delta_m^n-\chi(m)\chi(n)-1$$

where δ_m^n is Kronecker's delta mod p, that is

$$\delta_a^b=\begin{cases}1 \text{ if } a\equiv b \pmod p\\ 0 \text{ otherwise .}\end{cases}$$

Identity (1) states the familiar fact that there are as many quadratic residues as non-residues of p.

Identity (2) is apparently due to Jacobsthal [1] and a simple proof is given in § 4.

2. Matrices of the first kind. Let a, b, c, d be any four numbers. We consider the matrix $M=M(a, b, c, d)$ whose general element a_{ij} is

$$a_{ij}=a+b\chi(i)+c\chi(j)+d\chi(ij)$$

and denote the general element of M^k by $a_{ij}^{(k)}$.

THEOREM 1. *The general element of* $M^k(a, b, c, d)$ *is*

$$a_{ij}^{(k)}=(p-1)^{k-1}\{a_k+b_k\chi(i)+c_k\chi(j)+d_k\chi(ij)\}$$

where k *is a positive integer and*

$$\begin{pmatrix}a_k & b_k\\ c_k & d_k\end{pmatrix}=\begin{pmatrix}a & b\\ c & d\end{pmatrix}^k$$

Proof. The assertion of the theorem is trivial for the case $k=1$. If true for $k=n$, we have

$$a_{ij}^{(n+1)}=\sum_{r=1}^{p-1}a_{ir}a_{rj}^{(n)}$$
$$=\sum_{r=1}^{p-1}\{a+b\chi(i)+c\chi(r)+d\chi(ir)\}\{a_n+b_n\chi(r)+c_n\chi(j)+d_n\chi(rj)\}\,.$$

Multiplying together the two factors under summation and using the facts that

$$(3)\qquad \chi^2(r)=1\,,\qquad \sum_{r=1}^{p-1}\chi(r)=0$$

we find

$$a_{ij}^{(n+1)}=(p-1)[A+B\chi(i)+C\chi(j)+D\chi(ij)] ,$$

where

$$A=aa_n+cb_n \qquad B=ba_n+db_n$$

$$C=ac_n+cd_n \qquad D=bc_n+dd_n$$

Hence

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix}=\begin{pmatrix} a_n & b_n \\ c_n & d_n \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}=\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{n+1},$$

Thus the induction from n to $n+1$ is completed.

THEOREM 2. *The characteristic roots of* $M(a, b, c, d)$ are

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

where ρ_1, ρ_2 *are the characteristic roots of the matrix*

$$N=\begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

that is, ρ_1, ρ_2 *are the roots of the equation*

$$\lambda^2-(a+b)\lambda+ad-bc=0 .$$

Proof. Let k be any positive integer, and denote by σ_k the sum of the kth powers of the characteristic roots of $M(a, b, c, d)$. Since σ_k is thus the trace of M^k we have by Theorem 1

$$\sigma_k=\sum_{i=1}^{p-1} a_{ii}^{(k)}=(p-1)^{k-1}\sum_{i=1}^{p-1}\{a_k+b_k\chi(i)+c_k\chi(i)+d_k\chi(i^2)\}=(p-1)^k(a_k+d_k)$$

by (3).

Now a_k+d_k, being the trace of N^k, has the value $\rho_1^k+\rho_2^k$ where ρ_1,ρ_2 are the characteristic roots of N.

Therefore

$$\sigma_k=\{(p-1)\rho_1\}^k+\{(p-1)\rho_2\}^k+0^k+\cdots+0^k .$$

Since this holds for all positive integers k and since the roots of a polynomial are determined by their sums of powers, it follows that the characteristic roots of M are those specified in the conclusion of the theorem.

Except for the case $p=3$ the matrix $M(a, b, c, d)$ is singular and so has no inverse. For $p=3$ the characteristic roots being, $2\rho_1$, $2\rho_2$ the determinant of M is $4\rho_1\rho_2=4(ad-bc)$ and its inverse (assuming that $ad-bc\neq 0$) is given by

$$4(ad-bc)M^{-1}=\begin{pmatrix} a-b-c+d & -a-b+c+d \\ -a+b-c+d & a+b+c+d \end{pmatrix} .$$

The rank of M which is in general 2 will becomc 1 if and only if $ad-bc=0$; that is, if and only if the general term is a product of two factors

$$a_{ii}=\{x+y\chi(i)\}\{z+w\chi(j)\} .$$

3. Matrices of the second kind. Let c be any constant and α an integer. We define $A_p=A_p(c, \alpha)$ as the matrix whose general element is

$$a_{ij}=c+\chi(\alpha+i+j) .$$

The properties of this matrix are more recondite than those of $M(a, b, c, d)$. The general element $a_{ij}^{(2)}$ of A_p^2 is not of the same form as a_{ij} but is

$$\begin{aligned} a_{ij}^{(2)}&=\sum_{r=1}^{p-1}\{c+\chi(\alpha+i+r)\}\{c+\chi(\alpha+r+j)\} \\ &=(p-1)c^2-1-c[\chi(\alpha+i)+\chi(\alpha+j)]-\chi(\alpha+i)\chi(\alpha+j)+p\delta_i^j \end{aligned}$$

as we see by applying (2). This prompts us to define a function $\psi_k(i, j)$ and three sequences C_k, S_k and P_k by

$$(4) \qquad \psi_k(i, j)=\begin{cases} p^{k/2}\delta_i^j & \text{if } k \text{ is even} \\ p^{(k-1)/2}\chi(\alpha+i+j) & \text{if } k \text{ is odd} \end{cases}$$

$$(5) \qquad a_{ij}^{(k)}=C_k+S_k[\chi(\alpha+i)+\chi(\alpha+j)]+P_k\chi(\alpha+i)\chi(\alpha+j)+\psi_k(i, j)$$

so that initially

$$(6) \qquad \begin{matrix} C_0=0 & C_1=c & C_2=(p-1)c^2-1 \\ S_0=0 & S_1=0 & S_2=-c \\ P_0=0 & P_1=0 & P_2=-1 . \end{matrix}$$

If we substitute from (4) and (5) into the relation

$$a_{ij}^{(k+1)}=\sum_{r=1}^{p-1}a_{ir}a_{rj}^{(k)}$$

we are led to a system of difference equations to determine C_k, S_k and P_k. Because of the nature of the function ψ these depend upon the parity of k. Setting $k=2m$ and $2m+1$ in turn we find

$$C_{2m+1}=(p-1)cC_{2m}-[1+c\chi(\alpha)]S_{2m}+cp^m$$

$$S_{2m+1}=(p-1)cS_{2m}-[1+c\chi(\alpha)]P_{2m}=-\chi(\alpha)S_{2m}-C_{2m}$$

$$P_{2m+1}=-S_{2m}-\chi(\alpha)P_{2m}$$

and

$$C_{2m+2}=(p-1)cC_{2m+1}-[1+c\chi(\alpha)]S_{2m+1}-p^m$$

$$S_{2m+2}=(p-1)cS_{2m+1}-[1+c\chi(\alpha)]P_{2m+1}-cp^m$$

$$=-\chi(\alpha)S_{2m+1}-C_{2m+1}$$

$$P_{2m+2}=-S_{2m+1}-\chi(\alpha)P_{2m+1}-p^m \ .$$

For simplicity in what follows we write χ for $\chi(\alpha)$. By simple elimination the above equations may be replaced by second order ones in which the variables are separated as follows.

(7) $$C_{2m+1}=AC_{2m}+BC_{2m-1}+(cp-\chi)p^{m-1}$$

(8) $$C_{2m+2}=AC_{2m+1}+BC_{2m}+(c\chi-1)p^m$$

(9) $$S_{2m+1}=AS_{2m}+BS_{2m-1}+p^{m-1}$$

(10) $$S_{2m+2}=AS_{2m+1}+BS_{2m}-cp^m$$

(11) $$P_{2m+1}=AP_{2m}+BP_{2m-1}+cp^m$$

(12) $$P_{2m+2}=AP_{2m+1}+BP_{2m}-p^m$$

where we have written

(13) $$c(p-1)-\chi=A \qquad cp\chi+1=B \ .$$

We define a sequence W_k by

$$W_k=(p-1)C_k-2\chi S_k+(p-1-\chi^2)P_k$$

so that

$$W_0=0 \ , \qquad W_1=c(p-1) \ ,$$

and a sequence T_k by

$$T_{2m+1}=W_{2m+1}-\chi p^m$$

(14) $$T_{2m}=W_{2m}+(p-1)p^m$$

with initial values

$$T_0=p-1\ ,\qquad T_1=A\ .$$

From (7)-(12) we deduce

$$T_{2m+1}=AT_{2m}+BT_{2m-1}-AP^m(p-3)$$

(15) $$T_{2m+2}=AT_{2m+1}+BT_{2m}+(p-B)p^m(p-3)\ .$$

This suggests a final substitution:

(16) $$V_k=\begin{cases}T_k-(p-3)p^{k/2} & \text{if } k \text{ is even}\\ T_k & \text{if } k \text{ is odd}\end{cases}$$

in terms of which (15) becomes simply

$$V_{k+1}=AV_k+BV_{k-1}$$

with

$$V_0=2\ ,\qquad V_1=A\ .$$

We are now in a position to prove the following.

THEOREM 3. *The characteristic roots of the matrix*

$$A_p=(a_{ij})=(c+\chi(\alpha+i+j))$$

consist in $p^{1/2}$ *and* $-p^{1/2}$ *each occurring with multiplicities* $(p-3)/2$ *and, in addition, the two roots of the quadratic equation*

$$\lambda^2-[c(p-1)-\chi(\alpha)]\lambda-cp\chi(\alpha)-1=0\ .$$

Using the abbreviations (13) *we may restate the theorem by asserting that the characteristic equation of* A_p *is*

$$(\lambda^2-p)^{(p-3)/2}(\lambda^2-A\lambda-B)=0\ .$$

Proof. We begin by noting that, from the definition (4),

$$\sum_{i=1}^{p-1}\varphi_k(i,i)=\begin{cases}(p-1)p^{k/2} & \text{if } k \text{ is even}\\ -\chi(\alpha)p^{(k-1)/2} & \text{if } k \text{ is odd}\end{cases}$$
$$=T_k-W_k\ .$$

Hence if we set $i=j$ in (5) and sum over i we obtain

$$\sum_{i=1}^{p-1}a_{ii}^{(k)}=(p-1)C_k-2\chi S_k+(p-1-\chi^2)P_k+T_k-W_k=T_k\ .$$

That is to say, the function T_k defined previously by (14) is the trace of the kth power of our matrix A_p.

Turning now to the function V_k, and denoting the two roots of $\lambda^2-A\lambda-B=0$ by ρ_1 and ρ_2 we see that

$$V_0=\rho_1^0+\rho_2^0\ , \qquad V_1=\rho_1+\rho_2$$

and in general by induction from k and $k-1$ to $k+1$

$$V_{k+1}=AV_k+BV_{k-1}=(\rho_1+\rho_2)(\rho_1^k+\rho_2^k)-\rho_1\rho_2(\rho_1^{k-1}+\rho_2^{k-1})=\rho_1^{k+1}+\rho_2^{k+1}\ .$$

Therefore (16) can be written in the form

$$T_k=\rho_1^k+\rho_2^k+\frac{p-3}{2}(p^{1/2})^k+\frac{p-3}{2}(-p^{1/2})^k\ . \tag{17}$$

Since T_k is the trace of A_p^k and so is the sum of kth powers of characteristic roots of A_p, it follows from (17) that these roots must be ρ_1, ρ_2 and $\pm p^{1/2}$ the latter two having multiplicities $(p-3)/2$.

As a corollary to Theorem 3 we obtain the determinant of A_p as the product of its characteristic roots, namely

$$\rho_1\rho_2(-p)^{(p-3)/2}=\chi(-1)Bp^{(p-3)/2}=\chi(-1)[1+cp\chi(\alpha)]p^{(p-3)/2}\ .$$

It follows that A_p is nonsingular provided c is not chosen as the negative reciprocal of $p\chi(\alpha)$, in other words provided $B\neq 0$.

The inverse of A_p is easily obtained. We simply substitute $m=0$ into (7), (9) and (11) and use the initial conditions (6) to find (assuming $B\neq 0$),

$$C_{-1}=\chi(\alpha)/(pB)$$
$$S_{-1}=-1/(pB)$$
$$P_{-1}=-c/B$$

and

$$\psi_{-1}(ij)=\chi(\alpha+i+j)/p\ .$$

Hence for the general element a_{ij}^{-1} of A_p^{-1} we find

$$pBa_{ij}^{-1}=\chi(\alpha)-\chi(\alpha+i)-\chi(\alpha+j)-cp\chi(\alpha+i)\chi(\alpha+j)+B\chi(\alpha+i+j)\ . \tag{18}$$

The reader may wish to verify, as an exercise in the use of (1) and (2), that (18) is indeed correct.

The general element $a_{ij}^{(k)}$ of A_p^k for an arbitrary integer k can be found in the form (5) by solving the difference equations (7)–(12) for C_k, S_k, and P_k as we did for the special combination we denoted by T_k. These functions are linear combinations of the kth powers of the characteristic roots of A_p. Various special cases are sufficiently simple to be interesting and useful. The cases of $c=0$ involve in general the Fibonacci numbers. For $c=0$ and $\alpha=0$ the reader will find that

$$a_{ij}^{(2m)}=p^m\delta_i^j-\frac{p^m-1}{p-1}\{\chi(ij)+1\}$$

(19)
$$a_{ij}^{(2m+1)}=p^m\chi(i+j)+\frac{p^m-1}{p-1}\{\chi(i)+\chi(j)\} .$$

Thus the inverse of the matrix

$$a_{ij}=\chi(i+j)$$

has for its general element

$$a_{ij}^{-1}=[\chi(i+j)-\chi(i)-\chi(j)]/p$$

which comes from putting $m=-1$ into (19).

4. Proof of Jacobsthal's Identity. To prove (2) we may write

$$S(a,\,b)=\sum_{k=0}^{p-1}\chi(a+k)\chi(b+k) .$$

Substituting r for $a+k$ and using the periodicity of χ we obtain

$$S(a,\,b)=S(0,\,b-a) ,$$

so that $S(a, b)$ depends only on the difference between its variables. If this difference is zero we have

$$S(0,\,0)=\sum_{k=0}^{p-1}\chi^2(k)=p-1 .$$

If the difference $b-a=\delta\neq 0$, we replace k by $t\delta$ (mod p) and write

$$S(0,\,\delta)=\sum_{k=0}^{p-1}\chi(k)\chi(\delta+k)=\sum_{t=0}^{p-1}\chi(t\delta)\,\chi(\delta+t\delta)=\chi^2(\delta)\sum_{t=0}^{p-1}\chi(t)\chi(t+1)=S(0,\,1) .$$

Thus $S(0, \delta)$ is not a function of δ. That is

$$(p-1)S(0,\,1)=\sum_{\delta=1}^{p-1}S(0,\delta)=\sum_{k=0}^{p-1}\chi(k)\sum_{\delta=1}^{p-1}\chi(k+\delta)=-\sum_{k=0}^{p-1}\chi^2(k)=-(p-1) .$$

Hence $S(0, \delta)=-1$ if $\delta\neq 0$. Thus in general we have

$$S(a,\,b)=p\delta_a^b-1 .$$

From this (2) follows at once.

The referee has called my attention to the fact that certain matrices of order $p+1=4k$ involving $\chi(i-j)$ have been considered by Payley [2] and Gilman from different point of view. Their results depend also on Jacobsthal's identity.

REFERENCES

1. E. Jacobsthal, *Andwendungen einer Formel aus der Theorie der quadratischen Restc*, Dissertation, Berlin 1906.
2. R. E. A. C. Payley, *On orthogonal matrices*, Jour. Math. Phys. **12** (1933), 311–320.

UNIVERSITY OF CALIFORNIA, BERKELEY

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 of the editors. Manuscripts intended for the outgoing editors should be sent to their successors. All other communications to the editors should be addressed to the managing editor, Alfred Horn at the University of California, Los Angeles 24, California.

50 reprints 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, c/o University of California Press, Berkeley 4, California.

Printed at Kokusai Bunken Insatsusha (International Academic Printing Co., Ltd.), No. 10, 1-chome, Fujimi-cho, Chiyoda-ku, Tokyo, Japan.

* During the absence of E. G. Straus.

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

Pacific Journal of Mathematics
Vol. 6, No. 3 BadMonth, 1956

Richard Arens and James Eells, Jr., *On embedding uniform and topological spaces* . . . 397
N. Aronszajn and Prom Panitchpakdi, *Extension of uniformly continuous transformations and hyperconvex metric spaces* . . . 405
Kai Lai Chung and Cyrus Derman, *Non-recurrent random walks* . . . 441
Harry Herbert Corson, III, *On some special systems of equations* . . . 449
Charles W. Curtis, *On Lie algebras of algebraic linear transformations* . . . 453
Isidore Heller, *Neighbor relations on the convex of cyclic permutations* . . . 467
Solomon Leader, *Convergence topologies for measures and the existence of transition probabilities* . . . 479
D. H. Lehmer, *On certain character matrices* . . . 491
Michael Bahir Maschler, *Minimal domains and their Bergman kernel function* . . . 501
Wm. M. Myers, *Functionals associated with a continuous transformation* . . . 517
Irving Reiner and Jonathan Dean Swift, *Congruence subgroups of matrix groups* . . . 529
Andrew Sobczyk, *Simple families of lines* . . . 541
Charles Standish, *A class of measure preserving transformations* . . . 553
Jeremiah Milton Stark, *On distortion in pseudo-conformal mapping* . . . 565