JOURNAL OF NUMBER THEORY 12, 122–127 (1980)

On the Eigenvectors of Schur's Matrix

PATRICK MORTON*

Department of Mathematics, University of Michigan, Ann Arbor, Michigan 48109

Communicated by D. J. Lewis

Received November 1, 1978

A basis of eigenvectors is given for the matrix $\mathfrak{A} = (e^{2\pi imn/q})$, $(1 \leqslant m, n \leqslant q)$. The eigenvectors arise from the characters on the reduced residue class group (mod q).

In this note we exhibit a simple basis of eigenvectors for the matrix

$$\mathfrak{A} = (e^{2\pi imn/q}) \qquad (1 \leqslant m, n \leqslant q), \tag{1}$$

where q is a positive integer. The eigenvalues of $\mathfrak{A}$ are well known. They are contained among the numbers $i^a q^{1/2}$ for $0 \leqslant a \leqslant 3$ (see [1]), a fact which follows from the observation that $\mathfrak{A}^4 = q^2 I$. Schur [3] used these eigenvalues to evaluate the familiar Gaussian sum

$$S = \sum_{n=1}^{q} e^{2\pi in^2/q},$$

which is the trace of the matrix $\mathfrak{A}$.

The eigenvectors we give arise from the characters of the reduced residue class group modulo q. We begin by recalling a few well-known facts about characters; these can be found in Hasse [2, Sects. 13, 20].

Let χ be a character modulo q. The least positive divisor $f = f(\chi)$ of q with the property that

$$\chi(n) = 1 \qquad \text{for every } n \equiv 1 \pmod f \text{ for which } (n, q) = 1,$$

is called the conductor of χ. The character χ can be uniquely defined on the integers m relatively prime to f if one sets

$$\chi(m) = \chi(n), \qquad \text{where} \qquad m \equiv n \pmod f \text{ and } (n, q) = 1.$$

* The author was a National Science Foundation Predoctoral Fellow at the time this article was written. The author's present address is: Department of Mathematics, California Institute of Technology, Pasadena, California 91125.

0022-314X/80/010122-06$02.00/0

With this definition χ becomes a character modulo f. In this note we always consider χ defined modulo its conductor, and we set

$$\chi(n) = 0 \quad \text{if} \quad (n, f(\chi)) > 1.$$

We shall also need the main properties of the Gaussian sum

$$\tau(\chi) = \sum_{r=1}^{f} \chi(r)\, e^{2\pi i r/f} \tag{2}$$

associated with χ. We have that

$$\tau(\chi)\,\tau(\bar{\chi}) = \chi(-1)\, f(\chi), \tag{3}$$

and

$$\sum_{r=1}^{f} \chi(r)\, e^{2\pi i a r/f} = \bar{\chi}(a)\,\tau(\chi), \qquad \text{for any integer } a. \tag{4}$$

Finally, we recall the orthogonality property

$$\begin{aligned} \sum_{\substack{n=1 \\ (n,q)=1}}^{q} \chi(n)\,\bar{\psi}(n) &= 0 \qquad \text{if} \quad \chi \neq \psi, \\ &= \phi(q) \qquad \text{if} \quad \chi = \psi, \end{aligned} \tag{5}$$

where χ and ψ are any characters (mod q) and ϕ is the Euler ϕ-function.

We now define a q-dimensional vector X_d for every character χ and every divisor d of $q/f(\chi)$. Let the nth component of X_d be

$$\begin{aligned} X_d(n) &= \chi(n/d) \qquad \text{if} \quad d \mid n, \\ &= 0 \qquad \text{if} \quad d \nmid n, \qquad \text{for} \quad 1 \leqslant n \leqslant q. \end{aligned} \tag{6}$$

For each character χ there are $d(q/f)$ such vectors, where $d(n)$ is the number of divisors of n. If $p(f)$ is the number of characters with conductor f, we see that there are in all

$$\sum_{f \mid q} p(f)\, d(q/f) = \sum_{d \mid q} \sum_{f \mid q/d} p(f)$$

such vectors. Since there are exactly $\phi(q/d)$ characters (mod q/d), and since every character with conductor dividing q/d gives rise to a character (mod q/d), it follows that the total number of vectors is equal to

$$\sum_{d \mid q} \phi(q/d) = q.$$

We now prove the following

LEMMA. *The q vectors X_d are independent.*

Proof. Assume that

$$\sum_{\chi} \sum_{d|q/f(\chi)} c_{\chi,d} X_d = 0,$$

where the first sum ranges over all the characters (mod q). From (6) we then have that

$$\sum_{\chi} \sum_{\substack{d|q/f \\ d|n}} c_{\chi,d}\chi(n/d) = 0 \qquad \text{for} \quad 1 \leqslant n \leqslant q. \tag{7}$$

If n is relatively prime to q, then (7) reduces to

$$\sum_{\chi} c_{\chi,1}\chi(n) = 0. \tag{8}$$

We now multiply through in (8) by $\bar{\psi}(n)$, where ψ is any character (mod q), and we sum over the reduced residues (mod q). By (5) this gives

$$0 = \sum_{\chi} c_{\chi,1} \sum_{(n,q)=1} \chi(n)\, \bar{\psi}(n) = \phi(q)\, c_{\psi,1}$$

Hence $c_{\chi,1} = 0$ for every χ.

Now let d_1 be any divisor of q and assume that $c_{\chi,d} = 0$ for all the divisors d of q which are less than d_1. Let m be any integer satisfying

$$1 \leqslant m \leqslant q/d_1 \qquad \text{and} \qquad (m, q/d_1) = 1. \tag{9}$$

If we set $n = md_1$ and note $(n, q) = d_1$, then by (7) and the inductive assumption we have

$$\sum_{\substack{\chi \\ f(\chi)|q/d_1}} c_{\chi,d_1}\chi(m) = 0. \tag{10}$$

This sum is over all the characters which are defined modulo q/d_1. If we multiply through in (10) by $\bar{\psi}(m)$, where ψ is any character (mod q/d_1), and sum over the integers m in (9), then we find from (5) as before that $c_{\chi,d_1} = 0$ for every χ with $f(\chi) \mid q/d_1$.

It now follows by induction that $c_{\chi,d} = 0$ for all χ and d, and this implies the assertion of the lemma.

In order to give a basis for the eigenvectors of $\mathfrak{A}$ we first compute the vectors $\mathfrak{A}X_d$. From (1) and (6) we see that the mth component of $\mathfrak{A}X_d$ is

$$\sum_{\substack{n=1\\ d|n}}^{q} e^{2\pi i mn/q}\chi(n/d) = \sum_{n=1}^{q/d} e\left(\frac{mn}{q/d}\right)\chi(n) \qquad (e(\theta) = e^{2\pi i\theta})$$

$$= \sum_{r=1}^{f} \chi(r) \sum_{k=0}^{q/fd-1} e\left(\frac{m(r+kf)}{q/d}\right)$$

$$= \sum_{r=1}^{f} \chi(r)\, e\left(\frac{mr}{q/d}\right) \cdot \sum_{k=0}^{q/fd-1} e\left(\frac{mk}{q/fd}\right)$$

$$= 0, \qquad \text{if} \quad q/fd \nmid m$$

$$= \frac{q}{fd}\sum_{r=1}^{f} \chi(r)\, e\left(\frac{r}{f}\,\frac{mdf}{q}\right), \qquad \text{if} \quad q/fd \mid m. \tag{11}$$

By (4) the last expression is equal to

$$\frac{q}{fd}\,\bar{\chi}\left(\frac{mdf}{q}\right)\tau(\chi);$$

thus (11) and (6) give that

$$\mathfrak{A}X_d = \frac{q}{fd}\,\tau(\chi)\,\bar{X}_{q/fd}\,. \tag{12}$$

Using (12) we may write down a basis for the eigenvectors of $\mathfrak{A}$. If χ is real and $d^2 = q/f$, then (12) implies that X_d is an eigenvector of $\mathfrak{A}$ corresponding to the eigenvalue $(q/f)^{1/2}\,\tau(\chi)$. Otherwise let $\lambda = \pm(\chi(-1)q)^{1/2}$, and consider the vector

$$E(\chi, d, \lambda) = d^{1/2}X_d + \frac{\lambda}{\tau(\bar{\chi})\, d^{1/2}}\,\bar{X}_{q/fd}\,. \tag{13}$$

By the lemma $E(\chi, d, \lambda) \neq 0$, and by (12) and (3) we have

$$\mathfrak{A}E(\chi, d, \lambda) = \frac{q}{f\,d^{1/2}}\,\tau(\chi)\,\bar{X}_{q/fd} + \frac{\lambda}{\tau(\bar{\chi})\,d^{1/2}}\,d\tau(\bar{\chi})\,X_d$$

$$= \lambda\left(d^{1/2}X_d + \frac{q\tau(\chi)}{\lambda f\, d^{1/2}}\,\bar{X}_{q/fd}\right)$$

$$= \lambda E(\chi, d, \lambda).$$

Thus $E(\chi, d, \lambda)$ is an eigenvector of $\mathfrak{A}$ corresponding to the eigenvalue λ.

An easy computation using (13) shows that

$$E(\bar{\chi}, q/fd, \lambda) = W(\chi, \lambda)\,E(\chi, d, \lambda), \tag{14}$$

where $W(\chi, \lambda) = [\lambda/\tau(\chi)](f/q)^{1/2}$. Since $|\tau(\chi)| = f^{1/2}$, $W(\chi, \lambda)$ has absolute value 1, and $E(\chi, d, \lambda)$ and $E(\bar{\chi}, q/fd, \lambda)$ are dependent vectors. However the lemma implies easily that (14) is the only set of dependence relations between the vectors given in (13). It follows that a quadruple $(\chi, \bar{\chi}, d, q/fd)$ contributes the independent eigenvectors

$$\begin{aligned} &E(\chi, d, \pm(\chi(-1)q)^{1/2}),\ E(\bar{\chi}, d, \pm(\chi(-1)q)^{1/2}), \quad \text{if } \chi \neq \bar{\chi},\ d^2 \neq q/f; \\ &E(\chi, d, \pm(\chi(-1)q)^{1/2}), \quad \text{if } \chi \neq \bar{\chi},\ d^2 = q/f \text{ or } \chi = \bar{\chi},\ d^2 \neq q/f; \\ &X_d, \quad \text{if } \chi = \bar{\chi} \text{ and } d^2 = q/f. \end{aligned} \tag{15}$$

By pairing the eigenvectors in (15) with the pairs (χ, d) $(d \mid q/f(\chi))$, it is easy to see that the total number of eigenvectors listed in (15) is

$$\sum_{\chi} \sum_{d \mid q/f(\chi)} 1 = \sum_{f \mid q} p(f)\, d(q/f) = q.$$

Hence we have the following result.

THEOREM. *The vectors listed in* (15) (*with* X_d *and* $E(\chi, d, \lambda)$ *defined by* (6) *and* (13)) *form a basis of eigenvectors for* $\mathfrak{A}$. *The respective eigenvalues are*

$$\pm(\chi(-1)\,q)^{1/2},\ \pm(\chi(-1)\,q)^{1/2},\ \textit{and}\ \left(\frac{q}{f}\right)^{1/2} \tau(\chi),$$

where $\tau(\chi)$ *is given by* (2).

We note the following corollary of the theorem, which is a consequence of the fact that the trace of $\mathfrak{A}$ is equal to the sum of its eigenvalues:

$$S = \sum_{n=1}^{q} e^{2\pi i n^2/q} = q^{1/2} \sum_{\substack{\chi = \bar{\chi} \\ q/f(\chi) = \text{square}}} \frac{\tau(\chi)}{f^{1/2}(\chi)}\,.$$

This can also be proved directly.

Similar results can also be proved for the matrix

$$\mathfrak{A}' = (e^{2\pi i S(xy\eta)}) \qquad (x, y \pmod{\mathfrak{q}}),$$

where S denotes the trace from a fixed algebraic number field K to Q, $\mathfrak{q}$ is some integral divisor of K, x and y are integers of K which run through a complete residue system (mod $\mathfrak{q}$), and η satisfies

$$\eta \cong \frac{\mathfrak{n}}{\mathfrak{q}\mathfrak{d}}, \qquad (\mathfrak{n}, \mathfrak{q}\mathfrak{d}) = 1,$$

where $\mathfrak{d}$ is the different of K/Q and $\mathfrak{n}$ is an integral divisor in K. As before, the eigenvectors of $\mathfrak{A}'$ arise from the characters on the reduced residue class group (mod $\mathfrak{q}$) in K.

ACKNOWLEDGMENT

Finally, I would like to thank Professor H. Montgomery for suggesting this problem to me.

REFERENCES

1. L. CARLITZ, Some cyclotomic matrices, *Acta Arith.* 5 (1959), 293–308.
2. H. HASSE, "Vorlesungen über Zahlentheorie," Springer-Verlag, Berlin, 1964.
3. I. SCHUR, Über die Gaußschen Summen, "Gesammelte Abhandlungen II," pp. 327–333, Springer-Verlag Berlin, 1973.