IJMMS 25:3 (2001) 167–173
PII. S016117120100480X
http://ijmms.hindawi.com

NOTE ON THE QUADRATIC GAUSS SUMS

GEORGE DANAS

(Received 17 March 2000)

ABSTRACT. Let p be an odd prime and $\{\chi(m) = (m/p)\}$, $m = 0,1,\dots,p-1$ be a finite arithmetic sequence with elements the values of a Dirichlet character $\chi \bmod p$ which are defined in terms of the Legendre symbol (m/p), $(m,p) = 1$. We study the relation between the Gauss and the quadratic Gauss sums. It is shown that the quadratic Gauss sums $G(k;p)$ are equal to the Gauss sums $G(k,\chi)$ that correspond to this particular Dirichlet character χ. Finally, using the above result, we prove that the quadratic Gauss sums $G(k;p)$, $k = 0,1,\dots,p-1$ are the eigenvalues of the circulant $p \times p$ matrix X with elements the terms of the sequence $\{\chi(m)\}$.

2000 Mathematics Subject Classification. Primary 11L05; Secondary 11T24, 11L10.

1. Introduction. The notions of Gauss and quadratic Gauss sums play an important role in number theory with many applications [10]. In particular, they are used as tools in the proofs of quadratic, cubic, and biquadratic reciprocity laws [5, 7].

In this article, we study the relation between the quadratic Gauss sums and the Gauss sums related to a particular Dirichlet character defined in terms of the Legendre symbol and prove that the Gauss sums $G(k,\chi)$, $k = 0,1,\dots,p-1$ which correspond to the Dirichlet character $\chi(m) = (m/p)$ are actually the quadratic Gauss sums $G(k;p)$, $(k,p) = 1$.

More precisely, consider the finite arithmetic sequence $\{\chi(m) = (m/p)\}$ with elements the values of a Dirichlet character $\chi \bmod p$ which are defined in terms of the Legendre symbol (m/p), $(m,p) = 1$ and a circulant $p \times p$ matrix X with elements these values. If $f(x)$ is a polynomial of degree $p-1$ with coefficients the elements of the arithmetic sequence $\{\chi(m)\}$, $m = 0,1,\dots,p-1$, then $X = f(T)$, where T is a suitable $p \times p$ circulant matrix, namely the rotational matrix; T is orthogonal, diagonalizable with eigenvalues the pth roots of unity. In addition, the matrices X,T have the same eigenvectors while if λ is an eigenvalue of T, then $f(\lambda)$ is the eigenvalue of X that corresponds to the same eigenvector [3, 12, 13].

Finally, using the above results, we give an algebraic interpretation of the quadratic Gauss sums, which also leads to a different way of computing them, by proving that they are the eigenvalues of the circulant $p \times p$ matrix X.

2. Preliminaries. For an extended overview on eigenvalues and eigenvectors the reader may consult [4, 8, 11] while for quadratic residues, Legendre symbol, character functions, and Dirichlet characters [1, 5, 7].

Let $\mathbb{C}$ be the set of complex numbers, A an $n\times n$ matrix with entries in $\mathbb{C}$ and

$$f(x) = a_nx^n + \cdots + a_1x + a_0, \quad a_i \in \mathbb{C},\ i = 0,1,\ldots,n \tag{2.1}$$

be a polynomial of degree n, where n is an integer greater than 1.

Proposition 2.1. *If λ is an eigenvalue of the $n\times n$ matrix A that corresponds to the eigenvector v, then the $n\times n$ matrix*

$$f(A) = a_nA^n + \cdots + a_1A + a_0I_n \tag{2.2}$$

has

$$f(\lambda) = a_n\lambda^n + \cdots + a_1\lambda + a_0 \tag{2.3}$$

as an eigenvalue that corresponds to the same eigenvector v.

Corollary 2.2. *If*

$$P_A(\lambda) = (\lambda-\lambda_1)\cdots(\lambda-\lambda_n) \tag{2.4}$$

is the characteristic polynomial of the matrix A with eigenvalues $\lambda_1,\ldots,\lambda_n$, then

$$P_{f(A)}(\lambda) = (\lambda - f(\lambda_1))\cdots(\lambda - f(\lambda_n)) \tag{2.5}$$

is the characteristic polynomial of the matrix $f(A)$.

Proposition 2.3. *If an $n\times n$ matrix A has n distinct eigenvalues, then so has the matrix $f(A)$. Moreover, if the matrix A is diagonalized by an $n\times n$ matrix S, then $f(A)$ is also diagonalized by S.*

Definition 2.4. Let m be an integer greater than 1, and suppose that $(m,n) = 1$. If $x^2 \equiv n \mod m$ is soluble, then we call n a quadratic residue $\mod m$; otherwise we call n a quadratic nonresidue $\mod m$.

Definition 2.5 (Legendre's symbol)**.** Let p be an odd prime, and suppose that $p \nmid n$. We let

$$\left(\frac{n}{p}\right) = \begin{cases} 1 & \text{if } n \text{ is a quadratic residue} \mod p, \\ -1 & \text{if } n \text{ is a quadratic nonresidue} \mod p. \end{cases} \tag{2.6}$$

It is easy to see that if $n \equiv n' \mod p$ and $p \nmid n$, then $(n/p) = (n'/p)$ which implies that the Legendre symbol is periodic with period p.

Let now $\{a_i\}$, $i = 0,1,\ldots,n-1$ be a finite arithmetic sequence in $\mathbb{C}$.

Definition 2.6. An $n\times n$ matrix

$$A = \begin{pmatrix} a_0 & a_1 & \cdot & \cdot & a_{n-1} \\ a_{n-1} & a_0 & \cdot & \cdot & a_{n-2} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ a_1 & a_2 & \cdot & \cdot & a_0 \end{pmatrix} \tag{2.7}$$

whose rows come by cyclic permutations to the right of the terms of the arithmetic sequence $\{a_i\}$, $i = 0,1,\ldots,n-1$ is called a circulant matrix.

In case that

$$a_i = \begin{cases} 1 & \text{if } i = 1, \\ 0 & \text{otherwise,} \end{cases} \tag{2.8}$$

the matrix A becomes

$$T = \begin{pmatrix} 0 & 1 & 0 & \cdot & \cdot & 0 \\ 0 & 0 & 1 & \cdot & \cdot & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & \cdot & 0 & 1 \\ 1 & 0 & 0 & \cdot & \cdot & 0 \end{pmatrix}. \tag{2.9}$$

The $n \times n$ matrix T, which is called the rotational matrix, is orthogonal, that is, $T^{-1} = T'$, such that $T^n = I_n$ and having as eigenvalues the nth roots of unity [3, 12]. Moreover, T is diagonalizable and if W is the $n \times n$ matrix whose columns are the eigenvectors of T,

$$W^{(k)} = \left(1 w^k w^{2k} \cdots w^{(n-1)k}\right)', \quad k = 0, 1, \ldots, n-1, \tag{2.10}$$

where $w = e^{2\pi i/n}$, then

$$W^{-1}TW = \begin{pmatrix} 1 & 0 & 0 & \cdot & \cdot & 0 \\ 0 & w & 0 & \cdot & \cdot & 0 \\ 0 & 0 & w^2 & \cdot & \cdot & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & \cdot & \cdot & w^{n-1} \end{pmatrix}. \tag{2.11}$$

3. Gauss and quadratic Gauss sums. In this section, we study the relation between the quadratic Gauss sums and the Gauss sums related to a particular Dirichlet character defined in terms of the Legendre symbol.

Definition 3.1. For every Dirichlet character $\chi \bmod n$ the sum

$$G(k, \chi) = \sum_{m=0}^{n-1} \chi(m) e^{2\pi i m k/n}, \quad k = 0, 1, \ldots, n-1, \tag{3.1}$$

is called the Gauss sum that corresponds to χ.

Definition 3.2. If k, n are integers with $n > 0$, then the trigonometric sum

$$G(k; n) = \sum_{r=0}^{n-1} e^{2\pi i r^2 k/n}, \quad (k, n) = 1, \tag{3.2}$$

is called quadratic Gauss sum.

Theorem 3.3. *If p is an odd prime with $\chi(m) = (m/p)$, $(m,p) = 1$, then*

$$G(k;p) = \sum_{r=0}^{p-1} e^{2\pi i r^2 k/p} = \sum_{m=0}^{p-1} \chi(m) e^{2\pi i m k/p} = G(k,\chi), \quad (k,p) = 1, \tag{3.3}$$

Proof. The number of solutions of the congruence

$$r^2 \equiv m \bmod p \tag{3.4}$$

is

$$1 + \left(\frac{m}{p}\right) \tag{3.5}$$

and therefore

$$\begin{aligned} G(k;p) &= \sum_{r=0}^{p-1} e^{2\pi i r^2 k/p} = \sum_{m=0}^{p-1} \left(1 + \left(\frac{m}{p}\right)\right) e^{2\pi i m k/p} \\ &= \sum_{m=0}^{p-1} \left(\frac{m}{p}\right) e^{2\pi i m k/p} = \sum_{m=0}^{p-1} \chi(m) e^{2\pi i m k/p} = G(k,\chi) \end{aligned} \tag{3.6}$$

which is the required result. □

4. The quadratic Gauss sums as eigenvalues of a suitable circulant matrix. In this section, we give an algebraic interpretation of the quadratic Gauss sums that correspond to a Dirichlet character $\chi \bmod p$ which is defined in terms of the Legendre symbol (m/p), $(m,p) = 1$. In fact, we prove that the quadratic Gauss sums $G(k;p)$, $(k,p) = 1$, are the eigenvalues of the circulant $p \times p$ matrix X with elements the values $\chi(m) = (m/p)$, $(m,p) = 1$.

Let now $n = p$ be an odd prime, $\chi(m) = (m/p)$ be a Dirichlet character $\bmod p$ that is defined in terms of the Legendre symbol (m/p), $(m,p) = 1$ and consider the circulant $p \times p$ matrix

$$X = \begin{pmatrix} \chi(0) & \chi(1) & \cdot & \cdot & \chi(p-1) \\ \chi(p-1) & \chi(0) & \cdot & \cdot & \chi(p-2) \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \chi(1) & \chi(2) & \cdot & \cdot & \chi(0) \end{pmatrix} \tag{4.1}$$

whose rows come by cyclic permutation to the right of the terms of the arithmetic sequence $\{\chi(m)\}$, $m = 0,1,\dots,p-1$.

Proposition 4.1. *If $f(x) = \chi(0) + \chi(1)x + \cdots + \chi(p-1)x^{p-1}$ is a polynomial with coefficients the terms of the arithmetic sequence $\{\chi(m)\}$, $m = 0,1,\dots,p-1$, then $X = f(T)$.*

Proof. We can write $T = (e_p e_1 \cdots e_{p-1})$, since the columns of T are the vectors $e_p, e_1, \dots, e_{p-1}$ relative to the standard basis of $\mathbb{C}^p$.

Observe also that

$$T^2 = (e_{p-1} e_p \cdots e_{p-2}), \ \dots, \ T^p = (e_1 e_2 \cdots e_p) = I_p. \tag{4.2}$$

Therefore,

$$\begin{aligned} f(T) &= \chi(0)I_p + \chi(1)T + \cdots + \chi(p-1)T^{p-1} \\ &= \chi(0)(e_1e_2\cdots e_p) + \chi(1)(e_pe_1\cdots e_{p-1}) + \cdots + \chi(p-1)(e_2e_3\cdots e_1) \\ &= \begin{pmatrix} \chi(0) & \chi(1) & \cdot & \cdot & \chi(p-1) \\ \chi(p-1) & \chi(0) & \cdot & \cdot & \chi(p-2) \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \chi(1) & \chi(2) & \cdot & \cdot & \chi(0) \end{pmatrix} = X. \end{aligned} \tag{4.3}$$

□

Thus, according to Proposition 2.1, the matrix X has the same eigenvectors with T, which are the row vectors

$$v_0 = (11\cdots 1),\ v_1 = (1w\cdots w^{p-1}),\ \ldots,\ v_{p-1} = \left(1w^{p-1}\cdots w^{(p-1)^2}\right), \tag{4.4}$$

where $w = e^{2\pi i/p}$, while its corresponding eigenvalues are

$$\begin{aligned} f(1) &= \chi(0) + \chi(1) + \cdots + \chi(p-1) \\ f(w) &= \chi(0) + \chi(1)w + \cdots + \chi(p-1)w^{p-1} \\ f(w^2) &= \chi(0) + \chi(1)w^2 + \cdots + \chi(p-1)w^{2(p-1)} \\ &\vdots \\ f(w^{p-1}) &= \chi(0) + \chi(1)w^{p-1} + \cdots + \chi(p-1)w^{(p-1)^2}. \end{aligned} \tag{4.5}$$

Combining now the above results and Theorem 3.3, we obtain the following theorem.

Theorem 4.2. *The eigenvalues of the $p\times p$ circulant matrix X are*

$$G(k;p) = G(k,\chi) = f(w^k) = \sum_{m=0}^{p-1} \chi(m)e^{2\pi imk/p}, \quad k = 0,1,\ldots,p-1, \tag{4.6}$$

the quadratic Gauss sums.

Notice that, equations (4.5) can be written in matrix notation as

$$\begin{pmatrix} f(1) \\ f(w) \\ f(w^2) \\ \cdot \\ \cdot \\ f(w^{p-1}) \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & \cdot & \cdot & 1 \\ 1 & w & w^2 & \cdot & \cdot & w^{p-1} \\ 1 & w^2 & w^4 & \cdot & \cdot & w^{2(p-1)} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 1 & w^{p-1} & w^{2(p-1)} & \cdot & \cdot & w^{(p-1)^2} \end{pmatrix} \begin{pmatrix} \chi(0) \\ \chi(1) \\ \chi(2) \\ \cdot \\ \cdot \\ \chi(p-1) \end{pmatrix}. \tag{4.7}$$

Furthermore, the $p\times p$ matrix

$$W = \begin{pmatrix} 1 & 1 & 1 & \cdot & \cdot & 1 \\ 1 & w & w^2 & \cdot & \cdot & w^{p-1} \\ 1 & w^2 & w^4 & \cdot & \cdot & w^{2(p-1)} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 1 & w^{p-1} & w^{2(p-1)} & \cdot & \cdot & w^{(p-1)^2} \end{pmatrix} \tag{4.8}$$

whose columns are the eigenvectors of X, diagonalize X, that is,

$$W^{-1}XW = \begin{pmatrix} f(1) & 0 & 0 & \cdot & \cdot & 0 \\ 0 & f(w) & 0 & \cdot & \cdot & 0 \\ 0 & 0 & f(w^2) & \cdot & \cdot & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & \cdot & \cdot & f(w^{p-1}) \end{pmatrix}. \tag{4.9}$$

Remark 4.3. Since every Dirichlet character χ $\bmod p$ is periodic $\bmod p$, it has a finite Fourier expansion [1, 7],

$$\chi(m) = \sum_{k=0}^{p-1} \alpha_p(k) e^{2\pi imk/p}, \quad m = 0,1,\dots,p-1, \tag{4.10}$$

where the coefficients $\alpha_p(k)$ are given by

$$\alpha_p(k) = \frac{1}{p}\sum_{m=0}^{p-1} \chi(m) e^{-2\pi imk/p}, \quad k = 0,1,\dots,p-1 \tag{4.11}$$

or equivalently

$$\alpha_p(k) = \frac{1}{p} G(-k,\chi). \tag{4.12}$$

If we consider now the Dirichlet character $\chi(m) = (m/p)$ which is defined in terms of the Legendre symbol (m/p), $(m,p) = 1$, then we deduce that the quadratic Gauss sum $G(k;p) = G(k,\chi)$, $k = 0,1,\dots,p-1$ is the Fourier transform of χ evaluated at k.

5. Conclusion. We have shown that the quadratic Gauss sums $G(k;p)$, $(k,p) = 1$ can be considered as the eigenvalues of a suitable circulant $p \times p$ matrix X with elements the terms of the arithmetic sequence $\{\chi(m) = (m/p)\}$. This leads both to an algebraic characterization and also to a different way of computing the quadratic Gauss sums by calculating the roots of the characteristic polynomial that correspond to the matrix X.

Moreover, this new point of view for the quadratic Gauss sums gives, in many cases, an easier way to calculate them (to my best knowledge) instead of a direct computation, since one can find several methods for computing the eigenvalues of a matrix or the roots of a polynomial [2, 6, 9].

References

[1] T. M. Apostol, *Introduction to Analytic Number Theory*, Undergraduate Texts in Mathematics, Springer-Verlag, New York, Heidelberg, 1976. MR 55#7892. Zbl 335.10001.

[2] Å. Björck and G. Dahlquist, *Numerical Methods*, Translated from the Swedish by Ned Anderson. Prentice-Hall Series in Automatic Computation, Prentice-Hall, Inc., Englewood Cliffs, N.J., 1974. MR 51#4620.

[3] P. J. Davis, *Circulant Matrices*, A Wiley-Interscience Publication. Pure and Applied Mathematics, John Wiley & Sons, New York, Chichester, Brisbane, 1979. MR 81a:15003. Zbl 418.15017.

[4] W. Greub, *Linear Algebra*, 4th ed., Graduate Texts in Mathematics, no. 23, Springer-Verlag, New York, Berlin, 1975. MR 51#5615. Zbl 317.15002.

[5] K. F. Ireland and M. I. Rosen, *A Classical Introduction to Modern Number Theory.* Revised edition of *Elements of Number Theory*, Graduate Texts in Mathematics, vol. 84, Springer-Verlag, New York, Berlin, 1982. MR 83g:12001. Zbl 482.10001.

[6] M. L. James, G. M. Smith, and J. C. Wolford, *Applied Numerical Methods for Digital Computation*, Harper & Row, New York, 1985.

[7] S. Lang, *Algebraic Number Theory*, Addison-Wesley Publishing Co., Inc., Reading, Mass., London, Don Mills, Ont., 1970. MR 44#181. Zbl 211.38404.

[8] D. Lay, *Linear Algebra and its Applications*, Addison-Wesley, 1994.

[9] W. H. Press, B. P. Flannery, S. A. Teukolsky, and W. T. Vetterling, *Numerical Recipes in Pascal*, The art of scientific computing, Cambridge University Press, Cambridge, New York, 1989. MR 91a:65001. Zbl 698.65001.

[10] M. R. Schroeder, *Number Theory in Science and Communication.* With applications in cryptography, physics, biology, digital information, and computing, Springer Series in Information Sciences, vol. 7, Springer-Verlag, Berlin, New York, 1984. MR 85j:11003. Zbl 542.10001.

[11] G. E. Shilov, *Linear Algebra.* Revised English edition. Translated from the Russian and edited by Richard A. Silverman, Dover Publications, Inc., New York, 1977. MR 57#6043.

[12] H. Terzidis and G. Danas, *The spectral analysis of the discrete Fourier transform*, submitted.

[13] ______, *The spectral analysis of the periods of the inverses of integers*, J. Inst. Math. Comput. Sci. Comput. Sci. Ser. **10** (1999), no. 1, 61–69. CMP 1 704 539.

George Danas: Technological Educational Institution of Thessaloniki, School of Sciences, Department of Mathematics, P.O. Box 14561, GR-54101 Thessaloniki, Greece

E-mail address: gpd@math.auth.gr